Citrix NetScaler 1000V Release Notes

Citrix NetScaler 11.0-66.11
First Published: 2016-05-31

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

11.0-66.11

The release notes provides the changes or enhancements, issues that are fixed, and known issues that exist in Build 66.11. The list of known issues is cumulative, that is, it includes known issues that existed in previous builds and issues that are newly found in this build.

Release history:

- Build 66.11 (2016-05-25) (Current build)
- Build 65.31 (2016-03-14)
- Build 64.34 (2015-12-30)
- Build 63.16 (2015-10-07)
- Build 62.10 (2015-08-12)
- Build 55.20 (2015-06-30)

What's New?

The enhancements and changes that are available in Build 66.11.

NetScaler Insight Center

- NetScaler Insight Center is now supported on KVM hypervisors.
  [# 631295]

Bug Fixes

The issues that are addressed in Build 66.11.

AAA-TM

- You cannot add an authentication virtual server as the target of a content switching virtual server in a partition.

  [# 624063]

- If you add a Negotiate Server with a Keytab file with a GUI, an error is issued: "Error in retrieving file. Directory does not exist." The error is only issued when it is executed within partition.

  [# 620774]

- 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.

  [# 623005]

Admin Partitions

- In a partitioned NetScaler appliance, for GSLB services that point to a local load balancing virtual server, the monitors that are bound to that GSLB service fail. Also, connection proxy between local load balancing virtual servers does not work.

  [# 613751]

Application Firewall

- 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.

[# 561845, 620915]

- In a cluster deployment, the NetScaler web application firewall (WAF) fails if starturl closure is enabled.

  [# 617680]

- After an upgrade from release 10.5 to a release 11.0 build, uploading a Word document triggers false positives for application firewall SQL and XSS violations during the file upload operation. With this fix, the behavior is the same as in 10.5. The application firewall inspects text, Javascript , HTML, XML and JSON contents when a file is uploaded. It doesn't inspect any other contents.

  [# 619354]

- On a partitioned NetScaler appliance, connections for incoming requests might be reset if the application firewall feature is enabled.

  [# 622826]

- In a cluster setup, while exporting application firewall learnt data, you might see the following error message:

  "communication error with aslearn"

  This message is because of a schema difference.

  [# 625807]

- The NetScaler appliance fails if you enable or disable the IP Reputation feature in any partition other than the default partition.

  [# 627505, 628073]

- 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.

  [# 628525]

- The secondary node in an HA deployment attempts to directly connect to AWS for signature auto updates. Instead, it should sync from the primary node.

  [# 617314, 628030]

- 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.

  [# 628789]

- The application firewall's SQL Injection special-character transform does not work properly if either of the following parameters is enabled in a profile:

  -crossSiteScriptingTransformUnsafeHTML

  -SQLInjectionTransformSpecialChars

  [# 617614, 624646, 624653]

- 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.

  [# 612284, 619056, 638110]

- When the application firewall cookie proxy check is enabled, the NetScaler appliance might become unresponsive while updating the cookies in the distributed hash table with a set of cookies from the server.

  [# 609394, 618385]

- 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.

  [# 603473]

- The NetScaler application firewall terminates the connection when the request comes with a tampered session cookie and the cookie protection is enabled.

  [# 574498, 591172]

Cache Redirection

- If a request to a cache redirection virtual server resolves to an IP address that belongs to a content switching virtual server configured on the NetScaler appliance, the appliance might fail.

  [# 621522, 626848]

- In the GUI, the Policy drop-down list does not display the cache redirection policies.

  [# 622402]

Cluster

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

[# 618663]

- 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.

  [# 614718, 615459]

Command Line Interface

- 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>.

  [# 554652, 596571]

DNS

- 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.

  [# 559064]

DataStream

- 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.

  [# 613239, 616404]

GSLB

- 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.

  [# 610065]

- 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.

  [# 615886]

Integrated Caching

- 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.

  [# 621356, 631356]

Load Balancing

- In a high availability setup in admin partition mode, the persistent sessions are not synchronised to the secondary node after performing force ha sync or force failover operation.

  [# 630344]

NITRO API

- If a large number of concurrent NITRO requests are issued, many requests time out.

  Workaround: Do not allow more than 20 NITRO calls at any given point.

  [# 616433]

NetScaler GUI

- The Goto Priority Expression field is missing for a Traffic Management session policy bound to a AAA user or group under Netscaler > Security > AAA > Policies > Session.

  [# 629828]

NetScaler Insight Center

- NetScaler Insight Center might intermittently become unresponsive and not populate any reports.

  [# 618370, 622539, 631395]

- In Security Insight, there might be a delay in receiving the safety profile configuration data for some applications.

[# 628733]

- The NetScaler appliance might become unresponsive or experience intermittent HA failovers under some ICA network conditions.

  [# 623729, 623379]

- In HDX-Insight, the location of public IP addresses is not displayed on the geo map.

  [# 631633]

Networking

- FTP in passive mode does not work in this build.

  [# 631929, 636586, 640213]

- The NetScaler appliance might fail if secure management access (HTTPS) is enabled on a SNIP6 address that is configured for a traffic domain.

  [# 618633]

- 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.

  [# 614786]

- The NetScaler appliance does not retain the entire 64 bit ID of IPv6 fragments of a session. As a result, the session might fail.

  [# 614042]

Policies

- A memory leak occurs when a responder action has blocking expressions (for example, stream analytics, HTTP callout, matches_location) and body or payload based expressions.

  [# 598252, 623764, 624637, 624759, 629247, 629344]

- Rewrite action block leading to subsequent action time outs.

  If multiple rewrite policies evaluate to TRUE for a particular protocol and direction (for example HTTP request or TCP response), and more than one associated action is selected for execution, they might not all execute. If one of the actions is suspended (blocked), the next selected action will time out, and any subsequent actions will be skipped.

The following functions in expressions can block:

* HTTP_CALLOUT

* MATCHES_LOCATION

* STREAM

* CHECK_LIMIT

* MATCHES

* BODY

* PAYLOAD

* MSSQL

* MYSQL

* ORACLE

* SUBSCRIBER

* DETERMINE_SERVICES

* Use of variables (in other words, $<variableName>)

Note: These expressions can block, depending on specific conditions that occur at the time of execution.

[# 628326]

SSL

- 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.

  [# 625966]

- The NetScaler appliance fails if it parses the value of an unknown certificate extension while the certificate is loading.

  [# 623996]

System

- A configuration loss occurs when you upgrade Content Switching (CS) entities above the following limits:

  Memory allotted to a packet engine 2GB 4GB

  Max number of content switching virtual servers 1200 2500

  Max number of content switching policies 1500 3500

  Max number of content switching virtual server bindings 3000 4000

  [# 628528]

- 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.

  [# 624327]

- 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.

  [# 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.

  [# 543293, 578993, 579965, 593378, 599535, 608479, 614368, 628579, 628763, 634338]

- 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.

  [# 605873]

- The "start nstrace" command has a new parameter, -capsslkeys, with which you can capture the SSL master keys for all SSL sessions. If the capsslkeys option is enabled, a file named nstrace.sslkeys is generated along with the packet trace and imported into Wireshark to decrypt the SSL traffic in the trace file.

  [# 603225]

- The NetScaler Weblog client intermittently fails because of incorrect indexing, leading to segmentation failure.

  [# 615895, 620767, 629214]

- A NetScaler appliance fails when an MPTCP subflow receives an Infinite DSS mapping in a partially retransmitted packet.

  [# 623426]

Telco

- In a high availability deployment with LSN and DS-Lite configuration, LSN and DS-Lite mappings for active FTP connections are not removed from the secondary node even after they time out or are flushed.

  [# 601920, 619864]

Known Issues

The issues that exist in Build 66.11.

AAA-TM

- When the NetScaler appliance is configured as a SAML Identity Provider (IdP) with Negotiate/Kerberos, authentication fails if you are running a client debugger such as Fiddler, that does not send negotiate headers.

  Workaround: Do not use Fiddler or a similar client debugger in such use cases.

  [# 576792]

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

  [# 551091]

- You cannot load balance external AAA servers, such as LDAP, RADIUS, or TACACS servers, in a non-default partition.

  [# 621010]

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

  [# 617370]

- The NetScaler appliance exhibits some inconsistency in the way expired cookies (TEMP) are handled:

  - On an existing TCP connection, access to backend resources is allowed.

  - On a new TCP connection, the request is denied.

  [# 610091]

- Forms based authentication on NetScaler failed once in 11.0 62.x. However, it never resurfaced. Users are advised to use later versions of 11.0.

  [# 584090]

Admin Partitions

- When a user is authenticated, the persistence cookie is set, and any subsequent request that includes the cookie and matches the basic pattern is granted access to the server. However, in a non-default partition, if you specify a value for the ns_aaatm_tempc_allow_patterns default pattern set, the value is ignored.

  [# 623404]

- RPCSVR services cannot be configured in admin partitions.

  [# 498477]

- The following two issues can occur if you add an external group as a system group on a NetScaler appliance and use the â€œset system groupâ€• command to configure the prompt string and timeout parameters at the system group level:

  1. Session timeout â€“ When a user from an external group logs on to the NetScaler command line interface (CLI), the session timeout set for the group is not applicable to sessions in the default and non-default partitions. However, if you configure the timeout parameter by using the â€œset system parameterâ€• or â€œset cli mode -timeout <seconds>â€• commands, the session times out as specified.

  2. Prompt string missing â€“ When a user from an external group logs on to the NetScaler command line interface (CLI), the prompt string does not appear in the default and non-default partitions. For example, in a default partition, instead of "<pstring>" only ">" appears, and in a non-default partition, instead of "<pstring-partitionname>" only "partitionname>" appears.

  However, if you set the prompt string by using the "set system parameter" or "set cli prompt" commands, the prompt string is displayed. For example, cliprompt> appears in a default partition, and cliprompt-partitionname> appears in a non-default partition.

  [# 632193, 632460]

- After adding an admin partition, make sure you save the configurations on the default partition. Otherwise, the partition setup configurations will be lost on system reboot.

  [# 493668, 516396]

- The auto synchronization of GSLB configuration fails if the local and remote GSLB sites are configured on two different partitions of a NetScaler appliance.

  [# 626958]

- Admin partitions are not supported on FIPS appliances. However, owing to this issue, you can create admin partitions on FIPS appliances. You are advised against creating such partitions as they will not function properly.

  [# 517145]

- In a non-default partition, if the network traffic exceeds the partition bandwidth limit, the FTP control connection fails but data connection remains established.

  [# 620673]

- With stateful connection failover configured on a partitioned NetScaler appliance, heavy FTP traffic and frequent failovers can cause the appliance to become unresponsive and fail.

  [# 612215, 482310, 598576]

AppFlow

- The NetScaler appliance does not export L7 AppFlow records when using HTTP/2.

  Workaround: Disable AppFlow or specify HTTP/1.1.

  [# 621721]

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

  [# 629223]

- 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.

  [# 552655, 563387]

Application Firewall

- In a high availability (HA) deployment, a memory leak can occur if auto-update of application firewall signatures is enabled or you update the signatures by using the -mergedefault option.

  [# 620878, 629043]

- When editing application firewall signatures, you cannot sort on the "Enabled" column.

  [# 621333]

- 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.

  [# 610116, 547969, 603473]

- In a high availability (HA) deployment with application firewall signatures configured on the NetScaler appliances, a file synchronization issue can lead to mismatched schema versions, which can affect signature management and functionality after a firmware upgrade to install a new build.

  Workaround: If you have not yet upgraded your firmware, perform the first of the following procedures. If the firmware has already been upgraded, perform the second procedure.

  Recommended procedure for upgrading the firmware in an HA deployment if application firewall signatures are configured

  1. Before you upgrade the firmware, disable Signature auto-update (if set).

  2. Drop into the shell from the CLI and delete the /nsconfig/updated_signatures.xml file (if present) from the primary appliance first, and then from the secondary appliance.

  3. Proceed with the recommended HA rolling upgrade procedure

  Recommended workaround if you have already done the firmware upgrade without the above steps and have encountered the issue

  1. Drop into the shell from the CLI and delete the /nsconfig/updated_signatures.xml file from the primary appliance, and then delete it from the secondary.

  2. On the primary, use the GUI to export all user-defined signatures from the primary and save them in a local file.

  3. Unbind the signatures from the profile(s) if already bound.

  4. Delete all user-defined signatures.

  5. Use the GUI to import all the signatures that you saved in the local file.

  6. Bind the signatures to the target profiles.

  [# 628064]

- 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]

- The application firewall learning engine is not able to connect to the packet engine in certain circumstances. When this happens, the aslearn process does not start and the application firewall learning functionality stops working.

[# 576713, 582879]

- 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]

- Application firewall memory allocation failures might occur, when the integrated cache is also enabled and the memory usage limit for the cache parameter is set to a high value.

  [# 567119, 568260]

- The application firewall learning engine stops recommending new rules when the learning database grows to approximately 20-22 megabytes in size. The database size limit is applied on a per profile basis.

  [# 554591]

- 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]

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

  show appfw JSONContentType

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

  > show appfw JSONContentType

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

  Done

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

  > show appfw JSONContentType

Done

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

add appfw JSONContentType ^application/json$ -isRegex REGEX

show appfw JSONContentType

[# 430014]

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

  [# 530277]

- On a NetScaler appliance that has standalone application firewall license, when you bind a classic application firewall policy to a load balancing virtual server, an error message is displayed in the graphical user interface. The binding operation is successful. The error message is harmless and can be safely ignored.

  [# 522712]

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

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

  [# 511254]

- The cookie consistency behavior has changed in release 11.0. In earlier releases, the cookie consistency check invokes sessionization. The cookies are stored in the session and signed. A "wlt_" suffix is appended to transient cookies and a "wlf_" suffix is appended to the persistent cookies before they are forwarded to the client. Even if the client does not return these signed wlf/wlt cookies, the application firewall uses the cookies stored in the session to perform the cookie consistency check.

  In release 11.0, the cookie consistency check is sessionless. The application firewall now adds a cookie that is a hash of all the cookies tracked by the application firewall. If this hash cookie or any other tracked cookie is missing or tampered with, the application firewall strips the cookies before forwarding the request to the back end server and triggers a cookie-consistency violation. The server treats the request as a new request and sends new Set-Cookie header(s).

[# 571943]

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

  [# 510509]

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

  [# 506653]

- 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.

  [# 505272, 505039]

- If you use the NetScaler GUI to access the application firewall security check violation log messages from a profile, the syslog viewer cannot display the logs if they are not in the CEF log format. You can enable CEF logging from the application firewall settings pane in GUI the or use the following command from CLI:

  > set appfw settings CEFLogging ON

  [# 630056]

- If a user request triggers an application firewall policy that is bound to the APPFW_BYPASS profile, the application firewall might fail to generate an SNMP alarm.

  [# 489691]

- On a NetScaler appliance running release 11.0 or later, the web application firewall (WAF) does not always function as expected if the DefaultCharset in a profile is not specified correctly. If a request does not have a content-type header, the WAF uses the DefaultCharset specified in a profile.

  [# 624978]

- The application firewall has memory limitations on the size of a WSDL that can be imported into the NetScaler appliance. The import operation might fail if the size of the WSDL file exceeds the allocated memory.

  [# 349504]

Audit Logging

- During synchronization and saving a system configuration, if Cache Redirection (CR) policy is configured before an audit message action, it results in an improper sequence of CR policy and audit message actions.

  [# 622905]

Cache Redirection

- In a cluster deployment, if a request is received by a node other than the node on which the client request is received, a packet loop delays the response to the request.

  [# 591265]

Clustering

- When WIonNS is deployed in a cluster setup, an error is thrown when you rename a service that points to the IP address of the cluster configuration coordinator.

  [# 583424]

- When a cluster is connected to more than one upstream router:

  - When AS OVERRIDE is not configured on the upstream router, spare nodes will learn VIP routes from one of the routers, but they will be dropped as the path contains its own AS to prevent loop formation.

  - When AS OVERRIDE is configured on any upstream router for cluster neighbors, upstream router will change AS path in VIP to its own AS while sending updates to cluster neighbors. Spare nodes will not detect any loop and learnt VIP routes are advertised to other routers.

  Spare nodes will not advertise their configured VIP routes but there is no such restriction on BGP learnt routes.

  [# 547749]

- When WIonNS is deployed in a cluster setup, if the service IP address is modified using the "set" command, the "show" command continues to display the previous IP address.

  [# 582805]

- When WIonNS is deployed in a cluster setup, an error is thrown if you change the IP address of the WI service to point to the IP address of the cluster configuration coordinator.

- [# 582801]When L2 mode and MBF is enabled in a cluster deployment, access to * 80 services can fail intermittently.

  [# 479899]

- When a node is removed from a L3 cluster, IPv6 SNIP addresses and routes are being erroneously cleared from the appliance. This behavior is seen only for IPv6 entities. IPv4 SNIPs and routes are not being removed from the appliance.

  [# 542693]

Command Line Interface

- When you use the Net::SSH::Perl library to connect to the NetScaler appliance, and run a command where an argument has a @ character, an error message appears indicating that the argument does not exist.

  For example, an error message appears if you use the @ character in the tacacsSecret parameter of the following command:

  > set authentication tacacsAction TACACS-0101 -tacacsSecret Sl4make5f0rd@enc5

  Workaround: Use one of the following alternate approaches:

  - If you use the Net::SSH::Perl library, include double quotes around the command when calling $ssh->cmd().

  - Use the Net::Telnet library.

  - Use the Net::SSH::Expect library.

  [# 346066]

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

  [# 512526, 527066, 545578, 631658, 635938]

Configuration Utility

- You cannot upgrade to NetScaler 11 from the following builds by using the Upgrade Wizard of the NetScaler GUI:

  - All builds of NetScaler 9.3

  - All builds of NetScaler 10.1

  - Any build before Build 57.x of NetScaler 10.5

  Workaround: Use the command line interface to upgrade the NetScaler appliance.

[# 563410]

DNS

- In a deployment with heavy DNS traffic and many DNS cache entries, some entries in the cache might not get updated or deleted, even after the TTL expires.

  [# 619124, 622308]

- 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]

GSLB

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

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

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

  [# 530638, 506432]

- In a typical GSLB deployment, when internal user logon is disabled, GSLB auto sync uses SSH keys to synchronize the configuration. In a partitioned environment, however, GSLB auto sync cannot use SSH keys to synchronize the configuration across the GSLB sites.

  Workaround: To use GSLB auto sync in partitioned environment, enable internal user logon and make sure that the partition user name is the same at the local and remote GSLB sites.

  [# 625997]

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

  Workaround: Manually update the server name in the other GSLB sites.

  [# 511994]

- On a NetScaler appliance, the default memory allocation is 10 MB per partition. In certain use cases, the allotted memory might not be sufficient for adding the maximum number of entities. You can increase the memory allocation by running the following command:

set partition <partition_name> -MaxMemLimit <limit>

For example, To increase the partition memory allocation to 50MB, at the NetScaler command prompt, type:

set partition p1 -MaxMemLimit 50

[# 614357]

High Availability

- If you upgrade a NetScaler appliance in a high availability (HA) setup to the latest build of the same release, HA synchronization and command propagation are disabled during the upgrade process. However, after both the appliances are upgraded to the same NetScaler software version, HA synchronization and command propagation are enabled automatically.

  [# 611197]

Integrated Cache

- The IC memory once set for an admin partition, cannot be reduced. An appropriate error message is displayed.

  For example, if the IC memory of admin partition is 10 GB, you cannot reduce it to 8 GB. The memory limit can however be increased to a required value.

  [# 568106, 570578]

- A NetScaler appliance fails multiple times after a cache parameter is enabled during an HA persistency test.

  [# 616635]

- After an upgrade, Content Acceleration feature is not supported.

  [# 597415]

Load Balancing

- A subscriber cannot initiate more that eight simultaneous sessions.

  [# 568052]

- IPV6 addresses are trimmed when data is retrieved from the packet engine because the prefix length variable is unset during the GET operation.

  [# 573463]

- When displaying the results of the "show lb monitor" command, the numbering of the user-defined monitors restarts from 1 instead of continuing the numbering from the list of built-in monitors.

  [# 511222]

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

  [# 540965]

- 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.

  [# 622807]

- The NetScaler appliance does not support an outbind operation. That is, the appliance does not support an operation in which the message center initiates an SMPP session to an ESME.

  [# 500169]

Monitoring

- If the IP address and port of a dispatcher for a user monitor are set to the IP address and port of a service, and this service is later deleted, the appliance fails if you try to add a service with the same IP address and port.

  [# 618052]

NITRO API

- For external users that require challenge-response, authentication through NITRO does not work.

  [# 558715]

- When using the .NET SDK, the application cannot establish HTTPS connection with the NetScaler appliance. This is a result of some certificate validation issues.

  [# 611316]

- 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

[# 591970, 597032]

NetScaler GUI

- The bridge group and VLAN association is not displayed in the network visualizer.

  [# 542214]

- An interface does not appear as tagged or untagged in the network visualizer.

  [# 540980]

- If you specify an invoke label, such as policy label or virtual server, in your policy you cannot view the details of the invoke label directly.

  Workaround: Select the invoke label and click Edit.

  [# 635940]

- In the network visualizer, if you click a tagged interface that is part of two or more VLANs, only the VLAN at the top of the list of bound VLANs is highlighted.

  [# 541011]

- In the NetScaler GUI, the page at System> Network > IPs does not display the Type for LSN NATIPs, and the value shown for Traffic Domain is incorrect.

  Workaround: Run the sh nsip command to display the values in the command line interface.

  [# 505121]

- The Surge protection feature cannot be configured in an admin partition. Since, surge protection parameters are part of the Change Global System Settings (System > Settings) dialog, when you try to update the global settings, the "Operation not supported" message is displayed.

  [# 498004]

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

  [# 452669, 391434, 453555, 453597, 478131, 479434, 481397, 502720, 573976, 622724]

NetScaler Insight Center

- When Web Insight displays URL records, the maximum size of a URL is limited to 1472 bytes.

  [# 500108]

- If you export CSV files of WAN Insight reports, many of the fields in the CSV files might be empty.

  [# 547380]

- When, during a scale-out deployment of NetScaler Insight, you configure the database and connector nodes and register them with the Insight server, the console might display error code 0003 for the connectors and databases.

  [# 631504]

- If the ICA Rtt column is the column in extreme left of the session details table, the pop-up box gets cropped in display.

  [# 573089]

- Hiding or displaying a URL, or changing the configuration, might take longer than expected.

  [# 570896, 574278]

- Unexplained failure of a NetScaler appliance. The issue has been assigned and is being investigated.

  [# 634906, 637383, 638170, 641156]

- In NetScaler Insight Center, export functionality is not supported in Security Insight.

  [# 618208, 618216]

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

  [# 505865]

- Web Insight includes geo data in daily, weekly, and monthly reports only.

[# 556534]

- Adding a new database node is now driven by auto-registration. When a kernel is imported, it requests input from user and auto-registers with the NetScaler Insight Center server. Removing a database node is currently not supported.

  [# 543632, 565706, 567628, 570264]

- NetScaler Insight Center does not report an application-launch failure caused by a user trying to launch an application or desktop to which the user does not have access.

  [# 609604]

- Security Insight might display an incorrect total-violations count for some applications, because of a delay in receiving the safety profile configuration data.

  [# 627373]

- In NetScaler Insight Center, the Postgres database might become unresponsive if there are any hardware related faults in the Insight Center system.

  [# 579097]

- If you select Enable URL Data Collection in the Web Insight URL Data Collection Settings, the NetScaler Insight Center virtual appliance's available memory reduces rapidly.

  [# 638324]

- In NetScaler Insight Center, the Google geo chart sometimes does not display all regions.

  [# 537007]

- In NetScaler Insight Center, some countries are not displayed on the Google geo chart.

  [# 537003]

- If you have configured the ICA session timeout value to a high value, say 10 minutes or more, and there is no traffic flow from the NetScaler appliances, neither the timeline chart nor the tabular chart displays any data. However, the Active sessions and Active Desktops columns display the data until the ICA session timeout occurs.

  [# 536056]

- Insight Agent should only be added after configuring and deploying Insight DB Cluster.

[# 570619]

NetScaler VPX Appliance

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

  [# 592395]

Networking

- In a high availability (HA) setup, high latency might occur during configuration synchronization, resulting in some configurations not getting synchronized to the secondary node. In this situation, an HA failover results in loss of configuration.

  [# 607929]

- A TCP connection involved in INAT times out at 120 seconds, regardless of what global timeout value you set for TCP client and server connections. For example, the connection times out at 120 seconds even after you run the following command:

  set ns timeout -anyTcpClient 50 -anyTcpServer 50

  [# 569874]

- For an RNAT connection, the NetScaler appliance drops the first packet that the server sends to the client.

  [# 543171]

- 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.

  [# 485260]

- In a cluster environment, vPath encapsulation may fail when MAC based forwarding is enabled.

  [# 580137]

- 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.

  [# 625841]

- If you configure an INAT rule with the useproxyport parameter disabled, connections to the server fail if the source port is in the reserve port range (0-1023).

[# 550488]

Platform

- If you add an NTP time server by specifying the server name (host name), and the ns.conf file is very large, the result is a race condition in which the NTP daemon (NTPD) is started before host name services are ready.

  Workaround: Do one of the following:

  -Restart the NTP daemon after starting the NetScaler appliance.

  -Add the NTP server by specifying the IP address of the server instead of specifying the host name.

  [# 573306]

- Interfaces on NetScaler VPX appliances are not hot-pluggable, except on NetScaler VPX appliances running on Amazon AWS.

  Workaround: Shut down the NetScaler VPX appliances before adding or deleting the interfaces.

  [# 578198]

Policies

- The command for configuring a content filtering action is being saved in a wrong order in the ns.conf file. Service is a mandatory parameter for adding a add content filtering action, but the add content filter action command is saved before the command that adds the service. As a result, when the build is upgraded, the content filtering action is not configured as required.

  [# 603551]

- While evaluating default syntax expression for local time zone, a NetScaler appliance incorrectly applies US daylight savings time (DST) rules in non-US timezone. 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 timezone is between 0800 and 1700. In the UK timezone, 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

- If you bind a certificate-key pair to a DTLS virtual server, the following incorrect error message might appear. Ignore it. No usable ciphers configured on the SSL vserver

  [# 542973]

- FIPS keys that are created on firmware version 2.2 are lost after you downgrade to firmware version 1.1.

  Workaround: Export the FIPS keys before you downgrade the firmware. Import the FIPS keys after the downgrade.

  [# 559796]

- 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 â€œAuthorizationsâ€□ is incorrect. It should be â€œAuthentications.â€□

  [# 627635]

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

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

  ERROR: Processing of certificate bundle file failed.

  Workaround: Specify only the file name. For example,

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

  [# 481878, 521933]

- If importing a certificate-key file fails because of a wrong file, and you run the command again with the correct file, the operation fails and the following error message appears:

  "ERROR: Import failed. Another resource with the same name being processed"

  Workaround: Import the file with a different name.

  [# 526433]

- 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]

- Adding a certificate revocation list (CRL) on the NetScaler appliance fails with the error message "Certificate Issuer Mismatchâ€□ for a DER certificate, and with the error message "Invalid CRLâ€□ for a PEM certificate. This issue is seen because the attribute type of the common name field for the CA certificate and the CRL are different.

  [# 623058, 634017]

- Even though the clientAuthUseBoundCAChain parameter can be enabled and disabled in the backend profile, it is supported only on the front end profile.

  [# 554782]

- Server Name Indication (SNI) is not supported on a DTLS virtual server. However, if you enable SNI on a DTLS virtual server, an appropriate error message does not appear.

  [# 572429]

- Even though TLS protocol versions 1.1 and 1.2 are not supported by firmware version 1.1, the protocols incorrectly appear as enabled by default on an SSL virtual server.

  Workaround: Disable TLS1.1/1.2 explicitly on the virtual server.

  [# 576274]

- The number of SSL cards that are UP is not displayed in the non-default partitions. Because SSL cards are shared between the default partition and the non-default partitions, the total number of SSL cards that are UP in all the non-default partitions is equal to the number of cards that are UP in the default partition.

  [# 628914]

- If you have configured an SSL_Bridge type service and bound an HTTPS monitor to it, an SSL handshake with an IIS server that uses the TLS v1.2 protocol fails. This is because the handshake requires a signature algorithm in the client hello.

  [# 628341]

- A certificate signing request (CSR) created by using the configuration utility might not be usable if you have not specified a common name.

  [# 588275]

- If you have configured a DTLS virtual server and also enabled the Default profile, clearing the configuration might cause the appliance to fail.

Note: On some STA services, if you enable DTLS, you donâ€™t have to explicitly create a DTLS virtual server, because it is automatically created. The automatically created DTLS server does not cause the configuration to fail if the Default profile is enabled.

[# 622916, 625989, 632989, 634897, 639567]

- The output of the "stat ssl vserver" command includes the statistics for non-SSL virtual servers.

  [# 627650]

- Secure renegotiation using SSLv3 protocol fails on MPX-FIPS appliances running firmware version 2.2.

  [# 550788]

Security Insight

- Security Insight uses late accounting for historical reporting. When you view the reports in the dashboard, you might observe the following behavior for the selected duration options:

  [1] 1 hour: Data for security violations triggered in last 1 minute might not be included.

  [2] 1 day: Data for security violations triggered in last 1 hour might not be included.

  [3] 1 week: Data for security violations triggered in last 1 day might not be included.

  [4] 1 month: Data for security violations triggered in last 1 day might not be included.

  [# 619713]

System

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

  [# 524320, 630772]

- A memory-availability check can result in TCP optimization being bypassed for an incoming connection when memory being used by other data structures (for example, PCB) and later freed. When this issue occurs, TCP optimization does not resume until you warm reboot the appliance.

  [# 629865]

- The NetScaler appliance might fail after it frees session entries for long lived TCP connections.

  [# 626027]

- When client sends a small window size (less than 8190 bytes) in its request packet to a NetScaler appliance, the appliance advertises a window size of 8190 bytes to the back-end server. Upon receiving this information, the server sends up to 8190 bytes of data to the appliance, and in turn the appliance, in transparent mode, sends the same amount of data to the client, even if the actual window size is less than the window size advertised by the client. If a device between the appliance and client checks the window size before accepting the data, that device might drop the data that does not fit in the clientâ€™s window size.

  Workaround: Enable the end point device (for example, TCP Buffer) in the NetScaler appliance.

  [# 622573]

- Modify interface operations are not supported with Cisco BD qsfp.

  [# 634273]

- For a client connection to a TCP virtual server, the NetScaler appliance incorrectly decrements the current number of client connections counter even when the TCP connection is terminated before the 3-way handshake is completed. The appliance incorrectly displays a large positive number of client connections even when there are no clients connected to the virtual server.

  [# 622309]

- After the 11.0 upgrade, frequently the secondary node becomes unreachable and goes into an 'unknown' state. The NetScaler appliance must be rebooted from the LOM to get back connectivity.

  [# 609401, 601816, 616054, 628184]

- The default setting for auto-negotiation is 'OFF', which causes an error if you configure the interface from the SVM.

  [# 598688]

- In previous releases, evaluation of an interface-based expression was based on the information available in the connection block and in the individual frame. Now, only the information in the frame is considered, and this information can change during the course of a transaction. As a result, the evaluation might be incorrect.

  Workaround: Use VLAN-based expressions instead.

  [# 597312]

- In a high availability environment, if you add Network Time Protocol (NTP) to a primary node by specifying the NTP server's DNS name, the command is not propagated to the secondary node.

  Workaround: Specify the NTP server's IP address.

[# 639529]

- If the maximum memory limit of a TCP Buffer (TCPB) is unequally divided among Packet Engines (PE) running on a NetScaler appliance, the PE will install the TCPB on a TCP connection without sufficient memory buffer. This leads to a connection reset.

  [# 587114]

- 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]

- In an Openstack Environment, if a custom flavor with an Ephemeral Disk of Size of less than 8GB is used to a start a NetScaler VPX or Cisco Nexus 1000v instance, the config drive is not attached to the instance.

  [# 578366]

- The updated host name for a NetScaler appliance does not appear on the LCD panel until after the appliance is restarted.

  [# 560854]

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

  [# 518272]

- The initial client connection on the NetScaler appliance might fail if a wildcard virtual server is configured and the useProxyPort option is disabled globally on the appliance.

  [# 542776, 571357]

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

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

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

  [# 545858]

- After an upgrade, a system user is unable to log on to a NetScaler appliance.

[# 619980]

Telco

- In a Large Scale NAT deployment, the NetScaler appliance does not generate and send an ICMP error message to the subscriber in the event of a port allocation failure.

  [# 540162]

- In a DS-Lite configuration with a server behind the B4 device, the NetScaler appliance does not properly process FTP packets that have the following set of characteristics:

  * Are from clients on the Internet

  * Are destined to the server

  * Match DS-Lite static NAT maps configured on the NetScaler appliance

  [# 601560]

- In an LSN deployment, FTP over Jumbo interfaces might not work.

  [# 503177]

- In the output of the "show lsn sipalgcall -callid" command, the port value of the SIP control channel is incorrect.

  [# 574257]

- An RTSP request might be logged on two different Syslog servers.

  [# 581086]

- If the provisional response to a SIP REGISTER message does not contain an expiry value, the NetScaler appliance drops the message.

  [# 574725]

Web Interface on NetScaler (WIonNS)

- If a SNIP address is added to subnet other than the one that includes the NSIP address, loop-back services go down.

  [# 585655]

- Since the install wi package command takes more than usual time to complete, it is not possible to return the status from other nodes. Hence it is required that all the WI related packages, that is, JRE+WI be present on system on the same path for all the nodes.

  [# 507753]

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

  [# 601304]

- **OpenJDK version for Web Interface on NetScaler (WIonNS)**

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

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

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

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

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

  [# 464854]

What's New in Previous NetScaler 11.0 Releases

The enhancements and changes that were available in NetScaler 11.0 releases prior to Build 66.11. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

Admin Partitions

- **Stateful Connection Failover/Mirroring Support in Admin Partitions**

The NetScaler appliance now supports stateful connection mirroring in admin partitions. You can now deploy TCP-based applications in an admin partition, so that failure of one NetScaler appliance does not make the application unavailable.

Note: The application must be deployed in a NetScaler high availability (HA) setup, and connection mirroring must be configured for the application.

[From Build 65.72] [# 599629]

- **GSLB Support in Admin Partitions**

  The NetScaler appliance now supports the GSLB feature in admin partitions. You can now deploy, with an admin partition, applications that need the GSLB feature to distribute traffic across globally located datacenters.

  [From Build 65.72] [# 436582, 405290, 504574, 506221]

- **AAA-TM Support in Admin Partitions**

  The NetScaler appliance now supports the AAA-TM feature in admin partitions. You can now deploy, with an admin partition, enterprise applications that require authenticated access.

  [From Build 65.72] [# 481384]

Application Firewall

- NetScaler now supports the IP Reputation feature, which is useful in identifying an IP address that is sending unwanted requests. You can use the IP reputation list to preemptively reject requests that are coming from an IP with a bad reputation. NetScaler uses WebRoot as the service provider for the dynamically generated malicious IP database and the metadata for those IPs. The IP Reputation feature can be configured by using PI Expressions in a policy. For example, you can configure an application firewall policy using expressions such as: CLIENT.IP.SRC.IPREP_IS_MALICIOUS.

  [From Build 65.72] [# 580866]

NetScaler Insight Center

- The following thin clients now support HDX Insight:

  -WYSE Windows based thin clients

  -WYSE Linux based thin clients

  -WYSE ThinOS based thin clients

-10Zig Ubuntu based thin clients

[From Build 65.72] [# 614892, 550997, 604388, 620422, 632370]

- **Viewing the GET or POST requests**

  The NetScaler Insight Center now displays the GET or POST requests that are sent by the client to a domain. To view the GET or POST requests, navigate to Domains > URLs > Clients > Http Request Method, or to Domains > URLs > Http Request Method > Clients.

  [From Build 65.72] [# 620323]

- **Security Insight**

  Web and web service applications that are exposed to the Internet have become increasingly vulnerable to attacks. To protect applications from attack, you require visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures. Security Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

  Security insight is included in NetScaler Insight Center, and it periodically generates reports based on your Application Firewall and NetScaler system security configurations. The reports include the following information for each application:

  -Threat index. A single-digit rating system that indicates the criticality of attacks on the application, regardless of whether or not the application is protected by a NetScaler appliance. The more critical the attacks on an application, the higher the threat index for that application.

  -Safety index. A single-digit rating system that indicates how securely you have configured the NetScaler devices to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index.

  -Actionable Information. Information that you need to lower the threat index and increase the safety index, which significantly improves application security. For example, you can review information about violations, existing and missing security configurations in Application Firewall and NetScaler security features, the rate at which the applications are being attacked, and so on.

  [From Build 65.72] [# 587137]

Networking

- **Stateful Connection Failover Support for RNAT**

Connection failover helps prevent disruption of access to applications deployed in a distributed environment. The NetScaler appliance now supports stateful connection failover for connections related to RNAT rules in a NetScaler High Availability (HA) setup.

In an HA setup, connection failover (or connection mirroring) refers to the process of keeping an established TCP or UDP connection active when a failover occurs. The primary appliance sends messages to the secondary appliance to synchronize current information about the RNAT connections. The secondary appliance uses this connection information only in the event of a failover. When a failover occurs, the new primary NetScaler appliance has information about the connections established before the failover and hence continues to serve those connections even after the failover. From the client's perspective this failover is transparent. During the transition period, the client and server may experience a brief disruption and retransmissions.

Connection failover can be enabled per RNAT rule. For enabling connection failover on an RNAT rule, you enable the connFailover (Connection Failover) parameter of that specific RNAT rule by using either NetScaler command line or configuration utility. Also, you must disable the tcpproxy (TCP Proxy) parameter globally for all RNAT rules in order for connection failover to work properly for TCP connections.

[From Build 65.72] [# 457167]

Platform

- **Support for SRIOV interfaces on ESX VPX**

  On Netscaler VPX running on ESX hypervisor 6.0, support is now available for SRIOV interfaces. The supported NIC is Intel 82599 10g NIC.

  Information on how to configigure ESX VPX for SRIOV interface is available in http://docs.citrix.com/en-us/netscaler/11/getting-started-with-vpx/install-vpx-on-esx.html

  For more information on the performance of VMXNET3 interface on ESX, please refer to the latest VPX datasheet.

  [From Build 65.72] [# 637341]

- **Support for VMXNET3 interfaces on ESX VPX**

  On a Netscaler VPX running on ESX hypervisor 6.0, support is now added for VMXNET3 interface, which is the para-virtualised driver from VMWare.

  For more information about configuring ESX VPX for VMXNET3 interface, see http://docs.citrix.com/en-us/netscaler/11/getting-started-with-vpx/install-vpx-on-esx.html.

  For more information about the performance of VMXNET3 interface on ESX, refer to the latest VPX datasheet.

[From Build 65.72] [# 637336]

[From Build 65.72] [# 618107]

SSL

- The NetScaler appliance now supports the following "signature algorithms" extensions in the back end client hello message:

  - RSA-MD5

  - RSA-SHA1

  - RSA-SHA256

  [From Build 65.72] [# 600155, 601059]

- **New Client Authentication Counters for SSL Virtual Servers**

  Two counters have been added to the output of the "stat ssl vserver" command as follows:

  1. ssl_ctx_tot_clientAuth_success: Tracks the number of successful client authentications for each SSL virtual server.

  2. ssl_ctx_tot_clientAuth_failures: Tracks the number of failed client authentications for each SSL virtual server.

  [From Build 65.72] [# 492684]

- **Using the SSL Chip Utilization Percentage Counter for Capacity Planning on MPX Appliances that use N3 Chips**

  Knowing the percentage utilization of all the SSL chips in an appliance over a period of time helps in capacity planning. The counter increments every 7 seconds and therefore provides real-time data, which can help you predict when an appliance is likely to reach capacity.

  Note: This feature is available on only the MPX appliances that use N3 chips, which include MPX 11515/11520/11530/11540/11542 and MPX 220140/22060/22080/22100/22120/24100/24150 appliances.

  Some models of MPX 14020/14030/14040/14060/14080/14100 and MPX 25100/25160/25200, which use N3 chips, also support this feature.

  [From Build 65.72] [# 416807, 197702]

- The NetScaler VPX appliance now supports AES-GCM/SHA2 ciphers on the front end.

[From Build 65.72] [# 498207]

- The NetScaler VPX appliance now supports TLS protocol versions 1.1 and 1.2 on the back end.

  [From Build 65.72] [# 543526, 579749, 619662]

System

- The "show connectiontable" command now displays additional information such as queued packets, allocated memory for data structures, and RTT measurements.

  [From Build 64.90] [# 628095, 250335]

- You can now enable auto-bootstrapping on a NetScaler VPX or NetScaler 1000v instance running on Hyper-V, by attaching a DVD ROM with an appropriate ISO file to the instance before booting it up.

  [From Build 65.72] [# 578451]

Fixed Issues in Previous NetScaler 11.0 Releases

The issues that were addressed in NetScaler 11.0 releases prior to Build 66.11. The build number provided below the issue description indicates the build in which this issue was addressed.

AAA-TM

- 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 65.72] [# 615885]

- 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 65.72] [# 610604, 618760, 623053]

- You cannot enter the FQDN for a RADIUS or LDAP server by using the NetScaler GUI.

  [From Build 65.72] [# 596382, 618884]

- Authentication fails if the server name in an LDAP action is changed from an FQDN to an IP address by using the "set ldapaction" command.

  [From Build 65.72] [# 614597]

- When RADIUS is used in nFactor authentication, the NetScaler appliance fails to complete the request if user is prompted for password change.

  [From Build 65.72] [# 612431]

- The Netscaler appliance intermittently fails if a user accesses a very long URL without proper AAA context.

  [From Build 65.72] [# 598837, 623059]

- 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 65.72] [# 613700]

- If a logout message from a session owner to a cached session is dropped, the NetScaler appliance might fail while trying to resend the message.

  [From Build 65.72] [# 620948]

Admin Partitions

- When the NSIP password is changed (by using the "set ns rpcnode" command) on the default partition, the GSLB auto-sync function does not work in the available admin partitions.

  [From Build 65.72] [# 621939]

Application Firewall

- When the application firewall cookie proxy check is enabled, the NetScaler appliance might become unresponsive while updating the cookies in the distributed hash table with a set of cookies from the server.

  [From Build 65.72] [# 609394, 618385]

- NetScaler application firewall handles memory incorrectly if XSS and "CrossSiteScriptingCheckCompleteURLs" are enabled in the application firewall profile. The errors also appear if "checkrequestHeaders" and finegrained relaxations are enabled.

[From Build 65.72] [# 606931]

- 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 65.72] [# 603473]

- 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 65.72] [# 610116, 603473]

- In release 10.5.e (enhancement builds only) as well as in the 11.0 release builds, application firewall processing of the Cookie header was changed. In those releases, every cookie is evaluated individually, and if the length of any one cookie received in the Cookie header exceeds the configured BufferOverflowMaxCookieLength, the Buffer Overflow violation is triggered. As a result of this change, requests that were blocked in 10.5 and earlier release builds might be allowed, because the length of the entire cookie header is not calculated for determining the cookie length. In some situations, the total cookie size forwarded to the server might be larger than the accepted value, and the server might respond with "400 Bad Request".

  With this fix, the change has been reverted. The behavior is now similar to that of the non-enhancement builds of release 10.5. The entire raw Cookie header is now considered when calculating the length of the cookie. Surrounding spaces and the semicolon (;) characters separating the name-value pairs are also included in determining the cookie length.

  [From Build 65.72] [# 614449]

- You might encounter unexpected failures if form field consistency protection is enabled on the application firewall profile and you try to retrieve the form from Distributed Hash Table (DHT).

  [From Build 65.72] [# 616191]

- In certain cases, if a custom error page containing variables is served to the client, the content length in the response is incorrect. As a result, the custom error page might not be visible in the client's browser.

  [From Build 65.72] [# 616947]

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

[From Build 65.72] [# 619978]

- The XSS transform for special characters in the application firewall might not work as expected if the -crossSiteScriptingTransformUnsafeHTML option or the sqlTransformAction option is set to ON in the profile.

  [From Build 65.72] [# 618707]

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

  [From Build 65.72] [# 621798]

- In a cluster setup, while exporting application firewall learnt data, you might see the following error message:

  "communication error with aslearn"

  This message is because of a schema difference.

  [From Build 65.72] [# 625807]

- 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 65.72] [# 598776, 597952]

- 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 65.72] [# 612284, 619056]

Audit logging

- You can now customize the log levels for logs generated for AAATM user logon or logoff, and for logs generated for executive commands by a NetScaler administrative user.

  [From Build 65.72] [# 386650]

Cache Redirection

- If a request to a cache redirection virtual server resolves to an IP address that belongs to a content switching virtual server configured on the NetScaler appliance, the appliance might fail.

  [From Build 65.72] [# 621522, 626848]

- In the GUI, the Policy drop-down list does not display the cache redirection policies.

  [From Build 65.72] [# 622402]

Configuration Utility

- If you log on to the appliance by using the GUI, the list of licenses is not retrieved.

  [From Build 65.72] [# 611772]

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

  [From Build 65.72] [# 485942]

Content Switching

- 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 65.72] [# 522510, 528782, 538223, 552913, 602829]

DNS

- 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 65.72] [# 605861]

- If, while resolving a domain name in DNS resolver mode, the NetScaler appliance does not receive a response from the first name server, it tries to resolve the domain name with the other name servers. During this process, if the address record for the associated NS record is not present, the NetScaler appliance fails.

  [From Build 65.72] [# 609967, 617204]

DataStream

- 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 65.72] [# 560401]

GSLB

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

  [From Build 65.72] [# 618789]

- When using the GUI in a partitioned environment, you cannot add GSLB services.

  [From Build 65.72] [# 622131]

- 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 65.72] [# 617267]

- In a content switching GSLB deployment, you can bind multiple domains to a CS GSLB virtual server, but the show cs vserver command shows only one domain bound to the CS GSLB virtual server.

  [From Build 65.72] [# 612916]

- For GSLB deployments in a partitioned environment, the options to synchronize the GSLB configuration and view the synchronization status are provided in the GUI.

  [From Build 65.72] [# 622147]

- If the ACK on PUSH option is disabled in the default TCP profile, the NetScaler appliance might fail while downloading the static proximity database.

  [From Build 65.72] [# 582102]

Integrated Cache

- A NetScaler appliance performing integrated caching becomes unresponsive if the length of the URL is 2040 (including the hostname, query parameter, and other specific information).

  [From Build 65.72] [# 605831, 612030, 612102, 636197]

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

  [From Build 65.72] [# 602984]

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

Workaround: Unset cache object persistency as follows:

> set cache parameter -enableHaObjPersist NO

[From Build 65.72] [# 589322]

- When the "clear config" command is issued, the NetScaler appliance can become unresponsive if more than one CPU tries to free the same shared memory.

  [From Build 65.72] [# 609928, 635303]

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

  [From Build 65.72] [# 581598]

- Disabling the Media Classification mode, even if the host header is missing in the GET request, does not cause a NetScaler appliance to fail.

  [From Build 65.72] [# 616021, 616757, 618970, 624338]

Load Balancing

- 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 65.72] [# 612943]

- In a high availability setup in admin partition mode, the persistent sessions are not synchronised to the secondary node after performing force ha sync or force failover operation.

  [From Build 65.72] [# 630344]

- The NetScaler appliance fails because of an incorrect initialization of template size in a stream analytics session info record.

  [From Build 65.72] [# 598391]

- Feature DNS

  Due to a memory overwrite issue, the prev value of dns_tot_ServerQueries counter is set to zero everytime during the end of perf collection cycle, that is every 7 seconds. This results in the difference between cur and prev value get accumulated to the global counterpart even if there is no traffic.

  [From Build 65.72] [# 615519, 580342]

- In a high availability setup, if a large number of services and service groups are configured, service state updates might fail because of a timer issue.

  [From Build 65.72] [# 605596, 609999]

NITRO API

- 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 65.72] [# 620458, 619154, 621601]

NetScaler Insight Center

- If you click on a country in the Geo Maps in the XenDesktop Director GUI, the GEO maps are not displayed.

  [From Build 65.72] [# 617872]

- The network panel in the XenDesktop Director GUI does not display a graph with the session details when you select another user.

  [From Build 65.72] [# 550209]

- The network panel in the XenDesktop Director GUI does not display a graph with the session details for the selected user.

  [From Build 65.72] [# 550227]

- If you use the refresh button, it does not have any effect on the slider. Refresh operation does not have any affect on the time shown in the slider. Also, when you change tabs, it does not impact the slider. You can change the time by changing the time duration.

  [From Build 65.72] [# 576469]

- In NetScaler Insight Center, updating fields in a private IP block fails.

  [From Build 65.72] [# 623022]

- The whitelist of Citrix Receiver versions used by HDX Insight now includes version 13.0.3.265571 of Citrix Receiver for Linux.

  [From Build 65.72] [# 614558, 606817]

- In the network panel in the XenDesktop Director GUI, the time slider for selecting the time period for a graph is not properly displayed.

  [From Build 65.72] [# 593699]

- The network panel in the XenDesktop Director GUI displays the details of all of the administrative user's sessions, instead of just the details for the selected session.

  [From Build 65.72] [# 594512]

- The NetScaler appliance might sometimes become unresponsive or experience intermittent HA failovers based on a particular ICA network condition.

  [From Build 65.72] [# 623729, 623379]

- NetScaler Insight Center might intermittently become unresponsive and not populate any reports.

  [From Build 65.72] [# 618370, 622539, 631395]

- NetScaler Insight Center restarts intermittently, and HDX insight reports might not show any data.

  [From Build 65.72] [# 606455]

- The network panel in the XenDesktop Director GUI displays session details of all users, instead of for just the selected user.

  [From Build 65.72] [# 607332]

- NetScaler Insight Center fails to generate the technical support file, because the namedpipe file causes an error in the creation of the technical support file.

  [From Build 65.72] [# 613622]

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

  [From Build 65.72] [# 585914, 613238, 630417, 635395, 635412]

- If the two NetScaler appliances in a double hop deployment are running different NetScaler software editions (Platinum, Enterprise, or Standard), NetScaler Insight Center fails to generate reports for these appliances on the NetScaler Insight Center dashboard.

  [From Build 65.72] [# 609452]

- Adding a private IP block in NetScaler Insight Center fails if you select a country name that has special characters.

  [From Build 65.72] [# 609646, 620408]

- NetScaler Insight Center does not cache reports after you enable database caching.

  [From Build 65.72] [# 611269]

- For some elements on the dashboard, NetScaler Insight Center does not fetch records for the specified time frame.

  [From Build 65.72] [# 611532, 612283]

Networking

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

  [From Build 65.72] [# 613457, 614545, 617179, 621236]

- 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 65.72] [# 608558]

- 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, neighbour adjacency does not get established.

  [From Build 65.72] [# 612419, 633722]

- The NetScaler appliance fails when it processes invalid UDP packets received at port 500 or port 4500.

  [From Build 65.72] [# 609537, 489498, 628985]

- For a sessionless virtual server configuration, the NetScaler appliance might forward packets for an incoming connection without changing their source MAC address with the MAC address of one of its interfaces. As a result, the connection fails.

  [From Build 65.72] [# 603477, 583499]

- 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 65.72] [# 599306]

- Forwarding sessions do no work as expected with bridge groups, because packets are not forwarded to the correct VLAN.

  [From Build 65.72] [# 600012]

- 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 65.72] [# 613454]

- A clear config operation does not remove VXLANS. The configuration utility and the CLI continue to show the VXLANs, but with incorrect IDs.

  [From Build 65.72] [# 574734]

- After the clear config operation, reconfiguring a VXLAN entity fails to retrieve the VXLAN SNMP counters.

  [From Build 65.72] [# 572525, 574734, 614924]

- The dynamic routing module on a NetScaler appliance might incorrectly save the command "redistribute intranet" as "redistribute trillâ€• 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 65.72] [# 620152]

- FTP in passive mode does not work in this build.

  [From Build 65.72] [# 631929]

- 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 65.72] [# 597458]

Policies

- The default timeouts for Rewrite Processing and for Advanced Expression Regex Evaluation have changed from 1 millisecond to less than the pitboss timeout of 5 seconds. This restores the default behavior for releases prior to 11.0. In addition, an optional -timeout parameter to "set the re-write param " CLI command

was added. The time is measured in milliseconds - see the man page. A "set policy param -timeout <value>" command has been added to the CLI. These ways of setting the timeout work for all partitions.

In release 11.0, the default timeouts for Rewrite Processing and for Advanced Expression Regex Evaluation have also changed from 1 millisecond to less than the pitboss timeout. This restores the default behavior from releases prior to 11.0. However, neither the CLI command, nor the GUI, nor the Nitro call is available. Instead, for 11.0, an nsapimgr command is available from the shell. This will only change the timeout on the default partition when Partitioning is used. Other partitions will only use the default. The syntax is as follows: "nsapimgr_wr.sh -ys arg1=<value> -ys call=ns_pixl_regex_set_time_limit" to set the time limit on regular expression evaluation in Advanced expressions. "nsapimgr_wr.sh -ys arg1=<value> -ys call=ns_rw_set_eval_time_limit" to set the time limit on Rewrite processing. For either of these, setting the value to 0 resets the limit to the default. These nsapimgr commands will not be supported after 11.0, and the CLI, GUI, or Nitro must be used.

[From Build 65.72] [# 577016, 578214]

- A memory leak occurs when a responder action has blocking expressions (for example, stream analytics, HTTP callout, matches_location) and body or payload based expressions.

  [From Build 65.72] [# 598252, 623764, 624637, 624759, 629247, 629344]

- Rewrite action block leading to subsequent action time outs.

  If multiple rewrite policies evaluate to TRUE for a particular protocol and direction (for example HTTP request or TCP response), and more than one associated action is selected for execution, they might not all execute. If one of the actions is suspended (blocked), the next selected action will time out, and any subsequent actions will be skipped.

  The following functions in expressions can block:

  * HTTP_CALLOUT

  * MATCHES_LOCATION

  * STREAM

  * CHECK_LIMIT

  * MATCHES

  * BODY

  * PAYLOAD

  * MSSQL

* MYSQL

* ORACLE

* SUBSCRIBER

* DETERMINE_SERVICES

* use of variables (in other words, $<variableName>)

Note: These expressions can block, depending on specific conditions that occur at the time of execution.

[From Build 65.72] [# 628326]

- 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 65.72] [# 605089]

SSL

- When clearing the NetScaler configuration, user-defined cipher groups that are bound to an internal SSL service might get corrupted. Subsequent cipher bind or unbind operations with that service will cause the appliance to become unresponsive.

  [From Build 65.72] [# 611894, 622042]

- The NetScaler appliance fails if it parses the value of an unknown certificate extension while the certificate is loading.

  [From Build 65.72] [# 623996]

- You cannot install a certificate on the appliance if the certificate is not in the /nsconfig/ssl directory. With this fix, you can install a certificate in the applianceâ€™s default partition from any location. For other partitions, the certificate must be in the /nsconfig/partitions/ssl/ directory.

  [From Build 65.72] [# 602631]

System

- A NetScaler appliance now processes delayed packet-free queues at a higher frequency. This prevents memory build up on the appliance.

  [From Build 64.90] [# 638117]

- A NetScaler appliance fails when it encounters an HTTP/2 connection level error on a TCP connection.

  [From Build 65.72] [# 615395]

- 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 65.72] [# 615487]

- The NetScaler Weblog client intermittently fails because of incorrect indexing, leading to segmentation failure

  [From Build 65.72] [# 615895, 620767, 629214]

- A NetScaler appliance fails when an MPTCP subflow receives an Infinite DSS mapping in a partially retransmitted packet.

  [From Build 65.72] [# 614842, 623426]

- A configuration loss occurs when you upgrade Content Switching (CS) entities above the following limits:

  Memory allotted to a packet engine 2GB 4GB

  Max number of content switching virtual servers 1200 2500

  Max number of content switching policies 1500 3500

  Max number of content switching virtual server bindings 3000 4000

  [From Build 65.72] [# 628528]

- 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 65.72] [# 611774, 598774]

- A NetScaler appliance becomes unresponsive when passing an HTML response with the HTML tag exceeding 16 characters.

  [From Build 65.72] [# 611723]

- 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 65.72] [# 610809, 577474, 579560, 622553]

- A NetScaler appliance might fail because of a segmentation fault if it receives a large HTTP/2 request Header that evicts the dynamic header table entry.

  [From Build 65.72] [# 615629]

- 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 65.72] [# 605258]

- A NetScaler appliance does not support Base64 decoded TASS cookie IDs of more than 64 characters. If Security Assertion Markup Language (SAML) or federation results in an ID longer than 64 characters, the appliance does not support the cookie ID.

  [From Build 65.72] [# 594603, 607019, 615811]

- **Support restore operation on the NetScaler Appliance by using a remotely stored backup**

  You can now use a remotely saved backup to restore a NetScaler appliance through the "add system backup <filename>", that adds the metadata to the remote backup package, so that the restore operation can successfully use the backup package.

  [From Build 65.72] [# 569974]

- A T1200 appliance that is used in a NetScaler deployment can become unresponsive or fail when generating the NetScaler tech support logs.

  [From Build 65.72] [# 606247, 624369, 624385]

- 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 65.72] [# 606493, 601655, 623185, 634334]

- 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 65.72] [# 583579, 594722, 626120]

- 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 65.72] [# 604971, 611176]

- A NetScaler appliance fails when it receives an MP_CAPABLE final acknowledgement in a single packet with the FIN flag set.

  [From Build 65.72] [# 583853, 583855, 588078, 601746, 602955]

- 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 65.72] [# 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 65.72] [# 601372]

- You cannot shut down or restart the virtual machine by using the VMware vSphere tool.

  [From Build 65.72] [# 607158]

- In certain cases, the NetScaler appliance might not retransmit the lost TCP segments resulting in a transaction failure.

  [From Build 65.72] [# 565938, 560394, 592227, 597160, 607864, 609068]

Telco

- With a large number of active subscribers, and a high traffic rate for SIP over TCP, the NetScaler appliance can fail during ALG processing.

  [From Build 65.72] [# 582464]

- In a high availability deployment with LSN and DS-Lite configuration, LSN and DS-Lite mappings for active FTP connections are not removed from the secondary node even after they time out or are flushed.

  [From Build 65.72] [# 601920, 619864]