NetScaler ADC (includes NetScaler Gateway)

Release Notes for NetScaler ADC (includes NetScaler Gateway) 14.1-51.80

April 28, 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 14.1-51.80 replaces Build 14.1-51.72.
- Build 14.1-51.80 includes the following enhancements along with the enhancements and fixes available in Build 14.1-51.72: CTXENG-69948.

What's New

- **Build 51.80 | CTXENG-66252**

  Support to export transaction logs directly from NetScaler to Kafka

  NetScaler now directly integrates with Kafka, a robust, scalable, and fault-tolerant platform for collecting and streaming logs. This integration enables the direct export of transaction logs from NetScaler to Kafka, eliminating the need for additional agents or nodes for data export.

  For more information, refer to the documentation on Export transaction logs directly from NetScaler to Kafka.

  Module - *Analytics Infrastructure*

- **Build 51.80 | CTXENG-66245**

  Support pull and push of counters to Prometheus from secondary node

  Starting from NetScaler 14.1-51.x, you can monitor metrics from the secondary node in a High Availability (HA) environment. The secondary node supports both push and pull mode of operation.

  Since the secondary node is passive and does not handle data traffic, its data-related counters are not present. However, the metrics that report the nodes health and state are available. When a new schema file is created or modified on the primary node, the changes are automatically synced to the secondary node.

  The following entities can be monitored on the secondary node:

  - Cluster_instance
  - Cluster_node

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

- Interface
- Netscaler
- Cpu
- Mempool
- Vlan
- partition

For more information, see https://docs.netscaler.com/en-us/citrix-adc/current-release/observability/prometheus-integration.

Module - *Analytics Infrastructure*

- **Build 51.80 | CTXENG-67291**

  Google re-Captcha v3 support for Enterprise console

  Google re-Captcha v3 support is now included for the Enterprise console that allows for an increased request limit based on the subscription plan.

  re-Captcha configuration on Google

  1. Sign in to https://console.cloud.google.com/ by using a gmail account and create a project.

  2. Go to https://console.cloud.google.com/security/recaptcha and create the site key. Note the created site key. For more information, see the Google re-Captcha document.

  3. Go to https://console.cloud.google.com/apis/ and create an API key. Note the created API key. For more information, see the Google re-Captcha document.

  4. Go to https://console.cloud.google.com/security/recaptcha and copy the server URL from the assessment API (copy till the term ”assessments”). Save the copied server URL.
  For example, if the assessment API is ”https://recaptchaenterprise.googleapis.com/v1/projects/tactile-reason-455709-p6/assessments?key=API_KEY”, you must copy the portion up to ”assessments”, which is ”https://recaptchaenterprise.googleapis.com/v1/projects/tactile-reason-455709-p6/assessments”. This extracted URL is used as the server URL in the ‘captchacation‘ command.

  re-Captcha configuration on NetScaler

  To configure display of re-Captcha

  At the command prompt, type:

  ```
  1 add authentication loginSchema singleauthcaptcha -
      authenticationSchema SingleAuthReCaptchav3Enterprise.xml
  2
  ```

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

```
add authentication loginSchemaPolicy singleauthcaptcha -rule true
    -action singleauthcaptcha

add authentication vserver auth SSL <IP> <Port>

add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-
    to-key-file>

bind ssl vserver auth -certkey vserver-cert

bind authentication vserver auth -policy singleauthcaptcha -
    priority 5 -gotoPriorityExpression END
```

To verify re-Captcha response from the browser

At the command prompt, type:

```
add authentication captchaAction -siteKey <sitekey> -secretKey <
    APIkey> -scoreThreshold<0 - 10> -serverurl <serverURL>

add authentication policy myrecaptcha -rule true -action
    myrecaptcha

bind authentication vserver auth -policy myrecaptcha -priority 1
```

The default value of ‘scoreThreshold‘ is 5.

For more information, see re-Captcha configuration for nFactor authentication.

Module - *Authentication, authorization, and auditing*

- **Build 51.80 | CTXENG-66275**

  Enhanced Persistence Cookie Security

  With the new enhanced Persistence Cookie Security feature, NetScaler can now encrypt persistence cookie names along with the cookie value.

  The following are the benefits:

  - Simplifies configuration management and reduces administrative overhead.
  - Ensures consistent application of security policies for persistence cookies across all your virtual servers, reducing the chance of misconfigurations.
  - Encrypts the default cookie name and value thereby enhancing security.

  Enable encrypted persistence cookies

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

You can enable encrypted persistence cookies either globally or selectively for specific load balancing virtual servers.

To enable globally by using CLI

At the command prompt, type:

```
set lb param –useencryptedPersistenceCookie ENABLED
```

Note: After enabling encryption, set a unique custom passphrase for enhanced security using the command 'set lb param -cookiePassphrase <custom_cookie_passphrase>'

To enable selectively on a load balancing profile by using CLI

1. Configure the load balancing profile. At the command prompt, type:

```
set lb profile <name> –useencryptedPersistenceCookie ENABLED –
   cookiePassphrase <custom_cookie_passphrase>
```

2. Associate the load balancing profile to the virtual server. At the command prompt, type:

```
set lb vserver <name> –lbprofilename <profile name>
```

To enable encrypted persistence cookies globally by using GUI

1. Navigate to **Traffic Management > Load Balancing**.

2. In the **Load Balancing** page, click **Change Load Balancing Parameters** under **Settings**.

3. In the **Configure Load Balancing Parameters** page, Select **Encode Persistence Cookie Values** and enter a passphrase in **Cookie Passphrase.**

To enable selectively on a load balancing profile by using GUI

1. Navigate to **Configuration** > **System** > **Profiles**.

2. Click the **LB Profile** tab, and then click the required profile.

3. In the **LB Profile** page, select **Encode persistence cookie values** and enter a passphrase in **Cookie Passphrase.**

4. Click **OK.**

Module - ***Load Balancing***

- **Build 51.80 | CTXENG-68204**

  Enhanced ICMPv6 responses for virtual servers

  NetScaler provides granular control over Internet Control Message Protocol version 6 (ICMPv6) responses based on virtual server states. This enhancement allows administrators to configure

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

how NetScaler responds to ICMPv6 requests destined for Virtual IPv6 addresses, considering the operational state of associated virtual servers. You can configure NetScaler to respond to IPv6 pings only when your services are healthy.

This feature offers the following benefits:

- Improved network monitoring and troubleshooting capabilities for IPv6 environments.
- Enhanced control over Virtual IPv6 address visibility and response behavior.
- Flexible configuration options to match different IPv6 deployment scenarios.

You can configure the ICMPv6 responses in the following two ways:

- IPv6 address related configuration
- Virtual server related configuration

IPv6 address related configuration

You can set rules that determine how your IPv6 address handles ICMPv6 requests. NetScaler uses these rules to determine whether to respond to incoming ICMPv6 echo requests:

- **NONE:** Responds always to ICMPv6 requests (default behavior).
- **ONE_VSERVER:** Responds if at least one virtual server on the IPv6 address is UP.
- **ALL_VSERVER:** Responds only if all virtual servers on the IPv6 address are UP.
- **VSVR_CNTRLD:** Uses per-virtual server settings to determine response behavior.

Configure IPv6 address with ICMP response control

To add a new IPv6 address and configure ICMPv6 response behavior, use the following command:

```
add ip6 <IPv6Address>/<Prefix_length> -type vip -icmpresponse <
    NONE|ONE_VSERVER| ALL_VSERVERS|VSVR_CNTRLD>
```

Examples:

```
add ns ip6 3f86::50/128 -type VIP -icmpResponse NONE
add ns ip6 3f86::51/128 -type VIP -icmpResponse ONE_VSERVER
add ns ip6 3f86::52/128 -type VIP -icmpResponse ALL_VSERVERS
add ns ip6 3f86::53/128 -type VIP -icmpResponse VSVR_CNTRLD
```

To modify the ICMP response behavior for an existing IPv6 address, use the following command:

```
set ip6 <IPv6Address>/<Prefix_length> -icmpresponse <NONE|
    ONE_VSERVER| ALL_VSERVERS|VSVR_CNTRLD>
```

Examples:

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

```
set ns ip6 3f86::50/128 -icmpResponse ONE_VSERVER
set ns ip6 3f86::51/128 -icmpResponse ALL_VSERVERS
set ns ip6 3f86::52/128 -icmpResponse VSVR_CNTRLD
set ns ip6 3f86::53/128 -icmpResponse NONE
```

To remove IPv6 address and reset the ICMP response setting to its default value, use the following command:

```
unset ip6 <IPv6Address>/<Prefix_length> -icmpresponse
```

Example:

```
unset ns ip6 3f86::50/128 -icmpresponse
```

To view the current IPv6 address configuration and ICMP response settings, use the following command:

```
show ip6 <IPv6Address>
```

Example:

```
show ns ip6 3f86::50
```

Note: GUI support for configuring ICMP response settings is not available for IPv6 addresses. Use the CLI commands for IPv6 ICMP response configuration.

Virtual server related configuration

NetScaler evaluates each virtual server's ICMP setting to decide whether that service affects ping responses. This feature supports the following virtual server types:

- Load Balancing
- Content Switching
- Cache Redirection
- Gateway/VPN virtual servers

The following configuration options are available:

- **PASSIVE:** This virtual server doesn't influence ping decisions - NetScaler responds normally (default)
- **ACTIVE:** This virtual server controls ping responses - NetScaler responds only when the service is UP.
- **Mixed PASSIVE and ACTIVE:** NetScaler responds if any ACTIVE virtual server is UP (PASSIVE virtual servers are ignored in the decision).

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

Configure ICMP response behavior for virtual server

To create a new virtual server and configure its ICMP response behavior, use the following command:

```
add lb/cs/cr/vpn vserver <name> <serviceType> <IPv6Address> <port>
    -icmpVsrResponse <PASSIVE|ACTIVE>
```

Examples:

```
add lb vserver web_vs HTTP 2001:db8::100 80 -icmpVsrResponse
   ACTIVE
add cs vserver content_vs HTTP 2001:db8::101 80 -icmpVsrResponse
   PASSIVE
add cr vserver cache_vs HTTP 2001:db8::102 80 -icmpVsrResponse
   ACTIVE
add vpn vserver ssl_vs SSL 2001:db8::103 443 -icmpVsrResponse
   PASSIVE
```

To modify the ICMP response behavior for an existing virtual server, use the following command:

```
set lb/cs/cr/vpn vserver <name> -icmpVsrResponse <PASSIVE|ACTIVE>
```

Examples:

```
set lb vserver web_vs -icmpVsrResponse PASSIVE
set cs vserver content_vs -icmpVsrResponse ACTIVE
set cr vserver cache_vs -icmpVsrResponse PASSIVE
set vpn vserver ssl_vs -icmpVsrResponse ACTIVE
```

To remove virtual server and reset the ICMP response behavior to its default value, use the following command:

```
unset lb/cs/cr/vpn vserver <name> -icmpVsrResponse
```

For more information, see https://docs.netscaler.com/en-us/citrix-adc/current-release/networking/ip-addressing/configuring-citrix-adc-owned-ip-addresses/configure-icmp-responses-for-virtual-servers.html.

Module - *Networking*

- **Build 51.80 | CTXENG-66855**

  Secure Management: Implement strict separation of Management and Data planes

  NetScaler now introduces the Secure Management feature, designed to significantly strengthen system security by fully isolating the management network from the data network. This enhancement provides a logical separation of all NetScaler functions into distinct management

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

and data plane categories. When enabled, each plane operates with its own dedicated routing table, ensuring that management traffic is kept entirely separate and distinct from data traffic.

This feature provides the following key benefits:

- Minimizes the risk of unauthorized access and protects sensitive management functions by preventing intermingling of management and data traffic.
- Ensures a clear distinction between management and data paths, preventing unauthorized access and improving network clarity.
- By separating functionalities, it enhances both the security and operational efficiency of NetScaler.
- Allows users to customize traffic handling and routing according to their specific network security and operational needs.
- Enables the creation and control of separate management and data plane routing tables, effectively mitigating various security threats.

For more information, see Implement strict separation of Management and Data planes in NetScaler.

Module - *Networking*

- **Build 51.80 | CTXENG-66495**

  Force completion of ISSU migration

  During In Service Software Upgrade (ISSU), NetScaler waits for existing connections to naturally close before completing the migration. However, some connections may be long-lived and prevent the migration from proceeding to completion.

  The ”Force ISSU Migration Completion” feature allows administrators to force the completion of ISSU migration by terminating long-lived active connections. The management-related sessions, such as CLI, GUI, and Console connections, are excluded from migration to ensure uninterrupted access. This enhancement improves the efficiency and reliability of ISSU processes.

  This feature can be used in the following scenarios:

  - When migration is ”in progress” and waiting for connections to close.
  - When rollback is ”in progress” and waiting for connections to close.

  Force completion of ISSU migration by using the CLI

  At the command prompt, type:

  ```
  1 complete ns migration
  ```

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

Force completion of ISSU migration by using the GUI

1. Navigate to **System > System Information > Migration** tab.

2. Click **Complete Migration** to terminate active migrated connections and mark the migration status as ”Complete.”

Module - ***Networking***

- **Build 51.80 | CTXENG-68452**

  Support for an extra Management CPU core on NetScaler VPX

  NetScaler VPX appliances typically use a single CPU core for management tasks, such as configuration, monitoring and control operations. In environments with significant management demands, this default configuration may lead to performance bottlenecks, resulting in slower response times and potential delays in management operations.

  This feature allows administrators to allocate an additional CPU core specifically for management functions. This enhancement enables a more efficient allocation of resources, leading to improved management operations without compromising data traffic processing capability. Users benefit from increased responsiveness and better management performance, particularly in environments with high management workload requirements.

  Important considerations:

  - This feature is supported only on NetScaler VPX instances with at least 4 vCPUs and more than two packet engines.
  - Activating this feature decreases the CPU cores allocated for data traffic processing.
  - Schedule this configuration change during a maintenance window, as the appliance must be rebooted for the changes to take effect.

  Configure an extra Management CPU core by using the CLI

  To enable the extra Management CPU core, use the following command:

  ```
  1 enable extramgmtcpu
  ```

  To disable the extra Management CPU core, use the following command:

  ```
  1 disable extramgmtcpu
  ```

  Note: A reboot is required for the configuration changes to take effect.

  To verify whether the extra management CPU core feature is enabled or disabled, use the following command:

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

```
show extramgmtcpu
ConfiguredState: DISABLED, EffectiveState: DISABLED
```

This command returns the configured and effective states of the extra management CPU core. This command helps administrators to quickly assess its operational status and determine if any further actions are needed to enable or disable it.

Configure an extra Management CPU core by using the GUI

1. Navigate to **Configuration > System > Settings**.
2. Select the **Configure Extra Management CPU** option.
3. In the **Configured State** drop-down menu, select **ENABLED**, and then click **OK**.
4. To apply the changes, go back to **Configuration > System** and click **Reboot**. Confirm the action by clicking **OK**.

Note: To disable the feature, select **DISABLED** in the **Configured State** drop-down menu.

For more information, see https://docs.netscaler.com/en-us/vpx/current-release/configure-extra-management-cpu.

Module - *Platform*

- **Build 51.80 | CTXENG-68107**

  Support for Rocky Linux

  NetScaler BLX now supports the Rocky Linux distribution 8.

  Module - *Platform*

- **Build 51.80 | CTXENG-67975**

  Support for Microsoft Hyper-V 2025 in NetScaler VPX

  NetScaler VPX now supports Microsoft Hyper-V 2025, enabling customers to deploy VPX instances on the latest Hyper-V platforms. This support offers improved performance, scalability, and security, while ensuring flexibility and future readiness for their virtualization strategy.

  Module - *Platform*

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

- **Build 51.80 | CTXENG-66686**

  NetScaler VPX Support on Nutanix Acropolis Hypervisor

  The new NetScaler VPX is now officially supported on Nutanix Acropolis Hypervisor (AHV). This integration enhances the user experience by allowing seamless management and deployment through Nutanix Prism, aligning with modern virtualization needs for improved performance and scalability.

  If you're using the legacy Citrix Ready VPX on Nutanix, you need to migrate to the new version for continued and full support coverage.

  For more information, see the following documentation:

  https://docs.netscaler.com/en-us/vpx/current-release/install-vpx-on-nutanix
  https://docs.netscaler.com/en-us/vpx/current-release/install-vpx-on-nutanix/migrate-from-citrix-ready-kvm-to-official-vpx-nutanix

  https://docs.netscaler.com/en-us/vpx/current-release/install-vpx-on-nutanix/faqs-vpx-on-nutanix

  Module - *Platform*

- **Build 51.80 | CTXENG-66087**

  Enhanced audit logging for TLS Session ID and SNI

  In today's security-conscious environment, comprehensive logs are paramount for in-depth troubleshooting and informed decision-making. Recognizing this critical need, NetScaler now enhances its frontend and backend logging to include Server Name Indication (SNI) details for both TLS 1.2 and TLS 1.3 sessions. Additionally, TLS Session ID (for TLS 1.2 sessions) and the TLS 1.3 client tracking ID (for TLS 1.3 sessions) are logged directly in the ns.log. It's important to note that while TLS Session ID is logged for both frontend and backend, the TLS 1.3 client tracking ID is specifically available in frontend logs only. This enhancement provides the granular visibility essential for maintaining a strong security posture and operational efficiency.

  The improved logging covers various SNI and TLS session scenarios, ensuring comprehensive visibility:

  - **ECH Handshakes:** The successfully negotiated SNI name is logged.
  - **SNI Sent, Disabled on Virtual Server:** If a client sends an SNI but it is disabled on the virtual server, NetScaler serves the default certificate (if bound). The event is logged as:

```
Client Req SNI "<Domain name>" -reason "No matching certificate
    found. Default certificate sent
```

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

- **SNI Enabled, No Match, ”Allow Unknown SNI” Configured:** If a client sends an SNI, SNI is enabled, but no matching certificate is found (and ”Allow unknown SNI” is configured), NetScaler serves the default certificate (if bound). The event is logged as:

```
-Client Req SNI "<Domain Name>" -reason "No matching certificate found. Default certificate sent
```

- **Client Connects Without SNI, SNI Enabled, No Match:** When a client connects without SNI, SNI is enabled on the virtual server, and no matching certificate is found, NetScaler rejects the connection. The event is logged as:

```
-Client Req SNI "<Domain Name>" -reason "No matching certificate found
```

- **Successful SNI Match:** The client provides an SNI and a corresponding certificate is found, the log shows:

```
-Client Req SNI "<Domain Name>" -reason "Matching certificate found
```

Enable TLS Session and SNI Logging

To enable the enhanced TLS session ID and SNI logging, configure the ‘*sslclientLogs*‘ parameter at the appropriate level.

Notes:

- SNI is logged for both TLS 1.2 and TLS 1.3 sessions, on both the frontend and the backend.
- The ** TLS Session ID is specific to TLS 1.2 and is logged for both frontend and backend connections.
- For TLS 1.3 sessions, the TLS Session ID is not present. Instead, the TLS 1.3 client tracking ID is logged, but only for frontend connections.

To enable enhanced TLS session ID and SNI logging by using CLI:

You can enable ‘sslclientLogs_‘_ using the ‘set sl‘ command for different entities:

1. **At the Virtual Server Level (Frontend):** To enable logging for a specific SSL virtual server:

```
set ssl vserver <name> -sslclientLogs ENABLED
```

2. **At the Service Level (Backend):** To enable logging for a specific SSL service:

```
set ssl service <service_name> -sslclientLogs ENABLED
```

3. **At the Service Group Level (Backend):** To enable logging for a specific SSL service group:

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

```
set ssl serviceGroup <servicegroup_name> -sslclientLogs ENABLED
```

4. **Using SSL Profiles:** If SSL profiles are enabled and in use, you can configure logging directly on the profiles.

- For Frontend SSL Profile: To enable logging for the default frontend SSL profile:

```
set ssl profile ns_default_ssl_profile_frontend -sslclientLogs
   ENABLED
```

If you are using a custom frontend SSL profile, replace ns_default_ssl_profile_frontend with the name of your custom profile.

- For Backend SSL Profile: To enable logging for the default backend SSL profile:

```
set ssl profile ns_default_ssl_profile_backend -sslclientLogs
   ENABLED
```

If you are using a custom backend SSL profile, replace ns_default_ssl_profile_backend with the name of your custom profile.

To enable Client Logs for Enhanced SSL Profiles (Frontend and Backend) by using GUI

1. Navigate to **System > Profiles> SSL Profile**.
2. Select the required profile (frontend or backend) and click **Edit**.
3. In the **Basic Settings** section, click the pencil icon.
4. Select **SSL client Logs**.
5. Click **OK**.

To enable client logs for a virtual server

1. Navigate to T*raffic Management > Load Balancing > Virtual Servers*.
2. Select the SSL virtual server and click **Edit**.
3. Under **Advanced Settings**, click **SSL Parameters**.
4. In the **SSL Parameters** section, click the pencil icon.
5. Select **SSL client Logs**.
6. Click **OK**.

To enable client logs for a service

1. Navigate to **Traffic Management > Load Balancing > Services**
2. Select the service and click **Edit**.

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

3. In the **SSL Parameters** section, click the pencil icon.
4. Select **SSL client Logs**.
5. Click **OK**.

For more information, see https://docs.netscaler.com/en-us/citrix-adc/current-release/ssl/audit-logging-tls .

Module - *SSL*

- **Build 51.80 | CTXENG-65949**

  Support for Hybrid Post-Quantum Cryptography on the front end.

  The rapid advancement of quantum computing presents a significant challenge to the security of modern digital communications. Using principles like superposition, entanglement, and interference, quantum computers will soon possess the power to break the asymmetric cryptographic algorithms that form the backbone of today's internet security, including RSA, DH/DHE/ECDH/ECDHE, and DSA.

  To address these critical challenges, NetScaler supports Hybrid Post-Quantum Cryptography (PQC) on the frontend. This feature allows your NetScaler to perform key exchange using quantum-resistant algorithms, safeguarding your communications against future quantum attacks.

  Major browsers, including Google Chrome, Mozilla Firefox, and Microsoft Edge, already support Hybrid PQC, with X25519MLKEM768 (0x11EC) being the most widely used cipher.

  Users can easily and securely negotiate key exchanges with NetScaler using Hybrid PQC (X25519_MLKEM768). This new feature provides protection against HNDL (Harvest Now Decrypt Later) and adheres to regulatory compliances.

  Note: This feature is available only for enhanced SSL Profile.

  Enable PQC on NetScaler

  To enable hybrid PQC on NetScaler, configure an SSL profile to include the X25519_MLKEM768 elliptic curve.

  You can bind elliptic curves to an SSL profile by using two methods:

  - Appending a specific curve
  - Rebinding all curves with a new one at the top of the list.

  Prerequisite: Ensure you are using an Enhanced SSL Profile.

  To enable PQC on NetScaler by using CLI

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

1. Add the X25519_MLKEM768 to the current list of elliptic curves that are bound to the SSL profile without removing any existing curves.
At the command prompt, type the following command:

```
bind ssl profile <name> -eccCurveName X25519_MLKEM768
```

Example:

```
bind ssl profile p1 -eccCurveName X25519_MLKEM768
```

2. Rebind all available elliptic curves to an SSL profile and prioritize X25519_MLKEM768 (the Hybrid PQC curve) at the top of the list
At the command prompt, type the following command:

```
bind ssl profile <name> -eccCurveName ALL
```

Example:

```
bind ssl profile p1 -eccCurveName ALL
```

To enable PQC on NetScaler by using GUI

1. Navigate to **Traffic Management > SSL > SSL Profiles.**
2. Select the **SSL Profile** and click **Edit.**
3. In the **SSL Profile** page, navigate to **Advanced Settings, select ECC Curve.**
4. In the **ECC Curve Binding** page, select either **All** or **X25519_MLKEM768**.
5. Click **Bind**.

For more information, see https://docs.netscaler.com/en-us/citrix-adc/current-release/ssl/hybrid-pqc.

Module - *SSL*

- **Build 51.80 | CTXENG-65935**

  Support for TLS 1.3 in zero touch certificate management

  Previously, if any client initiated a TLS 1.3 handshake, and the virtual server was in Zero Touch Certificate Management mode, NetScaler would default to using TLS 1.2.

  NetScaler now supports the TLS 1.3 feature for Zero Touch Certificate Management. This enhancement ensures your connections are always established with the highest possible security and improved performance, leading to reduced application response times.

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

Note: By default, the TLS 1.3 feature is disabled. To enable it, see: Support for TLS 1.3 protocol

Module - *SSL*

- **Build 51.80 | CTXENG-67510**

  Support for HTTP and TCP attack detection and logging

  NetScaler now provides comprehensive logging capabilities for HTTP and TCP attack events and non-RFC compliant traffic. This feature enhances security monitoring by providing detailed visibility into dropped packets and security violations.

  Previously, Layer 4 to Layer 7 packets dropped due to security violations or RFC non-compliance were only tracked through 'newnslog' counters. These counters provide limited visibility into violation details and no information about affected clients and services.

  The new logging functionality enables administrators to identify malicious traffic sources with complete connection details and monitor RFC compliance violations for troubleshooting and security purposes. Also, administrators can track attack patterns with contextual information for forensic analysis and configure flexible logging levels to filter events based on severity requirements.

  Configure audit log (Syslog and Nslog) with HTTP and TCP attack logging by using the CLI

  To implement the HTTP and TCP attack detection and logging feature, a new '-protocolViolations' parameter is added to audit log related commands. This parameter enables logging of protocol violations and attack events for specified protocols. The '-protocolViolations' parameter currently supports the following values:

  - **ALL:** Enables logging for all supported protocol violations and attacks
  - **NONE:** Disables protocol violation logging (default value).

  The '-protocolViolations' parameter is available in the following audit log configuration commands:

```
1 set syslogparams [-protocolViolations <protocol> ...]
2 add audit syslogAction <name> <syslog server IP> <loglevel> [-
     protocolViolations <protocol> ...]
3 set nslogparams [-protocolViolations <protocol> ...]
4 add audit nslogAction <name> <nslog server IP> <loglevel> [-
     protocolViolations <protocol> ...]
```

  Configure audit log (Syslog and Nslog) with HTTP and TCP attack logging by using the GUI

  1. Navigate to **Configuration > System > Auditing > Syslog or Nslog**.
  2. Select the **Servers** tab.

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

3. Click **Add**.
4. In the **Create Auditing Server** page, populate the relevant fields.
5. Select the **Protocol Violations** check box.
6. Click **Create**.

For more information, see HTTP and TCP attack detection and logging.

Module - *System*

- **Build 51.80 | CTXENG-66431**

  URL Categorization removal from NetScaler URL Filtering

  The NetScaler **URL Filtering** feature no longer includes **URL Categorization**.

  Module - *System*

- **Build 51.80 | CTXENG-65956**

  Support for HTTP and TCP attack detection and logging

  NetScaler now provides comprehensive logging capabilities for HTTP and TCP attack events and non-RFC compliant traffic. This feature enhances security monitoring by providing detailed visibility into dropped packets and security violations.

  Previously, Layer 4 to Layer 7 packets dropped due to security violations or RFC non-compliance were only tracked through ‘newnslog‘ counters. These counters provide limited visibility into violation details and no information about affected clients and services.

  The new logging functionality enables administrators to identify malicious traffic sources with complete connection details and monitor RFC compliance violations for troubleshooting and security purposes. Also, administrators can track attack patterns with contextual information for forensic analysis and configure flexible logging levels to filter events based on severity requirements.

  Configure audit log (Syslog and Nslog) with HTTP and TCP attack logging by using the CLI

  To implement the HTTP and TCP attack detection and logging feature, a new ‘-protocolViolations‘ parameter is added to audit log related commands. This parameter enables logging of protocol

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

violations and attack events for specified protocols. The '-protocolViolations' parameter currently supports the following values:

- **ALL:** Enables logging for all supported protocol violations and attacks
- **NONE:** Disables protocol violation logging (default value).

The '-protocolViolations' parameter is available in the following audit log configuration commands:

```
set syslogparams [-protocolViolations <protocol> ...]
add audit syslogAction <name> <syslog server IP> <loglevel> [-
   protocolViolations <protocol> ...]
set nslogparams [-protocolViolations <protocol> ...]
add audit nslogAction <name> <nslog server IP> <loglevel> [-
   protocolViolations <protocol> ...]
```

Configure audit log (Syslog and Nslog) with HTTP and TCP attack logging by using the GUI

1. Navigate to **Configuration > System > Auditing > Syslog or Nslog**.
2. Select the **Servers** tab.
3. Click **Add**.
4. In the **Create Auditing Server** page, populate the relevant fields.
5. Select the **Protocol Violations** check box.
6. Click **Create**.

For more information, see [Will add doc link here].

Module - *System*

- **Build 51.80 | CTXENG-69948**

  Support for additional NetScaler Fixed-term Bandwidth license codes to enable transition to LAS-based licensing

  NetScaler now supports additional NetScaler Fixed-term Bandwidth license entitlements (license codes). This allows customer with NetScaler Perpetual license to transition from file-based licensing to LAS-based licensing using NetScaler Fixed-term Bandwidth license. It also enables existing NetScaler Fixed-term Bandwidth license customer to transition from file-based licensing to LAS-based licensing.

  To use LAS, your NetScaler must be running one of the following minimum versions or later:

  - NetScaler ADC: 14.1 build 51.80, 13.1 build 60.29, 13.1 build 37.247 (FIPS)
  - NetScaler SVM: 14.1 build 51.83, 13.1 build 60.30

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

Module - *User Interface*

- **Build 51.80 | CTXENG-69332**

  LAS support for NetScaler deployments for NetScaler Fixed-term Bandwidth license

  NetScaler now supports the License Activation Service (LAS) licensing mechanism. LAS is a new cloud-based licensing solution that offers a modern alternative to traditional file-based licensing. LAS introduces new modules for the activation of Citrix and NetScaler products, ensuring a seamless and modern approach to license management.

  Starting from this release, LAS is supported on the following NetScaler deployments:

  - **NetScaler ADC:** 14.1 build 51.80, 13.1 build 60.29, 13.1 build 37.247 (FIPS) or later
  - **NetScaler SVM:** 14.1 build 51.83, 13.1 build 60.30 or later

  Note:

  LAS for NetScaler deployments supports NetScaler Fixed-term Bandwidth licenses. All other forms of legacy NetScaler licenses, such as perpetual licenses, are not supported with LAS.

  For more information, see License Activation Service.

  Module - *User Interface*

- **Build 51.80 | CTXENG-68622**

  LAS Enforcement on NetScaler, NetScaler Console on-prem, and NetScaler Console Service

  File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version. The minimum required NetScaler versions that are LAS compatible are:

  - NetScaler ADCs : 14.1 -51.80, 13.1-60.29, 13.1-37.247 (FIPS)
  - NetScaler SVM: 14.1-51.83, 13.1-60.30
  - NetScaler Console Service: Supported from early September 2025.
  - NetScaler Console on-prem: 14.1-51.83

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

Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing deprecation/EOL is from Console on-prem release 14.1-51.83 onwards and Console on-prem release 13.1-60.26 onwards.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.

LAS based licenses may not be available to customers where prohibited by law or regulations.

Should you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Module - ***User Interface***

- **Build 51.80 | CTXENG-68347**

  Deprecation of NetScaler Reporting tool

  The Reporting tool is now deprecated on the following platforms:

  - NetScaler BLX
  - NetScaler CPX
  - NetScaler VPX on Nutanix

  Key changes in reporting capabilities
  Starting with NetScaler release 14.1 build 51.x, some changes are implemented to NetScaler reporting capabilities across multiple form factors and platforms.

  - **GUI changes:**
    The **Reporting** tab in the NetScaler GUI is removed from BLX and VPX on Nutanix platforms.
  - **CLI and API changes:**
    All reporting-related CLI commands are hidden across all NetScaler form factors and platforms. Consequently, these commands no longer appear in Man pages or be accessible through the NetScaler SDKs.
    Important: If you are using the NetScaler SDK with Reporting API commands, your automation scripts might be affected after upgrading to the NetScaler release 14.1 build 51.x.
  - **Backend process changes:**
    The reporting backend process (nscollect) is disabled by default on BLX, CPX, and VPX on Nutanix platforms.

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

Recommended alternatives

To help you continue monitoring and analyzing your systems, we recommend using the following supported alternatives:

- Export metrics from NetScaler to third-party observability tools, such as Prometheus and Splunk. For detailed information, refer to the Observability documentation.
- Use the Network Reporting feature on NetScaler Console. This feature currently supports limited counters. For more information, refer to the Network Reporting on NetScaler Console documentation.

Module - *User Interface*

- **Build 51.80 | CTXENG-68283**

  Perpetual Licensing changes - SA Date enforcement and NetScaler build-specific Burn-In Date

  Starting from this release, there are some changes related to Perpetual licensing that includes SA Date enforcement and NetScaler build-specific Burn-In Date.

  Terminology description:

  - **Subscription Advantage (SA) date:** A date present in perpetual license files, introduced to limit upgrades to NetScaler versions released only up to a certain date.
  - **Burn-In Date (BID):** A date associated with every NetScaler version and build.

  The following changes are introduced in Perpetual licensing:

  Change 1: SA Date check and enforcement:

  This check and enforcement is introduced to block NetScaler customers who are running their NetScaler instances on perpetual licenses with expired maintenance, resulting in unsupported deployments.

  If the Burn-In Date of the NetScaler build you are trying to upgrade to is later than the SA date in the perpetual license file used on your NetScaler instance, your NetScaler instance becomes unlicensed after the upgrade. Some NetScaler VPX versions already had this check and enforcement. It is now introduced for NetScaler form-factors: VPX, MPX, and SDX starting from the following NetScaler releases:

  - NetScaler ADCs: 14.1 51.x, 13.1-60.x, 13.1-37.x (FIPS)
  - NetScaler SVM: 14.1 51.x, 13.1-60.x

  This check occurs during boot up after a NetScaler upgrade. To avoid your NetScaler instance becoming unlicensed, obtain a supported NetScaler license with active maintenance.

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

Note: If you are using a perpetual license on your NetScaler instance and have active maintenance, you must use the latest file that you received during your most recent maintenance renewal. Otherwise, your NetScaler becomes unlicensed after upgrading to the above mentioned NetScaler builds.

Change 2: Burn-In Date specific to each build:

Earlier, the Burn-In Date for all builds across a major NetScaler version used to be the same. Now, each unique NetScaler build has its own Burn-In Date (approximately based on its release date) starting from the following NetScaler releases:

- NetScaler ADCs: 14.1-51.x, 13.1 60.x, 13.1 37.x (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1 60.x

Module - *User Interface*

- **Build 51.80 | CTXENG-68033**

  Enforce password rotation and password history for local accounts

  NetScaler now includes improved password security features for local user accounts.

  This feature allows administrators to:

  - Force users to change their passwords regularly
  - Remember previous passwords to prevent users from reusing old ones
  - Set how often passwords must be changed

  These features help keep user accounts more secure by ensuring passwords stay fresh and can't be reused. This helps organizations meet security standards and prevents problems from weak or old passwords.

  Configure password rotation and history for local accounts

  This feature is enabled by setting the ‘passwordhistorycontrol‘ parameter in system settings. Upon activation, the system applies default values for the following options:

  - **Daystoexpire**: 30 (Number of days before the password expires)
  - **Warnpriorndays**: 5 (Number of days prior to password expiration when users are warned)
  - **pwdhistoryCount**: 6 (Number of passwords retained in the history)

  ‘Daystoexpire‘ and ‘Warnpriorndays‘ can be adjusted for system groups when ‘passwordhistorycontrol‘ is enabled. Once enabled, ‘Daystoexpire‘, ‘Warnpriorndays‘, and ‘pwdhistoryCount‘ in system parameters cannot be unset. These values cannot be modified if ‘passwordhistorycontrol‘ is disabled.

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

Points to note:

- Saving the configuration is required after enabling passwordhistorycontrol to initiate password history recording for each partition.
- New passwords must also be saved.

Warning: Saving the configuration while ‘passwordhistorycontrol‘ is disabled, permanently erases all previous user password history.

Limitation

The ‘passwordhistorycontrol‘ option is not supported when NetScaler is configured with multi-factor authentication (MFA). If enabled alongside MFA, when attempting to log in with multi-factor authentication, if a local system user password has expired and shares the same username as external user, the CLI will return the error ”Session Expired or killed. Please login again.” during login. This specific issue does not manifest when logging in through the GUI. It is recommended to disable the Password History Control feature when multi-factor authentication is configured on NetScaler.

For more information, see Enforce password rotation and password history for local accounts.

Module - *User Interface*

Fixed Issues

- **Build 51.80 | NSHELP-39208**

  The HTTP2 packet is corrupted when the connection chain ID is added to the packet, and both of the following conditions are met:

  - Connection chaining is enabled on AppFlow.
  - HTTP2 is in action.

  Module - *Analytics Infrastructure*

- **Build 51.80 | NSHELP-39713**

  When a high number of entities are configured, stats responses for entity name requests might miss some entity names.

  Module - *Analytics Infrastructure*

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

- **Build 51.80 | NSAUTH-16503**

  In an HA deployment, users must re-login to the Advanced Authentication and Authorization - Traffic Management (AAA-TM) virtual server or the NetScaler Gateway virtual server after both nodes are upgraded to the latest version.
  In a cluster deployment, users might encounter authentication failures or repeated re-authentication prompts until all nodes are upgraded to the latest version.

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

- **Build 51.80 | NSAUTH-16527**

  The user is not locked out of NetScaler after multiple invalid login attempts. This happens when **persistentLoginAttempts** is set to **DISABLED** in **set aaa parameter**.

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

- **Build 51.80 | NSHELP-39518**

  The syslog audit data sent from NetScaler includes the bearer token in the authorization header.

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

- **Build 51.80 | NSHELP-39847**

  In an nFactor authentication scenario, a temporary account lockout might occur, preventing legitimate users from logging in to NetScaler. This issue arises only when both of the following conditions are met:

  - maxLoginAttempts value is configured in nFactor authentication and the user name 'Anonymous' is entered repeatedly, exceeding the configured maxLoginAttempts value.
  - A passwordless factor precedes any password-based mechanism in the nFactor authentication configuration.

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

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

- **Build 51.80 | NSHELP-40004**

  NetScaler crashes during certificate-based authentication due to a missing or invalid session context. The issue occurs because the session context is not properly saved during the authentication process, causing errors in the asynchronous tasks.

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

- **Build 51.80 | NSHELP-40086**

  NetScaler might crash when configured as an OAuth Relying Party (RP).

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

- **Build 51.80 | NSHELP-39662**

  In rare cases, a memory leak might occur on the device when the bot trap feature is enabled on a bot profile.

  Module - ***Bot Management***

- **Build 51.80 | NSHELP-40441**

  In NetScaler release 14.1 build 47.x, you might not be able to add a proxy server IP address in the Bot Management settings. Although both the GUI and CLI commands appear to run successfully, the configuration is not applied or saved.

  Module - ***Bot Management***

- **Build 51.80 | NSHELP-39933**

  NetScaler might crash when attempting to remove DNS records corresponding to a DNS zone configured in proxy mode.

  Module - ***Load Balancing***

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

- **Build 51.80 | NSHELP-40036**

  NetScaler might crash when traffic reaches a GSLB virtual server and the following conditions are met:

  - The GSLB virtual server is initially bound to a GSLB service group without a priority order.
  - Later a priority order is configured by using the set command.

  Module - *Load Balancing*

- **Build 51.80 | NSHELP-42361**

  NetScaler might crash when attempting to remove DNS records corresponding to a DNS zone configured in proxy mode.

  Module - *Load Balancing*

- **Build 51.80 | NSHELP-42438**

  NetScaler might crash when attempting to remove DNS records corresponding to a DNS zone configured in proxy mode.

  Module - *Load Balancing*

- **Build 51.80 | NSHELP-39114**

  GSLB load balancing with least connection method might fail, causing traffic to be directed to a single site rather than being distributed across multiple locations. This issue is caused due to an incorrect ”Current Server Connections” count on the content switching virtual server.

  Module - *NetScaler Gateway*

- **Build 51.80 | NSHELP-39410**

  NetScaler Gateway does not support user names starting with special characters.

  Module - *NetScaler Gateway*

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

- **Build 51.80 | NSHELP-39721**

  The primary node crashes when a null client connection is accessed prematurely while processing the refresh STA ticket request's response in the ICA protocol workflow. The crash occurs as the client connection is accessed before it is assigned a value.

  Module - *NetScaler Gateway*

- **Build 51.80 | NSHELP-39593**

  The Link Aggregation Control Protocol (LACP) information is missing in the Management Service user interface under the **Systems > Channels > LACP** section after the upgrade to NetScaler SDX version 14.1 build 38.x.

  Module - *NetScaler SDX Appliance*

- **Build 51.80 | NSHELP-39826**

  SNMP alerts for NetScaler SDX interface state from **Up** to **Down** are not triggered and received in NetScaler Console.

  Module - *NetScaler SDX Appliance*

- **Build 51.80 | NSHELP-39931**

  NetScaler VPX bandwidth is incorrectly set to the minimum range after bandwidth checkout operations. This issue occurs when burst mode is enabled and the SDX Management Service is not rebooted following the bandwidth checkout process.

  Module - *NetScaler SDX Appliance*

- **Build 51.80 | NSSVM-6518**

  The ”Allow Basic Authentication” option is now disabled by default. In previous releases, this option was enabled by default.

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

Module - *NetScaler SDX Appliance*

- **Build 51.80 | NSHELP-39103**

  NetScaler might fail to remove rules from the Learned Rules list, resulting in a ”Resource already exists” error when attempting to add new rules. This issue occurs when the length of form fields in HTTP requests exceeds 128 characters.

  Module - *NetScaler Web App Firewall*

- **Build 51.80 | NSHELP-40137**

  The Auto_update_signature process on a secondary NetScaler might fail to delete temporary directories (located at /tmp/appfwXXXXX) when encountering errors during temporary file creation. However, this process functions correctly on the primary NetScaler. This issue occurs due to insufficient disk space in the /tmp partition.

  Module - *NetScaler Web App Firewall*

- **Build 51.80 | NSHELP-38815**

  NetScaler VPX instances on SDX might experience repeated crashes, specifically related to i40e Fortville interfaces, following Virtual Function (VF) reset failures.

  Module - *Platform*

- **Build 51.80 | NSHELP-39790**

  In some RPM-based Linux distributions, the Nitro API might fail because the ping feature does not work.

  Module - *Platform*

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

- **Build 51.80 | NSHELP-39964**

  NetScaler VPX instances using AWS Elastic Network Adapter (ENA) interfaces are incorrectly reporting Cyclic Redundancy Check (CRC) errors for certain rare packet types, resulting in legitimate packets being dropped.

  Module - *Platform*

- **Build 51.80 | NSHELP-39977**

  On certain platforms, NetScaler BLX does not boot up normally after a reboot due to an issue with the IPv6 MTU configuration setting, which is now rectified.

  Module - *Platform*

- **Build 51.80 | NSHELP-40079**

  On NetScaler BLX version 14.1 build 38.x, files stored within the ‘/flash‘ directory are unexpectedly removed after a system reboot. This issue results in a critical loss of data persistence for files stored in the ‘/flash‘ directory across reboots, causing operational disruptions.

  Module - *Platform*

- **Build 51.80 | NSHELP-40367**

  On NetScaler SDX running Single Bundle Image (SBI) with i40e driver 2.19, users see errors when attempting to add more than 35 partition MAC addresses to the NetScaler VPX.
  The NetScaler VPX console displays the following message:

  ```
  ixlv: WARNING: Error adding VF mac filter!
  ```

  The ”Dom0/var/log/kern.log” records show the following message:

  ”Cannot add more MAC addresses, trusted VF exhausted its resources”.

  This condition does not impact the actual traffic related to the MAC addresses.

  Module - *Platform*

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

- **Build 51.80 | NSLINUX-7882**

  Enumeration fails when StoreFront is configured behind a load balancing server in NetScaler BLX.

  Module - *Platform*

- **Build 51.80 | NSLINUX-8109**

  When adding a new load balancing user monitor, NetScaler accepts a custom dispatcher IP during configuration. However, it always displays the default dispatcher IP address (192.0.0.2) in the monitor details, regardless of which IP address is actually configured.

  Module - *Platform*

- **Build 51.80 | NSLINUX-8933**

  NetScaler HA setup using NSIPv6 might not function correctly in NetScaler VPX instances on Nutanix-AHV hypervisor.

  Module - *Platform*

- **Build 51.80 | NSPLAT-32187**

  When the additional management CPU is not enabled in NetScaler, the syncer kernel thread might enter a tight loop, resulting in high CPU usage. You can monitor the processes consuming resources by running the `top` command-line tool.

  Module - *Platform*

- **Build 51.80 | NSPLAT-33590**

  NetScaler VPX instances running on Microsoft Azure might experience SSH and TCP session failures. This issue can occur randomly after a VPX reboot or upgrade and is caused due to changes in Azure hypervisor layer.

  Module - *Platform*

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

- **Build 51.80 | NSHELP-39762**

  NetScaler might crash when variable configuration is used in a non-default partition.

  Module - *Policies*

- **Build 51.80 | NSHELP-38195**

  Incoming requests to the external HSM might temporarily fail, when the SafeNet Gateway restarts. This issues occurs in one of the following conditions:

  - A processing thread within the gateway becomes unresponsive.
  - A thread remains busy for an extended period, preventing normal operation.

  Module - *SSL*

- **Build 51.80 | NSHELP-39578**

  An HTTP-ECV health monitor might fail to get a valid response from the backend server. This issue occurs when TLS 1.3 is disabled in the enhanced profile, but enabled on the backend server.

  Module - *SSL*

- **Build 51.80 | NSHELP-40135**

  When using the SSL configuration converter tool, duplicate SSL profiles might be created for the virtual server-based acceleration with a wildcard IP address, resulting in redundant configurations between the SSL virtual server and the virtual server-based acceleration.

  Module - *SSL*

- **Build 51.80 | NSHELP-40150**

  The Primary node and secondary node might crash and generate core dumps when a forced failover is initiated.

  Module - *SSL*

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

- **Build 51.80 | NSHELP-39365, NSHELP-40205**

  A false alarm with an error message related to configuration quality assurance parameters (CQA-PARAM) failure is seen in both high availability and standalone setups. This fix eliminates the false alarm; no workaround is needed.

  Module - *System*

- **Build 51.80 | NSHELP-39515**

  NetScaler might crash when the AppFlow client-side measurements are enabled with the Rewrite feature.

  Module - *System*

- **Build 51.80 | NSHELP-39535**

  The HTTP/2 connections incorrectly reset if individual headers exceed a fixed 16 KB limit, ignoring the configured ‘`maxHeaderFieldLen`` setting in the HTTP profile.

  Module - *System*

- **Build 51.80 | NSHELP-39587**

  NetScaler Web Logging (NSWL) shows inconsistency in logging client username. It only logs the actual username when the username length is greater than zero, but logs a double space (””) when the username field is empty.

  Module - *System*

- **Build 51.80 | NSHELP-39857**

  If you try to specify a CA certificate for the import URL while configuring an HTML page import for a responder action, the following error message might appear:

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

”certificate file is missing.”

Module - *User Interface*

- **Build 51.80 | NSHELP-39989**

  SSH login to the NetScaler might fail when multiple streams or channels attempt to authenticate using the same SSH connection concurrently.

  Module - *User Interface*

- **Build 51.80 | NSHELP-40201**

  Creating and restoring backup files fail with a ”Cannot allocate memory” error because some files are removed from NetScaler.

  Module - *User Interface*

- **Build 51.80 | NSHELP-40373**

  An error might occur when binding profiles to a load balancing virtual server if you are logged into a non-default partition.

  Module - *User Interface*

- **Build 51.80 | NSHELP-40396**

  Users might see an error message when creating a syslog server with transport types other than HTTP.

  Module - *User Interface*

- **Build 51.80 | NSHELP-40405**

  SSL certificates and related SSL menus might not appear in the GUI on a NetScaler MPX 14030 appliance running firmware version 14.1-43.50.

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

Module - *User Interface*

- **Build 51.80 | NSHELP-40526**

  Multi-factor authentication fails in NetScaler, with the following error message, after users enter the second-factor password. This issue occurs due to a session validation error during the authentication process.

  ”invalid username or password”

  Module - *User Interface*

- **Build 51.80 | NSUI-22054**

  On a NetScaler VPX running on the Linux platform, the **Tech Support** dialog box stops responding at ”Running CLI commands...” after clicking **Generate Tech Support**. This prevents the generation or download of the tech support bundle.

  Module - *User Interface*

Known Issues

- **Build 51.80 | NSHELP-38696**

  If Appflow (Logstream) is active, the ‘newnslogs‘ file might experience frequent rollovers, leading to partial dumps and loss of performance data.

  Module - *Analytics Infrastructure*

- **Build 51.80 | NSAUTH-2147** The Configure Authentication LDAP Server page on the NetScaler GUI becomes unresponsive if you pursue the following steps:

  - The Test LDAP Reachability option is opened.
  - Invalid login credentials are populated and submitted.
  - Valid login credentials are populated and submitted.

  Workaround: Close and open the Test LDAP Reachability option.

  Module - *Authentication, authorization, and auditing*

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

- **Build 51.80 | NSAUTH-5916**

  ADFS proxy profile can be configured in a cluster deployment. The status for a proxy profile is incorrectly displayed as blank upon issuing the following command.
  ‘show adfsproxyprofile <profile name>‘

  Workaround: Connect to the primary active NetScaler in the cluster and run the ‘show adfsproxyprofile <profile name>‘ command. It would display the proxy profile status.

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

- **Build 51.80 | 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 51.80 | NSHELP-40311**

  The 'show serviceGroup <svcg_name>' command output displays incorrect response time units.

  Module - ***Load Balancing***

- **Build 51.80 | 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***

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

- **Build 51.80 | NSHELP-40690**

  NetScaler might crash when an invalid memory access occurs. This issue occurs when NetScaler receives a DNS response with a non-standard opcode.

  Module - *Load Balancing*

- **Build 51.80 | 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*

- **Build 51.80 | NSHELP-40748**

  NetScaler might crash when the following conditions are met:

  - An OCSP responder is configured with DNS recursion enabled.
  - No name servers are available for the DNS lookup.

  Module - *Load Balancing*

- **Build 51.80 | NSLB-7679**

  In a high-availability setup, subscriber sessions of the primary node might not be synchronized to the secondary node. This is a rare case.

  Module - *Load Balancing*

- **Build 51.80 | CGOP-11830** An error message appears when you add or edit a session policy from the NetScaler GUI.

  Module - *NetScaler Gateway*

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

- **Build 51.80 | NSHELP-40687**

  Enterprise bookmark launches using Clientless VPN on NetScaler Gateway fails due to incorrect decoding of URL fragment identifiers.

  Module - *NetScaler Gateway*

- **Build 51.80 | 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 51.80 | NSHELP-40503**

  A crypto device error alert might be generated due to occasional communication errors from domain zero (Dom-0).

  Module - *NetScaler SDX Appliance*

- **Build 51.80 | 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*

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

- **Build 51.80 | NSSVM-7079**

  For the Fixed Capacity subscription license type, the NetScaler SDX Management Service GUI displays the activation blob renewal date information. However, it does not alert or send proactive notifications about the activation blob expiry. Customers are advised to monitor the activation blob expiry date displayed in the GUI and renew the blob before it expires to ensure uninterrupted functioning of the product.

  Module - ***NetScaler SDX Appliance***

- **Build 51.80 | NSSVM-7409**

  When NetScaler SDX is configured to use Console-based licensing (for example, Pooled Bandwidth or Flexed), and legacy file-based license files are still present locally on the SVM, SDX becomes unlicensed when any such local license expires. As a result, both the SVM and all NetScaler VPX instances on SDX become unlicensed.

  Workaround:

  Delete local file-based `.lic` licenses from the SVM, except zero-capacity software licenses, which must not be deleted.

  The local file-based licenses are located in the `/mpsconfig/license` SVM folder and must be deleted from that folder using the shell prompt.

  Module - ***NetScaler SDX Appliance***

- **Build 51.80 | NSSWG-1436**

  URL categorization in the URL Filtering feature is no longer available on NetScaler. Additionally, the FEO feature does not work as intended.

  Module - ***NetScaler Secure Web Gateway***

- **Build 51.80 | NSHELP-40544**

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

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

Module - *NetScaler Web App Firewall*

- **Build 51.80 | NSHELP-40738**

  During Device Under Test (DUT), a false positive is triggered when Signature Rule 1109 is enabled.

  Module - *NetScaler Web App Firewall*

- **Build 51.80 | NSHELP-36236**

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

  Module - *Networking*

- **Build 51.80 | NSNET-33932**

  On NetScaler VPX-Linux deployments, memory allocation errors might occur when you configure route redistribution (connected, RIP, or RIPng routes) on OSPF6. These errors can disrupt the routing functionality.

  Module - *Networking*

- **Build 51.80 | NSHELP-39313**

  NetScaler VPX with Accelerated Networking enabled in Azure might crash when the Azure hosts dynamically detach and reattach SR-IOV NICs.

  Module - *Platform*

- **Build 51.80 | NSHELP-39562**

  NetScaler VPX on XenServer might crash or become unresponsive after a live migration, necessitating a forced reboot to restore functionality.

  Module - *Platform*

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

- **Build 51.80 | 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 51.80 | NSHELP-40519**

  NetScaler GUI might not display the cloud profiles on a VPX instance deployed in Azure, AWS, GCP cloud. This issue occurs when the following conditions are met:

  - The backend returns a failure code 0x413.
  - More than 20 cloud profiles are added.

  Module - *Platform*

- **Build 51.80 | NSLINUX-5**

  Installation of a NetScaler BLX appliance might fail on a Debian based Linux host (Ubuntu version 18 and later) with the following dependency error:

  ”The following packages have unmet dependencies: blx-core-libs:i386 : PreDepends: libc6:i386 (>= 2.19) but it is not installable”

  Workaround: Run the following commands in the Linux host CLI before installing a NetScaler BLX appliance:

  - dpkg --add-architecture i386
  - apt-get update
  - apt-get install libc6:i386

  Module - *Platform*

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

- **Build 51.80 | NSLINUX-64**

  The following interface operations are not supported for Intel ‘X710 10G (i40e)‘ interfaces on a NetScaler BLX appliance with DPDK:

  - Disable
  - Enable
  - Reset

  Module - *Platform*

- **Build 51.80 | NSLINUX-155**

  When you enable NetScaler BLX managed host on Oracle cloud, the gateway configuration of the Linux host is not added to NetScaler BLX.

  Module - *Platform*

- **Build 51.80 | NSLINUX-7437**

  The RDP Proxy functionality is not supported in BLX Gateway.

  Module - *Platform*

- **Build 51.80 | 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*

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

- **Build 51.80 | 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 51.80 | NSLINUX-8831**

  The ‘unset mgmtparam‘ command for the ‘mgmthttpport‘ and ‘mgmthttpsport‘ parameters does not function correctly on the NetScaler VPX on Nutanix hypervisor.

  Workaround: Use the ‘set mgmtparam‘ command to explicitly configure the default port values.

  Examples:
  set mgmtparam -mgmthttpport 80
  set mgmtparam -mgmthttpsport 443

  This workaround restores the management ports to their default values instead of using the unset command.

  Module - *Platform*

- **Build 51.80 | NSPLAT-4520** When you delete an autoscale setting or a VM scale set from an Azure resource group, delete the corresponding cloud profile configuration from the NetScaler instance. Use the ”rm cloudprofile” command to delete the profile.

  Module - *Platform*

- **Build 51.80 | 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*

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

- **Build 51.80 | NSPOLICY-1267** Connections might hang if the size of processing data is more than the configured default TCP buffer size.

  Workaround: Set the TCP buffer size to maximum size of data that needs to be processed.

  Module - *Policies*

- **Build 51.80 | 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 51.80 | NSSSL-3184, NSSSL-1394, NSSSL-1379** An expired session ticket is honored on a non-CCO node and on an HA node after an HA failover.

  Module - *SSL*

- **Build 51.80 | NSSSL-4001** An incorrect warning message, ”Warning: No usable ciphers configured on the SSL vserver/service,” appears if you try to change the SSL protocol or cipher in the SSL profile.

  Module - *SSL*

- **Build 51.80 | NSSSL-4427** Session Key Auto Refresh incorrectly appears as disabled on a cluster IP address. (This option cannot be disabled.)

  Module - *SSL*

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

- **Build 51.80 | NSSSL-6213** You can create multiple Azure Application entities with the same client ID and client secret. The NetScaler appliance does not return an error.

  Module - *SSL*

- **Build 51.80 | NSSSL-6478** You cannot add an Azure Key Vault object if an authentication Azure Key Vault object is already added.

  Module - *SSL*

- **Build 51.80 | NSSSL-9572**

  On a heterogeneous cluster of NetScaler SDX 22000 and NetScaler SDX 26000 appliances, there is a config loss of SSL entities if the SDX 26000 appliance is restarted.

  Workaround:

  1. On the CLIP, disable SSLv3 on all the existing and new SSL entities, such as virtual server, service, service group, and internal services. For example, 'set ssl vserver <name> -SSL3 DISABLED'.
  2. Save the configuration.

  Module - *SSL*

- **Build 51.80 | NSBASE-18402**

  ICA sessions might fail within a few minutes of being launched if you use the HTML5 browser and the QUIC transport protocol.
  Workaround: Set the maximum idle timeout value to 3600 seconds when you configure the QUIC profile.

  Module - *System*

- **Build 51.80 | NSHELP-39670**

  With connection multiplexing enabled in transparent mode, NetScaler terminates the client-side connection while keeping the server-side TCP connection active.

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

This issue occurs when the client sends a Selective Acknowledgment (SACK) block that acknowledges both data and the FIN sent by NetScaler, and this SACK block is mapped to server-side sequence numbers. This mapping incorrectly includes the acknowledgment of the Finish (FIN) packet, which was only present on the client connection.

Module - *System*

- **Build 51.80 | NSCONFIG-3188**

  Users might fail to log in to the downgraded NetScaler appliance if the following sequence of conditions is met:

  1. You perform one of the following steps:

     - After upgrading to the current build, you add a system user or change the password of an existing system user, and save the configuration.
     - Provision a new VPX, BLX, or CPX instance with the current build.

  2. Downgrade the appliance to one of the following builds:

     - 13.0-47.x or earlier
     - 12.1-56.x or earlier
     - 11.1-64.x or earlier

  To view the list of users affected after the downgrade, at the command prompt, type:

  ```
  query ns config -changedpassword [-config <full path of the
     configuration file (ns.conf)>]
  ```

  Workaround: Reset the password of the affected users. For more information, see [How to reset root administrator (nsroot) password](https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html).

  *Note: *If you are downgrading a previously upgraded build, then while downgrading use the backed up configuration file (ns.conf) of the earlier build to avoid this issue.

  Module - *User Interface*

- **Build 51.80 | NSCONFIG-8068**

  Users might fail to log in to the downgraded NetScaler appliance if the following sequence of conditions is met:

  1. You perform one of the following steps:

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

- After upgrading to the current build, you add a system user or change the password of an existing system user, and save the configuration.
- Provision a new NetScaler VPX, BLX, or CPX instance with the current build.

2. Downgrade the appliance to one of the following builds:

- 13.1-4.x
- 13.0-82.x or earlier
- 12.1-62.x or earlier

To view the list of users affected after the downgrade, at the command prompt, type:

```
query ns config -changedpassword [-config <full path of the
   configuration file (ns.conf)>]
```

Workaround: Reset the password of the affected users. For more information, see [How to reset root administrator (nsroot) password](https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html).

Note: If you are downgrading a previously upgraded build, then while downgrading use the backed up configuration file (ns.conf) of the earlier build to avoid this issue.

Module - *User Interface*

- **Build 51.80 | NSUI-13024**

  Create/Monitor CloudBridge Connector wizard might become unresponsive or fails to configure a cloudbridge connector.

  Workaround: Configure cloudbridge connectors by adding IPSec profiles, IP tunnels, and PBR rules by using the NetScaler GUI or CLI.

  Module - *User Interface*

- **Build 51.80 | NSUI-14752**

  In NetScaler GUI, the ”Help” link present under the ”Dashboard” tab is broken.

  Module - *User Interface*

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

- **Build 51.80 | 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*

© 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).