Citrix NetScaler 1000V Release Notes

Citrix NetScaler 11.0-64.34
2016-01-12

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

11.0-64.34 4

Points to Note 4

What’s New? 5

Bug Fixes 14

Known Issues 25

What's New in Previous NetScaler 11.0 Releases 39

Fixed Issues in Previous NetScaler 11.0 Releases 70

11.0-64.34

The release notes provides the changes or enhancements, issues that are fixed, and known issues that exist in Build 64.34. 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 64.34 (2015-12-30) (Current build)
- Build 63.16 (2015-10-07)
- Build 62.10 (2015-08-12)
- Build 55.20 (2015-06-30)

Points to Note

Some important aspects to keep in mind while using Build 64.34.

Web Interface on NetScaler (WIonNS)

- **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.

  [From Build 64.34] [# 464854]

What's New?

The enhancements and changes that are available in Build 64.34.

AAA-TM

- When used as a SAML SP, the NetScaler appliance can now extract multi-valued attributes from a SAML assertion. These attributes are sent is nested XML tags such as:

  <saml:Attribute FriendlyName="groups" Name="groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified?>

  <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string?>

  <AttributeValue>grp1</AttributeValue>

  <AttributeValue>grp2</AttributeValue>

  <AttributeValue>grp3</AttributeValue>

  </saml:AttributeValue>

  </saml:Attribute>

  [# 577853]

- **Increased Length of SAML Attributes for Extraction**

  In the SAML Service Provider (SP) module, names of the attributes that can be extracted from an incoming SAML assertion can be up to 127 bytes long. The previous limit was 63 bytes.

  [# 581644]

- When used as a SAML IdP, the NetScaler appliance can now send multi-valued attributes in a SAML assertion.

  [# 588125]

- **Support for Redirect Binding for SAML IdP**

  When used as a SAML Identity Provider (IdP), the NetScaler appliance now supports redirect bindings (in addition to POST binding).

  Using the CLI:

  > set authentication samlIdPProfile <name> -samlBinding REDIRECT

  Using the GUI:

  Navigate to Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy, and in the required SAML IdP policy, configure the SAML binding as "Redirect" for the SAML IdP profile.

  [# 564947, 590768]

- **Configuring Validity for SAML Assertions**

  A NetScaler appliance can be configured to provide SAML authentication to an application by playing the role of the SAML Identity Provider (IdP) and/or the SAML Service Provider (SP). If the system time on NetScaler SAML IdP and the peer SAML SP is not in sync, the messages might get invalidated by either party.

  To avoid such cases, you can now configure the time duration for which the assertions will be valid. This duration, called the "skew time," specifies the number of minutes for which the message should be accepted. The skew time can be configured on the SAML SP and the SAML IdP.

  - When the NetScaler is used as a SAML IdP, configure the skew time on the SAML IdP profile, to accept incoming requests from SP and to send assertions.

  --- Using the CLI: > set samlidpProfile <name> -skewTime 30

  --- Using the GUI: Navigate to Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy, and in the required SAML IdP policy, configure the skew time for the SAML IdP profile.

  - When the NetScaler is used as a SAML SP, configure the skew time on the SAML action.

  --- Using the CLI: > set samlaction <name> -skewTime 30

  --- Using the GUI: Navigate to Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy, and in the required SAML SP policy, configure the skew time for the SAML action.

  [# 582266]

- **SAML IdP Validating the SAML SP**

  When used as a SAML Identity Provider (IdP), the NetScaler appliance can be configured to serve assertions only to SAML Service Providers (SP) that are pre-configured on or trusted by the IdP. For this configuration, the SAML IdP must have the service provider ID (or issuer name) of the relevant SAML SPs.

  Using the CLI:

  > set samlidpProfile <name> -serviceProviderID <string>

  Using the GUI:

  Navigate to Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy, and in the required SAML IdP policy, configure the SP ID for the SAML IdP profile.

  [# 582265]

Admin Partitions

- The NetScaler appliance now supports FTP load balancing in admin partitions.

  [# 568811]

- The following load balancing features can now be configured in admin partitions:

  - DBS autoscale

  - Stateless connection mirroring

  - RDP

  - Radius

  - Graceful shutdown

  For the detailed list of NetScaler feature support on admin partitions, see http://docs.citrix.com/en-us/netscaler/11/system/admin-partition/admin-partition-config-types.html.

  [# 588406]

Cluster

- **Cluster versioning**

  When you are upgrading a cluster to NetScaler 11.0 build 64.x from an earlier NetScaler 11.0 build, cluster configuration propagation is disabled.

  Traditionally, this issue occurred only during an upgrade of a cluster to a different NetScaler version (for example, from 10.5 to 11.0). This exception arises because the cluster version in build 64.x is different from the one in previous NetScaler 11.0 builds.

  Note: Normally, the cluster version matches the NetScaler version.

  Configuration propagation remains disabled until all the cluster nodes are upgraded to Build 64.x.

  [# 591877]

- **Reducing the Minimum Value for the Dead Interval**

  You can now set the dead interval for a cluster instance to a minimum value of 1 second.

  Note: If the dead interval value is less than 3 seconds, set the hello interval parameter to 200 ms.

  [# 573218]

Command Line Interface

- The NetScaler administrator can now specify the maximum number of concurrent sessions a user can log on to the CLI. Although logons to the configuration utility do not count against the limit, all logon attempts are denied after the limit is reached. For example, if the maximum number of concurrent sessions is set to 20, a user can log on to the CLI 19 times and can log on to the configuration utility any number of times. Once the user logs on to the CLI for the 20th time, he or she can no longer log on to the CLI or the configuration utility. Any logon attempt then results in a system error message.

  [# 491778]

GSLB

- **Ability to specify GSLB Site IP address as source IP address for an RPC node**

  You can now configure the NetScaler appliance to use GSLB Site IP address as the source IP address for an RPC node.

  [# 531395]

- **NetScaler GSLB deployments support NAPTR records**

  In GSLB deployments, the NetScaler appliance now supports DNS queries with NAPTR records. You can now configure a NetScaler appliance to receive DNS queries with NAPTR records from clients (for example, Mobile Management Entity (MME))and respond with the list of services configured for a domain. Also, the NetScaler appliance monitors the health of the services and in the response it provides only the list of services that are up.

  [# 468647]

Load Balancing

- With the following new OID, you can use SNMP to learn the current number of server connections per service.

  svcCurSrvrConnections, 1.3.6.1.4.1.5951.4.1.2.1.1.59

  [# 548470]

- **Support for Unauthenticated Stores**

  In earlier releases, the StoreFront monitor tried to authenticate anonymous stores. As a result, a service could be marked as DOWN and you could not launch XenApp or XenDesktop by using the URL of the load balancing virtual server.

  The probe order has changed. The monitor now determines the state of the StoreFront store by successively probing the account service, the discovery document, and then the authentication service, and skips authentication for anonymous stores.

  [# 575549]

- With the following new OID, you can use SNMP to learn the effective state of a virtual server.

  vsvrCurEffState, 1.3.6.1.4.1.5951.4.1.3.1.1.75

  [# 538499]

- **Retaining the Original State of a Service Group Member after Disabling and Enabling a Virtual Server**

  A new global option, -retainDisableServer, enables you to retain a service-group member's state when a server is disabled and reenabled.

  Previously, a member's state would change from DISABLED to ENABLED under the following set of conditions:

- Two applications are deployed on the same port on a virtual server.

- Two service groups with a common member are bound to this virtual server, and the common member is enabled in one group and disabled in the other.

- The server is disabled and then reenabled.

Under these conditions, disabling the server disables all the service group members, and reenabling the server enables all the members, by default, regardless of their earlier states. To bring the members back to the original states, you must manually disable those member(s) in the service group. This is a cumbersome task and prone to errors.

[# 493692]

Networking

- **Keeping a VIP address in the Backup State**

  You can force a VIP address to always stay in backup state in a VRRP deployment. This operation is helpful in maintenance or testing of the deployment.

  When a VIP address is forced to stay in backup state, it does not participate in VRRP state transitions. Also, it cannot become master even if all other nodes go down.

  To force a VIP address to stay in backup state, you set the priority of the associated VMAC address to zero. To ensure that none of the VIP addresses of a node handle traffic during a maintenance process on the node, set all the priorities to zero.

  [# 553311]

- **Keeping a VIP address in the Backup State**

  By default, for configurations with USIP option disabled or with USIP and use proxy port options enabled, the NetScaler appliance communicates to the servers from a random source port (greater than 1024).

  The NetScaler supports using a source port from a specified port range for communicating to the servers. One of the use case of this feature is for servers that are configured to identify received traffic belonging to a specific set on the basis of source port for logging and monitoring purposes. For example, identifying internal and external traffic for logging purpose.

  [# 420067, 420039]

- **Delaying Preemption**

  By default, a backup VIP address preempts the master VIP address immediately after its priority becomes higher than that of the master VIP. When configuring a backup VIP address, you can specify an amount of time by which to delay the preemption. Preemption delay time is a per-node setting for each backup VIP address.

  The preemption delay setting for a backup VIP does not apply in the following conditions:

  * The node of the master VIP goes down. In this case, the backup VIP takes over as the master VIP after the dead interval set on the backup VIP's node.

* The priority of the master VIP is set to zero. The backup VIP takes over as the master VIP after the dead interval set on the backup VIP's node.

[# 553246]

SSL

- **2048-bit Default Certificates on the NetScaler VPX Instance**

  You no longer need a license on your VPX instance to generate a 2048-bit default certificate. After upgrading your VPX instance to release 11.0, if you want to replace the old internal default 512-bit certificate, delete all your old certificate-key pairs that have "ns-" as the first three characters, and then restart the instance to automatically generate a 2048-bit default certificate.

  [# 451441, 405363, 458905, 465280, 540467, 547106, 551603, 559154, 584335, 588128]

- **Graceful Cleanup of SSL sessions after change in any SSL entity parameter**

  Some operations - for example, updating a certificate to replace a potentially exposed certificate, using a stronger key (2048-bit instead of 1024-bit), adding/removing a certificate from a certificate chain, or changing any of the SSL parameters - should clean the SSL sessions gracefully instead of abruptly terminating existing sessions. With this enhancement, existing connections continue to use the current settings but all new connections use the new certificate or settings. However, connections that are in the middle of a handshake or sessions that are renegotiating are terminated, and session reuse is not allowed. To clear the sessions immediately after a configuration change, you must disable and reenable each entity.

  [# 529979]

- If you downgrade the software on your NetScaler appliance that does not have a license to release 9.3 build 61.66 or earlier, some commands related to the default server certificate might not be saved in the running configuration. As a result, after restarting, secure access (HTTPS) to the appliance fails.

  [# 551603, 559154]

- **Enhanced SSL Profile**

  The SSL infrastructure on the NetScaler appliance is continually updated to address the ever growing requirements for security and performance. Vulnerabilities in SSLv3 and RC4 implementation have emphasized the need to use the latest ciphers and protocols to negotiate the security settings for a network connection. Implementing any changes to the configuration, such as disabling SSLv3, across thousands of SSL end points is a cumbersome process. Therefore, settings that were part of the SSL end points configuration have been moved to the SSL profile, along with the default ciphers. To implement any change in the configuration, including cipher support, you need only modify the profile. If the profile is enabled, the change is immediately reflected in all the end points that the profile is bound to.

  Important: After the upgrade, if you enable the profile, you cannot reverse the changes. That is, the profile cannot be disabled.

  [# 533640]

- **New Counters in SSL Statistics**

  Because TLS 1.1 and 1.2 are becoming the primary security protocols, the transaction and session statistics for these protocols are now included in the SSL statistics.

  [# 336395, 559165, 560353]

System

- **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.

  [# 569974]

- **Support for MPTCP Version Negotiation**

  A client can now establish an MPTCP connection with NetScaler appliance even if the client's and the NetScaler appliance's MPTCP versions does not match. If the MPTCP version of the client is higher than the one supported on the appliance, the client falls back to a lower or equal version. If the appliance supports that version, the MPTCP session continues. Otherwise, the appliance falls back to a normal TCP session.

  [# 529883]

- **Specifying a domain name for a logging server**

  When configuring an auditlog action, you can specify the domain name of a syslog or nslog server instead of its IP address. Then, if the server's IP address changes, you don?t have to change it on the NetScaler appliance.

  [# 314438]

Telco

- **IP Prefix NAT**

  The NetScaler appliance supports translating a part of the source IP address instead of the complete address of packets received on the appliance. IP prefix NAT includes changing one or more octets or bits of the source IP address.

  The NetScaler appliance supports IP prefix NAT for traffic related to virtual servers and services for which the NetScaler does not maintain any session information. For example, virtual servers and services of type ANY, UDP, and DNS.

  IP prefix NAT is useful in a deployment of NetScaler appliances and optimization devices (for example, Citrix ByteMobile) for identifying traffic from different client networks, which share the same network address, for meeting different optimization needs for traffic from each client network.

  [# 590571]

- **Configuring DS-Lite Static LSN Maps**

The NetScaler appliance supports manual creation of DS-Lite LSN mappings, which contain the mapping between the following information:

* Subscriber's IP address and port, and IPv6 address of B4 device or component

* NAT IP address and port

Static DS-Lite LSN mappings are useful in cases where you want to ensure that the connections initiated to a NAT IP address and port map to the subscriber IP address and port through the specified B4 device (for example, web servers located in the internal network).

[# 558406]

- **Port Block Size in a Large Scale NAT Configuration**

  Deterministic NAT and Dynamic NAT with port block allocation significantly reduce the LSN log volume. For these two types of configuration, the NetScaler appliance allocates a NAT IP address and a block of ports to a subscriber.

  The minimum port block size for deterministic LSN configuration and dynamic LSN configuration with port block has been reduced from 512 ports to 256. This reduction of the minimum port block doubles the maximum number of subscribers for a NAT IP address in an LSN configuration. It also reduces the number of unused ports assigned to subscribers who do not need more than 256 ports at a time.

  The port block size parameter can be set while adding or modifying an LSN group as part of an LSN configuration. A value of 256 (default) or a multiple of 256 can be set to the port block size parameter.

  For instructions on configuring Large Scale NAT, see Configuration Steps for LSN.

  For some sample LSN configurations, see Sample LSN Configurations.

  [# 581285]

- **Deterministic NAT Allocation for DS-Lite**

  Deterministic NAT allocation for DS-Lite LSN deployments is a type of NAT resource allocation in which the NetScaler appliance pre-allocates, from the LSN NAT IP pool and on the basis of the specified port block size, an LSN NAT IP address and a block of ports to each subscriber (subscriber behind B4 device).

  The appliance sequentially allocates NAT resources to these subscribers. It assigns the first block of ports on the beginning NAT IP address

  to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. At that point, the first port block on the next NAT address is assigned to the subscriber, and so on.

  The NetScaler appliance logs the allocated NAT IP address and the port block for a subscriber. For a connection, a subscriber can be identified by just its mapped NAT IP address and port block. For this reason, the NetScaler appliance does not log the creation or deletion of an LSN session.

[# 582325]

- **Logging MSISDN Information for a Large Scale NAT configuration**

  A Mobile Station Integrated Subscriber Directory Number (MSISDN) is a telephone number uniquely identifying a subscriber across multiple mobile networks. The MSISDN is associated with a country code and a national destination code identifying the subscriber's operator.

  You can configure a NetScaler appliance to include MSISDNs in LSN log entries for subscribers in mobile networks. The presence of MSISDNs in the LSN logs helps the administrator in faster and accurate back tracing of a mobile subscriber who has violated a policy or law, or whose information is required by lawful interception agencies.

  [# 581315, 502083]

- **Idle Session Management of Subscriber Sessions in a Telco Network**

  Subscriber-session cleanup on the NetScaler appliance is based on control plane events, such as a RADIUS Accounting Stop message, a Diameter RAR (session release) message, or a "clear subscriber session" command. In some deployments, the messages from a RADIUS client or a PCRF server might not reach the appliance. Additionally, during heavy traffic, the messages might be lost. A subscriber session that is idle for a long time continues to consume memory and IP resources on the appliance. The idle session management feature provides configurable timers to identify idle sessions, and cleans up these sessions on the basis of the specified action.

  [# 574138]

- **IPv6 Prefix based Subscriber Sessions**

  A telco user can be uniquely identified by the IPv6 prefix rather than the complete IPv6 address. The NetScaler appliance now uses the prefix instead of the complete IPv6 address (/128) to identify a subscriber in the database (subscriber store). For communicating with the PCRF server (for example, in a CCR-I message), the appliance now uses the framed-IPv6-Prefix AVP instead of the complete IPv6 address. The default prefix length is /64, but you can configure the appliance to use a different value.

  [# 574135]

- **Subscriber Session Event Logging**

  The NetScaler appliance currently maintains millions of subscriber sessions in its database (subscriber store) but does not log these messages. Telco administrators need reliable log messages to track the control plane messages specific to a subscriber. They also need historical data to analyze subscriber activities. The appliance now supports logging of RADIUS control plane accounting messages and Gx control plane logging messages. Some of the key attributes are MSISDN and time stamp. By using these logs, you can track a user by using the IP address, and the MSISDN if available.

  [# 575621, 575623]

Bug Fixes

The issues that are addressed in Build 64.34.

AAA-TM

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

  [# 540396]

- When kerberos token decryption fails, the NetScaler appliance responds with a 200 response with error message, instead of sending a 401 response.

  [# 567233, 593994]

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

  [# 599264, 610045]

- The NetScaler appliance might become unresponsive if the persistence cookie feature is enabled in AAA-TM deployments.

  [# 599701, 607138, 608997]

- Single sign-on to server does not succeed when native clients, such as iOS clients, connect to the NetScaler appliance using Active Sync protocol and send cookies along with authorization header.

  [# 597221]

- The status of a LDAP server on the authentication dashboard of the NetScaler GUI, will be shown as UP, regardless of the actual status of the LDAP server, for the following combinations:

  - Security type is SSL and port is 389.

  - Security type is TLS or PLAINTEXT and port is 636.

  [# 567376, 567379, 592941]

Action Analytics

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

  [# 595915, 602701]

Admin Partitions

- When creating an admin partition, you can now set the memory limit to a minimum value of 5 MB.

  [# 580419]

- **Setting L2 and L3 parameters in Admin Partitions**

On a partitioned NetScaler appliance, the scope of updating the L2 and L3 parameters is as follows:

- For L2 parameters that are set by using the "set L2Param" command, the following parameters can be updated only from the default partition, and their values are applicable to all the admin partitions: maxBridgeCollision, bdgSetting, garpOnVridIntf, garpReply, proxyArp, resetInterfaceOnHAfailover, and skip_proxying_bsd_traffic. The other L2 parameters can be updated in specific admin partitions, and their values are local to those partitions.

- For L3 parameters that are set by using the "set L3Param" command, all parameters can be updated in specific admin partitions, and their values are local to those partitions. Similarly, the values that are updated in the default partition are applicable only to the default partition.

[# 513564]

- In an admin partition, changes done to enable or disable a NetScaler feature or mode, are not saved. Therefore, after rebooting the NetScaler appliance, the status of the feature or mode is reset to its default value.

  [# 594845]

- Partition administrators cannot upload scriptable monitor scripts to a partition. This can only be done by NetScaler superusers. Also, scriptable monitors for an admin partition cannot be configured by using the GUI.

  [# 583756]

AppFlow

- The NetScaler appliance might become unresponsive if you enable the client side measurement option for an AppFlow action.

  [# 595238]

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

  [# 601915, 601924, 607217]

Application Firewall

- Signatures version may not get updated correctly if updated_signatures.xml file is present in /nsconfig folder. With this fix, this file is removed during build installation and the version of the application firewall signatures is updated accurately.

  [# 588640]

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

  [# 574498, 591172]

- The NetScaler appliance might become unresponsive when processing a request, because of an interoperability issue between the application firewall, SSL, and the responder module. The issue arises under the following set of circumstances:

  The configuration includes an application firewall profile protecting an SSL virtual server. A responder policy is configured to reset the connection, and this policy is bound either globally or to the virtual server that receives the request.

  [# 592429, 612052]

- The application firewall buffers the entire request for security check inspections. Therefore, when the client sends the expect 100-continue header in the request, the application firewall sends the 100-continue response to get the entire request from the client. The application firewall modifies the expect 100-continue header received from the client and corrupts it before forwarding the processed request to the server. In the 11.0 release, the header was not corrupted before it was forwarded request to server. With this fix, the expect 100-continue header from the client is modified and a corrupted header is sent to the server.

  [# 598607]

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

  [# 601064]

- The NetScaler appliance might fail when the application firewall receives an HTTP response with an attribute value that exceeds 1 MB in length.

  [# 592018]

- In a cluster deployment, accessing the application firewall learned data might display "Error in retrieving Application Firewall learning data. Communication error with aslearn". This error is triggered if buffer overflow occurs when the cluster configuration coordinator tries to get learned data from the other nodes of the cluster.

  [# 607187]

- When the application firewall redirects a blocked request to a customized error page, the ${NS_APPFW_SESSION_ID};variable on the error page might not display the session ID accurately. If the request does not contain a session cookie, the variable might display a hyphen (-) instead of the session ID.

  [# 599052]

- If the application firewall cookie proxy check is enabled and the server tries to expire and modify the same cookie in the same response, the NetScaler appliance might fail because of memory corruption.

  [# 603694, 609394]

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

  [# 591176, 593996, 597440, 601359]

- When URLTransform or CVPN policies are configured, application firewall code is invoked to carry out the validation of http packet information even if application firewall feature is disabled. When streaming code is engaged, the application firewall is not processing the conditional headers accurately and might reset connection and respond with RST code 9856. With this fix, parsing and validating the request headers is handled correctly by the application firewall module.

  [# 593960, 605920]

- NetScaler application firewall resets the connection when the request contains tampered session cookie and the cookie protection is enabled.

  [# 591172, 574498]

- When a user-defined application firewall signature object is updated by using the configuration utility, the enabled rules might get disabled and the configured actions in some signature rules might not be preserved.

  [# 561567]

- The application firewall has extended external format signature support for a new scan tool called WebInspect. The WebInspect scan tool, provided by Hewlett Packard (HP), is designed to analyze the web applications and web services for security vulnerabilities. As stated in the following Data Sheet link from HP, "WebInspect provides the broadest dynamic application security testing coverage and detects new types of vulnerabilities that often go undetected by black-box security testing technologies": http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-5363ENW.pdf.

  See http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/signatures.html" for the details of importing and configuring signatures.

  [# 588914, 609060]

Cluster

- When WIonNS is deployed in a cluster setup, if you add a service that points to the NSIP of a newly joined node, the command fails on the newly joined node but succeeds on the other cluster nodes.

  [# 584699]

Configuration Utility

- The configuration utility does not reflect the correct count of cached objects whereas this number is shown correctly through the command line interface.

  [# 607622, 608517]

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

[# 604646]

- If you click a VLAN in the network visualizer, details such as VLAN ID and bound interfaces are not displayed in a separate pane.

  [# 540943]

- When starting a nstrace and another instance is already running, an option to stop this is not available in the configuration utility. One has to login through the command line interface to stop the trace.

  [# 603476]

- The integrated caching feature is not available on the GUI.

  [# 601429]

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

  [# 609334]

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

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

  [# 597708]

- When an HTML page is imported, the content is copied to /nsconfig/ssl and then to /var/download/responder. The content is not removed from /nsconfig/ssl, although it serves no purpose there. With this fix, the content is copied directly to to /var/download/responder.

  [# 590268]

Content Switching

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

  [# 601203]

DNS

- The NetScaler appliance fails, if there is a cache miss when the backend DNS server is accessed directly through the NetScaler appliance.

  [# 609074]

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

  [# 581723]

GSLB

- Initiating 280k SIP sessions with 40k subscribers might cause the NetScaler appliance to fail.

  [# 582459, 591247]

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

  [# 590336]

- **GSLB Service Selection using Content Switching**

  Description: You can now configure a content switching (CS) policy to customize a GSLB deployment so that you can:

  * Restrict the selection of a GSLB service to a subset of GSLB services bound to a GSLB virtual server for the given domain.

  * Apply different Load Balancing methods on the different subsets of GSLB services in the deployment.

  * Apply spillover policies on a subset of GSLB services, and you can have a backup for a subset of GSLB services.

  * Configure a subset of GSLB services to serve a specific type of content.

  * Define a subset GSLB services with different priorities, and define the order in which the services in the subset are applied to a request.

  For more information, see Configuring GSLB Service Selection Using Content Switching.

  [# 503588]

High Availability

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

  [# 580703, 579037, 595104, 595491, 595506, 596002, 596215, 599250, 599396, 604164, 605112, 608450, 608485, 610589]

Load Balancing

- 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.

  [# 605596, 609999]

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

  [# 596524, 597295]

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

  [# 564295]

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

  [# 566644]

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

  [# 554841]

- A secure StoreFront monitor intermittently fails to sends probes.

  Workaround: If your deployment allows non-secure connections, use a non-secure StoreFront monitor.

  [# 559164, 582153]

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

  [# 574137]

NITRO API

- The NetScaler appliance might become unresponsive when a NITRO request is fetching a large number of bound entities.

  [# 530805, 562748, 567856]

Networking

- If a connection matches a RNAT rule, the NetScaler appliance probes for the existence of the destination server before processing the connection based on the RNAT rule. The connection that is used for probing is sometimes left idle on the appliance and a new connection is opened once the client connection is successfully established. This probe connection stays idle for the configured idle timeout (2.5 hours) thus holding up resources on the server.

  Now, these probe connections are flushed within a minute if they remain idle.

  [# 588694, 588551]

- The NetScaler appliance might erroneously forward DHCP broadcast packets to the default router. As a result, the broadcast packets go in loops between the appliance and the router.

  [# 591657, 595649]

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

  [# 587718]

- The configuration utility does not display any route monitors configured on the NetScaler appliance.

  [# 589128]

- On a NetScaler appliance with a NetScaler owned IP address configured with a VMAC address on a traffic domain, when a peer device sends an ARP request with unicast MAC for this IP address, the NetScaler appliance responds with the physical MAC address instead of the VMAC address. As a result, the NetScaler appliance drops packets forwarded by the peer device if the packets are destined to the physical MAC address for that IP address.

  [# 588912]

- A NetScaler appliance might consume a high percentage of CPU cycles, because the appliance repeatedly updates the active connections with changes in MAC addresses of servers.

  [# 579099]

- Binding a redundant interface set (for example, LR/1) to NSVLAN might cause the NetScaler appliance to become unresponsive.

  [# 597071]

- 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.

  [# 597458]

- In a high availability configuration, when the connection between primary and secondary goes down and comes up again, the secondary node receives HA INIT request from the primary node and it terminates all BGP connections.

  [# 588509]

Optimization

- A NetScaler appliance crashes when Media classification mode is enabled and HTTP request of bigger URLs are received.

  [# 589825, 594694, 606589, 607919]

- Enabling the media classification feature causes the NetScaler appliance to become unresponsive.

[# 581123, 584501, 588400, 590438, 594672, 595638, 601727, 601862, 603667, 604126, 607439, 609907, 611899]

Platform

- OpenSSL libraries are now integrated to operate in the FIPS mode.

  [# 523834]

SSL

- If you are running FIPS firmware 2.2 on your appliance, some commands might fail after 9 days.

  [# 600267]

- If you restart a NetScaler appliance that has FIPS firmware version 2.2, the FIPS key might be temporarily unavailable.

  [# 572645, 563418, 576719, 594569, 603072]

- If you upgrade the FIPS firmware on your appliance to version 2.2 and then restart it, you might notice some loss in the configuration.

  [# 597313]

- Even though SSL renegotiation is set to deny (that is, denySSLReneg is set to ALL), the server responds with the "server reneg" extension in the initial SSL handshake.

  [# 559082]

- In the OpenSSL interface in the NetScaler configuration utility, if you type a command before the OpenSSL> prompt appears, the OpenSSL> prompt might not appear at all. As a result, any commands that you type are not run in OpenSSL mode.

  [# 595413]

- If the passphrase for a certificate contains the "$" character, the configuration utility becomes unresponsive.

  [# 591743]

- NetScaler VPX virtual appliances do not support AES-GCM/SHA2 ciphers, but in earlier builds you can bind these ciphers, incorrectly, to an SSL virtual server. From the current build, you cannot bind these ciphers to the virtual server. If you have bound AES-GCM/SHA2 ciphers to a VPX instance that you upgrade to the current build, the bind commands in the configuration return an error. In a comparison of the configurations of the old and new build, the missing bindings can be mistakenly construed as a configuration loss.

  [# 609476]

- If you have configured optional client-certificate authentication and your policies target client certificate x509 extensions, such as auth keyid, a transaction with a client that doesn't have a certificate might cause the appliance to fail or to use stale values from a previous transaction.

  [# 593091]

- If you enable the DH parameter while creating an SSL profile by using the configuration utility, the following error message appears:

  Error in retrieving File. Invalid args in query parameters

  [# 594922]

- If TLS1.1/1.2 protocol is used with AES/3DES ciphers, the length of the TCP window at the back end shrinks to zero. As a result, after some time, the connection is terminated.

  [# 591600, 595713, 596278, 596556, 596566, 598045, 599524, 600591, 604409, 604929]

- In release 10.5 or later, TLS protocol versions 1.1 and 1.2 are enabled by default, but you can disable them for all services except SSL_BRIDGE and dynamic services, which can't otherwise be configured. In this release, you can disable TLS1.1/1.2 on SSL_BRIDGE and dynamic services by enabling the new svctls1112disable and montls1112disable parameters, as follows:

  set ssl param -svctls1112disable enable -montls1112disable?enable

  After the new parameters are enabled, you cannot disable them by using the "set ssl param" command. You must edit the configuration (ns.conf) file as follows:

  1.??? Remove these parameters from the "set ssl param? command.

  2.??? Save the configuration.

  3.??? Restart the appliance.

  [# 602502, 599209, 609284]

System

- Failed SNMP requests were not removed properly, therefore, subsequent set requests were retained in the queue. This lead to all SNMP requests getting blocked and high memory usage, due to which the SNMP module stops responding.

  [# 590289, 584527, 596242]

- When adding a syslog action for which the netProfile parameter is set, the Subnet IP (SNIP) address is used as the source IP address for sending log messages. If the netProfile parameter is not set, the NetScalerIP (NSIP) address is used as the source IP for sending the log messages.

  [# 595449]

- Some events may be logged twice if DEBUG level is enabled for syslog, by using the "set audit syslogParam" command.

  [# 594485]

- A Netscaler appliance has high memory consumption if Front End Optimization (FEO) feature is enabled.

  Work around: Disable the feature or reboot the appliance.

[# 591928]

- If weblog data is sent over a TCP connection that the NetScaler appliance has terminated because of buffer overflow, the appliance fails. With the fix, the connection is checked to ensure that it is not closed before the weblog data is sent.

  [# 593968, 574996]

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

  [# 538212]

- A NetScaler appliance might crash if you attempt to start the nstrace instance with advanced filter expression.

  [# 493737, 526095, 598148]

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

  [# 565938, 560394, 592227, 597160, 607864, 609068]

- The appliance might fail under the following set of conditions:

  1. A pipelined HTTP request is received that spans multiple TCP segments.

  2. An internal HTTP response generated by NetScaler for the HTTP request in condition 1, is terminated by a TCP segment that has the TCP FIN flag set.

  3. The appliance receives another HTTP request on the same connection.

  [# 587817, 587879, 589416, 594044, 595927, 601915, 610728]

- If the NetScaler appliance receives a data or an acknowledgement packet without the Data Sequence Signal (DSS) option before the MPTCP connection is established, the appliance does not seamlessly fallback to regular TCP.

  [# 588909]

- In a HA setup, if a domain-based SNMP manager is added on the secondary appliance, the NetScaler appliance stops responding eventually. You must configure the SNMP manager on the primary appliance.

  [# 581355, 593292, 595943]

- For a NetScaler appliance with extended memory configured for Large Scale NAT (LSN) feature, after warm rebooting the appliance, when the appliance is added as secondary node to an appliance that does not have the extended memory configured for LSN, the secondary appliance becomes unresponsive.

  [# 593261]

- A NetScaler appliance might occasionally fail when a client connects to an HTTP/SSL server and the server sends a 101 (switching protocols) response. The connection is closed before data can be sent or received from the client.

  [# 576561, 587759]

- When parsing a host name with no Path component, the URL parsing logic does not search for a question mark (?), so an entire string might be interpreted as the host name. This causes an error when the appliance tries to resolve the DNS name. With this fix, the parsing logic searches for question marks.

  Eg:
  http://example.com.php?&curuserid=94315577&host=wscdny203.live.changba.com&token=T59d105c1c74042e&localip=221.235.187.75&clientip=80.95.239.1&bless=1&channelsrc=market_%E7%99%BE%E5%BA%A6

  [# 587858]

- When the NetScaler appliance receives MPTCP traffic, the number of established client connections is high, because both MPTCP sessions and subflows are treated as client connections.

  With this fix, the SNMP OID of following MIBs have changed to:

  mptcpCurSessWithoutSFs: 130

  vsvrCurMptcpSessions: 73

  vsvrCursubflowConn: 74

  [# 583292]

- After you upgrade a Netscaler appliance to 10.5 build, the Client-Server Link Mapping check box is now available in the TCP Connections page

  [# 551611, 519966]

Telco

- SIP registration might fail, if authentication is enabled in the SIP proxy server.

  [# 579797]

Known Issues

The issues that exist in Build 64.34.

AAA-TM

- You cannot enter user-defined values for the user name and group name fields on the CERT Profile page for the AAA-Application Traffic feature or the NetScaler Gateway feature.

  With this fix, you can specify user-defined values for these fields by selecting New in the User Name Field list and the Group Name Field list and then entering a value.

[# 597706]

- 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]

Admin Partitions

- 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]

- RPCSVR services cannot be configured in admin partitions.

  [# 498477]

- 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]

- 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]

AppFlow

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

  [# 585914, 613238]

AppFlow Insight

- Hiding or displaying a URL, and some configuration changes might take longer than expected.

  [# 570896, 574278]

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]

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

  [# 549255]

- 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 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 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]

- "Operation timed out" error is displayed in the CLI and the configuration utility while viewing learned rules. This error is only seen intermittently.

  [# 527190]

- 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]

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

  [# 530277]

- The application firewall CSRF Security check uses sessions. By default, there is a limit of 100,000 sessions per PE. If this limit is exceeded, the connection gets reset and the browser appears frozen.

Workaround: Decrease the session timeout and increase the session limit by using the following commands:

From CLI: > set appfw settings -sessiontimeout 300

From shell: root@ns# nsapimgr_wr.sh -s appfw_session_limit=200000

[# 579533]

- 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]

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

  [# 548432]

- 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]

- 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]

- 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]

- When you perform the ?Skip? operation using configuration utility(GUI), the application firewall learned rules might not be deleted. This occurs because nitro is sending wrong "Location" (?Field?) data to GUI. With this fix, the GUI converts ?Field? into ?FORMFIELD?. The skip operation now works as expected and removes the skipped rules.

  [# 603473]

- 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]

- 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]

- 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]

Cisco RISE Integration

- Cisco RISE now supports the following commands:

  - show rise param

  - set rise param

  Following is the usage of the set rise param command:

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

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

  RISE-MPX-194-80> show rise param

DirectMode: ENABLED IndirectMode: ENABLED

Done

[# 497410]

Cluster

- 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]

- 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 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 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 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]

Command Line Interface

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

  [# 512526, 527066, 545578]

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

  For example, 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 to execute the command:

  - Use Net::SSH::Perl library and include double quotes around the command when calling $ssh->cmd().

  - Use the Net::Telnet library.

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

  [# 346066]

- 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]

Configuration Utility

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

  [# 540980]

- In the NetScaler configuration utility, 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]

- 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]

- The subnet mask does not appear after an IPv4 address in the network visualizer.

  [# 540927]

- 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]

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

  [# 542214]

GSLB

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

  [# 582102]

- 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]

- 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]

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]

Load Balancing

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

  [# 573463]

- 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]

- 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 the state of the IPv6 service on which a client's persistent session is running changes to out-of-service, the session might lose persistence before the client's transaction is completed.

  [# 571771]

NITRO API

- 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]

- 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]

NetScaler Insight Center

- Adding a new data node is now driven by Auto Registration. When a kernel is imported, it requests for input from user and does an auto registration with the Insight Server. This allows the Insight Deployment Manager GUI to display the same. Removing a datanode is not presently supported.

  [# 543632, 567628, 565706, 570264]

- If you use the refresh button, it does not have any effect on the slider. Refresh operation does not have any effect 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.

  [# 576469]

- Geo report is only available for daily, weekly, and monthly reports for Web Insight.

  [# 556534]

- HDX Insight reports are not generated for Linux VDAs.

  [# 580138]

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

  [# 570619]

Networking

- 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]

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

  [# 546066]

- An active FTP connection might get reset for no apparent reason, regardless of the state of the random source port.

  [# 507908, 611357, 609496]

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

  [# 574734]

- 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]

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

  [# 572525, 574734]

- 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]

Optimization

- An increase in the IC memory is observed when the content accelerator feature is enabled.

  Workaround: Disable the content accelerator feature.

  Note: The content accelerator feature is no longer supported on the NetScaler appliance.

  [# 597415]

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]

- 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]

- 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]

Protection

- 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]

SSL

- 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]

- 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]

- In both, default or admin partitions, when trying to import a password-protected key file, you get an error indicating that the key file is invalid. This error occurs because the NetScaler cannot import such key files.

  [# 512334]

- 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]

- 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]

- 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 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]

- 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]

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

  [# 554782]

- 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]

System

- 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 rare circumstances, the VPX instance can dump kernel core after a warm restart.

  [# 559176]

- 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]

- 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]

- 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]

Telco

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

  [# 574257]

- 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]

- Where there are over 140K SIP calls over UDP, the NetScaler appliance can fail during ALG processing.

  [# 574303, 582451]

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

  [# 574725]

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

  [# 582464]

- For a DS-Lite configuration with more than 90 million sessions, the NetScaler appliance might fail if you remove LSN pools.

  [# 580597]

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

  [# 581086]

WAN Insight

- If you upgrade NetScaler Insight Center appliance to release 10.5 build 55.8xxx.e, the compression ratio values will be displayed as -NA-.

  [# 554960]

- On the NetScaler Insight Center dashboard, the latency values displayed on the graph and the network topology diagram might not match due to time synchronization issues.

  [# 533063]

- NetScaler Insight Center displays the latency value between two hops as 0 ms, though the minimum latency value is 1 ms.

  [# 553536]

- NetScaler Insight Center takes two minutes to display the current connection details on the dashboard.

  [# 536696]

- CSV report exports elements that are present in the GUI. Additional elements like Client IP and Branch IP in the application node are denoted as 0.0.0.0 or " " as these are not present in GUI.

  [# 547380]

Web Interface on NetScaler (WIonNS)

- 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]

vPath

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

  [# 580137]

What's New in Previous NetScaler 11.0 Releases

The enhancements and changes that were available in NetScaler 11.0 releases prior to Build 64.34. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

AAA-TM

- **Supporting Encrypted Assertions on SAML SP**

  When used as a SAML SP (service provider), the NetScaler appliance can now decrypt the encrypted tokens that it receives from the a SAML IdP. No configuration is required on the NetScaler.

  [From Build 55.20] [# 291693]

- **OAuth/OpenID-Connect Mechanisms for AAA-TM**

  The NetScaler AAA-TM feature now supports OAuth and OpenID-Connect mechanisms for authenticating and authorizing users to applications that are hosted on applications such as Google, Facebook, and Twitter.

  Note: OAuth on NetScaler is currently qualified only for Google applications.

  A major advantage is that user's information is not sent to the hosted applications and therefore the risk of identity theft is considerably reduced.

  In the NetScaler implementation, the application to be accessed is represented by the AAA-TM virtual server. So, to configure OAuth, an action must be configured and associated with a AAA-TM policy which is then associated with a AAA-TM virtual server. The configuration to define a OAuth action is as follows:

  > add authentication OAuthAction <name> -authorizationEndpoint <URL> -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID <string> -clientSecret <string> [-defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-Attribute2 <string>] [-Attribute3 <string>] ....

  Note:

  - Refer to the man page for information on the parameters.

  - Attributes (1 to 16) are attributes that can be extracted in OAuth response. Currently, these are not evaluated. They are added for future reference.

  [From Build 55.20] [# 491920]

- **Fallback from Certificate to Other Authentication Mechanisms**

When authentication is configured to be done by using certificates and then followed by LDAP or other authentication mechanisms, the following behavior holds true:

- In previous releases: If certificate authentication fails (or was skipped), the other authentication mechanism is not processed.

- From this release onwards: Even if certificate authentication is not done, the other authentication mechanism is processed.

[From Build 55.20] [# 550946]

- **Using Certificates to Log on to a SAML IdP**

  When used as a SAML IdP (identity provider), the NetScaler appliance now allows logon using certificates.

  [From Build 55.20] [# 512125]

- **Using Cookies to Track SAML Sessions**

  In a deployment where a NetScaler appliance is configured as a SAML IdP (identity provider) for multiple SAML SPs (service provider), the appliance allows a user to access multiple SPs without explicitly authenticating every time.The appliance creates a session cookie for the first authentication and every subsequent request uses this cookie for authentication.

  [From Build 55.20] [# 503882]

- **Including Additional Attributes in SAML IdP Assertion**

  When used as a SAML IdP (identity provider), the NetScaler appliance can now be configured to send 16 additional attributes in addition to the NameId attribute. These attributes must be extracted from the appropriate authentication server. For each of them, you can specify the name, the expression, the format, and a friendly name.

  These attributes must be specified in the SAML IdP profile as follows:

  From the CLI:

  > set authentication samlIdPProfile <name> [-Attribute1 <string> -Attribute1Expr <string> [-Attribute1FriendlyName <string>] [-Attribute1Format (URI | Basic)]] [-Attribute2 <string> -Attribute2Expr <string> [-Attribute2FriendlyName <string>] [-Attribute2Format (URI | Basic)]]

  For example, the following command adds the attribute "MyName":

  > add authentication samlIdPProfile ns-saml-idp -samlSPCertName nssp -samlIdPCertName nssp -assertionConsumerServiceURL "http://nssp.nsi-test.com/cgi/samlauth" -Attribute1 MyName -Attribute1Expr http.req.user.name -Attribute1FriendlyName Username -Attribute1Format URI

  From the GUI:

  Navigate to the screen where you configure the SAML IdP profile, and specify the additional attributes as required.

[From Build 55.20] [# 460680, 504703]

- **Using the SHA256 Algorithm to Sign SAML IdP Assertions**

  When used as a SAML IdP (identity provider), the NetScaler appliance can now be configured to digitally sign assertions by using the SHA256 algorithm. Additionally, you can configure the appliance to accept only digitally signed requests from the SAML SP (service provider).

  These configurations must be specified in the SAML IdP profile as follows:

  From the CLI:

  > set authentication samlIdPProfile <name> [-rejectUnsignedRequests (ON | OFF)] [-signatureAlg (RSA-SHA1 | RSA-SHA256)] [-digestMethod (SHA1 | SHA256)]

  From the GUI:

  Navigate to the screen where you configure the SAML IdP profile, and specify the corresponding parameters.

  [From Build 55.20] [# 474977]

- The configuration of a AAA-TM virtual server in the NetScaler GUI is simplified for ease of configuring the required authentication mechanism.

  [From Build 55.20] [# 524386]

- The output of "show ns ip" now also includes the aaadnatIp address.

  [From Build 55.20] [# 472912]

- **Using 401-based Authentication to Log on to a SAML IdP**

  When used as a SAML IdP (identity provider), the NetScaler appliance now allows logon using the following 401-based authentication mechanisms: Negotiate, NTLM, and Certificate.

  [From Build 55.20] [# 496725, 508689]

- The NetScaler appliance now supports the SiteMinder SAML SP.

  [From Build 55.20] [# 488077]

- **Encrypting SAML IdP Assertion**

  When used as a SAML IdP (identity provider), the NetScaler appliance can now be configured to encrypt the assertions by using the public key of the SAML SP (service provider).

  Note:

  - Make sure the SAML SP certificate is specified.

  - For enhanced security, it is recommended that you encrypt assertions that contain sensitive information.

This configuration must be specified on the SAML IdP profile as follows:

On the CLI:

> set authentication samlIdPProfile <name> [-encryptAssertion (ON | OFF)] [-encryptionAlgorithm <encryptionAlgorithm>]

On the GUI:

Navigate to the screen where you configure the SAML IdP profile and specify the corresponding parameters.

[From Build 55.20] [# 482185]

- **Fallback to NTLM Authentication**

  When the NetScaler appliance is configured for Negotiate authentication and sends a 401 Negotiate response to client, if client is not able to reach domain controller or is not domain joined, then it automatically falls back to NTLM authentication and the client starts NTLM handshake. The NetScaler appliance is able to verify the credentials presented as part of NTLM authentication.

  This feature allows user logins locally or remotely.

  [From Build 55.20] [# 509829]

- **Logging Errors in NetScaler Log Files**

  The NetScaler appliance now stores AAA authentication logs.

  - Errors and warnings are logged in the /var/nslog/ns.log file

  - Information and debug level logs are logged in the /var/log/nsvpn.log file.

  [From Build 55.20] [# 482228, 479557]

- **Support for Redirect Binding for SAML SP**

  When used as a SAML SP (service provider), in addition to POST bindings, the NetScaler appliance now supports redirect bindings. In redirect bindings, SAML assertions are in the URL, as against POST bindings where the assertions are in the POST body.

  Using the CLI:

  > add authentication samlAction <name> . . . [-samlBinding (REDIRECT | POST)]

  [From Build 55.20] [# 493220, 462777, 493224]

- **Multi-Factor (nFactor) Authentication**

  The NetScaler appliance now supports a new approach to configuring multi-factor authentication. With this approach, you can configure any number of authentication factors. You can also customize the login form as required.

  In NetScaler terminology, this feature is called "nFactor Authentication." For more information, see

http://docs.citrix.com/en-us/netscaler/11/security/ns-aaa-app-trafc-wrapper-con-10/multi-factor-nfactor-authentication.html.

[From Build 62.10] [# 482250, 451913, 549966]

Admin Partitions

- **Getting Web Logs for Specific Partitions/Users**

  Using the NetScaler Web Logging (NSWL) client, the NetScaler can now retrieve the web logs for all the partitions with which the logged in user is associated. To view the partition for each log entry, customize the log format to include the %P option. You can then filter the logs to view the logs for a specific partition.

  [From Build 55.20] [# 534986]

- **Getting NetScaler Trace for Specific Partitions**

  You can now generate the NetScaler trace for a specific admin partition. To do so, you must access that admin partition and run the "nstrace" operation. The trace files for the admin partition will be stored in the /var/partitions/<partitionName>/nstrace/ directory.

  [From Build 55.20] [# 496937, 515294]

- Scriptable monitors can now be configured on the admin partitions that are available on a NetScaler appliance.

  [From Build 55.20] [# 535494]

- **Supporting Dynamic Routing in Admin Partitions**

  While dynamic routing (OSPF, RIP, BGP, ISIS, BGP+) is by default enabled on the default partition, in an admin partition, it must be enabled by using the following command:

  > set L3Param -dynamicRouting ENABLED

  Note: A maximum of 63 partitions can run dynamic routing (62 admin partitions and 1 default partition).

  [From Build 55.20] [# 514848]

- **Configuring Integrated Caching on a Partitioned NetScaler**

  Integrated caching (IC) can now be configured for admin partitions. After defining the IC memory on the default partition, the superuser can configure the IC memory on each admin partition such that the total IC memory allocated to all admin partitions does not exceed the IC memory defined on the default partition. The memory that is not configured for the admin partitions remains available for the default partition.

  For example, if a NetScaler appliance with two admin partitions has 10 GB of IC memory allocated to the default partition, and IC memory allocation for the two admin partitions is as follows:

  - Partition1: 4 GB

  - Partition2: 3 GB

Then, the default partition has 10 - (4 + 3) = 3 GB of IC memory available for use.

Note: If all IC memory is used by the admin partitions, no IC memory is available for the default partition.

[From Build 55.20] [# 481444, 484618]

- **Setting L2 and L3 parameters in Admin Partitions**

  On a partitioned NetScaler appliance, the scope of updating the L2 and L3 parameters is as follows:

  - For L2 parameters that are set by using the "set L2Param" command, the following parameters can be updated only from the default partition, and their values are applicable to all the admin partitions: maxBridgeCollision, bdgSetting, garpOnVridIntf, garpReply, proxyArp, resetInterfaceOnHAfailover, and skip_proxying_bsd_traffic. The other L2 parameters can be updated in specific admin partitions, and their values are local to those partitions.

  - For L3 parameters that are set by using the "set L3Param" command, all parameters can be updated in specific admin partitions, and their values are local to those partitions. Similarly, the values that are updated in the default partition are applicable only to the default partition.

  [From Build 55.20] [# 513564]

- **Partition Specific Load Balancing Parameters**

  When you update load balancing parameters in an admin partition, the updates now apply to that partition only. You can have different load balancing parameter settings in different partitions.

  Note:

  - In previous releases, any updates to these parameters were applied across all partitions, regardless of the partition in which the changes were made.

  - These parameters are set in the CLI by using the "set lb parameter" command or in the GUI by navigating to Traffic Management > Load Balancing.

  [From Build 62.10] [# 563004]

Application Firewall

- All application firewall graphical user interface (GUI) dialog boxes, including the ones for signatures, visualizer, and syslog viewer, are now completely free from any java dependencies and show a significant improvement in the overall performance. The HTML based GUI dialogues have been re-organized for enhanced user experience and intuitive workflow of information. Instead appearing in of pop-up dialog boxes with tabs, the information is now displayed as an in-line expansion. You can expand all the configuration sections and scroll up and down for a comprehensive view.

  [From Build 55.20] [# 506157]

- The field format rules specify the inputs that are allowed in the target form fields. You can also limit the minimum and the maximum allowed length for the inputs. The application

firewall learning engine monitors the traffic and provides field format recommendations based on the observed values. If the initial field format learned rules are based on a small sample of data, a few non typical values might possibly result in a recommendation that is too lenient for the target field. Updates to the application firewall have now decoupled violations and learning for the field formats. The firewall learns the field formats regardless of the violations. The learning engine monitors and evaluates all the incoming new data points to recommend new rules. This allows fine tuning the configuration to specify optimal input formats with adequate min/max range values. If a rule has already been deployed for a field/URL combination, the GUI allows the user to update the field format. A dialog box asks for confirmation to replace the existing rule. If you are using the command line interface, you have to explicitly unbind the previous binding and then bind the new rule.

[From Build 55.20] [# 450326, 483677, 513927]

- The application firewall is fully supported in striped, partially striped, or spotted configurations. The two main advantages of striped and partially striped virtual server support in cluster configurations are the following:

  - Session failover support: Striped and partially striped virtual server configurations support session failover. The advanced application firewall security features, such as Start URL Closure and the Form Field Consistency check, maintain and use sessions during transaction processing. In ordinary high availability configurations, or in spotted cluster configurations, when the node that is processing the application firewall traffic fails, all the session information is lost and the user has to reestablish the session. In striped virtual server configurations, user sessions are replicated across multiple nodes. If a node goes down, a node running the replica becomes the owner. Session information is maintained without any visible impact to the user.

  - Scalability: Any node in the cluster can process the traffic. Multiple nodes of the cluster can process the incoming requests served by the striped virtual server. This improves the application firewall's ability to handle multiple simultaneous requests, thereby improving the overall performance.

  Security checks and signature protections can be deployed without the need for any additional cluster-specific application firewall configuration. You just do the usual application firewall configuration on the configuration coordinator (CCO) node for propagation to all the nodes.

  Cluster details are available at http://docs.citrix.com/en-us/netscaler/11/system/clustering.html.

  [From Build 55.20] [# 408831, 403780]

- The NetScaler application firewall module offers data leak prevention and supports credit card protection. It can examines the credit card numbers in the response and takes the specified action if a match is found. In some scenarios, it might be desirable to exclude a specific set of numbers from the credit card security check inspection. For example, server responses for some internet applications might include a string of digits that is not a credit card number but matches the pattern of a credit card number. These responses can trigger false positives and therefore get blocked by the application firewall's Credit Card security check. The application firewall now offers the ability to learn and deploy relaxations for the credit card numbers. The credit card relaxation rule provides the flexibility to exclude a

specific string of numbers from the safe commerce check without compromising credit card security. These numbers are not examined in the responses even if the credit card check is ON.

Examples of CLI Commands:

1. Bind the credit card number to profile:

bind appfw profile <profile-name> -creditCardNumber <any number/regex> "<url>"

2. Unbind credit card number from profile:

unbind appfw profile <profile-name> -creditCardNumber <credit card number> "<url>"

3. Log: Enable Logging of credit card Numbers

add appfw profile <profilename> - doSecureCreditCardLogging <ON/OFF>

set appfw profile <profilename> - doSecureCreditCardLogging <ON/OFF>

4. Learn:

show appfw learningdata <profilename> creditCardNumber

rm appfw learningdata <profilename> -creditcardNumber <credit card number> "<url>"

export appfw learningdata <profilename> creditCardNumber

[From Build 55.20] [# 383298]

- All application firewall graphical user interface (GUI) dialog boxes, including the ones for signatures, visualizer, and syslog viewer, are now completely free from any java dependencies and show a significant improvement in the overall performance. The HTML based GUI dialogues have been re-organized for enhanced user experience and intuitive workflow of information. Instead appearing in of pop-up dialog boxes with tabs, the information is now displayed as an in-line expansion. You can expand all the configuration sections and scroll up and down for a comprehensive view.

  [From Build 55.20] [# 520048]

- Geolocation, which identifies the geographic location from which requests originate, can help you configure the application firewall for the optimal level of security. For example, if an excessively large number of requests are received from a specific area, it is easy to determine whether they are being sent by users or a rogue machine. The application firewall offers you the convenience of using the built-in NetScaler database or any other geolocation based database to identify the source of origin of coordinated attacks launched from a country. This information can be quite useful for enforcing the optimal level of security for your application to block malicious requests originating from a specific geographical region. Geolocation logging uses the Common Event Format (CEF).

  To use Geolocation Logging

  1. Enable CEFLogging and GeoLocationLogging.

  >set appfw settings GeoLocationLogging ON CEFLogging ON

2. Specify the database

>add locationfile /var/netscaler/inbuilt_db/Citrix_Netscaler_InBuilt_GeoIP_DB.csv

or

add locationfile <path to database file>

[From Build 55.20] [# 483703]

- The NetScaler application firewall offers SQL/XSS security check protections to detect and block possible attacks against the applications. You now have much tighter security control when configuring SQL/XSS protections. Instead of deploying relaxation rules that completely bypass the security check inspection for a field, you now have an option to relax a specific subset of violation patterns. You can continue to inspect the relaxed field in the incoming requests to detect and block the rest of the SQL/XSS violation patterns. The commands used in relaxations and learning now have optional parameters for value type and value expression. You can specify whether the value expression is a regular expression or a literal string.

  Command Line Interface:

  bind appfw profile <name> -SQLInjection <String> [isNameRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Keyword| SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]

  unbind appfw profile <name> -SQLInjection <String><formActionURL> [-location <location>][-valueType (Keyword|SpecialString|Wildchar) [<valueExpression>]]

  bind appfw profile <name> -crossSiteScripting <String> [isNameRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag| Attribute|Pattern) [<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]

  unbind appfw profile <name> -crossSiteScripting <String> <formActionURL> [-location <location>] [-valueType (Tag|Attribute|Pattern) [<valueExpression>]]

  [From Build 55.20] [# 450324, 483683]

Cache Redirection

- **Support for default syntax expressions**

  You can now use default syntax expressions in cache redirection policies. The NetScaler appliance provides built-in cache redirection policies based on default syntax expressions, or you can create custom cache redirection policies to handle typical cache requests. In addition to the same types of evaluations done by classic cache redirection policies, the default syntax policies enable you to analyze more data (for example, the body of an HTTP request) and to configure more operations in the policy rule (for example, directing requests to either cache or origin server).

  [From Build 55.20] [# 490297, 495915, 536986, 536992, 537010, 537014, 538269]

Cluster

- **Routing in a L3 Cluster**

In a L3 cluster, different nodegroups can have different VLANs and subnets associated with them. This can result in a VLAN getting exposed only in some nodes. Therefore, you can now configure dynamic routing on a VLAN to expose the VLAN to ZebOS even when there are no IP addresses with dynamic routing that are bound to it. The command to configure this is:

> add/set vlan <id> -dynamicRouting (ENABLED | DISABLED)

Note:

- This option is also available for VXLAN and BridgeGroups.

- This configuration can also be used for L2 clusters.

[From Build 55.20] [# 531868]

- **Disabling Steering on the Cluster Backplane**

  By default, a NetScaler cluster steers traffic over the cluster backplane, from the flow receiver node to the flow processor node. You can disable steering so that the process becomes local to the flow receiver and thereby ensure that the flow receiver also becomes the flow processor. Such a configuration can come in handy when you have a high latency link.

  Note: This configuration is applicable only for striped virtual servers.

  Steering can be disabled at the global NetScaler level or at the individual virtual server level. The global configuration takes precedence over the virtual server setting.

  - At the global level, steering can be disabled for all striped virtual servers. It is configured at cluster instance level. Traffic meant for any striped virtual server will not be steered on cluster backplane. The command is:

  > add cluster instance <clId> -processLocal ENABLED

  - At a virtual server level, you can disable steering for a specific striped virtual server. It is configured on a striped virtual server. Traffic meant for that virtual server will not be steered on cluster backplane. The command is:

  > add lb vserver <name> <serviceType> -processLocal ENABLED

  For more information, see http://docs.citrix.com/en-us/netscaler/11/system/clustering/cluster-managing/cluster-steering-disable.html.

  [From Build 55.20] [# 539136]

- **Nodegroup for Datacenter Redundancy**

  A cluster nodegroup can now be configured to provide datacenter redundancy. In this use case, nodegroups are created by logically grouping the cluster nodes. You must create active and spare nodegroups. When the active nodegroup goes down, the spare nodegroup which has the highest priority (the lower priority number) is made active and it starts serving traffic.

For more information, see http://docs.citrix.com/en-us/netscaler/11/system/clustering/cluster-managing/cluster-nodegroups-datacenter-redundancy.html.

[From Build 55.20] [# 495019]

- **Reduce Backplane Steering for Spotted and Partially-striped Virtual Serves when Using ECMP**

  With the Equal Cost Multiple Path (ECMP) mechanism, virtual server IP addresses are advertised by all active cluster nodes. This means that traffic can be received by any cluster node, which then steers the traffic to the node that must process the traffic. While there are no hassles in this approach, there can be a lot of redundant steering in case of spotted and partially striped virtual servers. Therefore, from NetScaler 11 onwards, spotted and partially striped virtual server IP addresses are advertised only by the owner nodes. This reduces the redundant steering.

  You can override this default behavior, by entering the following command in the VTYSH shell:

  ns(config)# ns spotted-vip-adv all-nodes

  [From Build 55.20] [# 317706]

- **Routing on Striped SNIP addresses**

  You can now run dynamic routing on a striped SNIP address in a NetScaler cluster. The routes advertised by the cluster have the striped SNIP as the next hop. There is just one adjacency with the cluster. Internally, the cluster picks one of the active nodes as the routing leader. When the current routing leader goes down, the routing ownership moves to an active node.

  Note:

  - Striped SNIP addresses are useful mainly for cluster LA (link aggregation) deployments. They can also be used for ECMP, but the multipath routing functionality is unavailable.

  - Striped SNIP addresses can also be used in asymmetrical topologies.

  - Routing on striped SNIPs and routing on spotted SNIPs can coexist in a cluster.

  To specify leader node configurations, in the VTYSH shell, use the "owner-node leader" command.

  [From Build 55.20] [# 329439]

- BridgeGroups are now supported in a NetScaler cluster deployment.

  [From Build 55.20] [# 494991]

- **Cluster to Include Nodes from Different Networks (L3 Cluster)**

  You can now create a cluster that includes nodes from different networks. To configure a cluster over L3, you must add the nodes of different networks to different nodegroups. For

more information, see http://docs.citrix.com/en-us/netscaler/11/system/clustering/cluster-setup.html.

You can transition an existing L2 cluster to an L3 cluster. For instructions, see http://docs.citrix.com/en-us/netscaler/11/system/clustering/cluster-usage-scenarios/cluster-migrate-between-l2-l3.html.

[From Build 55.20] [# 374289, 317257]

- **Link Redundancy based on Minimum Throughput**

  In a dynamic cluster link aggregation (LA) deployment that has link redundancy enabled, you can configure the cluster to select the partner channel or interface on the basis of its throughput. To do this, configure a threshold throughput on the channel or interface as follows:

  > set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer>

  The throughput of the partner channels is checked against the configured threshold throughput. The partner channel that satisfies the threshold throughput is selected in FIFO manner. If none of the partner channel meets the threshold, or if threshold throughput is not configured, the partner channel with the maximum number of links is selected.

  [From Build 55.20] [# 508993]

- **Web Interface on NetScaler (WIonNS) Support on a Cluster**

  WIonNS can now be configured on a NetScaler cluster deployment. To use WIonNS on a cluster, you must do the following:

  1. Make sure that the Java package and the WI package are installed in the same directory on all the cluster nodes.

  2. Create a load balancing virtual server that has persistency configured.

  3. Create services with IP addresses as the NSIP address of each of the cluster nodes that you want to serve WI traffic.

  4. Bind the services to the load balancing virtual server.

  Note: If you are using WIonNS over a VPN connection, make sure that the load balancing virtual server is set as WIHOME.

  [From Build 62.10] [# 498295, 489463]

- **FTP Load Balancing Support on a Cluster**

  FTP load balancing is now supported in a NetScaler cluster deployment.

  [From Build 62.10] [# 513612]

DNS

- **Enable or disable negative caching of DNS records**

The NetScaler appliance supports caching of negative responses for a domain. You can enable or disable negative caching from the command line, by setting cacheNegativeResponses with the set dns parameter command, or in the configuration utility, in the Configure DNS Parameters dialog box.

Note: You can enable or disable negative caching independent of global caching. By default, negative caching is enabled.

[From Build 55.20] [# 391254]

- **Rewrite and responder support for DNS**

  The rewrite and responder features now support DNS. You can now configure rewrite and responder functionalities to modify DNS requests and responses as you would for HTTP or TCP requests and responses.

  [From Build 55.20] [# 405769]

- **Support for DNS Logging**

  You can now configure a NetScaler appliance to log DNS requests and responses. The logs are in SYSLOG format. You can use these logs to:

  - Audit the DNS responses to the client

  - Audit DNS clients

  - Detect and prevent DNS attacks

  - Troubleshoot

  [From Build 55.20] [# 419632, 561291]

GSLB

- Support for binding a single Virtual Server as a backup for multiple GSLB Virtual servers

  In a GSLB site deployment, you can now bind a single virtual server as a backup virtual server for multiple GSLB virtual servers in the deployment.

  [From Build 55.20] [# 373061]

- **GSLB Service Selection using Content Switching**

  Description: You can now configure a content switching (CS) policy to customize a GSLB deployment so that you can:

  * Restrict the selection of a GSLB service to a subset of GSLB services bound to a GSLB virtual server for the given domain.

  * Apply different Load Balancing methods on the different subsets of GSLB services in the deployment.

  * Apply spillover policies on a subset of GSLB services, and you can have a backup for a subset of GSLB services.

* Configure a subset of GSLB services to serve a specific type of content.

* Define a subset GSLB services with different priorities, and define the order in which the services in the subset are applied to a request.

For more information, see Configuring GSLB Service Selection Using Content Switching.

[From Build 63.16] [# 503588]

HDX Insight

- HDX Insight now supports displaying of Appflow records from Netscaler cluster.

  [From Build 62.10] [# 525758]

Load Balancing

- **IPv6 Support for HTTP based User Monitors**

  You can now use IPv6 addresses in the following monitors:

  - USER

  - SMTP

  - NNTP

  - LDAP

  - SNMP

  - POP3

  - FTP_EXTENDED

  - STOREFRONT

  - APPC

  - CITRIX_WI_EXTENDED

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

  [From Build 55.20] [# 510111]

- **Support for Secure LDAP Monitor**

  You can now monitor LDAP services over SSL. To monitor the LDAP services over SSL, use the built-in LDAP monitor or create a user monitor and enable the "secure" option.

  [From Build 55.20] [# 418061, 556530]

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

  At the NetScaler command prompt, type:

  set lb parameter -useSecuredPersistenceCookie Enabled-cookiePassphrase test

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

[From Build 55.20] [# 347108, 323325, 348588]

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

  [From Build 55.20] [# 524079, 559022]

- **Automatic Restart of the Internal Dispatcher**

  In earlier releases, if the internal dispatcher failed, the services that used scriptable monitors also went down and the appliance had to be restarted. From release 11, if the internal dispatcher fails, the pitboss process restarts it. As a result, you no longer have to restart the appliance. For information about user monitors, see http://docs.citrix.com/en-us/netscaler/11/traffic-management/load-balancing/load-balancing-custom-monitors/understand-user-monitors.html.

  [From Build 55.20] [# 368128]

- The following global timeouts has been introduced for TCP sessions on a NetScaler appliance related to RNAT rules, forwarding sessions, or load balancing configuration of type ANY:

  * Any TCP Client. Global idle timeout, in seconds, for TCP client connections. Client timeout set for an entity overrides the global timeout setting.

  * Any TCP Server. Global idle timeout, in seconds, for TCP server connections. Server timeout set for an entity overrides the global timeout setting.

  These timeout can be set either from the NetScaler command line (set ns timeout command) or from the configuration utility (System > Settings > Change Timeout Values page).

  Note: For applying these timeouts to a virtual server or service of type ANY, set these timeouts before adding the virtual server or the service.

  [From Build 55.20] [# 507701]

- **New Trap for Spillover**

  If you have configured spillover on a virtual server and also configured a trap listener on the appliance, an SNMP trap is now sent to the trap listener when the virtual server experiences spillover. The trap message displays the name of the virtual server that experienced the spillover, the spillover method, the spillover threshold, and the current spillover value. If the spillover is policy based, the rule causing it appears in the Spillover Threshold field. If the virtual server is DOWN or disabled, the status message "vserver not up" appears in the trap message.

  [From Build 55.20] [# 486268, 475400]

- **Setting the Maintenance State for your Server with Minimal Interruption**

You can now set the maintenance state for your server with minimal interruption and without changing any configuration on the NetScaler appliance. In the maintenance state, the server continues to accept persistent client connections while new connections are load balanced among the active servers. On the NetScaler appliance, configure a transition out of service (TROFS)-enabled monitor and bind it to a service representing the server. Specify a trofsCode or trofsString in the monitor. Upon receipt of a matching code or string from the server in response to a monitor probe, the appliance places the service in the TROFS state. During this time, it continues to honor persistent client connections.

To avoid disrupting established sessions, you can place a service in the TROFS state by doing one of the following:

- Adding a TROFS code or string to the monitorâ€”Configure the server to send a specific code or string in response to a monitor probe.

Note: This enhancement is available from release 10.5 build 56.16.

- Explicitly disable the service and:

- Set a delay (in seconds).

- Enable graceful shut down.

Adding a TROFS Code or String

Note: This enhancement is not applicable to GSLB services.

From release 10.5, build56.16, if you bind only one monitor to a service, and the monitor is a TROFS-enabled monitor, it can place the service in the TROFS state on the basis of the server's response to a monitor probe. This response is compared with the value in the trofsCode parameter for an HTTP monitor or the trofsString parameter for an HTTP-ECV or TCP-ECV monitor. If the code matches, the service is placed in the TROFS state. In this state, it continues to honor the persistent connections.

If multiple monitors are bound to a service, the effective state of the service is calculated on the basis of the state of all the monitors that are bound to the service. Upon receiving a TROFS response, the state of the TROFS-enabled monitor is considered as UP for the purpose of this calculation. For more information about how a NetScaler appliance designates a service as UP, see http://docs.citrix.com/en-us/netscaler/11/traffic-management/load-balancing/load-balancing-advanced-settings/set-monitor-threshold.html.

Important!

- You can bind multiple monitors to a service, but only one monitor must be TROFS-enabled.

- You can convert a TROFS-enabled monitor to a monitor that is not TROFS-enabled, but not vice versa.

[From Build 55.20] [# 408103]

NetScaler Insight Center

- You can configure NetScaler Insight Center to display the geo maps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

  [From Build 55.20] [# 502478]

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

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

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

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

  [From Build 55.20] [# 490147, 482900]

- **Hop Diagram Support**

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

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

  [From Build 55.20] [# 443824]

- You can now configure NetScaler Insight Center to display the reports in your local time or GMT time.

  [From Build 55.20] [# 491073]

- You can now increase the storage space of NetScaler Insight Center to 512 GB.

  [From Build 55.20] [# 425761, 553254]

- The NetScaler Insight Center configuration utility now displays the progress of the upgrade process.

  [From Build 55.20] [# 519788, 522021]

- Multi-Hop support for NetScaler Insight Center enables Insight Center to detect which Citrix appliances a connection passes through and in which order, for improved reporting.

  [From Build 55.20] [# 383172]

- You can now configure a DNS server when you set up NetScaler Insight Center. Configuring a DNS server helps resolve the host name of a server into its IP address.

For example, while creating an email server, you now have an option to specify the server name of the server rather than the IP address.

[From Build 55.20] [# 514612]

- **Exporting Reports**

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

  For more information, see http://docs.citrix.com/en-us/netscaler-insight/11-0/viewing-reports/ni-export-report-con.html.

  [From Build 55.20] [# 320860]

Networking

- **Logging HTTP Header Information**

  The NetScaler appliance can now log header information of HTTP requests related to an LSN configuration. The following header information of an HTTP request packet can be logged:

  - URL that the HTTP request is destined to.

  - HTTP Method specified in the HTTP request.

  - HTTP version used in the HTTP request.

  - IP address of the subscriber that sent the HTTP request.

  An HTTP header log profile is a collection of HTTP header attributes (for example, URL and HTTP method) that can be enabled or disabled for logging. The HTTP header log profile is then bound to an LSN group. The NetScaler appliance then logs HTTP header attributes, which are enabled in the bound HTTP header log profile for logging, of any HTTP requests related to the LSN group.

  An HTTP header log profile can be bound to multiple LSN groups but an LSN group can have only one HTTP header log profile.

  [From Build 55.20] [# 496835]

- **Configuring Communication Intervals for an Active-Active Deployment**

  In an active-active deployment, all NetScaler nodes use the Virtual Router Redundancy Protocol (VRRP) to advertise their master VIP addresses and the corresponding priorities in VRRP advertisement packets (hello messages) at regular intervals.

  VRRP uses the following communication intervals:

  * Hello Intervalâ€”Interval between successive VRRP hello messages that a node sends, for all of its active (master) VIP addresses, to the other nodes of the VRRP deployment. For a VIP address, nodes on which the VIP address is in the inactive state use the hello messages as verification that the master VIP address is still UP.

* Dead Intervalâ€”Time after which a node of a backup VIP address considers the state of the master VIP address to be DOWN if VRRP hello messages are not received from the node that has the master VIP address. After the dead interval, the backup VIP address takes over and becomes the master VIP address.

You can change these intervals to a desired value on each node. They apply to all VIP addresses on that node.

[From Build 55.20] [# 512843]

- **Changing the Priority of a VIP Address Automatically in an Active-Active Deployment**

  To ensure that a backup VIP address takes over as the master VIP before the node of the current master VIP address goes down completely, you can configure a node to change the priority of a VIP address on the basis of the states of the interfaces on that node. For example, the node reduces the priority of a VIP address when the state of an interface changes to DOWN, and increases the priority when the state of the interface changes to UP. This feature is configured on each node. It applies to the specified VIP addresses on the node.

  To configure this feature on a node, you set the Reduced Priority (trackifNumPriority) parameter, and then associate the interfaces whose state is to be tracked for changing the priority of the VIP address. When any associated interface's state changes to DOWN or UP, the node reduces or increases the priority of the VIP address by the configured Reduced Priority (trackifNumPriority) value.

  [From Build 55.20] [# 512848]

- **Support of IPv6 Dynamic Routing Protocols on VXLANs**

  The NetScaler appliance supports IPv6 dynamic routing protocols for VXLANs. You can configure various IPv6 Dynamic Routing protocols (for example, OSPFv3, RIPng, BGP) on VXLANs from the VTYSH command line. An option IPv6 Dynamic Routing Protocol has been added to VXLAN command set for enabling or disabling IPv6 dynamic routing protocols on a VXLAN. After enabling IPv6 dynamic routing protocols on a VXLAN, processes related to the IPv6 dynamic routing protocols are required to be started on the VXLAN by using the VTYSH command line.

  [From Build 55.20] [# 472432]

- The NetScaler appliance supports sending static IPv6 routes through a VXLAN. You can enable the NetScaler appliance to send an IPv6 route through either a VXLAN or a VLAN. A VXLAN parameter is added to the static IPv6 route command set.

  [From Build 55.20] [# 472443]

- **Jumbo Frames Support for NetScaler VPX Appliances**

  NetScaler VPX appliances now support receiving and transmitting jumbo frames containing up to 9216 bytes of IP data. Jumbo frames can transfer large files more efficiently than is possible with the standard IP MTU size of 1500 bytes.

  A NetScaler appliance can use jumbo frames in the following deployment scenarios:

- Jumbo to Jumbo. The appliance receives data as jumbo frames and sends it as jumbo frames.

- Non-Jumbo to Jumbo. The appliance receives data as regular frames and sends it as jumbo frames.

- Jumbo to Non-Jumbo. The appliance receives data as jumbo frames and sends it as regular frames.

Jumbo Frames support is available on NetScaler VPX appliances running on the following virtualization platforms:

- VMware ESX (Note that NetScaler VPX appliances running on VMware ESX support receiving and transmitting jumbo frames containing up to only 9000 bytes of IP data.)

- Linux-KVM

For configuring Jumbo Frames on a NetScaler VPX appliance, you must:

- Set the MTU of the interface or channel of the VPX appliance to a value in the range 1501-9216. Use the NetScaler command line interface or the configuration utility of the VPX appliance to set the MTU size.

- Set the same MTU size on the corresponding physical interfaces of the virtualization host by using its management applications.

[From Build 55.20] [# 464830, 478103, 485905]

- **OSPFv3 Authentication**

  For ensuring the integrity, data origin authentication, and data confidentiality of OSPFv3 packets, OSPFv3 authentication must be configured on OSPFv3 peers.

  The NetScaler appliance supports OSPFv3 authentication and is partially compliant with RFC 4552. OSPFv3 authentication is based on the two IPSec protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). The NetScaler supports only the AH protocol for OSPFv3 authentication.

  OSPFv3 authentication use manually defined IPSec Security Associations (SAs) between the OSPFv3 peers and does not rely on IKE protocol for forming dynamic SAs. Manual SAs define the security parameter Index (SPI) values, algorithms, and keys to be used between the peers. Manual SAs require no negotiation between the peers; therefore, same SA must be defined on both the peers.

  You can configure OSPFv3 authentication on a VLAN or for an OSPFv3 area. When you configure for a VLAN, the settings are applied to all the interfaces that are member of the VLAN. When you configure OSPFv3 authentication for an OSPF area, the settings are applied to all the VLANs in that area. The settings are in turn applied to all the interfaces that are members of these VLANs. These settings do not apply to member VLANs on which you have configured OSPFv3 authentication directly.

  [From Build 55.20] [# 471703]

- **Specifying a VLAN in a Static ARP Entry**

In a static ARP entry, you can specify the VLAN through which the destination device is accessible. This feature is useful when the interface specified in the static ARP entry is part of multiple tagged VLANs and the destination is accessible through one of the VLANs. The NetScaler appliance includes the specified VLAN ID in the outgoing packets matching the static ARP entry. If you don't specify a VLAN ID in an ARP entry, and the specified interface is part of multiple tagged VLANs, the appliance assigns the interface's native VLAN to the ARP entry.

For example, say NetScaler interface 1/2 is part of native VLAN 2 and of tagged VLANs 3 and 4, and you add a static ARP entry for network device A, which is part of VLAN 3 and is accessible through interface 1/2. You must specify VLAN 3 in the ARP entry for network device A. The NetScaler appliance then includes tagged VLAN 3 in all the packets destined to network device A, and sends them from interface 1/2.

If you don't specify a VLAN ID, the NetScaler appliance assigns native VLAN 2 for the ARP entry. Packets destined to device A are dropped in the network path, because they do not specify tagged VLAN 3, which is the VLAN for device A.

[From Build 55.20] [# 520355]

- **Redundant Interface Sets**

  A redundant interface set is a set of interfaces in which one interface is active and the others are on standby. If the active interface fails, one of the standby interfaces takes over and becomes active.

  Following are the main benefits of using redundant interface sets:

  - The back-up links between the NetScaler appliance and a peer device ensure connection reliability.

  - Unlike link redundancy using LACP, no configuration is required on the peer device for a redundant interface set. To the peer device, a redundant interface set appears as individual interfaces, not as a set or collection.

  - In a high availability (HA) configuration, redundant interface sets can minimize the number the HA failovers.

  A redundant interface set is specified in LR/X notation, where X can range from 1 to 4. For example, LR/1.

  [From Build 55.20] [# 355237, 186503, 249551]

- **GRE Payload Options in a GRE IP Tunnel**

  For a configured GRE IP tunnel, the NetScaler appliance encapsulates the entire Layer 2 packet, including the Ethernet header and the VLAN header (dot1q VLAN tag). IP GRE tunnels between NetScaler appliances and some 3rd party devices might not be stable, because these 3rd party devices are not programmed to process some or the Layer 2 packet headers.

  To configure a stable IP GRE tunnel between a NetScaler appliance and a 3rd party device, you can use a new parameter with the GRE IP tunnel command set. You can set the GRE

payload parameter to do one of the following before the packet is sent through the GRE tunnel:

- Carry the Ethernet header but drop the VLAN header

- Drop the Ethernet header as well as the VLAN header

- Carry the Ethernet header as well the VLAN header

[From Build 55.20] [# 518397]

- **Blocking Traffic on Internal Ports**

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

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

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

  At the command prompt, type:

  > set l3param -implicitACLAllow [ENABLED|DISABLED]

  Note: The parameter implicitACLAllow is enabled by default.

  Example

  > set l3param -implicitACLAllow DISABLED

  Done

  [From Build 55.20] [# 529317]

- **As-Override Support in Border Gateway Protocol**

  As a part of BGP loop prevention functionality, if a router receives a BGP packet containing the router's Autonomous System Number (ASN) in the Autonomous Systems (AS) path, the router drops the packet. The assumption is that the packet originated from the router and has reached the place from where it originated.

  If an enterprise has several sites with a same ASN, BGP loop prevention causes the sites with an identical ASN to not get linked by another ASN. Routing updates (BGP packets) are dropped when another site receives them.

  To solve this issue, BGP AS-Override functionality has been added to the ZebOS BGP routing module of the NetScaler.

  With AS-Override enabled for a peer device, when the NetScaler appliance receives a BGP packet for forwarding to the peer, and the ASN of the packet matches that of the peer, the

appliance replaces the ASN of the BGP packet with its own ASN number before forwarding the packet.

[From Build 55.20] [# 503566]

- **Client Source Port for Server Side Connections related to INAT and RNAT Rules**

  The NetScaler appliance, for INAT and RNAT rules, now supports using client port as the source port for server side connections. A parameter Use Proxy Port has been added to the INAT and RNAT command set. When Use Proxy Port is disabled for an INAT rule or a RNAT rule, the NetScaler appliance retains the source port of the client's request for the server side connection. When the option is enabled (default), the NetScaler appliance uses a random port as the source port for the server side connection.

  You must disable this parameter for proper functioning of certain protocols that require a specific source port in the request packet.

  [From Build 55.20] [# 399821]

- **Layer 2 PBR Support for Forwarding Sessions**

  In earlier releases, Layer 2 information (for example, destination MAC address, source VLAN, and Interface ID) about packets related to forwarding sessions were ignored during a PBR lookup. In other words, any packet related to a forwarding session was not considered for matching against a PBR having Layer 2 parameters as its condition.

  Now, layer 2 information about a packet related to a forwarding session is matched against layer 2 parameters in the configured PBRs.

  This feature is useful in a scenario where packets related to a forwarding session must be processed by another device before being sent to their destination.

  Following are the benefits of this support:

  - Instead of defining new PBRs that are based on Layer 3 parameters, you can use existing PBRs based on Layer 2 parameters for sending the packets related to forwarding sessions to the desired next hop device.

  - In a deployment that includes NetScaler appliances and optimization devices (for example, Citrix ByteMobile and Citrix CloudBridge appliances), PBRs based on Layer 2 parameters can be very handy compared to other, complex configuration for identifying the forwarding session related packets for PBR processing.

  - Identifying forwarding session related Ingress packets for sending them to the optimization device.

  - Identifying egress packets, which also matched a forwarding session rule, from the optimization device for sending the packets to the desired next hop device.

  [From Build 55.20] [# 484458]

- **MAC Address Wildcard Mask for Extended ACLs**

A new wildcard mask parameter for extended ACLs and ACL6s can be used with the source MAC address parameter to define a range of MAC addresses to match against the source MAC address of incoming packets.

MAC Address Wildcard Mask for PBRs

A new wildcard mask parameter for PBRs and PBR6s can be used with the source MAC address parameter to define a range of MAC addresses to match against the source MAC address of outgoing packets.

[From Build 55.20] [# 391630]

Optimization

- **Media classification support on the NetScaler appliance**

  You can now monitor and display the statistics of the media traffic going through the NetScaler appliance.

  [From Build 55.20] [# 493103]

- **Support for JPEG-XR image format in Front End Optimization (FEO)**

  The front end optimization feature now supports the conversion of GIF, JPEG, TIFF, and PNG images to JPEG-XR format as part of the image optimization functionality.

  [From Build 55.20] [# 504044]

- **Support for WebP image format in Front End Optimization (FEO)**

  The front end optimization feature now supports the conversion of GIF, JPEG, and PNG images to WEBP format as part of the image optimization functionality.

  [From Build 55.20] [# 509338]

Policies

- **Transaction Scope Variables**

  Transaction scope variables are added to variables feature. You can now use transaction scope variables to specify separate instances with values for each transaction processed by the NetScaler appliance. Transaction variables are useful for passing information from one phase of the transaction to another. For example, you can use a transaction variable to pass information about the request onto the response processing.

  [From Build 55.20] [# 444109]

- **Policy extensions support on NetScaler appliance**

  The NetScaler appliance now supports policy extensions, which you can use to add customized functions to default syntax policy expressions. An extension function can accept text, double, Boolean or number values as input, perform a computation, and produce a text, double, Boolean or number result.

  [From Build 55.20] [# 248822]

SSL

- **Support for Checking the Subject Alternative Name in addition to the Common Name in a Server Certificate**

  If you configure a common name on an SSL service or service group for server certificate authentication, the subject alternative name (SAN), if specified, is matched in addition to the common name. Therefore, if the common name does not match, the name that you specify is compared to the values in the SAN field in the certificate. If it matches one of those values, the handshake is successful. Note that in the SAN field, only DNS names are matched.

  [From Build 55.20] [# 439161]

- **2048-bit Default Certificates on the NetScaler Appliance**

  With this release, the default certificate on a NetScaler appliance is 2048-bits. In earlier builds, the default certificate was 512-bits or 1024-bits. After upgrading to release 11.0, you must delete all your old certificate-key pairs starting with "ns-", and then restart the appliance to automatically generate a 2048-bit default certificate.

  [From Build 55.20] [# 451441, 405363, 458905, 465280, 540467, 551603, 559154]

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

  The NetScaler VPX appliance now supports TLS protocol versions 1.1 and 1.2 on the front end. [From Build 55.20] [# 424463, 481970]

- **Changes to the Default Cipher Suite**

  If user-defined ciphers or cipher groups are not bound to an SSL virtual server, the DEFAULT cipher group is used for cipher selection at the front end and the ALL cipher group is used for cipher selection at the back end. In this release, the predefined cipher suites, such as DEFAULT and ALL, are modified to give strong ciphers a higher priority. For example, earlier RC4-MD5 was given a higher priority but it is deprioritized in the new list because it is a weak cipher.

  [From Build 55.20] [# 226713, 258311, 384491]

- **Support for Displaying the Hex Code of a CIpher**

  The show ciphersuite command now displays the IETF standard hexadecimal code of the cipher. It is helpful in debugging, because a hex code is unique to a cipher but the cipher name might differ on the NetScaler appliance, OpenSSL, and Wireshark.

  At the NetScaler command line, type:

  show ciphersuite

  In the configuration utility, navigate to Traffic Management > SSL > Cipher Groups.

  [From Build 55.20] [# 491286]

- **New SNMP OIDs for SSL transactions per second**

  The following SNMP OIDs have been added to the display the SSL transactions per second:

NS-ROOT-MIB::sslTotTransactionsRate.0 = Gauge32: 0

NS-ROOT-MIB::sslTotSSLv2TransactionsRate.0 = Gauge32: 0

NS-ROOT-MIB::sslTotSSLv3TransactionsRate.0 = Gauge32: 0

NS-ROOT-MIB::sslTotTLSv1TransactionsRate.0 = Gauge32: 0

[From Build 55.20] [# 449923]

- **Stricter Control on Client Certificate Validation**

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

  For more information, see http://docs.citrix.com/en-us/netscaler/11/traffic-management/ssl/config-ssloffloading/ssl-profiles.html.

  [From Build 55.20] [# 533241]

- **Support for SNI with a SAN Extension Certificate**

  The NetScaler appliance now supports SNI with a SAN extension certificate. During handshake initiation, the host name provided by the client is first compared to the common name and then to the subject alternative name. If the name matches, the corresponding certificate is presented to the client.

  [From Build 55.20] [# 250573]

- **DH Key Performance Optimization**

  DH key generation is optimized on a VPX appliance by adding a new parameter dhKeyExpSizeLimit. You can set this parameter on an SSL virtual server or on an SSL profile and bind the profile to the SSL virtual server. The key generation is optimized as defined by NIST in http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf. Additionally, the minimum DH count is set to zero. As a result, you can now generate a DH key for each transaction as opposed to a minimum of 500 transactions earlier. This helps to achieve perfect forward secrecy (PFS).

  [From Build 55.20] [# 498162, 512637]

- **Support for TLS_FALLBACK_SCSV signaling cipher suite value**

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

For more information, see http://docs.citrix.com/en-us/netscaler/11/traffic-management/ssl/customize-ssl-config/config-protocol-settings.html.

[From Build 55.20] [# 509666, 573528]

- **Support for Additional Ciphers on a DTLS Virtual Server**

  EDH, DHE, ADH, EXP, and ECDHE ciphers are now supported on a DTLS virtual server.

  [From Build 55.20] [# 508440, 483391]

- **Support for Auto-Detection of the Certificate-Key Pair Format**

  The NetScaler software has been enhanced to automatically detect the format of the certificate-key pair. To do so, the format of the certificate and key file should be the same. If you specify the format in the inform parameter, it is ignored by the software. Supported formats are PEM, DER, and PFX.

  [From Build 55.20] [# 209047, 432330, 481660]

System

- **Support for HTTP/2 on the NetScaler Appliance**

  The NetScaler appliance supports HTTP/2 connections with clients supporting HTTP/2 protocol.

  [From Build 55.20] [# 490096, 505747]

- The NetScaler introduces a new role called sysadmin. A sysadmin is lower than a superuser is terms of access allowed on the appliance. A sysadmin user can perform all NetScaler operations with the following exceptions: no access to the NetScaler shell, cannot perform user configurations, cannot perform partition configurations, and some other configurations as stated in the sysadmin command policy.

  [From Build 55.20] [# 548516]

- **Maintaining minimum number of reuse pool connections in HTTP Profiles**

  You can now specify the minimum number of reuse pool connections to be opened from the NetScaler appliance to a particular server. This setting helps in optimal memory utilization and reduces the number of idle connections to the server.

  [From Build 55.20] [# 397478]

- The NetScaler Web Logging (NSWL) client logs a hyphen (-) instead of a user name when %u is specified in the log format.

  [From Build 55.20] [# 238440, 239481, 247372, 422873]

- **Showtechsupport utility enhancement**

  If your NetScaler appliance has Internet connectivity, you can now directly upload the newly generated collector archive to the Citrix technical support server from the appliance.

[From Build 55.20] [# 480797]

- **Support for FACK on TCP profiles**

  The TCP profiles on a NetScaler appliance now support forward acknowledgement (FACK). FACK avoids TCP congestion by explicitly measuring the total number of data bytes outstanding in the network, and helping the sender (either a NetScaler ADC or a client) control the amount of data injected into the network during retransmission timeouts.

  [From Build 55.20] [# 439130]

- **NTP Version Update**

  In NetScaler release 11, the NTP version has been updated from 4.2.6p3 to 4.2.8p2.

  If you upgrade your NetScaler appliance from any earlier release to release 11, the NTP configuration is automatically upgraded with additional security policies. For more information about configuring an NTP server, see http://docs.citrix.com/en-us/netscaler/11/system/basic-operations/configuring-clock-sychronization.html.

  [From Build 55.20] [# 440375, 440591]

- The NetScaler appliance fails intermittently when trace is started in 'RX' mode.

  [From Build 55.20] [# 576067]

- **User configurable congestion window for TCP profile**

  You can now set the maximum congestion window size for a TCP profile on the NetScaler appliance.

  [From Build 55.20] [# 248711]

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

  [From Build 55.20] [# 480258, 494482, 523853]

- Support for milliseconds, microseconds, and nanoseconds in Time Format Definition table

  You can now configure NetScaler web logging clients to capture transaction times in milliseconds, microseconds, and nanoseconds for logging on the NetScaler appliance.

  [From Build 55.20] [# 505840, 505377]

- The NetScaler appliance generates SNMP clear alarm traps for successful cases of haVersionMismatch, haNoHeartbeats, haBadSecState, haSyncFailure, and haPropFailure error events in an HA configuration.

  [From Build 55.20] [# 368832]

Telco

- **Provide Visibility into SLA Reports**

  An ISP often purchases international bandwidth from upstream ISPs, who then become layer 2 ISPs. To provide the redundancy required for reliable service to its customers, the purchasing ISP negotiates Service Level Agreements with multiple layer 2 ISPs. The SLAs stipulate a penalty in the event that the layer 2 ISP fails to maintain a specified level of service.

  NetScaler Insight Center and the NetScaler cache redirection feature can now be used to monitor the traffic flowing through the NetScaler appliances and calculate SLA breaches. The NetScaler cache redirection feature helps save bandwidth over international links. NetScaler Insight Center works with the NetScaler cache redirection feature to calculate, and provide visibility into, the percentage of bandwidth saved and any breaches of the SLA. ISP administrators are alerted whenever there is a breach for response time, hit rate/sec, or bandwidth.

  For a specific domain, NetScaler calculates the following SLA breaches and forwards the data to NetScaler Insight Center:

  * SLA Breach. A breach that occurs when a metric (response time, hits, or bandwidth) crosses the defined threshold value. For example, SLA breach is considered if the response time for a specific domain crosses 100 ms.

  * SLA Breach Duration. Time period in which a SLA breach lasted. For example, SLA Breach Duration is considered 5 mins, if the response time for a domain is greater than 100 ms consistently for 5 mins.

  * Breached Request Percentage. Percentage of requests whose response time is not within the minimum response time and maximum response time range. For example, if you configure this value as 10%, then among 100 requests, the response time of 10 requests are not within the minimum response time and maximum response time.

  NetScaler Insight Center then calculates the following SLA breaches:

  * SLA Breach Frequency- SLA Breach Frequency is the defined as the number of times the SLA breach occurs for the SLA Breach Duration. For example, SLA Breach Frequency is considered 1, if the response time for a domain is greater than 100 ms consistently for 5 mins.

  All of these metrics are calculated for a SLA group, which contains a list of domains defined by the ISP administrator.

  [From Build 62.10] [# 495288, 501269, 501277, 501278, 501279, 501280]

- **Provide Internet Access to a Large Number of Private IPv4 Subscribers of a Telecom Service Provider (Large Scale NAT)**

  The Internet's phenomenal growth has resulted in a shortage of public IPv4 addresses. Large Scale NAT (LSN/CGNAT) provides a solution to this issue, maximizing the use of available public IPv4 addresses by sharing a few public IPv4 addresses among a large pool of Internet users. LSN translates private IPv4 addresses into public IPv4 addresses. It includes network address and port translation methods to aggregate many private IP addresses into fewer public IPv4 addresses. LSN is designed to handle NAT on a large scale.

The NetScaler supports LSN and is compliant with RFC 6888, 5382, 5508, and 4787. The NetScaler LSN feature is very useful for Internet Service Providers (ISPs) and carriers providing millions of translations to support a large number of users (subscribers) and at very high throughput. The LSN architecture of an ISP using Citrix products consists of subscribers (Internet users) in private address spaces accessing the Internet through a NetScaler appliance deployed in ISP's core network.

The following lists some of the LSN features supported on a NetScaler appliance:

* ALGs: Support of application Layer Gateway (ALG) for SIP, PPTP, RTSP, FTP, ICMP, and TFTP protocols.

* Deterministic/ Fixed NAT: Support for pre-allocation of block of ports to subscribers for minimizing logging.

* Mapping: Support of Endpoint-independent mapping (EIM), Address-dependent mapping (ADM), and Address-Port dependent mapping.

* Filtering: Support of Endpoint-independent filtering (EIF), Address-dependent filtering, and Address-Port-dependent filtering.

* Quotas: Configurable limits on number of ports and sessions per subscriber.

* Static Mapping: Support of manually defining an LSN mapping.

* Hairpin Flow: Support for communication between subscribers or internal hosts using public IP addresses.

* LSN Clients: Support for specifying or identifying subscribers for LSN NAT by using IPv4 addresses and extended ACL rules.

* Logging: Support for logging LSN session for law enforcement. In addition, the following are also supported for logging:

** Reliable SYSLOG: Support of sending SYSLOG messages over TCP to external log servers for a more reliable transport mechanism.

** Load balancing of Log Servers. Support for load balancing of external log servers for preventing storage of redundant log messages.

** Minimal Logging: Deterministic LSN configurations or Dynamic LSN configurations with port block significantly reduces the LSN log volume.

For more information about the Large Scale NAT feature, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-introduction.html.

[From Build 62.10] [# 316909]

- **Subscriber-Aware Traffic Steering**

  Traffic steering is directing subscriber traffic from one point to another based on subscriber information. When a subscriber connects to the network, the packet gateway associates an IP address with the subscriber and forwards the data packet to the NetScaler appliance. The

appliance communicates with the PCRF server over the Gx interface to get the policy information. Based on the policy information, the appliance performs one of the following actions:

- Forwards the data packet to another set of services

- Drops the packet

- Performs LSN if configured on the appliance

For more information about subscriber-aware traffic steering, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-telco-subscriber-management.html.

[From Build 62.10] [# 402473]

- **Provide Internet Access to IPv4 Subscribers Through the IPv6 Core Network of a Telecom Service Provider (Dual-Stack Lite)**

  Because of the shortage of IPv4 addresses, and the advantages of IPv6 over IPv4, many ISPs have started transitioning to IPv6 infrastructure. But during this transitioning, ISPs must continue to support IPv4 along with IPv6 because most of the public Internet still uses only IPv4, and many subscribers do not support IPv6.

  Dual-Stack Lite (DS-Lite) is an IPv6 transition solution for ISPs with IPv6 infrastructure to connect their IPv4 subscribers to the Internet. DS-Lite uses IPv6 tunneling to send a subscriber's IPv4 packet over a tunnel on the IPv6 access network to the ISP. The IPv6 packet is de capsulated to recover the subscriber's IPv4 packet and is then sent to the Internet after NAT address and port translation other LSN related processing. The response packets traverse through the same path to the subscriber.

  The NetScaler appliance implements the AFTR component of a DS-Lite deployment and is compliant with RFC 6333.

  For more information about the DS-Lite feature, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/dual-stack-lite.html.

  [From Build 62.10] [# 407162]

- **Subscriber-Aware Service Chaining**

  Service chaining is determining the set of services through which the outbound traffic from a subscriber must pass before going to the Internet. Multiple services, such as antivirus services, parental control services, firewalls, and web filter, are running in a Telco network. Different subscribers have different plans and each plan has specific services associated with it. The decision to direct a subscriber's request to a service is based on the subscriber information. Instead of sending all the traffic to all the services, the NetScaler appliance intelligently routes all requests from a subscriber to a specific set of services on the basis of the policy defined for that subscriber. The appliance receives the subscriber information from the PCRF over a Gx interface.

For more information about subscriber-aware service chaining, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-telco-subscriber-management.html.

[From Build 62.10] [# 561747]

- **Support for RADIUS Accounting Message**

  The NetScaler appliance can now dynamically receive the subscriber information through a RADIUS accounting message. It receives the subscriber IP address and MSISDN and uses this information to retrieve the subscriber rules from the PCRF server.

  For more information about RADIUS Accounting Message, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-telco-subscriber-management.html.

  [From Build 62.10] [# 526981]

- **Support for Gx Interface**

  The NetScaler appliance can now dynamically receive the subscriber information over a Gx interface. The appliance communicates with the PCRF server over the Gx interface, receives the subscriber information, and uses this information to direct the flow of traffic. The PCRF server can send updates over this interface at any point during the subscriber session.

  For more information about Gx interface, see http://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-telco-subscriber-management.html.

  [From Build 62.10] [# 402469]

- **High Availability Support for Dynamic Subscriber Sessions**

  In the absence of a high availability (HA) setup, the subscriber information that is received from the RADIUS client is lost if the appliance fails. With HA support, the subscriber sessions are continually synchronized on the secondary node. In the event of a failover, the subscriber information is still available on the secondary node.

  [From Build 63.16] [# 574838]

Fixed Issues in Previous NetScaler 11.0 Releases

The issues that were addressed in NetScaler 11.0 releases prior to Build 64.34. The build number provided below the issue description indicates the build in which this issue was addressed.

AAA-TM

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

  [From Build 63.16] [# 577778, 595104, 595185]

AppFlow

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

  [From Build 63.16] [# 574420]

Application Firewall

- After processing a request that consists of multiple headers of the same type, a subsequent request might invoke a 302 response due to the way the application firewall stores the information regarding the parsed headers. With this fix, the variable which stores the information regarding the headers is reinitialized accurately prior to processing the next request.

  [From Build 62.10] [# 580564]

- If, when processing a form for response-side security check inspection, the application firewall resets a connection, the partially parsed form is not freed. The result is a memory leak. With this fix, the memory allocated to the partially parsed forms is freed when a connection is reset.

  [From Build 62.10] [# 572637, 581520]

- The NetScaler appliance might become unresponsive when processing a request, because of an interoperability issue between the application firewall, SSL, and the responder module. The issue arises under the following set of circumstances:

  The configuration includes an application firewall profile protecting an SSL virtual server.

  A responder policy is configured to reset the connection, and this policy is bound either globally or to the virtual server that receives the request.

  [From Build 63.16] [# 592429]

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

  [From Build 63.16] [# 591176, 593996, 597440, 601359]

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

  [From Build 63.16] [# 547978]

- NetScaler application firewall resets the connection when the request contains tampered session cookie and the cookie protection is enabled.

  [From Build 63.16] [# 591172, 574498]

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

  Workaround: Use the Adobe PDF browser plugin.

[From Build 63.16] [# 372768]

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

  [From Build 63.16] [# 577742]

- After processing a request that consists of multiple headers of the same type, a subsequent request might invoke a 302 response due to the way the application firewall stores the information about the parsed headers. With this fix, the variable that stores the information regarding the headers is reinitialized accurately before the next request is processed.

  [From Build 63.16] [# 580564]

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

  [From Build 63.16] [# 580273]

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

  Workaround: Use the command line interface (CLI) to access the learned data.

  [From Build 63.16] [# 584621]

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

  [From Build 63.16] [# 574498, 591172]

Cluster

- You cannot add LB routes in a link load balancing setup that is deployed on a cluster.

  [From Build 62.10] [# 574717]

- In a cluster setup, for active FTP, the server cannot initiate a data connection from a random port.

  [From Build 62.10] [# 559230, 571042]

- In a NetScaler cluster, a "sh nslogaction" command that is issued from the NSIP address of a cluster node, goes into an infinite loop. The issue is not observed when the command is issued from the cluster IP address.

  [From Build 62.10] [# 574333, 573645]

- In a cluster setup, a command that is executed on the cluster configuration coordinator is propagated to the other cluster nodes. Therefore, a command that takes a long time to complete (such as "save ns config"), can take a little extra time to complete on all the cluster

nodes. During this time, if you execute another command on the cluster (through another session), that command will fail because the previous command is not yet complete.

[From Build 63.16] [# 551607, 495270, 562651]

Command Line Interface

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

  [From Build 63.16] [# 583625]

Configuration Utility

- The operation to download the nstrace file from the configuration utility fails.

  [From Build 62.10] [# 571814, 581955]

- You cannot configure the service path AVP by using the configuration utility.

  Workaround: Use the NetScaler command line to configure the service path AVP. At the command prompt, type:

  set subscriber gxinterface -servicepathAVP 1001 1005

  [From Build 62.10] [# 576603]

- You cannot configure the service path AVP by using the configuration utility.

  Workaround: Use the NetScaler command line to configure the service path AVP. At the command prompt, type:

  set subscriber gxinterface -servicepathAVP 1001 1005

  [From Build 63.16] [# 576603]

- The values for the parameters on the "Configure Load Balancing Parameters" page do not appear even though they have been set.

  [From Build 63.16] [# 583741]

- The operation to download the nstrace file from the configuration utility fails.

  [From Build 63.16] [# 571814, 581955]

- SUBSCRIBER expressions do not appear in the list for rewrite and responder policies and action.

  [From Build 63.16] [# 583751]

DNS

- The query logs contain incorrect information if the UDP payload size in the OPT record is not 1280. Also, if a load balancing virtual server on the NetScaler appliance receives a request with the CD bit set, and the "RecusionAvailable" parameter is disabled on the DNS or DNS-TCP load balancing virtual server, the CD bit is not logged.

  [From Build 63.16] [# 579942]

GSLB

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

  [From Build 63.16] [# 578969]

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

  [From Build 63.16] [# 582925]

High Availability

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

  [From Build 63.16] [# 560640, 566710, 576012, 576096, 579037, 582354, 590730]

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

  [From Build 63.16] [# 580703, 579037, 595491, 595506, 596002, 596215, 599250, 599396, 604164, 605112, 608450, 608485]

Load Balancing

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

  [From Build 63.16] [# 575171, 576012]

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

  [From Build 63.16] [# 583647]

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

  [From Build 63.16] [# 587812]

- When editing a service group in the configuration utility, the cacheable option is automatically set to true.

  [From Build 63.16] [# 592235]

NITRO API

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

  [From Build 63.16] [# 583395, 457969]

- For the .NET SDK, when "nitro.dll" is used along with a version later than 4.0 of the "Newtonsoft.json.dll" file, "private" properties cannot be serialized.

[From Build 63.16] [# 567162, 571309]

NetScaler Insight Center

- The NetScaler Insight Center appliance throws an error when modifying the name of a threshold record. To fix this issue, the name field has been made read-only.

  [From Build 62.10] [# 573550]

- If there are more than 25 records to display in the skip flow window, then only 25 records are displayed as the window does not provide support for pagination.

  [From Build 62.10] [# 576471]

- The NetScaler Insight Center appliance might fail and not respond, when you add, update, or delete the private IP address block that is used for geo location.

  [From Build 62.10] [# 576477, 581927]

- **Media Classification Support for Insight Center**

  Web Insight supports content and media type classification reports. Viewing these features are optional similar to the existing HTTP header fields User Agents, Operating Systems, Request Methods etc. You can enable or disable these features from the Configuration section. For media classification and httpContentType Appflow parameter, you must first enable Appflow on virtual server from Insight center configuration.

  Insight Center's Web Insight dash board reports the following Media types:

  1) Uncategorized

  2) FLV F4V Audio

  3) FLV F4V Video

  4) MP4 M4V Audio

  5) MP4 M4V Video

  6) GP 3G2 Video

  7) ADTS Audio

  8) APPLE Video

  9) MICROSOFT Video

  10) AAC Audio

  11) MICROSOFT PLAYLIST Video

  12) APPLE PLAYLIST Video

  13) MP3 Audio

  14) Unknown

[From Build 62.10] [# 558890]

- An exported report displays the time duration as "custom" irrespective of the time duration selected in the report.

  [From Build 62.10] [# 577426]

- The SNMP daemon runs on NetScaler Insight Center even though NetScaler Insight Center does not support SNMP requests.

  [From Build 63.16] [# 537253]

- The NTP server configuration on NetScaler Insight Center is not propagated to the connector, agent, and database nodes.

  [From Build 63.16] [# 579777]

Networking

- Duplicate address detection might fail for a global IPv6 address.

  [From Build 62.10] [# 560243]

- High availability (HA) synchronization fails if the NetScaler IP (NSIP) addresses of the nodes in the HA configuration are IPv6 addresses.

  [From Build 62.10] [# 573935]

- A PBR6 rule might not get evaluated if you set the operator option to NEQ (!=) for source and destination IPv6 addresses.

  [From Build 62.10] [# 575906]

- An ACL6 rule might not get evaluated if you set the operator option to NEQ (!=) for source and destination IPv6 addresses.

  [From Build 62.10] [# 573516]

- ICMPv6 requests with a payload greater than 1232 bytes (fragmented ICMPv6 requests) from a nondefault NetScaler admin partition might not succeed.

  [From Build 62.10] [# 506332]

- The NetScaler appliance might assign the NTP module a port that is used by some other feature module. Therefore, an incoming NTP response can be processed by the feature module. This can result in the failure of the NetScaler appliance.

  [From Build 63.16] [# 588477]

- You cannot configure INAT46, INAT64, or INAT66 rules by using the configuration utility.

  Workaround: Use the command line interface.

  [From Build 63.16] [# 582682]

- In a high availability configuration, when the connection between primary and secondary goes down and comes up again, the secondary node receives HA INIT request from the primary node and it terminates all BGP connections.

  [From Build 63.16] [# 588509]

- The output of the show ACL does not display the correct hits for ICMP packets that match the ACL rules.

  [From Build 63.16] [# 585265]

Policies

- The NetScaler appliance fails to respond when a blocking log action is configured with a responder action.

  [From Build 62.10] [# 574458, 574593]

- Some IP based expressions might not work for IP addresses starting from octet 128 or greater (128.x.x.x - 254.x.x.x).

  The following expressions are not impacted:

  - EQ, IN_SUBNET, IS_IPV6, GET1, GET2, GET3, GET4, MATCHES, MATCHES_LOCATION, APPEND, TYPECAST_TEXT_T, TYPECAST_IPv6_ADDRESS_AT

  The following expressions do not work:

  GT, GE, LT, LE, BETWEEN, NE, ADD, SUB, MUL, DIV, MOD, NEG, BITAND, BITOR, BITXOR, BITNEG, LSHIFT, RSHIFT, TYPECAST_TIME_AT, TYPECAST_IP_ADDRESS_AT, TYPECAST_DOUBLE_AT, TYPECAST_UNSIGNED_LONG_AT, WEEKDAY_STRING, WEEKDAY_STRING_SHORT, SIGNED8_STRING, UNSIGNED8_STRING, SIGNED16_STRING, UNSIGNED16_STRING, SIGNED32_STRING

  [From Build 63.16] [# 534244]

SSL

- You cannot enable TLSv1.1/1.2 on a front end SSL service after explicitly disabling it.

  [From Build 62.10] [# 574589]

- If you have a large number of SSL services (greater than 3000) in the backend, CPU usage increases exponentially and the appliance fails.

  [From Build 63.16] [# 581193]

- If you have configured optional client-certificate authentication and your policies target client certificate x509 extensions, such as auth keyid, a transaction with a client that doesn't have a certificate might cause the appliance to fail or to use stale values from a previous transaction.

  [From Build 63.16] [# 593091]

- If you update the certificate-key pair for a service group, the change is not reflected in the individual services that are bound to this service group. As a result, the old certificate-key pair continues to be used for negotiation in the SSL handshake.

  [From Build 63.16] [# 554925]

- If TLS1.1/1.2 protocol is used with AES/3DES ciphers, the length of the TCP window at the back end shrinks to zero. As a result, after some time, the connection is terminated.

  [From Build 63.16] [# 591600, 595713, 596278, 596556, 596566, 598045, 599524, 600591, 604929]

- In some cases, when client authentication is enabled, incorrect data form a client leads to a memory leak on the NetScaler appliance. If a large number of clients send incorrect data, the appliance fails.

  [From Build 63.16] [# 570754]

- If you use the "add ssl certkey" command to add an encrypted .pfx file, the password is now encrypted and saved in the configuration file (ns.conf). In earlier releases, the password was not saved, so automatic execution of the add ssl certkey command failed when the appliance was restarted.

  [From Build 63.16] [# 591167]

- If you downgrade the software on your NetScaler appliance that does not have a license to release 9.3 build 61.66 or earlier, some commands related to the default server certificate might not be saved in the running configuration. As a result, after restarting, secure access (HTTPS) to the appliance fails.

  [From Build 63.16] [# 551603, 559154]

- An incoming SSL record that spans more than 256 TCP packets and contains TCP header options causes memory corruption in the Cavium command buffer structure. As a result, the NetScaler appliance fails.

  [From Build 63.16] [# 573904, 583295, 590222]

System

- The option to set the transport type has been removed from the SET and UNSET operations. You can specify the transport type while adding a Syslog action. In a Syslog action, by default the transport type is set as UDP.

  Note: Once you have set the transport type in a Syslog action, you cannot change the transport type.

  [From Build 62.10] [# 580890]

- The NetScaler appliance fails intermittently when trace is started in 'RX' mode.

  [From Build 62.10] [# 576067]

- If a NetScaler appliance that is sending auditlog messages over TCP (audit syslogaction specifies TCP as the transport protocol) has more than 200 million active sessions, the rate at

which the syslogs are sent drops to 700 Kbps or lower, and the appliance consumes a high percentage of the CPU cycles.

[From Build 63.16] [# 580309]

- Management CPU usage is high when you use the configuration utility's memory usage diagnostic tool (System > Diagnostics > Memory usage).).

  [From Build 63.16] [# 586328]

- When SPDY Protocol is enabled and SPDY Traffic is received on the NetScaler appliance, the TCP current clients counter goes to negative values and shows a very large value in the stat or the SNMP OID.

  [From Build 63.16] [# 551562, 551786, 568554]

- The upgrade wizard in the configuration utility puts the NetScaler software in the /var directory instead of the /var/nsinstall/<build id> directory.

  [From Build 63.16] [# 586721]

- In NetScaler Insight Center, and NetScaler VPX on ESX, the Vmtoolsd daemon fails during start up and creates a core dump in the directory /var/core. It does not affect normal VPX functionality. However, operations such as "Shut Down Guest" and "Restart Guest" from the vSphere client summary tab fail.

  [From Build 63.16] [# 570166, 477094, 498384, 520519, 530951, 543554, 555689, 585809]

- The NetScaler appliance might become unresponsive if it receives a retransmitted TCP jumbo frame that carries the TCP FIN flag.

  [From Build 63.16] [# 571176]

- After cleaning up an MPTCP session, the NetScaler appliance might not set the DATA_FIN flag in the TCP header of the data or acknowledgement packet if there is no subflow for sending the data.

  [From Build 63.16] [# 553650]

- For a NetScaler appliance with extended memory configured for Large Scale NAT (LSN) feature, after warm rebooting the appliance, when the appliance is added as secondary node to an appliance that does not have the extended memory configured for LSN, the secondary appliance becomes unresponsive.

  [From Build 63.16] [# 593261]

- In a high availability setup, if stateful connection failover is configured on a virtual server that has been serving traffic for some time, running the "clear config extended" command results in a warm restart on both the primary and secondary appliances. Unsetting connection failover on the virtual server results is a warm restart on only the secondary appliance.

  [From Build 63.16] [# 575108, 581862]

- If you execute NTP commands, such as enable ntp sync and show ntp status, the NetScaler appliance might become unresponsive because of a memory leak.

[From Build 63.16] [# 529787, 546378, 574866, 581849]

- The NetScaler appliance might become unresponsive if front end optimization (FEO) is enabled with the SSL and rewrite features.

  [From Build 63.16] [# 583829]

- If a server advertises a maximum segment size (MSS) greater than 1460 bytes, a TCP transaction might not generate a response after passing through the NetScaler appliance.

  [From Build 63.16] [# 584079]

- On rebooting the NetScaler appliance, the timeout is not set to the value specified by the "set ns timeout" command.

  [From Build 63.16] [# 587074]

Telco

- In a network setup that includes both dynamic and deterministic types of clients, the first request from a deterministic client is not served if a dynamic client has sent a request.

  [From Build 63.16] [# 576602]

- After a failover occurs in a high availability configuration, some LSN static maps might become inactive on the new secondary node.

  Workaround: Delete the LSN static maps on the primary node and then add them again.

  [From Build 63.16] [# 487318]

Web Interface on NetScaler (WIonNS)

- After upgrading to nswi-1.8.tgz, existing WI sites are not accessible till you remove the sites and then add them back.

  [From Build 62.10] [# 576883]

- WIonNS v1.7 does not work when WebFront is installed.

  Workaround: Upgrade to WIonNS v1.8.

  [From Build 63.16] [# 577988]