Citrix NetScaler 1000V Release Notes

Citrix NetScaler 10.5-57.7
May 27, 2015

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

10.5-57.7

The release notes provides the changes or enhancements, issues that are fixed, and known issues that exist in Build 57.7. The list of known issues is cumulative, that is, it includes known issues that existed in previous builds and issues that are newly found in this build.

Release history:

- Build 57.7 (2015-05-18) (Current build)
- Build 56.15 (2015-03-30) Replaces: 56.12
- Build 55.8 (2015-02-02)
- Build 54.9 (2014-12-17)
- Build 53.9 (2014-11-14)
- Build 52.11 (2014-11-03)
- Build 51.10 (2014-11-03)
- Build 50.10 (2014-10-21)

Note:

- This build includes fixes for 18 issues that were known issues in the previous build of the NetScaler 10.5 release.
- These release notes do not document security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

Points to Note

The list of points to note available in Build 53.9.

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 54.9] [#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 54.9] [#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 reinstall the Web Interface on NetScaler version 10.5 by using OpenJDK1.7.

  [From Build 54.9] [#464854]

Fixed Issues

The issues addressed in Build 57.7.

AAA-TM

- When doing Kerberos authentication, the nskrb binary may leak memory for each transaction.

  [# 547284, 533888]

- When traffic domains are used with AAA-TM deployment, user login might fail at times during password change or password challenge messages.

  [# 551205]

Application Firewall

- The response for an XML GET request might be truncated if, in addition to any of the XML checks, the creditcard or safeobject checks are enabled for the application firewall profile.

[# 539777]

- URL Transformation, SSL VPN, and CVPN features leverage the application firewall processing engine and enforce the content-length check of the built-in dummy application firewall profile. For some transactions, this check truncates the processed data.

  [# 532338, 526029, 539487]

- A 64 bit memory leak in the application firewall module might lead to cache misses. The memory leak occurs when the cache is turned on and any of the advanced application firewall security checks are enabled. The application firewall memory leak is now fixed, and the fix resolves the interoperability issue with the cache module.

  [# 549466]

- Enabling the NetScaler application firewall XML Format check might block the contents of a response when the user accesses an embedded link in some applications. The response might be truncated even when the XML format check is deployed in a non-block mode.

  [# 528902, 558724]

Configuration Utility

- In the configuration utility, you cannot create a virtual server with port number 0.

  [# 547877]

High Availability

- In a high availability configuration, with failSafe mode enabled on the secondary node, the node might briefly become primary when restarted.

  [# 534795]

- After an HA configuration is stabilized from a “spilt brain” condition (both nodes primary), connections are not immediately synchronized between the current primary and the current secondary node. This latency might result in an HA failover.

  [# 537496]

Load Balancing

- IPv6 Support for HTTP based User Monitors

  You can now use IPv6 addresses in the following HTTP based user monitors:

  - StoreFront (SF)

  - AppController (APPC)

  - Web Interface Extended (WI)

  - NT LAN Manager (NTLM)

  [# 510111]

Networking

- In an active-active configuration with the sendToMaster parameter enabled, the backup nodes might not forward packets to the master node.

  [# 554336]

- $ is an invalid value for the port parameter of any extended ACL, but no error message appears if you specify this value. If, while using the configuration utility to configure an extended ACL, you set the port parameter to $, no error message appears, but the ACL is not configured.

  [# 383958, 411806]

Policy

- The default SSL virtual server configurations are disturbed, if HTTP callouts are configured on the NetScaler appliance.

  [# 551626]

SSL

- If a spike in traffic occurs while the NetScaler ADC is doing a DH-based handshake, some packets might be dropped, because a DH handshake consumes a high number of CPU cycles.

  [# 484525]

- If you run the "update ssl certkey" command to modify the certificate-key pair that is bound to a service group, a duplicate entry is seen for the same certificate key pair in the running configuration.

  [# 550138, 552436, 552701]

- In a NetScaler cluster setup, if we add a certificate with the subject name greater than 64 characters, then subsequent SSL certkey addition fails with the "No such certificate file exists" error even though the certkey file is present on all cluster nodes.

  [# 554917]

- In the configuration utility, when binding ciphers to an SSL virtual server, the order in which the ciphers are bound is reversed in the configuration file. For example, if ciphers were bound in order of a, b, c, and d, the configuration file shows the order as d, c, b, a.

  This issue is now fixed.

  [# 552812, 558824]

- If the backend service is of type SSL_TCP, SSL reuse handshake using SSLv3 with backend servers fails and the connection is terminated.

  [# 529471]

SureConnect

- SureConnect (SC) should be enabled on one entity. If you enable SC or configure SC policies on a load balancing virtual server, do not enable SC on any of the services or service groups that are bound to this virtual server. Doing so can result in

configuration loss during reboot or lead to inconsistent configuration across an HA pair.

[# 526782]

System

- The NetScaler Gateway floods the network with acknowledgement packets, sent from its VIP address, when merging the reassembly queue on the NetScaler appliance. The flood of packets causes a firewall outage.

  [# 545133, 550627]

- Data that the NetScaler VPX appliance sends to a TCP peer might be corrupted if the peer has sent a TCP Maximum Segment Size (MSS) value greater than 1460 bytes on a TCP connection that the appliance initiated.

  [# 549904, 503614, 532794, 543864, 548338, 552628]

- Enabling the AppFlow feature during a transaction causes the NetScaler appliance to fail.

  [# 547739, 527797, 531101]

- During the execution of the "nstrace.sh" script (from shell) or the "start nstrace" command (from CLI), when the trace file is rolled over, some packets might not be available in the trace. The number of packets that will be dropped from the trace is directly proportional to the traffic rate.

  [# 480258, 494482, 523853]

- If the NetScaler appliance receives a Websocket upgrade request, and an HTTP-body based policy is bound globally or to a virtual server, the appliance does not forward the request to server until a TCP FIN flag is received from the client.

  [# 536576, 549318]

- If an authentication policy is bound to NetScaler system global, authentication of weblog and auditlog services fails.

  [# 498025, 521636, 534432]

User Interface

- In certain cases, an attempt to add or bind a load balancing virtual server, service, or service group can fail if the internal ID assigned to the virtual server, service or service group conflicts with the internal ID of an existing virtual server, service, or service group.

  Workaround: Try creating the virtual server, service, or service group again.

  [# 516162, 358664, 538009, 540912, 542248, 542721, 546566, 549368]

Known Issues

The issues that exist in Build 57.7.

AAA-TM

- In NetScaler 9.3 and previous versions, the NetScaler ADC used a SNIP address as the source IP address for authentication requests unless the administrator configured a static route to a different interface. In NetScaler 10.1 and subsequent versions, the ADC uses the NSIP address as the source for authentication requests even when a static route points to a different interface.

  To force the ADC to use a SNIP (not the NSIP) as the source IP address in version 10.1 or later, you can set up a load balancing virtual server with an authentication service, and then configure that load balancing virtual server to perform the authentication.

  [# 457817]

- If AAA-TM is configured to use NTLM authentication, either by itself or as fallback when Kerberos is not available, the NetScaler ADC might become unresponsive when a user attempts to authenticate through NTLM.

  [# 492626]

- The NetScaler ADC AAA-TM user interface has a timeout of 20 seconds. If authentication through an external authentication server takes more than 20 seconds, the following message appears in the logs: "libaaa recv failed." This message does not indicate authentication failure or any other problem that affects users. It can safely be ignored.

  [# 437454]

- When AAA-TM logs users off after their sessions time out, the traffic management session associated with the user is not terminated. If the number of abandoned traffic management sessions exceeds internal limits, the NetScaler ADC might become unresponsive.

  [# 481876]

- Clients using RPC over HTTP cannot connect to Kerberos enabled sites through AAA-TM servers.

  [# 528693]

- The NetScaler implementation of Kerberos does not fully implement the kutil functionality. While this does not impact Kerberos authentication, it restricts some administrative tasks such as the ability to merge keytab files.

  [# 551091]

- When IBM Tivoli IdP is used for SAML authentication with NetScaler appliance as the service provider, there could be an issue with SAML assertion verification.

  [# 540396]

- Sharepoint documents do not open in Internet Explorer unless the traffic management fully qualified domain name (FQDN) is added to trusted sites.

  [# 528778]

Acceleration

- The classic-policy expression used by the default acceleration policy fails to identify an Internet Explorer browser whose signature does not comply with the IE user-agent string standards.

  [# 535130]

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).

  [# 483427]

Application Firewall

- A POST request with an attached word document is silently blocked by the application firewall for a customized application.

  [# 530277]

- In 10.5 builds, the application firewall does not support white space character in the name of the imported object. After upgrading a 9.3 build to a 10.5 build, an error message might be displayed when removing an imported object which has white space character in the name.

  [# 549954]

- When cookie consistency check is deployed in the proxing mode, the application firewall does not expire the cookies as expected. This occurs when the server sends the Set-cookie header without the domain information. Protected resources are vulnerable to access through reuse of these cookies after the session has expired.

  [# 548577]

- If the server sends less data than the amount specified in the Content-length header, the NetScaler application firewall might send a 9845 response and reset the connection.

  [# 506653]

- A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.

  [# 427798]

- For some malformed requests, the NetScaler application firewall log messages might not include the client IP address.

  [# 510006]

- 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.

  [# 489691]

- In the NetScaler configuration utility, after 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.

  [# 457954]

- If the user sends a request that contains the string "Javascript" without a non-alphanumeric delimeter, the Cross-Site Scripting check does not block the request. This is expected behavior. Without a delimiter, the keyword "Javascript" cannot trigger code execution and therefore poses no threat to the protected web application.

  [# 457926, 506333]

- In NetScaler 9.3, if there is a standalone application firewall license, the user is able to bind a classic application firewall policy to the load balancing virtual server. However, in NetScaler 10.1, the design is changed. If the load balancing feature is not licensed, binding a classic application firewall policy to the load balancing virtual server now results in an error message.

  [# 510509]

- The Skip operation for the application firewall learned rules might take longer than expected.

  [# 547978]

- The application firewall Graphical User Interface might display a warning when the Qualys signature file is uploaded to the NetScaler appliance. The transformation program that reads the input file is treating a warning message as an error.

  [# 547282]

- In the RDX Graphical User Interface (GUI), the deploy or skip operation might not work for application-firewall recommended learned rules that contain non-printable characters.

  [# 551621]

- If a server sends a large value for the viewstate attribute in its HTML response, this value might get truncated during application firewall processing and display an error: "view state MAC fail".

  [# 539487, 526029, 547104]

- During an upgrade of a NetScaler appliance from version 10.0 to version 10.1 (build 121.1 or subsequent), the default JSON content type is not automatically configured. The default JSON content type is configured when version 10.1 (build 121.1) is installed on new hardware or in a new VPX instance. To check whether your appliance or instance has the correct default setting, log onto the NetScaler command line and type the following command:

  show appfw JSONContentType

  If the default content type is configured, the command output is similar to the following example:

> show appfw JSONContentType

1) JSONContenttypevalue: "^application/json$" IsRegex: REGEX

Done

If it is not, the screen shows only the following:

> show appfw JSONContentType

Done

To add the default content type to the configuration, after upgrading to 10.1 (121.1), log onto the NetScaler command line, and then type the following commands to configure the default content type and verify the configuration:

add appfw JSONContentType ^application/json$ -isRegex REGEX

show appfw JSONContentType

[# 430014]

- The Graphical User Interface (GUI) for the NetScaler application firewall has significantly changed to provide enhanced user experience and remove browser plugin dependencies. The GUI steps in the current application firewall documents are in need of revision. Some of them do not match the new GUI display.

  [# 548432]

- 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.

  [# 466329]

- On a NetScaler ADC that has the application firewall enabled and the buffer overflow check configured to block, the following error message might appear in the logs: "Internal error: additional data generated after partial response <blocked>." This error message indicates that a partial response was sent before the remainder of the response was blocked.

  [# 498912]

- In the RDX Graphical User Interface (GUI), selecting the "Remove All Learned Data" action in the application firewall Learned Rules section might not remove the learned data for some of the security checks for the profile.

  [# 549255]

- The Perl script that parses and merges the application firewall signatures during schema version upgrade can cause Perl to crash on the NetScaler ADC. These crash files can fill up the space on the hard drive, preventing access to the Graphical User Interface.

  [# 532248]

- The customer's application does not work when the application firewall is deployed to inspect the request for security check violations. When the application firewall forwards the request to the backend server, the server responds with a 403 HTTP error code, indicating that it cannot properly validate the CORBA session, and sends the page without the expected data in the form fields. The root cause is under investigation.

  Workaround: Turn off form field tagging and credit card checks.

  [# 511254]

- 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.

  [# 472476, 418036]

Application firewall

- On the NetScaler ADC, if you use the configuration utility to change an action for the Content-type security check for an application firewall profile, the change is not reflected in the command line. The show command still shows the old action. Similarly, if use the command line to set the action, it might not be visible in the configuration utility.

  Workaround: Use the set command from the command line to configure actions for the Content-type security check.

  [# 524646]

Cache Redirection

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

  [# 442353]

Cisco RISE Integration

- If RISE feature is not enabled and we try to disable it, an error message is displayed for all the features.

  [# 513761]

- In a vPC-Direct deployment for RISE, shutting a (RISE) service on the N7k removes the component links from the static LA channel on the NetScaler. They are however still part of the port channel on the N7k and could result in dropped traffic. It is recommended that the administrator manually shut down the port channel as well, on the N7k, when the corresponding RISE service is shut down.

  [# 502591]

- Cisco RISE now supports the following commands:

  - show rise param

- set rise param

Following is the usage of the set rise param command:

set rise param [-directMode (ENABLED | DISABLED)] [-indirectMode (ENABLED | DISABLED)]

The show rise param command displays the current setting. For example,

RISE-MPX-194-80> show rise param

DirectMode: ENABLED IndirectMode: ENABLED

Done

[# 497410]

Citrix NetScaler 1000V

- Throughput fluctuates between 4.6Gbps to 5.0Gbps with NS1000V-5G license on KVM/

  [# 501120]

- Throughput fluctuates between 4.6 Gbps to 5.3 Gbps with NS1000V-5G license on an ESX.

  [# 501098]

- When the OFFLOAD option is enabled with the server IP and vPath IP in the same subnet, the first packet that NetScaler offloads is dropped by the virtual ethernet module (VEM).

  [# 443545]

CloudPlatform

- The NetScaler 10.5 release does not support Citrix CloudPlatform.

  [# 447834]

Cluster

- The "force cluster sync" operation takes a long time to execute for large NetScaler configurations.

  [# 525671]

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

  [# 480324]

- In a cluster setup, the "add ns httpProfile" command can fail after an upgrade from a NetScaler 10.1 build to a NetScaler 10.5 build. This happens because the NetScaler running configuration does not include the "add ns httpProfile" command, even though it is available in the NetScaler configuration file (ns.conf).

  [# 538489]

Command Line Interface

- The NetScaler command line interface exists abruptly upon executing the "show dns addRec -format old" command.

  [# 512526, 527066, 545578]

Configuration Utility

- If you use the Google Chrome browser to access the NetScaler configuration utility and use the browse button to select a local file, the selected file name displays in the respective field. However, if you click the Browse button again to select a different file, and then, cancel the operation, the previously selected file name is cleared from the field.

  [# 531567]

- You cannot use the configuration utility to add signatures to an existing application firewall profile using the wizard, if the application firewall policy is not globally bound.

  Workaround: Use the command line interface .

  [# 470941]

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

  [# 454246, 478532, 500166]

- When you use the XenMobile wizard to configure load balancing for XenMobile 10, the server certificates for the device management services being load balanced are not automatically bound for application management services also being load balanced. The server certificates for application management load balancing services must be manually bound during the wizard flow.

  [# 524762]

- 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.

  [# 486590]

- You cannot change the setting of Tag all VLANs option of a network interface (System > Network > Interface) by using the configuration utility for NetScaler VPX instances running on VMware ESX server.

  [# 494788, 513198]

- When you open a content switching policy in the configuration utility (Traffic Management > Content Switching > Policies), an editing window appears unexpectedly.

  [# 558656]

- When you use the local file upload option in the Upgrade Wizard, through Internet Explorer or Firefox, the browser does not display the progress of the file upload. Wait for the upload to complete, even though the browser might not seem to be responding.

[# 558465]

- The configuration utility does not display a No Policy button in the binding section of policy label configuration at System > AppFlow > Policy Labels.

  [# 558893]

- The Upgrade Wizard sometimes does not display a message when the appliance is rebooting. However, the NetScaler appliance reboots and the upgrade is successful.

  Workaround: Reload the NetScaler GUI through the browser.

  [# 557379]

- You cannot change the setting of the Tag all VLANs option of a network interface (System > Network > Interface) by using the configuration utility for NetScaler VPX instances running on Microsoft Hyper-V hypervisor.

  [# 513198]

- If you use a Chrome browser to access the NetScaler graphical user interface (GUI), the browser might display the Page Unresponsive error message.

  Workaround:

  If you are using a Windows computer, do the following:

  1. Right-click the shortcut icon that you use to open the Chrome browser, and select Properties from the pop-up menu.

  2. In the Google Chrome Properties dialog box, click the Shortcut tab and, in the Target field, append the following value: --disable-hang-monitor

  For example: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe --disable-hang-monitor" http://www.google.com

  3. Close all instances of the Chrome browser, and restart the Chrome browser.

  If you are using a MAC computer, do the following:

  1. Open the terminal.

  2. Launch the Chrome browser from the terminal and append the --disable-hang-monitor value, as follows:

  open -a /Applications/Google\ Chrome.app --args --disable-hang-monitor

  [# 400073, 401262]

- 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."

[# 466245, 475388]

- 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 cached object.

  [# 457623]

- In a cluster setup, the configuration utility does not allow you to bind IP addresses to a bridge group.

  Workaround: Use the equivalent CLI command (bind bridgegroup) to perform this operation.

  [# 519487]

- 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.

  [# 459906, 485041]

- 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.

  [# 485942]

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

  [# 452669, 391434, 453555, 453597, 478131, 479434, 481397, 502720]

- You cannot create load balancing virtual servers or NetScaler Gateway virtual servers with the same name pattern used for virtual servers created in the XenMobile wizards.

  [# 485698]

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

  [# 483421]

- 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.

  [# 414807]

Content Switching

- The netProfile configured on a load balancing (LB) virtual server does not work as expected if the LB virtual server is the target virtual server for a content switching virtual server.

  [# 536377]

- If MAC-mode is enabled on a load balancing virtual server that is associated with a content switching virtual server, you must enable MAC-based forwarding (MBF) explicitly by running the "enable ns mode MBF" command.

  [# 528717]

DNS

- When the NetScaler appliance receives a truncated DNS response from one of the configured name servers, it does not retry the request over TCP.

  [# 527780]

- In a large DNS deployment, using the GUI to display the large number of DNS records might cause a spike in which management CPU usage approaches 100%.

  [# 528024]

- A DNS key cannot be created by using the default units for the "Expires" or "Notification Period" fields.

  [# 512372]

Documentation

- The configuration utility's Welcome page prompts you to enter a SNIP address, but you do not have to configure a SNIP for NetScaler VPX on Azure. You can skip this step.

  [# 559971]

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.

  [# 475535]

GSLB

- If you rename a server associated with a GSLB service and then run the sync gslb command, the GSLB configuration might not synchronize with the other GSLB sites.

  Workaround:

  Manually update the server name in the other GSLB sites.

  [# 511994]

- You can incorrectly set the CIP option while using the NetScaler command line to add a canonical name (CNAME) based GSLB service. The CIP option is valid for IP-based GSLB services only.

  [# 510195]

- GSLB force sync option fails, if the following conditions are met:

  * The same load balancing (LB) monitor is bound to a GSLB service as well as other LB entities.

  * The server IP address already exists in the slave node under non-GSLB entity (the entity with same server IP address but with different server name) and the master node tries to synchronize the configuration.

  [# 530638, 506432]

- Loading a new location file that has a coordinate outside the correct range (-90 to +90 latitude or -180 to +180 longitude) can cause the appliance to fail.

  Recommendation: After loading any location file, use the command, “show locationparameters” to get a summary of the coordinates loaded and any parsing errors. The specific problems are reported in /var/log/ns.log.

  [# 550294]

High Availability

- When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) build 126.x, the updates made in the Webinterface.conf file are overwritten 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 "set ns param -internaluserlogin DISABLED" command.

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

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

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

  5. Reenable the "internaluserlogin" parameter with the "set ns param -internaluserlogin ENABLED" command.

  6. Save the configurations.

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

  [# 471294]

- In a high availability configuration, if a NetScaler packet processing engine (NSPPE) fails on the primary node, both the nodes might go into a warm reboot loop.

  [# 479666, 507519, 541503]

- In a high availability configuration with throughput based failover configured for an LA channel, failover might not happen when the maximum throughput of the LA channel falls below the configured threshold.

  [# 546938]

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".

  [# 440107, 440389]

Load Balancing

- If the load balancing (LB) feature is not licensed, and you try to enable an LB virtual server, an error message appears.

  [# 466094, 534755]

- If a NetScaler appliance sending a DNSSEC negative response over UDP is not able to include the required records (for example, SOA, NSECs, and RRSIG records) in the Authority section, the appliance might send a truncated response in the wrong packet format.

  [# 540965]

- If Single Sign-On (SSO) is enabled for POST requests that have a payload larger than 300MB, request packet accumulation can cause memory allocation failures, and SSO might also fail.

  Workaround: Do one of the following:

  1. Disable SSO if large POST requests are involved.

  2. Set the number of packets after which SSO is bypassed. The default is 16. That is, if a request exceeds 16 packets, SSO is bypassed.

  [# 551623]

- If you configure cookie persistence and custom cookie on a virtual server, and later change the name or IP address of the virtual server, persistence is not honored.

  [# 524079]

- The Citrix-WI-Extended monitor cannot be used if the Web Interface server is not set up for explicit authentication mode.

  [# 480852]

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

  [# 456144, 527395]

NetScaler Insight Center

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

  [# 414214]

- In some situations, the tables shown in the exported reports might not have borders.

  [# 471239]

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

  Workaround: The tabular representation displays the details.

  [# 484578]

- The HDX Insight dashboard might display the host delay value for XenDesktop 7.5 as zero.

  [# 505865]

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

  [# 446120]

- The error indicated by the following message can occur when you use an IE8 browser to access NetScaler Insight Center from XenDesktop 5.6 or XenApp 6.5:

  " Object does not support this property or method."

  [# 402105]

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

  [# 405936]

- 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.

  [# 405853]

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

  [# 486295]

- The NetScaler Insight Center configuration utility displays the following error message, if you navigate to Configuration > Inventory and choose a NetScaler IP address to view the Application list:

  Error in retrieving Virtual servers configuration.Get Virtual Server from NetScaler failed. Error in get NS resource.

  [# 514990, 523318]

NetScaler VPX Appliance

- NetScaler VPX release 10.5 is supported on XenServer versions 6.0 and later. When an instance of NetScaler VPX, which is provisioned on XenServer version 5.6 or earlier, is upgraded to release 10.5, the instance may become unresponsive after a restart.

  [# 456118]

- NetScaler VPX instances running on Hyper-V 2012 might consume a high percentage of CPU cycles while processing 2G traffic.

  [# 512284]

- NetScaler VPX cannot be directly imported into Hyper-V on Windows Server 2012 R2 using the "Import Virtual Machine" function of Hyper-V Manager.

  Workaround: Create the VPX instance by using the New > Virtual Machine function and connecting the "Dynamic.vhd" file from the Virtual Hard Disks directory which is present after unzipping the release image.

  Note: The newly created VPX instance MUST be configured with a minimum of 2GB memory and with 2 vcpus; setting the vcpus is done by changing the virtual machine settings after the instance is created, but before booting.

  [# 428107]

- A NetScaler that is deployed on the Hyper-V may crash or unexpectedly reboot if it uses three or more virtual interfaces in the VPX instance.

  [# 467734, 469552, 471601, 476833, 484210, 489880]

- In a high availability (HA) configuration on Amazon AWS, HA failover might not happen properly.

  Workaround: Warm restart the NetScaler VPX instances.

  [# 493725]

Networking

- RNAT source IP persistency is not supported on a virtual server configured for link load balancing.

  [# 546066]

- In an HA configuration in INC mode running the OSPF routing protocol, the secondary node drops all L3 traffic that has the destination that was advertised by the secondary node.

  [# 318684]

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

  [# 485385]

- 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.

  [# 455936]

- 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.

  [# 422858]

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

  [# 420198]

- 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.

  [# 470980]

- NetScaler VPX instances running on a XenServer/HyperV hypervisor do not support Link Layer Discovery Protocol (LLDP).

  [# 477413]

- Jumbo frames are not supported on NetScaler VPX appliances.

  [# 485905]

- 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-byte packets.

  [# 429006]

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

  [# 439294]

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

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

  [# 486131]

- 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 display Source IP Persistency as ENABLED for only one of these rules.

  [# 459679]

Platform

- Some AAA bindings are not found in the running configuration on rebooting VPX on ESX platform. However, these bindings are present in the ns.conf configuration file. This happens when the VPN virtual server's parameter UITHEME is set to CUSTOM. This issue is specific to VPX on ESX only.

  [# 524055]

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

  [# 402113]

- In rare conditions, a 10G interface might stop processing the traffic.

  Workaround: Reset the interface.

  [# 519000, 519041]

Policy

- If an HTTP message that includes invalid characters is processed by a rewrite action containing “XPATH_HTML_WITH_MARKUP()” in the target expression, the NetScaler appliance might fail.

  [# 557908]

- Some IP based expressions on the NetScaler appliance may not work for the IP addresses starting from octet 128 or greater (128.x.x.x - 254.x.x.x).

  [# 534244]

- If you enable USIP mode globally and configure an OSCP responder policy to talk to external OSCP servers, the HTTP callout functionality used by SSL OSCP uses a dummy IP address (127.128.129.130) by default. This might cause a TCP connection failure.

  Workaround: Disable USIP globally and enable USIP on each service, as required.

  [# 548829]

SSL

- On a NetScaler VPX, the configuration for binding the ECC curve to the SSL virtual server is lost when the appliance is restarted.

  [# 560175, 563831]

- A "certificate mismatch" error message appears if the order of certificates in the .pfx file is not as follows:

  - Server certificate (should be the first certificate in the file)

  - Intermediate certificate(s)

  - Root CA certificate

  The server key can be anywhere in the file.

  [# 535145]

- If you disable SSLv3 on the "nskrpcs-127.0.0.1-3009" service, an "ERROR: Operation not permitted" message appears even though SSLv3 has been successfully disabled on the service.

  [# 521569]

- If you try to add a certificate bundle with the complete path to a certificate-bundle 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

  [# 481878, 521933]

- 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.

  [# 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,

  > show ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]

  [# 402423]

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

  [# 455821]

- If you use the configuration utility to bind a cipher group to an SSL entity, individual ciphers in the group are bound instead of the group.

  Workaround: Use the command line to bind the cipher group.

  [# 564565]

System

- If the SSL offload feature is enabled, customers may experience latency when accessing certain websites.

  [# 539469]

- Syslog messages generated by user action are logged as error messages instead of informational messages.

  [# 538212]

- The virtual IP (VIP) address of a load balancing virtual server cannot be changed if the LB virtual server and syslog server have same configuration (ip, port, service) and use the same server information. In such cases, if the syslog server's IP address is changed, the syslog server uses different server information and does not update the server information used by the LB virtual server. As a result, the LB virtual server displays an error message when you try to change its VIP address.

  [# 522665]

- 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.

  [# 462557]

- 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

  [# 481008]

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

  [# 483524]

- The maximum memory that can be configured for an admin partition is 2048 MB. Setting a value greater than this means that the value is automatically truncated to 2048 MB. This memory limit is per packet engine of the NetScaler.

  [# 504426]

- FTP connections through a TCP wildcard virtual server on the NetScaler appliance might fail for one of the following reasons:

  - A mismatch in TCP parameters is preventing the appliance from reusing the probe connection.

  - The server is sending data before the client-side TCP connection is established.

  [# 545858]

- 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.

[# 427126, 441982, 452885, 456645]

- 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.

  [# 428209]

- 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.

  [# 431913]

- 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.

  [# 472833]

- 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.

  [# 447571]

- 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.

  [# 452382, 459464, 530627]

- When the time zone is changed, the updated time zone is shown in the configurations, but other processes use the time of the previous time zone. This can result in inconsistency in the system time.

  Workaround: Reboot the NetScaler appliance after changing the time zone.

  [# 527795]

- If the HTML injection feature is enabled, the NetScaler appliance injects JavaScript into responses sent to clients. If a subsequent request from one of the clients is generated from the JavaScript, the appliance responds with a 404 error.

  [# 518272]

User Interface

- The names of GSLB entities are case sensitive. If you have entities with the same name in different cases (uppercase or lowercase) on different nodes in your GSLB deployment, GSLB synchronization fails.

Workaround:

Change the entity names so that the same name is always in same case (either uppercase or lowercase).

[# 533475]

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 reinstall the Web Interface on NetScaler version 10.5 by using OpenJDK1.7.

  [# 464854]

- 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.

  [# 397150]

What's New in Previous 10.5 Builds

The enhancements and changes that were available in NetScaler 10.5 releases prior to Build 57.7. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

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]

- 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]

- 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]

- 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]

- When sending SAML Authentication request to external identity provider, the NetScaler ADC now offers an option to send the thumbprint of the certificate that was used to sign the message instead of sending the complete certificate. When the "sendThumbprint" option in SAML action is set to ON, the ADC allows putting the thumbprint in SAML auth request instead of the full X509 certificate. The "sendThumbprint" option is off by default.

  [From Build 54.9] [# 505673]

- SHA256 Signature and Digest Algorithms Support

  AAA now supports encrypted SAML assertions. The NetScaler implementation of SAML allows signing certificates of less than 2048 bits, but displays a warning message. It also supports the SHA256 hash algorithm for signatures and digests. Citrix recommends that all signing certificates be of at least 2048 bits, and that you use SHA256 as SHA-1 is no longer considered secure.

  [From Build 56.15] [# 440382, 457134]

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

- 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]

- 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]

- 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

- 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]

- 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]

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

  [From Build 50.10] [# 407100]

- Traffic domains are now supported on a NetScaler cluster.

  [From Build 50.10] [# 415065]

- MPTCP is now supported on a NetScaler cluster.

  [From Build 50.10] [# 423654]

- 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]

- 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]

- 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]

- GSLB support in a Cluster

  Global server load balancing can now be configured on a NetScaler cluster. To do this, you must log on to the cluster IP address to define the GSLB entities and then bind these entities to a a single member cluster node group.

  For detailed information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-cluster-gslb-con.html.

  [From Build 52.11] [# 326601]

- From NetScaler 10.5 Build 52.11, the cluster feature is licensed with the Platinum and Enterprise licenses. In earlier releases, the cluster feature was licensed by a separate cluster license file.

  Note:

  - If you have configured a cluster in an earlier build, the cluster will work with the separate cluster license file. No changes are required.

  - When you configure a new cluster in Build 52.11 and then downgrade to an earlier build, the cluster will not work as it now expects the separate cluster license file.

  [From Build 52.11] [# 486259]

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

- 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]

- 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]

- 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 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]

DNS

- 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]

- 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]

DataStream

- 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]

- 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]

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]

- Viewing the configuration details of the entities bound to a GSLB domain

  You can now view the configuration details of the entities bound to a GSLB domain. The details include the configuration of the virtual servers, services, and the monitors bound to the GSLB domain. To view the details, you can use either the command line or the configuration utility.

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

  [From Build 56.15] [# 343525]

Integrated Caching

- 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]

- Increased Metadata Cache Capacity

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

  [From Build 50.10] [# 417677]

Load Balancing

- 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]

- 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]

- 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]

- Uploading and Retrieving Files for NetScaler SDX Using NITRO

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

  [From Build 50.10] [# 408441]

- 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

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- You can now install NetScaler Insight Center on Microsoft Hyper-V version 6.2.

  [From Build 52.11] [# 463402]

- You can now limit the number of days for which the generated reports can persist in the database, after which the reports are permanently deleted.

  To change the value, on the Configuration tab, click System and in the right-pane from the System Settings group, click Limit Data Duration Persistency.

  [From Build 54.9] [# 521503]

- If you do not want the URL reports to be displayed on the Web Insight node of the dashboard, you can now disable the URL data collection settings.

  To modify the setting, on the Configuration tab, navigate to System, and in the right-pane, from the System Settings group, click Change URL Data Collection Settings.

  [From Build 54.9] [# 522345]

- NetScaler Insight Center now supports monitoring NetScaler appliances deployed in LAN user mode. The dashboard now displays the following user access types, depending on the NetScaler deployment:

  - Remote user: User connected to XenApp or XenDesktop server through a NetScaler Gateway.

  - Transparent mode user: User connected to XenApp or XenDesktop server directly, with no intervening virtual server.

  - LAN user: Internal user connected to XenApp or XenDesktop server directly, without configuring the routing rules on a NetScaler ADC.

  [From Build 56.15] [# 490147, 482900]

Networking

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- 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]

- vPath feature is available for all the NetScaler platforms from version 10.5 Build 52.11 onwards. To use this feature no special license file is required. For more information on vPath, see http://support.citrix.com/proddocs/topic/netscaler-vpx-10-5/ns-vpath-con.html

  [From Build 52.11] [# 416393]

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

- 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]

- 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]

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 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]

- 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]

- 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]

- 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]

- Display HSM Model Number

  The output of the "show fips" command now displays the HSM model number as shown below. This is especially helpful if you are conducting an audit of the FIPS card in a NetScaler appliance and cannot open the appliance without voiding the warranty.

  > sh fips

  FIPS HSM Info:

  HSM Label : NetScaler FIPS

  Initialization : FIPS-140-2 Level-2

  HSM Serial Number : 2.1G1037-IC000253

HSM State : 2

HSM Model : NITROX XL CN1620-NFBE

Hardware Version : 2.0-G

Firmware Version : 1.1

Firmware Release Date : Jun04,2010

Max FIPS Key Memory : 3996

Free FIPS Key Memory : 3994

Total SRAM Memory : 467348

Free SRAM Memory : 62580

Total Crypto Cores : 3

Enabled Crypto Cores : 3

Done

[From Build 52.11] [# 385499]

- Support for additional ciphers with TLS protocol version 1.2

  Twelve new ciphers are supported with TLS protocol version 1.2 on all MPX platforms, and on SDX platforms if an SSL chip is assigned to the instance when you provision it.

  1) Cipher Name: TLS1.2-AES128-GCM-SHA256

  Description: TLSv1.2 Kx=RSA Au=RSA Enc=AES-GCM(128) Mac=SHA-256

  2) Cipher Name: TLS1.2-AES256-GCM-SHA384

  Description: TLSv1.2 Kx=RSA Au=RSA Enc=AES-GCM(256) Mac=SHA-384

  3) Cipher Name: TLS1.2-DHE-RSA-AES128-GCM-SHA256

  Description: TLSv1.2 Kx=DH Au=RSA Enc=AES-GCM(128) Mac=SHA-256

  4) Cipher Name: TLS1.2-DHE-RSA-AES256-GCM-SHA384

  Description: TLSv1.2 Kx=DH Au=RSA Enc=AES-GCM(256) Mac=SHA-384

  5) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256

  Description: TLSv1.2 Kx=ECC-DHE Au=RSA Enc=AES-GCM(128) Mac=SHA-256

  6) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

  Description: TLSv1.2 Kx=ECC-DHE Au=RSA Enc=AES-GCM(256) Mac=SHA-384

  7) Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256

  Description: TLSv1.2 Kx=ECC-DHE Au=RSA Enc=AES(128) Mac=SHA-256

8) Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384

Description: TLSv1.2 Kx=ECC-DHE Au=RSA Enc=AES(256) Mac=SHA-384

9) Cipher Name: TLS1.2-AES-256-SHA256

Description: TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA-256

10) Cipher Name: TLS1.2-AES-128-SHA256

Description: TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA-256

11) Cipher Name: TLS1.2-DHE-RSA-AES-128-SHA256

Description: TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA-256

12) Cipher Name: TLS1.2-DHE-RSA-AES-256-SHA256

Description: TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA-256

[From Build 53.9] [# 460472]

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.

  For more information, see http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-sys-session-timeout-tsk.html.

  [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]

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

  [From Build 50.10] [# 406270]

- 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]

- 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]

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]

Fixed Issues in Previous 10.5 Builds

The issues that were addressed in NetScaler 10.5 releases prior to Build 57.7. The build number provided below the issue description indicates the build in which this issue was addressed.

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]

- The NetScaler SAML service provider (SP) feature now supports SiteMinder.

  [From Build 52.11] [# 488077]

- The AAA-TM SAML service provider (SP) now includes a parameter indicating the trust level assigned to a user authentication request in SAML redirects to the identity provider (IDP). This information enables the IDP to request appropriate authentication credentials.

  [From Build 52.11] [# 484933]

- 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 52.11] [# 480298]

- In forms-based single sign-on (SSO), if the designated response size is 0, the NetScaler ADC does not search for the complete response, as it normally would for responses with sizes above 0. It therefore fails to find the login form, and forms-based SSO authentication fails.

  [From Build 52.11] [# 493308]

- The NetScaler ADC no longer sets the NSC_TMAA session cookie during a secure load balancing virtual server session.

  [From Build 52.11] [# 474918, 502915]

- If the hostname that sends an incoming request does not match the domain configured on the authentication virtual server, the NetScaler ADC returns an HTTP 500 error. As a workaround, configure an authentication profile and include the hostname.

  [From Build 52.11] [# 488015]

- AAA now supports SAML HTTP Redirect bindings. These bindings include an HTTP Refresh command and target URL as a base64-encoded SAMLResponse query string parameter in a SAML HTTP GET response.

  [From Build 52.11] [# 482174]

- When AAA is configured to authenticate users to a Microsoft Sharepoint 2013 server by using NTLM, the user might be prompted to retype his or her credentials even though the user entered those credentials correctly. After the user retypes the credentials, he or she is logged on successfully. The issue is that initially the NetScaler ADC sends an incorrect domain to Sharepoint.

  [From Build 52.11] [# 476885]

- The NetScaler AAA SAML service provider (SP) does not send a SAML logout message to the SAML identity provider (IdP), so users who log onto SAML are unable to log off.

  [From Build 53.9] [# 501565]

- In the NetScaler configuration utility, filtering the active AAA sessions does not work if the filtering is based on Intranet IP addresses. All active AAA sessions are shown, regardless of IP address. With this fix, the configuration utility successfully displays only the AAA sessions active at the IP addresses that you specify.

  [From Build 53.9] [# 446755, 468475]

- The NetScaler SAMLIDP now offers 16 SAML attributes. Four options are available for configuring each of these attributes to include attribute name, attribute value, attribute friendly name, and attribute URI specification. You can use the Citrix default syntax expressions to set the attribute values.

  [From Build 53.9] [# 460680, 504703]

- As part of enhancement for Office365 integration, the NetScaler SAML IDP now sends Destination, SubjectConfirmationData, InResponseTo, and a Conditions section with an Audience field in the SAML Response.

  [From Build 53.9] [# 505951]

- The NetScaler ADC does not handle an authentication request if the incoming base64 decoded kerberos ticket is more than 10 kilobytes. This fix increases the buffer-size limit to accommodate tickets of up to 65 kilobytes.

  [From Build 53.9] [# 505809, 507692]

- If, after successful completion of the single factor authentication, the user attempts to access a resource that requires a higher level (level 2) authentication, in some load balancing topologies, the NetScaler ADC might,respond with a generic 404 message. With this fix, if the initial user authentication used single factor authentication, the ADC sends a logon page to prompt the user to again provide credentials for level 2 authentication.

  [From Build 53.9] [# 501883]

- The NetScaler ADC now offers the ability to configure 16 attributes in an LDAP action. These attributes are sent to the Active Directory (AD) during a user search. These values are extracted and stored. During the user session, they can be invoked/referenced in PI expressions.

  [From Build 53.9] [# 301241]

- The NetScaler fails to parse incoming assertions if it finds a duplicate Status code tag. As per SAML specification, unlike other tags, the StatusCode tag can come nested within itself. With this fix, the nested StatusCode tags are allowed in the assertion during SAML Authentication.

  [From Build 54.9] [# 523158]

- If a user name or password consists of UTF8 characters, basic authentication fails on the NetScaler ADC. With this fix, the ADC now passes the encoding type in the 401 challenge so that the incoming data is accurately encoded.

  [From Build 54.9] [# 507386]

- If an authentication profile has a space in its name, the NetScaler parser only takes the first part of the string up to the space character as the name of the profile. The NetScaler ADC may fail if during user authentication it comes across another entity that matches this partial string. With this fix, we now use URLencoding for the profile name to accurately process special characters .

  [From Build 54.9] [# 512078]

- The NetScaler Gateway and AAA-TM now support advanced expressions in SSO (single sign-on). The attribute values that are extracted as part of the authentication “http.req.user.attribute(1..16)” can now be used for setting the username and password credentials. For more information, see http://support.citrix.com/article/CTX200261

  [From Build 54.9] [# 452352, 482255, 495610]

- When a user attempts to use the two form factor method to log on to AAA-TM, the NetScaler ADC might become unresponsive.

  [From Build 55.8] [# 502710, 522858]

- NetScaler ADC as a SAML service-provider now supports SAML single logout through the front channel. Only service-provider initiated single logout flow is currently supported. Identity-provider initiated logout is not yet supported.

  [From Build 55.8] [# 517314]

- The NetScaler appliance sometimes sends a 401 error message to a client that sent a valid authorization header.

  [From Build 56.15] [# 532675]

- For Kerberos authentication, due to the reuse of server-side connections, the server does not display the appropriate user's page.

  [From Build 56.15] [# 532861]

- In a AAA-TM setup that has 401 authentication enabled on the load balancing virtual server, the NetScaler appliance can, in some cases, go down if it receives a malformed authorization header.

  [From Build 56.15] [# 530792]

- The NetScaler appliance can fail if the logout of the AAA-TM session is initiated through a traffic policy. The configuration that can lead to this is of the form:

> add tm trafficAction testAction1 -InitiateLogout ON

> add tm trafficPolicy testPolicy1 <rule> testAction1

[From Build 56.15] [# 527651]

- The NetScaler appliance can crash if there is an authentication failure in 401-based authentication when web authentication is used.

  [From Build 56.15] [# 527131]

- Currently, the NetScaler appliance does not fallback to NTLM if PKINIT over back-channel fails.

  [From Build 56.15] [# 532718]

- When you upgrade the firmware of a HA setup to NetScaler 10.5 Build 56.12, the secondary appliance becomes unresponsive if the primary appliance has active AAA-TM sessions.

  Workaround: Remove all active AAA-TM sessions before upgrading.

  [From Build 56.15] [# 554849, 555618]

Action Analytics

- The NetScaler crashes due to an issue in hash calculation and comparison of the action analytics records. The crash is observed when the NetScaler receives URLs that differ only in case.

  Examples:

  http://10.217.6.239/TesT/

  http://10.217.6.239/TEST/

  http://10.217.6.239/TEsT/

  http://10.217.6.239/TeST/

  Note post fix:

  Stream analytics record creation will be case sensitive. For example, WWW.GOOGLE.COM and www.google.com will result in two seperate records.

  If this is not desired, stream selector results should be converted to one case. Example:

  add stream selector sel1 HTTP.REQ.hostname.to_lower

  [From Build 53.9] [# 406457]

AppFlow

- If you delete an appflow action, the NetScaler ADC might fail.

  [From Build 53.9] [# 499172, 501216]

- The HTML Injection JavaScript is incorrectly inserted into one of the JavaScript responses sent by the server, causing the page to fail to load.

[From Build 55.8] [# 472971]

- If the HTML injection feature is enabled, the NetScaler appliance injects JavaScript into responses sent to clients. If a subsequent request from one of the clients is generated from the JavaScript, the appliance responds with a 404 error.

  [From Build 56.15] [# 365404]

Application Firewall

- 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]

- 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]

- The application firewall parses multipart forms correctly according to the appropriate RFC.

  [From Build 52.11] [# 479840, 472476, 482042]

- 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 52.11] [# 464641]

- If you use the configuration utility to make changes to the HTML Cross-Site Scripting check, Allowed/Denied patterns, the application firewall becomes unresponsive after the first POST request it receives after you save your changes. (The Allowed/Denied patterns are accessed through the Modify Signature dialog box.) If you use the command line to make the same changes, no problems occur.

  [From Build 52.11] [# 459031, 463351]

- 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 53.9] [# 443673]

- The application firewall PCI-DSS report does not contain information about the "SQLInjectionCheckSQLWildChars" parameter.

  [From Build 53.9] [# 423150]

- If a NetScaler ADC receives a request for an object that it cached before the application firewall configuration was modified to add any advanced security check protection, the ADC responds with HTTP Error 503 for subsequent requests to access this cached object, because the object does not contain the expected application firewall metadata. With this fix, the existing cached objects without the required

metadata are considered stale and are flushed. The request is served from the origin server and the cache is updated with refreshed data.

[From Build 53.9] [# 473322, 466491]

- If a response contains href links that include query parameters, the NetScaler application firewall triggers false positives for CSRF and form field consistency violations if these links are accessed. With this fix, if CSRF or Field Consistency checks are enabled, the URLs in the hrefs are added to the URL Closure table even if startURL Closure is not enabled.

  [From Build 53.9] [# 488369]

- NetScaler Application Firewall Default Signature object now has rules that can be enabled to protect against Shellshock vulnerability (CVE-2014-6271, CVE-2014-7169) which could allow arbitrary code execution.

  [From Build 53.9] [# 505272, 505039]

- The NetScaler ADC might fail if a transaction is aborted before the application firewall completes processing the request.

  [From Build 53.9] [# 481899]

- If CEF logging is turned on, only the format of application firewall log messages is expected to change, but the format of other logs is also affected, causing problem with their display. With this fix, turning on the application firewall CEF logging does not modify the format or display of other logs.

  [From Build 53.9] [# 476206]

- If the NetScaler application firewall receives a request with percent-encoded space character, such as "login%20name" for a form field login name, the deployed learned rule containing the encoded character (%20) fails to work as relaxation rule. The security check violation is still triggered. Note that the browser converts the space to a "+" character. For such a request, the corresponding learned rule with "login +name" for "login name" works as expected when deployed as a startURL relaxation rule.

  Workaround: Edit the relaxation rule to replace "%20" with "\s*" for requests with percent encoded space characters.

  [From Build 54.9] [# 315183]

- During upgrade from release 10 to 10.1, the names of the application firewall learning database files with uppercase or mixed case characters get converted to all lowercase characters. This results in two sets of database files and breaks the learned rule functionality. With this fix, learning data can be successfully retrieved after upgrade for profiles with names in mixed case characters.

  [From Build 54.9] [# 446134, 483207]

- If a user-created signature has an uppercase character in the name, the application firewall profile bound to the signature is not saved in the configuration during an upgrade from a release 10.1 build to a release 10.5 build. If a user creates a signature name with uppercase characters, release 10.1 stores it that way. But in release 10.5, the signature name is converted to a lowercase string in the database.

As a result of the database mismatch, the command to add the application firewall profile fails during an upgrade to a release 10.5 build.

[From Build 54.9] [# 511657, 512129]

- The NetScaler ADC might display an error message when you bind a classic application firewall policy to a load balancing virtual server or to the global bind point, because classic application firewall policies do not support the "gotopriorityexpression" and "invoke" properties. With this fix, properties that are not supported for application firewall policies are no longer included in the bind command. The binding is now successful, and you can see the bound entities.

  [From Build 55.8] [# 522720]

- Configuration changes in the action settings of the Content Type security check in the application firewall profile are not saved accurately. Changes made by using the configuration utility are not reflected in the command line interface, and vice versa. With this fix, changes made through any user interface are saved and displayed accurately in both the configuration utility and the command line.

  [From Build 56.15] [# 537910]

- The PCI DSS report is showing version 2 in the Configuration Utility. With this fix, the PCI DSS compliance report is updated with version 3 information.

  [From Build 56.15] [# 452012]

- The naming convention for application firewall import objects has changed from 10.1 build to 10.5 build. If a user creates a signature name with uppercase or mixed case characters, release 10.1 stores it that way. But in release 10.5, the signature name is converted to a lowercase string in the database. As a result of the database mismatch, these signatures become unusable after the 10.1 build to a 10.5 build upgrade. With this fix, the configuration is migrated accurately during the upgrade.

  [From Build 56.15] [# 539766, 546424, 548286]

- The NetScaler ADC might fail if a request attempts to access uninitialized variable for an application firewall protected resource. This might be seen when the path ends with "/..".

  [From Build 56.15] [# 517750, 530793]

- The external syslog servers are not able to properly display the audit-log messages from the NetScaler application firewall, because the messages are longer than expected. With this fix, the messages are the correct length.

  [From Build 56.15] [# 528170]

Application Templates

- If you use AppExpert templates to create applications or public endpoints that have names longer than 18 characters, an "HTTP 1.1 Service Unavailable" error message is displayed to the users.

  [From Build 55.8] [# 524252]

Cache Redirection

- Applying multiple ACL rules causes excessive consumption of CPU cycles. As a result, the NetScaler ADC might become unresponsive.

  [From Build 53.9] [# 502366, 505091]

- An invalid HTTP request received on a cache redirection virtual server configured on the NetScaler ADC is sent to the cache server. This results in errors and degraded performance.

  With the fix, invalid HTTP requests are redirected to the origin server instead of the cache server.

  [From Build 53.9] [# 497866, 502366]

- When the cache redirection virtual server is configured as a forward proxy, if an ASYNC memory allocation failure happens, the NetScaler appliance might fail to respond while trying to access a page on the a server that is already configured as a service on the NetScaler.

  [From Build 54.9] [# 486578, 491485, 502030, 519399]

- The NetScaler ADC fails if the cache redirection virtual server and the httpport parameter point to the same service. For example, the following configuration causes the ADC to fail:

  set ns param -httpport 80

  add cr vserver cr1 http * 80

  set cr vserver cr1 -listenpoliciy "client.ip.src.eq(1.1.1.1)"

  Workarounds:

  Add a listen policy when you add the cache redirection virtual server. For example:

  set ns param -httpport 80

  add cr vserver cr1 -td 0 HTTP * 80 -range 1 -cacheType TRANSPARENT -Listenpolicy "CLIENT.IP.DST.EQ(4.4.4.10)"

  Or:

  Unset the httpport parameter. For example:

  unset ns param httpport

  add cr vserver cr1 http * 80

  [From Build 55.8] [# 509690]

Cluster

- In a cluster setup, if a NSVLAN is configured, you cannot bind a VLAN to a traffic domain.

  [From Build 54.9] [# 517663]

- The load balancing configurations of a cluster node that is shut down are not available when you access the cluster configuration coordinator through its NetScaler IP address, instead of through the cluster IP address.

  [From Build 56.15] [# 522245]

- If you upgrade a node in a cluster to NetScaler 10.5 build 54.9 or later while the other nodes are running an earlier build, the node being upgraded might stop responding.

  [From Build 56.15] [# 543117, 511764, 544264]

- NetScaler cluster nodes may send a large number of ARP requests if a large number of ARP entries are learned over a cluster LA interface.

  [From Build 56.15] [# 519327, 542633]

- In a cluster, for services that need probing, SYN packets are processed locally (on the flow receiver) even though syncookie is disabled. Therefore, the NetScaler 10.5 54.x and 55.x builds are not suitable for cluster deployment.

  [From Build 56.15] [# 539657]

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]

- 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 52.11] [# 480639]

- The user monitor scripts that use SOAP::Lite might not work.

  [From Build 54.9] [# 503214]

- NetScaler ADC fails to run the commands that have arguments accepting string values and starting with a hyphen (-).

  For example, NetScaler ADC fails to run the following command because the expected value is a string for uat argument that begins with a hyphen.

  bind policy patset ps_adi_any_robots_deny -uat -index 1

  [From Build 56.15] [# 508618, 508815]

Configuration Utility

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

  [From Build 51.10] [# 482609, 485852]

- 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]

- 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]

- Some usability issues while configuring content switching by using the NetScaler configuration utility.

  [From Build 51.10] [# 491215]

- 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]

- 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]

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

  [From Build 51.10] [# 484583]

- The default value for packet count is 45, and the default Encryption Trigger Timeout is 1 ms, but the configuration utility displays both values, incorrectly, as 0.

  [From Build 52.11] [# 494915]

- If you have configured Mobile Device Manager by using the XenMobile wizard in release 10.1.e build, and then upgraded to release 10.5, the service configuration does not appear in the configuration utility.

  Workaround: Rename the two MDM virtual servers by adding "_MDM_" at the beginning. For example, rename _XM_ABC_192.168.1.1_443 to _XM_MDM_ABC_192.168.1.1_443.

  [From Build 52.11] [# 493946]

- The configuration utility might display an error message while adding IPv6 routes in non-default traffic domains.

  [From Build 52.11] [# 499592]

- 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 52.11] [# 460020]

- A NetScaler ADC displays a Java error if you access it by using an sshd connection.

  [From Build 52.11] [# 451546]

- The configuration utility displays the "Resource already exists" error if you configure a content switching virtual server with the IP address 10.69.129.128.

  [From Build 52.11] [# 490142]

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

  [From Build 52.11] [# 441408]

- The configuration utility displays the "Resource already exists" error if you configure a content switching virtual server with the IP address 10.69.129.128 .

  Workaround: Configure the content switching virtual server with a different IP address.

  [From Build 53.9] [# 490142]

- After the first reboot of a cluster setup that has large configurations, the NetScaler ADC takes more time to load those configurations and to log you on.

  [From Build 53.9] [# 483442]

- 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 53.9] [# 456428]

- If you bind a CA certificate to a load balancing virtual server using the configuration utility, the Link Certificate view is not displayed in the foreground.

  [From Build 54.9] [# 485539, 502285]

- 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 54.9] [# 447915]

- If you create a GSLB service by using a server name with alphanumeric characters, the server name does not get converted to a server IP address, and the server IP address value is null. As a result, GSLB synchronization fails.

  [From Build 54.9] [# 501644, 505641, 509379]

- If, in the NetScaler configuration utility, after you navigate to AppExpert > Responder> Policies and click "Hide built-in responder policies" or "Show built-in responder policies," the page does not immediately refresh, and continuous clicking prevents the page from refreshing.

  [From Build 54.9] [# 496336]

- To create a certificate signing request, you must click "Create Certificate Signing Request (CSR)" on the SSL overview page for each CSR. To view or manage your CSRs, click "Manage Certificates / Keys / CSRs" under Tools on the SSL overview page.

  [From Build 54.9] [# 503590]

- An error message appears if you try to replace an SSL client certificate that is bound to an SSL service.

  [From Build 54.9] [# 514538, 513837]

- 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 54.9] [# 375277, 322602, 334465, 396405, 412455, 419503, 438382, 438534, 438796, 441853, 446387, 448361]

- If an unauthorized user logs on to a NetScaler ADC. the ADC displays the following error message:

  "Error in retrieving version. Cannot read property 'replace' of undefined".

  [From Build 54.9] [# 517146, 513730]

- The statistics of service group members do not appear correctly in the configuration utility.

  [From Build 54.9] [# 521579, 508630, 519918, 521983]

- When you are configuring an admin partition, the state of the LACP channel is incorrectly displayed in the list of channels (Network > Channels). This issue is not present in the default partition.

  [From Build 55.8] [# 517606, 518444]

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

[From Build 55.8] [# 353015]

- The NetScaler Graphical User Interface does not support the search functionality to search records in the file browser.

  Workaround: Use the search functionality of internet browser.

  [From Build 55.8] [# 503589]

- Evaluating an advanced expression on different browsers gives different results. This issue arises because the sample payload gets changed on different browsers.

  [From Build 55.8] [# 524123, 521279]

- NetScaler authentication fails if you use special characters such as %0 or %1 in the password.

  [From Build 56.15] [# 505536]

- If you use the configuration utility to update an existing certificate-key pair (load the updated certificate or key using the same certificate-key file name), the old details continue to appear until you restart the appliance.

  Workaround: Use the NetScaler command line to update certificates.

  [From Build 56.15] [# 533255]

- If, while using the configuration utility to create a service group member for a load balancing service group (Traffic Management > Load Balancing > Service Groups), you specify the port value as a wild card (*), the Configure Service Group screen displays an incorrect value.

  [From Build 56.15] [# 530025]

- NetScaler authentication fails if you use special characters such as & or ; in the password.

  [From Build 56.15] [# 542557, 542644, 544420, 547508]

- The Upgrade Wizard does not work intermittently in some browsers in NetScaler 10.5 Build 56.12. This issue is fixed in NetScaler 10.5 Build 56.15.

  [From Build 56.15] [# 544588, 557380]

- After you create a virtual server by using the XenApp and XenDesktop wizard, if you delete the virtual server and restart the appliance, the deleted virtual server still exists.

  [From Build 56.15] [# 524975]

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

  Workaround: The workaround differs for the different versions:

  - In NetScaler 10.1, provide only the FIPS key. For example, rsa.key.

- In NetScaler 10.5, you must specify the complete file path to the FIPS key. For example, nsconfig/ssl/folder1/folder2/rsa.key.

[From Build 56.15] [# 483226]

Content Optimization

- If you enable FEO and the Web traffic that reaches NetScaler has "//" at the beginning of the URL, then NetScaler may not respond as intended.

  [From Build 55.8] [# 529356, 533790, 534403]

Content Switching

- If an invalid HTTP request that spans multiple TCP segments is sent to a content switching virtual server, the NetScaler ADC might skip the load balancing decision and initiate a connection from the SNIP address to the content switching virtual server. This can cause the ADC to fail.

  To prevent this problem, the ADC closes the client connection when this situation arises.

  [From Build 54.9] [# 501856]

- If you perform the following sequence of actions, the second command fails when the restart process runs the commands, because that process adds the gotoprioorityexpression to the second binding:

  1. Bind a policy to a content switching virtual server and specify a gotoprioorityexpression.

  2. Bind a filter or compression policy to another content switching virtual server without specifying a gotoprioorityexpression.

  3. Save the configuration and restart the appliance.

  [From Build 55.8] [# 523636, 532832, 533690]

DNS

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

  [From Build 51.10] [# 462862]

- If the number of records in a DNS response for a domain exceeds the Netscaler ADC limit, or if one of the records in the response contains invalid data, the NetScaler ADC does not cache the response. As a result, DNS resolution using NetScaler nameserver entities fails.

  [From Build 52.11] [# 437529]

- The DNS cache entries are not flushed if the DNS caching feature has been disabled for approximately 250 days.

  [From Build 52.11] [# 471707]

- If a server sends a NODATA response that has CNAME record in the answer section and no records in the authoritative and additional sections, the response is marked for CNAME caching on the NetScaler ADC, because it is incorrectly assumed to be a

referral response. As a result, the ADC sends a blank response to subsequent queries, of any query type, for the canonical name.

[From Build 52.11] [# 477552]

- If, while adding a DNS record (such as addrec and nsrec) from the GUI or by using the NITRO API, you specify the TTL value as 3600, the value of the minimum TTL of the SOA record is used instead.

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

  [From Build 53.9] [# 382478]

- When a NetScaler ADC is deployed as a DNS server with caching enabled, and "flush dns proxyRecords" is used when the ADC is serving a large volume of traffic and has a large number of records in its cache, the ADC might fail.

  [From Build 53.9] [# 484069]

DataStream

- The NetScaler ADC fails if source IP persistence is enabled on a MySQL or MSSQL virtual server that is receiving traffic.

  [From Build 54.9] [# 510805, 516687]

- If you use SQL server driver for SQL Server 2000 SP1, the databases are not enumerated for Kerberos authentication on the NetScaler ADC, because the ADC does not process the SSPI packet correctly.

  [From Build 54.9] [# 507709]

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

  - The appliance is configured in transparent mode.

  - The appliance performs Windows authentication for MSSQL requests.

  [From Build 56.15] [# 539922]

Front End Optimization

- If you define an FEO policy to match only the HTML traffic, the domain sharding configuration in the policy’s action is lost when the policy is triggered.

  [From Build 55.8] [# 529329]

GSLB

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

  [From Build 51.10] [# 488161]

- In rare cases, high management-CPU usage occurs and a large number of error messages appear in the log file. As a result, queries to the location database might fail, and the backup load balancing method is used for site load balancing.

  [From Build 52.11] [# 453144, 455417]

- Configuring a hash based backup load balancing method on a GSLB virtual server might cause the NetScaler ADC to fail if traffic triggers the backup method.

  [From Build 53.9] [# 496676]

- 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 53.9] [# 485811]

- If you have deployed the NetScaler ADC in a high availability (HA) setup in INC mode, you cannot leverage a SNIP address to host the ADNS Service or a site IP address, because these addresses do not float across the HA nodes. An independent site IP address with SSH enabled is required. With this fix, SSH can be enabled on an independent site IP address.

  [From Build 54.9] [# 505546, 505526, 523055]

- Synchronization of the GSLB configuration fails if the RPC-node password of the GSLB sites contains an exclamation point (!).

  [From Build 54.9] [# 511192, 511521, 524390]

- If you force synchronization of the GSLB configuration, the non-default settings on the RPC node are lost. As a result, the GSLB auto-sync functionality is lost.

  [From Build 54.9] [# 497412]

- The NetScaler ADC fails if a VPN session action, a WI home page, or DBS services are configured with a domain name that at the same time is managed by a GSLB virtual server configured with static proximity or RTT load balancing methods.

  [From Build 55.8] [# 433094, 469937, 517974]

- If the disablePrimaryOnDown parameter is configured on the primary GSLB virtual server, the primary GSLB virtual server remains in DISABLED state even after its health state is UP. The backup GSLB virtual server continues to serve the traffic until HA failover or you manually enable the primary GSLB virtual server.

  [From Build 55.8] [# 517961]

- The show gslb service command now displays the following values related to the GSLB service:

  -Last State Change

  -Time since last state change

  -Client and Server idle timeout

  [From Build 55.8] [# 498854]

- If the length of the domain name bound to a GSLB virtual server exceeds 31 characters, the domain name is displayed as HASHED STRING during an SNMP MIB Walk operation.

  [From Build 55.8] [# 511878]

- All GSLB features except DNS views, auto sync, and static proximity are supported for IPv6.

  [From Build 56.15] [# 519589]

- If you set the backup load balancing method to the same method that is already configured, the backup load balancing method defaults to round robin.

  [From Build 56.15] [# 531553]

- If a spillover policy is bound to a GSLB virtual server of type UDP, the show ns runningConfig command does not display the policy binding. The policy binding functions properly, but the configuration might be lost if a failover occurs or if the appliance is restarted.

  [From Build 56.15] [# 528060]

- GSLB synchronization fails if you change the RPC node passwords.

  [From Build 56.15] [# 497338, 516259, 522602, 548845]

Graphical User Interface

- If you enable NTP synchronization on a NetScaler ADC, the ntpd service binds to port 3010. The binding causes resource conflicts, because the port was reserved for the nsnetsvc service.

  [From Build 54.9] [# 502309, 503357]

HTML Injection

- The JavaScript inserted by NetScaler ADC for obtaining client side measurements contains a syntax error. This interferes with page rendering which leads to Outlook Web App displaying error popups.

  [From Build 55.8] [# 518072, 518272]

High Availability

- By default, HA synchronization enables the following features and modes on the secondary appliance:

  - Features: Web logging (WL) and surge protection (SP)

  - Modes: L3 and Edge

  [From Build 54.9] [# 512034, 516783]

- When there are a large number of sessions (in the order of millions, due to, for example load balancing persistence) to be synchronized, and the link between the primary and secondary appliance is very slow, the primary appliance quickly consumes all the NetScaler buffer. Therefore, there is no buffer to allocate to other sub-systems. This can result in various disruptions such as failover.

  [From Build 55.8] [# 519085, 525203, 533671]

- With Layer 2 mode enabled, the secondary node in a high availability configuration forwards DHCP packets coming from the server.

[From Build 56.15] [# 521424]

- In a high availability configuration, if the diff ns config command includes the -ignoreDeviceSpecific parameter, the command fails and does not display the difference in configurations between the two nodes.

  [From Build 56.15] [# 524146, 526699]

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]

- When a byte-range request is sent for an object, and if that object is expired, a request is sent to the server to revalidate the object. If that object is now modified on the server, the full response is served to the NetScaler. In such a scenario, the NetScaler appliance can crash.

  [From Build 52.11] [# 494910, 497793]

Load Balancing

- 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]

- 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]

- If you have configured the RADIUS PI expression CLIENT.UDP.RADIUS.ATTR_TYPE(<avp code>) for content switching, rule-based persistency, or the token load balancing method, and you typecast the result of this expression to an integer or IP address by using the expression TYPECAST_NUM_AT / TYPECAST_IP_ADDRESS_AT, the typecast operation fails.

  [From Build 52.11] [# 482113]

- 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 52.11] [# 489197]

- You can now bind loopback members (for example 127.0.0.1) to service groups. Previously, you could bind loopback members to services only.

  [From Build 53.9] [# 504209]

- If a semantically incorrect command is entered while a domain based service is being resolved to a NetScaler-owned IP address, the NetScaler ADC displays the state of the service incorrectly.

[From Build 53.9] [# 502338]

- A very slow memory leak occurs on the secondary node in a high availability pair if all of the following conditions are met:

  a) The configuration is large (approximately 4MB).

  b) The configuration includes a large number of "bind lb group" commands.

  c) Configuration changes very frequently, resulting in frequent synchronization.

  [From Build 53.9] [# 457639]

- If a load balancing virtual server on which persistence is configured is bound to a load balancing group that has no persistence setting, the NetScaler ADC does not change the virtual server's persistence setting. As a result, when traffic arrives at the virtual server, it tries to create a persistence session, but that session fails and the number of sessions increases.

  [From Build 54.9] [# 497470]

- A Storefront service on a NetScaler ADC is not marked as DOWN even though all the storefront services bound to the StoreFront server are manually brought down.

  [From Build 54.9] [# 460040]

- The NetScaler ADC might fail if a high idle timeout value is set on a TFTP load balancing virtual server and the ADC runs out of memory.

  [From Build 54.9] [# 505543]

- The SIP monitor probe has an invalid character in the VIA header. As a result, the probe fails and an incorrect service state might appear.

  [From Build 55.8] [# 519644]

- Load Balancing

  The NetScaler ADC might fail after you rename a server that is bound to a service group. This problem does not occur if you assign a name to a server that was identified by its IP address.

  [From Build 55.8] [# 443027]

- Load Balancing

  If your spillover policy contains the ACTIVETRANSACTIONS or the SURGECOUNT expression (for example, <expression>. ACTIVETRANSACTIONS.GT(<N>)), traffic might spill over to the virtual server bound to this policy even though the current value of the counter has not reached N. This is because these two expressions use an arbitrary number for comparison.

  For example, spillover to a virtual server bound to the following policy might occur before the active transactions counter reaches a value of 10:

  SYS.VSERVER("A').ACTIVETRANSACTION.GT(10) -action spillover

  [From Build 55.8] [# 516615]

- If you have set the persistence type to COOKIEINSERT, you can now encrypt the cookie in addition to any existing SSL encryption by using the NetScaler command line and configuration utility.

  At the NetScaler command prompt, type:

  set lb parameter -useSecuredPersistenceCookie Enabled-cookiePassphrase test

  In the configuration utility, navigate to Traffic Management > Load Balancing > Change Load Balancing Parameters and select Use Secured Persistence Cookie and Cookie Passphrase and enter a passphrase.

  [From Build 55.8] [# 347108, 323325, 348588]

- Unsetting one of the load balancing virtual server parameters, such as redirect URL, backup virtual server, push virtual server, or authentication profile, incorrectly unsets the appflowLog parameter.

  [From Build 56.15] [# 523239]

- If the DNS load balancing virtual server is configured with DNS rate limiting or analytic policies, the appliance might fail under certain heavy load conditions.

  [From Build 56.15] [# 528070]

- When you bind a DNS policy to the DEFAULT_GLOBAL bind point, the policy's priority is automatically set to 65545, which exceeds the supported priority range. The "operation not permitted" error message appears.

  Workaround: Before binding the policy, manually set its priority to a value within the range of 1-65535, and make sure that the priority you set is not used in other bound DNS policies.

  [From Build 56.15] [# 488011]

NS-CLI

- If a stringmap is bound to a NetScaler policy and the stringmap value contains a single word starting with "#" then the stringmap binding is lost after the system reboot.

  [From Build 55.8] [# 383850]

- NetScaler ADC will generate “SNMP clear alarm traps” for the successful cases of haVersionMismatch, haNoHeartbeats, haBadSecState, haSyncFailure, and haPropFailure error events in HA configuration.

  [From Build 55.8] [# 368832]

- The memory allocation API, malloc, returns a NULL value if it does not obtain memory for 'nscollect utility'. If the 'nscollect utility' tries to dereference this NULL pointer, it results in a memory segmentation error.

  Workaround: Restart the nscollect utility.

  [From Build 55.8] [# 528818, 529425]

NetScaler Insight Center

- 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]

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

  [From Build 51.10] [# 484659, 487457]

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

  [From Build 51.10] [# 490416]

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

  [From Build 51.10] [# 486792]

- NetScaler Insight Center does not display reports for traffic that passes through any NetScaler virtual servers other than HTTP virtual servers.

  [From Build 52.11] [# 498430]

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

  Error fetching licensing information.

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

  [From Build 52.11] [# 496805]

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

  [From Build 52.11] [# 473936, 473967]

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

  'Excess connection than the CFE limit for NetScaler'

  [From Build 53.9] [# 484492]

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

  [From Build 53.9] [# 409634]

- If you access NetScaler Insight Center by using a secure connection, the geo maps do not display any data.

  [From Build 53.9] [# 502560]

- As part of the bandwidth calculation for active and inactive sessions, NetScaler Insight Center displays the following four metrics instead of the bandwidth metric:

  -Total Bytes: Bytes transferred per session

  -Bytes per Interval: Total bytes transferred per session interval (5 mins, 1 hour, 1 day , 1 week, 1 month)

  -Session Bandwidth: Rate at which data is transferred over the session.

  -Bandwidth per Interval: Rate at which data is transferred over the session interval.

  [From Build 54.9] [# 515365, 518368]

- You cannot export reports on NetScaler Insight Center if the type of communication between the monitored devices and NetScaler Insight Center is HTTPS, and Secure Access only is enabled.

  [From Build 56.15] [# 535450]

- When you launch XenApp through Citrix Receiver (standard edition), the app launch duration is not calculated and is shown as zero.

  [From Build 56.15] [# 388096, 423109]

- NetScaler Insight Center might fail if you enable geo data collection.

  [From Build 56.15] [# 533052]

- The NetScaler Insight Center dashboard sometimes displays the applications as desktops.

  [From Build 56.15] [# 530782]

- You cannot install an SSL certificate on a NetScaler Insight Center virtual appliance.

  [From Build 56.15] [# 541712]

- If you disable HTML Injection, the Web Insight node of NetScaler Insight Center displays incorrect WAN latency values.

  [From Build 56.15] [# 541469]

NetScaler VPX Appliance

- When you upgrade an instance of NetScaler VPX on Amazon AWS to release 10.5 build 50.9, the SSL feature of the VPX instance might not support more than 512 bit encryption.

  [From Build 51.10] [# 487876, 488699]

Networking

- 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 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]

- 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]

- 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]

- 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]

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

  [From Build 51.10] [# 483502]

- On a NetScaler ADC, ND6 entries might get in INCOMPLETE state due to synchronization mismatch among different internal modules. As a result NetScaler fails to serve traffic for that IPV6 address.

  [From Build 52.11] [# 480100, 483728]

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

  [From Build 52.11] [# 477415]

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

  [From Build 52.11] [# 477402]

- Feature: Load Balancing

  For a DHCP load balancing configuration, the NetScaler ADC does not forward any unicast DHCP relay agent (UDP port 67) packets, which are received by the virtual server, to the bound servers.

  [From Build 52.11] [# 497057]

- The NetScaler ADC drops IPv4 packets related to the following protocols:

  - IPv6 encapsulation (41)

  - Fragment Header for IPv6 (44)

  - ICMP for IPv6 (58)

[From Build 52.11] [# 490190]

- The NetScaler ADC might fail to evaluate listen policies, containing source or destination ipv6 address/subnet, for certain IPv6 addresses.

  [From Build 52.11] [# 496564]

- Old or stale OSPF LSAs might exist after a warm restart, or restart after a power failure, resulting in triple flip.

  [From Build 52.11] [# 441005]

- With more than 1000 IP tunnels configured on a NetScaler ADC, the internal data structure for these IP tunnels might not be updated for some events. This changes the status of these IP tunnels to the DOWN state.

  [From Build 52.11] [# 491473]

- For a load balancing server configured on a non-default traffic domain, on modifying the IP address of the server also changes the name of the server.

  [From Build 53.9] [# 496237]

- With MAC based forwarding (MBF) option enabled, the NetScaler ADC does not update Layer 2 information such as MAC address, interface ID, and VLAN ID, for a dynamic service even when the associated router is inactive. As a result, the router drops the packets destined to the IP address specified by the dynamic service.

  [From Build 53.9] [# 490341]

- On running the "show connectiontable -detail LINK" command in NetScaler command line interface, the NetScaler ADC might become unresponsive.

  [From Build 53.9] [# 500720]

- The NetScaler ADC might not update its bridge and ARP tables with the information received from GARP messages.

  [From Build 54.9] [# 497277]

- An Access Control List (ACL) rule specifying the TCP protocol and the Established option might not get evaluated if another ACL rule with a higher priority also specifies TCP.

  [From Build 54.9] [# 510173]

- Now, the NetScaler appliance sends all ARP replies from the first interface (lexicographical order) of an LA channel.

  [From Build 54.9] [# 486632]

- An ACL6 rule might not get evaluated for a series of TCP packets.

  [From Build 55.8] [# 528554]

- 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 a NetScaler ADC works with a minimum MTU value of 520.

  [From Build 55.8] [# 485391]

- In response to a packet sent with IP over IP encapsulation carrying an inner TCP header, the NetScaler packet processing engine (NSPPE) fails if the NetScaler ADC receives an ICMP Need Fragment error response.

  [From Build 55.8] [# 528069]

- If you bind an interface with a unit number greater than 31 to a VLAN that is used as a Sync VLAN in an HA configuration, the Sync VLAN becomes unoperational.

  [From Build 55.8] [# 507345]

- On receiving Generic Routing Encapsulation (GRE) packets as IP fragments on a virtual server with protocol ANY, the NetScaler ADC fails and is rebooted. This occurs only when you do not explicitly configure a GRE tunnel on the NetScaler ADC.

  [From Build 55.8] [# 522538]

- If you disable the TCP Proxy parameter while creating a Reverse Network Address Translation (RNAT) rule on a multi-core NetScaler ADC, the NAT operation fails.

  [From Build 55.8] [# 508631, 509453]

- On a NetScaler ADC, when the MTU of a VLAN and Intermediate System to Intermediate System (IS-IS) Link Sate Packet (LSP) is set to a value lower than 1500, the IS-IS process fails to send the IS-IS protocol data units (PDUs) of the specified MTU size until the process is restarted.

  [From Build 55.8] [# 485374]

- Blocking Traffic on Internal Ports

  The NetScaler appliance does not block traffic that matches an ACL rule if the traffic is destined to the appliance's NSIP address, or one of its SNIP addresses, and a port in the 3008-3011 range.

  This behavior is now specified by the default setting of the new Implicit ACL Allow (implicitACLAllow) parameter (of the L3 param command). You can disable this parameter if you want to block traffic to ports in the 3008-3011 range. An appliance in a high availability configuration makes an exception for its partner (primary or secondary) node. It does not block traffic from that node.

  To disable or enable this parameter by using the command line interface

  At the command prompt, type:

  > set l3param -implicitACLAllow [ENABLED|DISABLED]

  Note: The parameter implicitACLAllow is enabled by default.

  Example:

  > set l3param -implicitACLAllow DISABLED

  Done

  [From Build 56.15] [# 529317]

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

  [From Build 56.15] [# 485260]

- In an active-active configuration, services bound to the backup VIP addresses do not send monitor probes to the associated servers.

  [From Build 56.15] [# 355965, 485260]

Platform

- NetScaler VPX instances running on VMware ESXi lose network connectivity when you apply either of the following patches:

  - ESXi550-201410401-BG

  - ESXi510-201410401-BG

  Workaround: For more information, see http://support.citrix.com/article/CTX200278.

  [From Build 55.8] [# 510673, 517241]

- The CPU usage of a NetScaler VPX instance running on VMware is constantly at 50% after an upgrade of the NetScaler software from release 10.1 to release 10.5.

  [From Build 56.15] [# 506700, 461089, 523888, 526203]

Policies

- Using the "SYS.CHECK_LIMIT" expression in conjunction with any boolean expression can cause the NetScaler to crash.

  [From Build 52.11] [# 493045]

- Rewrite policy bindings to virtual servers can be lost when you upgrade the NetScaler firmware to version 10.1.128.11. If the rewrite policy is bound to a load balancing virtual server, the policy bindings are not displayed as part of the server configuration, but they are saved when the user saves the configuration. If the rewrite policy is bound to a content switching virtual server, the policy bindings are lost when the user saves the configuration.

  [From Build 54.9] [# 508510, 513724, 517150, 518535, 519945]

Policies

- The NetScaler appliance can crash or the data can get corrupted when the URL (or other string) satisfies the following criteria:

  - Length is more than 1300 bytes (800 bytes for HTML_XML_SAFE).

  - Has at least one unsafe character.

  - A significant initial part of the string does not need encoding (or some smaller initial part of the string does not need encoding and there are lots of characters needing encoding)

- One of the following functions is used on the string in the expression:

* HTTP_URL_SAFE - unsafe characters are not allowed. Safe characters are: a-z, A-Z, 0-9, "-", "_", ".", "!", "~", "*", "'", "(", ")", ";", ":", "@", "?", "=", "$", "%", "&", "+", ",", "/".

* HTTP_HEADER_SAFE - new line ('\n') characters are unsafe.

* HTML_XML_SAFE - unsafe characters are '<', '>' and '&'.

* APPEND_QUERY_PARAMETER - same as HTTP_URL_SAFE

Workaround: As a workaround, remove uses of these functions from your expressions if strings can be long (or truncate the strings to 1300 bytes (800 bytes for HTML_XML_SAFE)). In a number of cases you can avoid using these functions if you concatenate the URL with some string constant to the left of it (for example "" + HTTP.REQ.URL) - if the input was encoded, so will be the result.

[From Build 53.9] [# 506761, #446507,#463284,#500444)]

Policy

- A NetScaler appliance that has a rewrite policy configured, becomes unresponsive, if all the following conditions are met:

  1. The rewrite action type is either "replace" or "insert_after".

  2. The HTTP response does not have the content-length header.

  3. The body of the HTTP response is split into multiple TCP packets with different TCP packets arriving with some time delay. This causes the policy rewrite engine to pause and resume the packet processing.

  4. The string specified in the rewrite action is present in the last packet of the HTTP response.

  [From Build 56.15] [# 554460]

- The Responder's HTML Page Import option fails if the name of the page being imported is in uppercase characters.

  [From Build 56.15] [# 530804]

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]

- In a setup with a large number of virtual servers, if only a few virtual servers receive most of the traffic while the other virtual servers are idle, there might be a delay in cleaning up the sessions.

  [From Build 53.9] [# 492087, 510038, 510483]

- The client certificate that is inserted in the backend HTTP header now conforms to the x509 PEM format, which includes spaces and carriage returns. To use the old method (without spaces and carriage returns), at the NetScaler shell prompt, type:

  nsapimgr -y -s ssl_cert_insertion_space=0

  [From Build 54.9] [# 495316]

- If the backend service is of type SSL_TCP, SSL reuse handshake using SSLv3 with backend servers fails and the connection is terminated.

  [From Build 56.15] [# 529471]

System

- 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]

- 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]

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

  [From Build 51.10] [# 488487]

- 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]

- 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 trying to log on to the NetScaler using the GUI or the NITRO API, external users (from LDAP, TACACS, and so on) get the following error message: 'User does not exist'.

  [From Build 52.11] [# 498221, 501681]

- 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 52.11] [# 463571]

- With AppFlow enabled, if any of the HTTP headers (URL, Host, Cookie, and so on) have a length of exactly 255, the NetScaler appliance could crash.

[From Build 52.11] [# 496726, 495235, 496997, 497181, 499667, 499733, 505523]

- The NetScaler appliance can crash when a large HTTP request URL has a space in it and if the request is broken into multiple packets.

  [From Build 52.11] [# 497321, 501856, 502116, 502902]

- 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 52.11] [# 484527]

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

  [From Build 52.11] [# 487437, 494371]

- A new HTTP profile option "rtspTunnel" allows RTSP over HTTP. The RTSP tunnel is detected by the presence of either one of the following

  - 'Accept: application/x-rtsp-tunnelled' request header

  - 'Content-Type: application/x-rtsp-tunnelled' response header

  Once the tunnel is detected, NetScaler stops HTTP tracking for that TCP connection and lets the RTSP flow go through. The "rtspTunnel" option is disabled by default.

  [From Build 52.11] [# 480219]

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

  [From Build 52.11] [# 471100, 425465, 484159, 484187]

- The NetScaler intermittently fails to generate traps due to issues in propagating the alarm state to the SNMP daemon.

  [From Build 52.11] [# 490192]

- When the NetScaler deployment has large configuration size, the NetScaler appliance can crash due to issues with memory allocation.

  [From Build 52.11] [# 478608]

- When a HTTP profile is bound to a virtual server or service, the configurations of this profile are considered over the configurations of the global HTTP profile (nshttp_default_profile). However, when connection multiplexing is disabled globally and enabled on the virtual server or service, the global setting for connection multiplexing is being considered. This issue has now been fixed.

  [From Build 53.9] [# 494013]

- Setting 'Request timeout' or 'Request timeout action' in HTTP Profiles can cause the NetScaler to fail in some situations.

  [From Build 54.9] [# 501100]

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

  [From Build 54.9] [# 490622, 496613]

- If you enable Front End Optimization (FEO) with SSL and HTTP compression, the NetScaler ADC fails.

  [From Build 54.9] [# 518322]

- If an incoming URL has two or more slashes at the beginning of the path to the file, the URL is not parsed correctly. This can affect the use of policy expressions and the functioning of features such as Rewrite, which use parsed information to examine URLs.

  [From Build 54.9] [# 519390]

- If you enable Front End Optimization (FEO) with SSL, cache extension, and HTTP compression, the NetScaler ADC fails.

  [From Build 54.9] [# 517652, 523715]

- If a non-HTTP request is received on an HTTP virtual server, the transaction might fail.

  [From Build 55.8] [# 504910]

- A NetScaler ADC processing SPDY traffic on SPDY enabled virtual servers fails intermittently if an HTTP response body received with chunked transfer-encoding and the response header is modified by other NetScaler features.

  [From Build 55.8] [# 519004, 528861]

- 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 55.8] [# 486257]

- NetScaler VPX instances, with build 10.5 and pay per hour license, running on Amazon AWS cloud might not support some Access Gateway features.

  [From Build 55.8] [# 531384]

- Multipath TCP does not work with NetScaler cache redirection feature.

  [From Build 56.15] [# 506056]

- Multiple instances of the nstraceaggregator daemon can run at the same time. As a result the NetScaler appliance might fail and corrupt the captured files.

  [From Build 56.15] [# 527119, 522584, 525657]

- If you enable the nstrace feature in TX mode with an advanced filter expression, the NetScaler appliance fails.

  [From Build 56.15] [# 494911, 481032, 511763, 528309, 532708, 538507]

- Multiple instances of the nstraceaggregator daemon can run at the same time. As a result the NetScaler appliance might fail and corrupt the captured files.

  [From Build 56.15] [# 532843, 534384]

- The NetScaler appliance fails if you enable both front end optimization and the application firewall.

  [From Build 56.15] [# 539454]

- The ns_monuploadd_err.pl script monitors the health of the NetScaler appliance by looking for errors recorded in the log files. The script decompresses the log files and does not remove the decompressed log files, which therefore consume disk space.

  [From Build 56.15] [# 532042, 447664, 532587, 533164]

- If you enable SPDY and the SPDY layer accumulates more than 8912 bytes of set-cookie values while processing a sever response, a buffer overrun causes the NetScaler appliance to fail.

  [From Build 56.15] [# 524949]

- 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 56.15] [# 377618, 341460, 351127, 364015, 475359, 481575, 499259]

- A NetScaler VPX virtual appliance with multiple packet engines fails if you enable the nstrace feature in TX mode with an advanced filter expression.

  [From Build 56.15] [# 528309]

- If an authentication policy is bound to NetScaler system global, authentication of weblog and auditlog services fails.

  [From Build 56.15] [# 498025, 521636, 534432]

- If password based authentication is used to open an SSH session to a NetScaler appliance, the wrong remote IP address is sent to the NetScaler syslog records.

  [From Build 56.15] [# 286861, 301935, 513312, 522183, 541332]

- A NetScaler appliance fails if it attempts to apply HTML injection to a server response that does not have a content type header.

  [From Build 56.15] [# 529493]

- If the NetScaler appliance uses the HTTP pipeline to parse an HTTP request, and the parsing process fragments the request packet, the appliance, after processing a

fragment, might not unset the flag indicating that the entire packet has been received. In that case, the appliance fails.

[From Build 56.15] [# 527320, 527211]

User Interface

- SSL

  If you add new ciphers by using the configuration utility, the order in which the configured ciphers are bound is not preserved.

  [From Build 55.8] [# 520088, 524139, 524140]

- Configuration Utility

  If you create a service on one of the screens that appear while you are configuring a virtual server, you cannot bind the service to the virtual server, because the OK button is not enabled.

  Workaround: Close the service pane and try to bind the service again.

  [From Build 55.8] [# 527388]

- Configuration Utility

  You can bind multiple services at the same time to a virtual server or a service group. However, you cannot unbind multiple services at the same time from a virtual server or from a service group.

  Workaround: Unbind each service separately.

  [From Build 55.8] [# 520751]

- Issue ID 0440208: If a new SSL certificate that requires a key is installed without the key, access to management service GUI is lost.

  [From Build 55.8] [# 440208]

- If you use an invalid filter expression when you start the nstrace process, an error message appears, but the NetScaler appliance starts two nstrace aggregator instances.

  [From Build 56.15] [# 536544]

- The SNMP counter of type cntr32 has been changed to a gauge counter.

  [From Build 56.15] [# 524080, 448724]

- The NetScaler appliance serves erroneous cache content if you use the XenApp/ XenDesktop wizard's auto-configured cache policies.

  [From Build 56.15] [# 426551, 545422]

XML

- Users who access a Microsoft Sharepoint server through a NetScaler ADC that has the application firewall enabled are unable to open any document type that requires software that is not part of the browser, such as Microsoft Office files.

[From Build 52.11] [# 450232]