Citrix NetScaler 1000V Release Notes

Citrix NetScaler 11.0-70.16

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

11.0-70.16

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

Note: Build 70.16 replaces Build 70.12

This release notes document describes the enhancements and changes and specifies the issues that exist, for the NetScaler release 11.0 Build 70.12.

Fixed Issues

The issues that are addressed in Build 70.12.

AppFlow

- If numerous GET requests are sent to a NetScaler appliance on which AppFlow is enabled, at some point the requests begin to time out.

  [# 671993, 674438]

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

  [# 629223]

Application Firewall

- On a NetScaler Application Firewall appliance in a high availability configuration, learning mode does not work after an upgrade to release 11.0 build 68.10.

  [# 662359]

- If you upgrade 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.

  [# 661111, 662359, 670726, 662734]

- The IP reputation feature does not get enabled when the application firewall add-on license is

  added. [# 675202]

- The NetScaler appliance crashes during a field-consistency check if processing a large number of form-select fields.

  [# 668627, 664482]

- An archive error can occur when application firewall profiles are exported and archived, because the export file is not removed from the /var/archive/appfw/ and /var/tmp directories after profile export is successful. The problem is caused by an uppercase profile name when the archived export file is saved with the same case as the profile name.

  [# 670744]

- NetScaler release 11.0 build 47 or later logs error messages when you enable the Application Firewall feature on a NetScaler appliance in high availability mode.

[# 660528]

- During the downgrade process, the NetScaler appliance becomes unresponsive and generates an aslearn core file if the application firewall schema profile of the learned database files is not installed properly.

  [# 670752]

- Application firewall signature rule #14990 has a PCRE expression pattern to detect the presence of a violation string in the Accept-Charset header. This expression is computationally intensive and results in generation of log message "PCRE match limit exceeded with regex..." With this fix, rule #14990 is deprecated and replaced by signature rule #999972, which has an optimized PCRE expression. The new rule shows the source as Snort and the Snort ID as 14990.

  [# 669824]

- The NetScaler appliance fails to restart after an upgrade to software release 11.1 build 51.21. The failure, caused by memory corruption in the AppSecure module, occurs while evaluating an invalid session cookie.

  [# 674361]

- On a NetScaler Application Firewall appliance in a high availability configuration, learning mode does not work after an upgrade to release 11.0 build 68.10.

  [# 662734]

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

  [# 674031]

DNS

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

  [# 660562]

- If the load balancing feature is disabled and DNS name servers are being used, DNS resolution uses the most recently configured name server. If that name server is disabled, one of the name servers that is UP is used for DNS resolution.

  [# 670588]

- When a NetScaler appliance on which DNSSEC is configured is an authoritative DNS server for two domain zones, the appliance might send the same RRSIG responses to both zones instead of responding to only the appropriate zone.

[# 671880]

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

  [# 666803]

- The set lb vserver command allows you to assign the same IP address to the DNS name server and the DNS virtual server. With this fix, neither the set lb vserver nor the add dns nameServer command, nor the NetScaler GUI, allows you to assign the same address to both virtual servers.

  [# 665651]

- In ADNS and resolver mode, the NetScaler appliance does not support the OPT option. Therefore, it strips this option when responding to a client. In proxy mode, the query is forwarded as-is to the back end. If the response contains the EDNS Client Subnet (ECS) option, the response is forwarded to the client as-is, but not cached. If the back end does not support ECS option and therefore strips this option from the response, the response is cached as well as forwarded.

  [# 672905]

Integrated Caching

- A NetScaler appliance fails if a Page Tracking session is enabled on the appliance by Appflow or AppQoE modules for partial content responses. This happens only for partial content responses served from Integrated Cache.

  [# 656556]

Load Balancing

- The NetScaler appliance dumps core and restarts if an autoscale service group is configured with SSL as the service type.

  [# 656734]

- The NetScaler appliance might become unresponsive because of an internal issue related to CRC check if custom monitors are configured for a load balancing configuration of type TFTP.

  [# 658860]

- In a cluster setup, the configuration of a service might be lost if you restart the appliance after you have configured a request timeout action (-reqTimeoutAction) in an HTTP profile and attached the profile to the service.

  [# 649994, 649940]

NetScaler GUI

- You cannot unbind a transform policy from a virtual server by using the GUI.

  [# 652579]

NetScaler Insight Center

- In HDX Insight, filter for application is not working for Active Session count.

  [# 662586]

NetScaler VPX Appliance

- When a remote tagged IP address is accessed through a NetScaler VPX appliance hosted on Linux KVM, the checksum value in each sent packet is incorrect.

  [# 655067, 668302]

- In an ESX environment, if a CLAG or Node LAG is created with one or more VMXNET3 interfaces on a NetScaler VPX instance, the NetScaler GUI might show the MAC address of the CLAG or Node LAG as 00:00:00:00:00:00.

  [# 642495]

- In an ESX environment, a CLAG channel that includes a VMXNET3 interface might continue to send LACPDUs to its partner even when it is in DETACHED state.

  [# 642389]

- A NetScaler VPX appliance running on a VMware ESX server and configured with a VMXNET3 network interface stops responding and restarts if any traffic is sent to a tagged interface. Also, in the log message, the VLAN ID of the tagged interface is incorrect.

  [# 671581, 676316]

- A NetScaler VPX instance might stop responding and dump core memory if you allocate a large disk size for log messages. The higher the rate of log messages, the more quickly the instance runs out of memory and fails.

  [# 646674]

Networking

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

[# 669005]

SSL

- The NetScaler appliance might dump core memory and restart if you bind a secure monitor to a domain based service.

  [# 661808, 662002, 672103, 672532, 674664, 671558, 674758]

- The NetScaler appliance displays high CPU usage because of a wrong computation of idle

  time. [# 571226, 652915]

- The "set ssl vserver" or the "unset ssl vserver" command fails and the following error message

  appears: Internal error

  [# 670927, 673889, 673829, 671270]

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

  [# 665340]

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

  [# 627650]

- The "stat ssl vserver" command for a content switching, cache redirection, or VPN virtual server fails, and the following error message appears:

  No such resource [vServerName,

  <vservername>] [# 644731, 671337]

- The SSL parameter "deny SSL renegotiation" is now set to ALL by default in all admin partitions. Previously, it was set to NO in the non-default partitions.

  [# 663601]

- An SSL handshake fails if a client hello includes an ECC extension but the NetScaler appliance does not support any of the ECDHE ciphers in the cipher list sent by the client. The handshake fails even if the list contains some non-ECDHE ciphers that are supported.

  [# 668239]

- If memory allocation fails during a TLS1.2 protocol handshake, the handshake is not terminated. As a result, the appliance might dump memory core and restart.

  [# 630547, 639222, 639465, 646023, 647371, 649201, 658037, 662933, 663160, 665797, 668460, 676013, 679036]

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

  certificate. [# 600815, 343395]

System

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

  [# 626848]

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

  [# 667214]

- Before processing auditlog, if the auditlog message size and log levels are not validated properly, it leads to an overflow of memory buffer and crashes other modules in a NetScaler appliance.

  [# 670496]

- An overflow of integers updates the NetScaler memory statistics with a false value. This results in SNMP memory traps not reaching the configured threshold.

  [# 663720, 612313]

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

  files. [# 647955]

- After an upgrade, a NetScaler Weblogging (NSWL) HTTP record size is miscalculated if the HTTP header size is greater than 16 kilobytes and it is not a multiple of the word boundary.

  [# 671996, 672244, 678903]

Known Issues

The issues that exist in Build 70.12.

AAA-TM

- 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]

- 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]

- 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 SAML authentication is configured on NetScaler with artifact binding but certificates are not configured correctly in the SAML action, NetScaler fails to send the artifact resolution request to the Identity Provider.

  [# 641913]

Admin Partitions

- RPCSVR services cannot be configured in admin partitions.

  [# 498477]

  The following two issues can occur if you add an external group as a system group on a NetScaler appliance and use the "set system group" command to configure the prompt string and timeout parameters at the system group level:

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

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

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

[# 632460]

- If you change the resource allocation for any of the Admin Partitions, the NetScaler appliance displays a blank screen.

  Workaround

  Do one of the following:

  1. Clear browser's cache and cookies.

  2. Access NetScaler GUI in browser incognito mode.

  3. Access NetScaler GUI through other web browsers.

  4. Disable "Use software acceleration" option in browser settings and restart your browser.

  [# 621722]

- 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]

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

  [# 612215, 482310, 598576, 642624, 672565]

- 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]

- The IC memory allotted to an admin partition, cannot be reduced.

  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]

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

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

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

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

[# 632193]

Application Firewall

- When XML output of an IBM AppScan report is imported into NetScaler, it shows zero entries if the report is based on version 2.2 of the IBM AppScan schema. Citrix supports the 2.0 schema, but must acquire information about version 2.2 of the IBM AppScan schema in order to solve this problem.

  [# 626154]

- 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]

- If you upgrade 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 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 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]

- 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]

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

  [# 624978]

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

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

  [# 571943]

- 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]

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

  column. [# 621333]

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

  [# 349504]

Audit Logging

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

  [# 622905]

Cache Redirection

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

  [# 591265]

Clustering

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

  - When Autonomous Systems (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 because the path contains its own AS to prevent loop formation.

  - When AS OVERRIDE is configured on any upstream router for cluster neighbors, the upstream router changes the AS path in VIP to its own AS while sending updates to cluster neighbors. Spare nodes do not detect a 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 learned routes.

  [# 547749]

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

  [# 583424]

- When a node is removed from a layer 3 cluster, IPv6 SNIP addresses and routes are being erroneously cleared from the appliance. IPv4 SNIP addresses and routes are not affected.

  [# 542693]

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

  [# 582801]

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

  [# 479899]

Command Line Interface

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

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

DNS

- In a high-availability setup, a failover might occur because of memory exhaustion on the appliance if all of the following conditions are met:

  - There is a large DNS-related configuration.

  - Heavy traffic is observed for a long duration.

  - CPU utilization for one CPU is very high.

  [# 621661]

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

  [# 599741]

GSLB

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

  Workaround:

  Manually update the server name on the other GSLB

  sites. [# 511994]

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

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

  [# 625997]

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

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

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

  [# 530638, 506432, 652849]

High Availability

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

  [# 611197]

Integrated Caching

- After an upgrade, the content acceleration feature is not supported.

  [# 597415]

Load Balancing

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

  application. [# 630435]

- 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]

- A subscriber cannot initiate more than eight simultaneous sessions.

  [# 568052]

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

  [# 573463]

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

  [# 500169]

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

  [# 511222]

NITRO API

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

  [# 558715]

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 Documentation

- The following XM wizard names: _XM_<VIP_IP> should be reserved. These names should not be re-used for additional configuration entities. If the same convention is re-used, the edit/delete of the XM wizard could delete the configuration; even though, it was not pushed by the wizard.

  [# 588178, 610159]

NetScaler GUI

- You cannot upgrade to NetScaler release 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]

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

  [# 540980]

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

  [# 642802, 668935]

- 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]

- Certificate bundles are not supported in cluster

  setups. [# 644199]

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

  Workaround: Display the values in the command line interface.

  [# 505121]

NetScaler Insight Center

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

  [# 547380]

- If Expander module in NetScaler appliance fails, the NetScaler Insight Center skips monitoring a few ICA connections.

  [# 631367]

  The current-connection details displayed on the NetScaler Insight Center dashboard have a latency of about 2 minutes.

  [# 536696]

  Insight Agent should only be added after configuring and deploying Insight DB

  Cluster. [# 570619]

NetScaler VPX Appliance

For IPv6 or LACP support, promiscuous mode must be enabled for VMXNET3 interfaces at the ESX Hypervisor.

[# 641748]

Untagged packets are allowed to pass through an SRIOV VF interface (Intel 82599 NIC) if the VMWare vCenter 6.0 Distributed Virtual Switch(DVS) is used to configure the VLAN trunk mode.

[# 616044]

The NetScaler VPX appliances are now supported on VMware ESX server version 6.0.

[# 592395]

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]

In an ESX environment, file transfer from a NetScaler instance to an external connection stalls if the MTU is changed during the file transfer.

[# 630639]

When you add custom DNS name server in the NetScaler VPX appliance through NetScaler CLI, DNS lookup fails. This happens due to a default Azure DNS server entry present in /etc/resolv.conf.

Workaround: Follow these steps:

1. Edit the /nsconfig/.AZURE/resolv.conf file to remove the entry "nameserver 168.63.129.16", and save the file.

2. Add the required DNS name server through NetScaler CLI, by using the command "add dns nameserver <dns server IP>".

3. Save the ns config file.

4. Restart the NetScaler VPX appliance.

[# 672344]

Traffic might not pass through an SRIOV interface if you use the VMWare vCenter 6.0 Distributed Virtual Switch (DVS) to reconfigure a VLAN trunk policy.

This is a known issue with VMWare vCenter 6.0. Please contact VMWare support for possible workarounds.

[# 622392]

In an ESX environment, the Interface HAMON Configuration option is not available in the NetScaler GUI.

[# 641498]

Networking

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]

The NetScaler appliance forwards TCP packets, destined to port 69 and matching an RNAT rule, to the destination without processing them.

[# 670455]

The NetScaler appliance might become unresponsive while processing a route dependency check for multiple recursive BGP routes if the next hop for any of the routes changes or goes down.

[# 625841]

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]

During a force sync operation in a cluster deployment, built-in compression policies fail on nodes because the nodes ignore the "Resource already exists" error for these built-in policies.

[# 648182]

If an interface and an IP address are bound to a VLAN, binding them to another VLAN fails with the following error message: "ERROR: Either the subnet is not directly connected or subnet already bound to another VLAN." The interface is unbound from its current VLAN and gets bound to the native VLAN.

[# 643341]

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

[# 543171]

Policies

After a restart, a NetScaler auto-provision daemon fails to communicate with the configuration

engine. [# 604823]

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]

SSL

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

[# 624090]

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

[# 660257]

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]

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

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

[# 654743]

If you 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]

Even though TLS protocol versions 1.1 and 1.2 are not supported by firmware version 1.1, the protocols 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:

No usable ciphers configured on the SSL vserver

You can safely ignore this message.

[# 542973]

If you add or remove an HSM key, the following error message appears. However, the key is added or removed successfully.

ERROR: Internal error while adding HSM key.

[# 577552]

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]

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]

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]

The NetScaler appliance dumps memory core and restarts if both of the following conditions are met:

- You try to bind a certificate of type SNI to an SSL virtual server.

- The certificate contains unsupported entries, such as â€œOther Nameâ€• in the SAN certificate extension

field. [# 635712, 648778, 653861, 659342]

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

[# 554782]

Security Insight

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

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

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

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

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

included. [# 619713]

System

If you do not configure the Maximum Transmission Unit (MTU) in the VLAN or NIC interface, a NetScaler appliance does not appropriately advertise the Maximum Segment Size (MSS) option in the TCP SYN packet sent to the back-end server, which results in packet drops and a transaction failure.

Workaround: Configure the correct MSS option in the TCP profile.

[# 627394]

If you enable AppQoe and AppFlow features with client-side-measurements, more memory is allocated for storing the URL and host header without freeing the first allocation. As a result, a memory leak occurs in the HI memory pool.

[# 640545]

If Front End Optimization (FEO) feature is enabled and Page Extend Cache is turned on in the FEO action, there is improper handling of cache objects leading to an appliance failure

[# 658045]

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

[# 560854]

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

[# 622309, 641490]

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]

If a NetScaler appliance sends a large number of packets on a TCP connection and if few packets get randomly dropped in the network, it leads to multiple sets of continuous packet loss (Holes). When the appliance retransmits the packets in these sets of continuous packet loss, it results in packet drops at the NetScaler Interface Card (NIC).

[# 643929]

The NetScaler appliance might stop functioning and report a segmentation violation if your configuration includes policies or actions that use the following functions and one of them fails to obtain the memory that it needs:

XPATH()

XPATH_WITH_MARKUP()

XPATH_JSON()

XPATH_JSON_WITH_MARKUP()

XPATH_HTML()

XPATH_HTML_WITH_MARKUP()

[# 656646]

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]

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 etc

[# 622573]

In a TACACS authentication configuration, if you clear the system global TACACS policy, the NetScaler appliance displays a warning error message: "Config NodeGroup changed, force cluster sync should be fired on the newly added node to be in sync."

[# 666392]

Telco

Two different Syslog servers might log the same RTSP request.

[# 581086]

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

[# 574725]

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]

WIoNS

Because the install WI package command takes more than the usual time to complete, it is not possible to return the status from other nodes. Therefore all the WI related packages, for example, JRE+WI, must be present on system, on the same path, for all the nodes.

[# 507753]

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

[# 601304]