NetScaler ADC (includes NetScaler Gateway)

Release Notes for NetScaler ADC (includes NetScaler Gateway) 14.1-72.61

August 13, 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.
- Upgrading NetScaler in an ICA proxy setup to 14.1-72.61 or later drops active sessions attempting to reconnect with pre-upgrade session tickets. Users must restart their sessions. Post-upgrade sessions and reconnections function normally without extra configuration.
- Build 14.1-72.61 replaces Build 14.1-72.57.
- Build 14.1-72.61 includes the following fixes along with the enhancements and fixes available in Build 14.1-72.57: NSBASE-20565, NSHELP-43402, NSUI-22801.
- Build 14.1-72.61 and later builds address the security vulnerabilities described in https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604.

What's New

- **Build 72.61 | CTXENG-72119**

  Support to send all the JSON fields for insights

  You can now export all the JSON fields for insight by enabling the `log_all_json_field` attribute in the NetScaler CPX YAML file. Enabling the `log_all_json_field` attribute overrides the fields mentioned in the individual data format file.

  This feature is useful in deployments like Kubernetes, where editing the data format file or copying an edited file is either not feasible or might not be straightforward.

  Module - ***Analytics Infrastructure***

- **Build 72.61 | CTXENG-72069**

  Support for usage tracking

  NetScaler supports usage tracking, which allows you to track the input and output tokens or requests based on criteria such as team, user, or application. To support this feature, NetScaler expects that the AI application sends the attributes such as the `userid` or `teamid` in the HTTP header (such as `X-user-id` or `X-org-id`). This feature uses processed insights for tracking.

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

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

Module - ***Analytics Infrastructure***

- **Build 72.61 | CTXENG-70765**

  Support for AI gateway in service groups

  NetScaler now supports an AI gateway in service groups. This enhancement allows configuring the backend profile using the `aigwprofile` parameter at the service group level, which can also be specified for individual member bindings at bind time.

  Any service item bound to the service group automatically inherits the backend profile defined at the service group level, provided a specific AI gateway profile is not already assigned during the binding process.

  To configure and bind the service groups while configuring the AI gateway, perform the following:

  Create a service group, one for each deployment. Attach the backend `aigwprofile` to it and bind the members to a service group.

  ```
  add servicegroup  <ServiceGroupName> <Protocol> -aigwProfileName <
      BackendProfileName>bind servicegroup <serviceGroupName> (<IP>@
      | <serverName>) <port>
  ```

  Example 1:

  ```
  add servicegroup AzureAI-SG SSL -aigwprofilename
      azureoai_backend_profile_sgbind servicegroup AzureAI-SG AzureAI
      -1-Svr 443 -aigwprofilename azureoai_backend_profile_1bind
      servicegroup AzureAI-SG AzureAI-2-Svr 443 -aigwprofilename
      azureoai_backend_profile_2
  ```

  Example 2:

  ```
  add servicegroup AzureAI-SG SSL -aigwprofilename
      openai_backend_profilebind servicegroup AzureAI-SG AzureAI-1-
      Svr 443bind servicegroup AzureAI-SG AzureAI-2-Svr 443
  ```

  In the example 2, because the aigwprofilename is not mentioned, it is going to be inherited from the service group that is already binded.

  Bind the model deployment services or service group to the load balancing virtual server.

  ```
  bind lb vserver <LbVserverName> <ServiceGroupName>
  ```

  Example:

  ```
  bind lbvserver AzureOpenAIGpt5.1 AzureAI-SG
  ```

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

For more information on configuring load balancing for AI models, see Configure load balancing for AI models.

Module - *Analytics Infrastructure*

- **Build 72.61 | CTXENG-70764**

  Support for content switching-based model routing for AI gateway traffic

  NetScaler supports content switching-based model routing, which enables the NetScaler AI gateway to send the incoming chat requests from AI agents and applications to different models. This enhancement uses the content switching feature of NetScaler to forward the requests to different AI models. When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. The priority of the policy defines the order in which the policies bound to the content switching virtual server are evaluated.

  For more information, see https:/docs.netscaler.com/en-us/citrix-adc/current-release/ai-gateway%23content-switching-based-model-routing.

  Module - *Analytics Infrastructure*

- **Build 72.61 | CTXENG-70828**

  OTP encryption support in Linux-based NetScaler Gateway environments

  OTP encryption is now supported in Linux-based NetScaler Gateway environments for Native OTP and Push Notification authentication. Previously, user device registration failed when OTP encryption was enabled with either of these authentication.

  Module - *Authentication, authorization, and auditing*

- **Build 72.61 | CTXENG-67602**

  Support OAuth Outbound Call from NetScaler to IDP

  NetScaler authentication can now route outbound OAuth calls to third-party identity providers (IDPs) through a explicitly configured. HTTP/HTTPS forward (web) proxy. This feature includes optional basic proxy-authorization and a customizable bypass list for selected domains or IP addresses.

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

Many enterprise environments restrict direct internet access from the NetScaler data plane, requiring all outbound traffic to traverse a corporate web proxy for security, auditing, and Data Loss Prevention (DLP) compliance. While modern federated authentication workflows (such as OAuth, SAML, and Google reCAPTCHA) require connectivity to external endpoints, NetScaler previously lacked a native mechanism to route these outbound calls through an explicit proxy.

A new global parameter, aaa proxyparam, allows administrators to configure a single explicit forward proxy ($IPv4:\text

{port}

$) for all AAA outbound HTTP/HTTPS traffic.

Note: Only IPv4 proxy addresses are supported in the initial release.

Some of the benefits of using single explicit forward proxy are:

- **Corporate egress compliance:** Aligns with corporate security policies that mandate proxy traversal for all outbound web traffic.
- **Expanded IdP integration:** Enables OAuth-based authentication (e.g., Microsoft Entra ID, Okta, Duo Universal Prompt, Google) and Intune device compliance checks in proxy-only networks.
- **Simplified administration:** A single, global-level configuration applies seamlessly across all OAuth outbound endpoints without impacting the end-user experience.
- **Granular Controls:** Utilizing an integrated NetScaler pattern set (`ns_aaa_proxy_bypasslist`), administrators can exclude specific IdP hostnames, domain suffixes, or IP prefixes from proxy routing.

This feature applies to the NetScaler authentication and authorization module (NetScaler Gateway and AAA-TM authentication virtual servers). It also applies to OAuth RP outbound calls: token, introspect, and userinfo (dynamic endpoints).

Notes:

- **Global scope impact:** The proxy configuration is enforced at the AAA global scope and applies to all OAuth outbound calls system-wide. Plan your rollout strategies accordingly.
- **Bypass list matching logic:** The integrated bypass list uses suffix matching for domain entries (e.g., `idp.aaa.local` matches itself and `sub.idp.aaa.local`) and prefix matching for IP entries (e.g., `192.168.1` matches `192.168.1.0` through `192.168.1.255`).
- **SSL Offload targeting:** When using the HTTPS-to-proxy approach using a load balancing offload setup, the proxy address configured in the `set aaa proxyparam` command must point to the **load balance virtual server IP address:port**, and not to the actual backend proxy.

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

Prerequisites

Ensure that the following prerequisites are met:

- NetScaler version 14.1-72.x or later.
- **DNS Resolution:** Outbound DNS for IdP hostname resolution must function either on the NetScaler appliance or on the forward proxy, depending on your network architecture.
- Reachability from NetScaler SNIP to the explicit proxy IP address :port.
- If Proxy-Authorization is required: the proxy username/password credentials (Basic).
- If HTTPS-to-proxy is required: a load balancing virtual server with an SSL_TCP service bound to the proxy IP address:port.
- NetScaler super user or AAA-config permission to run `set aaa proxyparam` and `bind policy patset ns_aaa_proxy_bypasslist`.

Configure outbound proxy for OAuth calls by using the CLI

1. Configure an HTTP forward proxy at the global level: `set aaa proxyparam -proxy <ip:port> -proxyAuthorization ( disabled | basic )-proxyUsername <string> {-proxyPassword}`

Example (no proxy authentication): `set aaa proxyparam -proxy[REDACTED]`

Example (Basic Proxy-Authorization): `set aaa proxyparam -proxy[REDACTED]-proxyAuthorization basic -proxyUsername proxyuser -proxyPassword <secret>`

1. Verify the configuration: `show aaa parameter`
2. To manage the bypass list (default patset `ns_aaa_proxy_bypasslist`):
   a) Show the current bypass list: show patset ns_aaa_proxy_bypasslist
   b) Bind a policy to the patset, for example, for a domain: `bind policy patset ns_aaa_proxy_bypasslist idp.aaa.local`
   c) Bind a policy to the patset, for example, for an IP prefix: `bind policy patset ns_aaa_proxy_bypasslist 192.168.1`
   d) Unbind a policy from the patset, for example, for a domain: `unbind policy patset ns_aaa_proxy_bypasslist idp.aaa.local`
3. To configure Secure (HTTPS-to-proxy) mode using load balance offload:
   a) Add a service for the OAuth IDP: `add service oauth_idp_service_ssl[REDACTED]SSL_TCP 3128`
   b) Add an load balance virtual server for OAuth: `add lb vserver oauth_lb_vserver_ssl TCP[REDACTED]3128`
   c) Bind the service to the load balance virtual server: `bind lb vserver oauth_lb_vserver_ssl oauth_idp_service_ssl`

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

d) Set the AAA proxy parameter to theload balance virtual server IP and port: `set aaa proxyparam -proxy[REDACTED]`

Configure outbound proxy for OAuth calls by using the GUI

1. Navigate to **Security > AAA - Application Traffic > Authentication > Settings > Change AAA proxy parameter**.
2. Configure **Proxy (IP:port)**, **Proxy Authorization (disabled/basic)**, and the optional **username/password**.
3. Manage the bypass list under **Security > AAA > Patsets > ns_aaa_proxy_bypasslist**.

Related topic

Web proxy support for outbound calls to IdP or third party endpoints

Module - *Authentication, authorization, and auditing*

- **Build 72.61 | CTXENG-71383**

  NetScaler netprofile support for DNS virtual servers

  In network deployments where data and DNS traffic follow separate network paths, maintaining control over the source IP address for DNS resolution is critical for routing and security. NetScaler now supports binding a netprofile to a DNS virtual server when it is configured as a name server. This ensures that the specific IP address defined in the netprofile is honored for outgoing DNS queries, providing greater flexibility in complex network topologies.

  Module - *Load Balancing*

- **Build 72.61 | CTXENG-71382**

  Support for DNS SVCB and HTTPS resource records

  NetScaler DNS now supports SVCB and HTTPS resource records as defined in RFC 9460. These records allow clients, such as modern browsers, to obtain service binding details directly from DNS responses. This feature reduces connection setup latency, improves performance, and enables faster adoption of secure protocols such as HTTPS and HTTP/2.

  Some of the benefits are:

  - Reduced connection latency
  - Improved performance for HTTP-based applications
  - Native support for modern DNS standards

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

Prerequisites

Before you begin, ensure that your environment meets the following requirements:

- **NetScaler Version:** 14.1 Build 72.x or later.
- **DNSSEC (Optional):** Configured and enabled if your specific use cases require DNSSEC.

Configure SVCB and HTTPS Records by using CLI

1. Add an SVCB record.

add dns svcbRec <domain> -priority <value> -targetName <target-domain> -svcbType SVCB

1. Add an HTTPS record.

add dns svcbRec <domain> -priority <value> -targetName <target-domain> -svcbType HTTPS -alpn h2 -port 443

1. View configured records.

show dns svcbRec

show dns svcbRec -svcbType HTTPS

Configure SVCB and HTTPS Records by using GUI

1. Navigate to **Traffic Management > DNS > Records > SVCB Records.**
2. Enter the details and click **Ok**.

Limitations

- **Custom parameters**: Custom SVCB parameter sets (svcbParamSet) are not supported. Only standard parameters defined in RFC 9460 are supported.
- **Unsupported RFC parameters:** Parameters defined in RFCs later than RFC 9460 are not supported, including:
  - dohpath
  - ohttp
  - tls-supported-groups
  - docpath
- **DNS answer logging:** DNS answer logging includes only the priority and target name. Service parameters are not logged.

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

Usage Guidelines

- HTTPS records: HTTPS records are a specialized form of SVCB records and utilize the same configuration model.
- Record prioritization: You can configure multiple SVCB or HTTPS records per domain by assigning priority values. The NetScaler appliance prefers endpoints with lower priority values.

Module - *Load Balancing*

- **Build 72.61 | CTXENG-70985**

  MCP gateway enhancements

  NetScaler now supports MCP-aware capabilities to enable secure, reliable, and governed access to backend Model Context Protocol (MCP) servers.

  - **MCP gateway proxy:** Provides a single entry point for MCP clients with dynamic routing to multiple backend MCP servers.
  - **Session persistence:** Ensures requests belonging to the same MCP session route to the same backend server, enabling reliable multi-step operations.
  - **Protocol-aware monitoring:** Adds MCP-specific health checks with multi-stage validation to ensure backend servers remain functionally healthy.
  - **Authentication support:** Supports multiple authentication models, including per-user and global tokens, OAuth-based access, and hybrid authentication flows.
  - **Tool-based rate limiting:** Enables fine-grained rate limiting based on MCP tool usage and user identity to prevent backend overload and abuse.
  - **Server access control:** Introduces allow listing and block listing to restrict access to approved MCP servers and block unauthorized endpoints.

  These capabilities provide centralized control, improved reliability, and enhanced security for MCP-based deployments.

  Module - *Load Balancing*

- **Build 72.61 | CTXENG-71938**

  NetScaler VPX support for AWS EC2 M7i and M8i instance families

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

NetScaler VPX now supports deployment on AWS EC2 M7i and M8i instance families, enabling customers to run VPX workloads on newer-generation infrastructure with improved scalability and performance characteristics.

Related topic

AWS-VPX support matrix

Module - *Miscellaneous*

- **Build 72.61 | CTXENG-71218**

  Default WAF protection for PORTAL endpoints

  Starting from release 14.1-72.61, when the WAF protection parameter is set to Default, PORTAL endpoints are also protected in addition to AUTH and VPN endpoints. Previously, the Default setting protected only AUTH and VPN endpoints.

  Module - *Miscellaneous*

- **Build 72.61 | CTXENG-70901**

  New period parameter added for time-window log collection

  NetScaler technical support bundle introduces functional improvements that make STS diagnostic collection more accurate and efficient by collecting the most relevant data within the existing scope and intent. As part of this enhancement, a new `-period` parameter is introduced and is valid only when `-time` parameter is specified, enabling a defined time window around the given time for log collection. This time-windowed collection applies to newnslog, text logs, and non-PE core files.

  To configure by using CLI

  At the command prompt, type:

  ```
  show techsupport -time <HH:MM_MMDDYYYY>  -period <
     time_window_in_hours>
  ```

  To configure by using the GUI

  1. Navigate to **Configuration > System > Diagnostics**.
  2. In the **Technical Support Tools** section, click **Generate support file**.

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

3. On the **Tech Support** page, select **Custom** if you want NetScaler to pick the corresponding logs at the given time.
   When **Custom** is selected, **Period** appears.
4. In **Period**, enter the duration in hours.
5. Click **Run**.

Module - *Miscellaneous*

- **Build 72.61 | CTXENG-67209**

  EDT support for Network Telemetry

  Network Telemetry feature now supports EDT connections. HDX Insight data for Secure HDX connections are now supported for EDT connections. For configuration details, see: Configure NetScaler Gateway to support HDX Insight.

  Module - *Miscellaneous*

- **Build 72.61 | CTXENG-70868**

  Secure Management support for VPX on Linux platforms

  NetScaler now extends the Secure Management feature to VPX on Linux platforms, addressing customer concerns about potential exposure of the management IP to load-balancing traffic. This enhancement enforces strict separation between management and data planes by creating dedicated routing tables for each plane, so management traffic remains isolated from application data traffic.

  With this enhancement, administrators can explicitly control whether specific traffic uses the management plane or the data plane through configurable overrides. This improves security posture, reduces the risk of unauthorized access to management functions, and provides greater operational flexibility for platform-specific traffic handling.

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

  Module - *Networking*

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

- **Build 72.61 | CTXENG-70490**

  Configure hold time for management CPU SNMP alerts

  You can now configure a `holdTime` parameter for the MGMT-CPU-USAGE SNMP alarm using the `set snmp alarm` command. This enhancement allows you to specify the interval, in seconds, at which NetScaler generates SNMP trap messages when the conditions defined in the SNMP alarm are met continuously over a given period of time.

  This parameter helps you to:

  - Prevent excessive alerts from transient management CPU spikes.
  - Configure precise monitoring for management CPU usage.

  Module - *Networking*

- **Build 72.61 | CTXENG-72942**

  Custom metrics for NetScaler CPX

  You can provide custom metrics configuration JSON files to a NetScaler CPX instance in Kubernetes using ConfigMaps. This allows you to add custom metrics schema files without overwriting the default metrics configuration files (`schema.json` and `reference_schema.json`) that ship with CPX.

  During startup, the NetScaler CPX instance places the default metrics configuration files in the `/var/metrics_conf` directory. If you mount a ConfigMap at `/cpx/custom_metrics_conf`, CPX validates each JSON file and copies the valid files into `/var/metrics_conf` alongside the defaults.

  Notes:

  - Custom JSON files must contain valid JSON. Invalid files are skipped during startup, and an error is logged in `boot.log`.
  - Default files (`schema.json`, `reference_schema.json`) are always placed first.
  - Custom files with the same name as a default file override the default file.

  Configure custom metrics

  You can configure custom metrics for NetScaler CPX by creating a ConfigMap and deploying the NetScaler CPX instance with the ConfigMap mounted.

  To configure by using CLI

  1. Create the custom metrics configuration JSON files that you want to provide to the NetScaler CPX instance.
     The following is the sample custom configuration file:

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

{{ {}}

```
"counter": "http_requests_total",
"label": "method",
"description": "Total HTTP requests by method"
```

{{ }}}

1. Create a ConfigMap from the files using the `kubectl create configmap` command. For example, to create a ConfigMap named `custom-metrics-conf` based on the configuration file `custom_schema.json`:

{{ kubectl create configmap custom-metrics-conf --from-file=custom_schema.json=./custom_schema.json}}

1. View the created ConfigMap using the `kubectl get configmap` command.

{{ kubectl get configmap custom-metrics-conf -o yaml}}

1. The following example shows a sample output:

{{ apiVersion: v1}}

{{ data:}}

```
custom_schema.json: |
{
"counter": "http_requests_total",
"label": "method",
"description": "Total HTTP requests by method"
```

{{ }}}

{{ kind: ConfigMap}}

{{ metadata:}}

```
creationTimestamp: 2026-05-14T06:26:50Z
name: custom-metrics-conf
namespace: default
resourceVersion: "8865149"
uid: c1c7cb5b-ea05-11e7-914a-926745c10b02
```

To configure using a YAML file

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

1. Specify the created ConfigMap, `custom-metrics-conf`, in the YAML file used to deploy the NetScaler CPX instance.
   The following sample configuration shows how to include the ConfigMap in the deployment YAML:

```
apiVersion: v1  kind: Pod  metadata:    name: cpx-1    labels:
        app: cpx-daemon    annotations:      NETSCALER_AS_APP: "
    True"  spec:    containers:    - name: cpx      image: "quay.
    io/netscaler/netscaler-cpx:14.1-72.56"      securityContext:
          privileged: true      volumeMounts:      - name:
    config-volume        mountPath: /cpx/bootup_conf      - name:
     custom-metrics-volume        mountPath: /cpx/
    custom_metrics_conf      env:        - name: "EULA"
    value: "yes"      imagePullPolicy: IfNotPresent    volumes:
       - name: config-volume      configMap:        name: cpx-
    config    - name: custom-metrics-volume      configMap:
          name: custom-metrics-conf
```

Deploy the NetScaler CPX instance. Once the NetScaler CPX instance deploys and starts, the default metrics configuration files (`schema.json` and `reference_schema.json`) are placed in `/var/metrics_conf`. The custom JSON files from the ConfigMap mounted at `/cpx/custom_metrics_conf` are validated and copied into `/var/metrics_conf`.

Module - *Platform*

- **Build 72.61 | CTXENG-72083**

  Support for next-generation NetScaler MPX and SDX platforms

  NetScaler introduces support for the following next-generation platforms:

  - MPX 9200
  - MPX 17000
  - SDX 9200
  - SDX 17000

  Related topics

  NetScaler MPX 9200
  NetScaler SDX 9200
  NetScaler SDX 17000

  Module - *Platform*

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

- **Build 72.61 | CTXENG-72047**

  Jumbo frame support for Mellanox ConnectX series NICs

  NetScaler BLX now supports jumbo frames on Mellanox ConnectX NICs: ConnectX-4, ConnectX-5, and ConnectX-6.

  Related topic

  NetScaler BLX limitations and usage guidelines

  Module - *Platform*

- **Build 72.61 | CTXENG-72002**

  NetScaler CPX support for Kubernetes probes

  Kubernetes manages container lifecycles through startup, liveness, and readiness probes to ensure applications initialize correctly and remain healthy. NetScaler CPX now supports the readiness probe in addition to the existing startup and liveness probes. This support ensures that Kubernetes routes traffic to NetScaler CPX only when it is fully operational and, if configured, has successfully completed its license checkout. By utilizing these probes, you can improve application availability and ensure that failed or unresponsive instances are recreated promptly.

  Some of the benefits are:

  - **Enhanced traffic management**: Ensures NetScaler CPX receives traffic only when it is ready to handle requests.
  - **Operational reliability**: Restarts unhealthy containers automatically to recover from failures.
  - **Licensing validation**: Delays the ready state until license checkouts are successful when using the **LAS_CPX_BANDWIDTH** parameter.
  - **Precise initialization**: Coordinates the transition from container startup to active health monitoring.

  Note: NetScaler CPX version 14.1-72.x or later is required to use the readiness probe. For more detailed information on probe mechanics, refer to the official Kubernetes documentation.

  Configure Kubernetes Probes for NetScaler CPX
  To configure probes for NetScaler CPX, you must define the probe parameters within your Kubernetes deployment YAML file.

  To configure probes using the CLI:

  You must edit your deployment YAML file to include the specific `exec` commands that Kubernetes uses to verify the state of the NetScaler CPX container.

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

Configure the readiness probe: Add the following snippet to define when the pod is ready to accept traffic. CPX creates the `/tmp/cpx_ready` file when it is prepared to handle traffic. If you configure the `LAS_CPX_BANDWIDTH` parameter, CPX creates this file after a successful license checkout; otherwise, it appears after the startup process finishes. Kubernetes uses this file for the readiness probe to determine when to route traffic to the pod. Include the readiness probe configuration in your deployment YAML to enable this check.

```
readinessProbe:     exec:   command:       - /bin/ls       - /tmp/
    cpx_ready     failureThreshold: 15    initialDelaySeconds: 60
        periodSeconds: 30   successThreshold: 1     timeoutSeconds:
     1
```

Module - *Platform*

- **Build 72.61 | CTXENG-67816**

  Support for Intel E810 network interface card on NetScaler BLX DPDK

  NetScaler BLX now supports the Intel E810 network interface card (NIC), with the ICE driver fully supported through Data Plane Development Kit (DPDK). This enhancement expands hardware compatibility and delivers improved data plane performance. Organizations can take advantage of the E810s advanced capabilities, including higher packet processing throughput and enhanced network acceleration, to achieve more efficient and scalable network operations.

  Related topic

  System requirements

  Module - *Platform*

- **Build 72.61 | CTXENG-72050**

  Responder policy support for UDP-based traffic

  You can now bind responder policies to UDP-based virtual servers, enabling traffic management for UDP services.

  Related topic

  Responder

  Module - *Policies*

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

- **Build 72.61 | CTXENG-72087**

  Bypass extended key usage extension in SSL certificates

  NetScaler now supports bypassing the Extended Key Usage (EKU) extension check in incoming X.509 v3 SSL certificates. This enhancement is managed through the `strictClientEKUCheck` parameter. By default, this parameter is **ENABLED** to maintain standard security behavior. Disabling this parameter allows certificates that are otherwise rejected due to EKU extension constraints.

  Some of the benefits are:

  - Provides flexibility in supporting a wider range of client certificates.
  - Simplifies certificate management in environments with non-standard EKU requirements.

  Configure EKU Bypass

  You can configure the EKU bypass mode at either the Enhanced SSL Profile level or at the SSL virtual server level.

  To configure EKU bypass by using the CLI:

  1. **At the Enhanced SSL Profile level**: To disable the strict EKU check for a specific profile, type:
     `set ssl profile <sslProfileName> -strictClientEKUCheck DISABLED`
  2. **At the SSL virtual server level**: To disable the strict EKU check for a specific virtual server, type:

  `set ssl vserver <vserverName> -strictClientEKUCheck DISABLED`

  To configure EKU bypass by using the GUI:

  1. Navigate to **System > Profiles > SSL Profile**.
  2. Select the required enhanced profile and click **Edit**.
  3. In the **Basic Settings** section, click the pencil icon to edit the parameters.
  4. Clear the **Strict Client EKU Check** check box to disable the extension check.
  5. Click **OK**.

  Module - *SSL*

- **Build 72.61 | CTXENG-70702**

  Conditional client authentication and HTTP/2 support

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

NetScaler now supports the conditional enabling of client authentication and HTTP/2 based on policy evaluation.

Some of the benefits are:

- Enforcement of organizational policies.
- Ability to make informed business decisions.

Configure conditional client authentication and HTTP/2

You can configure conditional client authentication and HTTP/2 enablement on NetScaler by using CLI.

Configure conditional client authentication:

1. Add an SSL action for in-handshake client authentication. Type:
   `add ssl action <action_name> -inhandshakeClientAuth[ENABLED | DISABLED]-inhandshakeClientCert[MANDATORY | OPTIONAL]`
2. Add an SSL policy with a rule and the defined action. Type:
   `add ssl policy <policy_name> -rule <rule_expression> -action <action_name>`
3. Bind the SSL policy to an SSL virtual server. Type:
   `bind ssl vserver <vserver_name> -policyName <policy_name> -priority <priority_number> -type CLIENTHELLO_REQ`

Note: The default value of `inhandshakeClientcert` is `MANDATORY`.

Configure conditional HTTP/2 enablement:

1. Add an SSL action for HTTP/2. Type:
   `add ssl action <action_name> -alpnHttp2[ENABLED | DISABLED]`
2. Add an SSL policy with a rule and the defined action. Type:
   `add ssl policy <policy_name> -rule <rule_expression> -action <action_name>`
3. Bind the SSL policy to an SSL virtual server. Type:
   `bind ssl vserver <vserver_name> -policyName <policy_name> -priority <priority_number> -type CLIENTHELLO_REQ`

Note:

- You must enable HTTP2 on the HTTP profile attached to the virtual IP address for this policy to select HTTP/2.
- Ensure that clients present cipher suites that adhere to the HTTP/2 RFC specification, because the `http2Strictcipher` parameter is enabled by default in the HTTP profile.

Limitation

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

- DTLS SSL policy bindings are not supported.
- SSL_TCP policy bindings are not supported.
- An SSL policy with an HTTP2 associated action is not supported on an HTTP_QUIC type virtual server.

Related topic

SSL built-in actions and user-defined actions

Module - *SSL*

- **Build 72.61 | CTXENG-68300**

  Support for handling DTLS multi-messages

  NetScaler now supports multiple DTLS handshake messages in a single DTLS record received in one datagram. This capability applies to both the client-side and server-side operations, allowing for the parsing and processing of bundled handshake messages that arrive within a single UDP datagram.

  Some of the benefits are:

  - **Fewer UDP packets:** Reduces the total number of datagrams transmitted by packing data more densely.
  - **Faster handshake completion:** Reduces the round-trip time and latency, leading to quicker connection establishment.
  - **Efficient processing:** Enables efficient handling and processing of DTLS handshake messages.
  - **Network optimization:** Optimizes network usage by decreasing protocol overhead.

  Module - *SSL*

- **Build 72.61 | CTXENG-69849**

  URL normalization support

  NetScaler now provides native URL normalization to standardize inconsistent URL formats into a single, predictable structure. This enhancement prevents security vulnerabilities that attackers exploit through non-normalized URLs to bypass security filters. The feature supports multiple normalization types including case normalization, percent-encoding normalization, path segment normalization, and removal of duplicate slashes.

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

Administrators can enable URL normalization on HTTP profiles and optionally forward normalized URLs to origin servers for enhanced security and consistent application processing. This helps ensure that security rules, search engines, and web crawlers treat different representations of the same web resource uniformly while optimizing technical resource usage.

Prerequisites

Make sure that an HTTP profile is configured on NetScaler.

Configure URL normalization by using CLI

- **Enable URL normalization:** When you enable normalizeURL, all incoming URLs are normalized before any other module processes them for further evaluation. When disabled, incoming URLs pass to the subsequent module as received.

Use the set httpprofile command to enable URL normalization.

```
set httpprofile <profilename> -normalizeURL ENABLED
```

- **Forward normalized URLs to origin:** Forwarding normalized URLs to the origin server is a security best practice. This option ensures that the origin server receives only normalized data, enhancing security and performance. When you enable this setting, NetScaler forwards normalized URLs to the origin server. When disabled, NetScaler forwards URLs to the origin server exactly as received from the client.

Use the set httpprofile command to forward normalized URLs to the origin server.

```
set httpprofile <profilename> -normalizeURLtoOrigin ENABLED
```

For more information, see https://docs.netscaler.com/en-us/citrix-adc/current-release/security/normalize-urls .

Module - *System*

Fixed Issues

- **Build 72.61 | NSHELP-41140**

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

  Module - *Analytics Infrastructure*

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

- **Build 72.61 | 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***

- **Build 72.61 | NSHELP-42527**

  When JSON export is configured, NetScaler might crash while generating certain logs.

  Module - ***Analytics Infrastructure***

- **Build 72.61 | NSAUTH-15835**

  NetScaler might generate additional logs during the authorization process.

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

- **Build 72.61 | NSHELP-41009**

  NetScaler crashes during the OAuth IdP password grant flow when a password exceeds the supported length.

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

- **Build 72.61 | 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 72.61 | NSHELP-41590**

  When you configure NetScaler as an OAuth relying party, NetScaler might create an internal domain-based service for the authorization endpoint but this service is not required.

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

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

- **Build 72.61 | NSHELP-42047**

  When only StoreFrontAuthAction is configured on NetScaler Gateway, users cannot reset their LDAP passwords through the NetScaler Gateway portal when authentication is delegated to StoreFront.

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

- **Build 72.61 | NSHELP-42533**

  Published applications fail to launch after upgrading to version 14.166.54 because requests are blocked by the Web Application Firewall (WAF).

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

- **Build 72.61 | NSHELP-42478**

  Page load failures might occur when the Bot Management Device Fingerprint feature is enabled. This issue occurs when the injected fingerprint script conflicts with Node.js-generated JavaScript served by the protected application.

  Module - ***Bot Management***

- **Build 72.61 | 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 72.61 | NSHELP-41450**

  In an HA setup, an SSL content switching virtual server of type GSLB is marked as DOWN in the new Secondary after an HA failover.

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

Module - *Load Balancing*

- **Build 72.61 | 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*

- **Build 72.61 | 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 72.61 | NSHELP-42051**

  NetScaler might crash when you add a GSLB service using the IP or port combination that another GSLB service already uses.

  Module - *Load Balancing*

- **Build 72.61 | NSHELP-42293**

  GSLB synchronisation might fail when the partition name contains spaces.

  Module - *Load Balancing*

- **Build 72.61 | NSHELP-42437**

  The system does not support configuring a listen policy on a content switching virtual server that includes a GSLB target type. This limitation prevents the application of the listen policy.

  Module - *Load Balancing*

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

- **Build 72.61 | NSHELP-42631**

  A NetScaler buffer (NSB) leak might occur when the NetScaler proactively updates cached records fetched from a DNS server. This issue occurs when DNS server health flaps.

  Module - ***Load Balancing***

- **Build 72.61 | NSHELP-42742**

  NetScaler load balancing might fail when receiving a jumbo RADIUS request that contains a Message-Authenticator attribute.

  Module - ***Load Balancing***

- **Build 72.61 | 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.

  Module - ***Miscellaneous***

- **Build 72.61 | GOPHDX-7908**

  When HDX Insight is disabled in NetScaler, the values of the parameters in Insight data show zero for network telemetry-enabled ICA sessions.

  Module - ***NetScaler Gateway***

- **Build 72.61 | NSHELP-39780**

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

  Module - ***NetScaler Gateway***

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

- **Build 72.61 | 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 72.61 | NSHELP-41888**

  A crash occurs in NetScaler Gateway when HDX Insight is active and an EDT session is established.

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-42003**

  When Gateway Insight is enabled with nFactor authentication, NetScaler experiences an increasing memory consumption in the SSLVPN(LOG) pool, resulting in high memory utilization that is cleared only after a reboot.

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-42149**

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

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-42529**

  In a high availability setup configured for Citrix Secure Private Access for hybrid deployment, the secondary NetScaler instance might crash on session timeout.

  Module - *NetScaler Gateway*

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

- **Build 72.61 | NSHELP-42553**

  NetScaler might crash when processing audio traffic over UDP.

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-41731**

  The Management Service displays incorrect throughput statistics for NetScaler VPX instances that use fixed file-based licensing.

  Module - *NetScaler SDX Appliance*

- **Build 72.61 | 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 72.61 | NSHELP-42084**

  When the Management Service retrieves BMC information from a XenServer while the BMC is busy, temporary "Get Device ID command failed" alerts might appear. These alerts can be safely ignored, and no action is required.

  Module - *NetScaler SDX Appliance*

- **Build 72.61 | NSHELP-42216**

  Nitro API response for the `xen_health_disk` object returns the wrong value for `disk_utilized` metrics.

  Module - *NetScaler SDX Appliance*

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

- **Build 72.61 | 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.

  Module - *NetScaler SDX Appliance*

- **Build 72.61 | NSHELP-43210**

  In some environments, launching a console from the following GUI paths fails:

  – **Instances select any instance Console action**

  A console UI error appears instead of opening the browser console.

  – **System Console Management Service / XenServer**

  Console launch does not proceed.

  Module - *NetScaler SDX Appliance*

- **Build 72.61 | NSHELP-43239**

  Users cannot modify the `logfacility` setting in NetScaler SDX Syslog Server configuration through the CLI.

  Module - *NetScaler SDX Appliance*

- **Build 72.61 | 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 72.61 | 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 72.61 | 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 72.61 | 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 72.61 | NSHELP-41875**

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

  Module - *NetScaler Web App Firewall*

- **Build 72.61 | 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*

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

- **Build 72.61 | NSHELP-42256**

  The **Deploy** or **Skip** button for learned rules in WAF profiles might fail to function as expected.

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

- **Build 72.61 | NSHELP-42476**

  The `HttpOnly` flag might not be added to the response cookie when Cookie flag option is configured within an application firewall profile.

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

- **Build 72.61 | NSHELP-42605**

  Configuring Application Firewall or Bot signature auto-updates by using the NetScaler GUI might fail or not take effect as expected.

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

- **Build 72.61 | NSHELP-42415**

  In an HA-INC deployment, the `dynamicRouting` L3 parameter configured in an admin partition is reset instead of being retained during HA failover.

  Module - ***Networking***

- **Build 72.61 | 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***

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

- **Build 72.61 | 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 72.61 | NSHELP-42376**

  When **CPU yield** is enabled, customers might observe high CPU usage in NetScaler version 14.1 build 72.23 and earlier builds.

  Module - *Platform*

- **Build 72.61 | NSHELP-42382**

  When migrating a NetScaler VPX deployed on Nutanix AHV from pooled licensing to LAS-based licensing using Console, SSL performance might be restricted. A hard reboot of the system is required to fully initialize the new performance limits.

  Module - *Platform*

- **Build 72.61 | NSHELP-43047**

  NetScaler CPX might fail to register successfully with License Activation Service (LAS).

  Module - *Platform*

- **Build 72.61 | NSHELP-43094**

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

During Azure maintenance windows, after HA failover is restored, secondary IP addresses might incorrectly remain on the standby node instead of migrating back to the primary node. This issue occurs because the failover retry logic caches stale Azure API responses and incorrectly determines that no IP addresses need to be moved back.

Module - *Platform*

- **Build 72.61 | 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 72.61 | NSHELP-43937**

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

  Module - *Platform*

- **Build 72.61 | NSLINUX-17**

  In a NetScaler BLX appliance with DPDK support, tagged VLANs are not supported for DPDK Intel i350 NIC ports. This is observed as it is a known issue present on the DPDK driver.

  Module - *Platform*

- **Build 72.61 | NSLINUX-8831**

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

  Module - *Platform*

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

- **Build 72.61 | NSPLAT-35556**

  NetScaler VPX running on Azure might crash during dynamic detach and reattach operations of the SR-IOV NIC used by Azure Accelerated Networking.

  Module - *Platform*

- **Build 72.61 | NSHELP-41726**

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

  Module - *Policies*

- **Build 72.61 | NSHELP-42429**

  NetScaler might crash when an `ns` variable is configured with the Least Recently Used (LRU) option.

  Module - *Policies*

- **Build 72.61 | 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 72.61 | NSHELP-42049**

  CRL parsing might fail for specific CRLs when they reach certain file sizes, even though the CRL addition succeeds.

  Module - *SSL*

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

- **Build 72.61 | NSHELP-42195**

  When upgrading from NetScaler 13.1 to 14.1, you might experience configuration loss if certificate or key file names contain special characters.

  Module - *SSL*

- **Build 72.61 | NSHELP-42320**

  In an HA setup, when the DEFAULT cipher group is removed from an SSL virtual server, it reappears on the secondary node immediately following an HA synchronization or failover.

  Module - *SSL*

- **Build 72.61 | NSHELP-42491**

  In rare cases, when a policy is configured, NetScaler might crash during TLS 1.3 handshakes when the system simultaneously processes SSL close-notify alerts and TCP FIN events.

  Module - *SSL*

- **Build 72.61 | NSBASE-19568**

  When the server-side TCP window reaches a 2 GB limit, the gRPC hold logic incorrectly opens the TCP window twice for held bytes, resulting in a zero window advertisement. This issue also includes incorrect accounting of chunk header and trailer bytes before they are passed to the application handler, affecting TCP window management and data transmission.

  Module - *System*

- **Build 72.61 | 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*

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

- **Build 72.61 | NSBASE-20565**

  When a virtual server receives an HTTP/1.1 chunked request (POST or PUT) and forwards it to an HTTP/2 backend service, the chunked transfer-encoding metadata is not stripped from the body before the HTTP/2 DATA frames are constructed.

  Module - *System*

- **Build 72.61 | NSBASE-20726**

  A denial-of-service vulnerability was identified in the HTTP/2 flow-control mechanism where certain request patterns could exhaust system resources and affect service availability.
  This issue is now resolved with the introduction of a mechanism to detect and terminate stalled HTTP/2 connections. Configure the `http2SmallWndTimeout` parameter in the HTTP profile to define the maximum permitted stall duration before a connection is closed. Setting this parameter to `0` will disable the check.

  Module - *System*

- **Build 72.61 | 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 72.61 | 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.

  Module - *System*

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

- **Build 72.61 | 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 72.61 | 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 72.61 | 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*

- **Build 72.61 | NSHELP-42563**

  HTTP/2 uploads through NetScaler might fail when features such as AppFirewall or Rewrite are configured to buffer and inspect the HTTP request body.

  Module - *System*

- **Build 72.61 | NSHELP-42738**

  NetScaler crashes during client connection reuse when a content inspection (CI) action for an Intrusion Detection System (IDS) uses a load balancing virtual server. The crash occurs because NetScaler attempts to access and dereference the CI profile from the CI server.

  Module - *System*

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

- **Build 72.61 | NSHELP-43402**

  ExtraHop files in the `/var/tmp/wasm` directory might be deleted 30 days after VM creation.

  Module - *System*

- **Build 72.61 | 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 72.61 | NSHELP-42027**

  When you attempt to view or edit an authentication action linked to an advanced authentication policy, the NetScaler GUI might not display the action details.

  Module - *User Interface*

- **Build 72.61 | NSHELP-42128**

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

  Module - *User Interface*

- **Build 72.61 | NSHELP-42181**

  When the user does not have full shell access permission, edit operations on the WAF signature file fail in the UI with the following error:
  ”Not authorized to execute this command [shell]”

  Module - *User Interface*

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

- **Build 72.61 | NSHELP-42399**

  In Fixed Bandwidth LAS licensing deployments, when uploading the License Activation Request (.tgz) file to the License Activation Service (LAS), users might encounter the following error: ”This vpx is already offline activated.”

  Module - *User Interface*

- **Build 72.61 | NSHELP-42456**

  When importing a Responder HTML page from the GUI, you might encounter an Unable to upload file error, which prevents completion of the system file update requests.

  Module - *User Interface*

- **Build 72.61 | NSHELP-42471**

  When you configure a load balancing monitor using the NetScaler GUI, the system returns a ”d.indexOf is not a function” error if you select and delete multiple certificates from the selection table before saving.

  Module - *User Interface*

- **Build 72.61 | NSHELP-42566**

  The NetScaler GUI might fail to unbind the SSL log profile from the SSL profile.

  Module - *User Interface*

- **Build 72.61 | NSHELP-42725, NSHELP-42994**

  NetScaler MPX 8000 appliances migrated to License Activation Service (LAS) using console-based licensing (Flexed/CPL) might come up unlicensed after a reboot.

  Module - *User Interface*

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

- **Build 72.61 | NSHELP-42792**

  In Fixed Bandwidth LAS licensing deployments, when uploading the License Activation Request (.tgz) file to the License Activation Service (LAS), users might encounter the following error:

  Activation request file integrity check failed.

  Module - ***User Interface***

- **Build 72.61 | NSUI-22522**

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

  Module - ***User Interface***

- **Build 72.61 | 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***

- **Build 72.61 | NSUI-22553**

  Administrators cannot view or manage profile configurations in the NetScaler 14.1 GUI when accessing **System > Profiles** in admin partition. This action returns an ”Operation not permitted” error.

  Module - ***User Interface***

Known Issues

- **Build 72.61 | NSAUTH-11151**

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

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 72.61 | NSHELP-42847**

  NetScaler VPX on Linux might crash while performing LDAP authentication.

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

- **Build 72.61 | NSHELP-43223**

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

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

- **Build 72.61 | NSHELP-43405**

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

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

- **Build 72.61 | NSHELP-43511**

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

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

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

- **Build 72.61 | NSHELP-44540**

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

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

- **Build 72.61 | NSHELP-41831**

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

  Module - ***Load Balancing***

- **Build 72.61 | NSHELP-42361**

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

  Module - ***Load Balancing***

- **Build 72.61 | NSHELP-42438**

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

  Module - ***Load Balancing***

- **Build 72.61 | NSHELP-42821**

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

  Module - ***Load Balancing***

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

- **Build 72.61 | NSHELP-43548**

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

  Module - *Load Balancing*

- **Build 72.61 | 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 72.61 | NSHELP-40999**

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

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-42506**

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

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

  Module - *NetScaler Gateway*

- **Build 72.61 | NSHELP-43313**

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

  Module - *NetScaler SDX Appliance*

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

- **Build 72.61 | 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 72.61 | 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 72.61 | NSHELP-36236**

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

  Module - ***Networking***

- **Build 72.61 | NSHELP-42632**

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

  Module - ***Platform***

- **Build 72.61 | NSHELP-43268**

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

  Module - ***Platform***

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

- **Build 72.61 | NSHELP-43508**

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

  Module - *Platform*

- **Build 72.61 | NSHELP-43592**

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

  Module - *Platform*

- **Build 72.61 | NSLINUX-7437**

  The RDP Proxy functionality is not supported in BLX Gateway.

  Module - *Platform*

- **Build 72.61 | 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 72.61 | 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 72.61 | NSLINUX-10080**

  On a NetScaler VPX instance deployed on Linux platform, the packet engine might crash on a long-running system because of memory exhaustion. NetScaler VPX recovers automatically after the crash.

  Module - *Platform*

- **Build 72.61 | 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 72.61 | NSHELP-43002**

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

  Module - *Policies*

- **Build 72.61 | NSHELP-43411**

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

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

Module - *Policies*

- **Build 72.61 | NSHELP-42609**

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

  Module - *SSL*

- **Build 72.61 | NSHELP-42955**

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

  Module - *SSL*

- **Build 72.61 | 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 72.61 | NSHELP-42508**

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

  Module - *System*

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

- **Build 72.61 | NSHELP-42526**

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

  Module - *System*

- **Build 72.61 | NSHELP-42021**

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

  Module - *User Interface*

- **Build 72.61 | 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 72.61 | NSHELP-42745**

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

  Module - *User Interface*

- **Build 72.61 | 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*

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

- **Build 72.61 | NSUI-23051**

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

  Module - ***User Interface***

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