Citrix NetScaler 1000V Release Notes

Citrix NetScaler 10.5-65.11

First Published: 2017-03-07

Cisco Systems, Inc.
www.cisco.com

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

Contents

10.5-65.11

Updated: February 10, 2017 | Release notes version: 1.0

This release notes document describes the enhancements and changes and specifies the issues that exist, for the NetScaler release 10.5 Build 65.11. See Release History.

Fixed Issues

The issues that are addressed in Build 65.11.

AAA-TM

The NetScaler appliance does not set the cookie domain that is configured in authentication profile specified at LB/CS vservers.

Due to this, cookie is set for domain on authentication vserver fqdn but for host at CS/LB vserver. This causes issues when cookie is being expired programmatically, such as responder policies.

[# 594634]

- In a high availability setup, a session does not time out even if a force timeout is configured on a traffic action that is bound to a load balancing or content switching virtual server and a force fail over is performed.

  [# 623053]

- In a multi-core NetScaler environment, user sessions sometimes do not get terminated if the decision to terminate is based on a force timeout value that is configured on a TM traffic action.

  [# 610604, 618760]

AppFlow

- A NetScaler load balanced server responds with a 411 error code for a corrupted HTTP request.

  [# 629223]

Application Firewall

- The Onhover pattern has been added to the default list of cross-site scripting (XSS) denied patterns that the Application Firewall looks for when scanning traffic.

  [# 665595]

- Executing force sync operation using the nssync -s command from the shell triggers NetScaler appliance reboot and crash. The nsnetsvc crash occurs when the import filename length exceeds MAX_FILE_PATH_LEN.

  [# 657920]

Configuration Utility

- If you create a cipher group and do not add any ciphers to it, an error message appears when you try to open the cipher group in the configuration utility.

  [# 604646]

DNS

- If the DNS server from which the cached DNS records are being served goes DOWN, the proactive DNS update queries are redirected to the back-end server.

  [# 660562]

- When the NetScaler appliance receives a DNS TCP packet that has dnspayloadlen as zero, the NetScaler appliance might dump core memory.

  [# 666803]

- A NetScaler appliance might fail while performing DNSSEC offloading if insufficient memory results in memory allocation failures.

  [# 594535]

DataStream

- The DataStream feature does not work if you use a MySQL database at the back end.

  [# 629504]

GSLB

- In a GSLB high availability setup, if a node stays in secondary state for more than 249 days, the service state might not be updated on this node after it becomes the primary node.

  [# 658093]

- The MEP connection for site metrics goes DOWN if the dynamic RTT and GSLB server persistence features are unused for more than 249 days. In some cases, however, the MEP connection for site metrics remains UP, but the MEP connection for network metrics goes DOWN.

  [# 658890]

Load Balancing

- If a GSLB service goes DOWN and then returns to the UP state, the configured hash-based load balancing methods might produce incorrect load balancing decisions, because the cache maintained for hash-based load balancing algorithms is not cleared when the GSLB service state is updated through MEP.

  [# 658463, 658940]

Networking

- On a NetScaler appliance, when a routing daemon (for example, BGP routing daemon) is restarted multiple times over a short period of time, the corresponding routing configuration (for example, BGP routing configuration) might get removed from the appliance.

  [# 669005]

- For extended ACL rules that are associated with NAT configurations (for example, RNAT rules and Large Scale NAT configurations), the NetScaler GUI displays the TCP established parameter as enabled even though the parameter is disabled.

  [# 597458]

- Restarting a NetScaler appliance that has a VLAN bound to a traffic domain and is configured as a SYNC VLAN or NSVLAN might cause configuration loss of binding between the VLAN and the traffic domain.

  [# 648839]

- In a high availability (HA) setup, after an HA force failover operation, the NetScaler appliance removes (but not properly) static default route6s of all non-default traffic domains from its memory.

  Though the "show route6 operation" does not display these route6s but adding them again fails with the following error message: "ERROR: Resource already exist". This is because these route6s were not completely removed from memory.

  This issue also happens on a standalone NetScaler appliance when a traffic domain that has default route6s is removed.

  [# 644265]

Policies

- If your NetScaler appliance is licensed for 135255 users but has insufficient Mem POLENG memory to support 135255 VPN sessions, the appliance might fail.

  [# 636579, 665701]

SSL

- SSL processing is delayed if the server sends a DES cipher with TLS1.2 protocol in the server_hello message to the NetScaler appliance. Although this combination is deprecated, the appliance tries to process it. The operation fails at the SSL card and blocks the card for a few seconds, causing latency in processing any new requests on the same card.

  [# 661628]

- In a cluster setup, you cannot make any change to a service or service group if you have associated a common name with the service or the service group and enabled or disabled server name indication (SNI).

  [# 665340]

- An SSL handshake fails if all the ECDHE ciphers in the cipher list sent by the client are not supported by the NetScaler appliance even though the list contains some non-ECDHE ciphers that are supported.

  [# 668239]

- If you try to load large certificate files (> 256kB), the NetScaler appliance might dump core and restart, because of insufficient memory.

  [# 643614, 624364, 646510, 667980]

- In a cluster setup, if you rename a load balancing virtual server of type SSL, the local database table that is used for all GET operations is not updated.

  [# 620964, 576828, 641041]

- The version displayed in syslog is SSLv2.0 even though the session is negotiated using TLSv1.2.

  [# 474417, 474413]

- If you upgrade to release 10.5, SSL client authentication fails if it uses a 4096-bit client certificate.

  [# 600815, 343395]

System

- By default, a NetScaler appliance ignores the non-standard and obsolete "Proxy-Connection" HTTP header. To change this behavior, use the nsamimgr command to set the proxyConnection parameter to 1. This setting prioritizes the Proxy-Connection header over the Connection header.

  For example, nsapimgr -ys proxyconnection=1

  [# 654560]

- The HTML-injection feature might cause dropped requests, closed connections, and possible failure of the NetScaler appliance. The HTML-injection feature generates a special request for each embedded object, for sending timestamp-related information to the EdgeSight server. The request URL contains the content type of the object. If the Content-Type field in the request contains a space, it should be percent-encoded, but the HTML-injection feature inserts the space as is. Therefore, by HTTP standards, the request is invalid. If the "drop invalid requests" option is enabled in the applicable HTTP profile, the request is dropped and the connection is closed. Also, if the URL spans multiple packets, the NetScaler appliance fails while processing the next packet after the request is marked invalid.

  [# 626848]

- The TCP timestamp is now an interoperable parameter for TCP and Multipath TCP (MPTCP) data transmission.

  [# 646496]

- In a MPTCP connection, if a client negotiates a Maximum Segment Size (MSS) value of more than 1460 bytes, and the NetScaler appliance receives an ICMP protocol error message after fragmenting and sending a Data Security Standard (DSS) packet, the appliance fails. This happens because of incorrect handling of DSS packets with a segment sizes.

  [# 648275]

- In an MPTCP connection, a NetScaler appliance sets the TCP PSH flag during retransmission of FastClose and DataFIN packets.

  [# 667765]

- start nstrace operation fails with the following error message: "one instance is already running".

  [# 668051]

- A NetScaler appliance constantly fails and dumps core memory, filling the Var directory with core files.

  [# 647955]

- If a FASTCLOSE packet from a NetScaler appliance to a client is lost, the multipath TCP (MPTCP) session does not notify the application about the abrupt connection closure and close the socket. As a result, the appliance does not retransmit the lost packet.

  [# 649968]

- 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.

  [# 449234, 457629, 496448]

- NetScaler appliance crashes when a large host-name header is received and AppFlow logging for host-name and domain-name is enabled.

  [# 660075, 664886]

- The NetScaler command line does not come out of the execution logic and does not display the command prompt when multiple grep with pipe operations are performed.

  [# 667214]

Known Issues

The issues that exist in Build 65.11.

AAA-TM

- When SAML is used in a high availability (HA) setup, a SAML single logout operation does not terminate the session on the secondary appliance.

  [# 590384]

- User-account lockout details for a AAA virtual server cannot be configured at the global level, but only at the AAA virtual server level, because the maxLoginAttempts and failedlogintimeout parameters are not supported at the global level.

  [# 483521]

- When executing the "unlock aaa user" command, the NetScaler appliance does not check whether that account was actually locked.

  [# 483544]

- In release 10.5, moving to a higher authentication level is not supported for 401-enabled load balancing virtual servers.

  [# 645501]

Acceleration

- If a compression module receives an HTTP header in two NetScaler Buffers (NSBs), where first the NSB has a complete header ending with "\r\n\r" and the other NSB header ends with "\n", the module does not handle the HTTP header properly. Page rendering in the client's browser is garbled.

[# 629128]

Application Firewall

- The application firewall allows configuring default field format parameters. The valid range for the maximum field format length is 1-65535. The GUI as well as CLI currently accepts zero as input even though zero is outside the allowed range.

  [# 608010, 603763, 629859]

- When a NetScaler appliance is upgraded from a 10.1 build to a 10.5 build, the application firewall signature names are converted to all lowercase characters. If the name of the signature contains any uppercase character, the conversion affects the binding between profile and signature. Any attempt to modify either the profile or the signature object displays an error message in the configuration utility.

  [# 568705]

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

  [# 547282]

Cache Redirection

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

  [# 442353]

Cisco RISE Integration

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

  [# 502591]

Clustering

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

  [# 538489]

- When Layer 2 mode and MBF are enabled in a cluster deployment, access to * 80 services can fail intermittently.

[# 479899]

Command Line Interface

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

  [# 512526, 527066, 545578, 631658, 635938, 643466, 652771, 667794]

Configuration Utility

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

  Workaround: Use the command line interface .

  [# 470941]

DNS

- Contrary to the information provided in the documentation, DNS Views prevent service selection if a service is not bound to the View.

  [# 580259]

- A NetScaler appliance configured for DNSSEC offloading might fail because of a race condition that can occur when the appliance receives a DNS query for a type A record for a domain that also has a CNAME record, and the canonical name identifies a domain that is in the zone offloaded for DNSSEC processing.

  [# 599741]

Integrated Caching

- The details of cache objects are not available in the NetScaler GUI. However, the list of cached objects is available.

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

  [# 457623]

- The NetScaler appliance fails while caching a 404 response.

  Workaround: Configure your Cache not to cache a 404 response.

  [# 608477]

- A VPX system can repeatedly fail if HA cache persistence is used along with HTML-injection.

  [# 581598]

Load Balancing

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

  [# 480852]

NITRO

- If you make a GET call with the service_args parameter on .NET SDK, the call fails with the exception Invalid argument value [internal].

  Workaround: Instead of the parameter

  $opts.args = "internal:true"

  Use the parameter:

  option.set_args("internal:true")

  [# 595938]

NetScaler GUI

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

  [# 486590]

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

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

  [# 466245, 475388]

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

  [# 524762]

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

  [# 531567]

- On a NetScaler instance deployed on Azure, the welcome page in the GUI prompts you to enter a SNIP address, but a SNIP address is not required to configure NetScaler VPX on Azure. You can skip this step.

  [# 559971]

- The Service hits and Service hits (Rate) counters by the "stat services" command do not apply to services, but to the service-virtual server binding. These counters are displayed in the graphical view of services and should be ignored.

  [# 538057]

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

  [# 483421]

- The service group members do not appear in the output of the "show lb vserver" command if it is run on a cluster IP address.

  [# 642802, 668935]

NetScaler Insight Center

- A NetScaler Insight Center screen might truncate an application name received from AppFlow.

  [# 607863]

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

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

  [# 514990, 523318]

Networking

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

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

  [# 429006]

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

  [# 439294]

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

[# 455936]

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

  [# 459679]

- The NetScaler appliance does not support IPIP tunnels on the client side.

  [# 623671]

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

  [# 485385]

- Configuring a Link Load Balancing virtual server as backup to a Load Balancing virtual server is not supported.

  [# 564040, 587817]

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

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

  [# 486131]

NetScaler VPX Appliance

- A NetScaler VPX instance does not reboot successfully when deployed on a KVM linux host with Xeon E5-26xx v2 processors.

  Workaround: Reload the kvm_intel module with enable_apicv=N parameter by using the following command:

  modprobe kvm_intel enable_apicv=N

  [# 587727, 615203, 642617, 657386]

Policies

- While evaluating default syntax expression for local time zone, a NetScaler appliance incorrectly applies US daylight savings time (DST) rules in non-US time zone. This results in setting an offset time for an hour. For example, the default expression !(SYS.TIME.GE (LOCAL 8h) & SYS.TIME.LE(LOCAL 17h)) returns 'False' if the local time in US time zone is between 0800 and 1700. In the UK time zone, this expression incorrectly returns 'False' if the local time is between 0700 and 0759 and returns 'True' if the local time is between 1700 and 1759 from 8 Mar 2015 (the start of US DST) to 28 Mar 2015 (the day before the start of UK DST) and also from 25 Oct 2015 (the day after the end of UK DST) to 31 Oct (the day before the end of US DST).

[# 556230]

SSL

- A few extra messages appear in the output if you run the show command for the back-end SSL service, service groups, or internal services on a cluster IP address.

  [# 669064]

- Deprecated commands might be lost from the configuration (ns.conf file) after you upgrade to a build that supports the default SSL profile.

  [# 598974, 671233]

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

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

  - Intermediate certificate(s)

  - Root CA certificate

  The server key can be anywhere in the file.

  [# 535145]

- On a NetScaler VPX instance, an error message does not appear if you enable TLS protocol version 1.1 or 1.2 on the backend SSL service or backend SSL profile. These protocols are not supported on a backend SSL service or profile.

  [# 658396]

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

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

  ERROR: Processing of certificate bundle file failed.

  Workaround: Specify only the file name. For example,

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

  [# 481878, 521933]

- After you bind a profile to an SSL virtual server, the "show running config" command incorrectly displays the settings that were in effect before the profile was bound to the virtual server. The SSL profile settings override any virtual server settings.

  [# 624090]

- On a platform that has N3 chips, you cannot use the NetScaler GUI to bind ECDHE, AES-GCM, or SHA2 cipher groups to a back-end service or service group, because these cipher groups are not listed in the GUI.

Workaround: Use the NetScaler command line. At the NetScaler command prompt, type:

bind ssl service <serviceName> -cipherName <string>

To bind a cipher to a service group, replace service with servicegroup in the above command.

[# 640546]

- The description string of a cipher in the output of the "show ssl service" command differs if the command is run on the NetScaler IP address and on the cluster IP address.

  [# 669128]

- An incorrect error message appears if you try to associate an SSL log profile with an SSL action of type DATA INSERTION.

  [# 653279]

- The online certificate status protocol (OCSP) URL does not resolve to the correct IP address after the DNS server resolves it to a new IP address.

  Workaround: See https://support.citrix.com/article/CTX218959.

  [# 654743]

- If you use the add crl command in release 9.3 to add a certificate revocation list (CRL) with refresh enabled, and you don't specify a method, the add crl command returns an error after an upgrade to a later release. Unlike 9.3, later releases do not have a default method.

  [# 604061]

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

  For example,

  > show ssl service svc1 -cipherDetails

  ERROR: No such resource [serviceName, svc1]

  [# 402423]

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

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

  [# 459987]

- If you update a certificate-key pair from DER to PEM format, the message "Invalid Certificate" appears.

Workaround: Add "-inform PEM" in the update command.

[# 630248]

System

- If you access a NetScaler appliance from the GUI, the TCP/IP Connection page supports only a set of classic and advanced policy expressions as a filter. If you use an unsupported expression as a filter, the NetScaler GUI does not display a warning message, and using the unsupported expression leads to an appliance failure.

  Note: You can type the show connectiontable command to view the list of supportable expressions.

  [# 614494]

- Downgrading from NetScaler 10.5

  If you downgrade from release 10.5 to any of the following builds, the error message "Cannot untar GUI" appears:

  * Release 10.1, build 122.17 or earlier

  * Release 10.0, build 78.6 or earlier

  * Release 9.3, build 65.8 or earlier

  Workaround: Reboot the NetScaler ADC and run the installns script again for the same build.

  [# 439341, 442550, 451897]

- If AppFlow and client side measurements are enabled, the NetScaler appliance deletes the NSC_ESNS cookie before forwarding the request to the backend server. A rule was rewritten and configured to insert the Pback cookie in the request sent to the backend server. We are corrupting the OutllookSession cookie when we are trying to do both insert and delete in the HTTP request at the same offset. This is causing sign-on problems. This issue is under investigation.

  [# 633371]

- FreeBSD version for Auditlog Server

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

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

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

  [# 447571]

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

  [# 452382, 459464, 530627]

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

  [# 483524]

- A NetScaler appliance is designed to work on a standalone or a high availability appliance. As a result, an issue is identified and all the log messages are sent to the NSLOG server.

  [# 609655]

- If, when you reboot a NetScaler appliance, the SNMP agent starts before the system monitoring application, the agent reads the Voltage and Fan Speed counter values as zero and sends low-threshold traps. Then, when the system monitoring application starts and updates the counter values, if the values are still less than the threshold values, the SMNP agent does not send traps to clear the low-threshold traps.

  [# 571914]

- The Syslog server continues to receive logs even after the syslog policies are unbound on the appliance

  [# 557257]

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

  [# 472833]

- SNMP requests intermittently fail to get a response from a NetScaler appliance if the response packet size is larger than 1460 bytes.

  [# 634283]

- Connection failover might fail if it is enabled on virtual servers that have the same IP address and port but different listen policies.

  [# 582087, 587620]

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

  [# 428209]

- Wireshark Version for Getting NetScaler Trace

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

  [# 462557]

User Interface

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

  Workaround:

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

  [# 533475]

Web Interface on NetScaler (WIonNS)

- If the NetScaler appliance is upgraded from version 10.1 to 10.5 and the maxSite setting of Web Interface on NetScaler is 3, the system does not have sufficient memory to handle 5000 users accessing Web Interface on NetScaler.

  [# 601304]

What's New in Previous NetScaler 10.5 Releases

The enhancements and changes that were available in NetScaler 10.5 releases prior to Build 65.11. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

AAA-TM

- Strong Encryption Support in Kerberos KCD

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

  [From Build 50.10] [# 427766]

- Responder After AAA

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

  [From Build 50.10] [# 258274, 258277]

- Extracting SAML Attributes from Keytab

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

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

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

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

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

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

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

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

  3) Do one of the following:

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

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

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

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

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

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

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

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

  8) Click Create or OK to save your changes.

[From Build 50.10] [# 405134]

- NetScaler as SAML IDP

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

  For more information, see the NetScaler documentation.

  [From Build 50.10] [# 406525]

- With previous versions of the NetScaler ADC, OWA 2010 connections did not timeout because OWA sends repeated keepalive requests to the server to prevent timeouts, which interfered with single sign-n and posed a security risk. AAA-tm now supports forced timeouts that ensure that OWA 2010 sessions timeout after the specified period of inactivity.

  For more information and configuration instructions, see the documentation.

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

- KCD Performance Improvements

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

  [From Build 50.10] [# 412687]

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

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

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

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

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

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

[From Build 50.10] [# 338718, 314443]

- Unlocking Locked-Out User Accounts

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

  unlock aaa user <userName>

  [From Build 50.10] [# 437164]

- Web-based Authentication

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

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

  [From Build 50.10] [# 431391]

- NetScaler Default Expressions support for authentication subsystem

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

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

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

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

[From Build 50.10] [# 418615]

- Renegotiate Support for Certificate-based Policies

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

  [From Build 50.10] [# 425621]

- Authentication Server Stickiness

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

  For example, assume that you have AAA configured on your ADC with three authentication policies--authpol1, authpol2, and authpol3--with priorities set to 10, 20, and 30 respectively. A user requests authentication, and the ADC discovers that the authentication server behind authpol1 does not respond to authentication requests. The ADC then tries authpol2, which responds. When other users attempt to authenticate after this situation occurs, the ADC skips authpol1 and proceeds directly to authpol2.

  [From Build 50.10] [# 358894]

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

  [From Build 54.9] [# 505673]

- SHA256 Signature and Digest Algorithms Support

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

  [From Build 56.22] [# 440382, 457134]

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

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

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

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

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

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

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

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

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

[From Build 50.10] [# 414985]

AppFlow

- Indication for End of Transaction

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

  [From Build 50.10] [# 252000]

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

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

  > add appflow action <name> -clientSideMeasurements ENABLED

  [From Build 50.10] [# 434577]

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

  [From Build 50.10] [# 423567]

Cisco RISE Integration

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

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

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

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

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

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

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

  [From Build 50.10] [# 413833]

Cluster

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

  > add cluster instance <clid> -quorumType None

  [From Build 50.10] [# 407139]

- Layer2 Mode Support in a Cluster

  You can now use the Layer2 mode in a NetScaler cluster.

  [From Build 50.10] [# 441320]

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

  [From Build 50.10] [# 407100]

- Link Redundancy Support in a Cluster

  The NetScaler cluster now provides link redundancy with LACP.

  [From Build 50.10] [# 415116]

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

  > add fis <name> -ownerNode <nodeId>

  Note:

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

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

  [From Build 50.10] [# 430035]

- Traffic domains are now supported on a NetScaler cluster.

  [From Build 50.10] [# 415065]

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

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

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

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

[From Build 50.10] [# 416827]

- MPTCP is now supported on a NetScaler cluster.

  [From Build 50.10] [# 423654]

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

  Note:

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

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

  [From Build 52.11] [# 486259]

- GSLB support in a Cluster

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

  [From Build 52.11] [# 326601]

Compression

- Specifying a Vary Header Value

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

  To specify the customized vary header globally:

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

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

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

[From Build 50.10] [# 346214]

Configuration Utility

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

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

- Distinguish between Commands Executed from Different NetScaler Interfaces

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

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

  [From Build 50.10] [# 361917]

Content Accelerator

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

  [From Build 50.10] [# 427565]

Content Switching

- Content Switching Support for Diameter

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

  [From Build 50.10] [# 413072]

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

  [From Build 50.10] [# 365650]

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

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

  [From Build 50.10] [# 386601]

- Multiple Port Content Switching Support for SSL_TCP Virtual Servers

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

  [From Build 50.10] [# 450367]

DNS

- Enabling or Disabling the Recursion Available Flag

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

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

- NAPTR DNS Record

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

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

  [From Build 50.10] [# 413773]

- CNAME Record Caching

  NetScaler ADC when deployed in a proxy mode does not always send the query for an address record to the back-end server. This happens when for an answer to a query for an address record, a partial CNAME chain is present in the cache. Under few conditions, ADC caches the partial CNAME record and serves the query from the cache.

  [From Build 50.10] [# 422509]

- AA bit set for response from NetScaler Cache

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

  [From Build 50.10] [# 285009]

DataStream

- Support for Database Specific Load Balancing for MySQL

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

  [From Build 50.10] [# 418490]

- Support for Fallback to NTLM Authentication

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

  [From Build 50.10] [# 382693]

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

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

  [From Build 50.10] [# 415485]

- Support for Transparent Deployment Mode in MySQL

You can now configure the NetScaler ADC to operate transparently between MySQL clients and servers, and to only log or analyze details of all client-server transactions. Transparent mode is designed so that the ADC only forwards MySQL requests to the server, and then relays the server's responses to the clients. As the requests and responses pass through the ADC, the ADC logs information gathered from them, as specified by the audit logging or AppFlow configuration, or collects statistics, as specified by the Action Analytics configuration. You do not have to add database users to the ADC.

[From Build 50.10] [# 410824]

- Any NetScaler VPX appliance subject to a limit on the number of DataStream transactions per second will no longer be restricted by license or platform model number.

  [From Build 52.11] [# 479490]

GSLB

- GSLB Auto Sync Enhanced to to Sync Static Proximity Database

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

  [From Build 50.10] [# 286236]

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

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

  [From Build 56.22] [# 343525]

Integrated Caching

- Increased Metadata Cache Capacity

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

  [From Build 50.10] [# 417677]

- Cache Object Persistence in a High Availability Setup

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

To enable this functionality globally, execute the following command:

> set cache parameter -enableHaObjPersist Yes

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

> set cache contentGroup <name> -persistHA Yes

[From Build 50.10] [# 329012]

Load Balancing

- Rate Limiting Support for Diameter

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

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

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

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

  [From Build 50.10] [# 399053]

- Increased Limits on the Number of Service Groups

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

  [From Build 50.10] [# 406355]

- Support for Jumbo Frames in RADIUS

  The NetScaler ADC now supports RADIUS jumbo frames.

  [From Build 50.10] [# 429415]

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

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

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

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

[From Build 50.10] [# 402361]

NITRO API

- Uploading and Retrieving Files for NetScaler Using NITRO

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

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

- Python SDK for NetScaler NITRO

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

  [From Build 50.10] [# 425725]

- Viewing the Statistics of Services and Service Groups that are Bound to a Load Balancing Virtual Server

  You can now view the statistics of services and service groups that are bound to a load balancing virtual server by using the following URL:

  http://<netscaler-ip-address>/nitro/v1/stat/lbvserver/<name>?statbindings=yes

  You cannot view these details by using the "http://<netscaler-ip-address>/nitro/v1/stat/lbvserver/<name>" URL which only gives the statistics of the load balancing virtual server.

  [From Build 58.11] [# 241950, 244603, 523907, 534804, 538057]

NetScaler Insight Center

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

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

  [From Build 50.10] [# 427187]

- Cache Redirection Insight Support

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

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

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

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

  [From Build 50.10] [# 409842]

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

  [From Build 50.10] [# 392016]

- Geo Map Support

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

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

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

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

  -Which region has the highest response time?

  -Which region is consuming the most bandwidth?

  [From Build 50.10] [# 322120]

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

  [From Build 50.10] [# 418196]

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

  [From Build 50.10] [# 423451]

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

  * 30 second data - Saves for 6 minutes

  * 5 minute data - Saves for 65 minutes

  * Hourly data - Saves for 25 hours

  * Daily data - Saves for 31 days

  [From Build 50.10] [# 404805]

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

  [From Build 50.10] [# 399329]

- HDX Insight Center reports now support the following metrics:

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

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

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

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

  [From Build 50.10] [# 424355]

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

  Client IP: IP address of the client

  Server IP: IP address of the server

  NetScaler IP: NetScaler IP address

  [From Build 50.10] [# 427504]

- Data Record Log Settings

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

[From Build 50.10] [# 421777]

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

  [From Build 50.10] [# 431957]

- Hop Diagram Support

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

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

  [From Build 50.10] [# 443824]

- EUEM Session Data on HDX Insight Reports

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

  [From Build 50.10] [# 367114]

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

  [From Build 50.10] [# 456295]

- Managing Session Timeout Period

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

  Enable this option while configuring user accounts or user groups.

  [From Build 50.10] [# 452424]

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

  [From Build 50.10] [# 414155]

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

[From Build 50.10] [# 463741]

- Exporting Reports

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

  [From Build 50.10] [# 320860]

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

  [From Build 50.10] [# 398322]

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

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

  [From Build 50.10] [# 474070]

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

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

  [From Build 50.10] [# 474067]

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

  [From Build 50.10] [# 471025]

- NetScaler Insight Center can now dynamically set the threshold value for the maximum number of hits on each URL.

  NetScaler Insight Center now facilitates efficient querying of its database.

  You can now enable NetScaler Insight Center to periodically remove the out-of-date content from its database.

  [From Build 50.10] [# 479004]

- Authentication and Authorization Support.

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

-Remote Authentication Dial In User Service (RADIUS)

-Terminal Access Controller Access-Control System (TACACS)

-Lightweight Directory Access Protocol (LDAP)

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

[From Build 50.10] [# 412466]

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

  [From Build 50.10] [# 378995]

- NetScaler Insight Center now displays reports for multi-stream ICA connections. All statistics that are maintained and reported for single-stream ICA connections are also displayed for multi-stream ICA connections.

  [From Build 52.11] [# 478744]

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

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

  [From Build 54.9] [# 522345]

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

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

  [From Build 54.9] [# 521503]

NetScaler VPX Appliance

- The NetScaler VPX appliance is now supported on VMware ESX server version 6.0.

  [From Build 59.13] [# 592395]

Networking

- Increased Number of Interfaces for Link Aggregation Channels

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

  [From Build 50.10] [# 437366, 389319]

- IPv6 Forwarding Session Rules

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

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

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

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

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

  [From Build 50.10] [# 251234]

- VMAC Based Traffic Domains

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

  [From Build 50.10] [# 425108]

- Support for VXLANs

  Now the NetScaler ADC supports Virtual eXtensiable Local Area Network (VXLANs). A VXLAN is an overlay solution that creates layer 2 overlay networks over layer 3 infrastructure by encapsulating Layer-2 frames in UDP packets. Each

VXLAN is identified by a unique 24-bit identifier called the VXLAN Network Identifier (VNI). Only network devices within the same VXLAN can communicate with each other.

[From Build 50.10] [# 366992]

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

  [From Build 50.10] [# 435000]

- ZebOS API Access

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

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

- Netprofile Support for Link Load Balancing Configurations

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

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

  [From Build 50.10] [# 356081]

- Support for Inter Traffic Domain Entity Bindings

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

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

  [From Build 50.10] [# 405295]

- Configuring Link Redundancy by using LACP channels

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

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

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

For example, set channel la/1 -lrMinThroughput 2000

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

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

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

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

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

[From Build 50.10] [# 346763]

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

  Source IP Persistency for RNAT Sessions

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

  Source IP Persistency for NetProfiles

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

[From Build 50.10] [# 437359]

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

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

  * Chassis ID

  * Port ID

  * Time-to-live value

  * System name

  * System description

  * Port description

  * System capabilities

  * Management address

  * Port VLAN ID

  * Link aggregation

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

  [From Build 50.10] [# 235640]

- vPath feature is available for all the NetScaler platforms from version 10.5 Build 52.11 onwards. To use this feature no special license file is required.

  [From Build 52.11] [# 416393]

Optimization

- Front End Optimization Support

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

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

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

Policies

- Variable Support for Policies

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

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

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

  Additionally, there are two variable types:

  - Singletons variables hold one ulong or text value.

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

  [From Build 50.10] [# 368447]

Responder

- The Responder feature now supports the Diameter protocol.

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

  [From Build 50.10] [# 318387]

- Embedded Expressions in Responder Responses

  You can now add Netscaler expressions with default syntax to HTML pages that are used with responder actions of the respondWithHtmlpage type. Any expression that is supported for use in a respondWith response can be used in a

respondWithHTMLPage response. To embed expressions in HTML pages simply surround the expressions with "${" and "}". This functionality enables you to include information about the request that generated the Responder action in the response.

[From Build 50.10] [# 423928]

Rewrite

- The Rewrite feature now supports the Diameter protocol.

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

  [From Build 50.10] [# 318382]

SSL

- SSL Renegotiation

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

  [From Build 50.10] [# 481577]

- Importing SSL Resources from Remote Hosts

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

  [From Build 50.10] [# 210405]

- Creating an SSL Profile

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

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

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

[From Build 50.10] [# 401011, 321967]

- SSL Certificate Chain

  As part of the SSL handshake, when a client requests a certificate, the NetScaler ADC presents a certificate and the chain of issuer certificates that are present on the ADC. An administrator can view the certificate chain for the certificates present on the ADC and install any missing certificates.

  [From Build 50.10] [# 437610]

- Support for Common Name Check during Server Authentication

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

  [From Build 50.10] [# 381821, 332628]

- Sending an SSLv2 Compliant Client Hello Message

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

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

- Support for DTLS Protocol

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

  [From Build 50.10] [# 400350]

- Setting the Limit for Disabled SSL Chips

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

  At the command prompt, type:

  > set ssl parameter -cryptodevDisableLimit <positive_integer>

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

[From Build 50.10] [# 376153]

- Support for TLS Protocol Version 1.1 and 1.2 on the NetScaler VPX Appliance

  The NetScaler VPX appliance now supports TLS protocol versions 1.1 and 1.2.

  [From Build 57.7] [# 424463, 481970]

- Stricter Control on Client Certificate Validation

  You can configure the SSL virtual server to accept only client certificates that are signed by a CA certificate bound to the virtual server. To do so, enable the ClientAuthUseBoundCAChain setting in the SSL profile bound to the virtual server.

  [From Build 57.7] [# 533241]

- Support for TLS_FALLBACK_SCSV signaling cipher suite value

  The NetScaler appliance now supports the TLS_FALLBACK_SCSV signaling cipher suite value. The presence of this SCSV extension in the Client Hello indicates that the client is retrying to connect to the server by using a lower SSL version, after its previous attempt to communicate with a higher version failed. Therefore, if the server finds this extension in Client Hello and also finds that the client is proposing a version that is lower than the maximum version supported by the server, it is a likely indication of a "man in the middle attack." The server drops these handshakes.

  [From Build 57.7] [# 509666]

System

- TCP Timestamp based on RFC 1323

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

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

- SNMP V3 Support for Traps

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

  [From Build 50.10] [# 416930]

- From NetScaler 10.5 onwards, if the MSS value of the bound TCP profile is 0, the MSS value is derived from the interface (and if applicable, VLAN) MTUs.

  [From Build 50.10] [# 422126, 425696]

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

  [From Build 50.10] [# 406270]

- SNMP Trap for Port Allocation Failures

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

  [From Build 50.10] [# 360334]

- Differentiated services code point (DSCP) Support

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

  [From Build 50.10] [# 436946]

- Explicit Congestion Notification (ECN)

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

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

  To enable ECN using the CLI:

  > add ns tcpProfile <name> -ecn ENABLED

  [From Build 50.10] [# 249145]

- Application Layer Protocol Negotiation (ALPN) Extension support

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

  [From Build 50.10] [# 430862]

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

  [From Build 50.10] [# 315474]

- MPTCP Enhancements

  The NetScaler now supports the following MPTCP enhancements:

  - One RTT subflow setup

  - Long-lived MPTCP sessions

  - MPTCP fast open

  [From Build 50.10] [# 435632]

- SPDY v3 Support

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

  [From Build 50.10] [# 329669]

- NetScaler support for D-SACK AND F-RTO

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

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

  To enable these settings by using the CLI:

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

  [From Build 50.10] [# 439129]

- Restrict Interface-level System Session Timeout

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

[From Build 50.10] [# 405501, 439031]

Traffic Domain

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

  client.traffic_domain.id

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

  [From Build 50.10] [# 403748]

- Features Supported in Traffic Domains

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

  * RNAT6

  * IPv4 and IPv6 Forwarding Sessions

  * NAT64

  * NAT46

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

  [From Build 50.10] [# 383056]

WIonNS

- 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

  [From Build 57.7] [# 508743]

Fixed Issues in Previous NetScaler 10.5 Releases

The issues that were addressed in NetScaler 10.5 releases prior to Build 65.11. The build number provided below the issue description indicates the build in which this issue was addressed.

AAA-TM

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

  [From Build 51.10] [# 483526]

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

  [From Build 52.11] [# 493308]

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

  [From Build 52.11] [# 476885]

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

  [From Build 52.11] [# 482174]

- 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.

  [From Build 52.11] [# 488015]

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

  [From Build 52.11] [# 484933]

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

[From Build 52.11] [# 480298]

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

  [From Build 52.11] [# 488077]

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

  [From Build 52.11] [# 474918, 502915]

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

  [From Build 53.9] [# 501565]

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

  [From Build 53.9] [# 505809, 507692]

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

  [From Build 53.9] [# 301241]

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

  [From Build 53.9] [# 501883]

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

  [From Build 53.9] [# 460680, 504703]

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

  [From Build 53.9] [# 505951]

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

[From Build 53.9] [# 446755, 468475]

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

  [From Build 54.9] [# 507386]

- The AAA-TM now support advanced expressions in SSO (single sign-on). The attribute values that are extracted as part of the authentication "http.req.user.attribute(1..16)" can now be used for setting the username and password credentials.

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

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

  [From Build 54.9] [# 512078]

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

  [From Build 54.9] [# 523158]

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

  [From Build 55.8] [# 517314]

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

  [From Build 55.8] [# 502710, 522858]

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

  [From Build 56.22] [# 530792]

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

  [From Build 56.22] [# 554849, 555618]

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

  > add tm trafficAction testAction1 -InitiateLogout ON

  > add tm trafficPolicy testPolicy1 <rule> testAction1

  [From Build 56.22] [# 527651]

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

  [From Build 56.22] [# 532861]

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

  [From Build 56.22] [# 532718]

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

  [From Build 56.22] [# 527131]

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

  [From Build 56.22] [# 532675]

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

  [From Build 57.7] [# 551205]

- During an upgrade from NetScaler 10.5 Build 54.x, or earlier releases, to Build 55.x, the NetScaler appliance becomes unavailable if the primary node of the HA pair has any active AAA-TM sessions.

  [From Build 57.7] [# 542327]

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

  [From Build 57.7] [# 547284, 533888]

- The NetScaler GUI does not show bindings for SAML policies.

  [From Build 57.7] [# 550885]

- The NetScaler appliance fails to respond if the SAML Identity Provider (IdP) sends an invalid SAML response with no data or invalid tags.

[From Build 58.11] [# 563983, 564310]

- If an organization has users and services in multiple domains, then when doing Kerberos Constrained Delegation, the NetScaler appliance might pick incorrect ticket when accessed in a particular order. This can result in users not being able to access the sites.

  [From Build 59.13] [# 575572, 589222]

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

  [From Build 59.13] [# 492626]

- The "show aaa session" command causes a high level of CPU usage when executed with the "-username" or "-group" option.

  [From Build 60.7] [# 577778, 595104, 595185]

- When a Kerberos ticket in a file (the AAA-TM system stores kerberos TGT in files) has expired, the NetScaler appliance updates the time offset in the request to KDC (Key Distribution Centre). This might cause Kerberos single sign-on to fail. You can remove the cached ticket files from the appliance.

  [From Build 60.7] [# 556464]

- When the NetScaler appliance is configured as SAML Service Provider (SP), the SAML Identity Provider (IdP) dishonors a logout request that is performed on the traffic management virtual server (load balancing or content switching) that uses a AAA-TM traffic policy.

  This happens because the NetScaler SP sends to the SAML IdP a SAML logoutRequest that contains "Conditions" XML tag.

  [From Build 61.11] [# 613700]

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

  [From Build 61.11] [# 540396]

- If the AAA virtual server is configured to an non-ActiveDirectory LDAP server, and an invalid password is used to logon, the NetScaler appliance becomes unresponsive.

  [From Build 62.9] [# 599264, 610045, 618322, 619123]

- When doing forms based SSO, if the backend server sets a cookie with the login form, NetScaler does not send those cookies to the client. This behavior was observed after a successful forms SSO attempt. This applies to forms based SSO access in AAA-TM products.

  [From Build 62.9] [# 624165]

- When using AAA-TM on a plain HTTP virtual server with no endpoint features enabled, the NetScaler appliance might acknowledge less data than the client has sent. That might cause some elements of pages to load incompletely, or time out.

  [From Build 62.9] [# 615885]

- If AAA-TM logout is configured through a traffic policy on the Netscaler appliance, and the server sends a chunked response, the user encounters an error.

  [From Build 62.9] [# 623005]

- In a multi-core NetScaler environment, user sessions sometimes do not get terminated if the decision to terminate is based on a force timeout value that is configured on a TM traffic action.

  [From Build 62.9] [# 610604, 618760, 623053]

- If SAML authentication is used to log on a user, and the SAML action is removed while there are active sessions, addition of a high availability node might cause occasional failures on the secondary node.

  [From Build 63.8] [# 621787]

- If you use the Kerberos protocol for single sign-on (SSO) to access a back-end server, the NetScaler appliance might fail if heavy traffic causes allocation failures, because the appliance might detect a call to free memory that has already been freed.

  [From Build 63.8] [# 637125]

- The NetScaler appliance fails if authentication is disabled while user authentication is in progress.

  [From Build 64.9] [# 617370]

Acceleration

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

  [From Build 58.11] [# 535130]

Action Analytics

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

  Examples:

  http://10.217.6.239/TesT/

  http://10.217.6.239/TEST/

http://10.217.6.239/TEsT/

http://10.217.6.239/TeST/

Note post fix:

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

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

add stream selector sel1 HTTP.REQ.hostname.to_lower

[From Build 53.9] [# 406457]

- A global flag that tracks stream sessions when the ICMP traffic processing begins is not initiated properly.

  [From Build 61.11] [# 595915, 602701]

Admin Partitions

- If you remove an admin partition, the NetScaler appliance fails or corrupts an SNMPD packet queue.

  [From Build 63.8] [# 618251]

AppExpert

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

  [From Build 55.8] [# 524252]

- The order in which AppExpert evaluates application units cannot be changed. With this fix, the NetScaler GUI displays a burger icon for each application unit. After hovering over the icon, you can move an application unit up or down in the order of evaluation.

  Navigation: Configuration > AppExpert > Application > Application Unit section

  [From Build 61.11] [# 567425]

AppFlow

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

  [From Build 53.9] [# 499172, 501216]

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

  [From Build 55.8] [# 472971]

- If a NetScaler failover occurs when ICA AppFlow is enabled, the Citrix Receiver reconnect fails because the Citrix Receiver does not support Automatic Client Reconnect (ACR) feature.

  [From Build 55.8] [# 522315, 522265]

- NetScaler Insight Center displays the WAN latency and DC latency values to be higher than the ICA RTT value.

  [From Build 56.22] [# 539118, 542627, 547563, 554799, 557958]

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

  [From Build 56.22] [# 365404]

- NetScaler Insight Center displays the WAN latency and DC latency values to be higher than the ICA RTT value.

  [From Build 58.11] [# 539118, 542627, 547563, 554799, 557958]

- Applications might fail to launch through a MAC Receiver if:

  -You enable data collection for LAN user mode by configuring a cache redirection virtual server of type HDX.

  -You configure global ICA ports.

  [From Build 58.11] [# 532714, 566994]

- The NetScaler appliance can become unavailable if there is a connection disruption and if the NetScaler is configured to generate AppFlow reports for ICA sessions, and the ICA session reconnects using Session Reliability.

  [From Build 58.11] [# 558848, 559231, 571878]

- AppFlow should not export the records for internal connections, like the Kernel RPC. When it attempts to export records for such an internal connection, it leads to AppFlow failure.

  [From Build 58.11] [# 547892, 531101]

- The NetScaler appliance does not perform policy evaluation for traffic other than related to SSL and Load balancing configurations. As a result, the appliance does not create AppFlow records for these traffic.

  [From Build 59.13] [# 552655, 563387]

- When routes are updated after an AppFlow collector is added, the NetScaler appliance sends ARP requests for the AppFlow collector IP address, even when the collector is reachable only through a router.

  [From Build 59.13] [# 574420]

- The NetScaler appliance might become unresponsive if you attempt to delete an AppFlow action while the traffic is flowing.

[From Build 61.11] [# 585914, 613238]

- The NetScaler appliance might become unresponsive if a request generated by a client is corrupted after execution of the client-side measurement script. This issue can occur if you enable the client side measurement option for an AppFlow action.

  [From Build 61.11] [# 601915, 601924, 607217]]

AppFlow Insight

- In cases where NetScaler generates an ACK packet, RTT calculation should be skipped because ACK is not coming from an external entity. This leads to NetScaler failure.

  [From Build 58.11] [# 571035, 573360, 576786]

Application Firewall

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

  [From Build 51.10] [# 486231]

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

  [From Build 51.10] [# 478109, 484323]

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

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

- If the application firewall receives a multipart POST request with a Content-Type header that contains a charset, it blocks that request as malformed.

  [From Build 52.11] [# 464641]

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

  [From Build 52.11] [# 459031, 463351]

- If a response contains href links that include query parameters, the NetScaler application firewall triggers false positives for CSRF and form field consistency violations if these links are accessed. With this fix, if CSRF or Field

Consistency checks are enabled, the URLs in the hrefs are added to the URL Closure table even if startURL Closure is not enabled.

[From Build 53.9] [# 488369]

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

  [From Build 53.9] [# 505272, 505039]

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

  [From Build 53.9] [# 481899]

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

  [From Build 53.9] [# 423150]

- Signature Bindings Not Shown in PCI-DSS Report

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

  [From Build 53.9] [# 443673]

- If a NetScaler ADC receives a request for an object that it cached before the application firewall configuration was modified to add any advanced security check protection, the ADC responds with HTTP Error 503 for subsequent requests to access this cached object, because the object does not contain the expected application firewall metadata. With this fix, the existing cached objects without the required metadata are considered stale and are flushed. The request is served from the origin server and the cache is updated with refreshed data.

  [From Build 53.9] [# 473322, 466491]

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

  [From Build 53.9] [# 476206]

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

[From Build 54.9] [# 315183]

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

  [From Build 54.9] [# 446134, 483207]

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

  [From Build 54.9] [# 511657, 512129]

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

  [From Build 55.8] [# 522720]

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

  [From Build 56.22] [# 537910]

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

  [From Build 56.22] [# 528170]

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

  [From Build 56.22] [# 539766, 546424, 548286]

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

  [From Build 56.22] [# 517750, 530793]

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

  [From Build 56.22] [# 452012]

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

  [From Build 57.7] [# 539777]

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

  [From Build 57.7] [# 532338, 526029, 539487]

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

  [From Build 57.7] [# 528902, 558724]

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

  [From Build 57.7] [# 549466]

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

  [From Build 58.11] [# 551621, 549232]

- When any form protection check is enabled and the default request content-type parameter of the application firewall profile is not configured, an incoming request without a content-type header is treated as a form, even if it is not a form. The transfer-encoding header gets deleted, and a content-length header gets added, but the request is forwarded to the server as a chunked request. The server is unable to process the chunked data and determines it to be a bad request. With this fix, the form analysis is carried out only when "multipart/form-data", or "application/x-www-form-urlencoded" content type is either specified in the request or set as the default request content type in the profile that is applied when the content-type is not specified in the request.

  [From Build 58.11] [# 559348]

- If a large number of long standing sessions expire and are freed during application firewall processing, a tight-loop condition might occur, causing the NetScaler appliance to fail.

  [From Build 58.11] [# 550657]

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

  [From Build 58.11] [# 539487, 526029, 547104]

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

  [From Build 58.11] [# 548577]

- The application firewall recommended learned rules for the Start URL security check do not contain the ^ in the beginning and the $ at the end of the URL.

  [From Build 58.11] [# 556847]

- During binding a signature to an application firewall profile, the NetScaler appliance might fail when it is under memory pressure.

  [From Build 58.11] [# 559060]

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

  [From Build 59.13] [# 549255]

- When a user attempts to upload a file to a server that is protected by the application firewall, the file upload fails. The underlying cause is that the application firewall included an invalid character in the MIME boundary when encoding the file.

  [From Build 59.13] [# 472476, 418036]

- During operations that require a large amount of memory, the NetScaler application firewall might not be able to allocate memory for active transactions. The NetScaler appliance might fail under such conditions.

  [From Build 59.13] [# 513506, 574322]

- During an application firewall security check inspection, a compressed response from the server might trigger a violation if the XML format check is enabled. With this fix, the Accept-Encoding request header is removed when the XML protections are enabled. If content compression is enabled on the server, the XML check inspection is bypassed when the server sends a compressed response.

[From Build 59.13] [# 580273]

- The Citrix application firewall silently resets the connection when it receives a malformed or invalid request. With this fix, the application firewall logs such events.

  [From Build 59.13] [# 577742]

- During application firewall processing, if the length of the pattern in the signature rule is longer than the payload text string currently being searched for a pattern match, the NetScaler appliance might fail. With this fix, application firewall skips such a rule and moves on to process the next signature rule.

  [From Build 59.13] [# 570830, 528946]

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

  [From Build 59.13] [# 549954]

- When an HTTPS virtual server is processing the traffic, the violation logs that the application firewall generates for a blocked malformed request might show the wrong IP address, and the transaction ID might be shown as zero.

  [From Build 59.13] [# 500933]

- The application firewall allows you to configure Credit Card security check by offering a set of check boxes to select the credit card(s) to protect. In the 10.5 release, the configuration utility offers this option when you navigate to the profile's relaxation rule section and select the credit card entry in the displayed table. This functionality is missing in the 58.11 build. With this fix, the option to configure Protected Credit cards has been relocated. From build 59.x onwards, you can navigate to the Advanced Settings pane of the target profile and double click Credit Card, or select the row and click Action Settings to display the Protected Credit Card check boxes .

  [From Build 59.13] [# 586016]

- An attempt to make a copy of the application firewall default signature object might fail in some appliances if there is insufficient space in the /tmp (on MFS, ram disk) folder. With this fix, the intermediary files that are created during the import operation to make a copy of the default signature object are now written in the /var/tmp (on HDD/SSD) that has more space.

  [From Build 59.13] [# 583298]

- The NetScaler appliance might fail when the application firewall is processing the cookie header(s) in an HTTP request. This occurs when the cookie transform action is enabled and all other security checks that apply to establishing a user session are disabled.

  [From Build 60.7] [# 597440]

- An attempt to make a copy of the application firewall default signature object might fail in some appliances if there is insufficient space in the /tmp (on MFS, ram disk) folder. With this fix, the intermediary files that are created during the import operation to make a copy of the default signature object are now written in the /var/tmp (on HDD/SSD) that has more space.

  [From Build 60.7] [# 583298]

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

  [From Build 61.11] [# 372768]

- The StarURL Relaxation rule might not work if the regular expression contains two sets of groups (). The following example shows a relaxation rule with two groups, (nstimmy.deva|abcd) and (login|enter|logout). The PI engine is not able to parse such Regular Expressions.

  Example: ^https://(nstimmy.deva|abcd)\.citrite\.net/admin/(login|enter|logout)/$

  [From Build 61.11] [# 578333]

- The application firewall uses a cached PCB pointer to retrieve connection information during asynchronous DHT operation. In a corner case scenario, this stale PCB gets freed which might cause the NetScaler appliance to fail.

  [From Build 61.11] [# 589321, 603432]

- Application firewall profiles that are exported and archived from one build cannot be restored to a system running a different build, because changes introduced in the newer releases can lead to compatibility issues. With this fix, the application firewall now logs an error message, in ns.log, if you attempt to restore an archived profile to a different build than the one from which it was exported.

  [From Build 61.11] [# 601064]

- The application firewall might experience a transient low-memory condition during a traffic surge if advanced security check protections (such as Form Field consistency, CSRF, form tagging and so on, which require rewriting the HTML forms in the response) are enabled for the profiles. This might result in a memory leak, and memory allocation failures might occur even after the traffic surge subsides.

  [From Build 61.11] [# 598776, 597952]

- When a new node is added to cluster, the configuration might get pushed to the new node before the imported objects are synced. As a result, the profile configuration might be lost if the profile has signature or other import object bindings. With this fix, a file sync is triggered to pull all the files from the CCO node to all the new nodes of the cluster before the configuration commands are pushed to new node.

  [From Build 61.11] [# 537375, 611422]

- With application firewall enabled, the presence of stale debug printf statements leads to an increase in the latency and CPU usage.

[From Build 61.11] [# 598829, 621260]

- Starturl relaxations might not work if regex expressions use grouping for matching multiple terms. The URL might not get matched against all the terms in the group.

  [From Build 62.9] [# 628789]

- If a client submits a form that includes a field named "as_fid", and the application-firewall profile has signatures enabled, the signatures might block form submissions from that client.

  [From Build 62.9] [# 628525]

- When the application firewall signature has upper case or mixed case characters in the name, the configured profile bindings for such a signature are not displayed in the signatures pane in the configuration utility.

  [From Build 62.9] [# 561845, 620915]

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

  [From Build 62.9] [# 547978]

- If learning thresholds for the application firewall security checks are set to a value greater than 1, the configuration utility displays the following error message when you try to access the learned data: "communication error with aslearn."

  [From Build 62.9] [# 622678]

- Application Firewall memory allocation errors might occur if the license on the NetScaler appliance restricts the number of packet engines.

  [From Build 62.9] [# 621798]

- When you use the NetScaler GUI to perform the Skip operation, the application firewall learned rules might not be deleted. This occurs because NITRO is sending wrong "Location" ("Field") data to the GUI. With this fix, the GUI converts "Field" into "FORMFIELD," and the Skip operation removes the skipped rules, as expected.

  [From Build 62.9] [# 603473]

- The import command to import an application firewall profile does not work, when the NetScaler appliance is deployed in a high availability set-up.

  [From Build 62.9] [# 560676]

- If you use the Mozilla Firefox browser to access the NetScaler GUI, you cannot make changes to the application firewall configuration.

  [From Build 62.9] [# 619978]

- In NetScaler web application firewall high availability deployments, application firewall sessions are not cleaned up on the secondary node. As a result, memory usage increases on the secondary node.

  [From Build 62.9] [# 612284, 619056]

- The NetScaler appliance might fail when application firewall is attempting to log messages regarding the user's session but the source string is NULL due to memory corruption.

  [From Build 63.8] [# 635738]

- The application firewall allows configuring default field format parameters. The valid range for the maximum field format length is 1-65535. The GUI as well as CLI currently accepts zero as input even though zero is outside the allowed range.

  [From Build 64.9] [# 608010, 603763, 629859]

- Under high memory utilization, the NetScaler appliance fails if you try to bind trusted learning clients to an application firewall profile. The following command might not work if the appliance is running low on memory.

  bind appfw profile <profile_name> - trustedLearningClients

  [From Build 64.9] [# 657009]

- A NetScaler appliance fails under the following set of conditions:

  - The appliance is configured to log for parsing errors in XML responses, and the configuration includes a confidential field. Webform fields can be designated as confidential fields to protect the information that users type into them.

  - The appliance receives a request in which query parameters are set.

  - A parsing error occurs during processing of the XML response.

  [From Build 64.9] [# 658561, 639647]

- If memory corruption results in a NULL source string, the NetScaler appliance might fail if the application firewall attempts to log messages about the user's session.

  [From Build 64.9] [# 635738]

- If a user-created signature name includes a space, the application firewall profile bound to the signature is not saved in the configuration after you upgrade to release 10.5 build 63.8.

  [From Build 64.9] [# 647080]

- A NetScaler AppFirewall appliance might run out of memory, because firewall sessions might not get cleaned up in a high availability environment if sync or propagation is disabled or the software versions running on a pair of nodes do not match. This is due to DHT not being able to clean up entries properly.

  [From Build 64.9] [# 646293, 645547, 658502]

- The NetScaler appliance fails if the signature match function accesses invalid memory while matching signature rules.

  [From Build 64.9] [# 643854]

- Applications might not load properly when the memory_max_allowed value for the AppFW pool is low. This low memory condition can also cause memory allocation errors that result in numerous connection resets.

  [From Build 64.9] [# 649031, 651536]

- The name of a user defined signature object must not contain a hash-mark character (#), but the feedback message lists it as an allowed character.

  [From Build 64.9] [# 648010]

- If the HTML response page contains a pair of hyphens (--) in the comment tag, the NetScaler appliance might parse the response page incorrectly. This could result in a violation.

  [From Build 64.9] [# 648104]

- When an application firewall signature object from an earlier release is imported to the NetScaler appliance using the CLI, it might not display the version of the existing *Default signature object. It might display an older version, even though during the import, the version gets updated to the same version as the version of the existing *Default signature object. However, if the same object is imported using GUI, the version reflects the version of the *Default signature object. This is a display issue and is only observed when CLI is used to import an object.

  [From Build 64.9] [# 614173]

Cache Redirection

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

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

  [From Build 53.9] [# 497866, 502366]

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

  [From Build 53.9] [# 502366, 505091]

- 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)"

[From Build 55.8] [# 509690]

- In a fully transparent CR deployment if a client sends two HTTP GET requests for the same connection, the first connection to the CACHE is closed when the second GET request is received. This happens because a specific flag is set to open new connection which forwards the second GET request to the cache. Since the first connection for the same 4 tuple is still open, NetScaler sends a reset signal.

  Fix: Do not set the flag to initiate the connection for the second GET request, since the previous connection already exists.

  [From Build 58.11] [# 541395]

- The Cache Redirection configuration is deleted when the NetScaler appliance is rebooted.

  [From Build 60.7] [# 432311, 582383]

Cluster

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

  [From Build 54.9] [# 517663]

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

  [From Build 56.22] [# 522245]

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

  [From Build 56.22] [# 539657]

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

  [From Build 56.22] [# 543117, 511764, 544264]

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

  [From Build 56.22] [# 519327, 542633]

- On a low bandwidth system, you get the following message when running the showtechsupport feature with the scope configured for the cluster:

  "This is a low bandwidth instance. Showtechsupport cannot be run with scope cluster. Please execute showtechsupport on each node."

  [From Build 59.13] [# 543558]

- In a cluster setup, HTTP profile configurations are lost when a cluster node is rebooted.

  [From Build 59.13] [# 570877]

- During an upgrade from a NetScaler 10.1 build to a NetScaler 10.5 build, running the "show audit messages" command can cause the NetScaler appliance to fail.

  [From Build 60.7] [# 546038]

- A NetScaler cluster does not respond to cURL HTTP requests from outside the datacenter, because the Path MTU Discovery (PMTUD) mode gets disabled when a cluster is created.

  [From Build 61.11] [# 541223]

- Important! Every NetScaler command is internally assigned a unique ID.

  For some commands like 'add cs policy' and 'add server', the unique ID generated on the cluster configuration coordinator (CCO) already exists for another command of same type in a non-CCO node. Therefore, the command execution on the non-CCO node fails.

  [From Build 62.9] [# 614718, 615459]

- The VRRP Feature does not work in a cluster setup that includes a node with a node ID of zero (0).

  [From Build 62.9] [# 618663]

- If a load balancing server is trying to synchronize its states, occasionally one or more cluster nodes might get stuck in a Service state. As a result, the other nodes in the cluster might be unavailable, which leads to an improper cluster formation.

  [From Build 64.9] [# 651828]

Command Line Interface

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

  [From Build 51.10] [# 488781]

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

  [From Build 52.11] [# 480639]

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

  [From Build 54.9] [# 503214]

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

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

  bind policy patset ps_adi_any_robots_deny -uat -index 1

  [From Build 56.22] [# 508618, 508815]

- Superusers, besides nsroot are not allowed to redirect the shell output from the NetScaler CLI. This issue is now fixed.

  [From Build 57.7] [# 543702]

- A customized CLI prompt is not persisted after rebooting the appliance.

  [From Build 60.7] [# 583625]

- The NetScaler CLI exhibits the following issues on running the "show" and "stat" commands on a service group.

  - When using the "show servicegroup -includeMembers" command: This command lists only one service per service group, although more than 1 service are bound to the service group(s).

  - When using the "stat servicegroupMember <ServiceGroupName> <Service-IP-address> <port>" command: This command does not work if you specify the <Service-IP-address>. Instead, you must specify the <Service-Name>.

  [From Build 63.8] [# 554652, 596571]

Configuration Utility

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

  [From Build 51.10] [# 491215]

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

  [From Build 51.10] [# 484583]

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

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

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

  [From Build 51.10] [# 482135]

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

[From Build 51.10] [# 482609, 485852]

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

  [From Build 52.11] [# 441408]

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

  [From Build 52.11] [# 499592]

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

  [From Build 52.11] [# 493946]

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

  [From Build 52.11] [# 460020]

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

  [From Build 52.11] [# 451546]

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

  [From Build 52.11] [# 494915]

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

  [From Build 52.11] [# 490142]

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

  [From Build 53.9] [# 483442]

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

  [From Build 53.9] [# 456428]

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

[From Build 53.9] [# 490142]

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

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

  [From Build 54.9] [# 517146, 513730]

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

  [From Build 54.9] [# 514538, 513837]

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

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

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

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

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

  [From Build 54.9] [# 485539, 502285]

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

  * HTTP Status Code

  * Ignore Marker Objects

  * Include-Not Ready Object

  [From Build 54.9] [# 447915]

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

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

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

  [From Build 54.9] [# 496336]

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

  [From Build 54.9] [# 503590]

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

  [From Build 55.8] [# 353015]

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

  [From Build 55.8] [# 524123, 521279]

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

  [From Build 55.8] [# 517606, 518444]

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

  [From Build 55.8] [# 503589]

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

  [From Build 56.22] [# 533255]

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

  [From Build 56.22] [# 530025]

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

  [From Build 56.22] [# 542557, 542644, 544420, 547508]

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

  [From Build 56.22] [# 544588, 557380]

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

  [From Build 56.22] [# 505536]

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

  [From Build 57.7] [# 547877]

- On the Configuration Utility, the Downloads page does not have the Gadgets option anymore.

  [From Build 57.7] [# 544420]

- The user expression and password expression fields of a TM traffic action cannot be configured through the configuration utility.

  [From Build 57.7] [# 489894]

- The Create Rewrite Action screen (AppExpert> Rewrite> Actions> Add) does not list the correct descriptions for some Action Types.

  [From Build 57.7] [# 553583]

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

  [From Build 58.11] [# 454246, 478532, 500166]

- If you create an SSL RSA key by using the NetScaler configuration utility, the default public exponent value incorrectly appears as 3.

  [From Build 58.11] [# 561151]

- The system backup and restore functionality is not available on the Cisco NetScaler GUI.

  [From Build 58.11] [# 553373]

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

  [From Build 58.11] [# 558656]

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

  [From Build 58.11] [# 558893]

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

  [From Build 59.13] [# 557379]

- An issue with the file download manager handler had with large files has been fixed.

  [From Build 59.13] [# 586879]

  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.

  [From Build 60.7] [# 494804]

- The connection to the appliance might be lost while generating the support file.

  [From Build 60.7] [# 531628, 543400, 567392, 585451]

- If you are using the configuration utility to run diagnostics on the NetScaler appliance, you cannot specify a traffic domain.

  [From Build 61.11] [# 609334]

- You cannot add user-defined values for the user name and group name fields on the Authentication CERT Profile page.

  With this fix, you can specify a user-defined value by navigating to Security > AAA - Application Traffic > Policies > Authentication > Basic Policies > CERT > Profiles and selecting New in the User Name Field list and the Group Name Field list.

  [From Build 61.11] [# 597708]

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

  [From Build 63.8] [# 557379, 585649, 609615, 617161, 646039]

Content Optimization

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

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

Content Switching

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

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

[From Build 54.9] [# 501856]

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

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

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

  3. Save the configuration and restart the appliance.

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

- If you bind a policy to a content switching virtual server, the ?-invoke policylabel? option is automatically appended to the bind command. This might cause a loss in the configuration after the appliance is restarted.

  [From Build 58.11] [# 547174]

- If you use the configuration utility to edit a URL-based content switching policy that is bound to a content switching virtual server, an error message appears, stating that the binding already exists. You must first unbind the policy from the virtual server, and then edit it while rebinding it to the same virtual server.

  [From Build 58.11] [# 555497]

- If a large number of content switching policies are bound to a content switching virtual server, using the configuration utility to bind a new policy without explicitly assigning a priority might result in the policy being assigned the priority of the first policy on the next page of the display. Since a policy is already assigned that priority, an error message stating that the priority is already used appears.

  [From Build 61.11] [# 601203]

- 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.

  [From Build 62.9] [# 522510, 528782, 538223, 552913, 602829]

DNS

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

  [From Build 51.10] [# 462862]

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

  [From Build 52.11] [# 437529]

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

  [From Build 52.11] [# 471707]

- If a server sends a NODATA response that has CNAME record in the answer section and no records in the authoritative and additional sections, the response is marked for CNAME caching on the NetScaler ADC, because it is incorrectly assumed to be a referral response. As a result, the ADC sends a blank response to subsequent queries, of any query type, for the canonical name.

  [From Build 52.11] [# 477552]

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

  [From Build 53.9] [# 484069]

- 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.

  [From Build 53.9] [# 382478]

- Non-standard query packets are altered before they are forwarded to back-end servers, which causes the server to respond with a "FORMAT error" message.

  [From Build 59.13] [# 559064]

- If caching is enabled, records present in the additional and authoritative section of a response are cached. If a request for the same records is answered by DNS cache, the Authoritative Answer (AA) bit is not set in the response but if the request for the same records is answered by querying the back-end server then the AA bit is set in the response.

  [From Build 59.13] [# 543222, 257952]

- If, while a DNS-TCP client request is in surge queue, the NetScaler appliance receives a FIN from the client and responds with a FIN or ACK before the queued request is forwarded to the backend server, the appliance might fail.

  [From Build 60.7] [# 581723]

- 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.

  [From Build 60.7] [# 382478]

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

  [From Build 61.11] [# 512372]

- If a NetScaler appliance in DNS resolver mode is configured to resolve queries with suffixes, the appliance fails if there is no address record for the NS record associated with one of the suffixes.

  [From Build 61.11] [# 605861]

DataStream

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

  [From Build 54.9] [# 507709]

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

  [From Build 54.9] [# 510805, 516687]

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

  - The appliance is configured in transparent mode.

  - The appliance performs Windows authentication for MSSQL requests.

  [From Build 56.22] [# 539922]

- A NetScaler client becomes unresponsive if:

  1. The NetScaler appliance receives the complete response to the client's query from the server.

  2. At the same time, the client sends an attention packet to the appliance.

  The client becomes unresponsive because the appliance closes the server-side connection but does not send the client a response to the attention packet.

  [From Build 62.9] [# 560401]

- If the NetScaler appliance receives a prelogin message request from a Visual Studio 2015 client, it sends an incorrect response. As a result, the client becomes unresponsive.

  [From Build 62.9] [# 613239, 616404]

- Front End Optimization

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

  [From Build 55.8] [# 529329]

GSLB

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

[From Build 51.10] [# 488161]

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

  [From Build 52.11] [# 453144, 455417]

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

  [From Build 53.9] [# 485811]

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

  [From Build 53.9] [# 496676]

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

  [From Build 54.9] [# 497412]

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

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

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

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

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

  -Last State Change

  -Time since last state change

  -Client and Server idle timeout

  [From Build 55.8] [# 498854]

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

  [From Build 55.8] [# 511878]

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

  [From Build 55.8] [# 517961]

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

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

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

  [From Build 56.22] [# 497338, 516259, 522602, 548845]

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

  [From Build 56.22] [# 528060]

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

  [From Build 56.22] [# 519589]

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

  [From Build 56.22] [# 531553]

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

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

  [From Build 58.11] [# 550294]

- If you have configured the canonical name as the GSLB domain in NetScaler appliance, when the backend server returns the CNAME record without the requested record, NetScaler appliance changes the TTL value of the GSLB domain with the TTL value of the CNAME record.

  [From Build 59.13] [# 582925]

- GSLB virtual server configured with Dynamic Proximity as LB method fails.

  [From Build 59.13] [# 578969]

- If a server entity (for example, a server IP address or server name) is associated with both a GSLB entity and a non-GSLB entity on a GSLB site, and the GSLB configuration is synced to another site that does not include this server entity, the synchronization removes the server entity and all other entities associated with that server.

  [From Build 61.11] [# 590336]

- In the GUI, on the GSLB statistics page, the local site MEP state is always displayed as DOWN instead of as a blank field.

  [From Build 62.9] [# 617267]

- The NetScaler appliance fails if you run the "show gslb domain" command on a non-gslb domain record.

  [From Build 62.9] [# 618789]

- When the MEP connection between two GSLB sites is reestablished after going down, the connection becomes active immediately, but the NetScaler GUI and CLI do not show it as UP for about 9 seconds.

  [From Build 62.9] [# 615886]

- In a GSLB deployment, if monitors are bound to GSLB services and the trigger monitor is set to MEP_DOWN. The remote GSLB services are incorrectly marked as down when MEP goes down due to temporary network outage but the MEP connection is still active.

  [From Build 63.8] [# 610065]

- The GSLB synchronization command sync gslb config displays incorrect information when used with the -preview argument.

  [From Build 63.8] [# 537944]

Graphical User Interface

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

  [From Build 54.9] [# 502309, 503357]

HTML Injection

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

  [From Build 55.8] [# 518072, 518272]

High Availability

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

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

- Modes: L3 and Edge

[From Build 54.9] [# 512034, 516783]

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

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

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

  [From Build 56.22] [# 521424]

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

  [From Build 56.22] [# 524146, 526699]

- 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.

  [From Build 57.7] [# 537496]

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

  [From Build 57.7] [# 534795]

- 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.

  [From Build 58.11] [# 479666, 507519, 541503]

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

  [From Build 58.11] [# 546938, 470980]

- When there is a HA issue, the synchronization of persistence sessions between the primary and secondary appliances can fail. This can cause some of the persistence sessions not being replicated on the secondary appliance.

  [From Build 59.13] [# 580703, 579037, 595491, 595506, 596002, 596215, 604164, 605112]

- The HA traffic between the HA pair is abnormally high. This issue is caused by a loop that repeatedly tries to push the same sessions to the secondary appliance after failover.

  [From Build 59.13] [# 560640, 566710, 576012, 576096, 579037, 582354, 590730]

- When there is a HA issue, the synchronization of persistence sessions between the primary and secondary appliances can fail. This can cause some of the persistence sessions not being replicated on the secondary appliance.

  [From Build 60.7] [# 580703, 579037, 595491, 595506, 596002, 596215, 599396, 604164, 605112]

Integrated Caching

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

  [From Build 51.10] [# 488145]

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

  [From Build 52.11] [# 494910, 497793]

- In an HA setup, if the integrated caching (IC) feature is not licensed, the IC configurations are not stored on the secondary appliance even though they are available on the primary appliance. With this fix, the IC configurations are also available on the secondary appliance.

  [From Build 58.11] [# 556437]

- 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.

  [From Build 60.7] [# 486535]

- When a flash cache is in use with HTTPS traffic, only the initial client request is serviced. Subsequent client requests fail.

  [From Build 61.11] [# 602984]

- The NetScaler GUI does not reflect the correct count of cached objects whereas this number is shown correctly through the CLI.

  [From Build 61.11] [# 607622, 608517]

- The NetScaler can stop responding when cache object persistency is configured in a HA setup.

  [From Build 61.11] [# 589322]

- If you set the PINNED option for a cache content group, caching continues in this group even if the group uses more than its allocated memory, until the integrated caching memory is exhausted. Because cached objects in these groups cannot be removed until the appliance is restarted, there might be a situation in which no more objects can be cached and the appliance resets the connections of clients who send additional requests.

  [From Build 62.9] [# 621356, 631356]

- The NetScaler appliance caches objects if front-end optimization (FEO) feature is enabled but the integrated caching feature is disabled.

  [From Build 63.8] [# 619578]

Load Balancing

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

  - a large number of SIP messages are received.

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

  [From Build 51.10] [# 484547]

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

  [From Build 51.10] [# 488007, 487724]

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

  [From Build 52.11] [# 482113]

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

  [From Build 52.11] [# 489197]

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

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

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

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

  [From Build 53.9] [# 457639]

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

  [From Build 53.9] [# 502338]

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

  [From Build 53.9] [# 504209]

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

  [From Build 54.9] [# 497470]

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

  [From Build 54.9] [# 505543]

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

  [From Build 54.9] [# 460040]

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

  At the NetScaler command prompt, type:

  set lb parameter -useSecuredPersistenceCookie Enabled-cookiePassphrase test

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

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

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

  [From Build 55.8] [# 519644]

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

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

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

  [From Build 55.8] [# 516615]

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

  [From Build 55.8] [# 443027]

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

  [From Build 56.22] [# 523239]

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

  [From Build 56.22] [# 528070]

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

  [From Build 56.22] [# 488011]

- IPv6 Support for HTTP based User Monitors

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

  - StoreFront (SF)

  - AppController (APPC)

  - Web Interface Extended (WI)

  - NT LAN Manager (NTLM)

  [From Build 57.7] [# 510111]

- The output of the "show lb vserver -format text" command shows parameters even that are not applicable for a virtual server type.

  [From Build 58.11] [# 550177]

- 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.

  [From Build 58.11] [# 524079, 559022]

- In a high availability setup, if custom cookie persistence is configured on a virtual server, part of the secondary node's configuration might not be synchronized with the primary after a failover occurs.

  [From Build 58.11] [# 552799, 552607]

- IPv6 Support for HTTP based User Monitors

  You can now use IPv6 addresses in the following monitors:

  - USER

  - SMTP

  - NNTP

  - LDAP

  - SNMP

  - POP3

  - FTP_EXTENDED

  - STOREFRONT

  - APPC

  - CITRIX_WI_EXTENDED

  Note: The monitor for MySQL does not support IPv6 addresses.

  [From Build 58.11] [# 510111]

- If an SSL monitor is bound to a domain-based service that is configured with non-default SSL settings, the monitor might not show the service as UP.

  [From Build 59.13] [# 575171, 576012]

- In a RADIUS load balancing setup, if Use Source IP (USIP) is configured on the RADIUS services, the server side connections are not reused, and requests are dropped.

  [From Build 59.13] [# 574120, 534888]

- In a load balancing group configuration, the "sh run" command sometimes runs in a loop, which exponentially increases the size of the temporary configuration file. As a result, saving the configuration and synchronizing the nodes in a high availability setup might fail.

  [From Build 59.13] [# 587812, 598499, 601918]

- In a load balancing group configuration, the NetScaler appliance might fail while synchronizing the statistics.

  [From Build 59.13] [# 557940, 574551]

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

  [From Build 59.13] [# 466094, 534755]

- If the "Invalid argument error" message appears intermittently in nsmund.log, treat it as a false positive. The error appears because a scenario was not handled correctly. However, if this message appears in the log every time a particular script runs, there is an issue with the arguments that are passed to the script.

  [From Build 59.13] [# 568719]

- In a RADIUS load balancing setup, requests might be dropped because the memory for the session entries is not freed until the idle timeout expires even though the transaction completed earlier.

  [From Build 59.13] [# 573155]

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

  [From Build 59.13] [# 551623]

- In a link load balancing (LLB) deployment, if persistence is enabled on a NetScaler appliance and a policy based routing (PBR) or LB route is configured, the appliance might fail intermittently.

  [From Build 60.7] [# 574137]

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

  [From Build 60.7] [# 551623]

- A secure StoreFront monitor intermittently fails to sends probes.

  [From Build 60.7] [# 559164, 582153]

- In a link load balancing (LLB) deployment, if persistence is enabled on a NetScaler appliance and a policy based routing (PBR) or LB route is configured, the appliance might fail intermittently.

[From Build 60.7] [# 554841]

- In a load balancing group configuration, the "sh run" command sometimes runs in a loop, which exponentially increases the size of the temporary configuration file. As a result, saving the configuration and synchronizing the nodes in a high availability setup might fail.

  [From Build 60.7] [# 587812, 598499, 601918]

- In certain cases, if the name of an FTP virtual server is greater than 32 characters, the virtual server lookup fails and the request is not served.

  [From Build 60.7] [# 566644]

- The appliance fails if non-reachable autoscale entities that are part of a service group later become reachable and, in the interim, the service group name has changed.

  [From Build 60.7] [# 583647]

- After editing a service group in the configuration utility, the cacheable option is automatically set to true, even if the value was previously configured as false.

  [From Build 60.7] [# 592235]

- While probing the back-end HTTP server by using an HTTP monitor, the appliance does not send the port number in the HTTP host header. This behavior is not compliant with RFC 2616.

  [From Build 61.11] [# 564295]

- The NetScaler appliance fails while trying to load balance a request that was received on a recently closed connection. This happens because the server tries to keep the connection alive by sending an RTSP request but the appliance cannot find the corresponding client side connection.

  [From Build 61.11] [# 612943]

- If the channel between the primary node and the secondary node is disrupted, the session deletion information sent from the primary node to the secondary node might get lost. As a result, while the persistent sessions are reduced to zero on the primary node, the secondary node reaches its limit.

  [From Build 61.11] [# 596524, 597295]

- The NetScaler appliance fails while trying to load balance a request that was received on a recently closed connection. This happens because the server tries to keep the connection alive by sending an RTSP request but the appliance cannot find the corresponding client side connection.

  [From Build 62.9] [# 612943]

- A secure HTTP-ECV monitor might time out if the back-end server sends a large certificate.

[From Build 64.9] [# 638148]

- In rare cases, during a high level of CPU usage, if you disable and enable a service with zero delay, the state of the service might be inconsistent on different packet engines.

  [From Build 64.9] [# 622807]

- In a high availability (HA) setup, after a forced HA synchronization, the configuration is first cleared and then reapplied on the secondary node. As part of the synchronization operation, the service state changes are logged in the ns.log file. Due to repeated forced synchronizations, these messages flood the ns.log file. However, the service state messages are applicable only to the primary node and not relevant to the secondary node. Therefore, these messages are not logged in the ns.log file on the secondary node.

  [From Build 64.9] [# 645197]

NITRO

- When using the NITRO API to upload a file, make sure that each directory in the file path has the 755 (read, write, execute) permission.

  For example, to upload a file to the "/nsconfig/ssl/" directory, the following directories must have the 755 permission:

  - flash (because the "/nsconfig" folder is actually a link to "/flash/nsconfig/" directory)

  - nsconfig

  - ssl

  [From Build 64.9] [# 591970, 597032]

- The NetScaler appliance might fail to respond when a NITRO request is fetching a large number of bound entities.

  [From Build 60.7] [# 530805, 562748, 567856]

- Configuring singleton entities such as lbparam, sslparam, csparam, and vpathparam by using the "application/vnd.com.citrix.netscaler.<entityname>+json" content-type, results in error. For example, you get an error when setting the vPath parameter as follows:

  - URL: /nitro/v1/config/vpathparam

  - Method: PUT

  - Content-type: application/vnd.com.citrix.netscaler.vpathparam+json

  - Request payload: {"vpathparam":{"encapsulation":"enabled"}}

  - Response: {"errorcode": -1,"message": "Entityname is missing","severity": "ERROR"}

  [From Build 60.7] [# 574321]

  The TCP connection is not persistent for NITRO requests. Therefore, the underlying TCP connection is getting closed for each NITRO request.

[From Build 60.7] [# 583395, 457969]

- If the NetScaler appliance receives a logon request that contains both the session token and the request payload with the logon credentials, the appliance creates a new connection without closing the previous connection. If the appliance receives multiple such requests, the following error message appears: CFE limit exceeded.

  [From Build 62.9] [# 620458, 619154, 621601]

NS-CBC

- In an IPSec tunnel, the NetScaler appliance might remove sessions between client and server before encrypting (IPSec) DNS response packets, resulting in the loss of these DNS packets in the tunnel.

  [From Build 60.7] [# 587718]

NetScaler CLI

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

  [From Build 55.8] [# 383850]

NetScaler GUI

- The details of a custom monitor bound to a service group are not displayed correctly in the NetScaler GUI. The details appear correctly in the CLI.

  [From Build 63.8] [# 640332]

Networking

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

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

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

  [From Build 51.10] [# 480573]

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

  [From Build 51.10] [# 480621]

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

  [From Build 51.10] [# 490398]

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

  [From Build 51.10] [# 432192]

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

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

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

  [From Build 51.10] [# 483502]

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

  [From Build 52.11] [# 496564]

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

  [From Build 52.11] [# 491473]

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

  - IPv6 encapsulation (41)

  - Fragment Header for IPv6 (44)

  - ICMP for IPv6 (58)

  [From Build 52.11] [# 490190]

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

  [From Build 52.11] [# 441005]

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

  [From Build 52.11] [# 480100, 483728]

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

  [From Build 52.11] [# 477402]

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

[From Build 52.11] [# 477415]

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

  [From Build 52.11] [# 497057]

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

  [From Build 53.9] [# 490341]

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

  [From Build 53.9] [# 500720]

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

  [From Build 53.9] [# 496237]

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

  [From Build 54.9] [# 497277]

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

  [From Build 54.9] [# 510173]

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

  [From Build 54.9] [# 486632]

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

  [From Build 55.8] [# 522538]

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

  [From Build 55.8] [# 507345]

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

  [From Build 55.8] [# 485391]

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

  [From Build 55.8] [# 528069]

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

  [From Build 55.8] [# 485374]

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

  [From Build 55.8] [# 508631, 509453]

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

  [From Build 55.8] [# 528554]

- Blocking Traffic on Internal Ports

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

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

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

  At the command prompt, type:

  > set l3param -implicitACLAllow [ENABLED|DISABLED]

  Note: The parameter implicitACLAllow is enabled by default.

  Example:

  > set l3param -implicitACLAllow DISABLED

  Done

  [From Build 56.22] [# 529317]

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

  [From Build 56.22] [# 355965, 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.

  [From Build 56.22] [# 485260]

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

  [From Build 57.7] [# 554336]

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

  [From Build 57.7] [# 383958, 411806]

- An attempt to access the configuration utility might fail if the logon address is an IPv6 address.

  [From Build 58.11] [# 553588]

- The NetScaler appliance might not accept untagged Link Layer Discovery Protocol (LLDP) packets that are received on an interface which has "tagall" enabled.

  [From Build 58.11] [# 539617]

- If you have configured an INAT rule in which the private IP address is set to a virtual IP address, the rule is removed after you restart the NetScaler appliance.

  [From Build 58.11] [# 556632]

- A PBR6 rule might not get evaluated if you set the operator option to NEQ (!=) for source and destination IPv6 addresses.

  [From Build 59.13] [# 575906]

- A load balancing monitor fails under the following set of conditions:

  -The site IP address of a GSLB site is the SNIP address of the NetScaler appliance.

  -The monitor is monitoring a load balancing virtual server.

  [From Build 59.13] [# 533270, 533081, 570389, 573536]

- A large number of IPv6 client connections (more than 2 million) can degrade the performance of a NetScaler appliance.

  [From Build 59.13] [# 575126]

- A NetScaler appliance might consume a high percentage of CPU cycles, because the appliance repeatedly updates the active connections with changes in MAC addresses of servers.

  [From Build 59.13] [# 579099]

- An ACL6 rule might not get evaluated if you set the operator option to NEQ (!=) for source and destination IPv6 addresses.

  [From Build 59.13] [# 573516]

- Both the appliances in a NetScaler HA setup might become unresponsive or fail if you modify/remove two or more ACL/ACL6 rules on the primary node and then force synchronization on the secondary node without applying the ACLs on the primary node.

  [From Build 59.13] [# 576810, 545920, 575433]

- If you configure a PBR rule for the ICMP protocol, and the "forwardicmpfragments" L3 parameter is enabled, the NetScaler appliance might become unresponsive.

  [From Build 59.13] [# 575476]

- If the IPv6 routes change, the IPv6-Ipv6 tunnel's encapsulation IP addressess are not obtained based on the latest route information. As a result, the tunnels use old encapsulation IP addresses to encapsulate packets.

  [From Build 59.13] [# 564252]

- In a high availability configuration, a virtual IP address is removed from the configuration after the appliance is restarted or after HA synchronization if the virtual IP address is specified in a net profile entity.

  [From Build 59.13] [# 567484]

- The NetScaler appliance might not properly process packets related to forwarding session entries configured on the appliance.

  [From Build 59.13] [# 565475, 582155]

- In a high availability configuration, if you remove an ACL rule from the primary node and modify another ACL rule on the primary node, but you do not apply the ACLs on the primary node before forcing synchronization on the secondary node, the secondary node might become unresponsive.

  [From Build 59.13] [# 545920]

- TFTP monitor probes might fail with the error "Probe Timed out."

  [From Build 59.13] [# 578663]

- The NetScaler appliance might assign the NTP module a port that is used by some other feature module. Therefore, an incoming NTP response can be processed by the feature module. This can result in the failure of the NetScaler appliance.

  [From Build 60.7] [# 588477, 603874]

- In a high availability configuration, when the connection between primary and secondary goes down and comes up again, the secondary node receives HA INIT request from the primary node and it terminates all BGP connections.

  [From Build 60.7] [# 588509]

- On a NetScaler appliance with a NetScaler owned IP address configured with a VMAC address on a traffic domain, when a peer device sends an ARP request with unicast MAC for this IP address, the NetScaler appliance responds with the physical MAC address instead of the VMAC address. As a result, the NetScaler appliance drops packets forwarded by the peer device if the packets are destined to the physical MAC address for that IP address.

  [From Build 60.7] [# 588912]

- The NetScaler appliance might erroneously forward DHCP broadcast packets to the default router. As a result, the broadcast packets go in loops between the appliance and the router.

  [From Build 60.7] [# 591657, 595649]

- For extended ACL rules that are associated in NAT configurations (for example, RNAT rules, Large Scale NAT configurations), the configuration utility displays the TCP established parameter as enabled for these ACL rules.

  [From Build 61.11] [# 597458]

- If a connection matches a RNAT rule, the NetScaler appliance probes for the existence of the destination server before processing the connection based on the RNAT rule. The connection that is used for probing is sometimes left idle on the appliance and a new connection is opened once the client connection is successfully established. This probe connection stays idle for the configured idle timeout (2.5 hours) thus holding up resources on the server.

  Now, these probe connections are flushed within a minute if they remain idle.

  [From Build 61.11] [# 588694, 588551]

- If an IPv6 virtual server with persistency enabled is removed from a traffic domain, the traffic domain information for the existing persistency sessions is lost, and the NetScaler appliance hosting the virtual server becomes unresponsive.

  [From Build 61.11] [# 608558]

- The NetScaler appliance fails when it processes invalid IPSec IKED related packets.

[From Build 61.11] [# 609537]

- You cannot securely access (HTTPS) the NetScaler GUI by using a subnet IP (SNIP) address that is configured on a traffic domain.

  [From Build 61.11] [# 600364]

- In a high availability set up, if the primary node has learnt a large number of routes, a failover might result in the new primary node to fail.

  [From Build 62.9] [# 400276, 580029]

- The NetScaler appliance might fail if secure management access (HTTPS) is enabled on a SNIP6 address that is configured for a traffic domain.

  [From Build 62.9] [# 618633]

- After the clear config operation, reconfiguring a VXLAN entity fails to retrieve the VXLAN SNMP counters.

  [From Build 62.9] [# 572525, 574734, 614924]

- For backend TCP connections, a NetScaler appliance might allocate the subnet IP address and port of an active connection to a new connection. As a result, the new TCP connection fails.

  [From Build 62.9] [# 613454]

- In a GSLB deployment of NetScaler appliances configured with OSPF routing protocol, the OSPF process running in one of the NetScaler appliances sources OSPF hello packets from the GSLB site IP address configured on the appliance. As a result, neighbor adjacency does not get established.

  [From Build 62.9] [# 612419, 633722]

- On a NetScaler appliance, connections might get reset between routing processes. As a result, the dynamic routes are occasionally deleted and added back.

  [From Build 62.9] [# 599306]

- The NetScaler appliance does not retain the entire 64 bit ID of IPv6 fragments of a session. As a result, the session might fail.

  [From Build 62.9] [# 614042]

- The dynamic routing module on a NetScaler appliance might incorrectly save the command "redistribute intranet" as "redistribute trill" in the ZebOS configuration file. Because the appliance does not support the "redistribute trill" command, after a failover in a high availability setup, the new primary node treats the "redistribute trill" command as an error and does not apply the subsequent commands in the ZebOS configuration file. This results in loss of configuration.

[From Build 62.9] [# 620152]

- An active FTP connection might get reset for no apparent reason, regardless of the state of the random source port.

  [From Build 62.9] [# 507908, 609496, 611357, 615638]

- The NetScaler appliance sends GARP request for a non-addressable virtual server when the virtual server's state changes to UP or DOWN.

  [From Build 63.8] [# 620697]

- Because the subnet mask for the GSLB IP address and the SNIP address are the same, the Netscaler appliance incorrectly selects the SNIP address instead of the GSLB IP address for GSLB connections. The user authentication process is affeced because of the wrong selection of the IP address.

  [From Build 63.8] [# 633722]

- In an active-active deployment using VRRP, a NetScaler appliance does not match its configured bridge ACL rules to the packets received from the inactive VIP addresses of the other NetScaler appliances.

  [From Build 63.8] [# 614786]

- The NetScaler appliance might become unresponsive while processing a route dependency check for multiple recursive BGP routes if the next hop for any of the routes changes or goes down.

  [From Build 63.8] [# 625841]

- The NetScaler appliance might fail if secure management access (HTTPS) is enabled on a SNIP6 address that is configured for a traffic domain.

  [From Build 63.8] [# 618633]

- During a "force sync" operation in a cluster deployment, performing a "save config" operation on a node might lead to a full or partial configuration loss on that node. With this fix, the "save config" operation is not permitted during a "force sync" operation.

  [From Build 64.9] [# 642375, 658619]

- When all ports of all IP addresses bound to a netprofile are used in different back-end connections, the NetScaler appliance uses one of the SNIP addresses, which is not bound to the netprofile, for a new back-end connection. Back-end systems reject the connection if the SNIP address is listed in their deny ACL rules. Now, the NetScaler appliance does not initiate any new back-end connection when all the ports of all IP addresses in a netprofile are being used.

  [From Build 64.9] [# 627547]

- In a high availability setup, secondary node advertises default routes even after performing "ns block-sec-rtadv" operation in VTYSH shell.

[From Build 64.9] [# 639541]

- A NetScaler appliance with OSPFv3 dynamic routing protocol configured might measure the length of OSPFv3 LSA packets in Network Byte Order instead of Host Byte Order for comparison with the minimum required packet length. As a result, the NetScaler appliance becomes unresponsive.

  [From Build 64.9] [# 652131]

- Restarting a NetScaler appliance that has a VLAN bound to a traffic domain and is configured as a SYNC VLAN or NSVLAN might cause configuration loss of binding between the VLAN and the traffic domain.

  [From Build 64.9] [# 648839]

- The NetScaler appliance might become unresponsive when one or both of the following conditions are met:

  - When you remove a traffic domain, which has ACLs, or ACL6s, or PBRs, or PBR6s rules, without performing apply operation for ACLs, or ACL6s, or PBRs, or PBR6s rules.

  - When you remove any ACL, or ACL6, or PBR, or PBR6 rule within a traffic domain and then remove the traffic domain before performing apply operation for ACLs, or ACL6s, or PBRs, or PBR6s rules.

  [From Build 64.9] [# 636269]

Optimization

- If the front end optimization feature is enabled on the NetScaler appliance, HTML pages containing question mark (?) characters fail to load in the client browser.

  [From Build 58.11] [# 565746]

- If the front end optimization feature is enabled, the NetScaler appliance sometimes fails if the HTTP response headers span multiple packets.

  [From Build 58.11] [# 558861, 562680]

- The NetScaler appliance fails if the cached objects are revalidated with the server while the front end optimization feature enabled.

  [From Build 58.11] [# 554497]

- Unavailability of the 32-bit metadata memory causes the NetScaler appliance to send cached requests to the servers.

  [From Build 58.11] [# 564643]

- The NetScaler appliance fails with Front End Optimization enabled and many objects queued for optimization.

  [From Build 58.11] [# 560751]

- A NetScaler appliance fails if the front end optimization (FEO) feature is enabled, the FEO action is configured for Extend Page Cache, and the server response does not include a Cache Control or Expires header.

  [From Build 63.8] [# 621122, 629593]

Policies

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

  [From Build 52.11] [# 493045]

  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 ('

  ') characters are unsafe.

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

  * APPEND_QUERY_PARAMETER - same as HTTP_URL_SAFE

  [From Build 53.9] [# 506761]

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

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

- Some IP based expressions might not work for IP addresses starting from octet 128 or greater (128.x.x.x - 254.x.x.x).

  The following expressions are not impacted:

  - EQ, IN_SUBNET, IS_IPV6, GET1, GET2, GET3, GET4, MATCHES, MATCHES_LOCATION, APPEND, TYPECAST_TEXT_T, TYPECAST_IPv6_ADDRESS_AT

  The following expressions do not work:

  GT, GE, LT, LE, BETWEEN, NE, ADD, SUB, MUL, DIV, MOD, NEG, BITAND, BITOR, BITXOR, BITNEG, LSHIFT, RSHIFT, TYPECAST_TIME_AT, TYPECAST_IP_ADDRESS_AT, TYPECAST_DOUBLE_AT, TYPECAST_UNSIGNED_LONG_AT,

WEEKDAY_STRING, WEEKDAY_STRING_SHORT, SIGNED8_STRING, UNSIGNED8_STRING, SIGNED16_STRING, UNSIGNED16_STRING, SIGNED32_STRING

[From Build 60.7] [# 534244]

- If packet tracing is configured with a default-syntax expression and non-TCP traffic is being processed, and rewrite action applied on a HTTP chunked message is occurring then the rewritten data maybe incorrect or it might crash a NetScaler appliance.

  [From Build 61.11] [# 598465]

- Under certain conditions, a NetScaler appliance does not insert an X-Forwarded-For field in the HTTP header for an HTTP CONNECT requests that are forwarded to server.

  [From Build 62.9] [# 605089]

- A NetScaler appliance fails if you perform a Clear Configuration operation.

  [From Build 64.9] [# 634124]

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

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

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

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

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

  [From Build 56.22] [# 554460]

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

  [From Build 56.22] [# 530804]

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

  [From Build 57.7] [# 551626]

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

  [From Build 58.11] [# 557908]

Responder

- The NetScaler appliance fails if it receives a new request while an embedded expression in the responder HTML page is in blocking state.

  [From Build 63.8] [# 556035]

SSL

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

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

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

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

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

  nsapimgr -y -s ssl_cert_insertion_space=0

  [From Build 54.9] [# 495316]

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

  [From Build 56.22] [# 529471]

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

  This issue is now fixed.

  [From Build 57.7] [# 552812, 558824]

- 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.

  [From Build 57.7] [# 484525]

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

  [From Build 57.7] [# 529471]

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

  [From Build 57.7] [# 550138, 552436, 552701]

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

  [From Build 57.7] [# 554917]

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

  [From Build 58.11] [# 560175, 563831, 564931]

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

  [From Build 58.11] [# 552812, 558824]

- If application data is received during an SSL renegotiation handshake, the appliance sends a RST flag.

  [From Build 59.13] [# 542034]

- Statistics for TLS1.1 and TLS1.2 transactions do not appear in the output of the stat ssl command.

  [From Build 59.13] [# 336395, 559165, 560353]

- If TLS1.1/1.2 protocol is used with AES/3DES ciphers, the TCP window at the backend reduces to zero. As a result, after some time, the connection is terminated.

  [From Build 59.13] [# 591600, 595713, 596278, 596556, 596566, 598045, 599524, 600591]

- In some cases, when client authentication is enabled, incorrect data form a client leads to a memory leak on the NetScaler appliance. If a large number of clients send incorrect data, the appliance fails.

  [From Build 59.13] [# 570754]

- If you have configured optional client-certificate authentication and your policies target client certificate x509 extensions, such as auth keyid, a transaction with a client that doesn't have a certificate might cause the appliance to fail or to use stale values from a previous transaction.

  [From Build 59.13] [# 593091]

- 2048-bit Default Certificates on the NetScaler Appliance

With this release, the length of the default certificate on a NetScaler appliance is a 2048 bits. However, upgrading to release 11.0 does not automatically install a 2048-bit certificate.

Note: Citrix recommends that you replace the default certificate with a certificate issued by a CA.

On a VPX appliance that does not have licenses, you can continue to use the old (512-bit) default certificate after the upgrade, although a 512-bit certificate-key pair is not secure and might not work with the latest browsers. If you have the proper licenses, you can delete all your old certificate-key pairs that have "ns-" as the first three characters, and then restart the appliance to automatically generate a 2048-bit default certificate.

[From Build 60.7] [# 451441, 405363, 458905, 465280, 540467, 547106, 551603, 559154, 584335, 588128]

- Even though SSL renegotiation is set to deny (that is, denySSLReneg is set to ALL), the server responds with the "server reneg" extension in the initial SSL handshake.

  [From Build 60.7] [# 559082]

- If you update the certificate-key pair for a service group, the change is not reflected in the individual services that are bound to this service group. As a result, the old certificate-key pair continues to be used for negotiation in the SSL handshake.

  [From Build 60.7] [# 554925]

- In release 10.5 or later, TLS protocol versions 1.1 and 1.2 are enabled by default, but can typically be controlled by configuration. For some types of services, however, configuration is not possible and the default settings are used: VPN and dynamically configured services like StoreFront and AppController, and SSL_BRIDGE services to which secure monitors are bound. To allow users to disable TLS 1.1 and 1.2 on these kinds of services, two SSL parameters have been introduced: montls1112disable and svctls1112disable. When set to ENABLED, these parameters disable TLS 1.1 and 1.2 for these types of cases. The montls1112disable option can be toggled on and off during runtime, but the svc1112disable option cannot. If you enable it and then want to disable it, you have to change its setting to DISABLED and then restart the appliance.

  [From Build 60.7] [# 602502, 599209]

- If you have a large number of SSL services (greater than 3000) in the backend, CPU usage increases exponentially and the appliance fails.

  [From Build 60.7] [# 581193]

- An incoming SSL record that spans more than 256 TCP packets and contains TCP header options causes memory corruption in the Cavium command buffer structure. As a result, the NetScaler appliance fails.

  [From Build 60.7] [# 573904, 583295, 590222, 606399]

- If you have configured optional client-certificate authentication and your policies target client certificate x509 extensions, such as auth keyid, a transaction with a client that doesn't have a certificate might cause the appliance to fail or to use stale values from a previous transaction.

  [From Build 60.7] [# 593091]

- If you downgrade the software on your NetScaler appliance that does not have a license to release 9.3 build 61.66 or earlier, some commands related to the default server certificate might not be saved in the running configuration. As a result, after restarting, secure access (HTTPS) to the appliance fails.

  [From Build 60.7] [# 551603, 559154]

- If TLS1.1/1.2 protocol is used with AES/3DES ciphers, the length of the TCP window at the back end shrinks to zero. As a result, after some time, the connection is terminated.

  [From Build 60.7] [# 591600, 595713, 596278, 596556, 596566, 598045, 599524, 600591, 604929]

- In release 10.5 or later, TLS protocol versions 1.1 and 1.2 are enabled by default, but you can disable them for all services except SSL_BRIDGE and dynamic services, which can't otherwise be configured. In this release, you can disable TLS1.1/1.2 on SSL_BRIDGE and dynamic services by enabling the new "svctls1112disable" and "montls1112disable" parameters, as follows:

  > set ssl param -svctls1112disable enable -montls1112disable enable

  After the new parameters are enabled, you cannot disable them by using the "set ssl param" command. You must edit the configuration (ns.conf) file as follows:

  1. Remove these parameters from the "set ssl param" command.

  2. Save the configuration.

  3. Restart the appliance.

  [From Build 61.11] [# 602502, 599209, 609284]

- TLS1.2 handshake fails with some back end servers if SHA2 certificates are bound to the server and client authentication is enabled on the server.

  [From Build 61.11] [# 600155, 601059]

- If the passphrase for a certificate contains the "$" character, the configuration utility becomes unresponsive.

  [From Build 61.11] [# 591743]

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

  [From Build 61.11] [# 564565]

- SSL internal services might fail if you modify any SSL parameters while the SSL feature is disabled or not licensed.

  [From Build 63.8] [# 601951]

- After you upgrade to this build, configuring a front-end service, or creating an internal service, with default ciphers results in a cipher inconsistency between a packet engine and the cluster configDB.

[From Build 63.8] [# 625966]

- The front end services appear as back-end services on the nodes of a cluster setup.

  [From Build 63.8] [# 632128]

- The appliance fails if a loop is created while linking the certificates. With this fix, the software checks whether a new certificate is already part of the link.

  [From Build 63.8] [# 612461]

- Adding a certificate revocation list (CRL) on the NetScaler appliance fails with the error message "Certificate Issuer Mismatch" for a DER certificate, and with the error message "Invalid CRL" for a PEM certificate. This issue occurs because the attribute type of the common name field is different for the CA certificate than for the CRL.

  [From Build 64.9] [# 623058, 634017]

- The NetScaler appliance displays high CPU usage because of a wrong computation of idle time.

  [From Build 64.9] [# 571226, 652915]

- In a cluster setup, if you rename a load balancing virtual server of type SSL, the local database table, which is used for all GET operations, is not updated.

  [From Build 64.9] [# 620964, 576828, 641041]

- In a cluster setup, the serial number and validity do not appear correctly in the output of the "sh ssl certkey" command.

  [From Build 64.9] [# 635851, 504829]

- In a cluster setup, if you try to update an existing certificate by replacing the old files with new certificate and key files, the following error message appears:

  ERROR: Resource already exists [certkeyName Contents, nglab-2016]

  [From Build 64.9] [# 633395]

- The output of the "stat ssl -detail" command is different for back-end entities than for front-end entities. The output for back-end entities does not include statistics for sessions, handshakes, or client authentications for TLS protocol versions 1.1 and version 1.2.

  At the back end, the label "Authorizations" is incorrect. It should be "Authentications."

  [From Build 64.9] [# 627635]

- In a cluster setup, if you have configured a front end service, or an internal service is created, with default ciphers, and then you upgrade to this build, there is a cipher inconsistency between a packet engine and the cluster configDB.

[From Build 64.9] [# 631258]

- The version displayed in syslog is SSLv2.0 even though the session is negotiated using TLSv1.2.

  [From Build 64.9] [# 474417, 474413]

- Support for ECC curves in Service Groups

  You can now bind ECC curves to back-end service groups by using the NetScaler command line.

  At the command prompt, type:

  bind ssl serviceGroup <serviceGroupName> -eccCurveName <eccCurveName>

  [From Build 64.9] [# 592418, 659240]

SureConnect

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

  [From Build 57.7] [# 526782]

System

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

  [From Build 51.10] [# 477709]

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

  [From Build 51.10] [# 488997, 493835]

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

  [From Build 51.10] [# 488487]

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

  [From Build 51.10] [# 478356]

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

  [From Build 51.10] [# 452240]

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

  [From Build 51.10] [# 484960]

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

  [From Build 52.11] [# 490192]

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

  [From Build 52.11] [# 478608]

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

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

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

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

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

  [From Build 52.11] [# 463571]

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

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

- If you change the IP address of a load balancing virtual server that shares the same server information (IP address, port and service) with an audit server and then clear the configurations, the NetScaler is expected to remove the virtual server, the audit server, and other NetScaler configurations. However, when you now add the virtual server with the original server details, the NetScaler throws an error message that says "resource already exists".

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

  [From Build 52.11] [# 484527]

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

  [From Build 52.11] [# 487437, 494371]

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

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

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

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

  [From Build 52.11] [# 480219]

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

  [From Build 52.11] [# 498221, 501681]

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

  [From Build 53.9] [# 494013]

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

  [From Build 54.9] [# 501100]

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

  [From Build 54.9] [# 517652, 523715]

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

  [From Build 54.9] [# 518322]

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

  [From Build 54.9] [# 490622, 496613]

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

  [From Build 54.9] [# 519390]

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

[From Build 55.8] [# 528818, 529425]

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

  [From Build 55.8] [# 519004, 528861]

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

  [From Build 55.8] [# 486257]

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

  [From Build 55.8] [# 504910]

- The NetScaler appliance generates SNMP clear alarm traps for successful cases of haVersionMismatch, haNoHeartbeats, haBadSecState, haSyncFailure, and haPropFailure error events in an HA configuration.

  [From Build 55.8] [# 368832]

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

  [From Build 56.22] [# 539454]

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

  Invalid response from the aggregator [Device not Configured]

  [From Build 56.22] [# 377618, 341460, 351127, 364015, 475359, 481575, 499259]

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

  [From Build 56.22] [# 532843, 534384]

- Launching of applications or desktops through a NetScaler appliance can fail, if the appliance is deployed in a multi-hop topology where the first hop performs load balancing and points to the second hop which performs gateway ICAProxy functionality.

  [From Build 56.22] [# 560747]

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

[From Build 56.22] [# 532042, 447664, 532587, 533164]

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

  [From Build 56.22] [# 528309]

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

  [From Build 56.22] [# 529493]

- If the NetScaler appliance uses the HTTP pipeline to parse an HTTP request, and the parsing process fragments the request packet, the appliance, after processing a fragment, might not unset the flag indicating that the entire packet has been received. In that case, the appliance fails.

  [From Build 56.22] [# 527320, 527211]

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

  [From Build 56.22] [# 527119, 522584, 525657]

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

  [From Build 56.22] [# 524949]

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

  [From Build 56.22] [# 286861, 301935, 513312, 522183, 541332]

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

  [From Build 56.22] [# 506056]

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

  [From Build 56.22] [# 494911, 481032, 511763, 528309, 532708, 538507]

- While handling PLAIN acknowledgement packets in a TCP VIP path, the NetScaler appliance drops FINACK packets.

  [From Build 56.22] [# 572046, 577192]

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

[From Build 56.22] [# 549904, 503614, 532794, 543864, 548338, 552628]

- 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.

  [From Build 57.7] [# 536576, 549318]

- 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.

  [From Build 57.7] [# 480258, 494482, 523853]

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

  [From Build 57.7] [# 498025, 521636, 534432]

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

  [From Build 57.7] [# 549904, 503614, 532794, 543864, 548338, 552628]

- The NetScaler appliance can become unavailable if you perform the following sequence of operations multiple times:

  1. Create a UDP load balancing virtual server (lbvserver).
  2. Configure a syslog audit server that has the same IP address and port as the UDP lbvserver.
  3. Bind the syslog audit policy to system global.
  4. Execute the "set audit syslogPolicy" command.
  5. Execute the "clear ns config" command.

  [From Build 57.7] [# 558143]

- In a cluster or HA setup, when you perform an operation that adds a new file (create/import SSL/APPFW), the files is synchronized to the other nodes (non-CCO nodes in a cluster or the secondary appliance in an HA setup). This synchronization either happens either periodically or when manually executed. If an operation that uses this file is executed before the file is synchronized, the operation fails, because the required file is not available.

  For example, if you import a certificate file, and then execute the "show cert key" command immediately, the command fails.

  This issue is fixed by synchronizing the files across all the nodes automatically, after they are added.

  [From Build 57.7] [# 535162, 288743, 389394, 470729, 562724]

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

[From Build 57.7] [# 547739, 527797, 531101]

- While handling PLAIN acknowledgement packets in a TCP VIP path, the NetScaler appliance drops FINACK packets.

  [From Build 58.11] [# 572046, 577192]

- NetScaler appliance may fail when trying to re-use the probe connection on wildcard vserver or service due to incorrect maximum segment size value learned from server.

  [From Build 58.11] [# 567413, 568270]

- NTP Version Update

  In NetScaler release 11, the NTP version has been updated from 4.2.6p3 to 4.2.8p2.

  If you upgrade your NetScaler appliance from any earlier release to release 11, the NTP configuration is automatically upgraded with additional security policies.

  [From Build 58.11] [# 440375, 440591]

- 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.

  [From Build 58.11] [# 506378]

- On performing the batch operation on the NetScaler appliance, the commands that are dependent on other commands can be lost from the NetScaler configuration file.

  [From Build 58.11] [# 527887]

- The NetScaler appliance can become unavailable if you perform the following sequence of operations multiple times:

  1. Create a UDP load balancing virtual server (lbvserver).
  2. Configure a syslog audit server that has the same IP address and port as the UDP lbvserver.
  3. Bind the syslog audit policy to system global.
  4. Execute the "set audit syslogPolicy" command.
  5. Execute the "clear ns config" command.

  [From Build 58.11] [# 558143]

- Launching of applications or desktops through a NetScaler appliance can fail, if the appliance is deployed in a multi-hop topology where the first hop performs load balancing and points to the second hop which performs gateway ICAProxy functionality.

  [From Build 58.11] [# 560747]

- If you execute NTP commands, such as enable ntp sync and show ntp status, the NetScaler appliance might become unresponsive because of a memory leak.

  [From Build 59.13] [# 529787, 574866, 581849]

- After cleaning up an MPTCP session, the NetScaler appliance might not set the DATA_FIN flag in the TCP header of the data or acknowledgement packet if there is no subflow for sending the data.

  [From Build 59.13] [# 553650]

- While handling PLAIN acknowledgement packets in a TCP VIP path, the NetScaler appliance drops FINACK packets.

  [From Build 59.13] [# 572046, 577192, 586755]

- The appliance might fail under the following set of conditions:

  1. A pipelined HTTP request is received that spans multiple TCP segments.

  2. An internal HTTP response generated by NetScaler for the HTTP request in condition 1, is terminated by a TCP segment that has the TCP FIN flag set.

  3. The appliance receives another HTTP request on the same connection.

  [From Build 59.13] [# 587817, 587879, 589416, 594044, 595927, 601915]

- On rebooting the NetScaler appliance, the timeout is not set to the value specified by the "set ns timeout" command.

  [From Build 59.13] [# 587074]

- Management CPU usage is high when you use the configuration utility's memory usage diagnostic tool (System > Diagnostics > Memory usage).

  [From Build 59.13] [# 586328]

- The NetScaler appliance might become unresponsive if it receives a retransmitted TCP jumbo frame that carries the TCP FIN flag.

  [From Build 59.13] [# 571176]

- If you enable the snmp alarm SERVICEGROUP-MEMBER-MAXCLIENTS, varbinds such as svcGrpMemberName, svcGrpMemberEstablishedConn, alarmHighThreshold, svcGrpMemberFullName, and sysIpAddress might be missing from the alert.

  [From Build 59.13] [# 578673]

- A NetScaler appliance might crash if you attempt to start the nstrace instance with advanced filter expression.

  [From Build 60.7] [# 493737, 526095, 598148]

- Support for MPTCP Version Negotiation

  A client can now establish an MPTCP connection with NetScaler appliance even if the client's and the NetScaler appliance's MPTCP versions does not match. If the MPTCP version of the client is higher than the one supported on the appliance, the client falls back to a lower or equal version. If the appliance supports that version, the MPTCP session continues. Otherwise, the appliance falls back to a normal TCP session.

  [From Build 60.7] [# 529883]

- While upgrading the NetScaler appliance from 10.5.53.x to 10.5.54.9 version, the Client-Server Link Mapping check box was unavailable on TCP/IP connections page. The check box is now available in the TCP Connections page.

  [From Build 60.7] [# 551611, 519966]

- A NetScaler appliance has high memory consumption if Front End Optimization (FEO) feature is enabled.

  Work around: To resolve this configuration issue, the customer needs to disable the FEO feature. Otherwise, the customer needs to reboot the NetScaler appliance.

  [From Build 60.7] [# 591928]

- For a load balancing configuration, the NetScaler appliance uses the server-side session information instead of the client-side session information for handling a client-side packet. As a result, the NetScaler appliance becomes unresponsive.

  [From Build 60.7] [# 584531, 576932, 597895, 607060]

- Entering the nstcpdump.sh command causes the Management CPU utilization to reach 100 recent.

  [From Build 60.7] [# 513048]

- Management access to the NetScaler appliance can slow down or become unavailable when the traffic domain identifier is not initialized for jumbo frames. However, virtual servers continue to serve traffic.

  [From Build 60.7] [# 583579, 594722]

- The host name configured for the NetScaler appliance is now displayed on the LCD panel.

  [From Build 60.7] [# 498991, 498994]

- If the NetScaler appliance receives a data or an acknowledgement packet without the Data Sequence Signal (DSS) option before the MPTCP connection is established, the appliance does not seamlessly fallback to regular TCP.

  [From Build 60.7] [# 588909]

- The appliance might fail under the following set of conditions:

  1. A pipelined HTTP request is received that spans multiple TCP segments.

2. An internal HTTP response generated by NetScaler for the HTTP request in condition 1, is terminated by a TCP segment that has the TCP FIN flag set.

3. The appliance receives another HTTP request on the same connection.

[From Build 60.7] [# 587817, 587879, 589416, 594044, 595927, 601915]

- The upgrade wizard in the configuration utility puts the NetScaler software in the /var directory instead of the /var/nsinstall/<build id> directory.

  [From Build 60.7] [# 586721]

- If a server advertises a maximum segment size (MSS) greater than 1460 bytes, a TCP transaction might not generate a response after passing through the NetScaler appliance.

  [From Build 60.7] [# 584079]

- The NetScaler appliance might become unresponsive if front end optimization (FEO) is enabled with the SSL and rewrite features.

  [From Build 60.7] [# 583829]

- Failed SNMP requests were not removed properly, therefore, subsequent set requests were retained in the queue. This lead to all SNMP requests getting blocked and high memory usage, due to which the SNMP module stops responding.

  [From Build 60.7] [# 590289, 584527, 596242]

- When SPDY Protocol is enabled and SPDY Traffic is received on the NetScaler appliance, the TCP current clients counter goes to negative values and shows a very large value in the stat or the SNMP OID.

  [From Build 60.7] [# 551562, 551786, 568554]

- When the NetScaler appliance receives MPTCP traffic, the number of established client connections is high, because both MPTCP sessions and subflows are treated as client connections.

  With this fix, the snmp oid of following mibs have changhttp://reno.citrite.net/images/edit-review.png?1427997750ed to:

  mptcpCurSessWithoutSFs: 130

  vsvrCurMptcpSessions: 73

  vsvrCursubflowConn: 74

  [From Build 60.7] [# 583292]

- The NetScaler appliance fails to respond when the HTML injection feature is enabled.

  [From Build 60.7] [# 542418]

- When you run multiple instances of nstcpdump.sh command, the system results in bad dump bad dump file format errors.

  [From Build 60.7] [# 584825]

- In a HA setup, if a domain-based SNMP manager is added on the secondary appliance, the NetScaler appliance stops responding eventually. You must configure the SNMP manager on the primary appliance.

  [From Build 60.7] [# 581355, 593292, 595943]

- Under stressful conditions (too many API requests) the NetScaler appliance is unable to retrieve LCD counters from the back end.

  [From Build 61.11] [# 533156, 599100]

- Some events may be logged twice if DEBUG level is enabled for syslog, by using the "set audit syslogParam" command.

  [From Build 61.11] [# 594485]

- A NetScaler appliance fails when it receives an MP_CAPABLE final acknowledgement in a single packet with the FIN flag set.

  [From Build 61.11] [# 583853, 583855, 588078, 601746, 602955]

- With the default TCP congestion control, a NetScaler appliance recovering from packet loss reduces the congestion window to half its previous length. With multiple packet loss events, the congestion window becomes small and delays transactions.

  [From Build 61.11] [# 606493, 601655]

- If, when processing a URL, the parser encounters a tag that has "#"as a source attribute, the URL is considered to be empty as # is a fragment identifier. This leads to corrupted values because we continue processing the empty URL.

  [From Build 61.11] [# 605258]

- A NetScaler appliance might occasionally fail when a client connects to an HTTP/SSL server and the server sends a 101 (switching protocols) response. The connection is closed before data can be sent or received from the client.

  [From Build 61.11] [# 576561, 587759]

- The NetScaler appliance does not reduce the received Maximum Segment Size (MSS) to accommodate TCP options (such as timestamps). Therefore, the NIC drops such packets.

  [From Build 61.11] [# 593209]

- A NetScaler appliance becomes unresponsive when passing an HTML response with the HTML tag exceeding 16 characters.

  [From Build 61.11] [# 611723]

- In certain cases, the NetScaler appliance might not retransmit the lost TCP segments resulting in a transaction failure.

  [From Build 61.11] [# 565938, 560394, 592227, 597160, 607864, 609068]

- NIC Failures detected during boot up do not prevent a NetScaler appliance from booting up and successfully starting the packet engines. The appliance displays an error message about the missing NICs.

  With this fix, if a NIC failure is detected during boot up, the appliance will not start Packet Engines and display an error message about the missing NICs.

  [From Build 61.11] [# 547260]

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

  [From Build 61.11] [# 538212]

- When parsing a host name with no Path component, the URL parsing logic does not search for a question mark (?), so an entire string might be interpreted as the host name. This causes an error when the appliance tries to resolve the DNS name. With this fix, the parsing logic searches for question marks.

  Eg:
  http://example.com.php?&curuserid=94315577&host=wscdny203.live.changba.com&token=T59d105c1c74042e&localip=221.235.187.75&clientip=80.95.239.1&bless=1&channelsrc=market_%E7%99%BE%E5%BA%A6

  [From Build 61.11] [# 587858]

- In a high availability setup with stateful connection failover option enabled on a virtual sever, if a network link that is used for synchronizing connection information between the nodes becomes DOWN.

  Both nodes take a lot a time to reestablish connection information synchronization through the remaining active links, as a result some connection information might not get synchronize to the secondary node.

  [From Build 61.11] [# 590574]

- If, when establishing an MPTCP connection, a NetScaler appliance receives a duplicate acknowledgment in the 3-way handshake process, the appliance reverts to a normal TCP connection.

  [From Build 61.11] [# 601372]

- When a NetScaler appliance is integrated with ESP or VPX devices functioning as E100 devices, it encounters buffer-allocation failure and packet-reception failure.

  [From Build 62.9] [# 604971, 611176]

- Client-based virtual machines are unable to access a NetScaler appliance if they are running on the same server (for example, VPX on Linux KVM). However, they are accessible if they are running on different servers.

  [From Build 62.9] [# 613108]

- A NetScaler appliance fails when an MPTCP subflow receives an Infinite DSS mapping in a partially retransmitted packet.

  [From Build 62.9] [# 614842, 623426]

- A NetScaler appliance fails if the Front End Optimization (FEO), Application Firewall, and SSL features are all enabled and the appliance encounters an error while parsing an HTML response.

  [From Build 62.9] [# 624327]

- A warning error message "Error =80000004 in nsagg_process_stat_request, closing connection" displays when a nscollect module requests counter information from a nsagregator daemon at every 5 minute interval. The nsaggregator daemon prints the warning message as response to the request received from nscollect module for more than 256 counters.

  [From Build 62.9] [# 610809, 577474, 579560, 622553]

- Due to a bug in Hard Disk Drive (HDD) monitoring logic, if a message in /var/log/messages matches "*ad* Device not configured" string pattern, it results in producing false positive errors.

  [From Build 62.9] [# 611774, 598774]

- A high availability pair fails if an HTTP response from a back-end server contains carriage return line feeds (CRLFs) after the HTTP Content Length and at the start of a new packet.

  [From Build 62.9] [# 547267, 623146]

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

  - One or more of the following features are configured on the appliance: cache redirection, content switching, AAA-TM, Clientless VPN, full tunnel VPN, forward proxy.

  - The client connection times out while the DNS name is being resolved using the FQDN of back-end servers.

  [From Build 62.9] [# 608479]

- In a wildcard virtual server configuration, a NetScaler appliance dynamically identifies an origin service by opening a probe connection. If the origin responds with a jumbo Maximum Segment Size (MSS), the appliance uses the MSS for future connections with the origin. If the jumbo frame support is disabled, it results in transactions failure.

  [From Build 62.9] [# 605873]

- Commands entered in the NetScaler CLI or GUI might fail because of a shortage of system resources or failure of system socket connections.

  With this fix, the NetScaler appliance attempts to reestablish the socket connections. After the socket connections are established, the appliance runs the failed commands internally.

  [From Build 62.9] [# 615487]

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

  - One or more of the following features are configured on the appliance: cache redirection, content switching, AAA-TM, Clientless VPN, full tunnel VPN, forward proxy.

  - The client connection times out while the DNS name is being resolved using the FQDN of back-end servers.

  [From Build 62.9] [# 543293, 578993, 579965, 593378, 599535, 608479, 614368, 628579, 628763, 634338]

  In a high availability setup, command propagation and configuration synchronization using secure RPC might fail if SSLv3 and TLS1.0 protocols are disabled for SSL internal services.

  [From Build 63.8] [# 613966]

- A NetScaler Policy Infrastructure (PI) connection reset code for a non HTTP type virtual server might cause a memory leak.

  [From Build 63.8] [# 626562, 632738, 634610]

- If, in a Multipath TCP (MPTCP) session with a single subflow, the client in the subflow signals a zero-window condition before the subflow connection times out, the NetScaler appliance uses small-window-protection logic to mark the subflow connection as a small-window attack from the client. The logic checks to determine whether the existing number of small window connections are more than the threshold value (set to 100, by default) and if true, the appliance resets the subflow causing the appliance to fail.

  [From Build 63.8] [# 639081]

- A NetScaler appliance fails on a network interface if it receives retransmitted data for which the maximum transmission unit (MTU) is larger than 1500 bytes.

  [From Build 63.8] [# 625776, 624763, 624779, 629314, 630646, 636283, 637479]

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

  - One or more of the following features are configured on the appliance: cache redirection, content switching, AAA-TM, Clientless VPN, full tunnel VPN, forward proxy.

  - The client connection times out while the DNS name is being resolved using the FQDN of back-end servers.

  [From Build 63.8] [# 543293, 578993, 579965, 593378, 599535, 608479, 614368, 628579, 628763, 634338]

- If a client on an IPV6 connection advertises an MSS value below 1360 (bytes), the NetScaler appliance responds with a MSS value below the (RFC) required minimum value of 1220 (bytes).

[From Build 63.8] [# 556475]

- A NetScaler appliance might become unresponsive if it has a TCP profile with the TCP keepalive option enabled and is bound to a load balancing virtual server. The cause is an interoperability issue between the TCP keepalive and TCP packet retransmission functionalities.

  [From Build 64.9] [# 619349, 626027]

- A NetScaler appliance fails if a TCP/IP session is simultaneously reused for TCP and Multipath TCP (MPTCP) operation and not mutually exclusive with TCP KeepAlive enabled for MPTCP subflows.

  [From Build 64.9] [# 654080]

- In a NetScaler appliance, if the Ring Receive buffer is full, the appliance starts to discard data packets at the Network Interface Card (NIC). As a result, the appliance drops packets leading to a probe failure.

  [From Build 64.9] [# 623977, 649735]

- If, after restarting a NetScaler appliance, you increase the cache memory limit while the front end optimization (FEO) feature is enabled, the appliance fails.

  [From Build 64.9] [# 626082, 628536, 633772, 642939]

- The NetScaler appliance might fail, because of memory corruption, if a policy uses an expression that applies the MATCHES (not MATCHES_LOCATION) function to an IPv4 or IPv6 address and there is an issue in communicating with the DNS server.

  [From Build 64.9] [# 630782, 630436, 631279, 637396, 650939, 650964]

- The CPU parameter value on the LCD panel does not match the value reported by the NetScaler CLI or GUI.

  [From Build 64.9] [# 643237]

- The TCP wait queue counter might be incorrect, because the NetScaler appliance does not update the counter properly during persistence probes.

  [From Build 64.9] [# 637919]

- If a NetScaler appliance has "TCP timestamp" parameter enabled in a TCP profile, some internal configurations and connections fail when the appliance attempts to communicate with the underlying freebsd.

  [From Build 64.9] [# 612251]

- If an imported responderhtmlpage content ends with an embedded expression or escaped embedded expression and if the responderhtmlpage is specified in the Add Responder Action command, it causes a NetScaler appliance to fail.

  [From Build 64.9] [# 640075]

- When a NetScaler appliance sends out full sized persist probe packet that is more than the client advertised window, firewall drops the packet causing the connection to fail.

  [From Build 64.9] [# 576980]

- During a TCP transaction, when the client advertises zero window to a NetScaler appliance, the appliance periodically sends zero window probe to ascertain if the client can open the window so that the NetScaler appliance can send in new data. When sending such a probe, the appliance sends a full maximum segment size (MSS) packet during first probe and from the second probe onwards, sends a 1-byte packet. If the client does not open the window after sending such a probe, but instead sends a TCP Reset or if the connection on the NetScaler appliance gets flushed for other reasons, then it may lead to duplicate buffer free on the appliance that might cause the appliance to fail.

  [From Build 64.9] [# 657742, 657753, 657771, 658352, 658507, 658526, 659842, 659849, 660345, 660812, 660998, 661018, 661266, 661511, 662353, 662493]

- If an imported responderhtmlpage content ends with an embedded expression or escaped embedded expression and if the responderhtmlpage is specified in the Add Responder Action command, it causes a NetScaler appliance to fail.

  [From Build 64.9] [# 629091]

- When parsing a host name with no Path component, the URL parsing logic does not search for a question mark (?), so an entire string might be interpreted as the host name. This causes an error when the appliance tries to resolve the DNS name. With this fix, the parsing logic searches for question marks.

  E.g.:
  http://example.com.php?&curuserid=94315577&host=wscdny203.live.changba.com&token=T59d105c1c74042e&localip=221.235.187.75&clientip=80.95.239.1&bless=1&channelsrc=market_%E7%99%BE%E5%BA%A6

  [From Build 64.9] [# 587858]

- An invalid compressed header in SPDY frames causes a NetScaler appliance to restart.

  [From Build 64.9] [# 637651]

- The Configd daemon fails if the number of session IDs exceeds the preset limit and existing client sessions are renumbered.

  [From Build 64.9] [# 639380, 657168, 657781]

User Interface

- Configuration Utility

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

  [From Build 55.8] [# 527388]

- SSL

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

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

- Configuration Utility

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

  [From Build 55.8] [# 520751]

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

  [From Build 55.8] [# 440208]

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

  [From Build 56.22] [# 524080, 448724]

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

  [From Build 56.22] [# 516162, 358664, 538009, 540912, 542248, 542721, 546566, 549368]

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

  [From Build 56.22] [# 536544]

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

  CB management service (SVM) causes failure due to memory leak..

  [From Build 59.13] [# 565742, 573215, 576357]

XML

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

  [From Build 52.11] [# 450232]

Release History

For details of a specific release, see the corresponding release notes.

- Build 65.11 (2017-01-27) (Current build)
- Build 64.9 (2016-10-19)
- Build 63.8 (2016-06-23)
- Build 62.9 (2016-04-20)
- Build 61.11 (2016-02-06)
- Build 60.7 (2015-11-18)
- Build 59.13 (2015-09-08) Replaces: 59.11
- Build 58.11 (2015-07-16)
- Build 57.7 (2015-05-18)
- Build 56.22 (2015-03-30) Replaces: 56.21
- Build 55.8 (2015-02-02)
- Build 54.9 (2014-12-17)
- Build 53.9 (2014-11-14)
- Build 52.11 (2014-11-03)
- Build 51.10 (2014-11-03)
- Build 50.10 (2014-10-21)