NetScaler ADC (includes NetScaler Gateway)

Release Notes for NetScaler ADC (includes NetScaler Gateway) 14.1-66.59

July 22, 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.
- SDX Bundle 14.1-66.62 replaces SDX Bundle 14.1-66.55. This build includes the following fixes in addition to the enhancements and fixes included in SDX bundle 14.1-66.55: NSHELP-42234, NSHELP-42330, NSHELP-42435, NSHELP-41004, NSHELP-40946.
- Build 14.1-66.59 replaces Build 14.1-66.54.
- Build 14.1-66.59 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300.
- Build 14.1-66.59 includes the following fixes, along with the enhancements and fixes available in Build 14.1-66.54: NSHELP-40946, NSHELP-41004, NSHELP-41834, NSHELP-42234, NSHELP-42252, NSHELP-42391.

What's New

- **Build 66.59 | CTXENG-69689**

  Client IP address validation using X-Forwarded-For (XFF) in AAA sessions

  In Gateway and AAA deployments, stolen session cookies can be reused by attackers to hijack authenticated sessions. This risk increases in proxy or NAT environments where the direct source IP address seen by NetScaler does not represent the real client IP address. NetScaler tries to capture the clients real IP address and associates it with the authenticated AAA session. Earlier, this capability was based on the client source IP address. NetScaler now associates the IP address in the X-Forwarded-For header as a user attribute, along with the client IP address seen in the IP address header, to optimize proxy and NAT-based deployments. By validating the client IP address using XFF instead of only the source IP address, NetScaler enforces stronger session integrity even when traffic passes through intermediate devices. This significantly reduces the attack surface for session hijacking in complex network topologies.

  For more information related to client IP address validation , see Client IP address validation using X-Forwarded-For (XFF) in AAA sessions.

  Module - *Authentication, authorization, and auditing*

Fixed Issues

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

- **Build 66.59 | NSHELP-41332**

  NSPPE crashes on the secondary node when a `syslogpolicy` is bound to a load-balancing virtual server. This issue occurs due to a continuous sync and clear configuration loop.

  Module - ***Analytics Infrastructure***

- **Build 66.59 | NSHELP-41560**

  After configuring an appflow collector of type REST (add appflow collector -transport REST), the 'show running config' or 'savec' command output goes into an infinite loop.

  Module - ***Analytics Infrastructure***

- **Build 66.59 | NSHELP-41699**

  When you enable metrics in the time series analytics profile, the secondary node exports metrics with SNIP address as the source IP address instead of the NSIP address.

  Module - ***Analytics Infrastructure***

- **Build 66.59 | NSHELP-41843**

  After adding an analytics profile with a data format file of type `JSON`, adding another profile with a non-existent data format file might cause NetScaler to crash.

  Module - ***Analytics Infrastructure***

- **Build 66.59 | NSHELP-40689**

  In a rare scenario, authentication response data might be inconsistent due to improper data buffer merging.

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

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

- **Build 66.59 | NSHELP-40758**

  In an HA deployment, NetScaler might crash while updating SSL certificates. This issue occurs when NetScaler is configured as either a SAML Service Provider (SP) or as a SAML Identity Provider (IdP).

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

- **Build 66.59 | NSHELP-40811**

  The **Log On** button on the NetScaler Gateway login page is disabled, even when reCaptcha is not configured.

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

- **Build 66.59 | NSHELP-40303**

  NetScaler might crash when processing jumbo MQTT packets.

  Module - ***Load Balancing***

- **Build 66.59 | NSHELP-40534**

  Location-based policy evaluation might fail after an update to the location database. This can impact Global Server Load Balancing (GSLB) decisions if the virtual server uses static proximity load balancing or a policy with a location-based expression.

  Module - ***Load Balancing***

- **Build 66.59 | NSHELP-40725**

  NetScaler crashes when you attempt to reconfigure an HTTP-ECV monitor. This issue occurs because the initial configuration attempt with a non-existent netprofile (using 'send', 'recv', and 'trofsstring' parameters) fails silently without returning an error.

  Module - ***Load Balancing***

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

- **Build 66.59 | NSHELP-40753**

  NetScaler might crash if internal services are not monitored on inactive cluster nodes.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-40956**

  The load balancing method in a GSLB setup is ignored when all the GSLB services in the primary preferred location are down.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-40997**

  When creating a GSLB virtual server by using the CLI, the optional `backupVserver` parameter is not stored in the backend configuration.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-41146**

  A memory leak might occur when the DNS recursive resolver feature is enabled.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-41161**

  GSLB synchronization might fail for the server entities used in GSLB service if these entities are renamed.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-41303**

  The backup GSLB parent site might incorrectly triggers monitor probes for a child site if the corresponding load balancing entity is missing from that child site.

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

Module - *Load Balancing*

- **Build 66.59 | NSHELP-41534**

  NetScaler might crash when a GSLB service group contains multiple members sharing the same IP address but using different ports.

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-41555**

  Health states for service group members might become inconsistent under specific conditions. This issue occurs when using the following configuration:

  - Autoscale service group
  - Monitor threshold
  - Multiple monitors bound to the service group

  Module - *Load Balancing*

- **Build 66.59 | NSHELP-42391**

  In an HDX Proxy deployment, the STA response used to refresh the reconnect ticket is delivered in multiple packets due to TCP fragmentation, causing NetScaler HA failover.

  Module - *Miscellaneous*

- **Build 66.59 | GOPHDX-7640**

  Users might experience audio loss in the launched app or desktop when all of the following conditions are met:

  - EDT Loss Tolerant mode is enabled
  - HDX Insight is disabled
  - SmartControl or InsightToDirector is enabled on the NetScaler

  Module - *NetScaler Gateway*

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

- **Build 66.59 | GOPHDX-8095**

  The STA server binding fails when the explicit path to `ctxsta.dll` is included in the STA server configuration. This issue occurs when you configure either a virtual server or a global binding from the CLI or the GUI.

  Module - *NetScaler Gateway*

- **Build 66.59 | NSHELP-41079**

  The NetScaler Gateway portal fails to display the background image configured for the login page when a custom WSTheme is bound.

  Module - *NetScaler Gateway*

- **Build 66.59 | NSHELP-41384**

  In a NetScaler high-availability setup, the secondary node repeatedly crashes during synchronisation when you use VPN Gateway with StoreFront integration and security certificates.

  Module - *NetScaler Gateway*

- **Build 66.59 | NSHELP-41399**

  NetScaler might crash due to the use of an uninitialized pointer during server-side connection cleanup.

  Module - *NetScaler Gateway*

- **Build 66.59 | NSHELP-41544**

  The Web Application Firewall (WAF) might block the VPN setclient request when the Always-On functionality is enabled.

  Module - *NetScaler Gateway*

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

- **Build 66.59 | NSHELP-41549**

  NetScaler might crash due to improper handling of pointer references in the UDP audio code.

  Module - *NetScaler Gateway*

- **Build 66.59 | NSHELP-39273**

  When the VPX internal network is enabled in NetScaler SDX GUI, the high availability status does not update immediately when a NetScaler VPX instance transitions from Primary to Secondary or vice versa. This delay prevents administrators from accurately monitoring the current role of each appliance in the HA pair.

  Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSHELP-40946**

  RADIUS authentication might fail if the `username` field has a `NULL` value.

  Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSHELP-41004**

  During the process of retrieving the status of all subsystems, the `svm_inventory` causes the SVM CPU usage to reach 100%.

  Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSHELP-41341**

  High CPU usage occurs during heavy SNMP traffic because the system checks for the existence of the mastools configuration file on every SNMP data request. This results in excessive file system operations that consume CPU resources and degrade system performance.

  Module - *NetScaler SDX Appliance*

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

- **Build 66.59 | NSHELP-41701**

  NetScaler Console might fail to fetch the maximum bandwidth capacity for older SDX platforms.

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-41807**

  NetScaler Console service might display incorrect pooled license allocation information for NetScaler Console on-prem after SVM transitions to LAS.

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-42234**

  Even after applying a LAS fixed bandwidth license, the following notification to transition from file-based licensing appears:

  ```
  Please transition to LAS (License Activation Service)based
  licensing from file based licensing to avoid any service disruption
  , please refer to product documentation for more details.
  ```

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-42330**

  NetScaler VPX instances become unlicensed if the required bandwidth is not available in NetScaler Console and you have configured the license using the LAS mechanism from the SDX console.

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-42435**

  In rare scenarios, a NetScaler VPX instance on SDX might become unlicensed if the following sequence of conditions is met:

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

1. It was previously licensed using a pooled license.
2. The license server is unavailable.
3. A LAS-based license is applied later.

Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSSVM-7262**

  On NetScaler SDX 14000 platform, the Management Service crashes after you apply an LAS fixed bandwidth blob.

  Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSSVM-7268**

  On NetScaler SDX 14000 platform, the instance count shows as zero after a fixed bandwidth license is applied. This issue occurs because LAS fixed bandwidth support is not available on SDX 14000.

  Module - *NetScaler SDX Appliance*

- **Build 66.59 | NSHELP-40845**

  Importing AppFW relaxation rules to another profile might fail when the configuration includes `denyURL` and `excludeResContentType` checks.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-40805**

  LSN port leaks might be seen for unexpected failure cases.

  Module - *Networking*

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

- **Build 66.59 | NSHELP-41030**

  In an HA setup with the Secure Management feature enabled, the syncVlan and traffic domain binding configuration is lost after a reboot. This issue occurs due to the sequence of commands in the `ns.conf` file and the legacy traffic domain design.

  Module - ***Networking***

- **Build 66.59 | NSHELP-41630**

  In an HA configuration, BGP default routes fail to synchronize between the primary and secondary nodes. This issue occurs when the two nodes are running different versions of the software.

  Module - ***Networking***

- **Build 66.59 | NSHELP-40332**

  In NetScaler High Availability (HA) deployments on cloud platforms, HA recovery remains incomplete after a split-brain resolution. The services are disrupted because cloud resources stay with the secondary node even after the primary resumes its role. This issue occurs because after split-brain recovery primary node is not alerted to reclaim cloud resources.

  Module - ***Platform***

- **Build 66.59 | NSHELP-40437**

  After the SDX single-bundle upgrade, VPX instances on the SDX platform that are connected to a Juniper switch from a 10G, 25G, or 40G port might fail to come up properly during system boot up. The issue is observed because LLDP / DCBx is enabled on the Juniper switch.

  Module - ***Platform***

- **Build 66.59 | NSHELP-40959**

  When VRID is configured on an i40e interface, the following error is continuously seen on the console:

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

Conflict in vrid <id> on interface <interface-name> vlan <vlan-id> bridge_group -<id> from MAC <vrrp-mac> IP <ip-address>
This error does not have any functional impact and can be ignored.

Module - *Platform*

- **Build 66.59 | NSHELP-41078**

  The AWS cloud-ha-daemon.log file continuously logs IAM permission status messages, creating repetitive entries that make it difficult to identify meaningful events and unnecessarily increase the log file size. With the fix, the logging now occurs only when the permission status changes or during the initial check, reducing log verbosity while maintaining visibility into status changes.

  Module - *Platform*

- **Build 66.59 | NSHELP-41248**

  A NetScaler VPX instance deployed on modern AWS instance types (such as c6i) with ENA NIC might crash due to a bug in the transmit (Tx) checksum offload mechanism. This issue does not affect the VPX instances deployed on older 5th generation AWS instance types such as c5, m5, or m4.

  Module - *Platform*

- **Build 66.59 | NSHELP-41335**

  The error counter ”nic_err_rx” on interface ”LO/1” increments every 7 seconds, even though there are no new occurrences of these errors.

  Module - *Platform*

- **Build 66.59 | NSHELP-41413**

  VPX instances on AWS reboot multiple times during startup. This behavior occurs when Instance Metadata Service (IMDS) is unavailable for any reason during instance initialization.

  Module - *Platform*

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

- **Build 66.59 | NSLINUX-9568**

  In NetScaler BLX, generic executables such as openssl, curl, and scp, which are dependent on the `libcrypto` and `libssl` libraries, might not work as expected. This issue is seen by default on RHEL 9 distributions. Users on other distributions might also encounter this issue if they upgrade the `libcrypto` and `libssl` libraries.

  We recommend you to run such commands directly from the host.

  Module - ***Platform***

- **Build 66.59 | NSHELP-40807**

  Rewrite action might not work if HTTP response is chunked and doesn't contain any body.

  Module - ***Policies***

- **Build 66.59 | NSHELP-41336**

  Importing a responder HTML page in a non-default partition fails when the partition name includes spaces.

  Module - ***Policies***

- **Build 66.59 | NSHELP-41675**

  NetScaler might crash when enabling the policy tracing feature if the filter expression uses an HTTP-based expression.

  Module - ***Policies***

- **Build 66.59 | NSHELP-41704**

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

NetScaler VPX crashes when trying to bind a rewrite policy to a Content Switching virtual server, and core files are generated. This issue occurs when you use the `CLIENT.SSL.CLIENT_CERT.VALID_NOT_AFTER` or `CLIENT.SSL.CLIENT_CERT.VALID_NOT_BEFORE` expressions and the certificate data is beyond the year 2037.

Module - ***Policies***

- **Build 66.59 | NSPOLICY-6125**

  The `<text_t>.TYPECAST_IP_ADDRESS_T.EQUALS_ANY` and `<text_t>.TYPECAST_IP_ADDRES.EQUALS_INDEX` expressions might not work correctly with patset.

  Module - ***Policies***

- **Build 66.59 | NSHELP-41934**

  High memory utilization is observed on the secondary node of the HA pair due to a memory leak during built-in registry re-creation.

  Module - ***Security***

- **Build 66.59 | NSHELP-40737**

  NetScaler might crash in the following scenarios:

  - Running the clear config command while the Azure Key Vault token response is pending.
  - Removing an Azure application when multiple Azure applications are configured with the same domain but different tenant IDs in the token endpoint.

  Module - ***SSL***

- **Build 66.59 | NSHELP-40804**

  In the cluster CCO node, the output of the `show ssl certKeyBundle` command might display an incorrect expiration status for certificates (”Days to expiration”).

  Module - ***SSL***

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

- **Build 66.59 | NSHELP-40854**

  When adding a Hardware Security Module (HSM) key by using the NetScaler CLI and GUI, the operation incorrectly returns an error message even though the key is successfully created.

  Module - *SSL*

- **Build 66.59 | NSHELP-40916**

  In high availability deployments, configuration synchronization might occur frequently on the secondary NetScaler VPX instance even when no configuration changes are made on the primary NetScaler VPX instance. Each synchronization operation clears and reapplies the entire configuration, leading to a memory leak on the secondary instance that can degrade system performance over time.

  Module - *SSL*

- **Build 66.59 | NSHELP-41204**

  On the Linux platform, you cannot create an SSL certificate with subjectAltName because an incorrect configuration file is loaded.

  Module - *SSL*

- **Build 66.59 | NSHELP-41508**

  Continuous and unnecessary sync operations are seen on the secondary node of HA. This issue occurs because a zero-touch status update command is run on the primary node.

  Module - *SSL*

- **Build 66.59 | NSHELP-41625**

  VDA session launch fails on the following Intel SSL chip-based platforms when the network telemetry feature is enabled, and the negotiated TLS version is TLS1.2 or earlier.

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

  - MPX 5900
  - MPX/SDX 8900
  - MPX/SDX 15000 and 15000-50G
  - MPX/SDX 16000
  - MPX/SDX 26000, 26000-50S, and 26000-100G
  - MPX/SDX 9100

Module - *SSL*

- **Build 66.59 | NSHELP-41745**

  After a backend service or secure monitor begins closing a TLS 1.3 connection, an incoming packet might trigger a memory leak.

  Module - *SSL*

- **Build 66.59 | NSHELP-40911**

  Webpages fail to load intermittently when Client Side Measurements is enabled in AppFlow.

  Module - *System*

- **Build 66.59 | NSHELP-41095**

  Connection is incorrectly reset for HTTP traffic if the header value has a single character described for a SIP header.

  Module - *System*

- **Build 66.59 | NSHELP-41356**

  POST requests related to Client Side Measurements from clients are processed without proper validation.

  Module - *System*

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

- **Build 66.59 | NSCONFIG-12834**

  NITRO calls might not function on Lightweight CPX (LWCPX) when the NS_CPX_LITE environment variable is set to 1.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-40924**

  The NetScaler GUI incorrectly indicates that the syslog advanced policy is not bound, despite it being globally bound.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-41000**

  Syslog log levels might show incorrect field selections when you select all the parameters except DEBUG in **System > Auditing > Syslog Auditing > Servers** and save the changes.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-41141**

  Downloading backup files from the NetScaler GUI is blocked.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-41298**

  The regex editor evaluator in the NetScaler GUI might fail for valid regex use cases.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-41331**

  When adding a file through the NetScaler GUI, the operation might fail and display the error: NetScaler error: Communication error (RPC data-size mismatch).

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

Module - *User Interface*

- **Build 66.59 | NSHELP-41489**

  In an HA setup, importing FIPS keys succeeds on the primary node but fails on the secondary node.

  Module - *User Interface*

- **Build 66.59 | NSHELP-41660**

  NetScaler GUI login does not work if you are logged in from the partition SNIP.

  Module - *User Interface*

- **Build 66.59 | NSHELP-41819**

  When a two-factor authentication is configured on NetScaler, the GUI displays an invalid username/password message even after the correct second factor password is entered.

  Module - *User Interface*

- **Build 66.59 | NSHELP-41822**

  When unbinding a rewrite policy from an authentication virtual server using the GUI, an error occurs stating that the policy label does not exist. However, the unbinding is successful when using the CLI and specifying TYPE AAA_RESPONSE.

  Module - *User Interface*

- **Build 66.59 | NSHELP-41834**

  The command `apply laslicense` might time out if the management CPU or disk IO wait is high.

  Module - *User Interface*

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

- **Build 66.59 | NSHELP-41951**

  The NetScaler Management GUI does not function when accessed through a Virtual IP (VIP) address, preventing administrators from managing the appliance through VIP-based connections.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-42020**

  NetScaler Management GUI is not accessible when the secure management feature is enabled.

  Module - ***User Interface***

- **Build 66.59 | NSHELP-42252**

  NetScaler upgrade might fail when pooled licensing is configured, but the license server is unreachable. When the license server is unreachable, the system displays a warning about the risk of NetScaler becoming unlicensed. You can ignore this warning and continue with the upgrade.

  Module - ***User Interface***

Known Issues

- **Build 66.59 | NSHELP-41140**

  When strings are encoded in JSON, they might be corrupted due to the presence of unescaped control characters.

  Module - ***Analytics Infrastructure***

- **Build 66.59 | NSHELP-41991**

  Buffers are not available when ‘newnslog‘ is disabled due to disk space constraints. Therefore, accessing buffers to write NetScaler Console messages might result in a crash.

  Module - ***Analytics Infrastructure***

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

- **Build 66.59 | NSAUTH-11151**

  Administrators cannot perform custom logging for authentication failures that happen due to invalid credentials. This issue occurs because the NetScaler responder policies fail to detect errors for login failures.

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

- **Build 66.59 | NSAUTH-17993**

  On a NetScaler VPX instance configured with authentication, SSL services might intermittently become unavailable for a short period. This issue occurs when the authentication daemon (AAAD) unexpectedly crashes and restarts.

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

- **Build 66.59 | NSHELP-41104**

  Rewrite policies might not work on a few authentication and authorization endpoints, preventing rewrite actions from taking effect.

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

- **Build 66.59 | NSHELP-40913**

  NetScaler might fail and dump core if an autoscale service group is configured and a DNS_TCP based monitor is active.

  Module - ***Load Balancing***

- **Build 66.59 | NSHELP-41752**

  The GSLB configuration synchronisation might fail if a GSLB subordinate sites are on VPX Linux platform and main site is on VPX Freebsd platform.

  Module - ***Load Balancing***

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

- **Build 66.59 | NSHELP-41932**

  When persistence groups are configured with traffic domains, mismatch between GUI and CLI validation might occur. This inconsistency prevents persistence group virtual server configurations from synchronizing to the secondary node, impacting high-availability deployments.

  Module - ***Load Balancing***

- **Build 66.59 | 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 66.59 | NSHELP-40801**

  When two namespaces with names having a common prefix have services with the same name, deleting an endpoint of a service in one namespace unintentionally removes the service group member bindings of another service deployed in another namespace.

  Module - ***Miscellaneous***

- **Build 66.59 | NSHELP-41134**

  During startup, the NetScaler Ingress Controller unbinds and rebinds SSL certificates when processing secure ingresses that share the same virtual server IP address and port.

  Module - ***Miscellaneous***

- **Build 66.59 | NSHELP-41484**

  NetScaler might generate the `lsof_<hostname>` file each time you create a support bundle. However, the system fails to remove these files immediately after the generation process is complete.

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

Module - ***Miscellaneous***

- **Build 66.59 | NSHELP-41640**

  The application crashes with continuous NITRO exception errors due to version incompatibility between NetScaler version 13.1 and NetScaler Ingress Controller version 3.3.2.

  Module - ***Miscellaneous***

- **Build 66.59 | NSHELP-39780**

  NetScaler rewrite policies are not applied on some of the gateway URLs.

  Module - ***NetScaler Gateway***

- **Build 66.59 | NSHELP-40999**

  The audit server might crash if the number of file descriptors exceeds the default maximum value.

  Module - ***NetScaler Gateway***

- **Build 66.59 | NSHELP-41816**

  In some login flows, the NetScaler Gateway login page might display a broken image for an icon when the Workspace theme is used. This is caused by missing images within the theme directory.

  Module - ***NetScaler Gateway***

- **Build 66.59 | NSHELP-42149**

  In a high availability setup, the primary node fails because of a crash in the IPsecALG module.

  Module - ***NetScaler Gateway***

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

- **Build 66.59 | NSHELP-42054**

  As part of instance backup and restore, the hidden files that start with "." are not backed up or restored.

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-42818**

  This issue will impact you if you have an SDX migrated or migrating from any type of NetScaler local license (fixed capacity subscription or perpetual license) file based licensing to any type of license with LAS based licensing and the legacy file-based licenses have not been deleted from the SVM.

  Impact: If there is any local legacy file-based license yet existing on the SVM after having transitioned to LAS, then the expiry of the file-based license triggers the un-licensing of the SDX (SVM and VPX on SDX) on the date of that license file expiry.

  Workaround: Delete the local file-based license(s) on the SVM after the migration to LAS has been done successfully. The file-based licenses would be located in SVM folder /mpsconfig/license and must be deleted from this folder using the shell prompt.

  Module - ***NetScaler SDX Appliance***

- **Build 66.59 | NSHELP-40544**

  Users might encounter memory allocation errors when the soapArrayCheck setting in the AppFW profile's XMLDOS configuration is enabled.

  Module - ***NetScaler Web App Firewall***

- **Build 66.59 | NSHELP-41008**

  DUT might crash when some XML protections are enabled and configured in a non-blocking mode.

  Module - ***NetScaler Web App Firewall***

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

- **Build 66.59 | NSHELP-41518**

  Client requests might fail if HTTP/2 header values contain space characters. These spaces can trigger header frame processing errors, particularly when the client sends improperly formatted header values.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-41642**

  The match URL functionality might fail for some relaxation rules in regular expression format while importing the application firewall relaxation rules.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-41647**

  NetScaler might crash when you enable Application Firewall, Integrated Caching, and Compression features simultaneously with advanced checks configured on the Application Firewall profile.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-41861**

  During an upgrade, imported object names fail to persist if they contain uppercase characters. This issue causes the loss of the corresponding configuration and prevents persistent settings.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-41875**

  In rare scenarios, configuring a large number of AppFW safe objects might trigger a failover.

  Module - *NetScaler Web App Firewall*

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

- **Build 66.59 | NSHELP-42188**

  In rare scenarios, a HA failover might occur when NetScaler has application firewall signatures with complex regex patterns.

  Module - *NetScaler Web App Firewall*

- **Build 66.59 | NSHELP-36236**

  A two-node cluster becomes inactive if a critical interface on one of the nodes is down.

  Module - *Networking*

- **Build 66.59 | NSHELP-42209**

  In rare scenarios, the data transfer over a TCP connection might stall completely if the following parameters or settings are configured:

  - SSL record length
  - TCP MSS settings
  - Mellanox Interface Jumbo MTU (more than 1500)

  Module - *Platform*

- **Build 66.59 | NSHELP-43886**

  During an upgrade, imported object names fail to persist if they contain uppercase characters. This issue causes the loss of the corresponding configuration and prevents persistent settings.

  Module - *Platform*

- **Build 66.59 | NSLINUX-7437**

  The RDP Proxy functionality is not supported in BLX Gateway.

  Module - *Platform*

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

- **Build 66.59 | NSLINUX-8026**

  On Oracle Linux, the NetScaler Packet Processing Engine (NSPPE) might crash during active traffic flow on a Mellanox interface when worker process value in the 'blx.conf' file is modified and NetScaler BLX is restarted using the 'systemctl restart blx' command.

  Workaround: To start the BLX service, follow these steps:

  1. Run the 'systemctl stop blx' command.
  2. Edit the blx.conf file, and run the 'systemctl start blx' command.

  Module - *Platform*

- **Build 66.59 | NSLINUX-8133**

  The ‘mgmthttpsport‘ command might not work as expected, leading to issues with HTTPS management access on NetScaler BLX.

  Workaround: Restart NetScaler BLX to apply the configuration.

  Module - *Platform*

- **Build 66.59 | NSPLAT-31350**

  In a NetScaler VPX high availability setup on AWS, a delay in failover might occur if the IAM service is unreachable. This issue occurs because NetScaler performs IAM permission checks before applying the cloud-specific configurations. Therefore, the failover process might be delayed when the IAM service is unavailable.

  Module - *Platform*

- **Build 66.59 | NSHELP-41726**

  When traffic is processed through an SSL virtual server, a 100 ms delay occurs during HTTP callouts. This latency specifically impacts the performance of the HTTP callout function.

  Module - *Policies*

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

- **Build 66.59 | NSHELP-41132**

  An Operation timed out error might occur when you add multi-megabyte OpenAPI specification files using the `add apispec` command.

  Module - *Security*

- **Build 66.59 | NSSSL-17320**

  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.

  Workaround: Rename the certificate and key files to remove any spaces.

  Module - *SSL*

- **Build 66.59 | NSBASE-20237**

  Customers see unexpected system restarts when Integrated Caching is enabled on high-memory VMs. This issue occurs because the packet engine (PE) takes longer to boot, misses heartbeat checks, and Pitboss sends a SIGABORT to the PE.

  Module - *System*

- **Build 66.59 | NSHELP-41138**

  Pipeline upload requests might fail when the backend service returns an error response instead of `200 OK` or `100 Continue` responses.

  Module - *System*

- **Build 66.59 | NSHELP-41671**

  Custom headers within gRPC response trailers might fail to propagate to the client. This issue impacts client applications that rely on custom headers in the gRPC response trailer.

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

Module - *System*

- **Build 66.59 | NSHELP-41702**

  When `-markHTTPHeaderExtraWSError` is enabled in the HTTP profile, NetScaler incorrectly terminates connection tracking when whitespace appears before and after the HTTP header values, even though such whitespace is RFC-compliant. This behavior can reduce HTTP standards compliance. As a workaround, remove the whitespace check preceding the HTTP header value.

  Module - *System*

- **Build 66.59 | NSHELP-41874**

  NetScaler might crash when an HTTP response is chunked without a body, containing only the final chunk. This issue occurs during transactions where SSL, rewrite, and compression (CMP) are enabled.

  Module - *System*

- **Build 66.59 | NSHELP-42091**

  NetScaler appliances crash or HTTP/3 connections terminate incorrectly, when you configure an HTTP_QUIC virtual server and the appliance receives specific sequences of QUIC packets. This problem occurs because of how the appliance processes these QUIC packet sequences.

  Module - *System*

- **Build 66.59 | NSHELP-42103**

  Pitboss logs might sometimes flood ns.log when the SSLVPN or IC feature is enabled and cache memory is set to 492 MB, specifically when the number of NetScaler packet engines is 4 or 5.

  Module - *System*

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

- **Build 66.59 | NSHELP-41585**

  When configuring a new audit server using the NetScaler GUI, the Syslog Compliance field automatically defaults to RFC5424, even if the value is explicitly left blank during setup.

  Module - *User Interface*

- **Build 66.59 | NSHELP-42128**

  The NetScaler Gateway VIP login page is not accessible when configured with the custom port 8443.

  Module - *User Interface*

- **Build 66.59 | NSHELP-42290**

  Starting from NetScaler build 14.1-60.x, filter expressions with special characters, such as && and `||`, fail when you run `nstrace` from the NetScaler GUI.

  Workaround: Use the NetScaler CLI.

  Module - *User Interface*

- **Build 66.59 | NSUI-20282**

  When you try to add the expression `HTTP.REQ.URL.LENGTH.GT(10).IF(HTTP.REQ.URL, HTTP.REQ.HEADER("Test"))`, the expression editor displays the following warning message, despite the expression being valid:

  ```
  Result expression types must be compatible
  ```

  Module - *User Interface*

- **Build 66.59 | NSUI-22522**

  LAS enforcement notification and some other error notifications are not displayed in the GUI.

  Workaround: For LAS-related error notification, you can run the 'show ns license' command on CLI, and the output has one key value: 'Days to LAS enforcement: 80'

  Module - *User Interface*

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

- **Build 66.59 | NSUI-22547**

  In admin partition, users are unable to generate a Support Bundle from the NetScaler GUI . The action either fails silently or returns an error, preventing administrators from collecting diagnostic data.

  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).