Citrix NetScaler 1000V Release Notes

Citrix NetScaler 11.1-55.13

First Published: 2017-10-04

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

Fixed Issues 5
Known Issues 14

11.1-55.13

Updated: October 3, 2017 | Release notes version: 1.0

This release notes document describes the enhancements and changes and specifies the issues that exist, for the NetScaler release 11.1 Build 55.13.

Fixed Issues

The issues that are addressed in Build 55.13.

AAA-TM

In rare scenarios, NetScaler dumps core if dialogue mode operation like password change operation happens during RBA authentication.

[# 684648]

NTLM authentication fails when the NetScaler tries to negotiate with an LB virtual server in front of the NTLM server.

[# 677747]

Client logons are delayed by 15 seconds if Kerberos Constrained Delegation (KCD) is used on a NetScaler appliance. The delay occurs during the process of issuing a Kerberos ticket to the client.

[# 683869]

Assigning a custom port other than the default to an authentication enabled load balancing virtual server causes the NetScaler appliance to display an error message.

[# 689832]

A load balancing virtual server on a NetScaler appliance sends a reset code to the client when it receives the second packet of the client's POST request.

[# 683216]

If the LDAP bind account password used on a NetScaler appliance contains the "at" special character (@), test connection performed on LDAP server fails, and the dashboard shows that the LDAP server is down.

[# 654375, 689891]

A NetScaler appliance can add multiple NetScaler AAA groups, but the “save config” operation saves only the first group.

[# 689212, 689457]

The NetScaler appliance crashes because of a failure to access the NetScaler AAA logon credentials. The failure occurs while attempting to match the rewrite policy against an AAA group.

[# 680099]

Admin Partitions

The CLI does not correctly display the command prompt to users who have read-only-access accounts created in the default partition and bound to a non-default partition.

[# 675151]

On a partitioned NetScaler appliance, the system memory counters are not updated properly unless they are cleared during partition deletion.

[# 681422, 682240]

When you access a partitioned appliance through the NetScaler GUI, the Dashboard does not display the "CPU vs. Memory Usage and HTTP Requests Rate" graph in the left pane.

[# 676700]

AppExpert

When a NetScaler appliance receives a client request for evaluating a responder policy, it might not log the responder data. Before evaluation, the appliance sets the ns_auditlog_module_id global variable and uses the data for log processing. If during the evaluation you block the log action and wait for more data, and while you are waiting the appliance receives another client request to evaluate a different policy, the responder log data is not recorded for the responder module.

[# 687140]

AppFlow

If an AppFlow policy is bound to ICA_REQUEST bindpoint for a virtual server with the ULFD mode enabled, disabling AppFlow for that virtual server from NetScaler MAS/NetScaler Insight Center can cause the NetScaler instance to become unresponsive.

[# 688260, 687559, 685968, 684245, 691851]

When ClientSide Measurements is enabled, and you access the NetScaler Gateway, then the Microsoft Internet Explorer browser displays an error.

[# 680567, 688758]

A NetScaler appliance crashes and dumps core if an ECDSA certificate is bound to the SSL virtual server that processes an SSL transaction.

[# 683567, 686195]

The NetScaler appliance crashes, dumps core, and restarts if a certificate is unbound from an SSL virtual server while an SSL transaction is in progress.

[# 679995]

Application Firewall

After an upgrade from an earlier release 11.0 build to release 11.1 build 55.4, the 'APPFW_RESET' and 'APPFW_DROP' AppFw profiles do not appear when you run the sh appfw profile command with the "more" option.

For example:

sh appfw profile | more

1) Name: APPFW_BYPASS LogEveryPolicyHit: OFF

2) Name: APPFW_RESET LogEveryPolicyHit: ON

3) Name: APPFW_DROP LogEveryPolicyHit: ON

4) Name: APPFW_BLOCK UseHTMLErrorObject: OFF

This issue does not occur after upgrading a NetScaler AppFirewall appliance to release 11.1 build 55.8.

[# 690261, 689327]

The NetScaler AppFirewall appliance crashes while copying form data if the form field consistency check is enabled.

[# 678297, 689073]

If you use the CLI of a NetScaler AppFirewall appliance to display an enum definition, the AS_CCARD_DEFAULT_CARD_TYPE default value for credit card options is not included.

[# 686540]

When you attempt to export learned data for an application firewall profile, the appliance fails because of improper initialization of a stack variable. The Aslearn process restarts continuously because of connection failure.

[# 684988]

The NetScaler packet processing engine fails to start when URL transform regression scripts are executed during a low-memory condition.

[# 687625]

Since release 11.1 build 41, the ImportSizeLimit parameter in the AppFW settings can be set to limit the size of the objects that are imported to the NetScaler appliance. This limit is now extended from 128 MB to 256 MB. Execute the following set command from the CLI to change the value to meet your requirement:

set appfw setting -importsizelimit

Maximum value: 268435456

Minimum value: 1

Default: 134217728

Example

> set appfw setting -importsizelimit 268435457

[# 682219]

Form based NetScaler AppFirewall checks can be bypassed by a multipart POST request in which the Content-type header has been tampered with.

[# 674658]

On a NetScaler appliance running release 11.1 build 64, SQL and cross-site scripting relaxations might not work for application or json content types. The AppFW logs display the following message, even when the relaxation rules are applied for User-Agent:

SQL Keyword check failed for header User-Agent.

[# 651054]

Traffic to a back-end application is blocked by the HTML cross-site scripting check when the profile type is XML. The cross-site scripting check fails for field with following tags; <?xml version="Bad tag: ?xml" <blocked>.

When you have cross-site scripting enabled, the application firewall makes the following changes to requests that match the HTML Cross-Site Scripting check:

Left angle bracket (<) to HTML character entity equivalent (<) Right angle bracket (>) to HTML character entity equivalent (>) This prevents browsers from interpreting unsafe html tags, such as <script>, and thereby executing malicious code. If you enable both request-header checking and XSS transformation, any special characters found in request headers are also modified as described above. If scripts on your protected web site contain cross-site scripting features, but your web site does not rely upon those scripts to operate correctly, you can safely disable blocking and enable transformation. This configuration allows legitimate web traffic while stopping any potential cross-site scripting attacks.

[# 685775]

Clustering

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

[# 614718, 615459]

DNS

When a NetScaler appliance in resolver mode receives a DNS response from a name server and forwards it to an alternative name server, the NetScaler appliance goes DOWN.

[# 682730, 683138, 680141]

Front End Optimization

The NetScaler appliance dumps core when the front end optimization (FEO) feature is enabled for one virtual server and an AppFlow action with client-side measurement is enabled for another virtual server.

[# 686146]

Load Balancing

If an add lb monitor command specifies an httprequest argument value of more than 77 characters, a subsequent show command shows an incorrect httprequest value for the HTTP requests that the monitor sends to the CLIP address. The NetScaler appliance's ns.conf file also contains the incorrect httprequest value for the monitor. Also, the other nodes (non-CCO) in the cluster are updated with the incorrect httprequest value by the configsync process.

[# 685856, 687784]

NetScaler: AAA-TM

A cached ticket is expired before server receives it. This happens when a NetScaler is used as a kerberos SSO to backend servers. This usually happens just around the time ticket expires, which is typically 10 hours.

[# 681026]

The maximum string size of Target Vserver Expression is 1500. If the configuration includes an expression greater than 1500, the NetScaler appliance crashes. With this fix, the maximum string size of Target Vserver Expression is limited to 1499.

[# 684131]

In a high availability (HA) setup, if domain-based services are configured and the secondary node does not receive any Service State Sync (SSS) update for the services for more than 247 days, a packet engine might crash when this node becomes the primary node.

[# 673446, 684550, 688305]

NITRO

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

[# 558715]

The .NET SDK GET call fails with the following exception if it is made with a parameter that accepts boolean values:

Invalid argument value [<attribute>].

Example:

When the “internal” attribute of service_args is set to “true”, a get on service_args yields the following exception:

Invalid argument value [internal]

[# 595938]

NetScaler 1000V Appliance

TCP services that go through tagged VLAN interfaces might go down.

[# 683196]

NetScaler GUI

You can now edit GUI parameters for a custom session policy in a cluster setup.

[# 689519]

If from the NetScaler GUI, you create a new session policy from an existing session policy, the attempt fails.

[# 689520]

NetScaler VPX Appliance

In a NetScaler VPX HA deployment running on AWS, when a failover makes the secondary node primary, the network interfaces are attached to the new primary in the wrong order.

For example, if the primary node has NICS 1/2 (AA:BB:CC:DD:EE:FF), 1/3 (12:34:56:78:90:12), and 1/4 (1A:2B:3C:4D:5E:6F), upon failover the new primary would have 1/2 (1A:2B:3C:4D:5E:6F), 1/3(AA:BB:CC:DD:EE:FF), 1/4(12:34:56:78:90:12). Here, the interface MAC order has changed. However, this behavior does not apply to the NIC that's configured with the NetScaler management IP address.

[# 675746]

If you use the following command to remove an allowed-VLAN list from an SR-10V interface, the list is not removed, and therefore you cannot configure new VLAN settings for the interface.

unset int -trunkallowedVlan

[# 657468]

If you try to use the VMware vSphere snapshot feature on a NetScaler VPX appliance running on a VMware ESX hypervisor, network connectivity to the NetScaler VPX instance is lost. This happens because a VPX appliance does not support the snapshot feature. This fix adds support for the snapshot feature. You can now use this feature to manage your VPX appliance.

[# 687305, 688953]

Networking

The NetScaler appliance drops ND6 solicitation packets received on interfaces that are in muted state.

[# 684119]

In a high availability setup, when a critical interface goes to DOWN state because of TX stall, HA failover might not happen.

[# 677815, 679068, 680001]

The NetScaler appliance does not process the BGP remote-as configuration for an IPv6 peer after a reboot resulting in the loss of BGP configuration for this peer.

[# 685123]

A NetScaler appliance might become unresponsive or a high CPU is observed during the following scenario:

* The appliance resolves a domain into two IP addresses, one of the IP addresses is a NetScaler owned IP address and the other is an external IP address.

* The appliance sends a packet destined to the external IP address from LO/1.

* The response packet keeps looping after the appliance receives it.

[# 669754, 669977, 687943]

Policies

A log message is not logged for the Responder module when the NetScaler appliance receives a request and processes policies for a different module while a client request sent to the Responder module awaits log processing.

[# 685375]

When an Advanced expression function in an ALT expression blocks the current evaluation of the expression, then upon resumption it may cause the NetScaler appliance to crash.

[# 687345]

SSL

If two certificates issued by two different CAs have the same OCSP URL, addition of one of the certificate-key pairs might fail.

Example

1. CA certificate C1 is used to issue certificate S1, which contains OCSP_URL1.

2. Certificate-key pairs for both C1 and S1 are added successfully on the NetScaler appliance.

3. CA certificate C2 is used to issue certificate S2, which also contains OCSP_URL1.

4. If you first add a certificate-key pair for S2, it is successful but adding a certificate-key for CA2 fails. If you reverse the order, adding a certificate-key for CA2 is successful but adding a certificate-key for S2 fails.

[# 694395]

In a cluster setup, a certificate update fails, with the following error, if the certificate is in DER format.

Error :: No such resource

[# 583715]

The NetScaler appliance dumps core and restarts if it receives a request while both session-ticket and SSL-session persistence are enabled.

[# 687575]

For requests less than 255 bytes long, you can configure the HTTP GET method for queries to an OCSP server. If you specify the GET method but the length is greater than 255 bytes, the appliance uses the POST method by default.

To set the method by using the NetScaler CLI

At the command prompt, type;

set ssl ocspResponder <name> -httpMethod GET

[# 676942]

Session ticket parameters are saved in the configuration (ns.conf) file even though session tickets are not enabled in the SSL profile. As a result, if you upgrade to release 12.0 builds 41.x or build 51.x, you might observe a loss in configuration.

[# 678514, 677813]

In rare cases, a NetScaler appliance might dump core and restart if you add a certificate revocation list (CRL) larger than 256 KB.

[# 674278, 678890]

The connection with the back-end server is terminated if OCSP validation for the server certificate fails, even though OCSP validation is optional.

[# 686998]

A NetScaler appliance might dump core and restart if you have configured policy based SSL renegotiation and a client sends multiple SSL records before renegotiation is initiated.

[# 673348, 682192, 682160, 684547, 684992, 687515]

If you try to add a certificate-key pair containing an unsupported OID in the Subject Alternative Name (SAN) field of the certificate, the following error message appears:

ERROR: Invalid OID for SAN entry in certificate

[# 688416]

In a high availability deployment, session-tickets functionality is lost after you issue a force failover twice. Sessions are resumed on the basis of session ID instead of session tickets.

[# 683034]

You cannot modify the internal OCSP responder parameters in this build.

[# 679708]

Some client authentication connections might be dropped if OCSP check is set to mandatory and an OCSP domain name entry is not found in the NetScaler DNS cache.

[# 675882, 677473]

The "update ssl certkey" command fails if the certificate-key pair is bound to a load balancing monitor.

[# 686633]

The NetScaler appliance might occasionally send a wrong certificate if SNI is enabled.

[# 675158]

If previous session key lifetime is configured, a session ticket expires later than expected. That is it adds the previous session key lifetime to the session ticket lifetime instead of expiring after the session ticket lifetime.

[# 687207]

Memory usage might continuously increase on a partitioned NetScaler VPX appliance processing SSL traffic. As a result, the appliance might become unresponsive after some time.

[# 685669]

The NetScaler appliance dumps core and restarts if both client authentication and session ticket are enabled and a session ticket reuse request is continuously received on the appliance.

[# 687777, 690238]

System

If you enable front end optimization (FEO) and configure integrated caching (IC) with cache selectors, the NetScaler appliance might crash.

[# 677943]

Instead of silently closing the connection, a NetScaler appliance in a wildcard configuration might send a response to the source of the request. Upon receiving a SYN request, the appliance sends a "probe connection" request to the back-end server and queues the SYN request. When the server sends a "reset" response, the appliance sends the response to the client instead of silently closing the connection.

[# 677729]

When a client times out and sends a message longer than one packet, TCP sends a FIN packet to the application handler (for example, SSL). When TCP receives the second packet, it directly sends the packet to the application handler. As a result, the application handler generates a close notify alert for the first packet and an RST alert for the second packet.

[# 686390]

Enabling both the AppFlow option and the AppQoE option might cause a memory leak, which can degrade performance and eventually cause the appliance to fail.

[# 640545, 685334, 686832, 687603]

A NetScaler appliance can become unresponsive if it hosts a wildcard load balancing virtual server that has the use source IP option enabled and the use proxy port option disabled. The failure occurs if the virtual server associates the outgoing probe-connection information with different incoming connections destined to the same server.

[# 689915]

In an SSL connection with a client, the NetScaler appliance does not evaluate the SSL policies for HTTP/2 streams.

[# 670556, 660674, 672227, 689849]

The NetScaler appliance does not send buffered log messages when the SYSLOG server is ready to accept them.

[# 686751]

If the integrated caching (IC) memory limit is set to a value greater than 4 GB and front end optimization (FEO) is enabled, the NetScaler appliance crashes.

[# 666208]

Some packets become invalid and are dropped when policies are applied. If HTTP/2 packets are dropped, the NetScaler appliance fails to send a rst_stream frame to the client, which causes the appliance to crash when new packets arrive.

[# 684370]

A NetScaler appliance in a high availability configuration crashes when using TCP transport to send log messages.

[# 685898]

An attempt to configure a NetScaler appliance that uses Cloudstack can cause the appliance to fail. If the Cloudstack AutoScale feature or an AutoScale policy is configured with the IP address a server, an attempt to configure the appliance through the NetScaler CLI instead of through CloudPlatform or Cloudstack binds the IP-address based server to the AutoScale Policy service group. This causes the appliance to crash.

[# 681426]

If the session ID maintained for clients exceeds the threshold of 16 million entries, the configuration engine might crash. That affects the management traffic. As a result, the management connection closes and the manager must log back on to the NetScaler appliance.

[# 676599]

If a client sends an HTTP/2 header continuation frame, the NetScaler appliance dumps core.

[# 681361, 683274]

HTTP/2 traffic can cause a NetScaler appliance to crash. If a responder policy matches an incoming HTTP/2 request, the appliance might drop the HTTP/2 request but fail to close the HTTP/2 stream. A subsequent packet in the same HTTP/2 stream can then cause a crash.

[# 688686]

If a load balancing virtual server configured with a backup server is down, the si_cur_Client counter underflows, causing client connections for the virtual server to display abnormal values in the NetScaler GUI.

[# 682762]

If multiple trap destinations have the same IP address but different SNMP versions, one of which is SNMPv3, modifying an SNMPv3 trap message leads to an appliance failure.

[# 683622, 683806]

In a high availability setup, the following command-propagation warning message appears when a backup is created for a large configuration file on the primary node: "Warning: There is no response from secondary. Propagation Timed out" However, creation of the backup file succeeds in both the nodes after some time.

[# 679376]

If a NetScaler-inserted cookie is deleted from the end of a cookie header, the appliance does not remove the preceding semicolon. As a result, an extra semicolon is sent at the end of the cookie header when forwarding it to the back-end server.

[# 687612]

Known Issues

The issues that exist in Build 55.13.

AAA-TM

If forms based Single Sign-On (SSO) is configured for Outlook Web Access (OWA) 2013 servers, the "successRule" configured in the forms SSO action must be corrected, because the server sends 64 byte cookie upon successful SSO.

[# 681730]

In rare scenarios, response cookie from OWA 2013 server is not greater than 70 bytes when the NetScaler appliance is configured with Forms Based SSO. Hence, length check for cookie value in success-rule configured in Forms SSO action on the NetScaler appliance needs to be updated with an appropriate value.

[# 676450]

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

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

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

[# 610091]

Despite binding loginSchema policies to AAA virtual server, administrator is able to bind Classic authentication policies. However, these are not used unless authentication policies are advanced.

[# 631362]

The back end is not accessible through a clientless VPN (CVPN). The issue occurs when SSO is ON, the proxy is specified in a traffic action, and the back-end credentials are different from the logon credentials.

Workaround:

Create a traffic policy based on back-end URL and create a trafficAction with SSO OFF and No Proxy. The backend should be accessible.

[# 689153]

A NetScaler appliance configured for NetScaler AAA with single sign-on is unable to log off from Online Web Access (OWA).

[# 688665]

If the primary and secondary passwords in a logon request are the same, and the first-factor authentication server prompts the user to change the password, the second-factor server uses the password that was sent in the logon request.

Workaround: Configure the second-factor authentication server to use the http.req.user.passwd expression if the first-factor server requests a password change.

[# 678553]

If you log on to the NetScaler Traffic Management (TM) virtual server using "401 Basic" authentication, you might observe authentication failures if your username or password contains special characters. This is because only UTF-8 characters below ASCII 128 (for example, A-Z, a-z, 0-9, and ~ ! @ # $ % ^ & * ( ) _ + - = [{] } \ | ; : ' " / ? . > , < special characters) are allowed.

[# 620845, 589509, 650263, 672340]

If a user name containing special characters is prefilled in the login forms, the RfWeb user interface fails to render the form.

Workaround: Escape the angular brackets.

Example:

Username is prefilled in the login forms on the basis of the value of the InitialValue tag in the authentication schema file.

Change

<InitialValue>${http.req.user.name}</InitialValue>

To

<InitialValue><![CDATA[${http.req.user.name}]]></InitialValue>

[# 646139]

If the back-end server's domain name does not include a dot, DNS resolution fails during Kerberos Single Sign-ON (SSO).

[# 667953]

A NetScaler appliance configured for NetScaler AAA with LDAP over SSL becomes unresponsive when the connection to the NetScaler AAA daemon is used fully. At this point, the packet engine is unable to process anymore authentication requests.

[# 660065, 674005]

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 upon system restart.

[# 493668, 516396]

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

[# 620673]

AppFlow

If multiple AppFlow policies are bound to the same bind point, only the last policy is chosen.

[# 603177, 647386]

When client-side-measurements is enabled on AppFlow action and if the incoming request is corrupted, the NetScaler appliance might become unresponsive.

[# 691229]

ICA parsing uses a lot of memory, so the NetScaler appliance reaches its memory limit with a lower than expected number of connections.

[# 459458]

Application Firewall

The NetScaler AppFirewall Cookie Consistency Check Stats and Learn options cause JBoss backend servers to respond with a 400 Bad Request. This occurs when a client sends multiple instances of the same cookie with different values. When the Cookie Consistency Check is configured for stats and learn, only the second cookie is forwarded to the backend server. The NetScaler appliance drops the first cookie.

[# 691967]

The NetScaler appliance fails to start and an HA failover occurs after an upgrade from release 11.0 build 68 to release 11.1 build 51.

[# 679546]

In an HA environment, a NetScaler appliance running release 11.0 does not learn new rules when the application firewall feature is enabled.

[# 672864]

If you upgrade a NetScaler appliance in a high availability (HA) setup from version 10.5.56.15 to version 11.1.51.1901 and skip 250 rules with active traffic, the GUI or CLI displays a "failed to skip some rules" error message and an operation time-out error message.

Workaround: Turn off the Learning feature when skipping learned rules.

[# 671807]

The NetScaler AppFirewall WAF service blocks valid field-format contents even when matching rules are present.

Workaround: In the field-format rules, insert two backslash characters (\\) before each dollar sign ($) character (\\$).

[# 691957]

The output of the appfw learningdata command does not include a caret and dollar sign (^$) at the beginning and end of a URL string. Therefore, the URLs are not in proper regex format. If you do not enclose a URL in ^$ characters when you specify a learned rule to be deleted, all the rules are deleted.

[# 668255]

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

> set appfw settings CEFLogging ON

[# 630056]

A NetScaler AppFirewall appliance with the compression feature enabled sometimes puts blank lines in HTTP response headers, resulting in garbled page rendering by the browser.

[# 629128]

The Application Firewall policy for HTTP requests (HTTP.REQ.HEADER) does not detect a content type with multiple lines.

[# 682676]

The IP address of a content switching virtual server cannot be accessed after an upgrade from a previous release to the current release. The POST request results in a 302 redirect error.

[# 687314]

A NetScaler Application Firewall appliance running release 10.5 build 66.6, 11.0, or 11.1 fails because of a packet-engine crash while applying an AppFirewall policy to the load balancing virtual server.

[# 691211]

The NetScaler application firewall should bypass requests from application firewall processing after the system reaches a specified CPU/memory usage limit, but there is currently no policy for reviewing CPU and memory capacity and bypassing the application firewall.

[# 660546]

If you have multiple application firewall policies configured on a load balancing virtual server, and a policy has a GotoPriority Expression of NEXT, the NetScaler AppFirewall policy order bypasses all security checks in that policy's profile and moves to the next policy.

[# 682935]

In the Visualizer, some buttons might not work if you use Mozilla Firefox or Internet Explorer.

Workaround: Use the Google Chrome browser.

[# 648272]

The NetScaler AppFirewall search filter for cookie consistency learned rules does not work.

[# 692560]

Websites from which you try to retrieve user records through a NetScaler appliance running release 11.1 build 50 do not properly display text in some languages (for example, Arabic). Garbled text, and characters such as question marks, appear instead.

Workaround: Disconnect the appliance from the application firewall.

[# 682115]

On a NetScaler application firewall appliance in high-availability mode, the aslearner process fails to convert a string value to an integer by using the standard library function atoi.

[# 692063]

In a high availability environment, a NetScaler appliance fails, because of low memory, while performing URL transformation or generating cross-site scripts to redirect URLs.

[# 692271]

A NetScaler AppFirewall appliance running release 11.0 build 70.12 might crash in a high availability environment.

[# 692023]

A NetScaler AppFirewall appliance running release 11.1 build 54.14 and serving as the primary node in an HA deployment crashes when freeing the allocator structure after completing the AppFirewall signature match. After a crash, the primary appliance restarts and becomes the secondary node.

[# 691725]

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]

A NetScaler AppFirewall appliance running release 10.5 build 66.6, 11.0, or 11.1 fails because of a packet-engine crash while applying an AppFirewall policy to the load balancing virtual server.

[# 691219]

Turning on the logging feature on a NetScaler Application Firewall appliance stops NStrace from generating reports for the logs.

[# 689215]

Application Firewall port information about open ports, such as port 443, is not suppressed. It can therefore be detected by port scan tools such as NMAP in targeted hacker attacks.

[# 674864]

The information that the GUI displays for the application firewall web services interoperability (WSI) check does not say that it is a prerequisite and cannot be disabled.

[# 650789, 650317, 658472]

Cache Redirection

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

[# 591265]

Clustering

In a cluster setup, if you use an interface on one node to create an LACP channel on another node, the channel is created and runs smoothly, but the system reports a configuration error.

[# 644080]

In a cluster setup, after a reboot, tagged VLAN configuration is lost on the vlan 1 interface.

[# 642947]

GSLB

When a remote GSLB service is configured with an external monitor on a GSLB site node, the state of this service might become inconsistent across packet engines, because of core-to-core message failures. In that case, the NetScaler appliance might generate incorrect replies to GSLB domain queries.

[# 658108, 679822, 692324]

Integrated Caching

If the response from the Integrated Caching (IC) module has trailing spaces in the content-length header, the HTTP/2 connection times out.

[# 688274]

Licensing

If you execute licensing commands simultaneously from multiple interfaces, such as NetScaler CLI, NITRO, or GUI, the commands might time out, because the licensing module processes the command serially. Here is the list of such commands:

Add/rm/show licenseserver

show licenseserverpool

set/unset capacity

[# 685146]

Load Balancing

The NetScaler appliance is unable to reuse an existing probe connection if an HTTP wildcard load balancing virtual server is configured in MAC mode with use source IP (USIP) mode enabled and the Use Proxy Port option turned off. As a result, the connection fails and client the receives a TCP reset.

[# 632872]

After a high availability failover, Web Interface on NetScaler displays "State Error" if you try to launch an application.

[# 630435]

The NetScaler appliance might crash if deletion of a service item and display of the service item are executed in parallel.

[# 691507]

NetScaler CLI

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

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

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

Workaround: Use one of the following alternate approaches:

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

- Use the Net::Telnet library.

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

[# 346066]

NetScaler CPX

Modifying the nf_conntrack_max sysctl variable to get better network performance can cause unexpected behavior. In that case, you have to increase the size of the connection-tracking and/or the hash table, and/or decrease timeout values.

[# 658734, 658736]

NetScaler GUI

LDAP configuration failed if the virtual server name started with an underscore ("_").

[# 646751]

In older versions of Internet Explorer version 7, the browser incompatibility message does not appear for NetScaler build 11.1. Instead, the logon page appears, and you can log on successfully.

[# 649052]

In a cluster setup, the content switching policies bound to a load balancing virtual server do not appear when you select “Show CS/CR Bindings” for that virtual server in the NetScaler GUI.

[# 689517]

If the feature "Force password change for nsroot user when default nsroot password is being used" is enabled and the nsroot password is changed at the first logon to the NetScaler appliance, the nsroot password change is not propagated to non-CCO nodes. Therefore, when an nsroot user logs on to non-CCO nodes, the appliance asks for password change again.

[# 658132]

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

[# 557379, 585649, 609615, 617161, 646039]

If the feature "Force password change for nsroot user when default nsroot password is being used" is enabled, and you log on as nsroot user, an extra session is created.

[# 657924]

Optimization

If a response from the StoreFront server does not have a Content Type field in the header, but the appliance expects a value in the Content Type field, the appliance crashes.

[# 688412]

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]

Policies

In some cases, an attempt to retrieve the configured rewrite policies on a NetScaler appliance causes the appliance to crash.

[# 691960]

A back-end server drops an HTTP GET request if the IP address of the server does not match the server IP address in the request.

[# 684825]

The NetScaler appliance can sometimes time out while restoring context for the rewrite feature.

Workaround: Modify the rewrite action to use regular (regex) expressions.

[# 675347]

If a policy expression name is same as any function name, subsequent use of the expression results in an error. In addition, if you restart the appliance and use the policy expression in a running configuration, the policy expression receives errors, which results in a configuration loss.

Workaround: Do not name a policy expression with the same name as any function. The simplest way to rename a policy expression is to add a prefix or suffix to the expression name (for example, myco_func or func_myco).

[# 637060]

Clearing a NetScaler system configuration causes the appliance to fail if an HTTP profile references a patset configuration entity.

Workaround: Avoid referencing a patset configuration entity in an HTTP profile.

[# 691227]

The audit framework has no mechanism to filter UndefHit logs generated in ns.log for undefined hits on rewrite or responder policies. To turn off log generation, you must remove HTTP transaction logging for undefined policies.

[# 690748]

SSL

If you have configured two SafeNet HSMs in a high availability setup on a standalone NetScaler appliance, and the primary HSM goes down, the secondary HSM does not serve traffic after a failover.

[# 628075]

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

[# 628914]

An incorrect error message is displayed in both the following cases:

1. Client authentication is enabled, root CA certificate is not bound to the SSL virtual server, and a request with a valid client certificate is sent to the virtual server.

2. Client authentication is enabled, root CA certificate is bound to the SSL virtual server, and a request with a wrong certificate is sent to the virtual server.

The error message that appears is "Handshake failure-Internal Error" instead of "No client certificate received."

[# 664574]

In the NetScaler GUI, the Show Bindings option in an SSL profile does not list the SSL entities to which the profile is bound.

[# 689516]

An SSL handshake might take a long time (many retries) to complete after you restart a NetScaler appliance.

[# 686713]

Session Key Auto Refresh incorrectly appears as disabled on a cluster IP address. (This option cannot be disabled.)

[# 687208]

ECDHE support with SSLv3 protocol on the NetScaler appliance is not compatible with RFC 4492, because SSLv3 does not support extensions and ECDHE needs extension support.

[# 610588, 657755]

If you restart the SafeNet network HSM, you must also restart the SafeNet gateway daemon.

[# 628067]

"Duplicate certificate error" appears when you try to bind a certificate containing a specific domain name to an SSL virtual server, if a certificate with a matching wildcard SAN entry is bound to the same virtual server.

[# 691769]

The SSL entities to which an SSL profile is bound do not appear when you run the show ssl profile <Default-Profile> command on a cluster IP (CLIP) address.

Workaround: You can view the bound entities from the NetScaler IP (NSIP) address.

[# 673458]

In a cluster setup, if a client certificate is bound to a back-end SSL service or service group, it appears as a "Server Certificate" instead of a "Client Certificate" when you run the "show ssl service" or the "show ssl servicegroup" command on the CLIP address.

[# 667389]

If you run the "sh ssl service group" command on the cluster IP (CLIP) address and on nodes of a cluster setup, ECC curves are displayed as unbound from the CLIP.

[# 660257]

An expired session ticket is honored by a non-CCO node.

[# 678176, 687205, 687098]

In some cases, a pipeline HTTP request is not forwarded to the back-end server if the back-end server sends a response before receiving the full request from a client.

[# 688100]

The previous session-key life-time value incorrectly appears as zero in the GUI.

Workaround: Access the CLI and enter the "show ssl profile <frontend profile name>" command to display the correct value.

[# 683023]

A session ticket issued by a non-CCO node is not honored by the CCO node.

[# 678175, 678522, 678526]

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]

You cannot set the previous session-key life time to its minimum value (0 seconds).

[# 687135]

In a high availability (HA) setup, if the primary node supports a SafeNet HSM, the HSM configuration is propagated to the secondary node even though the secondary node is not configured to support the

SafeNet HSM. For information about configuring an HA setup with SafeNet network HSMs, see the NetScaler documentation for SafeNet network HSM.

[# 628082]

In a cluster setup, the CRL distribution points in a CA certificate-key pair configured on the cluster IP address do not appear when you run the show ssl certkey command.

[# 691929]

The SSL entities to which a policy is bound do not appear in the output of the "show ssl policy" command if it is run on the cluster IP address.

[# 668520]

After you restart a NetScaler appliance, all the ECC curves might be bound a virtual server or service even though they were unbound from that virtual server or service before the appliance was restarted.

[# 691889]

If you create a custom cipher group and bind it to an SSL entity, the profile name "SSL_EMBEDDED_PROFILE" incorrectly appears in the output of the "show ciphergroup" command. This error does not occur if you enable the Default profile before creating the custom cipher group and binding it to the SSL entity.

[# 637230]

A NetScaler appliance might run out of memory and crash if it receives a non-handshake record, such as an alert message, before a DTLS handshake is complete.

[# 685145]

A NetScaler appliance crashes when session ticket is enabled and continuous session ticket reuse requests are received.

[# 692481, 692823]

System

No Error or Warning is announced if a user tries to set trunk mode on the loopback interface.

[# 643131]

A NetScaler appliance does not open a new connection to the back-end server if the following set of conditions is met:

- The global maxconn parameter is set to 1.

- The appliance is unable to reuse the connection for probing.

As a result, the transaction fails.

[# 636416]

Connections can become unresponsive because of data loss that occurs under the following set of conditions:

* Different traffic domains are configured on the virtual server and the service.

* Data insertion causes the NetScaler appliance to split packets.

[# 685510]

A NetScaler appliance might not honor persistence for a load balancing virtual server with a wildcard configuration if information about the back-end server is not available.

[# 556385]

When you run the set command on a NetScaler appliance, the ns.log file stores the command with all parameter values, including customer provided values.

[# 674165]

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

Workaround: Enable the end point processing features on NetScaler to control the complete TCP stack independently. Such features are TCP Buffering, SSL Offload and so on.

[# 622573]

If you force Quick ACK mode by sending Keep Alive probes in the middle of a three-way handshake, it causes the appliance to reset the back-end server connection.

[# 690047]

A NetScaler appliance might not initiate a rewrite action correctly if data is modified in adjacent fields in the message.

[# 657565, 686496]

A NetScaler appliance in a clustered setup displays a "Cannot allocate memory" error message if you use the set command to set the server domain name in a SYSLOG action.

Workaround: Delete the SYSLOG action in which you set the domain name, and add a new SYSLOG action that specifies the server domain name instead of the server IP address.

rm syslogaction

add syslogaction -loglevel [-options ...]

[# 687067]

If a NetScaler appliance sends a large number of packets on a TCP connection, and the network randomly drops a few of the packets, multiple sets of continuous packet loss ("holes") are created. When the appliance retransmits the packets, the network interface card (NIC) drops packets.

[# 643929]

If a client using the NITRO API over HTTPS to connect to a NetScaler appliance reuses the same source IP address and port within two TCP maximum segment lifetime (MSL) timeout intervals, the connection might be dropped with a TCP reset. Similarly, client TCP connections might be dropped under the following set of conditions:

* Source IP address is enabled and proxy port disabled in the client's connection request.

* A previous server connection still exists on the appliance and has persisted for two TCP MSL timeout intervals.

[# 692613]

Regression in handling of "=" in BMC LDAP validation process.

[# 681731]

A system user (using internal or external authentication) logging into a NetScaler appliance observes a blank screen if command policies are not bound to users or user groups.

Workaround: Log into the appliance through the NetScaler command interface.

[# 693394]

HTTP headers can be corrupted by the following series of events:

* The rewrite feature inserts an end-of-header mark, but the next packet contains more header bytes.

* The compression (CMP) feature interprets the incorrectly marked HTTP header-end as the actual end of the header, and tries to insert a content-encoding header.

[# 691308]

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

Workaround: Specify the NTP server's IP address.

[# 639529]

The HTML page rendering might fail if you insert a prebody script before the header tag. The HTML specification requires the character-encoding declaration to be serialized within the first 1024 bytes of the document, and the script might push the meta tag past the 1024-byte limit.

[# 305196, 393696]

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

[# 633371, 682640]

Telco

In a high availability setup, forcing synchronization does not synchronize Port Control Protocol (PCP) mappings to the secondary node.

[# 647630]

Upgrade and Downgrade

Repetitive messages appear in log files when you restart the NetScaler appliance after upgrading the firmware. The messages appear regardless of whether you use the GUI or the CLI to perform the upgrade. The repetitive logging stops when you log back on to the appliance.

[# 690534]

You cannot log on to the NetScaler appliance after upgrading its firmware. This issue is caused by insufficient storage space. To verify that that is the problem, check to see if the /var directory is 100% full. To fix the problem, delete unnecessary files. The following procedure is recommended:

1) At the shell prompt, type the df -h command to display the disk-usage statistics. If they indicate that the /var directory is full, take the following steps.

2) Check for any trace files in the /var/nstrace directory. Delete unnecessary files. Back up required files, including files that need to be analyzed, to a location outside the NetScaler appliance.

3) Check for files in the /var/core or /var/crash directory. These files indicate a problematic condition and should be analyzed. Back up these files to a location outside the NetScaler appliance and send them to Citrix Technical Support for further analysis. Delete the backed up files from the NetScaler appliance.

4) Check for any user-initiated downloads, such as build files, and delete the older ones. Generally, build files are downloaded to the /var/nsinstall directory.

[# 638818]