Citrix NetScaler 1000V Release Notes

Citrix NetScaler 10.1
April 10, 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

Chapter 1

Build 131.7

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 131.7

Replaces build: None

Release date: March 2015

Release Notes version: 1.0

Language supported: English (US)

Bug Fixes

AAA-TM

- Issue ID 530792: 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.
- Issue ID 527651: 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

AppFlow

- Issue ID 472971: The HTML Injection JavaScript is incorrectly inserted into one of the JavaScript responses sent by the server, causing the page to fail to load.

Application Firewall

- Issue ID 528170: 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.
- Issue ID 511480: After an upgrade from a 9.3 build, the user interfaces display inaccurate information about classic policy bindings and inheritance. With this fix, both the configuration utility and the command line interface display the information accurately.

Cache Redirection

- Issue ID 509690: 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

Command Line Interface

- Issue ID 508618, 508815: 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

Configuration Utility

- Issue ID 353015: 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 Target Load Balancing Virtual Server list in the "Create Content Switching Action" dialog box (Content Switching > Actions > Add).
- Issue ID 521579, 508630, 519918, 521983: The statistics of service group members do not appear correctly in the configuration utility.
- Issue ID 522511, 517993: The NetScaler configuration utility displays the following error message if a user with no shell access logs on to the NetScaler appliance: "Not authorized to execute this command".
- Issue ID 522654: If you configure a command policy for a system user (System> User Administration > Users > <username> >Edit > Insert) by using the NetScaler configuration utility, the check-boxes do not function as expected on the Command Policies screen.
- Issue ID 375277, 322602, 334465, 396405, 412455, 419503, 438382, 438534, 438796, 441853, 446387, 448361: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.
- Issue ID 420736, 536924: When you use the configuration utility to create a certificate, an error message appears even if the validity period specified is within the acceptable range.
- Issue ID 524143: The NetScaler configuration utility displays the following error message if a user with no shell access logs on to the NetScaler appliance: "Not authorized to execute this command".
- Issue ID 529177: Although the default value of the sslv2redirect parameter is “Disabled,” the configuration utility incorrectly shows this value as “Enabled” for a new SSL virtual server.

Content Switching

- Issue ID 523636, 532832, 533690: If you perform the following sequence of actions, the second command fails when the restart process runs the commands, because that process adds the gotoprioritypressionto the second binding:

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

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

  3. Save the configuration and restart the appliance.

GSLB

- Issue ID 497412: 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.
- Issue ID 433094, 469937, 517974: 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.
- Issue ID 505932: A NetScaler appliance in a GSLB configuration might fail if the public IP address of a GSLB service is different on two GSLB sites and, on one of the sites, the public IP address for that service is the address of a load balancing virtual server.
- Issue ID 517961: If the disablePrimaryOnDown parameter is configured on the primary GSLB virtual server, the primary GSLB virtual server remains in the DISABLED state even after its health state is UP. The backup GSLB virtual server continues to serve the traffic until HA failover, or until you manually enable the primary GSLB virtual server.
- Issue ID 498854: 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
- Issue ID 511878: 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.
- Issue ID 519589: All GSLB features except DNS views, auto sync, and static proximity are supported for IPV6.

High Availability

- Issue ID 524146, 526699: 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.
- Issue ID 519085, 525203, 533671, 534616, 537991, 539518, 541525: If the link between the primary and secondary appliance is very slow and there are a large

number (millions) of sessions to be synchronized (because of, for example, load balancing persistence), the primary appliance quickly consumes all the NetScaler memory available for buffering. The lack of buffer space for other subsystems can result in various disruptions, such as failover.

Load Balancing

- Issue ID 516615: 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

- Issue ID 505543: 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.
- Issue ID 519644: 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.
- Issue ID 443027: 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 previously identified by its IP address.

NetScaler Insight Center

- Issue ID 541712: You cannot install an SSL certificate on a NetScaler Insight Center virtual appliance.

Networking

- Issue ID 522538: Upon receiving Generic Routing Encapsulation (GRE) packets as IP fragments on a virtual server with protocol ANY, the NetScaler ADC fails and restarts. This occurs only when you do not explicitly configure a GRE tunnel on the NetScaler ADC.
- Issue ID 438901: In a high availability (HA) configuration, ACL rules that are configured to block SSH related packets also block HA file synchronization that internally uses the SSH protocol.
- Issue ID 355965, 485260: In an active-active configuration, services bound to the backup VIP addresses do not send monitor probes to the associated servers.
- Issue ID 528554: An ACL6 rule might not get evaluated for a series of TCP packets.
- Issue ID 507345: 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.

Platform

- Issue ID 510673, 517241, 538267: 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.

System

- Issue ID 524949: 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.
- Issue ID 527320, 527211: If the NetScaler appliance uses the HTTP pipeline to parse an HTTP request, and the parsing process fragments the request packet, the appliance might not UNSET the NS_FINAL_DATA flag after receiving a fragment of the packet. In that case, the appliance will fails.
- Issue ID 504910: If a non-HTTP request is received on an HTTP virtual server, the transaction might fail.
- Issue ID 532042, 447664, 532587, 533164: 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.
- Issue ID 451841, 332826 , 346327 , 361979 , 465489 , 485864: When upgrading the NetScaler software from release 9.3, without a cache license, to release 10.0 or later, with a cache license, you have to apply the cache configuration manually to enable the integrated caching feature.
- Issue ID 519004, 528861: 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.
- Issue ID 286861, 301935, 513312, 522183, 541332: 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.
- Issue ID 486257: 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.
- Issue ID 528309: A NetScaler VPX virtual appliance with multiple packet engines fails if you enable the nstrace feature in TX mode with an advanced filter expression.
- Issue ID 488110, 496136: The save ns config command and the nsnetsvc process fail under low memory conditions.
- Issue ID 494911, 481032, 511763, 528309, 532708, 538507: If you enable the nstrace feature in TX mode with an advanced filter expression, the NetScaler appliance fails.
- Issue ID 506378: The NetScaler backup and restore functionality now creates a backup of each of the following configuration files: inetd.conf, ntp.conf, syslog.conf, newsyslog.conf, crontab, host.conf, hosts, ttys, sshd_config, httpd.conf, monitrc, rc.conf, ssh_config, localtime, issue, and issue.net.

User Interface

- Issue ID 528818, 529425: The memory allocation API, malloc, returns a NULL value if it does not obtain memory for the nscollect utility. If the nscollect utility tries to dereference this NULL pointer, the result is a memory segmentation error.
- Issue ID 368832: The NetScaler ADC generates SNMP clear alarm traps for successful cases of haVersionMismatch, haNoHeartbeats, haBadSecState, haSyncFailure, and haPropFailure error events in an HA configuration.
- Issue ID 524080, 448724: The SNMP counter of type cntr32 has been changed to a gauge counter.

WIonNS

- Issue ID 508743: You can now optionally configure agCallbackURL from agURL. The agURL would represent the front end Access Gateway (AG) for the client. The agCallback is for communication between Web Interface (WI) and AG. Also, The agCallbackURL is an optional parameter. Use the following command to configure agCallbackURL:

  add wi site /Citrix/new http://agee.citrix.com http://sta.citrix.com -agCallbackUrl http://callback.citrix.com

Known Issues and Workarounds

AAA-TM

- Issue ID 437454: 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.
- Issue ID 530287, 536545: In a high availability setup, AAA-TM sessions are not removed from the secondary appliance even after the AAA-TM sessions are logged out.

  Workaround: Remove the sessions manually by executing the "kill aaa sess" command. You might have to execute the command multiple times.
- Issue ID 332831: The rule (expression) in a AAA-TM policy can be from one to 1434 characters in length. If you enter a longer rule, AAA-TM displays an "invalid rule" error.
- Issue ID 457817: 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.

- Issue ID 481876: 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.
- Issue ID 519898: The "set appfw" command cannot be executed on the Netscaler ADC if TACACS server is used for authorization. An error message -"Not authorized to execute this command" might be seen.

Acceleration

- Issue ID 535130: 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.

AppFlow

- Issue ID 396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.
- Issue ID 327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.
- Issue ID 525568: The timestamp in AppFlow records are not in NTP format.

Application Firewall

- Issue ID 427798: A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.
- Issue ID 430014: 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

- Issue ID 283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.
- Issue ID 510006: For some malformed requests, the NetScaler application firewall log messages might not include the client IP address.
- Issue ID 506653: 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.
- Issue ID 511654: For some requests, the application firewall log message for a Field Consistency violation might not include the name of the field that triggered the violation.
- Issue ID 519792: The NetScaler appliance might fail if improperly written regular expressions used in the application firewall configuration result in excessive processing time.

  Workaround: Use efficient regular expressions.
- Issue ID 498912: 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.
- Issue ID 489691: 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.
- Issue ID 466329: 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.
- Issue ID 451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.
- Issue ID 532248: 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.

- Issue ID 530277: A POST request with an attached word document is silently blocked by the application firewall for a customized application.
- Issue ID 372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

  For example, if you had two sets of custom signatures, named "custom_signatures" and "custom_signatures_2", that were based on copies of the default signatures file, you would update the signatures on your NetScaler ADC by issuing the following commands:

  > update appfw signatures "*Default Signatures"

  > update appfw signatures "custom_signatures"

  > update appfw signatures "custom_signatures_2"
- Issue ID 455652: The auto-update operation restores the default SQL/XSS patterns in the signatures. If the user edits a signature to remove any of the SQL/XSS patterns, the removed patterns might reappear in the signature when it is auto-updated.
- Issue ID 457926, 506333: 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.

Application firewall

- Issue ID 511254: 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.
- Issue ID 510509: In release 9.3, if a NetScaler ADC has only a standalone application firewall license, the user is able to bind a classic application firewall policy to the load balancing virtual server. In release 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 in both the CLI and the GUI.

Cluster

- Issue ID 519327, 542633: 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.

Command Line Interface

- Issue ID 512526, 527066, 545578: The NetScaler command line interface exists abruptly upon executing the "show dns addRec -format old" command.

Configuration Utility

- Issue ID 490130: When you use the configuration utility to create a FIPS key, the FIPS wizard fails to respond.
- Issue ID 459703: In a high availability setup, if you run the "add ssl certkey" command on the primary node, and the certificate and key files are not present on the secondary node, the command fails on the secondary node. However, the configuration utility does not display an error message.
- Issue ID 400073, 401262: 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
- Issue ID 469755: If you open the NetScaler ADC configuration utility on multiple browser tabs, and if you disable a feature on one of the tabs, the other tabs are not automatically refreshed.

  Workaround: Manually refresh the tabs.
- Issue ID 388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml

- Issue ID 374437: If, when using the configuration utility to configure a NetScaler ADC, you press Alt+Tab to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press Alt+Tab a second time.
- Issue ID 499223: The maximum length for creating a NetScaler ADC system user password (System > User Administration > Users) is 127. The GUI tooltip displays this value as 255, which is incorrect.
- Issue ID 414807: 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.
- Issue ID 389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 470941: 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 .
- Issue ID 414422: When using the Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.
- Issue ID 482135: Java Runtime Environment (JRE) does not work on Internet Explorer version 10.

  Workaround: Press F12 and set the Document Mode and Browser mode to Internet Explorer 9.
- Issue ID 485314: On the Reporting tab of the NetScaler GUI, if you have chosen to use the time zone settings of the NetScaler ADC, the System Overview graph does not reflect the time zone set on the NetScaler ADC. The values in the graph are for the GMT time zone.
- Issue ID 483226: 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: In release 10.1, provide only the FIPS key. For example, rsa.key.

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

Content Switching

- Issue ID 541667: If your content switching virtual server is associated with a load balancing virtual server that has a backup virtual server, and if the primary load balancing virtual server is disabled, an HTTP 503 error message appears for some time before the traffic is directed to the backup virtual server.

- Issue ID 522510, 528782, 538223: In certain cases, if the state of a load balancing virtual server changes, the NetScaler appliance might fail while changing the state of the associated content switching virtual server.

Content Switching/Load Balancing

- Issue ID 399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

DNS

- Issue ID 458313: When NetScaler is configured as DNS proxy and it receives a DNSSEC query with Checking Disbaled (CD) bit set, it does not pass the bit as is to the server at the back end. It instead turns the bit off. This impacts deployments where the NetScaler is load balancing DNSSEC aware resolver. The impact is that the resolver will check the DNSSEC signatures even if the client had not requested to do so by setting the CD bit.
- Issue ID 382478: 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.
- Issue ID 458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.

  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache, with the AA bit unset and TTL decremented.

  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache, with the AA bit set and the original TTL.

GSLB

- Issue ID 499523: In all releases of 10.0 and 10.1, the "show server" output does not include IP address and state information for GSLB services.

  This feature works in all builds of the 9.3 and 10.5 releases.

Graphical user Interface

- Issue ID 511638: If you do not specify the deployment details when you import the SharePoint AppExpert template, you cannot configure backend servers.

High Availability

- Issue ID 534795: In a high availability configuration, with failSafe mode enabled on the secondary node, the node might briefly become primary when restarted.
- Issue ID 471294: 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.

- Issue ID 479666, 507519, 541503: 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.
- Issue ID 537496: 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.

  Workaround: After the HA pair is stabilized, perform a forced synchronization, on either the primary or the secondary node.

  To perform a forced synchronization use the following command:

  force ha sync

Integrated Caching

- Issue ID 440107, 440389: 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".
- Issue ID 486535: In a NetScaler deployment that has integrated caching and SSL enabled, the NetScaler can crash in the following scenario:

  1. Client1 requests for an object that is not in cache.

  2. While the NetScaler fetches the object from the backend server, client2 (a slow client) sends a request for the same object.

  3. Client1 now decides to reset the connection.

  4. When available, NetScaler serves the object to the client2.

  However, since client2 is slow, large data is piled up on the NetScaler that needs to be forwarded to client2. When the NetScaler tries to send this large data to the client, the NetScaler can crash.

Load Balancing

- Issue ID 464952: If a DNS autoscale service group is bound to a virtual server, the "show lb vserver" command output displays one extra service bound to the virtual server.
- Issue ID 466094, 534755: If the load balancing (LB) feature is not licensed, and you try to enable an LB virtual server, an error message appears.
- Issue ID 540965: 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.
- Issue ID 455133: If the FQDN is not resolvable, you might notice high CPU utilization on the NetScaler ADC.
- Issue ID 441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.
- Issue ID 460040: 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.
- Issue ID 516606, 528242: If all of the following conditions are present, they might lead to a situation in which CPU usage is significantly different among the packet engines (PEs):

  1. The maximum number of clients (maxclients) for a service is set to a value less than the number of PEs in the system.

  2. Connections to this service have a high degree of connection reuse, that is, multiple requests are sent on the same TCP connection.

  3. Requests for connections to this service cause a surge queue buildup.

  If the maxclient setting is less than the number of PEs, only some PEs can open connections. After the maxclient limit is reached, PEs that have open connections are not likely to close them, because they are using those connections to process the traffic generated by high connection reuse and the large surge queue. As a result, the other PEs might not be able to open new connections. They therefore have a lower level of CPU usage, because they cannot participate in processing the surge queue.

  This is expected behavior and usually does not cause any issues. However, if some of the PEs have near 100% CPU usage while the other PEs have relatively low CPU usage, you might want to limit the maximum requests per connection by using the "set service <name> -maxReq <positive_integer>" command, so that the PEs close connections that have delivered the specified number of requests. This evens out the CPU usage, because it allows the other PEs to open connections to the service.
- Issue ID 524079: 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.

SureConnect

- Issue ID 526782: 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.

NetScaler 1000V

- Issue ID 471373: EULA should not be prompted when interface type is modified from Shared to Passthrough for a NetScaler-VSB provisioned on Nexus 1010/1110 platforms.

NetScaler Insight Center

- Issue ID 441163: NetScaler Insight Center might not display reports under the following set of conditions:

  -NetScaler ADCs that are configured for Network Address Translation (NAT) are added to the NetScaler Insight Center inventory.

  -A NetScaler ADC and a NetScaler Insight Center virtual appliance are in different networks and are configured for NAT.

- Issue ID 388096, 423109: When you launch XenApp through Citrix Receiver (standard edition), the app launch duration is not calculated and is shown as zero.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue ID 409634: All the metrics except bandwidth and hits display the average values.
- Issue ID 379876, 424686, 437964: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.
- Issue ID 446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue ID 386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later build is supported.

  Workaround: To upgrade to build 120.13 or later, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same.

- Issue ID 399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off:

The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.

- Issue ID 397236: On the Dashboard > HDX Insight > Users page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but the right pane displays the values for the period selected from the drop-down list.
- Issue ID 394526: On the Dashboard > Web Insight > Applications page, the values shown when you select "Response Time" from the drop-down list can be incorrect.
- Issue ID 368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.

NetScaler VPX Appliance

- Issue ID 405383, 360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.
- Issue ID 405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platforms MacVTap interfaces.

  Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).

Networking

- Issue ID 318684: 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.
- Issue ID 485260: 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.
- Issue ID 529317: 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

- Issue ID 323127: The NetScaler ADC might become unresponsive if you run the show route operation during a dynamic route addition or deletion process.
- **Issue ID 371613**

  In a high availability configuration with the network firewall mode set to BASIC on the current secondary node, synchronization of configuration files from the primary to secondary node fails, regardless of whether you run the "sync HA files" command from the NetScaler command line or by using the Start HA files synchronization dialog box in the configuration utility.

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

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

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

  On the primary node:

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

  On the secondary node:

  > add acl ACL-example -srcIP 198.51.100.9 -protocol TCP -destport 22
- Issue ID 383958, 411806: $ 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.
- Issue ID 507908: An active FTP connection might get reset for no apparent reason, regardless of the state of the random source port.
- Issue ID 399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.

Platform

- Issue ID 402111: VLAN tagging is not supported on a Netscaler VPX instance operating in MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, or MacVTap-Passthrough interface mode.
- Issue ID 402113: L2 mode is not supported on NetScaler VPX instances running on a Linux-KVM host.
- Issue ID 407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.
- Issue ID 407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.

Policies

- Issue ID 422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

  Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP.

  !CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)

- Issue ID 390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

Reporting

- Issue ID 368982: After you import a custom data source, the charts for the counters under "System entities statistics" are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 521569: 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.
- Issue ID 402423: 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]

- Issue ID 455821: An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.
- Issue ID 509608: If a certificate has a validity of 100 years, Days to Expiration incorrectly appears as 0 in the NetScaler command line interface and the configuration utility.
- Issue ID 519368: In rare cases, the "update ssl certKey" command fails and, in spite of displaying a "Resource already exists" error message, creates a stale duplicate entry with the same certificate-key pair in the configuration file (ns.conf).
- Issue ID 468198: If the format of a CRL is incorrect or the issuer of a CRL does not match the specified CA certificate, and you run the "show crl" command, an error message showing the CRL status as invalid appears.

System

- Issue ID 480258, 494482, 523853: 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.
- Issue ID 524320: If an LACP channel is bound to nine or more interfaces and is a member of a tagged VLAN, deleting the channel from a service VM can cause the NetScaler appliance to fail intermittently.
- Issue ID 529493: A NetScaler appliance fails if it attempts to apply HTML injection to a server response that does not have a content type header.
- Issue ID 427126, 441982, 452885, 456645: 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.
- Issue ID 523473: Every Domain Based Service (DBS) on a NetScaler appliance is assigned two monitors. Therefore, the limit of 7500 monitors can result in a memory allocation failure when you add a new service to the appliance.
- Issue ID 430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.
- Issue ID 508410: HA SYNC takes longer than expected for NetScaler 1000V. For example, for synchronizing ns.conf file of 38.4 KB size, it takes 70-100 seconds.
- Issue ID 377618, 341460, 351127, 364015, 481575, 499259: 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]
- Issue ID 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.
- Issue ID 501100: Setting 'Request timeout' or 'Request timeout action' in HTTP Profiles can cause the NetScaler to fail in some situations.
- Issue ID 536576: 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.
- Issue ID 522665: 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.

User Interface

- Issue ID 542702: If, while upgrading a NetScaler appliance, you change the RSS key type, the configuration utility does not display a warning message to restart the NetScaler appliance.
- Issue ID 475830, 449234: A large configuration file puts a heavy load on the management CPU. The resulting delay in displaying the output of the "show ns runningconfig" command might exceed the timeout value.

  Workaround: If you are using a script to fetch the output for "show ns runningConfig" command, and the script has a placeholder for timeout value, modify the script to increase the timeout value to 500 seconds.

Web Interface

- Issue ID 397150: 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.

XML API

- Issue ID 363145: The following APIs are not available in version 10.1 or later:

  - bindservicegroup_state2

  - unsetnslimitidentifier_selectorname. Use unsetnslimitidentifier_selector instead.

Chapter 2

Build 130.13

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 130.13

Replaces build: 130.11

Release date: February 2015

Release Notes version: 3.0

Language supported: English (US)

Bug Fixes

AAA-TM

- Issue ID 505809, 507692: 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.
- Issue ID 474918, 502915: The NetScaler ADC no longer sets the NSC_TMAA session cookie during a secure load balancing virtual server session.
- Issue ID 507386: 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.

Action Analytics

- Issue ID 406457: 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

Application Firewall

- Issue ID 315183: 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.

- Issue ID 443673: The Application Firewall PCI-DSS report does not display signature bindings. The Profile Settings section of the report shows bound signatures as "Not Set".
- Issue ID 476206: 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.
- Issue ID 473322, 466491: 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.
- Issue ID 472476, 418036: 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.
- Issue ID 488369: 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.
- Issue ID 481899: The NetScaler ADC might fail if a transaction is aborted before the application firewall completes processing the request.
- Issue ID 423150: The application firewall PCI-DSS report does not contain information about the "SQLInjectionCheckSQLWildChars" parameter.
- Issue ID 505272, 505039: 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.

Cache Redirection

- Issue ID 502366, 505091, 514785: Applying multiple ACL rules causes excessive consumption of CPU cycles. As a result, the NetScaler ADC might become unresponsive.
- Issue ID 497866, 502366: 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.

Citrix NetScaler 1000V

- Issue ID 499050

NetScaler-VSB supporting 9 virtual NICs comes up with 7 virtual NICs. This happens when there is an existing NetScaler-VSB (pre 10.5-52.x) on Nexus1110x that supports 7 virtual NICs.

CloudBridge Connector

- Issue ID 440781: When the state of a CloudBridge connector tunnel is DOWN, there is a delay in displaying the related log messages (from the /tmp/iked.debug file) on the Create CloudBridge Connector page of the configuration utility.

Cluster

- Issue ID 486259: From NetScaler 10.5 Build 52.x, 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.x and then downgrade to an earlier build, the cluster will not work as it now expects the separate cluster license file.

Configuration Utility

- Issue ID 490142: 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.

- Issue ID 489884: The configuration utility does not display SSL policies if you navigate to Traffic Management > SSL > Policies to create a policy.

  Workaround: Navigate to Traffic Management > SSL and, in the right pane, select SSL Policy Manager. Or click the refresh button on the top right corner to display the SSL policies.

- Issue ID 375277, 322602, 334465, 396405, 412455, 419503, 438382, 438534, 438796, 441853, 446387, 448361: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.

- Issue ID 511565: If a connection from a client to a NetScaler ADC is closed without the client logging out, the session created for that connection remains active until the configured timeout period lapses. If this occurs frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.

- Issue ID 501644, 505641, 509379: 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.

- Issue ID 494804: If the number of interfaces that you created are more than eight, the Reporting tab in the configuration utility displays only eight interfaces to be monitored.
- Issue ID 512427: If a user with read-only permissions opens a monitor (Configuration > Traffic Management >Load Balancing> Monitors), the configuration utility displays the 'Not authorized to execute this command' error message.

Content Switching

- Issue ID 501856: 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.

DNS

- Issue ID 382478: 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.
- Issue ID 437529: 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.

Data Stream

- Issue ID 507709: 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.

GSLB

- Issue ID 485811: 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.

Graphical User Interface

- Issue ID 513132: A user session is not terminated if the user logs out of NetScaler ADC by using the configuration utility. The session is terminated only after the session timeout is complete.
- Issue ID 502309, 503357: 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.

Load Balancing

- Issue ID 502338: 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.

- Issue ID 489400: In a high availability setup, a failover might disconnect active connections even though stateful connection failover is enabled on the virtual servers.

  Workaround:

  Check the output of the “show rpcnode” command. If it shows an asterisk (*) for the SRCIP parameter, run the “set rpcnode <remote NSIP> -scrip <local NSIP>” command.

- Issue ID 497470: 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.

  Workaround: Run the “set lb group –persistenceType” command to reset the persistence on the virtual servers that are bound to the group.

- Issue ID 457639: 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.

- Issue ID 504209: You can now bind loopback members (for example 127.0.0.1) to service groups. Previously, you could bind loopback members to services only.

NITRO API

- Issue ID 507594: When AppFlow is enabled on a NetScaler, the following query, which requests console messages from nsconmsg tool, results in httpd core dump due to large buffer length.

  http://<NSIP>/nitro/v1/config/clioutput?args=command:"shell+nsconmsg+%2DK+%2Fvar%2Fnslog%2Fnewnslog+%2Dd+consmsg"

NetScaler Insight Center

- Issue ID 505985, 507879, 507882: The NetScaler ADCs being monitored by NetScaler Insight Center might fail if, while ICA sessions are active, you enable AppFlow for ICA and then either clear the configuration or disable and re-enable AppFlow on NetScaler Insight Center.

- Issue ID 490680: The NetScaler ADC might fail if you enable AppFlow for ICA and access XenApp or XenDesktop through the Windows Receiver client.

Networking

- Issue ID 508631, 509453: 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.

- Issue ID 441005: Old or stale OSPF LSAs might exist after a warm restart, or a restart after a power failure, resulting in a triple flip.

- Issue ID 510173: 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.
- Issue ID 502213, 512248: The NetScaler ADC might become unresponsive when ICMP error packets match a forwarding session rule.
- Issue ID 496237: For a load balancing server configured on a non-default traffic domain, modifying the IP address of the server also changes the name of the server.
- Issue ID 490341: With MAC based forwarding (MBF) 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.
- Issue ID 497277: The NetScaler ADC might not update its bridge and ARP tables with the information received from GARP messages.

Platform

- Issue ID 498929: NetScaler VPX instances running on Xen Server might consume a high percentage of CPU cycles while processing 1G traffic.
- Issue ID 484123: NetScaler supports Multi-PE for Hyper-V.
- Issue ID 487169: On a NetScaler ADC that has a Small Form-factor Pluggable (SFP) interface with part number FTLF8519P2BNL, disabling this interface might not disable the interface of the peer device.

Policies

- Issue ID 508510, 513724, 517150, 518535, 519945: 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.

Policies

- Issue ID 506761, 519776, 446507, 463284, 500444: 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.

SSL

- Issue ID 492087, 510038, 510483: 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.
- Issue ID 494093, 485932, 492191, 492797, 497321: If session reuse is enabled on the NetScaler and a network error occurs, the NetScaler attempts to clear the session information so that it is not reused for a subsequent session request from the same client. In rare cases, the NetScaler might fail during this cleanup process.

System

- Issue ID 418028, 409722, 467187: The nsnetsvc process size increases when the "stat" command is executed.
- Issue ID 497321, 501856, 502116, 502902, 517374: 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.
- Issue ID 494013: 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.

Known Issues and Workarounds

AAA-TM

- Issue ID 457817: In NetScaler 9.3 and previous versions, the NetScaler ADC used the SNIP 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 the SNIP (not the NSIP) as the source IP address in version 10.1 and subsequent versions, 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 action.

- Issue ID 437454: The NetScaler ADC AAA-TM user interface has a timeout of 20 seconds. If authenticating 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 that authentication failed or any other problem that affects users. It can safely be ignored.
- Issue ID 481876: 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.
- Issue ID 332831: The rule (expression) in a AAA-TM policy can be from one to 1434 characters in length. If you enter a longer rule, AAA-TM displays an "invalid rule" error.

AppFlow

- Issue ID 327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.
- Issue ID 396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.
- Issue ID 472971: The HTML Injection JavaScript is incorrectly inserted into one of the JavaScript responses sent by the server, causing the page to fail to load.

Application Firewall

- Issue ID 498912: 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.
- Issue ID 489691: 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.
- Issue ID 455652: The auto-update operation restores the default SQL/XSS patterns in the signatures. If the user edits a signature to remove any of the SQL/XSS patterns, the removed patterns might reappear in the signature when it is auto-updated.
- Issue ID 466329: 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.
- Issue ID 399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

For example, if you had two sets of custom signatures, named "custom_signatures" and "custom_signatures_2", that were based on copies of the default signatures file, you would update the signatures on your NetScaler ADC by issuing the following commands:

> update appfw signatures "*Default Signatures"

> update appfw signatures "custom_signatures"

> update appfw signatures "custom_signatures_2"

- Issue ID 283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.
- Issue ID 430014: 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

- Issue ID 457926, 506333: 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.
- Issue ID 451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you

configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.

- Issue ID 427798: A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.
- Issue ID 511654: For some requests, the application firewall log message for a Field Consistency violation might not include the name of the field that triggered the violation.
- Issue ID 364134: In the configuration utility, when you perform the Show Bindings operation, globally bound auditing syslog policies do not appear under Application Firewall. This issue occurs only in a cluster setup.

  Workaround: Display the bindings in the command line interface, by using the "show system global" command.
- Issue ID 510006: For some malformed requests, the NetScaler application firewall log messages might not include the client IP address.
- Issue ID 372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 511254: 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.

  The workaround is to turn off form field tagging and credit card checks.

Cache Redirection

- Issue ID 509690: 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)"

  Workaround:

  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

Command Line Interface

- Issue ID 512526: The NetScaler command line interface exists abruptly on executing the "show dns addRec -format old" command.

Configuration Utility

- Issue ID 485314: On the Reporting tab of the NetScaler GUI, if you have chosen to use the time zone settings of the NetScaler ADC, the System Overview graph does not reflect the time zone set on the NetScaler ADC. The values in the graph are for the GMT time zone.
- Issue ID 499223: The maximum length for creating a NetScaler ADC system user password (System > User Administration > Users) is 127. The GUI tooltip displays this value as 255, which is incorrect.
- Issue ID 490130: When you use the configuration utility to create a FIPS key, the FIPS wizard fails to respond
- Issue ID 483226: 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: In release 10.1, provide only the FIPS key. For example, rsa.key.

  In release 10.5, you must specify the complete file path to the FIPS key. For example, nsconfig/ssl/folder1/folder2/rsa.key.
- Issue ID 470941: You cannot use the configuration utility to add signatures to an existing application firewall policy.

  Workaround: Use the command line interface .
- Issue ID 374437: If, when using the configuration utility to configure a NetScaler ADC, you press Alt+Tab to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press Alt+Tab a second time.
- Issue ID 459703: In a high availability setup, if you run the "add ssl certkey" command on the primary node, and the certificate and key files are not present on the secondary node, the command fails on the secondary node. However, the configuration utility does not display an error message.
- Issue ID 400073, 401262: 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

- Issue ID 389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

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

- Issue ID 414422: When using the Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.

- Issue ID 469755: If you open the NetScaler ADC configuration utility on multiple browser tabs, and if you disable a feature on one of the tabs, the other tabs are not automatically refreshed.

  Workaround: Manually refresh the tabs.

- Issue ID 414807: 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.

- Issue ID 388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml

- Issue ID 353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list in the "Create Persistency Group" dialog box (Load Balancing > Persistency Groups > Add) and in the "Create Persistency Group" dialog box list that appears when you click the "Name" button in the list "Create Content Switching Action" dialog box "Content Switching > Actions > Add).

- Issue ID 482135: Java Runtime Environment (JRE) does not work on Internet Explorer version 10.

Workaround: Press F12 and set the Document Mode and Browser mode to Internet Explorer 9.

- Issue ID 456428: 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.
- Issue ID 278002, 273176, 389874: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.

Content Switching/Load Balancing

- Issue ID 399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

DNS

- Issue ID 458313: When NetScaler is configured as DNS proxy and it receives a DNSSEC query with Checking Disbaled (CD) bit set, it does not pass the bit as is to the server at the back end. It instead turns the bit off. This impacts deployments where the NetScaler is load balancing DNSSEC aware resolver. The impact is that the resolver will check the DNSSEC signatures even if the client had not requested to do so by setting the CD bit.
- Issue ID 458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.

  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.

  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.

GSLB

- Issue ID 497412: If you perform a force sync of the GSLB configuration, the non-default settings on the RPC node are lost. As a result, the GSLB auto-sync functionality is lost.
- Issue ID 511878: If the length of the domain name bound to a GSLB virtual server exceeds 31 characters, the domain name is displayed as HASHED STRING while performing an SNMP MIB Walk operation.

Graphical user Interface

- Issue ID 511638: If you do not specify the deployment details when you import the SharePoint AppExpert template, you cannot configure backend servers.

HTTP Profiles

- Issue ID 501100: Setting 'Request timeout' or 'Request timeout action' in HTTP Profiles can cause the NetScaler to fail in some situations.

High Availability

- Issue ID 471294: 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.

Integrated Caching

- Issue ID 486535: In a NetScaler deployment that has integrated caching and SSL enabled, the NetScaler can crash in the following scenario:

  1. Client1 requests for an object that is not in cache.

  2. While the NetScaler fetches the object from the backend server, client2 (a slow client) sends a request for the same object.

  3. Client1 now decides to reset the connection.

  4. When available, NetScaler serves the object to the client2.

  However, since client2 is slow, large data is piled up on the NetScaler that needs to be forwarded to client2. When the NetScaler tries to send this large data to the client, the NetScaler can crash.

- Issue ID 440107, 440389: 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".

Load Balancing

- Issue ID 499523: In all releases of 10.0 and 10.1, "show server" is missing information for GSLB services: IP address and state.

  This feature works in all releases of 9.3 and 10.5.

- Issue ID 460040: 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.
- Issue ID 455133: If the FQDN is not resolvable, you might notice high CPU utilization on the NetScaler ADC.
- Issue ID 277862: With a NetScaler Web 2.0 Push configuration in streaming mode, if the length of the response from the server is in the range of 10^n - 2^4n bytes, where n=1, 2, 3, and so on (for example, 1-15, 100-255, or 1000-4095 bytes), the push virtual server adds a byte to the response that it sends to the client. As a result, after the first response, subsequent updates sent on the same connection are lost.
- Issue ID 464952: If a DNS autoscale service group is bound to a virtual server, the "show lb vserver" command output displays one extra service bound to the virtual server.
- Issue ID 505543: 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.
- Issue ID 441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.
- Issue ID 516615: 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
- Issue ID 516606: If all of the following conditions are present, they might lead to a situation in which CPU usage is significantly different among the packet engines (PEs):

  1. The maximum number of clients (maxclients) for a service is set to a value less than the number of PEs in the system.

  2. Connections to this service have a high degree of connection reuse, that is, multiple requests are sent on the same TCP connection.

  3. Requests for connections to this service cause a surge queue build up.

  If the maxclient setting is less than the number of PEs, only some PEs can open connections. After the maxclient limit is reached, PEs that have open connections are not likely to close them, because they are using those connections to process the traffic generated by high connection reuse and the large surge queue. As a result, the other PEs might not be able to open new connections. They therefore have a lower level of CPU usage, because they cannot participate in processing the surge queue.

This is expected behavior and usually does not cause any issues. However, if some of the PEs have near 100% CPU usage while the other PEs have relatively low CPU usage, you might want to limit the maximum requests per connection by using the "set service <name> -maxReq <positive_integer>" command, so that the PEs close connections that have delivered the specified number of requests. This evens out the CPU usage, because it allows the other PEs to open connections to the service.

NS-Platform

- Issue ID 524320: If an LACP channel is bound to nine or more interfaces and is a member of a tagged VLAN, deleting the channel from a service VM can cause the NetScaler appliance to fail intermittently.

NetScaler 1000V

- Issue ID 471373: EULA should not be prompted when interface type is modified from Shared to Passthrough for a NetScaler-VSB provisioned on Nexus 1010/1110 platforms.

NetScaler Insight Center

- Issue ID 397236: On the Dashboard > HDX Insight > Users page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but, the right pane displays the values for the period selected from the drop-down list.
- Issue ID 379876, 424686, 437964: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.
- Issue ID 409634: All the metrics except bandwidth and hits display the average values.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue ID 368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.
- Issue ID 385821: When an ICA session is initiated by launching XenDesktop, the user name is displayed along with the domain name "(user-id@domain-name)".
- Issue ID 388096, 423109: When you launch XenApp through Citrix Receiver (standard edition), the app launch duration is not calculated and is shown as zero.
- Issue ID 446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue ID 399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off:

The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.

- Issue ID 386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later builds is supported.

  Workaround: To upgrade to build 120.13 or later build, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same .
- Issue ID 441163: NetScaler Insight Center might not display reports under the following set of conditions:

  -NetScaler ADCs that are configured for Network Address Translation (NAT) are added to the NetScaler Insight Center inventory.

  -A NetScaler ADC and a NetScaler Insight Center virtual appliance are in different networks and are configured for Network Address Translation (NAT.)
- Issue ID 394526: In the Dashboard > Web Insight > Applications page, the values shown when you select "Response Time" from the drop-down list can be incorrect.

NetScaler VPX Appliance

- Issue ID 405383, 360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.
- Issue ID 405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platforms MacVTap interfaces.

  Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).

Networking

- Issue ID 507345: 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.
- Issue ID 399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.
- Issue ID 383958, 411806: $ 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.

- Issue ID 318684: In an HA configuration in INC mode running the OSPF routing protocol, the secondary node drops all the L3 traffic that has the destination that was advertised by the secondary node.
- Issue ID 485260: 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.
- Issue ID 323127: The NetScaler ADC might become unresponsive if you run the show route operation during a dynamic route addition or deletion process.
- Issue ID 371613: In a high availability configuration with the network firewall mode set to BASIC on the current secondary node, synchronization of configuration files from the primary to secondary node fails, regardless of whether you run the "sync HA files" command from the NetScaler command line or by using the Start HA files synchronization dialog box in the configuration utility.

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

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

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

  On the primary node:

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

  On the secondary node:

  > add acl ACL-example -srcIP 198.51.100.9 -protocol TCP -destport 22
- Issue ID 528554: An ACL6 rule might not get evaluated for a series of TCP packets.

Platform

- Issue ID 402113: L2 mode is not supported on NetScaler VPX instances running on a Linux-KVM host.
- Issue ID 402111: VLAN tagging is not supported on a Netscaler VPX instance operating in MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, or MacVTap-Passthrough interface mode.
- Issue ID 407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.
- Issue ID 407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.
- Issue ID 510673, 517241: NetScaler VPX instances running on VMware ESXi loose 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.

Policies

- Issue ID 390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

- Issue ID 422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

  Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP.

  !CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)

Reporting

- Issue ID 368982: After you import a custom data source, the charts for the counters under "System entities statistics" are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 468198: If the format of a CRL is incorrect or the issuer of a CRL does not match the specified CA certificate, and you run the "show crl" command, an error message showing the CRL status as invalid appears.
- Issue ID 402423: In a cluster setup, if you include the "cipherdetails" option in the "show ssl service" or "show ssl vserver" command, an incorrect message appears. This is only a display issue.

  For example,

  > sh ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]

- Issue ID 455821: An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.

System

- Issue ID 480258, 494482: 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.

- Issue ID 427126, 441982, 452885, 456645: 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.
- Issue ID 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.
- Issue ID 430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.
- Issue ID 377618, 341460, 351127, 364015, 481575, 499259: 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]
- Issue ID 508410: HA SYNC takes longer than expected for NetScaler 1000V. For example, for synchronizing ns.conf file of 38.4 KB size, it takes 70-100 seconds.

User Interface

- Issue ID 440208: If a new SSL certificate that requires a key is installed without the key, access to management service GUI is lost.
- Issue ID 475830, 449234: A large configuration file puts a heavy load on the management CPU. The resulting delay in displaying the output of the "show ns runningconfig" command might exceed the timeout value.

  Workaround: If you are using a script to fetch the output for "show ns runningConfig" command, and the script has a placeholder for timeout value, modify the script to increase the timeout value to 500 seconds.

Web Interface

- Issue ID 397150: 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.

XML API

- Issue ID 363145: The following APIs are not available in version 10.1 or later:

  - bindservicegroup_state2

  - unsetnslimitidentifier_selectorname. Use unsetnslimitidentifier_selector instead.

Chapter 3

Build 129.22

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 129.22

Replaces build: 129.11

Release date: October 2014

Release Notes version: 2.0

Language supported: English (US)

Enhancements

Networking

- Issue ID 486632: Now, the NetScaler appliance sends all ARP replies from the first interface (lexicographical order) of an LA channel.

Policies

- Issue ID 388879: You can now get the ethertype by using an advanced policy expression.

  Examples:

  - CLIENT.ETHER.ETHERTYPE.EQ(IPv4)

  - SERVER.ETHER.ETHERTYPE.EQ(IPv6)

SSL

- Issue ID 385499:

  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

Bug Fixes

AAA-TM

- Issue ID 474918, 502915: The NetScaler ADC no longer sets the NSC_TMAA session cookie during a secure load balancing virtual server session.
- Issue ID 493308: 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.
- Issue ID 476885: 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.
- Issue ID 488015: 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.
- Issue ID 478374: The Authorization header received from the client with the user credentials for 401 based authentication for KCD was intentionally corrupted by the NetScaler ADC as “Ahoutrization” before forwarding it to the backend. To avoid the risk of decoding the user-supplied credentials by using simple base64decode, the ADC now removes the incoming authorization header containing user credentials, and inserts a new Authorization header with a Kerberos token before sending the payload to the backend application.

Application Firewall

- Issue ID 479840, 472476, 482042: The application firewall parses multipart forms correctly according to the appropriate RFC.
- Issue ID 513952: The SQL wildcard characters (%, _, ^, []) were accidentally removed from the Citrix application firewall default signature object. This breaks the SQL wildcard functionality when the default signature file and its clones are used. This fix restores the wildcard characters in the default signature file. The application firewall detects them and flags the SQL Injection check violations.

  Workaround: You can manually add the wildcard characters to the affected builds, or you can upgrade to the latest build.
- Issue ID 503856: The NetScaler application firewall “Click to Rule” functionality is not working in the 51.x and the 52.x builds of release 10.5. With this fix, the user can successfully select the pertinent log message in the syslog viewer and deploy it as a relaxation rule.

- Issue ID 486231: If you update default signatures on the primary NetScaler ADC in an HA pair, you cannot sync the updated signatures to the secondary ADC.

  Workaround: Export the updated signatures, and import them on the secondary ADC.

- Issue ID 459031, 463351: 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.
- Issue ID 464641: If the application firewall receives a multipart POST request with a Content-Type header that contains a charset, it blocks that request as malformed.

Cache Redirection

- Issue ID 497866, 502366: 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.

Citrix NetScaler 1000V

- Issue ID 499050: NetScaler-VSB supporting 9 virtual NICs comes up with 7 virtual NICs. This happens when there is an existing NetScaler-VSB (pre 10.5-52.x) on Nexus1110x that supports 7 virtual NICs.

Cluster

- Issue ID 480071, 483171: When upgrading a cluster node to NetScaler 10.5, from any build of NetScaler 10.1, make sure that the "syncookie" parameter is disabled on the TCP profiles. Otherwise, there can be disruption in traffic flow.

Command Line Interface

- Issue ID 480639: The rbaOnResponse system parameter fails to work after you upgrade NetScaler ADC nCore or nCore VPX from version 9.3 to 10.x.

Configuration Utility

- Issue ID 488748: If you bind a load balancing monitor to a load balancing service, the Configure Service dialog box displays an incorrect value for response time on the Monitor tab.
- Issue ID 475653: If you bind a content switching policy to a content switching virtual server, an incorrect value appears in the Configure Virtual Server (Content Switching) dialog box. The error is on the CSW tab, in the Hits column under Policies.
- Issue ID 483340: The NetScaler Application Delivery Controller (ADC) and NetScaler Gateway are vulnerable to the arbitrary code execution in a SOAP interface, as described at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7140.

  With this fix, the ADC and NetScaler Gateway do not allow a remote attacker to execute arbitrary code.

- Issue ID 490142: 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.

- Issue ID 451546: A NetScaler ADC displays a Java error if you access it by using an sshd connection.

DNS

- Issue ID 484069: 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.
- Issue ID 471707: The DNS cache entries are not flushed if the DNS caching feature has been disabled for approximately 250 days.
- Issue ID 477552: 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.

DataStream

- Issue ID 479472, 501750: If a service group is used to load balance MSSQL servers that require Kerberos Constrained Delegation, the NetScaler ADC fails to use the proper service port to fetch tickets.

GSLB

- Issue ID 453144, 455417: 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.

High Availability

- Issue ID 469857: On a HA setup, even though the source IP is not explicitly set to *, the output of the "show ns rpcNode" commands shows the source IP as *. Therefore, when HA failover happens for the second time, the LB persistency session information is not propagated to the secondary node. This means that the information is not available when a forced failover is performed on the new primary node.

  The fix ensures that the NetScaler IP (NSIP) address of the local box is always set as the source IP address in a HA setup.

Integrated Caching

- Issue ID 488145: 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.

Load Balancing

- Issue ID 482113: 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.
- Issue ID 489197: 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.

Networking

- Issue ID 490190: The NetScaler ADC drops IPv4 packets related to the following protocols:
  - IPv6 encapsulation (41)
  - Fragment Header for IPv6 (44)
  - ICMP for IPv6 (58)
- Issue ID 460246: In a transparent cache redirection deployment, when a request is destined to a MAC address (say MAC-A) and the response for the request is sent from another MAC address (say MAC-B), the NetScaler ADC sends further requests to MAC-B. If MAC-B stops handling the requests, the session might get hung.
- Issue ID 480621, 478048: 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.
- Issue ID 432192: The CPU usage might be approximately 10% higher in NetScaler 10.5 version as compared to NetScaler 9.3 version.
- Issue ID 471651, 479882, 485831, 493232: 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.
- Issue ID 496564: The NetScaler ADC might fail to evaluate listen policies, containing source or destination ipv6 address/subnet, for certain IPv6 addresses.
- Issue ID 477402: In a high availability (HA) configuration, VMAC configuration might be lost when continuous HA failover happens.
- Issue ID 491473: 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.
- Issue ID 475622: The LACP channels of a NetScaler ADC might take around 7 minutes to become functional (UP state) after the NetScaler is restarted.
- Issue ID 480573: 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.

- Issue ID 480100, 483728: 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.

Policies

- Issue ID 493045: Using the "SYS.CHECK_LIMIT" expression in conjunction with any boolean expression can cause the NetScaler to crash.
- Issue ID 473721: The maximum value of the RelayState attribute that can be sent with the assertion that NetScaler sends is increased to 512 bytes. This applies to cases where the administrator configures a traffic policy to send assertion to a relying party.

Platform

- Issue ID 501834: For NetScaler platforms that have Small Form-factor Pluggable (SFP) transceivers, with part number FTLF8519P3BNL, the bootup log files show that the SFPs are unsupported, even though they are functioning properly. This issue occurs in the following releases:

  - NetScaler 9.3 Build 67.5 or earlier

  - NetScaler 10.1 Build 129.11 or earlier

  - NetScaler 10.5 Build 52.11 or earlier

SSL

- Issue ID 510483, 527995, 528484: Deployments with one or more SSL virtual servers with SNI enabled might have small memory leaks for each connection. Eventually, after millions of connections, the appliance runs out of memory and fails.
- Issue ID 484525: 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.

System

- Issue ID 471100, 425465, 484159, 484187: Changes made to the time zone are not reflected till the NetScaler appliance is warm rebooted.
- Issue ID 490192: The NetScaler intermittently fails to generate traps due to issues in propagating the alarm state to the SNMP daemon.
- Issue ID 480219: 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.
- Issue ID 478356: 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.

- Issue ID 484527: 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.

- Issue ID 477709: SNMP walk shows the operational status of a LA channel as DOWN even when it is in the PARTIAL-UP state.

XML

- Issue ID 450232: 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.

Known Issues and Workarounds

AAA-TM

- Issue ID 481876: 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.
- Issue ID 332831: The rule (expression) in a AAA-TM policy can be from one to 1434 characters in length. If you enter a longer rule, AAA-TM displays an "invalid rule" error.
- Issue ID 437454: The NetScaler ADC AAA-TM user interface has a timeout of 20 seconds. When authenticating to an external authentication server, if authentication takes more than 20 seconds, the following message appears in the logs: "libaaa recv failed". This message does not indicate that authentication failed or any other problem that affects users, and can safely be ignored.

Action Analytics

- Issue ID 406457: 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

AppFlow

- Issue ID 472971: The HTML Injection JavaScript is incorrectly inserted into one of the JavaScript responses sent by the server, causing the page to fail to load.
- Issue ID 396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.
- Issue ID 327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.

Application Firewall

- Issue ID 283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.
- Issue ID 399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

  For example, if you had two sets of custom signatures, named "custom_signatures" and "custom_signatures_2", that were based on copies of the default signatures file, you would update the signatures on your NetScaler ADC by issuing the following commands:

  > update appfw signatures "*Default Signatures"

  > update appfw signatures "custom_signatures"

  > update appfw signatures "custom_signatures_2"
- Issue ID 372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 443673: 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".
- Issue ID 427798: A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.
- Issue ID 457926: 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.

- Issue ID 466329: 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.
- Issue ID 451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.
- Issue ID 489691: 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.
- Issue ID 430014: 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

- Issue ID 364134: In the configuration utility, when you perform the Show Bindings operation, globally bound auditing syslog policies do not appear under Application Firewall. This issue occurs only in a cluster setup.

  Workaround: Display the bindings in the command line interface, by using the "show system global" command.

- Issue ID 498912: 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 th elogs: "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.
- Issue ID 472476, 418036: 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.
- Issue ID 423150: The application firewall PCI-DSS report does not contain information on the "SQLInjectionCheckSQLWildChars" parameter.

Content Switching

- Issue ID 501856: An invalid HTTP request that spans multiple TCP segments that is sent to a content switching virtual server can cause the NetScaler to skip the load balancing decision and initiate a connection from the SNIP to the content switching virtual server. This can cause the NetScaler appliance to crash.

  Preventive fix: There is a preventive fix that closes the client connection when this situation arises.

Citrix NetScaler 1000V

- Issue ID 471373:EULA should not be prompted when interface type is modified from Shared to Passthrough for a NetScaler-VSB provisioned on Nexus 1010/1110 platforms.
- Issue ID 508410: HA SYNC takes longer than expected for NetScaler 1000V. For example, for synchronizing ns.conf file of 38.4 KB size, it takes 70-100 seconds.

Configuration Utility

- Issue ID 482135: Java Runtime Environment (JRE) does not work on Internet Explorer version 10.

  Workaround: Press F12 and set the Document Mode and Browser mode to Internet Explorer 9.
- Issue ID 374437: If, when using the configuration utility to configure the NetScaler appliance, you press "Alt+Tab" to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press "Alt+Tab" a second time.
- Issue ID 353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list in the "Create Persistency Group" dialog box (Load Balancing > Persistency Groups > Add and in the "Create Persistency Group" dialog box list that appears when you click the "Name" button in the list "Create Content Switching Action" dialog box "Content Switching > Actions > Add).
- Issue ID 456428: 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.

- Issue ID 470941: You cannot use the configuration utility to add signatures to an existing application firewall policy.

  Workaround: Use the command line interface .

- Issue ID 389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

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

- Issue ID 459703: In a high availability setup, if you run the "add ssl certkey" command on the primary node, and if the certificate and key files are not present on the secondary node, the command fails on the secondary node. However, an error message is not displayed in the configuration utility.

- Issue ID 388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml

- Issue ID 485314: On the Reporting tab of the NetScaler GUI, if you choose to use the time zone settings of the NetScaler ADC, the System Overview graph does not reflect the time zone set on the NetScaler ADC. The values in the graph are for the GMT time zone.

- Issue ID 400073, 401262: 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

- Issue ID 414807: 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.
- Issue ID 489884: The configuration utility does not display SSL policies if you navigate to Traffic Management > SSL > Policies to create a policy.

  Workaround: Navigate to Traffic Management > SSL and, in the right pane, select SSL Policy Manager. Or click the refresh button on the top right corner to display the SSL policies.
- Issue ID 490130: When you use the configuration utility to create a FIPS key, the FIPS wizard fails to respond
- Issue ID 278002, 273176, 389874: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.
- Issue ID 414422: When using the Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.
- Issue ID 499223: The maximum length for creating a NetScaler ADC system user password (System > User Administration > Users) is 127. The GUI tooltip displays this value as 255, which is incorrect.
- Issue ID 483226: The key filename property of Import FIPS key (Configuration > Traffic Management > SSL > FIPS > FIPS keys >Action > Import > Key Filename) fails if you provide an incomplete filepath, folder1/folder2/rsa.key, where folder1 and folder2 are the folders within the nsconfig/ssl path.

  Workaround: In release 10.1, provide only the FIPS key.

  In release 10.5, you must specify the complete file path to the FIPS key.
- Issue ID 375277, 322602, 334465, 396405, 412455, 419503, 438382, 438534, 438796, 441853, 446387, 448361: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.
- Issue ID 469755: If you open the NetScaler ADC configuration utility on multiple browser tabs, and if you disable a feature on one of the tabs, the other tabs are not automatically refreshed.

  Workaround: Manually refresh the tabs.

Content Switching/Load Balancing

- Issue ID 399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

DNS

- Issue ID 382478: 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.

- Issue ID 458313: When NetScaler is configured as DNS proxy and it receives a DNSSEC query with Checking Disbaled (CD) bit set, it does not pass the bit as is to the server at the back end. It instead turns the bit off. This impacts deployments where the NetScaler is load balancing DNSSEC aware resolver. The impact is that the resolver will check the DNSSEC signatures even if the client had not requested to do so by setting the CD bit.

- Issue ID 458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.

  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.

  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.

- Issue ID 437529: 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.

GSLB

- Issue ID 497412: If you perform a force sync of the GSLB configuration, the non-default settings on the RPC node are lost. As a result, the GSLB auto-sync functionality is lost.

High Availability

- Issue ID 471294: When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) to build 126.x, the updates made in the Webinterface.conf file are over-written by the previous version of the file. This is due to the rolling upgrade of HA nodes or due to the file sync operation between HA nodes.

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

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

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

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

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

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

6. Save the configurations.

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

Integrated Caching

- Issue ID 486535: In a NetScaler deployment that has integrated caching and SSL enabled, the NetScaler can crash in the following scenario:

  1. Client1 requests for an object that is not in cache.

  2. While the NetScaler fetches the object from the backend server, client2 (a slow client) sends a request for the same object.

  3. Client1 now decides to reset the connection.

  4. When available, NetScaler serves the object to the client2.

  However, since client2 is slow, large data is piled up on the NetScaler that needs to be forwarded to client2. When the NetScaler tries to send this large data to the client, the NetScaler can crash.

- Issue ID 440107, 440389: 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".

Load Balancing

- Issue ID 457639: 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.

- Issue ID 460040: 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.

- Issue ID 497470: 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.

  Workaround: Run the “set lb group –persistenceType” command to reset the persistence on the virtual servers that are bound to the group.

- Issue ID 464952: If a DNS autoscale service group is bound to a virtual server, the "show lb vserver" command output displays one extra service bound to the virtual server.

- Issue ID 441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.
- Issue ID 489400: In a high availability setup, a failover might disconnect active connections even though stateful connection failover is enabled on the virtual servers.

  Workaround:

  Check the output of the “show rpcnode” command. If it shows an asterisk (*) for the SRCIP parameter, run the “set rpcnode <remote NSIP> -scrip <local NSIP>” command.
- Issue ID 455133: If the FQDN is not resolvable, you might notice high CPU utilization on the NetScaler ADC.
- Issue ID 277862: With a NetScaler Web 2.0 Push configuration in streaming mode, if the length of the response from the server is in the range of 10^n - 2^4n bytes, where n=1, 2, 3, and so on (for example, 1-15, 100-255, and 1000-4095 bytes), the push virtual server adds a byte to the response that it sends to the client. As a result, after the first response, subsequent updates sent on the same connection are lost.

NetScaler Insight Center

- Issue ID 388096, 423109: Netscaler Insight Center (Issue IDs 0388096, 0423109)

  When you launch XenApp through Citrix Receiver (standard edition), the app launch duration is not calculated and is shown as zero.
- Issue ID 424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later builds is supported.

  Workaround: To upgrade to build 120.13 or later build, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same .
- Issue ID 441163: NetScaler Insight Center might not display reports under the following set of conditions:

  -NetScaler ADCs that are configured for Network Address Translation (NAT) are added to the NetScaler Insight Center inventory.

  -A NetScaler ADC and a NetScaler Insight Center virtual appliance are in different networks and are configured for Network Address Translation (NAT.)
- Issue ID 399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 379876, 424686, 437964: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.

- Issue ID 368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.
- Issue ID 394526: In the Dashboard > Web Insight > Applications page, the values shown when you select "Response Time" from the drop-down list can be incorrect.
- Issue ID 397236: On the Dashboard > HDX Insight > Users page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but, the right pane displays the values for the period selected from the drop-down list.
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off:

  The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.
- Issue ID 446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue ID 386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue ID 409634: All the metrics except bandwidth and hits display the average values.

NetScaler VPX Appliance

- Issue ID 405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platforms MacVTap interfaces.

  Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).
- Issue ID 405383, 360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.

Networking

- Issue ID 318684: In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic that has the destination that was advertised by the secondary node.
- Issue ID 399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.
- Issue ID 371613: In a high availability configuration with the network firewall mode set to BASIC on the current secondary node, synchronization of configuration files from the primary to secondary node fails, regardless of whether you run the "sync

HA files" command from the NetScaler command line or by using the Start HA files synchronization dialog box in the configuration utility.

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

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

For example, for an HA configuration in which the primary nodes NSIP address is 198.51.100.9 and the secondary nodes NSIP address is 198.51.100.27, you would run the following commands:

On the primary node:

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

On the secondary node:

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

- Issue ID 497277: The NetScaler ADC might not update its bridge and ARP tables with the information received from GARP messages.
- Issue ID 485260: In an active-active high availability configuration using Virtual Router Redundancy Protocol (VRRP) protocol, PING to a virtual IP address (VIP) might fail from a node, which is a backup node for this VIP address.
- Issue ID 383958, 411806: $ 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.
- Issue ID 323127: The NetScaler ADC might become unresponsive if you run the show route operation during a dynamic route addition or deletion process.

Platform

- Issue ID 407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.
- Issue ID 402113: L2 mode is not supported on Netscaler VPX instances running on a Linux-KVM host.
- Issue ID 402111: VLAN tagging is not supported on Netscaler-VPX operating on MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, MacVTap-Passthrough interface Modes.
- Issue ID 407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.

Policies

- Issue ID 422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP.

!CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)

- Issue ID 390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

Reporting

- Issue ID 368982: After you import a custom data source, the charts for the counters under "System entities statistics" are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 468198: If the format of a CRL is incorrect or the issuer of a CRL does not match the specified CA certificate, and you run the "show crl" command, an error message showing the CRL status as invalid appears.
- Issue ID 455821: An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.
- Issue ID 402423: In a cluster setup, if you include the "cipherdetails" option in the "show ssl service" or "show ssl vserver" command, an incorrect message appears. This is only a display issue.

  For example,

  > sh ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]
- Issue ID 494093: If session reuse is enabled on the NetScaler and a network error occurs, the NetScaler attempts to clear the session information so that it is not reused for a subsequent session request from the same client. In rare cases, the NetScaler might fail during this cleanup process.

System

- Issue ID 377618, 341460, 351127, 364015, 481575, 499259: 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]
- Issue ID 430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.

- Issue ID 427126, 441982, 452885, 456645: 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.
- Issue ID 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.

User Interface

- Issue ID 475830: A large configuration file puts a heavy load on the management CPU. The resulting delay in displaying the output of the "show ns runningconfig" command might exceed the timeout value.

  Workaround: If you are using a script to fetch the output for "show ns runningConfig" command, and the script has a placeholder for timeout value, modify the script to increase the timeout value to 500 seconds.

Web Interface

- Issue ID 397150: 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.

XML API

- Issue ID 363145: The following APIs are not available in version 10.1 or later:

  - bindservicegroup_state2

  - unsetnslimitidentifier_selectorname. Use unsetnslimitidentifier_selector instead.

Chapter 4

Build 128.8

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 128.8

Replaces build: None

Release date: July 2014

Release Notes version: 1.0

Language supported: English (US)

Bug Fixes

AAA-TM

- Issue ID 317157: AAA-TM now supports relative URLs as form Action URLs in forms-based SSO logon forms. You do not have to specify an absolute path to the web form when configuring forms-based SSO.

AppFlow

- Issue ID 478480:If a browser executes the JavaScript that is inserted into the response of the main page, it sends a special request intended for the NetScaler ADC. AppFlow records for this request must not be generated. While handling this behavior, the logic in one part of the code assumes that the AppFlow records must not be sent, but another part of the code assumes that the records must be sent. As a result, the NetScaler ADC fails to respond.

DNS

- Issue ID 462862: Statistics do not appear correctly for a DNS load balancing virtual server.
- Issue ID 422509: 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

Integrated Caching

- Issue ID 466452, 469584, 469588, 470925: While revalidating cached objects, the integrated caching feature performs some incorrect accounting of the cache size. This causes the NetScaler appliance to crash.
- Issue ID 427479, 463589, 482725, 502413: The output of the "stat cache -d" command displays an incorrect value for the utilized memory parameter.

Load Balancing

- Issue ID 478949: The NetScaler ADC fails if requests requiring IP fragmentation are forwarded to a virtual server that is configured for sessionless load balancing in IP mode.

Networking

- Issue ID 414407, 485512: The default speed for an LACP channel is set to NONE instead of AUTO.
- Issue ID 477507: If you have configured active FTP with random source port option enabled for an FTP virtual server, the NetScaler ADC might not handle data

connections properly for this FTP server and (NetScaler) might become unresponsive.

Platform

- Issue ID 483073: NetScaler-VSB provisioning does not succeed on Nexus 1010/1110 Platforms.

SSL

- Issue ID 474417, 474413: The version displayed in syslog is SSLv2.0 even though the session is negotiated using TLSv1.2.
- Issue ID 414388, 345883, 349858, 428257, 428259: 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.

System

- Issue ID 481442: When different TCP profiles are bound to a virtual server and to the services that are bound to that virtual server, and one of the profiles has window scaling as ENABLED and the other has it as DISABLED, NetScaler sometimes considers that window scaling is ENABLED. The expectation in such a case is that NetScaler considers window scaling as DISABLED.
- Issue ID 478895: The "show ns runningConfig" command may produce partial output if invoked while another "show ns runningConfig" command, from the same or other admin session is in progress.
- Issue ID 452240: 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.

Known Issues and Workarounds

AAA-TM

- Issue ID 332831: The rule (expression) in a AAA-TM policy can be from one to 1434 characters in length. If you enter a longer rule, AAA-TM displays an "invalid rule" error.

AppFlow

- Issue ID 327439: AppFlow records generated by the NetScaler appliance cannot be seen on SPLUNK.
- Issue ID 396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.

Application Firewall

- Issue ID 372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

Workaround: Use the Adobe PDF browser plugin.

- Issue ID 430014: 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

- Issue ID 283780: When you enable the sessionless URL closure feature, you must also enable the URL closure feature. If you do not enable URL closure, the sessionless URL closure feature does not work.
- Issue ID 399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

  For example, if you had two sets of custom signatures, named "custom_signatures" and "custom_signatures_2", that were based on copies of the default signatures file, you would update the signatures on your NetScaler ADC by issuing the following commands:

  > update appfw signatures "*Default Signatures"

  > update appfw signatures "custom_signatures"

> update appfw signatures "custom_signatures_2"

- Issue ID 423150: The application firewall PCI-DSS report does not contain information on the "SQLInjectionCheckSQLWildChars" parameter.
- Issue ID 427798: A NetScaler ADC that has the application firewall feature enabled might reset the connection after a protected web server issues an HTTP 204 response.
- Issue ID 443673: 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".
- Issue ID 451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.
- Issue ID 464641: If the application firewall receives a multipart POST request with a Content-Type header that contains a charset, it blocks that request as malformed.
- Issue ID 466329: 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.
- Issue ID 472476, 418036: 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.
- Issue ID 364134: In the configuration utility, when you perform the Show Bindings operation, globally bound auditing syslog policies do not appear under Application Firewall. This issue occurs only in a cluster setup.

  Workaround: Display the bindings in the command line interface, by using the "show system global" command.
- Issue ID 489691: 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.

Content Switching

- Issue ID 501856: An invalid HTTP request that spans multiple TCP segments that is sent to a content switching virtual server can cause the NetScaler to skip the load balancing decision and initiate a connection from the SNIP to the content switching virtual server. This can cause the NetScaler appliance to crash.

Configuration Utility

- Issue ID 388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml

- Issue ID 414807: 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.
- Issue ID 353015: Load balancing virtual servers that are used by AppExpert applications are displayed in nodes other than the AppExpert node. For example, they are displayed in the Available Virtual Servers list in the "Create Persistency Group" dialog box (Load Balancing > Persistency Groups > Add and in the "Create Persistency Group" dialog box list that appears when you click the "Name" button in the list "Create Content Switching Action" dialog box "Content Switching > Actions > Add).
- Issue ID 278002, 273176, 389874: If you use the configuration utility to enable or disable an extended ACL or ACL6, the utility does not warn you that the change does not take effect until you apply ACLs.
- Issue ID 469755: If you open the NetScaler ADC configuration utility on multiple browser tabs, and if you disable a feature on one of the tabs, the other tabs are not automatically refreshed.

  Workaround: Manually refresh the tabs.
- Issue ID 374437: If, when using the configuration utility to configure the NetScaler appliance, you press "Alt+Tab" to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press "Alt+Tab" a second time.
- Issue ID 375277, 322602, 334465, 396405, 412455, 419503, 438382, 438534, 438796, 441853, 446387, 448361: If a NetScaler connection from a client is closed without the client logging out, the session created for that connection remains active until the configured timeout period elapses. If this happens frequently, after about the 20th occurrence the user might get a "Connection limit to CFE exceeded" error message.
- Issue ID 459703: In a high availability setup, if you run the "add ssl certkey" command on the primary node, and if the certificate and key files are not present on the secondary node, the command fails on the secondary node. However, an error message is not displayed in the configuration utility.
- Issue ID 490130: When you use the configuration utility to create a FIPS key, the FIPS wizard fails to respond
- Issue ID 389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 483226: The key filename property of Import FIPS key (Configuration > Traffic Management > SSL > FIPS > FIPS keys >Action > Import > Key Filename) fails if

you provide an incomplete filepath, folder1/folder2/rsa.key, where folder1 and folder2 are the folders within the nsconfig/ssl path.

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

- Issue ID 414422: When using the Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.
- Issue ID 456428: 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.
- Issue ID 470941: You cannot use the configuration utility to add signatures to an existing application firewall policy.

  Workaround: Use the command line interface .

Content Switching/Load Balancing

- Issue ID 399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

DNS

- Issue ID 458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.

  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.

  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.
- Issue ID 458313: When NetScaler is configured as DNS proxy and it receives a DNSSEC query with Checking Disbaled (CD) bit set, it does not pass the bit as is to the server at the back end. It instead turns the bit off. This impacts deployments where the NetScaler is load balancing DNSSEC aware resolver. The impact is that the resolver will check the DNSSEC signatures even if the client had not requested to do so by setting the CD bit.

Documentation

- Issue ID 407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.

High Availability

- Issue ID 471294: When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) to build 126.x, the updates made in the Webinterface.conf file are over-written by the previous version of the file. This is due to the rolling upgrade of HA nodes or due to the file sync operation between HA nodes.

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

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

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

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

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

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

  6. Save the configurations.

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

Integrated Caching

- Issue ID 440107, 440389: 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".

Load Balancing

- Issue ID 455133: If the FQDN is not resolvable, you might notice high CPU utilization on the NetScaler ADC.
- Issue ID 441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.
- Issue ID 460040: 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.
- Issue ID 464952: If a DNS autoscale service group is bound to a virtual server, the "show lb vserver" command output displays one extra service bound to the virtual server.
- Issue ID 277862: With a NetScaler Web 2.0 Push configuration in streaming mode, if the length of the response from the server is in the range of 10^n - 2^4n bytes, where n=1, 2, 3, and so on (for example, 1-15, 100-255, and 1000-4095 bytes), the push virtual server adds a byte to the response that it sends to the client. As a result, after the first response, subsequent updates sent on the same connection are lost.

NetScaler Insight Center

- Issue ID 385821: When an ICA session is initiated by launching XenDesktop, the user name is displayed along with the domain name "(user-id@domain-name)".

- Issue ID 409634: All the metrics except bandwidth and hits display the average values.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue ID 424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later builds is supported.

  Workaround: To upgrade to build 120.13 or later build, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same .
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off:

  The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.
- Issue ID 446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue ID 394526: In the Dashboard > Web Insight > Applications page, the values shown when you select "Response Time" from the drop-down list can be incorrect.
- Issue ID 397236: On the Dashboard > HDX Insight > Users page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but, the right pane displays the values for the period selected from the drop-down list.
- Issue ID 368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.
- Issue ID 399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 379876, 424686, 437964: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.

NetScaler VPX Appliance

- Issue ID 405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platforms MacVTap interfaces.

Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).

- Issue ID 405383, 360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.

Networking

- Issue ID 383958, 411806: $ 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.
- Issue ID 399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.
- Issue ID 318684: In an HA configuration in INC mode where both the nodes run the OSPF routing protocol, the secondary node drops all the L3 traffic that has the destination that was advertised by the secondary node.
- Issue ID 371613: In a high availability configuration with the network firewall mode set to BASIC on the current secondary node, synchronization of configuration files from the primary to secondary node fails, regardless of whether you run the "sync HA files" command from the NetScaler command line or by using the Start HA files synchronization dialog box in the configuration utility.

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

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

  For example, for an HA configuration in which the primary nodes NSIP address is 198.51.100.9 and the secondary nodes NSIP address is 198.51.100.27, you would run the following commands:

  On the primary node:

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

  On the secondary node:

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

Platform

- Issue ID 402111: VLAN tagging is not supported on Netscaler-VPX operating on MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, MacVTap-Passthrough interface Modes.
- Issue ID 402113: L2 mode is not supported on Netscaler VPX instances running on a Linux-KVM host.
- Issue ID 407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.

Policies

- Issue ID 422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

  Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP.

  !CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)

- Issue ID 390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

- Issue ID 425465: After changing the time zone on a NetScaler appliance, you must restart the appliance so that policies referencing the LOCAL system use the new time zone instead of the old one. Otherwise, policies that should match do not, and policies that should not match do.

Reporting

- Issue ID 368982: After you import a custom data source, the charts for the counters under "System entities statistics" are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 455821: An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.
- Issue ID 494093: If session reuse is enabled on the NetScaler and a network error occurs, the NetScaler attempts to clear the session information so that it is not reused for a subsequent session request from the same client. In rare cases, the NetScaler might fail during this cleanup process.
- Issue ID 402423: In a cluster setup, if you include the "cipherdetails" option in the "show ssl service" or "show ssl vserver" command, an incorrect message appears. This is only a display issue.

  For example,

  > sh ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]

System

- Issue ID 377618, 341460, 351127, 364015: 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]

- Issue ID 430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.
- Issue ID 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.

Web Interface

- Issue ID 397150: 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.

XML API

- Issue ID 363145: The following APIs are not available in version 10.1 or later:

  - bindservicegroup_state2

  - unsetnslimitidentifier_selectorname. Use unsetnslimitidentifier_selector instead.

Chapter 5

Build 127.10

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 127.10

Replaces build: None

Release date: June 2014

Release Notes version: 1.0

Language supported: English (US)

Bug Fixes

Application Firewall Issues

- Issue ID 472094: Any application firewall profile that has either the "AlwaysExceptFirstRequest" or the "AlwaysExceptStartURLs" option enabled cannot be viewed in the configuration utility. These options are available from the command line only. When upgrading to either the current 10.1 maintenance release or the 10.5 beta release of the NetScaler operating system from any previous release, any profile which had the "always" option enabled has that option changed to "AlwaysExceptStartURLs." Profiles that have the "if_present" or "OFF" options enabled are not affected.
- Issue IDs 456650, 313950: A NetScaler ADC that is configured as an HA pair, and that has the application firewall feature enabled, might experience repeated failovers from the primary to the secondary node when processing HTML traffic with large tag attribute values.
- Issue ID 455284: NetScaler ADCs that are configured as an HA pair with the application firewall enabled might become unresponsive or reboot when the application firewall is processing a large web form.

AAA Application Traffic Issues

- Issue ID 317157: AAA-TM now supports relative URLs as form Action URLs in forms-based SSO logon forms. You do not have to specify an absolute path to the web form when configuring forms-based SSO.

Content Switching Issues

- Issue ID 460259: The output of the "stat cs vserver -fullValues" command now displays the number of requests per second. In earlier builds, the output displayed the total number of requests.

Configuration Utility Issues

- Issue IDs 473832, 474471: The configuration utility might display the following error message when you create a monitor by navigating to Traffic Management > Load balancing > Monitors and click Add: Error creating view. Model must not be null
- Issue ID 0448851: The System > Cluster > Manage Cluster screen allows a user to create a cluster without providing a Cluster IP address.
- Issue ID 403766: In the Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop wizard, applying the application firewall policies through the Security settings creates an error condition.

- Issue ID 409057: The Traffic Management > Load balancing > Set Up NetScaler for XenApp/XenDesktop wizard, displays a distorted view of the published resources when you apply the application firewall settings in the Security section.
- Issue ID 446373: For VPX Netscalers, you can edit ifalias from the Graphical User Interface properly. If you are using Cluster VPX, you can only edit ifalias using the command line interface and not the Graphical User Interface.

DataStream Issues

- Issue ID 415485: 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.

Integrated Caching Issues

- Issue IDs 466452, 469584, 469588, 470925: While revalidating cached objects, the integrated caching feature performs some incorrect accounting of the cache size. This causes the NetScaler appliance to crash.

GSLB Issues

- Issue ID 465500: GSLB static proximity stops working, if you remove the custom records after the database ideal times out. If you have not removed the custom records, then it starts to work when a new connection request is made.

Load Balancing Issues

- Issue ID 475980: The NetScaler ADC does not set the mandatory flag in a Route-Record AVP. As a result, some diameter implementations might reject the AVP.
- Issue ID 471938: In a deployment with multiple MAC-mode virtual servers, some changes in the configuration can result in a MAC-mode virtual server failing to serve traffic. Changes that can cause the problem include:
  - Disabling and enabling the interface through which the MAC of a service is learnt.
  - Removing virtual servers or clearing their configurations.
  - Changes caused by high availability failovers.

NetScaler Insight Center Issues

- Issue ID 450474: On the dashboard, when you navigate to Web Insight > Devices > (device record) and click on HTTP Request Methods, HTTP Response Status, Operating Systems, or User Agents, and then from the bread crumb navigation click

Application from the respective drop down list, the graph does not display any details.

Networking Issues

- Issue ID 477507: If you have configured active FTP with random source port option enabled for an FTP virtual server, the NetScaler ADC might not handle data connections properly for this FTP server and (NetScaler) might become unresponsive.
- Issue IDs 475466, 475462, 486447: RNAT configuration might be lost in a NetScaler ADC after you restart it.
- Issue ID 457119: In a high availability (HA) configuration, the secondary node might forward BOOTP and DHCP related traffic using a configured VMAC address instead of interface's MAC address.
- Issue ID 438557: The NetScaler appliance might consume excessive CPU cycles when processing ACL rules.
- Issue IDs 469033, 467726: In a high availability configuration, you might lose your VLAN configuration if you upgrade the secondary node to build 125.x from builds: 122.17, 123.11,124.13.
- Issue ID 448316: The NetScaler ADC might not remove the session information of an FTP connection from its memory while closing the connection. When the NetScaler ADC allocates the same memory block for a connection related to a UDP DNS service, the NetScaler ADC becomes unresponsive.

SSL Issues

- Issue IDs 460918, 474003: Next Protocol Negotiation (NPN) TLS extension cannot be explicitly enabled or disabled. It is automatically enabled when SPDY is enabled on a HTTP profile, and disabled when SPDY is disabled.
- Issue IDs 459688, 446760: If you use the configuration utility to configure FIPS appliances in a high availability setup, FIPS keys are not exported or imported between the nodes, because the option to enable secure information management (SIM) is not available.

System Issues

- Issue IDs 465808, 458962: NetScaler s now provides OpenStack support for Generic KVM and Cisco KVM VPX.
- Issue IDs 451285, 441843, 457850: If TCP buffering or caching is enabled on a NetScaler appliance receiving an ACK packet that has ACK_NO at the left edge of the SACK block, the packet engine enters a loop while processing the packet.
- Issue ID 450398: The NetScaler nstrace utility does not filter out all IPv6 packets when a IPv4 only filter is entered.

- Issue IDs 450054, 450787, 453207, 453481, 459354: When the NetScaler has application firewall disabled but SSO enabled, and if the NetScaler memory is less, all unused memory (appfw memory) is not recovered. This leads to an erroneous value for the "ActualInUse" memory counter.
- Issue IDs 455041, 478635, 484981: The NetScaler system backup tar file does not include the following files:
  - /nsconfig/ns.conf
  - /nsconfig/Zebos.conf
  - /nsconfig/rc.netscaler
  - /nsconfig/snmpd.conf
  - /var/log/wicmd.log
  - /nsconfig/nsbefore.sh
  - /nsconfig/nsafter.sh
- Issue ID 478895: The "show ns runningConfig" command may produce partial output if invoked while another "show ns runningConfig" command, from the same or other admin session is in progress. Workaround: Re-execute the "show ns runningConfig" command to fetch the entire running configuration.

Known Issues and Workarounds

Application Firewall Issues

- Issue ID 399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files. For example, if you had two sets of custom signatures, named "custom_signatures" and "custom_signatures_2", that were based on copies of the default signatures file, you would update the signatures on your NetScaler ADC by issuing the following commands:

  > update appfw signatures "*Default Signatures"

  > update appfw signatures "custom_signatures"

  > update appfw signatures "custom_signatures_2"
- Issue ID 451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.

- Issue ID 466329: 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.
- Issue ID 443673: Signature Bindings Not Shown in PCI-DSS ReportThe Application Firewall PCI-DSS report does not display signature bindings. The Profile Settings section of the report shows bound signatures as "not set".
- Issue ID 372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 364134: In the configuration utility, when you perform the Show Bindings operation, globally bound auditing syslog policies do not appear under Application Firewall. This issue occurs only in a cluster setup.Workaround: Display the bindings in the command line interface, by using the "show system global" command.
- Issue ID 430014: 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 JSONContentTypeIf 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

AppFlow Issues

- Issue ID 396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.
- Issue ID 478480: If a browser executes the JavaScript that is inserted into the response of the main page, it sends a special request intended for the NetScaler

ADC. AppFlow records for this request must not be generated. While handling this behavior, the logic in one part of the code assumes that the AppFlow records must not be sent, but another part of the code assumes that the records must be sent. As a result, the NetScaler ADC fails to respond.

Content Switching

- Issue ID 501856: An invalid HTTP request that spans multiple TCP segments that is sent to a content switching virtual server can cause the NetScaler to skip the load balancing decision and initiate a connection from the SNIP to the content switching virtual server. This can cause the NetScaler appliance to crash.

Configuration Utility

- Issue ID 374437: If, when using the configuration utility to configure the NetScaler appliance, you press **Alt+Tab** to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press **Alt+Tab** a second time.
- Issue ID 389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 459703: In a high availability setup, if you run the â€œadd ssl certkeyâ€ command on the primary node, and if the certificate and key files are not present on the secondary node, the command failsÂ on the secondary node. However, an error message is not displayed in the configuration utility.
- Issue ID 388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml
- Issue ID 482135: Java Runtime Environment (JRE) does not work on Internet Explorer version 10.Workaround: Press F12 and set the Document Mode and Browser mode to Internet Explorer 9.
- Issue ID 483226: The key filename property of Import FIPS key (**Configuration** > **Traffic Management** > **SSL** > **FIPS** > **FIPS keys** >**Action** > **Import** > **Key** Filename) fails if you provide an incomplete filepath, folder1/folder2/rsa.key, where folder1 and folder2 are the folders within the nsconfig/ssl path.

  Workaround: Provide the complete file path nsconfig/ssl/folder1/folder2/rsa.key, or provide only the file name, rsa.key.
- Issue IDs 374304 and 377460: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a "No such resource" error message appears, even if the rename operation is successful.

Workaround: Use the mouse to click the OK button instead of pressing the ENTER key on the keyboard.

- Issue ID 414807: 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.
- Issue ID 414422: When using the **Traffic Management** > **Load Balancing** > **Set Up NetScaler for XenApp/XenDesktop** wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.
- Issue ID 469755: If you open the NetScaler ADC configuration utility on multiple browser tabs, and if you disable a feature on one of the tabs, the other tabs are not automatically refreshed.

  Workaround: Manually refresh the tabs.

DNS

- Issue ID 458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.
  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.
  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.

Integrated Caching

- Issue IDs 440107 and 440389: 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".

High Availability

- Issue ID 471294: When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) to build 126.x, the updates made in the Webinterface.conf file are over-written by the previous version of the file. This is due to the rolling upgrade of HA nodes or due to the file sync operation between HA nodes.To avoid this issue, use the following steps when upgrading the HA nodes:
  a. Before upgrading, run the command: "set ns param -internaluserlogin DISABLED"
  b. Upgrade the secondary HA node to NetScaler 10.1 Build 126.x release.

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

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

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

f. Save the configurations.

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

Load Balancing

- Issue ID 399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.
- Issue ID 441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.

NetScaler Insight Center

- Issue ID 385821: When an ICA session is initiated by launching XenDesktop, the user name is displayed along with the domain name "(user-id@domain-name)".
- Issue ID 399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue ID 394526: In the **Dashboard** > **Web Insight** > **Applications** page, the values shown when you select "Response Time" from the drop-down list can be incorrect.
- Issue ID 424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later builds is supported.Workaround: To upgrade to build 120.13 or later build, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same .

- Issue ID 368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.
- Issue ID 409634: All the metrics except bandwidth and hits display the average values.
- Issue ID 397236: On the **Dashboard** > **HDX Insight** > **Users** page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but, the right pane displays the values for the period selected from the drop-down list.
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off:The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue IDs 379876, 437964, and 424686: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.

Networking

- Issue ID 399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.
- Issue ID 475462: The NetScaler appliance might not properly processes ACL based RNAT rules.
- Issue IDs 383958 and 411806: $ 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.

Platform

- Issue ID 407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.
- Issue ID 402113: L2 mode is not supported on Netscaler VPX instances running on a Linux-KVM host.
- Issue ID 407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.
- Issue ID 402111: VLAN tagging is not supported on Netscaler-VPX operating on MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, MacVTap-Passthrough interface Modes.

Policy

- Issue ID 422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

  Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP.!CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)

- Issue ID 425465: After changing the time zone on a NetScaler appliance, you must restart the appliance so that policies referencing the LOCAL system use the new time zone instead of the old one. Otherwise, policies that should match do not, and policies that should not match do.
- Issue ID 390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

Reporting

- Issue ID 368982: After you import a custom data source, the charts for the counters under "System entities statistics" are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 494093: If session reuse is enabled on the NetScaler and a network error occurs, the NetScaler attempts to clear the session information so that it is not reused for a subsequent session request from the same client. In rare cases, the NetScaler might fail during this cleanup process.

System

- Issue ID 430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.
- Issude IDs 377618, 341460, 364015 and 351127: 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]

- Issue IDs 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.

VPX

- Issue ID 405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platforms MacVTap interfaces.Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).
- Issue IDs 405383 and 360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.

Web Interface

- Issue ID 397150: 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.

XML API

- Issue ID 363145: The following APIs are not available in version 10.1 or later:
  - bindservicegroup_state2
  - unsetnslimitidentifier_selectorname. Use unsetnslimitidentifier_selector instead.

Chapter 6

Build 126.12

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 126.12

Replaces build: None

Release date: May 2014

Release Notes version: 1.0

Language supported: English (US)

Enhancements

SSL Issues

- Issue ID 0459472: SSL hardware offload is now supported on a NetScaler 1000V virtual appliance running on a Nexus 1110-X appliance that has an SSL card. For this to work, you must install a Citrix SSL hardware license on the NetScaler 1000V virtual appliance.

Changes

Caching Stored Procedures and SQL Queries Issues

- Issue ID 0453973: If connection multiplexing is disabled in a database profile, stored procedures and SQL batch queries are not cached, despite caching being enabled for the profile. With this enhancement, you can enable caching, if connection multiplexing is disabled, by setting the new "enableCachingConMuxOFF" parameter in the profile.

  At the command prompt, type:

  add dbProfile <name> -conMultiplex **DISABLED** -enableCachingConMuxOFF **ENABLED**

  or

  set dbProfile <name> -enableCachingConMuxOFF `ENABLED`

  In the configuration utility, select "Enable caching when connection multiplexing OFF".

SNMP Issues

- Issue ID 0418044: A new SNMP OID, `vsvrEstablishedConn` (1.3.6.1.4.1.5951.4.1.3.1.1.71) is available for current client connections in the ESTABLISHED state at the vserver level.

Bug Fixes

Application Firewall Issues

- Issue ID 0407347: By default, the application firewall's SQL Injection signatures patterns and security checks do not prevent SQL injection attacks that use the percent (%) or underscore (_) characters. To work around this issue, add the percent and underscore characters to each signatures object as SQL special characters.

- Issue ID 0424879: A user with a web proxy that allows the user to modify the HTTP header can on rare occasions bypass certain security checks when sending content that would normally be blocked. For example, a user might bypass the HTML and XML SQL injection checks when sending an SQL special symbol to a protected web application, as long as the special symbol is not combined with an SQL command. A user might also be able to send a modified cookie by intercepting and including all cookies that the application firewall sent to the user, including the NetScaler cookie. Finally, the user might be able to use a web form to upload a script and save that script as a different file type. It does not appear that this technique can be used to cause an actual security breach.
- Issue IDs 0443207, 0355620: If an attacker includes an SQL special character that is not followed by an SQL keyword in web form data filtered by the application firewall, the application firewall does not block the request because it classifies a special character that does not include a keyword as a false positive.
- Issue ID 0457454: After automatic update of the application firewall signature rules, custom signature rules with versions lower than the current signatures are automatically disabled.

AppFlow Issues

- Issue IDs 0441332, 0401672, 0357422: If HTML Injection is enabled, the NetScaler ADC injects JavaScript into the response to obtain client-side page-load time and client-side page-render time details. The JavaScript triggers a special request that is intended only for the NetScaler ADC, but the NetScaler ADC creates an additional request by forwarding the request to the server.

Cluster Issues

- Issue ID 0455148: In some cases, the MSR routes remain in DOWN state since probing ownership is incorrectly being distributed across the cluster. MSR in cluster needs spotted SNIPs and probing ownership must be with the local node alone.

Configuration Utility Issues

- Issue IDs 0447077, 0460857: If you create a monitor by using the graphical user interface and choose the default browse option to select the in-built monitor scripts from the /nsconfig/monitors folder, the folder does not display any scripts to choose..
- Issue ID 0448851: The **System** > **Cluster** > **Manage Cluster** screen allows a user to create a cluster without providing a Cluster IP address.

Compression Issues

- Issue ID 0456734: The output of the "show cmp parameter" command incorrectly displays the label as "Disable External Cache" instead of "Enable External Cache".

- Issue ID 0456734: The output of the "show cmp parameter" command incorrectly displays the label as "Disable External Cache" instead of "Enable External Cache".

Command Line Interface Issues

- Issue ID 0436772: When you run the command show techsupport to generate a tar of system configuration data, in certain scenarios, the NetScaler ADC might ignore to collect certain large files.
- Issue ID 0436772: When you run the command show techsupport to generate a tar of system configuration data, in certain scenarios, the NetScaler ADC might ignore to collect certain large files.

DataStream Issues

- Issue ID 0451036: NTLM authentication is now supported on all Windows clients.

Load Balancing Issues

- Issue IDs 0369369, 0252157, 0438593: In NetScaler deployments where a load balancing virtual server is deployed behind another virtual server, the count of the number of request bytes is inadvertently doubled.
- Issue ID 0434925: If you add a server with a name that contains an IP address and a string, and then use that server to add a service, the error message “service already exists” appears.
- Issue IDs 0441973 and 0442098: If you bind policies in one of the following orders of priority, and then run the “show running config” or the “save config” command, the command runs repeatedly:
  - Syslog, nslog, syslog
  - Nslog, syslog, nslog
- Issue ID 0456632: If a user tries to use a long URL (more than 1024 bytes) to access a protected resource for the first time (that is, without a valid cookie), the NetScaler ADC returns a 500 error.
- Issue ID 0454497: When the primary virtual IP address is down and no backup is configured, spillover persistence fails to decrement the session allocation counter. This leads the NetScaler appliance to believe that sessions are alive and therefore reject new client requests.

NetScaler Insight Center Issues

- Issue ID 0401514: On an HTTP virtual server, after you enable AppFlow by selecting the expression TRUE and the **HTML Injection** box, if you change the policy expression and disable HTML injection, the rewrite and responder policies are still bound to the load balancing virtual server.

- Issue ID 0409885: The report for desktop session count also includes the count of XenApp sessions, which are launched by the user.
- Issue ID 0451609: If a NetScaler ADC is deployed in transparent mode for HDX Insight, Citrix Receiver fails to launch the applications or desktops if use source IP (USIP) is enabled and use subnet IP (USNIP) is disabled.
- Issue ID 0452989: If a NetScaler ADC is deployed in transparent mode for HDX Insight, Citrix Receiver fails to launch the applications or desktops if the appflow policy is not bound to a global bind point.
- Issue ID 0456449: On the **Dashboard** > **Web Insight** > **Applications** page, the report for a specific application does not display the client type and client version details.
- Issue ID 0453764: On the dashboard, HDX Insight reports do not display the active sessions and also displays an incorrect value for session launch count.

Networking Issues

- Issue ID 0452434: In a high availability configuration in INC mode, net profile and IPset commands propagate to the secondary node.
- Issue IDs 0469033, 0467726: In a high availability configuration, you might lose your VLAN configuration if you upgrade the secondary node to build 125.x from builds: 122.17, 123.11,124.13.

SSL Issues

- Issue ID 0437018: On a Nitrox-2 chip based platform, if you bind cipher groups, such as HIGH and AES, to your virtual server, the unsupported ECDHE cipher might also be bound. This cipher does not cause any problems. To remove it, you must unbind the cipher group.
- Issue IDs 0451698, 0446674, 0452080: In a high availability setup, the force ha sync command appends the DEFAULT cipher group to the user-defined ciphers on the virtual server of the secondary node.

System Issues

- Issue IDs 0335202, 0341155, 0404099, 0248103: When web server logging and audit logging are enabled on the NetScaler, the TCP current clients counter goes to negative values and shows a very large value in the stat or the SNMP OID.
- Issue IDs 0396628, 0402205: With large number of configuration entries in the ns.conf file, the commands in the /nsconfig/rc.netscaler file might not be applied after the appliance is restarted.
- Issue IDs 0401111, 0414273, 0413721, 0408648, 0399769, 0375425, 0460731, 0424726, 0408267: If TCP buffering or caching is enabled on a NetScaler appliance receiving an ACK packet that has ACK_NO at the left edge of the SACK block, the packet engine enters a loop while processing the packet.

- Issue ID 0432612: The NetScaler ADC forwards unprocessed packets to the load balancing virtual servers without selecting a service, because of an HTTP out-of-order packet processing issue. Instead of being dropped, these connections queue up at the virtual servers. The ADC fails to respond while processing these connections.
- Issue ID 0446300: The NetScaler ADC might fail during an nstrace operation.
- Issue IDs 441843, 457850, 451285: If TCP buffering or caching is enabled on a NetScaler appliance receiving an ACK packet that has ACK_NO at the left edge of the SACK block, the packet engine enters a loop while processing the packet.
- Issue ID 0453108: The NetScaler appliance drops a connection if it receives 255 back-to-back old packets (re-transmissions). The limit is configurable and the default value has been increased.
- Issue ID 0453811: The state of services for which NATPCB is allocated starts flapping because of NATPCB allocation failure.
- Issue ID 0450580: High CPU usage is observed when evaluating listen policy named expressions on a virtual server that picks up every packet.
- Issue IDs 0462797, 0441758, 0446780, 0455911, 0457505, 0459435, 0468798, 0476812: Memory leak found in shell '/bin/sh' while performing management CPU profiling in "nsproflog.sh" thereby causing swap zone issues.
- Issue ID: 0370288: If you are using the show virtual-service-blade command, the output shows junk characters.

vPath Issues

- Issue ID 0460298: On a NetScaler 1000V appliance, vPath offload packets cannot be carried over tagged interfaces.
- Issue ID 0421257: The NetScaler interfaces (CLI and GUI) incorrectly refer to "vPath" as "Vpath".
- Issue ID 0424974: vPath routes are not distinctly identified in a cluster.
- Issue ID 0443252: The "stat vpath" command does not provide the vPath offload status.
- Issue ID 0458072: On executing the "clear route VPATH", the CLI does not display an error message indicating that the operation is not permitted. Also, there is an extraneous "|" character in the output of the "show route" command.
- Issue ID 0458083: The labels of the output of the "stat vpath" command are truncated.
- Issue ID 0445402: vPath offload is by default ENABLED. Therefore, even when the vPath feature is disabled, vPath offload remains in enabled state. The default state of vPath offload is now changed to DISABLED.
- Issue ID 0449065: When upgrading the kernel from NetScaler 10.1 Build 124.7, the NetScaler crashes due to a mismatch in the kernel and the vPath library.

- Issue ID 0447725: SNMP support provided for vPath counters.

VPX Issues

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

  ```
  sysctl netscaler.ns_vpx_halt_method=2
  ```

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

  ```
  sysctl netscaler.ns_vpx_halt_method=2
  ```

Web Interface Issues

- Issue ID 0450811: In a high availability setup, if the failover operation is performed twice, a user trying to launch an application is unable to proceed after the AGESSO.jsp page appears. If the domain controller is configured for x number of logon retries, and the user refreshes the page x number of times, the account is locked. With this fix, the user is able to launch the application. However, if an application is launched immediately after failover, and the launch takes longer than usual (about 75 seconds), a session error page might appear, in which case the user has to log on again.
- Issue ID 0456120: Upgrading a NetScaler ADC from release 10 to release 10.1 deletes a set of customized options of the add wi site command.
- Issue ID 0458113: Neither the CLI nor the configuration utility allows a user to configure a pre-login message of more than 255 characters.

Known Issues and Workarounds

Application Firewall Issues

- Issue ID 0364134: In the configuration utility, when you perform the **Show Bindings** operation, globally bound auditing syslog policies do not appear under Application Firewall. This issue occurs only in a cluster setup. Display the bindings in the command line interface, by using the **show system global** command.
- Issue ID 0466329: 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.
- Issue ID 0372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

Workaround: Use the Adobe PDF browser plugin.

- Issue ID 0430014: 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
```

- Issue ID 0399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files. For example, if you had two sets of custom signatures, named **custom_signatures** and **custom_signatures_2**, that were based on copies of the default signatues file, you would update the signatures on your NetScaler ADC by issuing the following commands: update appfw signatures "*Default Signatures" update appfw signatures "custom_signatures" update appfw signatures "custom_signatures_2".
- Issue ID 0451014: On a NetScaler ADC that has the application firewall enabled and the HTML SQL injection feature configured to block, when the ADC detects an SQL violation on a page with a web form, a second violation might be generated for the Form Action URL. This is expected behavior. To avoid unexpected blocks, when you configure a relaxation for a web form, be sure to include a relaxation for the Form Action URL as well.

AppFlow Issues

- Issue ID 0396892: The AppFlow exporter might not export the correct information. Therefore, the client IP address shown on the NetScaler Insight Center dashboard might be incorrect.

Content Switching/Load Balancing Issues

- Issue ID 0399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

Configuration Utility Issues

- Issue ID 0361793 (nCore and nCore VPX): The count of the number of load balancing virtual servers, which is shown in the configuration summary, includes the load balancing virtual server that is created during the configuration of EdgeSight Monitoring, even though that load balancing virtual server is not displayed in the **Load Balancing**> **Virtual Servers** pane.
- Issue IDs 0374304, 0377460: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a `No such resource` error message appears, even if the rename operation is successful.

  Workaround: Use the mouse to click the **OK** button, instead of pressing the ENTER key on the keyboard.
- Issue ID 0374437: If, when using the configuration utility to configure the NetScaler appliance, you press **Alt+Tab** to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press **Alt+Tab** a second time.
- Issue ID 0388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml.
- Issue ID 0389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 0414422: When using the **Traffic Management** > **Load Balancing** > **Set Up NetScaler for XenApp/XenDesktop** wizard, Web Interface on NetScaler does not publish XenDesktop applications if the load balancing virtual server is configured to listen on two XenDesktop servers.
- Issue ID 0414807: When using the **Traffic Management** > **Load Balancing** > **Set Up NetScaler for XenApp/XenDesktop** wizard, an error is displayed if:
  - More than one service group is bound to the virtual server that is used for load balancing the XenApp/XenDesktop servers.

- More than one service is bound to the service group.

- Issue ID 0403766: When using the **Traffic Management > Load Balancing > Set Up NetScaler for XenApp/XenDesktop** wizard, applying the application firewall policies through the **Security** settings creates an erroneous condition.
- Issue ID 0409057: When using the **Traffic Management > Load balancing > Set Up NetScaler for XenApp/XenDesktop** wizard, you get a distorted view of the published resources when you apply the application firewall settings in the **Security** section.
- Issue ID 0411152: When you use the **Traffic Management > Load balancing > Set Up NetScaler for XenApp/XenDesktop** wizard, applying the Optimization settings makes applications and desktops unavailable when StoreFront is accessed through a VPN.

  Workaround: Do not apply the optimization settings.

DNS Issues

- Issue ID: 0458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.

  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.
  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.

High Availability Issues

- Issue ID 0443588: In a High Availability configuration, after you remove an HA configuration from one of the two nodes, if you confirm the following prompt message, "Do you want to remove ha node from remote system also ?", an error message might get displayed and the HA configuration is not removed from the remote node.
- Issue ID 0471294: When upgrading HA nodes that have Web Interface on NetScaler (WIonNS) to build 126.x, the updates made in the Webinterface.conf file are over-written by the previous version of the file. This is due to the rolling upgrade of HA nodes or due to the file sync operation between HA nodes.

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

  a. Before upgrading, run the command: "set ns param –internaluserlogin DISABLED".

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

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

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

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

f. Save the configurations.

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

Integrated Caching Issues

- Issue IDs 0440107, 0440389: 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".

Load Balancing Issues

- Issue ID 0441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.

NetScaler Insight Center Issues

- Issue ID 0368967: In a graph that displays a very low number of data points, the time value displayed on the x-axis includes milliseconds. The value displayed for milliseconds has no significance.
- Issue ID 0446120: In some instances, the bar line on a graph appears outside the time points on the x-axis.
- Issue IDs 0379876, 0424686, 0437964: The time values on the graphs display overlapping values, mostly in the 5-minute-interval view.
- Issue ID 0385821: When an ICA session is initiated by launching XenDesktop, the user name is displayed along with the domain name `(user-id@domain-name)`.
- Issue ID 0386911: When launching n instances of an application, the NetScaler appliance sends n-1 termination records for the application. Consequently, the HDX Insight node displays only a single instance of this application as active.
- Issue ID 0394526: On the **Dashboard** > **Web Insight** > **Applications** page, the values shown when you select **Response Time** from the drop-down list can be incorrect.
- issue ID 0397236: On the **Dashboard** > **HDX Insight** > **Users** page, the report for user sessions displays incorrect values. The left pane displays the average values for the entire session, but, the right pane displays the values for the period selected from the drop-down list.

- Issue ID 0399626: In transparent mode, after you initiate a session and launch an application through Citrix Receiver (Enterprise edition) from a Windows 8 client, the session terminates and resumes when you launch subsequent applications. Consequently, HDX Insight reports include session termination records.
- Issue ID 0409634: All the metrics except bandwidth and hits display the average values.
- Issue ID 414160: The following error message appears when NetScaler Insight Center installed on VMware ESX is powered on or off: The VMware Tools power-on script did not run successfully in this virtual machine. If you have configured a custom power-on script in this virtual machine, make sure that it contains no errors. You can also submit a support request to report this issue.
- Issue ID 414214: On the HDX Insight reports, a Y-axis value of 0 is sometimes shown at a location higher than the x axis.
- Issue ID 0424673: Upgrading NetScaler Insight Center on a VMware ESX server from build 118.7 or 119.7 to build 120.13 or later is not supported. However, upgrading from build 120.13 to later builds is supported.

  Workaround: To upgrade to build 120.13 or later build, perform a fresh installation. To retain your existing configurations, make sure that the IP address of the NetScaler appliance and the IP address of NetScaler Insight Center remain the same .
- Issue ID 0324010: A higher than normal load on NetScaler Insight Center or on the database can cause the afdecoder subsystem to stop functioning. As a result, NetScaler Insight Center is unable to connect to the database.

  Workaround: Restart the appliance by running the following command on the command line interface:

  ```
  #/etc/rc.d/analyticsd restart
  ```
- Issue ID 0331944: If no devices have been added to the inventory, the Getting Started wizard is displayed. You cannot access the Configuration tab.
- Issue IDs 0333555 and 346171: After you enable appflow on some virtual servers, even though no error message appears, the Insight column does not display a check box indicating that the feature is enabled.

  Workaround: Refresh the screen. If appflow is enabled, the check box in the Insight column is selected.
- Issue ID 0350977: When you enable Appflow from NetScaler Insight Center, complex policy expressions are not accepted. This issue occurs when you directly type the complex expression in the text box.

  Workaround: Copy and paste the expression from a Notepad.
- Issue IDs 0388096 and 0423109: When you launch XenApp through Citrix Receiver (standard edition), the app launch duration is not calculated and is shown as zero.
- Issue IDs 0388563 and 0438710: The following behavior is seen during a high availability failover on a NetScaler appliance that has active ICA session applications launched:

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

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

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

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

- Issue ID 0388875: When you navigate to **Configuration** > **Inventory** and click on a NetScaler IP address, only one page of load balancing virtual servers is displayed. For example, if you have selected a page size of 25, and the number of load balancing virtual servers (including those associated with content switching virtual servers) exceeds 25, n-25 load balancing virtual servers are not displayed.
- Issue ID 0402105: The following error 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."
- Issue IDs 0404100 and 0404822: The VPN option on the View drop- down list is available for NetScaler 10.0 appliances.
- Issue ID 0404204: NetScaler 10 appliances do not support clearing AppFlow configurations from a virtual server.
- Issue ID 0404477: If you use Internet Explorer to open Desktop Director on an RDP machine, the graph displays extra dotted lines even though everything works fine functionally.
- Issue ID 0405853: If AppFlow is enabled for a virtual server on more than one NetScaler Insight Center virtual appliance, then the clear AppFlow configurations (select **Configuration** > **Inventory** > <ipaddress> > **Application List** > <ipaddress> >**Action** > **Clear AppFlow Configuration**) does not work on the virtual server that has the lowest priority.
- Issue ID 0405951: The count of embedded objects displayed in the waterfall chart can be wrong for recurrent page requests if the NetScaler integrated cache or browser cache is enabled.
- Issue ID 0405953: The waterfall chart displays a blank tooltip when you hover over the blank space between the x-axis and the y-axis.
- Issue ID 421657: If the ICMP port used to verify the network reachability of a NetScaler appliance from NetScaler Insight Center is blocked, the internal routing in NetScaler Insight Center is disrupted and the HDX Insight node is not displayed on the dashboard.

Networking Issues

- Issue IDs 0383958, 0411806: `$` is an invalid value for the port parameter of any extended ACL, but no error message appears if you specify this value. If, while using the configuration utility to configure an extended ACL, you set the port parameter to `$`, no error message appears, but the ACL is not configured.

- Issue ID 0399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.

Platform Issues

- Issue ID 0402111: VLAN tagging is not supported on Netscaler-VPX operating on MacVTap-Bridge, MacVTap-Private, MacVTap-VEPA, MacVTap-Passthrough interface Modes.
- Issue ID 0402113: L2 mode is not supported on Netscaler VPX running on a Linux-KVM host.
- Issues ID 0407184: LACP is not supported on Netscaler VPX instances operating in Bridge, MacVTap-Bridge, MacVTap-Private, or MacVTap-VEPA interface mode.
- Issue ID 0407185: Live migration of a NetScaler virtual machine running on a Linux-KVM host is not supported.

Policy Issues

- Issue ID 0425465: After changing the time zone on a NetScaler appliance, you must restart the appliance so that policies referencing the LOCAL system use the new time zone instead of the old one. Otherwise, policies that should match do not, and policies that should not match do.

Policies Issues

- Issue ID 0390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

- Issue ID 0422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of CLIENT.IP.PROTOCOL.EQ(ICMP) to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

  Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP. ‘!CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)’ .

Reporting Issues

- Issue ID 0368982: After you import a custom data source, the charts for the counters under the **System entities statistics** are inaccurate, because of issues in the third party charting engine.

Signature Bindings Not Shown in PCI-DSS Report Issues

- Issue ID 0443673: The Application Firewall PCI-DSS report does not display signature bindings. The Profile Settings section of the report shows bound signatures as “not set”.

SSL Issues

- Issue IDs 0459688, 0446760: If you use the configuration utility to configure FIPS appliances in a high availability setup, FIPS keys are not exported or imported between the nodes, because the option to enable secure information management (SIM) is not available.

  Workaround: Use the command line to enable SIM. For more information, see http://support.citrix.com/proddocs/topic/netscaler-traffic-management-10-1-map/ns-tmg-fips-configure-fips-ha-tsk.html.

- Issue ID 0469556: In rare cases, in which an unusually large number of new SSL requests are received, freeing an SSL session takes longer than expected. As a result, after some time available memory is exhausted.

System Issues

- Issue IDs 0377618, 0351127, 0364015: 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] .
- Issue ID 0430154: On a NetScaler 1000V instance, transmit congestion occurs on virtual interfaces in high traffic conditions.
- Issue ID 0455041: The NetScaler system backup tar file does not include the following files:

  /nsconfig/ns.conf

  /nsconfig/Zebos.conf

  /nsconfig/rc.netscaler

  /nsconfig/snmpd.conf

/var/log/wicmd.log

/nsconfig/nsbefore.sh

/nsconfig/nsafter.sh

- Issue IDs 449234, 457629: In deployments with large configurations (in the order of 2 MB), when the load on the management CPU is high, the execution of the "show ns runningConfig" command can take a large amount of time.

  Workaround: If you're executing the command manually, then there is no workaround. However, if you are using a script to fetch the the output of the "show ns runningConfig" command, and if the script has a timeout, then modify the script to increase timeout to 500 seconds. The command could be executed within that time period.

- Issue ID 478895: The "show ns runningConfig" command may produce partial output if invoked while another "show ns runningConfig" command, from the same or other admin session is in progress. Workaround: Re-execute the "show ns runningConfig" command to fetch the entire running configuration.

System/Application Firewall Issues

- Issue ID 0437307: On a NetScaler ADC that is not configured to use jumbo frames and that protects a server that is configured to use jumbo frames, if the application firewall is enabled and at least one profile is configured, the ADC might become unresponsive for a period of time and then reset the connection.

VPX Issues

- Issue ID 0405164: On a NetScaler VPX instance running on a Linux-KVM platform, dynamic routing protocols OSPF and ISIS fail to run on the platform’s MacVTap interfaces.

  Workaround: Enable promiscuous mode on these MacVTap interfaces, using either the Linux-KVM graphical interface (Virt-Manager) or the Linux-KVM command line interface (virsh).

- Issue IDs 0405383, 0360482: A NetScaler VPX instance might fail to restart on a Linux-KVM virtualization platform using processors that do not support the constant_tsc CPU feature.

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

  ```
  sysctl netscaler.ns_vpx_halt_method=2
  ```

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

  ```
  sysctl netscaler.ns_vpx_halt_method=2
  ```

Web Interface Issues

- Issue ID 0397150: 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.

XML API Issues

- Issue ID 0363145: The following APIs are not available in version 10.1 or later: `bindservicegroup_state2` `unsetnslimitidentifier_selectorname`. Use `unsetnslimitidentifier_selector` instead.

Chapter 7

Build 125.9

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 125.9

Replaces build: 125.8

Release date: April 2014

Release notes version: 5.0

Language supported: English (US)

Enhancements

Support for Three New Licenses for NS1000V

- ENH ID 0454051: NS1000V on Cisco Nexus 1000V and ESX platform now supports the following three new license:
  - 10M
  - 200M
  - 3000M

Changes

SSL

- Issue ID 0376153: 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
  ```

  A chip is marked disabled after the third failed reinitialization attempt.
- Issue ID 0455821: An SSL chip is disabled at the third reinitialization attempt. That is, the maximum reinitialization limit is 2. Earlier, this limit was 5.

Bug Fixes

Application Firewall

- Issue ID 0428852: On a NetScaler ADC with limited CPU and memory, if the application firewall is enabled, out-of-memory errors might accumulate in the NetScaler log, causing rapid rotation of log files.
- Issue IDs 0436100 & 0447536: On a NetScaler ADC that has the application firewall enabled and the Form Field Consistency check or Field Formats check enabled, a memory leak might cause the ADC to become unresponsive, requiring a manual restart. The underlying issue is a failure to process certain types of web form content properly. Appliances or VPX instances that have limited CPU and memory are especially likely to experience this issue.
- Issue ID 0445552: On a NetScaler ADC HA pair configured to use the Citrix VPN, single sign-on, and the Application Firewall, a memory page issue might cause the primary ADC to reboot, failing over to the secondary ADC.

- Issue ID 0448610: On a NetScaler ADC that has the application firewall enabled and an XML or Web 2.0 profile configured, if a response-side check (such as the Credit Card or Safe Object check) is enabled along with at least one XML-based check, Lotus Notes webmail does not load correctly. Specifically, the frame that should contain the user's inbox is blank.
- Issue IDs 0448961, 0449223, 0449851, & 0450070: When using CVPN or the application firewall credit card or safe object security checks, memory issues might cause the Netscaler ADC to become unresponsive or restart.
- Issue IDs 0446304, 0447206, 0444746, 0444810, 0448814, 0449393, 0449396, 0451162, 0451860, 0452078, and 0452427: If you use the single sign on (SSO) feature on your NetScaler ADC, it might become unresponsive or restart.
- Issue ID 0450939: On a NetScaler ADC that has the application firewall enabled and an XML or Web 2.0 profile configured, if any XML security checks are enabled, certain web content does not load correctly.
- Issue IDs 0452846, 0453768, 0456263, 0459327, and 046450: On a NetScaler ADC that has the application firewall enabled, when a Google Chrome user opens a large PDF file on a protected web server, the ADC might become unresponsive. The same file, if downloaded with Internet Explorer or Mozilla Firefox, causes no problems. The cause is a loop in a backup queue.
- Issue ID 0453111: On a NetScaler ADC that has the application firewall enabled, and that has either limited available memory or a small memory cache configured, a memory page issue might cause the ADC to become unresponsive or reboot.

AAA Application Traffic

- Issue ID 0382693: Currently AAA supports Kerberos authentication only with Datastream Windows Authentication. AAA does not support fallback to NTLM if Kerberos authentication fails.
- Issue ID 0435529: When the NetScaler ADC is configured to use AAA with SAML authentication, and it receives a response from the IDP, it reformats the response in standard SAML format. (This process is sometimes called "canonicalizing" the response.) The ADC might not reformat SAML <samlp: response> namespace prefix tags correctly, because it expects <saml: assertion> format. In that case, digest verification fails.
- Issue ID 0441290: When performing Kerberos authentication or authorization, instead of accepting the hostname that the user provided in the request, AAA-TM now performs a DNS lookup on the hostname IP, and uses the canonical FQDN for that IP when constructing a server SPN.
- Issue ID 0453125: AAA-TM now supports the use of RFC822 name-based (SAN) client certificates to authenticate users. SAN client certificates work in exactly the same way as other client certificates. To configure the NetScaler ADC to use SAN client certificate authentication, follow the client certificate authentication instructions in the AAA-TM documentation.

Command Line Interface

- Issue ID 0441505: A response policy bound to a VPN virtual server is no longer bound to the virtual server after you restart the NetScaler ADC.

Configuration Utility

- Issue ID 0443850: If you use the configuration utility to create a NetScaler-owned IP address, and provide the OSPF LSA Type1 area value, the Type1 area value is not displayed when you click on the created IP address to view or edit the details.
- Issue ID 0446549: After you set the SSO Domain (Single Sign-on Domain) value, the value is not displayed on the configuration utility when you navigate to **Security** > **AAA Application Traffic** > **Settings** > **Change Global Settings**.
- Issue ID 0447077: If you create a monitor by using the graphical user interface and choose the default browse option to select the in-built monitor scripts from the /nsconfig/monitors folder, the folder does not display any scripts to choose.
- Issue ID 0449229: The configuration utility includes an option to enable Net Profile when you create a StoreFront monitor, but that option should not be enabled for a StoreFront monitor.

Content Switching

- Issue ID 0428991: The NetScaler appliance fails in the following scenario:
  a. Create a content switching virtual server (CS1) and bind a policy (P1) to it.
  b. Rename the virtual server (CS1) to CS2.
  c. Create another content switching virtual server named CS1 and bind P1 to the new CS1.
  d. Send traffic to virtual server CS1.
- Issue ID 0445561: If an HTTP content switching virtual server is bound to an SSL virtual server that has a backup SSL virtual server, the following error message appears:

  ERROR: The backup vserver of the target vserver is not compatible with the CS vserver.
- Issue ID 0449261: You must bind only a load balancing (LB) virtual server as the default or target LB virtual server to a content switching (CS) virtual server. Global server load balancing (GSLB), cache redirection (CR), virtual private network (VPN), and CS virtual servers must not be bound to a CS virtual sever as the default or target virtual server.

Integrated Caching

- Issue ID 0427598: The NetScaler appliance fails to respond when it receives multiple byte-range requests for the same objects at almost the same time and where the starting range of byte-range is greater than 1MB.
- Issue IDs 0436298 and 0434877: When refreshing a cache object for a conditional GET to an expired object, the memory is deducted two times but is returned only once when the cache cell goes away. This causes the memory that is used for a content group to slowly increase and finally reach the maximum memory that a content group can use. The NetScaler appliance is therefore unable to cache objects for that content group.

Load Balancing

- Issue ID 0451670: The configuration for the NetScaler Web 2.0 Push feature is not saved in the configuration (ns.conf) file. As a result, if you run the **show running config** command, the push configuration is not shown.
- Issue ID 0452648: In direct server return mode, the NetScaler ADC does not send a RST flag to the client after the idle timeout has expired.

Networking

- Issue ID 0448738: On a NetScaler ADC configured for link load balancing with RNAT, access to external sites fails intermittently.
- Issue ID 0449175: In a High Availability configuration, if you set the maxFlips, maxFlipTime or syncvlan parameter of the set HA node command, the NetScaler ADC adds a duplicate entry of the add HA node command to the running configuration.

NITRO API

- Issue ID 0444986: When importing an AppExpert template that has back end services configured, the NetScaler ADC reports a protocol mismatch error even if other service parameters (service name, IP address and port) are not the same.

Policies

- Issue ID 0430148: Error messages displayed during policy binding are shown as hexadecimal code instead of the corresponding warning message.

SNMP

- Issue ID 0407594: The aggregateBWUseHigh and aggregateBWUseNormal SNMP traps are frequently generated even though the bandwidth is less than the set value for the alarm.

SSL

- Issue ID 0436205: If you add a certificate revocation list (CRL) with refresh enabled, the appliance might perform a core dump and restart.

System

- Issue ID 0447623: When a client's MPTCP token is invalid in the C2C steered MP_CAPABLE final ACK, the packet is dropped silently without flushing out the RSS filter. This filter is never deleted. If the client reuses the same 4-tuple as the filter, the incoming packet may go into the steering loop between the PEs. This will lead to very high CPU utilization.
- Issue ID 447618: The NetScaler VPX appliance is now supported on VMware vSphere Hypervisor (ESXi) versions 5.1 and 5.5. This means that a NetScaler virtual instance can be instantiated on the 5.1 or 5.5 versions of the ESXi hypervisor.

Known Issues and Workarounds

Application Firewall

- Issue ID 0364134: In the configuration utility, when you perform the **Show Bindings** operation, globally bound auditing syslog policies do not appear under **Application Firewall**. This issue occurs only in a cluster setup.

  Workaround: Display the bindings in the command line interface, by using the **show system global** command.
- Issue ID 0372768: If you use the default browser PDF plugin to view an application firewall report, embedded links might be inactive.

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 0399596: When you update the application firewall signatures from the NetScaler command line, you must update the default signatures first, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files.

  For example, if you had two sets of custom signatures, named **custom_signatures** and **custom_signatures_2**, that were based on copies of the default signatues file,

you would update the signatures on your NetScaler ADC by issuing the following commands:

```
update appfw signatures "*Default Signatures"
update appfw signatures "custom_signatures"
update appfw signatures "custom_signatures_2"
```

- Issue ID 0430014: 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
  ```

- Issue ID 0443673: The Application Firewall PCI-DSS report does not display signature bindings. The Profile Settings section of the report shows bound signatures as "not set".

Configuration Utility

- Issue ID 0361793: The count of the number of load balancing virtual servers, which is shown in the configuration summary, includes the load balancing virtual server that is created during the configuration of EdgeSight Monitoring, even though that load balancing virtual server is not displayed in the **Load Balancing** > **Virtual Servers** pane.
- Issue ID 0374304: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a `No such resource` error message appears, even if the rename operation is successful.

Workaround: Use the mouse to click the **OK** button, instead of pressing the ENTER key on the keyboard.

- Issue ID 0374437: If, when using the configuration utility to configure the NetScaler appliance, you press **Alt+Tab** to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press **Alt+Tab** a second time.
- Issue ID 0388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml.
- Issue ID 0389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 0448851: The **System** > **Cluster** > **Manage Cluster** screen allows a user to create a cluster without providing a Cluster IP address.

Content Switching/Load Balancing

- Issue ID 0399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

Domain Name System

- Issue ID 0458244: If DNS caching is enabled and the NetScaler ADC receives a query that is not cached, it forwards the query to the name server. It sends the response from the server to the client and also caches the records in the Answer, Authority, and Additional sections of the DNS response. The response from the server can have the AA bit set or unset.
  - If the AA bit is set and a query is received for a record that was cached and a part of the Authority or Additional section, the ADC responds to the query from its cache with the AA bit unset and TTL decremented.
  - If a subsequent query is received for a record that is cached and was part of the Answer section, the ADC responds to the query from its cache with the AA bit set and the original TTL.

High Availability

- Issue ID 0443588: In a High Availability configuration, after you remove an HA configuration from one of the two nodes, if you confirm the following prompt message "Do you want to remove ha node from remote system also ?", an error message might get displayed and the HA configuration is not removed from the remote node.

Integrated Caching

- Issue ID 0440107: 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".

Load Balancing

- Issue ID 0441776: The NetScaler ADC might fail or become unresponsive if the FTP virtual server name exceeds 32 characters and L2Conn is enabled on the virtual server.

Networking

- Issue ID 0383958: `$` is an invalid value for the port parameter of any extended ACL, but no error message appears if you specify this value. If, while using the configuration utility to configure an extended ACL, you set the port parameter to `$`, no error message appears, but the ACL is not configured.
- Issue ID 0399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.
- Issue ID 0469033: In a high availability configuration, you might lose your VLAN configuration if you upgrade the secondary node to build 125.9 from builds 122.17, 123.11, or 124.13.

Policies

- Issue ID 0390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

- Issue ID 0422967: If a wildcard virtual server (** IP address and port values) that accepts both IPv4 and IPv6 packets uses a listen policy of

`CLIENT.IP.PROTOCOL.EQ(ICMP)` to capture ICMP traffic, it also captures IPv6 packets in which the second byte of the source IPv6 address has a value of 01).

Workaround: First use an expression that filters the IPv4 traffic, and then use an expression that reads the protocol value from the filtered IPv4 packets and checks for a protocol value of ICMP. `'!CLIENT.IP.SRC.IS_IPV6 && CLIENT.IP.PROTOCOL.EQ(ICMP)'`

- Issue ID 0425465: After changing the time zone on a NetScaler appliance, you must restart the appliance so that policies referencing the LOCAL system use the new time zone instead of the old one. Otherwise, policies that should match do not, and policies that should not match do.

Reporting

- Issue ID 0368982: After you import a custom data source, the charts for the counters under the **System entities statistics** are inaccurate, because of issues in the third party charting engine.

SSL

- Issue IDs 0414388 and 0345883: 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.

System/Application Firewall

- Issue ID 0437307: On a NetScaler ADC that is not configured to use jumbo frames and that protects a server that is configured to use jumbo frames, if the application firewall is enabled and at least one profile is configured, the ADC might become unresponsive for a period of time and then reset the connection.

vPath

- Issue ID 0460298: On a NetScaler 1000V appliance, vPath offload packets cannot be carried over tagged interfaces.

Web Interface

- Issue ID 0397150: 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.

XML API

- Issue ID 0363145: The following APIs are not available in version 10.1 or later:
  - `bindservicegroup_state2`
  - `unsetnslimitidentifier_selectorname`

  Use `unsetnslimitidentifier_selector` instead.

Chapter 8

Build 124.14

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 124.14

Replaces build: None

Release date: March 2014

Release notes version: 1.0

Language supported: English (US)

Enhancements

vPath

- ENH ID 0407707: You must now explicitly enable vPath on the NetScaler 1000V virtual appliance.
  - Using the command line interface: `enable ns feature vpath`
  - Using the graphical user interface: Navigate to **Configuration** > **System** > **Settings** > **Configure advanced features** > **vPath**
- ENH ID 0414234: You can now specify whether the NetScaler must offload to the VEM, sessions for which the NetScaler has no matching configurations and hence not interested in. When the offload parameter is enabled, the NetScaler adds an extra 24 bytes to the vPath header.
  - Using the command line interface: `set vPathParam -srcIP <ip_addr> -offload ENABLED`
  - Using the graphical user interface: Navigate to **Configuration** > **System** > **Settings** > **Configure VPath Parameters**

Bug Fixes

- Issue ID 0415152: Port 0/2 in NetScaler 1000V hosted on the Nexus 1010/1110 platform is used for only internal communication. Do not configure it to for data or control traffic.
- Issue ID 0415624: In the configuration utility, you are prompted to reenter your login credentials after accepting the end user licensing agreement (EULA). For security reasons, the password is not stored.
- Issue ID 0427510: For server originated UDP packets, applications must base the maximum payload size on the available path MTU information.
- Issue ID 0416631: The NetScaler 1000V virtual appliance does not support the scale out model with the NetScaler TriScale clustering feature.

Known Issues and Workarounds

Application Firewall

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

  Workaround: Use the Adobe PDF browser plugin.

- Issue ID 0399596: When you update the application firewall signatures from the NetScaler command line, you must first update the default signatures, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files. For example, if you had two sets of custom signatures, named **custom_signatures** and **custom_signatures_2**, that were based on copies of the default signature file, you would update the signatures on your NetScaler appliance by issuing the following commands:
  - update appfw signatures "*Default Signatures"
  - update appfw signatures "custom_signatures"
  - update appfw signatures "custom_signatures_2"

Configuration Utility

- Issue ID 0361793: The count of the number of load balancing virtual servers, which is shown in the configuration summary, includes the load balancing virtual server that is created during the configuration of EdgeSight Monitoring, even though that load balancing virtual server is not displayed in the **Load Balancing** > **Virtual Servers** pane.
- Issue ID 0374304: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a `No such resource` error message appears, even if the rename operation is successful.

  Workaround: Use the mouse to click the **OK** button, instead of pressing the ENTER key on the keyboard.
- Issue ID 0374437: If, when using the configuration utility to configure the NetScaler appliance, you press **Alt+Tab** to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press **Alt+Tab** a second time.
- Issue ID 0388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml
- Issue ID 0389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

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

Content Switching/Load Balancing

- Issue ID 0399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

Domain Name System

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

Monitoring

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

Multipath TCP Support

- Issue ID 0331338: With USIP enabled, MPTCP requests do not go through.
- Issue ID 0400819: MPTCP does not support FTP data connections.
- Issue ID 0400861: Virtual servers to which a listen policy is bound accept connections from the first subflow only.
- Issue ID 0400875: Multiple spillover persistence sessions are created for a single MPTCP transaction.
- Issue ID 0401793: MPTCP does not support IPv6 addresses.

NetScaler 1000V Appliance

- Issue ID 0371005: If you deploy a standalone NetScaler 1000V on a secondary Nexus appliance, you are prompted to enter an IP address, netmask, gateway, and host name for the primary NetScaler node.

  Workaround: Enter dummy values for IP address, netmask, gateway, and host name.

- Issue ID 0439061: Due to changes in the vPath library, you cannot upgrade from NetScaler 10.1 Build 123.x and earlier builds to this release.

  Workaround: You must install the NetScaler 1000V ESXi package or Nexus 1010/1110 package.

Networking

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

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

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

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

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

  and the following command on the secondary node:

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

- Issue ID 0383958: `$` is an invalid value for the port parameter of any extended ACL, but no error message appears if you specify this value. If, while using the configuration utility to configure an extended ACL, you set the port parameter to `$`, no error message appears, but the ACL is not configured.
- Issue ID 0399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.

Policies

- Issue ID 0390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

Reporting

- Issue ID 0368982: After you import a custom data source, the charts for the counters under **System entities statistics** are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with an RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

System

- Issue ID 0430071: ISIS packets are dropped at the Nexus 1000V distributed virtual switch (DVS) as there is no option to enable promiscuous mode on the DVS. However, this issue is not observed when the virtual machines are connected through the ESX virtual switch with promiscuous mode ON.
- Issue ID 0430154: On the NetScaler 1000V, transmit congestion is experienced on virtual interfaces in high traffic conditions.

XML API

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

Chapter 9

Build 120.21

Topics:

Release version: Citrix NetScaler 1000V, version 10.1 build 120.21

Replaces build: None

Release date: November 2013

Release notes version: 1.0

Language supported: English (US)

Enhancements

Cluster Support

- ENH ID 0416631: You can now create a cluster of NetScaler appliances. For detailed information, see the *NetScaler-Admin-Guide-10-1.pdf*.

FTP and TFTP Support

- ENH ID 0422421: The NetScaler 1000V virtual appliance supports load balancing for FTP and TFTP.

Pre-fragmentation Support for vPath Packets

- ENH ID 0427507: The NetScaler 1000V supports pre-fragmentation of vPath encapsulated packets.

System

- Issue ID 0427510: In a NetScaler 1000V deployment with vPath configured, the maximum value for the Maximum Segment Size (MSS) is 1380.
- Issue ID 0427511: Communication between a server which has been added as a NetScaler service and another backend server is now supported without performing additional configurations.

Known Issues and Workarounds

Application Firewall

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

  Workaround: Use the Adobe PDF browser plugin.
- Issue ID 0399596: When you update the application firewall signatures from the NetScaler command line, you must first update the default signatures, and then issue additional update commands to update each custom signatures file that is based on the default signatures. If you do not update the default signatures first, a version mismatch error prevents updating of the custom signatures files. For example, if you had two sets of custom signatures, named **custom_signatures** and **custom_signatures_2**, that were based on copies of the default signature file, you would update the signatures on your NetScaler appliance by issuing the following commands:

- update appfw signatures "*Default Signatures"
- update appfw signatures "custom_signatures"
- update appfw signatures "custom_signatures_2"

Configuration Utility

- Issue ID 0361793: The count of the number of load balancing virtual servers, which is shown in the configuration summary, includes the load balancing virtual server that is created during the configuration of EdgeSight Monitoring, even though that load balancing virtual server is not displayed in the **Load Balancing** > **Virtual Servers** pane.
- Issue ID 0374304: If you access the configuration utility through Internet Explorer 9 or 10 and rename a virtual server, a `No such resource` error message appears, even if the rename operation is successful.

  Workaround: Use the mouse to click the **OK** button, instead of pressing the ENTER key on the keyboard.
- Issue ID 0374437: If, when using the configuration utility to configure the NetScaler appliance, you press **Alt+Tab** to switch between programs, the current dialog box might disappear, hidden behind the main configuration utility screen. To reach the dialog box, press **Alt+Tab** a second time.
- Issue ID 0388534: If you access the NetScaler configuration utility from the Start screen on a Windows 8 machine, the Java based configuration views are not displayed.

  Workaround: Switch to the Desktop screen to display Java based configuration views. Microsoft Windows 8 does not support plug-ins on the Start screen, and therefore Java cannot run on the Start screen. For more information, see http://www.java.com/en/download/faq/win8_faq.xml
- Issue ID 0389328: If you use the Google Chrome browser to access the NetScaler configuration utility, and the monitor resolution is low, you might not be able to use the mouse to scroll the screen.

  Workaround: Use the arrow keys on the keyboard to scroll the screen.
- Issue ID 0438216: In the NetScaler configuration utility, virtual servers whose names begin with "APP_" or "app_" are not displayed.

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

Content Switching/Load Balancing

- Issue ID 0399575: When you configure load balancing virtual servers in a content switched environment, the service types of primary and backup virtual servers must be the same. If you assign a backup virtual server with a service type of TCP to a load balancing virtual server with a service type of HTTP, any content switching action bound to the load balancing virtual server fails.

Domain Name System

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

Monitoring

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

Multipath TCP Support

- Issue ID 0331338: With USIP enabled, MPTCP requests do not go through.
- Issue ID 0400819: MPTCP does not support FTP data connections.
- Issue ID 0400861: Virtual servers to which a listen policy is bound accept connections from the first subflow only.
- Issue ID 0400875: Multiple spillover persistence sessions are created for a single MPTCP transaction.
- Issue ID 0401793: MPTCP does not support IPv6 addresses.

NetScaler 1000V Appliance

- Issue ID 0371005: If you deploy a standalone NetScaler 1000V on a secondary Nexus appliance, you are prompted to enter an IP address, netmask, gateway, and host name for the primary NetScaler node.

  Workaround: Enter dummy values for IP address, netmask, gateway, and host name.
- Issue ID 0415152: Port 0/2 in NetScaler 1000V hosted on the Nexus 1010/1110 platform is used for only internal communication. Do not configure it to for data or control traffic.
- Issue ID 0415624: In the configuration utility, you are prompted to reenter your login credentials after accepting the end user licensing agreement (EULA). For security reasons, the password is not stored.
- Issue ID 0427510: For server originated UDP packets, applications must base the maximum payload size on the available path MTU information.

Networking

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

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

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

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

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

  and the following command on the secondary node:

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

- Issue ID 0383958: `$` is an invalid value for the port parameter of any extended ACL, but no error message appears if you specify this value. If, while using the configuration utility to configure an extended ACL, you set the port parameter to `$`, no error message appears, but the ACL is not configured.
- Issue ID 0399436: The NetScaler appliance does not create session entries for ICMPv6 packets that match a forwarding-session rule.

Policies

- Issue ID 0390584: You cannot use the configuration utility to define classic SSL policies. However, you can use the configuration utility to bind and unbind classic SSL policies.

  Workaround: Use the CLI to define classic SSL policies.

  Note: Citrix encourages the use of default syntax policies rather than classic policies.

Reporting

- Issue ID 0368982: After you import a custom data source, the charts for the counters under **System entities statistics** are inaccurate, because of issues in the third party charting engine.

SSL

- Issue ID 0343395: On the NetScaler appliance, TLS protocol version 1.2 does not support a client certificate with an RSA 4096-bit key.
- Issue ID 0345883: On the NetScaler appliance, TLS protocol version 1.2 does not support ephemeral Diffie-Hellman cipher suites.

System

- Issue ID 0430071: ISIS packets are dropped at the Nexus 1000V distributed virtual switch (DVS) as there is no option to enable promiscuous mode on the DVS. However, this issue is not observed when the virtual machines are connected through the ESX virtual switch with promiscuous mode ON.
- Issue ID 0430154: On the NetScaler 1000V, transmit congestion is experienced on virtual interfaces in high traffic conditions.

XML API

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