NetScaler ADC (includes NetScaler Gateway)

Release Notes for NetScaler ADC (includes NetScaler Gateway) 14.1-73.58

November 12, 2026

Notes

- This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.
- Build 14.1-73.58 replaces Build 14.1-73.49.
- Upgrading NetScaler in an ICA proxy setup to Build 14.1-73.37 or later drops active sessions attempting to reconnect with pre-upgrade session tickets. Users must restart their sessions. Post-upgrade sessions and reconnections function normally without extra configuration.
- Build 14.1-73.58 also includes fixes for the following issues that existed in the previous NetScaler ADC 14.1 release build: GOPHDX-9751, NSHELP-42791, NSHELP-44589, NSHELP-44985, NSHELP-45059, NSHELP-44524, and NSHELP-45833.
- Build 14.1-73.57 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305.
- Build 14.1-73.49 replaces Build 14.1-73.46.
- Build 14.1-73.49 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697263&articleTitle=Citrix_S
- Build 14.1-73.46 replaces Build 14.1-73.41.
- Build 14.1-73.46 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697191.
- Build 14.1-73.41 replaces Build 14.1-73.37.
- Build 14.1-73.41 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174.
- Build 14.1-73.37 replaces Build 14.1-73.33.
- Build 14.1-73.37 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096.
- Build 14.1-73.37 also includes fixes for the following issues that existed in the previous NetScaler ADC 14.1 release build: NSCONFIG-14995, NSHELP-44094, NSHELP-44357, NSAUTH-19942, NSAUTH-19927.
- Build 14.1-73.33 replaces Build 14.1-73.30 and Build 14.1-73.32.
- Build 14.1-73.33 includes the following fixes along with the enhancements and fixes available in Build 14.1-73.30: GOPHDX-9270, NSAUTH-19342.
- Build 14.1-73.32 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939.

What's New

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | CTXENG-72064**

  Support for GSLB context in OAuth grant tokens

  NetScaler now includes GSLB context in OAuth authorization code grant access and refresh tokens, providing complete information for OIDC flows.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | CTXENG-73074**

  Warning on untagged VLAN assignment

  You now receive a warning message when you assign an untagged VLAN to an interface that already has a native VLAN bound to it. This enhancement helps you to:

  - Avoid unintended replacement of the existing native VLAN configuration.
  - Prevent accidental network configuration changes.

  Example:

  ```
  1 add vlan 5Done bind vlan 5 ifnum 0/1/2 Warning: [Untagged VLAN
      bind replaced the existing native VLAN on this interface.]
  ```

  Module - ***Networking***

- **Build 73.58 | CTXENG-73469**

  Support for NetScaler VPX on Google Cloud C4 and C4D instance families

  NetScaler VPX now supports deployment on the Google Cloud Platform (GCP) C4 and C4D machine family instances. This enhancement expands the range of qualified GCP instances on which you can run NetScaler VPX, with validated NIC driver compatibility (gVNIC/GVE) on the C4 and C4D families. As a result, you gain access to the latest high-performance compute options for your cloud deployments.

  Related topic

  Deploy a NetScaler VPX instance on the Google Cloud Platform

  Module - ***Platform***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | CTXENG-72011**

  Connection pooling for the NetScaler ExtraHop integration

  NetScaler now uses connection pooling for its integration with ExtraHop. By reusing established connections when sharing TLS session information, NetScaler reduces the latency seen at the start of a session.

  Configure NetScaler ExtraHop connection pooling

  1. Import the settings file.
     Settings file content:{ ”warmup_connection_count” : <per PE value from 1 to 8> }
  2. In the configuration for sending SSL secret keys securely to the ExtraHop Discover Appliance, add the service with the WebAssembly (WASM) module.
     add service <name> (<IP> | <serverName>) <serviceType> <port> -wasmModule <wasm module name>

  Related topic

  https://docs.netscaler.com/en-us/citrix-adc/current-release/third-party-security-solutions/integrate-extrahop-discover-appliance-with-netscaler.html

  Module - *System*

- **Build 73.58 | CTXENG-73563**

  Increase in API session token limits

  NetScaler now supports up to 3,000 API authentication (session ID) tokens per appliance. Previously, the tokens were limited to 1,000 per appliance. This enhancement unblocks large-scale automation deployments that require each client or worker to hold its own session.

  Module - *User Interface*

Fixed Issues

- **Build 73.58 | NSHELP-43600**

  When you try to re-add an existing analytics profile, NetScaler might not create a new analytics profile, but also silently delete the existing analytics profile of the same name.

  Module - *Analytics Infrastructure*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSAUTH-19342**

  During failover or reconnection after an upgrade, NetScaler drops all active VPN and Authentication, Authorization, and Auditing sessions that were created before the upgrade. As a result, you must reauthenticate.

  Sessions that are created after the upgrade are not affected, and no configuration changes are required.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSAUTH-19942**

  After an upgrade, NetScaler drops all active VPN and authentication, authorization, and auditing sessions that were created before the upgrade. Users must reauthenticate after a failover or when reconnecting to the upgraded NetScaler.

  Sessions established after the upgrade are not affected, and no configuration changes are required.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-41804**

  When the user data encryption certificate is updated, password reset functionality might fail because user data in LDAP remains encrypted with the old certificate.

  With this fix, the OTP encryption tool supports KBA, alternate email, and OTP, enabling seamless upgrades of all user data, preventing password reset failures after certificate updates, and eliminating the need for device re-registration.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-42847**

  NetScaler VPX on Linux might crash while performing LDAP authentication.

  Module - ***Authentication, authorization, and auditing***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43405**

  Self-Service Password Reset (SSPR) fails on NetScaler deployments running on AHV hypervisor. During the password reset flow, authentication breaks at the user data decryption stage causing the SSPR email authentication to terminate early. As a result, users do not receive password reset emails and cannot recover their accounts through self-service.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-43511**

  NetScaler crashes when an authentication request arrives for a virtual server whose bind configuration does not exist.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-44223**

  The LDAP authentication fails if the connection between NetScaler and the LDAP server takes more than 2 seconds to establish, which triggers a timeout.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-41831**

  NetScaler might crash when you clean up a cache tracking record that is already deleted.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-42375**

  The packet engine might crash and trigger an HA failover when all backend DNS services are unavailable due to heavy traffic.

  Module - ***Load Balancing***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-42821**

  If you use the `client.src.ip.matches_location` expression in a policy to filter clients by location, policy evaluation might fail. This issue occurs when client location is configured in custom locations and location database file is not applied.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-42959**

  Disabling health monitoring resets the state of all the members instead of simply bypassing the health check. As a result, disabled servers incorrectly appear in the UP state.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-43006**

  You might experience delays in RADIUS authentication because the RADIUS Access-Request Identifier might not be preserved across concurrent requests when usip is enabled (-usip YES) and useproxyport is disabled (-useproxyport NO) on the RADIUS service.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-43548**

  The HA synchronization might fail if `sourceIPWhitelisting` is enabled in the GSLB parameters.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-44589**

  GSLB services might experience flapping at remote sites. This issue occurs when all of the following conditions are met:

  - The local site points to external servers. As a result, NetScaler has no corresponding virtual servers and relies exclusively on monitoring for its health status.
  - NetScaler GSLB deployment is exceptionally large (handling thousands of GSLB services).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- The GSLB site `triggermonitor` is configured to a value other than Always.

Workaround Change the GSLB site `triggermonitor` setting to Always.

Module - ***Load Balancing***

- **Build 73.58 | GOPHDX-9270**

  Upgrading NetScaler in an ICA proxy setup to 14.1-73.33, 13.1-63.21, 14.1-73.33 FIPS, and 13.1-37.277 FIPS or later drops active sessions attempting to reconnect with pre-upgrade session tickets. Users must restart their sessions. Post-upgrade sessions and reconnections function normally without extra configuration.

  Module - ***NetScaler Gateway***

- **Build 73.58 | GOPHDX-9507**

  After upgrading NetScaler in an ICA proxy setup to build 14.1-73.x, 14.1-73.x FIPS, 13.1-64.x, 13.1-37.x FIPS or later, active sessions attempting to reconnect using pre-upgrade session tickets are dropped. Affected users must restart their sessions. New sessions and subsequent reconnections are not affected.

  Module - ***NetScaler Gateway***

- **Build 73.58 | GOPHDX-9751**

  After upgrading NetScaler in an ICA proxy setup to build 14.1-73.x, 14.1-73.x FIPS, 13.1-64.x, 13.1-37.x FIPS or later, active sessions attempting to reconnect using pre-upgrade session tickets are dropped. Affected users must restart their sessions. New sessions and subsequent reconnections are not affected.

  Module - ***NetScaler Gateway***

- **Build 73.58 | NSHELP-41024**

  In an HA deployment, performing a full sync or clear-config on a node with a large configuration might cause the node to miss HA peer heartbeats for several seconds. As a result, the peer might incorrectly mark the node as DOWN and trigger a failover.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-42506**

  NetScaler might crash, resulting in a high-availability failover if the following conditions are met:

  - HDX Insight is enabled.
  - ICA session using session reliability reconnects while a virtual-channel data frame is still being reassembled.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-42953**

  NetScaler Gateway crashes after sending an ICA file to the client.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-43768**

  The CSP-related errors block the full VPN flow on macOS devices when the default CSP header is enabled in AAA parameters.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-43783**

  EPA device certificate scans might fail when using 4096-bit certificates.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-43908**

  NetScaler might generate a core dump during DTLS ICA launch in an ICA-Proxy double-hop setup when DTLS listener is enabled.

  Module - *NetScaler Gateway*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-44213**

  NetScaler Gateway using EDT (adaptive transport) with Network telemetry can trigger intermittent packet engine crashes, resulting in an HA failover.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-45059**

  When the Logout Action in StoreFront is configured to None, ICA sessions might disconnect unexpectedly following an authentication, authorization, and auditing session logoff.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-43146**

  If a NetScaler SDX has two Z-Cap license files, one with a shorter expiry period and another with a permanent license, the UI displays the expiry information based on the file order. As a result, it might incorrectly show the shorter expiry period instead of the permanent license.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-43313**

  On a NetScaler VPX instance configured with Cluster Link Aggregation (CLA), the interfaces and channels on the Citrix Hypervisor (XenServer) host, the SDX Management Service (SVM), and the VPX instance are incorrectly reported as out of sync. This mismatch triggers a false alarm.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-43316**

  The `xen_health_interface` API reports incorrect member-NIC status for bonded interfaces, because its response does not match the state shown in CLI output.

  Module - *NetScaler SDX Appliance*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43694**

  NetScaler Console rejects the extension blob if the host ID in the extension blob does not exactly match (case-sensitive) the NetScaler Console GUI host ID.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-43755**

  NetScaler SDX shows an incorrect count of local license files.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSSVM-7473**

  Applying a fixed-bandwidth license blob on SVM might fail due to folder permission issues on NetScaler version 14.1-72.x.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-42791**

  When NetScaler Web Application Firewall streaming mode is enabled, requests with a body, such as file uploads or form submissions, might hang indefinitely. This issue occurs only if a body security check, such as SQL injection or XS, is not configured on the profile. The streaming engine prematurely marks processing as complete before all network data arrives, which prevents remaining data packets from reaching the backend server.

  Module - *NetScaler Web App Firewall*

- **Build 73.58 | NSHELP-40982**

  When you run `stat ns partition <partition-name> -clearstats full`, it resets most of the partition's statistics but **does not clear the drop counters** (the counters that

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

track dropped packets or requests for the partition). Those drop counters keep their old, accumulated values instead of resetting to zero.

Module - *Networking*

- **Build 73.58 | NSHELP-42586**

  After you upgrade to NetScaler version 14.1 build 66.x, some of the OSPF routes might be missing from the routing table. The routes are present in the OSPF database (ZebOS) but are not installed in the NetScaler packet engine (PE).

  Module - *Networking*

- **Build 73.58 | NSHELP-43495**

  After an upgrade, an OSPF simple password of eight characters is truncated by one character.

  Module - *Networking*

- **Build 73.58 | NSHELP-44208**

  After you upgrade NetScaler from version 14.1-60.58 to 14.1-66.x or later, SNMP OIDs are truncated for entity names (such as virtual servers, services, or servicegroups) that are longer than 16 characters. As a result, SNMP-based monitoring fails for the affected entities.

  Module - *Networking*

- **Build 73.58 | NSHELP-44524**

  When a packet engine (PE) receives a request to add or delete a route, an internal flag check might fail, resulting in the command being dropped with the error: ”dropping propagated command on primary.” Because the command is not propagated to all PEs, the route change succeeds on some PEs and fails on others, resulting in inconsistent routing entries in a multi-PE environment.

  Module - *Networking*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-45833**

  On NetScaler BLX, BGP sessions fail to establish when TCP MD5 authentication (BGP neighbor password) is configured. The sessions remain in the OpenSent or OpenConfirm state, and the peer router reports an MD5 message digest mismatch. As a result, routes (such as VIP routes) are not advertised to the peer. This issue occurs because the TCP window field of BGP packets is modified after the MD5 signature is computed.

  Module - *Networking*

- **Build 73.58 | NSHELP-42584**

  On some platforms, ARP responses can arrive on a packet engine other than PE-0, which can cause ARP resolution to fail and increment the `arp_err_unsolicited_replies` counter.

  Module - *Platform*

- **Build 73.58 | NSHELP-42632**

  On officially supported NetScaler VPX deployments on Nutanix, legacy SSL certificates cannot be installed after an in-place upgrade. This issue occurs because the NetScaler VPX does not include OpenSSL legacy provider support, which is required for legacy-crypto certificates and PKCS%2312/PFX formats.

  Module - *Platform*

- **Build 73.58 | NSHELP-42686**

  NITRO API calls fail in the following scenarios:

  - After you log in to the NetScaler CLI and then make NITRO API calls through the shell to the NSIP of the same appliance.
  - When processes running in the management plane make NITRO API calls to the NSIP of the same appliance without any user interaction.

  Module - *Platform*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43268**

  On Linux-based NetScaler, 192.0.0.1/2 is reserved as the loopback address. To avoid IP conflicts, ARP resolution for the 192.0.0.0/24 subnet is blocked on all external interfaces.

  Module - *Platform*

- **Build 73.58 | NSHELP-43346**

  In a NetScaler high availability (HA) pair on Azure, the secondary IP addresses might not move to the current primary node during a failover if the Azure resource group name is empty at startup.

  Module - *Platform*

- **Build 73.58 | NSHELP-43508**

  On Ubuntu, certain NetScaler BLX log files, such as `nitro.log` and `callhome.log`, might stop updating after log rotation. This issue occurs due to a file ownership mismatch between `logrotate` and `rsyslog` utilities.

  Module - *Platform*

- **Build 73.58 | NSHELP-43592**

  When SELinux is set to enforcing mode, NetScaler BLX might fail to start with permission-denied errors while accessing the `/nsconfig/blx-lic-mac-file` and `/nsconfig/blx-host-id` files. This issue does not occur when SELinux is set to permissive mode.

  Module - *Platform*

- **Build 73.58 | NSLINUX-9869**

  Under sustained high-throughput traffic, NetScaler VPX on Linux might stop processing traffic and become unreachable after approximately 5 to 6 hours, requiring a restart for recovery. This

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

issue is most consistently observed on multi-PE NetScaler deployments running on the Xen hypervisor.

Module - *Platform*

- **Build 73.58 | NSHELP-43002**

  NetScaler might crash when an AppFlow policy encounters the `undef` state while processing a transaction and AppFlow module action is also set as `undef` action, and later a responder action encounters the `undef` state while processing the same or a subsequent transaction.

  Module - *Policies*

- **Build 73.58 | NSHELP-43411**

  NetScaler might crash when you run the `show connectiontable` command with a VXLAN-related filter expression while the `listen` parameter is enabled.

  Module - *Policies*

- **Build 73.58 | NSAPISEC-4189, NSAPISEC-4190**

  An underflow error in the URL-decoding path causes an out-of-bounds memory access and triggers a core dump. This issue occurs when the API security feature canonicalizes incoming request URLs during endpoint lookups.

  Module - *Security*

- **Build 73.58 | NSHELP-42545**

  NetScaler might crash when handling heavy ECDHE transactions simultaneously with bulk traffic on the MPX 14000 FIPS platform.

  Module - *SSL*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-42609**

  The NetScaler packet engine might crash due to a defect in backend TLS 1.3 connection state handling during teardown. On NetScaler SDX platforms with multiple instances, a crash in one instance can also affect other instances sharing the same crypto hardware.

  Module - *SSL*

- **Build 73.58 | NSHELP-42955**

  In rare cases, the SSL converter might fail to process the binding as expected when a customer unbinds and rebinds the DEFAULT cipher group on an SSL virtual server.

  Module - *SSL*

- **Build 73.58 | NSHELP-44094**

  In NetScaler, when you install an SSL certificate within an admin (non-default) partition using `add ssl certKey`, the command fails with the following error message:

  ```
  ERROR: No such certificate file exists
  ```

  This issue occurs even though the certificate (`.crt`) and key (`.key`) files are present in the target partition's SSL directory (`/var/partitions/<partition_name>/nsconfig/ssl/`).

  Module - *SSL*

- **Build 73.58 | NSHELP-44985, NSHELP-45088**

  nsppe might crash when backend SSL services or secure monitors configured to use TLS 1.3 close a connection to the backend server.

  Module - *SSL*

- **Build 73.58 | NSSSL-17320**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Certificate integrity checks might fail if the certificate or key file names contain spaces. The system cannot parse file names with spaces correctly, causing valid files to be incorrectly reported as missing.

Module - *SSL*

- **Build 73.58 | NSHELP-42508**

  When Enhanced ISN (EISN) generation is enabled on NetScaler, some TCP connections reset unexpectedly. This issue happens when the first data packet received after the TCP handshake is out of order.

  Module - *System*

- **Build 73.58 | NSHELP-42526**

  A memory leak occurs when the clear ns config command is run because the memory allocated for cache actions is not freed.

  Module - *System*

- **Build 73.58 | NSHELP-43429**

  NetScaler might experience high memory utilization, leading to failovers, crashes, or unresponsiveness when a TCP connection receives a sustained stream of small packets. This issue occurs because the TCP window management function repeatedly inflates the advertised receive window without enforcing an upper limit, causing unbounded memory consumption on connections with window scaling enabled.

  Module - *System*

- **Build 73.58 | NSHELP-43547**

  NetScaler might crash when an HTTP response header is received from the backend server and forwarded to an HTTP/2 client. This issue occurs when the HTTP/2 client is still sending the HTTP/2 request body.

  Module - *System*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43683**

  NetScaler might crash in some scenarios when the `Tail Loss Probe` TCP profile parameter is enabled.

  Module - ***System***

- **Build 73.58 | NSCONFIG-14125**

  After running the ”sync ha files misc” or ”sync ha files all” command, the secondary node might lose its license after an upgrade or reboot.

  Module - ***User Interface***

- **Build 73.58 | NSCONFIG-14995**

  For NetScaler VPX, BLX, or CPX instances using LAS with Pooled or Flexed licensing, bandwidth allocations must be in multiples of 10 Mbps.

  Upgrading to NetScaler 14.1 73.x causes instances with non-multiple bandwidth allocations to reject the invalid value, enter a grace period, and transition to an unlicensed state. Administrators must ensure all bandwidth allocations are in multiples of 10 Mbps before upgrading.

  Module - ***User Interface***

- **Build 73.58 | NSHELP-42596**

  CNAME services are missing in the binding list for CNAME GSLB virtual servers.

  Module - ***User Interface***

- **Build 73.58 | NSHELP-42745**

  The management GUI API schema blocks endpoints, such as '/logon', that are not part of the schema.

  Module - ***User Interface***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43493**

  The `domainIP` and `cookieDomain` parameters might not be available for the unset operation.

  Module - *User Interface*

- **Build 73.58 | NSHELP-43575**

  When you click **Migrate Config** in **Load Balancing Visualizer**, the screen stays greyed out even after the operation completes.

  Module - *User Interface*

- **Build 73.58 | NSHELP-43792**

  NetScaler displays an incorrect grace period status in the following scenarios:

  - When a license token is corrupted, the device enters a 721-hour grace period.
  - When a VPX license grace period expires, the grace period status continues to display for several hours.

  Module - *User Interface*

- **Build 73.58 | NSHELP-43862**

  The ”convert ns config” operation, used by the nsconf2IaC conversion tool, returns empty results instead of complete output on Linux-deployed NetScaler VPX.

  Module - *User Interface*

- **Build 73.58 | NSHELP-44007**

  Bandwidth allocations must be in multiples of 10 Mbps. If an invalid bandwidth value is assigned from NetScaler Console, the NetScaler instance does not honor the value. Consequently,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

the instance becomes unlicensed upon its next reboot and blocks the `save ns config` command.

This issue applies to NetScaler VPX, BLX, and CPX form factors. NetScaler MPX and SDX form factors are not impacted.

Module - ***User Interface***

- **Build 73.58 | NSHELP-44357, NSHELP-44721**

  In a NetScaler high availability setup, files that you modify on the primary node do not synchronize to the secondary node. The secondary node continues to use outdated copies of configuration files, such as SSL certificates and keys. As a result, any feature that relies on these files might fail on the secondary node.

  Module - ***User Interface***

Known Issues

- **Build 73.58 | NSHELP-44729**

  NetScaler Console periodically runs a get bind operation. If the ”get bind” and ”save config” operations run at the same time, NetScaler might crash.

  Module - ***Analytics Infrastructure***

- **Build 73.58 | NSHELP-44306**

  When client certificate authentication is configured on NetScaler Gateway or Authentication virtual server, `ns.log` records the entry `OAUTH INTUNE: DeviceID extraction error` on every login, even if `Intune OAuth` is not enabled.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-44535**

  NetScaler might crash during Gateway login when configured with client certificate authentication as the primary method and LDAP authentication with group extraction as the secondary method.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-44540**

  NetScaler might crash and trigger a high availability (HA) failover when updating an SSL certificate key or during HA synchronization, due to errors in the certificate cleanup routine.

  Module - ***Authentication, authorization, and auditing***

- **Build 73.58 | NSHELP-43888**

  A NetScaler VPX instance might crash while processing a DNS response received over TCP that is split across multiple segments. This issue occurs because of a memory-handling error in which VPX accesses memory that was already freed.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-43893**

  DNS resolution over TCP might fail for load balancing virtual server-based nameservers. This issue occurs when a truncated UDP response requires a TCP retry, but NetScaler does not sends the request to the DNS_TCP load-balancing nameserver.

  Module - ***Load Balancing***

- **Build 73.58 | NSHELP-43985**

  After an upgrade from FreeBSD to Linux operating system, configurations that include scriptable monitors of non-USER types (such as LDAP and MySQL) fail to apply.

  Workaround: After NetScaler comes up on the Linux build, reapply the monitor command using `-dispatcherip 192.0.0.2` instead of `127.0.0.1`.

  Module - ***Load Balancing***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-44390**

  The Packet Engine might crash because of a NULL-pointer dereference in the DNS recursive resolver. This issue occurs on an ADNS service that has recursive resolution enabled when the root nameservers have no cached glue A-records.

  Module - ***Load Balancing***

- **Build 73.58 | NSLB-12381**

  When an SSL or GeoDB file is synced by using the GSLB sync mechanism, NetScaler incorrectly displays the status as failure, even though the file synchronization is successful.

  Module - ***Load Balancing***

- **Build 73.58 | GOPHDX-7990**

  In a high-availability NetScaler Gateway (ICA proxy) deployment, a packet engine might restart and generate a core dump during HA failover if HDX sessions with UDP audio are active at that time. When this occurs, traffic is briefly interrupted while the packet engines recover. The occurrence of this issue depends on traffic conditions and failover timing.

  Module - ***NetScaler Gateway***

- **Build 73.58 | NSHELP-43762**

  NetScaler Gateway memory usage increases steadily over time, eventually preventing users from accessing the logon page or establishing VPN connections. This issue occurs when a VPN session policy is configured with client security expressions (post-authentication EPA scans) and session handling spans multiple packet engines, causing a buffer memory leak.

  Module - ***NetScaler Gateway***

- **Build 73.58 | NSHELP-44174**

  New RDP bookmark creation fails on the NetScaler Gateway portal home page.

  Module - ***NetScaler Gateway***

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-44509**

  NetScaler crashes when an ICA app or desktop session is launched over the EDT(DTLS-over-UDP) transport.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-44710**

  NetScaler might crash while exporting Gateway Insight events to NetScaler Console.

  Module - *NetScaler Gateway*

- **Build 73.58 | NSHELP-44359**

  Heavy bursts of SNMP traffic might cause high memory consumption in NetScaler SDX Management service.

  Workaround: Rate-limit the number of traps generated in the Management Service.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-44727**

  On NetScaler SDX, the Management Service (SVM) sent an nsNotifyRestart SNMP trap every hour, even though the snmpd process was not actually restarting. This occurred because the trap was unnecessarily triggered whenever the log file was rotated during routine log maintenance.

  Module - *NetScaler SDX Appliance*

- **Build 73.58 | NSHELP-43880**

  The NetScaler GUI Regex evaluator incorrectly returns a 'no-match' status for valid regex patterns.

  Module - *NetScaler Web App Firewall*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-43939**

  Custom Web App Firewall and BOT signature objects containing spaces in their names are dropped during upgrades.

  Module - *NetScaler Web App Firewall*

- **Build 73.58 | NSHELP-44550**

  In rare scenarios, NetScaler might restart unexpectedly when a Web Application Firewall profile applies Web Services Interoperability (WSI) or XML message-validation checks to server responses.

  Module - *NetScaler Web App Firewall*

- **Build 73.58 | NSHELP-44204**

  In rare scenarios, the NetScaler packet engine (PE) might crash because of failed buffer validation checks in the packet transmission path.

  Module - *Networking*

- **Build 73.58 | NSHELP-43937**

  On NetScaler BLX appliances, packet engines might restart unexpectedly when the BLX timer process loses timer ticks. This delay in heartbeats can trigger the process monitor to restart the packet engines.

  Module - *Platform*

- **Build 73.58 | NSHELP-44386**

  In high availability deployments, the secondary node might crash and reboot when signature updates are repeatedly pushed to the primary node through the NetScaler Console asset-delivery job. Primary nodes, standalone appliances, and automatic signature updates are unaffected.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workaround: Temporarily disable the NetScaler Console asset-delivery job. The recommended long-term solution is to upgrade to the latest build.

Module - *Security*

- **Build 73.58 | NSHELP-42021**

  When a show operation fetches any entity that contains sensitive data, the config engine might crash due to incorrect memory access.

  Module - *User Interface*

- **Build 73.58 | NSHELP-44095**

  If a disk space issue exists during loading, the application disables the **Next** button. Even after you clear disk space, the **Next** button is not enabled.

  Module - *User Interface*

- **Build 73.58 | NSHELP-44307**

  In a high availability or cluster setup, configuration and file synchronization might intermittently fail with a ”SYNC Failure - Save remote config failed” error. The synchronization succeeds in a subsequent attempt.

  Module - *User Interface*

- **Build 73.58 | NSHELP-44348**

  Updating an `SSLCertKey` on a non-FIPS platform might fail. This issue occurs because the underlying `sslfipskey` API call is only supported on FIPS-enabled platforms.

  Module - *User Interface*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Build 73.58 | NSHELP-44539**

  When you upgrade to build 14.1-72.61, the SVM UI prevents you from changing the `nsroot` user password. This affects administrators who manage user passwords through the SVM UI.

  Workaround: Use the command-line interface to change the password.

  Module - ***User Interface***

- **Build 73.58 | NSUI-23051**

  The **Next-Gen API OpenAPI Specification** link under Documentation returns a 404 error.

  Module - ***User Interface***

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).