NetScaler Application Delivery Management 13.1

Contents

Release notes

June 18, 2024

The NetScaler Application Delivery Management (ADM) 13.1 release notes describe the new features, enhancements to existing features, and the known issues in a build. The release notes document for the 13.1 release includes the following sections:

- **What's New**: The new features and enhancements to existing features released in a build.
- **Known Issues**: The issues that exist in a build, and their workarounds, wherever applicable.
- **Fixed Issues**: The issues addressed in a build.

> **Note**
>
> These release notes do not document security related fixes. For a list of security related fixes and advisories, see the security bulletin.

To view the release notes document for a specific build of release 13.1, click the corresponding link in the following table. When the release notes are updated for a build, the version number of the release notes and the publish date are also updated. The release notes publish date might not be the same as the build GA date.

Release notes for NetScaler Console on-prem software version 13.1	Publish date	Version
Build 13.1-53.22 (Build 53.22 replaces Build 53.17 and includes the new NetScaler telemetry program)	June 18, 2024	2.0
Build 13.1-52.19	Mar 12, 2024	1.0
Build 13.1-51.14	Dec 14, 2023	1.0
Build 13.1-50.23	Oct 20, 2023	1.0
Build 13.1-49.13	Jul 18, 2023	1.0
Build 13.1-48.47	Jun 14, 2023	2.0
Build 13.1-45.61	Apr 26, 2023	2.0
Build 13.1-42.47	Mar 23, 2023	3.0
Build 13.1-37.38	Dec 01, 2022	2.0
Build 13.1-33.50	Oct 31, 2022	2.0

Release notes for NetScaler Console on-prem software version 13.1	Publish date	Version
Build 13.1-30.52	Oct 31, 2022	2.0
Build 13.1-27.62	Oct 31, 2022	2.0
Build 13.1-24.38	Oct 31, 2022	2.0
Build 13.1-21.53	Oct 31, 2022	2.0
Build 13.1-17.42	Oct 31, 2022	2.0
Build 13.1-12.50	Oct 31, 2022	2.0
Build 13.1-9.60	Oct 31, 2022	2.0
Build 113.1-4.43	Sep 14, 2021	1.0

Migrate on-premises NetScaler ADM to Citrix Cloud

March 11, 2024

You can migrate on-premises **NetScaler ADM 13.0 64.35 or a later version** to Citrix Cloud. If your ADM has 12.1 or an earlier version, you must first upgrade to **13.0 64.35 or a later version** and then migrate to Citrix Cloud. For more information, see the Upgrade section.

ADM service through Citrix Cloud enables you to get:

- Faster releases, approximately every two weeks with latest feature updates.
- Machine-learning based analytics for application security and bot, performance, and usage.
- Various other features that are currently supported only in ADM service, such as peak and lean period analytics, machine-learning based analytics for application security and bot, application CPU analytics, and many more.

For a successful migration, you must:

- Ensure to have internet connection in on-premises ADM for Citrix Cloud accessibility
- Configure the ADM service agent
- Get the client and secret CSV file from Citrix Cloud
- Validate the ADM service licensing

- Migrate using a script

After you migrate from on-premises ADM to ADM service, if you want to again continue with on-premises ADM, you can use the rollback script. For more information, see Roll back to onpremises ADM.

Configure the ADM service agent

To enable communications between NetScaler instances and NetScaler ADM, you must configure an agent. NetScaler agents are, by default, automatically upgraded to latest build. You can also select a specific time for the agent upgrade. For more information, see Configuring agent upgrade settings.

- If your existing on-premises ADM (standalone or HA pair) has no on-premises agents configured, you must configure at least one agent for ADM service.
- If your existing on-premises ADM (standalone or HA pair) has configured with on-premises agents for multisite deployments, you must configure the same number of agents for ADM service.

For more information on configuring an agent, see the Getting Started section.

Get the client and secret CSV file from Citrix Cloud

After you configure the agent, get the client and secret CSV file from the Citrix Cloud page:

1. Log on to citrix.cloud.com
2. Click the **Home** icon and select **Identity and Access Management**
3. From the **API Access** tab, enter a secure client name and click **Create Client**.
4. ID and Secret is generated. Click **Download** and save the CSV file in the on-premises ADM.

   For example, save the CSV file to the /var directory.

Validate the ADM service licenses

You must obtain licenses for ADM service.

- The VIP licenses in ADM service must be more than or equal to the on-premises VIP licenses.

  > **Note**
  >
  > If VIP licenses are lesser, then virtual servers are selected randomly and the VIP-level configuration for ADM service fails.

- If you use ADM on-premises deployment as a license server, reallocate your licenses to ADM Service before migration. For more information, see Configure an ADM server only as the pooled license server and How to reallocate a license file.
- If you are using the pooled licenses in on-premises ADM, you must obtain the pooled licenses for ADM service and then allocate licenses to the ADC instances. For more information, see Configure Pooled Licensing. The following supported ADC versions enable you to modify the license allocation from ADM:
  - NetScaler SDX: 13.0 74.11 or later versions.
  - NetScaler VPX and MPX: 13.0 47.24 or later versions, 12.1 58.14 or later versions, and 11.1 65.10 or later versions.

Migrate using a script

- Using the ADM 82.x build, you can select the feature and then migrate.
- For ADM 76.x or later builds, the migration scripts (`servicemigrationtool.py` and `config_collect_onprem.py`) are available as part of the build, available at `cd /mps/scripts`.
- For ADM earlier than 76.x builds, you must download the migration scripts and copy the scripts in on-premises ADM.

> Note
>
> Ensure that the on-premises ADM has internet connectivity during migration.

1. Using an SSH client, log on to the on-premises ADM.

> Note
>
> For an ADM HA pair, log on to the primary node.

2. Type **shell** and press **Enter** to switch to bash mode.
3. Copy the client ID and secret CSV file. For example, copy the file to the /var directory.

   After you copy the CSV file, you can validate if the CSV file is present.

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```


> Note
>
> For an ADM HA pair, copy the CSV file in the primary node.

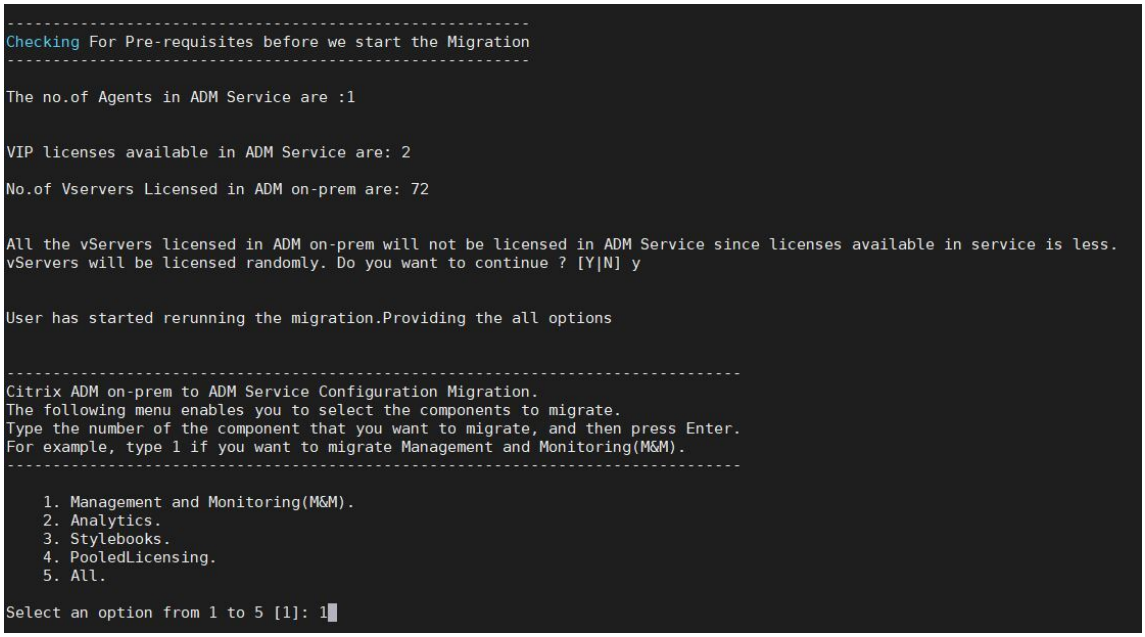
4. For ADM **13.0 82.xx version**, run the following commands to complete the migration:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

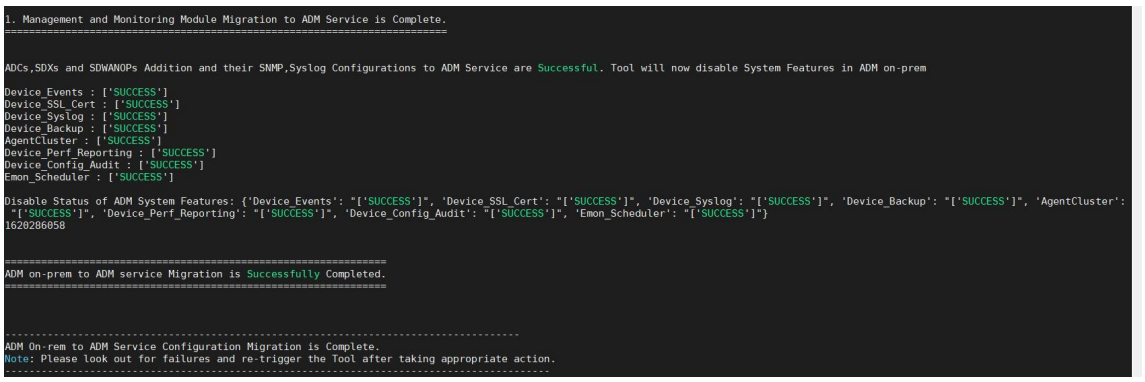
   For example, `python servicemigrationtool.py /var/secureclient.csv`

   After you run the migration script, the tool displays the following options:



   Based on the choice you provide, only that feature gets migrated to ADM service.

   In the example, option 1 is selected. The tool completes the Management and Monitoring (M&M) migration and displays the following message:



   The **Management and Monitoring (M&M)** feature includes:

- ADC Instances, tags, instance groups, profiles, custom apps, config jobs, SNMP, syslog configurations.
- Sites, IP blocks, network reporting, analytics thresholds, notification settings, data pruning settings.
- Config audit templates, polling intervals, event rules and settings.
- RBAC groups, roles, and policies

The **Analytics** feature includes:

- Appflow configuration per vserver from ADC instances.
- Appflow configuration per SDWAN device.

> Note:
>
> - The Management and Monitoring (M&M) feature is automatically migrated, even if you select any other feature (2, 3, or 4).
> - You can specify only one feature at a time.
> - After you complete migrating any feature, if you want to migrate any other feature later, the feature that is already migrated is not shown in the list. For example, if you complete migrating the **Analytics** feature first, the next time you run the migration script, you can see only the **StyleBooks**, **Pooled Licensing**, and **All** options.
> - When you migrate pooled licensing, it migrates all types including vservers.

5. For ADM **13.0 76.xx version**, run the following commands to complete the migration:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

   For example, `python servicemigrationtool.py /var/secureclient.csv`

6. For ADM earlier than 13.0 76.xx version:

   a) Download the migration script from the following location:
   `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Save the two scripts in on-premises ADM. For example, save in the /var directory

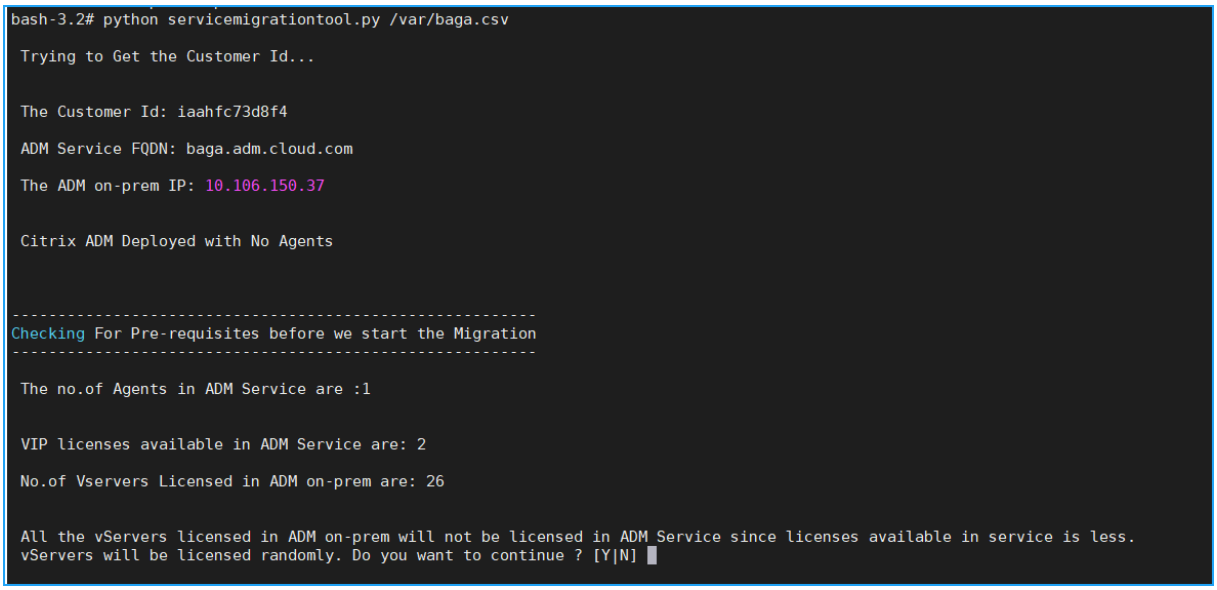
c) Run the following commands to migrate:

i. `cd /var`

ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

For example, `python servicemigrationtool_27.py /var/secureclient.csv`

After you run the script, it checks the prerequisites and then proceeds with the migration. The script first checks for the license availability. The following message is displayed only if you have lesser ADM service license than the on-premises license.



If you select **Y**, the migration continues by licensing the VIP randomly. If you select **N**, the script stops the migration.

If you have the unsupported ADC instance version for the pooled license server, the following message is displayed:


```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Changing of PooledLicense Server will be effective for below SDX/ADC versions
--------------------------------------------------------------------------------
  For SDX Versions: 13.0 74.11 Onwards
  For ADC Versions: 13.0 47.24 and Onwards
                    12.1 58.14 and Onwards
                    11.1 65.10 and Onwards
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------

 The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

 The List of SDXs supported for Pooled License Server change are:
[]

 The List of ADCs not supported for Pooled License Server change are:
[]

 The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

 Migration will change the License Server to ADM Service Agent.
 Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

 Do you want to continue with rest of the migration ? [Y|N]
```

If you select **Y**, the migration process continues by changing the license server. If you select **N**, the script prompts if you want to proceed with rest of the migration. The script stops the migration if you select **N**.

Depending upon the on-premises configuration, the approximate time for the migration to complete is between a few minutes and a few hours. After the migration is complete, you see the following message:

```
--------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

The migration is successful once all the ADC instances and their respective configurations are successfully moved to ADM service. After successful migration, the on-premises NetScaler ADM stops processing the following instance events:

- SSL certificates
- Syslog messages
- Backup
- Agent cluster
- Performance reporting
- Configuration audit
- Emon scheduler

Roll back to onpremises ADM

If you want to roll back to on-premises ADM, ensure that the prerequisites are met.

Prerequisites

If your on-premises ADM (before migrating to ADM service) is:

- Used as a pooled license server, ensure you have the required pooled licenses in the on-premises ADM.
- Configured with on-premises ADM agents, ensure the agents are available in "UP"status.

Use the rollback script

> Note
>
> After rollback, the same configurations (before migration) in Analytics, SNMP, pooled licensing are again available in on-premises ADM. If you have made any changes to these configurations after migration, these changes are not reflected in on-premises ADM.

- For **ADM 82.xx or later** builds, the rollback script is available as part of the build and accessible at `/mps/scripts`.
- For **ADM earlier than 79.xx** builds, you can either upgrade to 82.x build and use the rollback script or you can download the rollback script and copy the script in on-premises ADM.

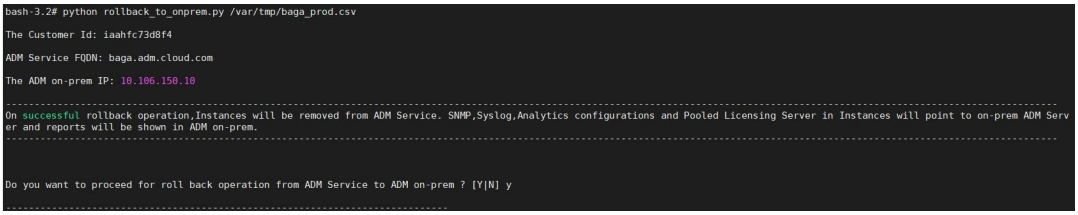
1. Using an SSH client, log on to the on-premises ADM.
2. Type shell and press Enter to switch to bash mode.
3. For ADM **13.0 82.xx** build, run the following commands to complete the rollback:

    a) cd /mps/scripts

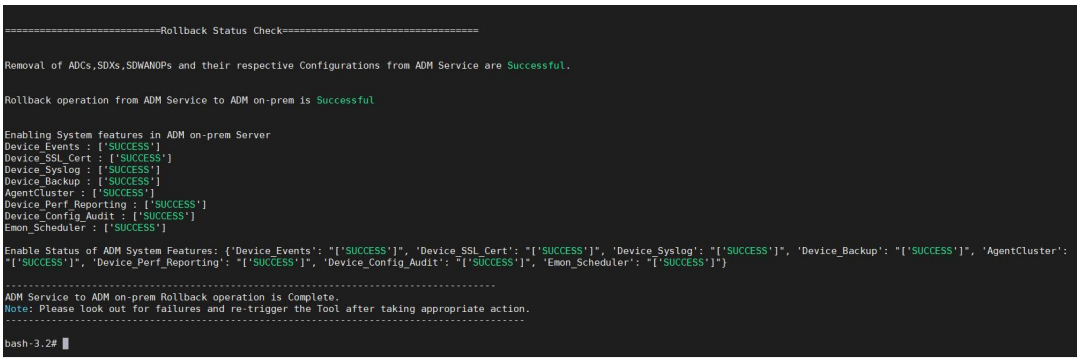
    b) python rollback_to_onprem.py <`path of ClientID/Secret File in ADM on-prem VM`>

    For example, `python rollback_to_onprem.py /var/ secureclient.csv.csv`

    The tool initiates the rollback operation and a prompt asks if you want to proceed. Type **Y** to proceed.



You can see the following message after the rollback gets completed.



4. For ADM earlier than 82.xx build:

   a) Download the rollback script from the following location:

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   b) For ADM 79.xx and 76.xx builds, save the script in `/mps/scripts` and run the following commands to roll back:

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

      For example, `python rollback_to_onprem.py /var/ secureclient.csv`

   c) For ADM earlier than 76.xx builds, save the script in on-premises ADM. For example, save it in the `/var` location and run the following commands to roll back:

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

      For example, `python rollback_to_onprem_27.py /var/secureclient.csv`

The tool initiates the rollback operation and a prompt asks if you want to proceed. Type **Y** to proceed.

FAQs

March 11, 2024

ADM service

Is ADM service agent optional similar to on-premises NetScaler agent?

No. ADM service agent is mandatory for ADM service and all communications between instances and ADM service happen through the ADM service agent. On-premises ADM agent is optional; however, you can configure the on-premises agent only for saving bandwidth consumption.

Why ADM service?

ADM service through Citrix Cloud provides the following benefits, without the need for new periodic builds:

- Cloud-based SaaS offering with easier onboarding and lesser cost of ownership than the on-premises NetScaler ADM.
- Faster releases, approximately every two weeks with latest feature updates.
- Machine-learning based analytics for application security, performance, and usage.
- Various other features that are currently supported only in ADM service, such as peak and lean period analytics, machine-learning based application security analytics for WAF and bot, application CPU analytics, and many more.

You might also join the NetScaler ADM service monthly webinar to understand the latest product features and solutions. Register for the webinar using the following link:

`https://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html`

What happens after migration if on-premises NetScaler ADM is an HA pair?

All configurations are moved to Citrix Cloud. Configuring a disaster recovery node is not required.

What happens if the agent goes down for any reason?

You can expect a potential data loss until the agent is up and running. However, you can also configure ADM agents for multisite deployments to ensure continuity if there is an agent failover. For more information, see Configure ADM agents for multisite deployment.

Is instance backup also migrated?

Backup is not included in migration.

Is historical data also migrated?

Historical data is not migrated. You can export the data from the on-premises ADM.

Are on-premises licenses also migrated?

No. The on-premises license file cannot be used for ADM service. You must obtain licenses for ADM service. For more information, see Licensing. If you are using pooled licenses in on-premises ADM, you must obtain pooled licenses for ADM service and then allocate licenses to instances.

What is not migrated from on-premises NetScaler ADM?

The following features cannot be migrated to ADM service:

- **RBAC** –In ADM service, the user access is based on the invite from the administrator. ADM service users must have an account in Citrix Cloud. As a result, the on-premises ADM users are not migrated.
- **Export schedules** –Export schedules include details such as drill-down and schedules from various pages. All these detailed export schedules are not migrated.
- **SSL Certificates/Keys/CSRs** –ADM service can only display the ADC SSL certificates/Keys/CSRs. As a result, SSL certs/keys uploaded to on-premises NetScaler ADM won't be migrated to ADM service.

On-premises NetScaler ADM is integrated with Citrix Director. What happens to the integration?

Director integration with ADM is currently supported only in on-premises ADM.

After migration, is it again required to license the instance or to enable analytics?

You must ensure that the licenses in ADM service are more than or equal to the on-premises VIP licenses. If the licenses are already more than the on-premises NetScaler ADM VIP, the virtual servers are automatically licensed. If not, the licenses are assigned randomly.

Migration tool

After running the migration script, error messages are displayed. What can be the issue?

A log file with failure reasons is displayed. You can take appropriate corrective actions and run the migration script again. In general, before you run the migration script, ensure to:

- Configure the ADM service agent
- Obtain the ADM service licenses
- Copy the correct path where you have stored the client and secure CSV file

The ADC instances have lower versions than the mentioned limitation for pooled licensing. What happens if the option 'Y'is selected to change the license server?

Change of license server happens only for the supported NetScaler MPX, VPX, and SDX versions.

What happens if the migration script has failed configuration regarding ADC instances?

The ADC instances continue to work on the on-premises ADM setup. You can take necessary action from the suggested failed reason and run the migration script again.

What happens if a few of the ADC instances fail to move to ADM service. Will rerunning the migration script help?

Yes. After you rerun the script, only the failed instances are migrated. Let's assume that two out of five instances have failed to move. After you have taken corrective actions and rerun the migration script, three instances that were moved successfully earlier show the "Device already exists"message. And the other two instances that failed earlier are migrated successfully.

Is there a log file to check the migration status?

Yes, a log file is generated in the `/var/mps/log/` directory. ADM with python3.7 has the log file as `servicemigrationtool.py.log` and ADM with python 2.7 has the log file as `servicemigrationtool_27.py.log`.

What happens if the session gets terminated while running the migration script?

You can rerun the migration script. In the new session, the already added instances from the last session display as "Device already exists", and the migration continues further.

What happens if ADM service has lesser licenses than the on-premises NetScaler ADM and the migration script is initiated?

After the migration script is run, a suggestion appears, mentioning about the licenses are lesser and prompts to continue or stop. If you want to continue with lesser licenses, the virtual servers are licensed randomly from the available licenses.

What happens when on-premises NetScaler ADM is migrated to the ADM service Express Account?

The ADM service Express Account has only two virtual server licenses, two StyleBook configuration packs, and two configuration jobs. If your on-premises ADM has more than these configurations and you initiate the migration with Express Account, the script can migrate only the mentioned configurations applicable for Express Account (two virtual server licenses, two StyleBook configuration packs, and two configuration jobs)

What happens if a Citrix Cloud invited user (other than Admin User who created Citrix Cloud account) tries to migrate on-premises ADM setup?

It is recommended that the administrator to run the migration script. An invited user does not have admin privileges (adminExceptSystem_group). As a result, groups, roles, and policies migration fail and the message "User doesn't have permission"is displayed.

As a solution, the administrator (who created the Citrix Cloud account) can change the group associated with invited user as "admin_group".

Rollback script

What happens if rollback script is used in on-premises ADM HA pair?

The on-premises ADM HA pair is restored with all configurations that were available before migration.

What happens to Disaster Recovery node after using the rollback script?

Disaster recovery node is also restored with all configurations before migration.

Troubleshooting

March 11, 2024

When you run the migration script for the first time, it checks for the prerequisites and proceeds with the migration. If all prerequisites are met, the migration completes without any errors. If any prerequisite fails, the script displays error messages with reasons. After fixing the errors, you must rerun the script again.

> Note
>
> If you see an error message that displays "already exists", it means that:
>
> - You might have run the migration script for more than one time and some configurations are already migrated to ADM service.
> - You might have manually created the same configuration in ADM service, before running the migration script.

Refer to some of the following error messages:

Manual profile added to ADM service

```
==================Profiles Addition to ADM Service====================


60.26 : FAILURE : Profile 60.26 already exists

 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

Workaround: If you have created admin profiles in NetScaler ADM service before running the migration script, ensure to delete those profiles and rerun the migration script.

NetScaler device added to ADM service

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

Workaround: In on-premises ADM, ensure the instance status and see if you can access the instance without any issues. If any issue persists, fix the issue, and rerun the migration script.

StyleBook custom templates import to ADM service

```
==============Stylebook custom templates Import to ADM Service====================


neustar.citrix.adc.stylebooks_5.0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.

neustar.citrix.adc.stylebooks_5.0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}

==============Stylebook repository Addition to ADM Service====================
```

Workaround: This error message is an example for the already migrated StyleBook. You can also see this error if you have manually created a StyleBook with the same name, version, and namespace, in NetScaler ADM service before running the migration script.

Configuration Jobs added to ADM service

```
==============Config Jobs Addition to ADM Service====================

config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

Workaround: This error occurs if you have subscribed to Express Account and have more than two configuration jobs. You must obtain a valid subscription to have all your configuration jobs to be migrated.

IP blocks added to ADM service

```
====================IP Blocks Addition in ADM Service======================

ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

Workaround: Delete the IP block that is manually created in ADM service and rerun the migration script.

Network dashboard report addition status

```
================Network Dashboard Reports Addition to ADM Service================

new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```


Workaround: Delete the dashboard that is manually created in ADM service and rerun the migration script.

All how to articles

March 11, 2024

NetScaler Application Delivery Management (NetScaler ADM) “How-to Articles”are simple, relevant, and easy to implement articles on the features of NetScaler ADM. These articles contain information about some of the popular NetScaler ADM features such as instance management, application management, StyleBooks, certificate management, and Analytics.

Click a feature name in the table below to view the list of how-to articles for that feature.

Topics				
Instance management	Event management	StyleBooks	Certificate management	NetScaler ADM System
	Configuration management	Authentication	Analytics	Network functions

Instance management

How to monitor globally distributed sites

How to manage admin partitions of NetScaler instances

How to add instances to NetScaler ADM

How to create instance groups on NetScaler ADM

How to configure sites for Geomaps in NetScaler ADM

How to force a failover to the secondary NetScaler instance by using NetScaler ADM

How to force a secondary NetScaler instance to stay secondary by using NetScaler ADM

How to back up and restore an instance using NetScaler ADM

How to use the NetScaler ADM dashboard to monitor an HAProxy instance

How to display the details of the frontends configured on HAProxy instances

How to display the details of the backends configured on HAProxy instances

How to display the details of the servers configured on HAProxy instances

How to restart an HAProxy instance from NetScaler ADM

How to back up and restore an HAProxy instance by using NetScaler ADM

How to edit the HAProxy configuration file by using NetScaler ADM

How to rediscover multiple NetScaler VPX instances

How to poll NetScaler instances and entities in NetScaler ADM

How to unmanage an instance on NetScaler ADM

How to trace the route to an instance from NetScaler ADM

Configuration management

How to create a configuration job on NetScaler ADM

How to use SCP (put) command in configuration jobs

How to upgrade NetScaler SDX instances by using NetScaler ADM

How to schedule jobs created by using built in templates in NetScaler ADM

How to reschedule jobs that were configured by using built in templates in NetScaler ADM

How to reuse executed configuration jobs

How to upgrade NetScaler instances using NetScaler ADM

How to use variables in configuration jobs on NetScaler ADM

How to use configuration templates to create audit templates on NetScaler ADM

How to create configuration jobs from corrective commands on NetScaler ADM

How to replicate running and saved configuration commands from one NetScaler instance to another on NetScaler ADM

How to use Record-and-Play to create configuration jobs

How to use configuration jobs to replicate configuration from one instance to multiple instances

How to use the master configuration template on NetScaler ADM

How to poll configuration audit of NetScaler instances

How to reuse configuration audit templates in configuration jobs

How to import and export configuration templates

How to generate configuration audit diff for ConfigChange SNMP traps

Certificate management

How to configure an enterprise policy on NetScaler ADM

How to install SSL certificates on a NetScaler instance from NetScaler ADM

How to update an installed certificate from NetScaler ADM

How to link and unlink SSL certificates by using NetScaler ADM

How to create a Certificate Signing Request (CSR) by using NetScaler ADM

How to set up notifications for SSL certificate expiry from NetScaler ADM

How to use the SSL dashboard on NetScaler ADM

How to poll SSL certificates from NetScaler Instances

StyleBooks

How to view different groups of StyleBooks

How to create your own StyleBooks

How to use user-defined StyleBooks in NetScaler ADM

How to use API to create configurations from StyleBooks

How to enable analytics and configure alarms on a virtual server defined in a StyleBook

How to create a StyleBook to upload files to NetScaler ADM

How to use API to create configurations to upload any file type

How to create a StyleBook to upload SSL certificate and certificate key files to NetScaler ADM

How to use API to create configurations to upload cert and key files

How to use Microsoft Skype for Business StyleBook in business enterprises

How to use Microsoft Exchange StyleBook in business enterprises

How to use Microsoft SharePoint StyleBook in business enterprises

Analytics

How to enable analytics on instances

How to configure adaptive thresholds

How to configure SLA management

How to configure database summarization for analytics

How to create thresholds and alerts using NetScaler ADM

How to disable URL data collection for analytics from NetScaler ADM

How to view the type of videos streamed and the data volume consumed from your network

How to view the peak data rate for a particular time frame

How to view the network efficiency

Event management

How to set event age for events on NetScaler ADM

How to schedule an event filter by using NetScaler ADM

How to set repeated email notifications for events from NetScaler ADM

How to suppress events by using NetScaler ADM

How to use the events dashboard to monitor events

How to create event rules on NetScaler ADM

How to modify the reported severity of events that occur on NetScaler instances

How to view the events summary in NetScaler ADM

How to display event severities and skews of SNMP traps on NetScaler ADM

How to export syslog messages using NetScaler ADM

How to suppress syslog messages in NetScaler ADM

How to configure prune settings for instance events

Authentication

How to enable fallback and cascade external authentication servers

How to add RADIUS authentication servers

How to add LDAP authentication servers

How to add TACACS authentication servers

How to extract authentication server group in NetScaler ADM

How to enable fallback local authentication

NetScaler ADM system

How to upgrade NetScaler ADM

How to reset the password for NetScaler ADM

How to generate a tech support file for NetScaler ADM

How to back up and restore your NetScaler ADM server in a single server deployment

How to back up and restore a NetScaler ADM configuration in an HA pair

How to enable shell access for non-default users in NetScaler ADM

How to configure NTP server on NetScaler ADM

How to configure SSL settings for NetScaler ADM

How to configure syslog purging interval for NetScaler ADM

How to view auditing information of NetScaler ADM

How to configure system notification settings of NetScaler ADM

How to monitor CPU, memory, and disk usage of NetScaler ADM

How to configure a cipher group for NetScaler ADM

How to create SNMP traps, managers, and users on NetScaler ADM

How to assign a host name to a NetScaler ADM server

How to configure system prune settings for NetScaler ADM

How to configure system backup settings by using NetScaler ADM

How to configure and view system alarms on NetScaler ADM

Network functions

How to generate reports for load balancing entities

How to export or schedule export of network functions reports

Overview

December 31, 2023

NetScaler Application Delivery Management (ADM) is a centralized management solution that simplifies operations by providing administrators with enterprise-wide visibility and automating management jobs that need to be run across multiple instances. You can manage and monitor NetScaler products that include NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX and NetScaler Gateway. You can use ADM to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

ADM is a virtual appliance that runs on Citrix Hypervisor, VMware ESXi, and Linux KVM. ADM addresses the application visibility challenge by collecting the following detailed information about web-application and virtual-desktop traffic:

- user-session-level information
- Webpage performance data
- database information flowing through the ADC instances at your site and provides actionable reports.

ADM enables IT administrators to troubleshoot and proactively monitor customer issues in a matter of minutes.

Features and solutions

March 11, 2024

NetScaler Application Delivery Management (ADM) provides the following features:

Application Analytics and Management

Application performance analytics

App Score is the product of a scoring system that defines how well an application is performing. It shows whether the application is performing well in terms of responsiveness, is not vulnerable to threats, and has all the systems up and running.

Application security analytics

The App Security Dashboard provides a holistic view of the security status of your applications. For example, it shows key security metrics such as security violations, signature violations, threat indexes. App Security dashboard also displays attack related information such as SYN attacks, small window attacks, and DNS flood attacks for the discovered ADC instances.

Networks

Instances

Enables you to manage the NetScaler and NetScaler Gateway instances.

Instance groups

Enables you to group your instances as follows:

- Static Group: Allow you to define a device group that you can use in different tasks such as, Configuration Jobs and so on.
- Private IP-block: Enables you to group your instances based on geographical locations.

Event management

When the IP address of an ADC instance is added to ADM, a NITRO call is sent by ADM and implicitly adds itself as a trap destination for the instance to receive its traps or events.

Events represent occurrences of events or errors on a managed ADC instance.

Certificate management

NetScaler ADM now streamlines every aspect of certificate management for you. Through a single console, you can establish automated policies to ensure the right issuer, key strength, and correct algorithms, while keeping close tabs on certificates that are unused or soon to expire. To begin using ADM's SSL dashboard and its functionalities, you must understand what an SSL certificate is and how you can use ADM to track your SSL certificates.

Configuration management

NetScaler ADM allows you to create configuration jobs that help you perform configuration tasks, such as creating entities, configuring features, replication of configuration changes, system upgrades, and other maintenance activities with ease on multiple instances. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on ADM.

Configuration audit

Enables you to monitor and identify anomalies in the configurations across your instances.

- Configuration Advice: Allows you to identify configuration anomaly.
- Audit template: Allows you to monitor the changes across a specific configuration.

Network reporting

You can optimize resource usage by monitoring your network reporting on ADM.

Analytics

Web Insight

Provides visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler by providing integrated and real-time monitoring of applications. Web Insight provides critical information such as user and server response time, enabling IT organizations to monitor and improve application performance.

HDX Insight

Provides end-to end visibility for ICA traffic passing through NetScaler. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues.

Gateway Insight

Provides visibility into the failures that users encounter when logging on, regardless of the access mode. You can view a list of users logged on at a given time, along with the number of active users, number of active sessions, and bytes and licenses used by all users at any given time.

Security Insight

Provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

SSL Insight

SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler by providing integrated and real-time and historic monitoring of secure web transactions.

TCP Insight

TCP Insight provides an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in ADC instances to avoid network congestion in data transmission.

Video Insight

The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by NetScaler instances to improve customer experience and operational efficiency.

WAN Insight

WAN Insight analytics enable administrators to easily monitor the accelerated and unaccelerated WAN traffic that flows between the data center and branch WAN optimization appliances. WAN Insight also provides visibility into clients, applications, and branches on the network, to help troubleshoot network issues effectively.

Orchestration

Cloud Orchestration

Enables integration of NetScaler products with OpenStack cloud orchestration. NetScaler ADM and OpenStack implement each other's APIs, enabling integration of the NetScaler instance's Load Balancing feature (LBaaS) with OpenStack cloud orchestration.

Orchestration

NetScaler ADM supports SDN in the enterprise network by integrating with SDN controllers of different vendors. ADM supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

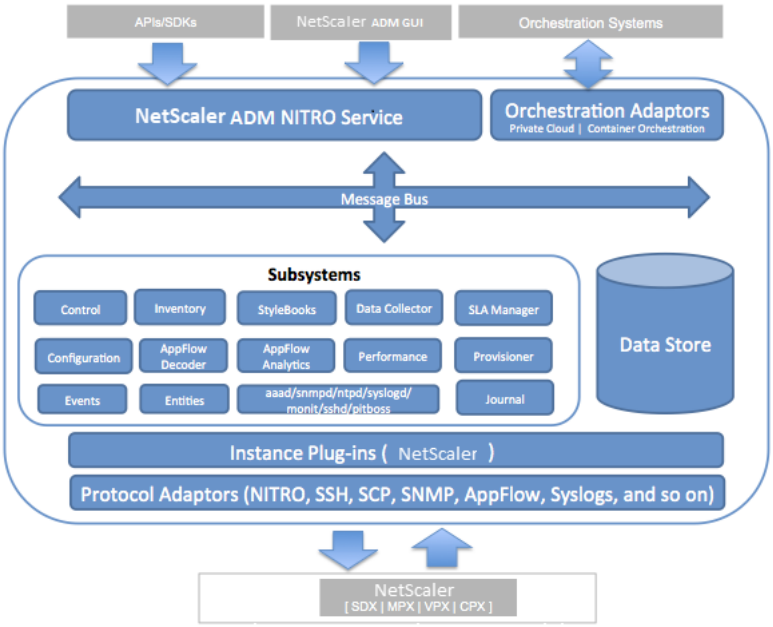
Architecture

December 31, 2023

The NetScaler Application Delivery Management (ADM) database is integrated with the server, and the server manages all the key processes, such as data collection, NITRO calls. In its data store, the server stores an inventory of instance details, such as host name, software version, running and saved configuration, certificate details, entities configured on the instance. A single server deployment is suitable if you want to process small amounts of traffic or store data for a limited time.

Currently, ADM supports two types of software deployments: single server and high availability.

The following image shows the different subsystems within ADM and how communication happens between the ADM server and managed instances.



The Service subsystem in ADM acts as a web server that handles HTTP requests and responses that are sent to subsystems within ADM from the GUI or API, using ports 80 and 443. These requests are sent to the subsystems over the message bus (message processing system) by using the IPC (inter-process communication) mechanism. A request is sent to the Control subsystem, which either processes the information or sends it to the appropriate subsystem. Each of the other subsystems—Inventory, StyleBooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner, and Journal—has a specific role.

Instance plug-ins are shared libraries that are unique to each instance type supported by ADM. Information is transferred between ADM and managed instances by using NITRO calls, or through the SNMP, Secure Shell (SSH), or Secure Copy (SCP) protocol. This information is then processed and stored in the internal database (data store).

How NetScaler ADM discovers instances

March 11, 2024

Instances are NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Application Delivery Management (ADM). To manage and monitor these instances, you must add them to the NetScaler ADM server. You can add the following NetScaler ADC appliances and virtual appliances to ADM:

- NetScaler instances
  - NetScaler MPX

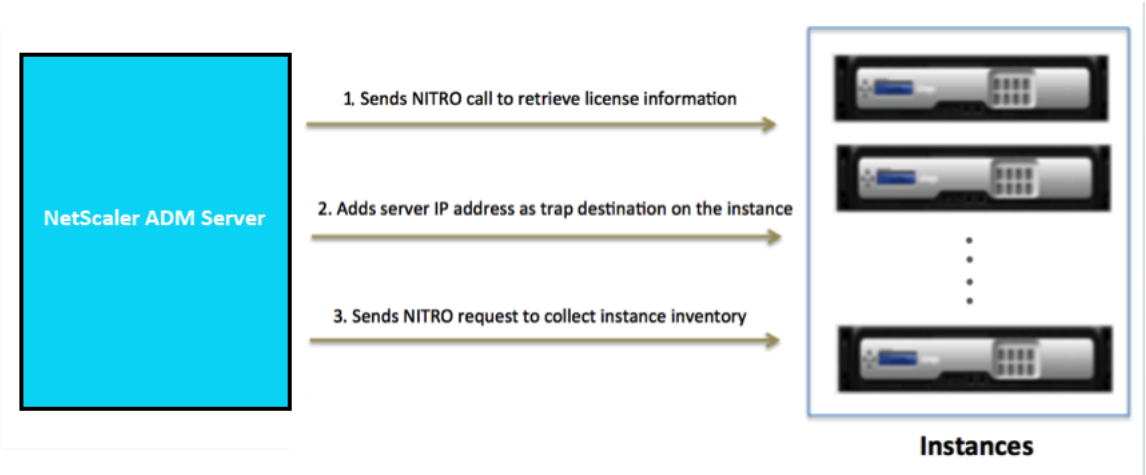
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gateway instances

You can add instances either while setting up the NetScaler ADM server for the first time or later.

> **Note**
>
> NetScaler ADM uses the NetScaler IP (NSIP) address of the ADC instances for communication. ADM can also discover ADC instances with a subnet IP (SNIP) address that has management access enabled on it. For information about the ports that must be open between the ADC instances and ADM, see Ports.
>
> If you want to add an ADC HA pair using SNIP, ensure to enable the Independent Network Configuration (INC) mode on the ADC HA pair. For more information to add instances, see Add instances.

When you add an instance to the ADM server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance.

The following diagram describes how ADM implicitly discovers and adds instances.



As shown in the diagram, the following steps are performed implicitly by NetScaler ADM.

1. NetScaler ADM uses the instance profile details to log on to the instance. Using an ADC NITRO call, ADM retrieves the license information of the instance. Based on the licensing information, it determines whether the instance is an ADC instance and the type of ADC platform (for example, NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX, or NetScaler Gateway). On successful detection of the instance, it is added to the ADM's database.

This step might fail if the instance profile does not include the correct credentials. For NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX, and NetScaler Gateway instances, this step might also fail if the licenses are not applied to the instance.

> **Note**
>
> Using HTTP, you can add all instances to ADM even if the licenses are not configured on the instances.

2. ADM adds its IP address to the list of trap destinations on the instance. This allows ADM to receive traps generated on the ADC instance.

   This step might fail if the number of trap destinations on the instance exceeds the maximum limit of trap destinations. The maximum limit on instances is 20.

3. ADM collects inventory from the instance by sending a NITRO request. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance.

   This step might fail because of network or firewall issues.

   To learn to add instances to ADM, see Add instances.

Polling overview

June 13, 2024

Polling is a process, where NetScaler Application Delivery Management (ADM) collects certain information from NetScaler instances. You might have configured multiple NetScaler instances for your organization, across the world. To monitor your instances through NetScaler ADM, NetScaler ADM has to collect certain information such as CPU usage, memory usage, SSL certificates, licensed features, license types, and so on from all managed ADC instances. The following are the different types of polling that occur between ADM and the managed instances:

- Instance polling
- Inventory polling
- Performance data collection
- Instance backup polling
- Configuration audit polling
- SSL certificate polling
- Entity polling

NetScaler ADM uses protocols such as NITRO call, Secure Shell (SSH), and Secure Copy (SCP) to poll information from NetScaler instances.

How NetScaler ADM polls managed instances and entities

NetScaler ADM automatically polls at regular intervals by default. NetScaler ADM also enables you to configure polling intervals for a few polling types and allows you to poll manually when required.

The following table describes the details of types of polling, polling interval, protocol used, and so on:

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Instance polling	Every 1 minute (by default)	Statistical information such as state, HTTP requests per second, CPU usage, memory usage, and throughput.	NITRO call.	No
Inventory polling	Every 60 minutes (by default)	Inventory details such as build version, system information, licensed features, and modes.	NITRO calls and SSH	No
Performance data collection	Every 5 minutes (by default)	Network reporting information	NITRO call	No
Instance backup polling	Every 12 hours (by default)	Backup file of the current state of the managed ADC instances	NITRO calls, SSH, and SCP.	Yes. Navigate to **Infrastructure > Instances > NetScaler**. Select the instance and from the **Select Action** list, click **Backup/Restore**.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Configuration audit polling	Every 10 hours (by default)	Configuration changes that occur on ADC instances (for example, running vs. saved configuration)	SSH, SCP, and NITRO call	Yes. Navigate to **Infrastructure > Configuration Audit**. On the Configuration Audit page, click **Settings** and configure the polling interval for Configuration Audit Polling. You can poll configuration audits manually and add all configuration audits of the instances immediately to NetScaler ADM. To do so, navigate to **Infrastructure > Configuration Audit** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
SSL certificates polling	Every 24 hours (by default)	SSL certificates that are installed on NetScaler instances.	NITRO calls and SCP	Yes. Navigate to **Infrastructure > SSL Dashboard**. On the SSL Dashboard page, click **Settings** to configure the polling interval You can poll SSL certificates manually and add all certificates of the instances immediately to NetScaler ADM. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Entity polling	Every 60 minutes (by default)	All entities that are configured on the instances. An entity is either a policy, virtual server, service, or action attached to an ADC instance. To enable entity polling, see Enable or disable ADM features.	NITRO calls.	Yes, but cannot be set to less than 10 minutes. To configure, navigate to **Infrastructure > Network Functions**. On the Networks Function page, click **Settings** to configure the polling interval. You can poll entities manually and add all entities of the instances immediately to NetScaler ADM. To do so, navigate to **Infrastructure > Network Functions** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network

> **Note**
>
> In addition to polling, events generated by managed ADC instances are received by NetScaler ADM through SNMP traps sent to the instances. For example, an event is generated when there is a system failure or change in configuration.

> During instance backup, SSL files, CA certificate files, ADC templates, database information, and so on are downloaded to NetScaler ADM. During a configuration audit, ns.conf files are downloaded and stored in the file system. All information collected from managed NetScaler instances are stored internally within the database.

Different ways of polling instances

The following are the different ways of polling that NetScaler ADM performs on the managed instances:

- Global polling of instances
- Manual polling of instances
- Manual polling of entities

Global polling of instances

NetScaler ADM automatically polls all the managed instances in the network depending on the interval configured by you. Though the default polling interval is 30 minutes, you can set the interval depending on your requirements by navigating to **Infrastructure > Network Functions** > **Settings**.

Manual polling of instances

When NetScaler ADM is managing many entities, the polling cycle takes a longer time to generate the report that might result in a blank screen or the system might still display earlier data.

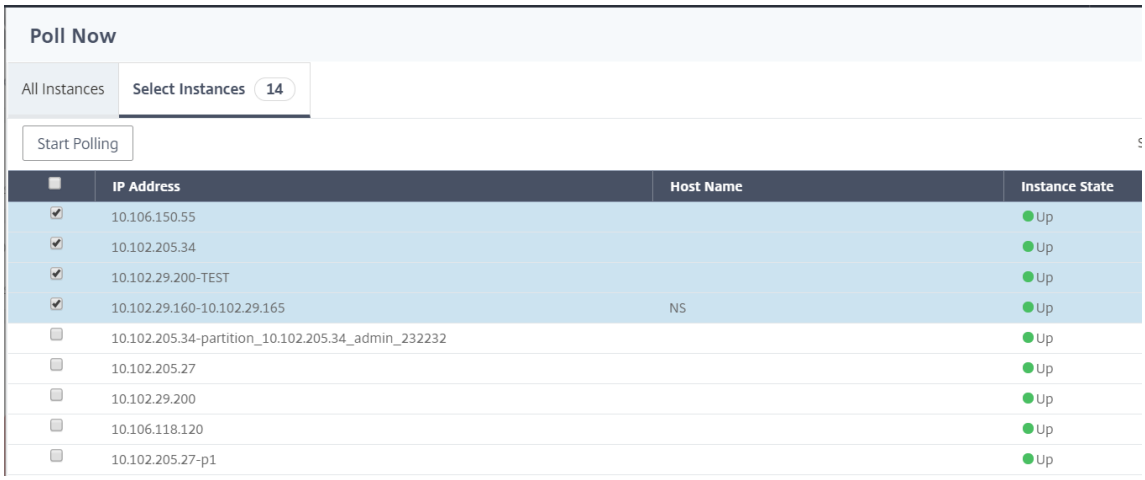
In NetScaler ADM, there is a minimum polling interval period when automatic polling does not happen. If you add a new NetScaler instance, or if an entity is updated, NetScaler ADM does not recognize the new instance or the updates made to an entity until the next polling happens. And, there is no way to immediately get a list of virtual IP addresses for further operations. You must wait for the minimum polling interval period to elapse. Though you can do a manual poll to discover newly added instances, this leads to the entire NetScaler network to be polled, which creates a heavy load on the network. Instead of polling the entire network, NetScaler ADM now allows you to poll only selected instances and entities at any given time.

NetScaler ADM automatically polls managed instances to collect information at set times in a day. Selected polling reduces the refresh time that NetScaler ADM requires to display the most recent status of the entities bound to these selected instances.

To poll specific instances in NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > Network Functions**.

2. On **Network Functions** page, at the top right-hand corner, click **Poll Now**.
3. The pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network or poll the selected instances.
    a) **All Instances** tab - click **Start Polling** to poll all the instances.
    b) **Select Instances** tab - select the instances from the list
4. Click **Start Polling**.



NetScaler ADM initiates manual polling and adds all the entities.

Manual polling of entities

NetScaler ADM also allows you to poll only a few selected entities that are bound to a particular instance. For example, you can use this option to know the latest status of a particular entity in an instance. In such a case, you need not poll the instance as a whole to know the status of one updated entity. When you select and poll an entity, NetScaler ADM polls only that entity and updates the status in the NetScaler ADM GUI.

Consider an example of a virtual server being DOWN. The state of that virtual server might have changed to UP before the next automatic polling happens. To view the changed status of the virtual server, you might want to poll only that virtual server so that the correct state is displayed on the GUI immediately.

You can now poll the following entities for any update in their status: services, service groups, load balancing virtual servers, cache reduction virtual servers, content switching virtual servers, authentication virtual servers, VPN virtual servers, GSLB virtual servers, and application servers.

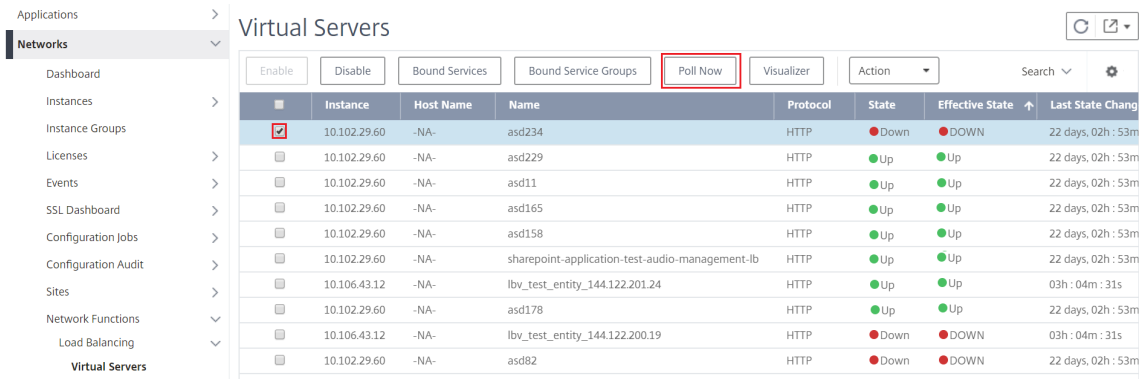
> **Note**
>
> If you poll a virtual server, only that virtual server is polled. The associated entities such as ser-

> vices, service groups, and servers are not polled. If you need to poll all associated entities, you must manually poll the entities or you must poll the instance.

To poll specific entities in NetScaler ADM:

As an example, this task assists you to poll load balancing virtual servers. Similarly, you can poll other network function entities too.

1. In NetScaler ADM, navigate to **Infrasturcture > Network Functions > Load Balancing > Virtual Servers**.
2. Select the virtual server that shows the state as DOWN, and click **Poll Now**. The status of the virtual server now changes to UP.



NetScaler telemetry program

June 18, 2024

Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. You may automatically or manually upload the required license and feature usage data to remain compliant with the NetScaler telemetry program described here. NetScaler Console configuration and feature usage data is also collected to manage, measure, and improve Citrix products and services. If you are an existing NetScaler Console customer, you must ensure to be compliant with the NetScaler telemetry program.

You can upload the required telemetry data using the following ways:

- **Automated collection mode** - This mode is enabled by default after you upgrade to **14.1 25.53 or later** / **13.1-53.22 or later** build. The automated mode creates an outbound connection to use the auto-enabled channel (endpoint URLs) and uploads the telemetry data automatically. You must only ensure that the endpoint URLs are reachable. Since the upload happens automatically, no action is required from your end unless the prerequisites fail. For more information, see Automated collection mode.

- **Manual collection mode** - This mode is enabled only if the automated mode is disabled. You must download the required telemetry data from the NetScaler telemetry homepage in NetScaler Console on-prem and complete the first upload to NetScaler Console service within 30 days. The subsequent uploads must be done every 90 days to remain compliant. For more information, see Manual collection mode.

The recommendation is to use the automated telemetry mode and upload the required data automatically, but you can also choose to disable the automated mode and upload it manually. In both automated and manual modes, data upload is required to remain compliant with the NetScaler telemetry program. You may choose to disable the optional telemetry data from being included in the data upload, but the required license compliance and feature usage telemetry data must be provided in both the automated and manual modes.

To remain compliant, the number of days since the last successful upload must not be greater than 90 days.

The following table provides the parameter details that are collected as part of NetScaler telemetry program:

Categories	Description	What do we use it for?	Required/Optional
License, and NetScaler deployment and usage telemetry	Information about license entitlement, allocation, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

For more information about the list of optional and required telemetry parameters, see Data governance.

Citrix requires that you transition to the most recent NetScaler Console build (14.1 25.53 or later / 13.1-53.22 or later) within 3 months starting from **18th June 2024**. After upgrading to NetScaler Console 14.1 25.53 or later / 13.1-53.22 or later, one of the telemetry modes (automatic or manual) must be actively functioning. Unless you have elected manual reporting, you agree to adjust your firewalls as necessary to allow automatic telemetry reporting.

Points to note:

- You must ensure that you transition to the latest build (14.1-25.53 and later / 13.1-53.22 and later) by **18th September 2024**.
- If you opt for manual telemetry mode, the first upload must be completed within 30 days of your transition to the above build, but no later than 18th October 2024. Thereafter the manual telemetry upload must be done every 90 days for your NetScaler Console on-prem to be compliant with the NetScaler telemetry program.

Citrix may suspend or terminate your Citrix Support for non-compliance of these requirements without liability, in addition to any other remedies Citrix may have at law or equity. These requirements do not apply to the extent prohibited by law or regulation. For more information, see Citrix License Telemetry FAQ.

Data governance

June 18, 2024

All existing NetScaler Console customers must be compliant with the NetScaler telemetry program by uploading the required telemetry data either through automated or manual mode. The NetScaler telemetry program is enabled starting from 14.1-25.53 and later / 13.1-53.22 and later build. For more information, see the NetScaler telemetry program.

Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. NetScaler Console configuration and feature usage data is also collected to manage, measure and improve Citrix products and services.

The automated telemetry collection mode enables you to use the **Security Advisory** feature in NetScaler Console on-prem that collects the optional telemetry parameters. You can disable the optional parameters, but not the required parameters.

> **Note:**
>
> If optional parameters are disabled, then the data telemetry contains only the required parameters.

The following table provides the parameter details that are collected as part of NetScaler telemetry program:

Categories	Description	What do we use it for?	Required / Optional
License, and NetScaler deployment and usage telemetry	Information about license entitlement, allocation, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

To disable the optional parameters:

1. In NetScaler Console on-prem, navigate to **NetScaler Telemetry** and disable **Security Advisory**.
2. Navigate to **Settings > Administration > Enable or disable the Console feature data sharing**, and clear the **I agree to share Console feature usage data** checkbox.

If your NetScaler Console is earlier than 13.1-53.22, you can create a Customer Identity on Citrix Cloud to send important statistics about NetScaler Console health, status, and other metrics from NetScaler Console on-prem deployment to Citrix Cloud account. Citrix collects statistics to understand the usage of NetScaler Console. For more information, see Data governance for Customer Identity.

Licensing

March 11, 2024

NetScaler Application Delivery Management (ADM) requires a verified NetScaler license to manage and monitor the NetScaler instances, when the instances are discovered through the `https` protocol.

NetScaler ADM supports the following license editions. Contact your NetScaler sales representative or partner to purchase an ADM license.

Express edition –You can manage and monitor any number of instances with the Express edition license. By default, the Express edition license is applied.

Advanced edition - It allows to manage the discovered applications and view analytics for the purchased virtual servers along with the free virtual servers.

Points to note:

- For build **13.1-9.x or earlier**, you can manage up to 30 discovered applications or virtual servers and view analytics. Beyond the 30 discovered applications or the 30 virtual servers, you must buy and apply an Advanced license. For example, if you buy 100 virtual server licenses, then you are entitled to you use up to 130 virtual server licenses.
- For build **13.1-12.x or later**, you can manage up to two discovered applications or virtual servers and view analytics. Beyond the two discovered applications or the two virtual servers, you must buy and apply an Advanced license. For example, if you buy 100 virtual server licenses, then you are entitled to you use up to 102 virtual server licenses.

Post upgrade to build 13.1-12.x:

- All the Express default free virtual servers remain functional for 30 days. You can select the 2 virtual servers and apply the 2 default licenses within the 30 days grace period. If no user action is taken 30 days post upgrade, ADM randomly applies license to 2 virtual servers and unlicenses the remaining virtual servers. You must buy and apply new Advanced licenses to enable these virtual servers.
- Post upgrade, the following are the changes in the ADM behavior:
  - ADM enforces a 30-day grace period.
  - Within the 30-day grace period, the allocation of new virtual servers for the 30 express free virtual servers is blocked.
    - For example, if the number of available virtual server licenses before you upgraded to 12.x was 30 and only 20 licensed virtual servers were used, you are only allowed to use the 20 virtual servers and not allowed to license the remaining 10 virtual servers in the 30-day grace period.
  - However, within the 30-day grace period, as an administrator, you can still apply Advanced ADM licenses and allocate new virtual servers.

Features	Options	Express edition	Advance edition	NetScaler License
Applications	Application Dashboard	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NetScaler Web App Firewall related information on App Dashboard needs Premium (or) Advanced with App Firewall license.
		Web Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.
		Service Graph	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.
		Configuration > StyleBooks	Unlimited	Unlimited
Security	Security Dashboard	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NetScaler Web App Firewall related information on Security Dashboard needs Premium (or) Advanced with App Firewall license.
		Security Violations	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.

Features	Options	Express edition	Advance edition	NetScaler License
		Users and endpoints	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.
Gateway	HDX Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
		Gateway Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.
Infrastructre	Infrasturcture Analytics	Unlimited	Unlimited	NA
		Instances	Unlimited	Unlimited
		SSL Dashboard	Unlimited	Unlimited
		Events	Unlimited	Unlimited
		Network Functions	Unlimited	Unlimited
		Network Reporting	Unlimited	Unlimited
		Pooled licenses	Unlimited	Unlimited
		Configuration > Configuration Jobs, Configuration Templates, and Configuration Advice	Unlimited	Unlimited
		Upgrade Jobs	Unlimited	Unlimited
		Orchestration	Unlimited	Unlimited
		WAN Insight	Unlimited	Unlimited

Features	Options	Express edition	Advance edition	NetScaler License
Settings	RBAC & External Authentication (instance level)	Unlimited	Unlimited	NA
		RBAC & External Authentication	Unlimited	Unlimited

*For Citrix Director integration with NetScaler ADM support –Citrix Director must have Premium license.

Licenses for more virtual servers are available in virtual server packs of 10. You can obtain a valid license and add the licenses on the NetScaler ADM servers through the NetScaler ADM GUI.

High Availability

The NetScaler ADM server can contain VIP, CICO, and pooled capacity licenses. When the licenses are issued to an ADM server, the licenses are bound to the host ID of the server. And, assigning licenses to a different ADM server is restricted.

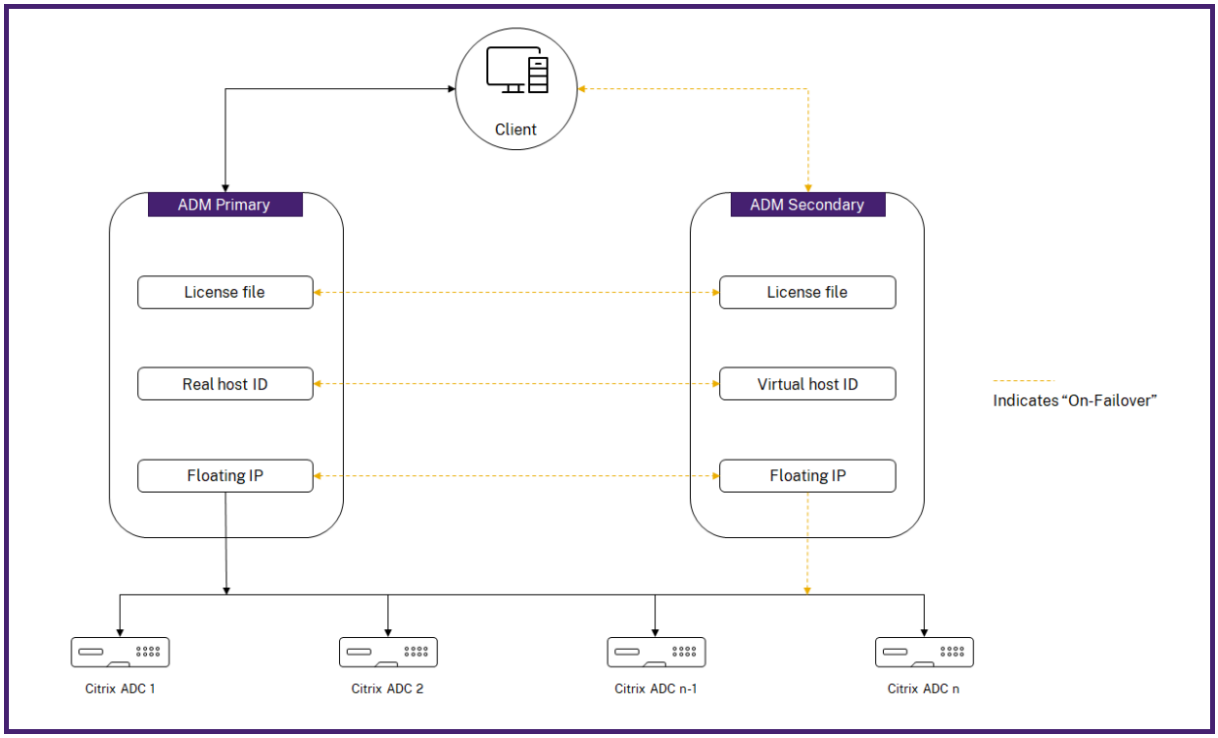
If you configure an ADM high-availability pair as a license server, the primary and secondary servers must have the same license files. Therefore, in the ADM high-availability deployment, NetScaler ADM supports you assign the same license files to both servers.

> **Note**
>
> - If you have installed NetScaler ADM 12.1.49.x or earlier releases, you get a grace period of 30 days to maintain the licensing on the secondary node. After the grace period, you must contact Citrix to rehost the original license.
> - For 12.1.50.x or later releases, the NetScaler ADM license is automatically synchronized to the secondary node.
> - Pooled licenses are automatically synchronized to the secondary node from 12.1.50.x or later release.

How licenses are synchronized between ADM high-availability nodes?

Whenever a failover occurs, the secondary server assumes the role of the primary server. The real host ID of the primary server is configured as the virtual host ID of the new primary server. The license files recognize the new primary server using the virtual host ID.

- **Real Host ID** - This ID is generated from a MAC Address of the ADM server. Each ADM standalone deployment has a unique host ID.
- **Virtual Host ID** - This ID is auto generated during HA deployment. The real host ID of an ADM primary server is used as the virtual Host ID of a secondary server. This ID is stored in the ADM database in an encrypted format and modifications to this ID is restricted. The virtual Host ID is preferred over the real Host ID.



Assume Node-1 is the primary server and Node-2 is the secondary server. The virtual Host ID of Node-1 is synchronized with Node-2.

1. License files available in Node-1 are synchronized to Node-2.
2. Any new license files on Node-1 are synchronized to Node-2 periodically.
3. ADM ensures that the License Server is running only on Node-1 to avoid doubling of license capacity.
4. NetScaler instances check out licenses from Node-1 using the floating IP address.

Licenses are locked to ADC instances. To check out licenses from a NetScaler ADM HA, instances require the specific appliance's IP address. When you apply licenses on a primary server that will be in charge of licensing, and it applies all future licenses on that instance. You can delete licenses only from the server on which you have installed the licenses.

Orchestration

The Orchestration module is independent of licensing and is always available.

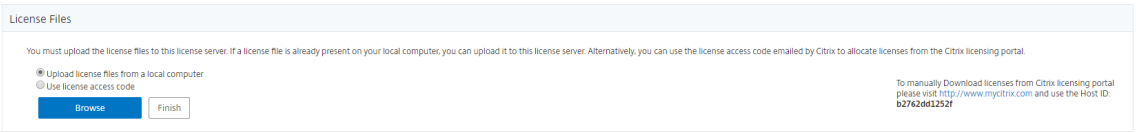
Upgrade the virtual server licenses

You can upgrade the licensing on NetScaler ADM to monitor and manage more virtual servers hosted on the NetScaler appliances.

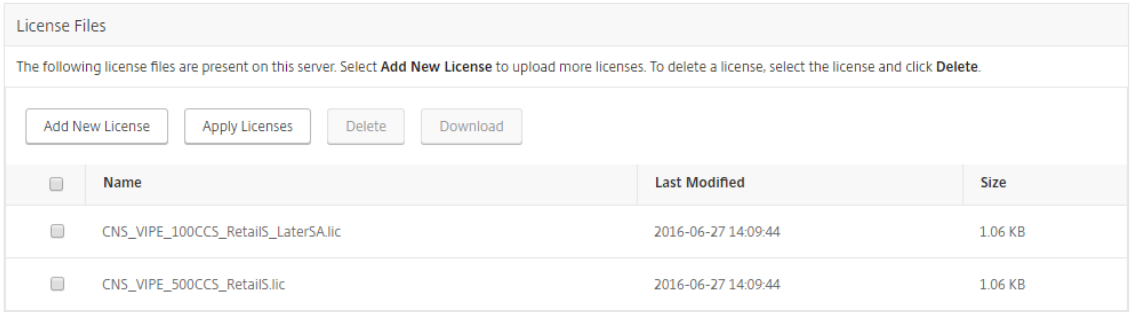
To upgrade your appliance licenses:

1. Log on to NetScaler ADM using the administrator credentials.
2. Navigate to **Infrastructure > Pooled Licensing**.
3. Go to **License Files**, and select one of the following options:
   - **Upload license files from a local computer**. If a license is already present on your local computer, click **Browse** and select the license file (.lic) that you want to use to allocate your licenses. Click **Finish**.
   - **Use License Activation Code**. Citrix emails the license access code for the license that you purchased. Enter the license access code in the text box and then click **Get Licenses**.

> **Note**
>
> If you select this option, the NetScaler ADM must be connected to the Internet, or a proxy server must be available.

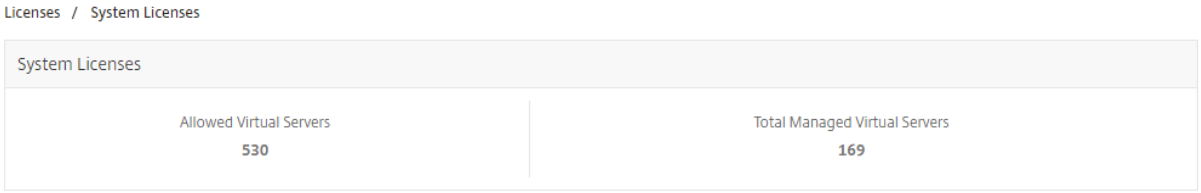


4. You can add more licenses from the License Settings page at any time.



Verification

You can verify the licenses installed on your NetScaler ADM by navigating to **Settings > Licensing & Analytics Configuration**.



Manage virtual servers

You can select the virtual servers or third-party virtual servers you want to manage and monitor through NetScaler ADM.

> **Points to note**
>
> - By default, NetScaler ADM automatically licenses the virtual servers randomly after each virtual server poll cycle.
> - If the total number of virtual servers discovered in your NetScaler ADM is lower than the number of installed virtual server licenses, NetScaler ADM, by default, licenses all the virtual servers.

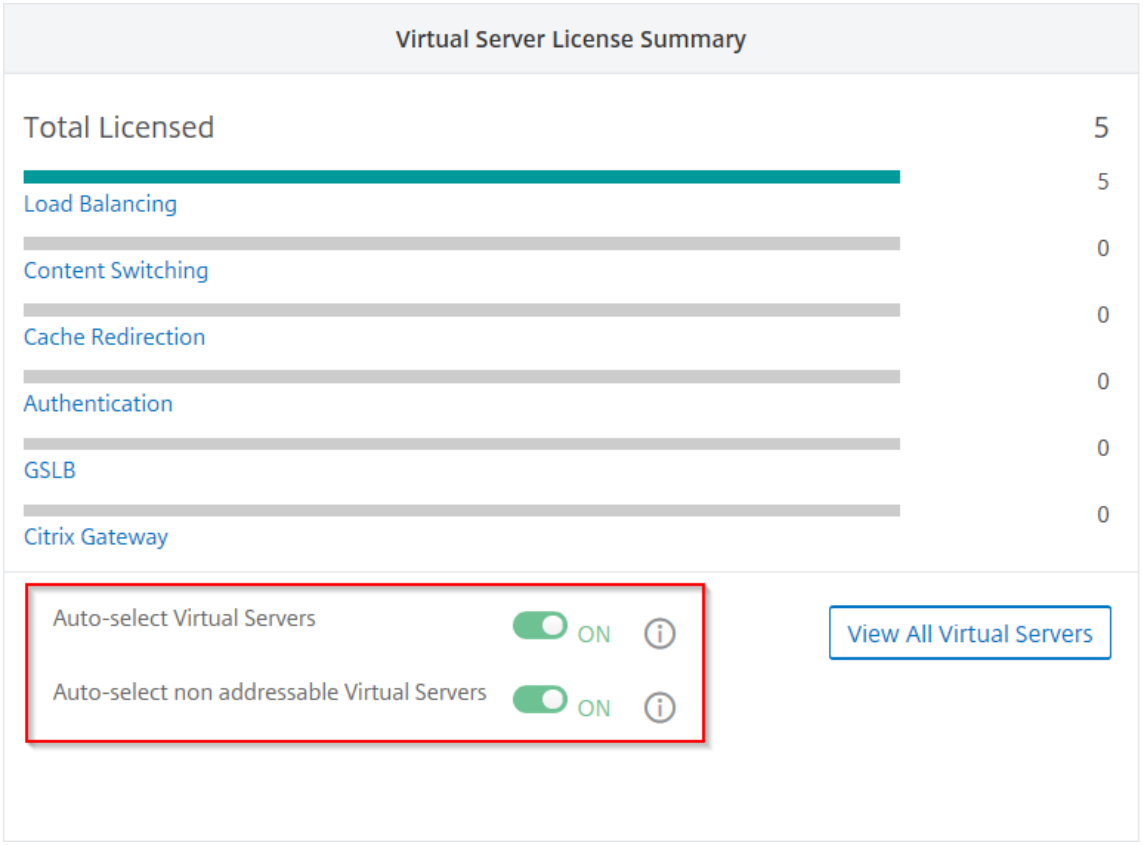
To select the virtual servers manually, or to restrict licensing to limited virtual servers, you have to first disable auto licensing the virtual servers, and then select the virtual servers you want to manage.

Disable auto-licensing virtual servers

1. Navigate to **Settings > Licensing & Analytics Configuration**.

   The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type, and license expiry information.

2. In **Virtual Server License Allocation**, disable **Auto Licensed Virtual Servers** and **Auto-select non addressable Virtual Servers**.

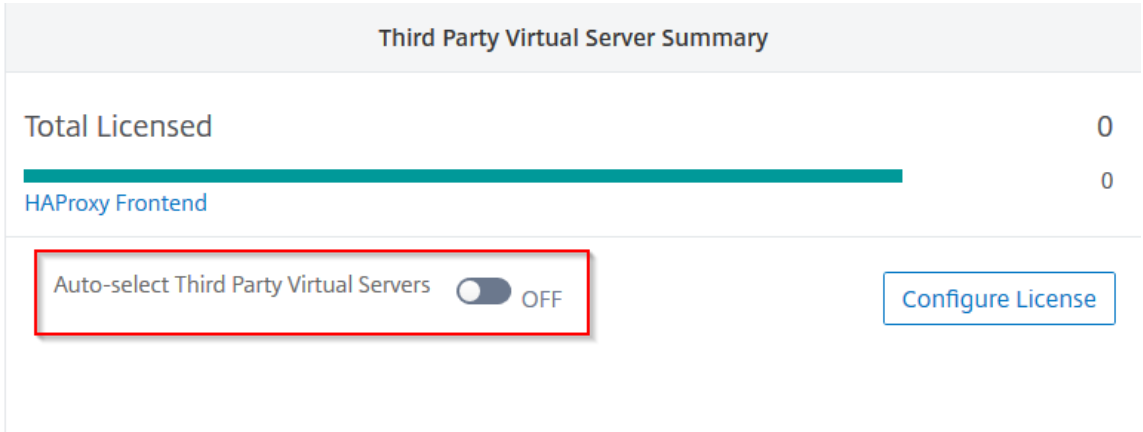


Select third-party virtual servers for licensing

1. Navigate to **Settings > Licensing & Analytics Configuration**.

   The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type, and license expiry information.

2. In **Third Party Virtual Server Summary**, disable **Auto-select Third Party Virtual Servers**.



Apply virtual server licenses manually

You can manually apply licenses to an individual virtual server.

1. In **Virtual Server License Allocation**, select **Configure Licenses**.

   The **All Vitrual Servers** page is displayed.
2. Filter unlicensed virtual servers using the property: `Licensed: No`.
3. Select the virtual server that you want to license.
4. Click **License**.

Configure policy based virtual server licensing

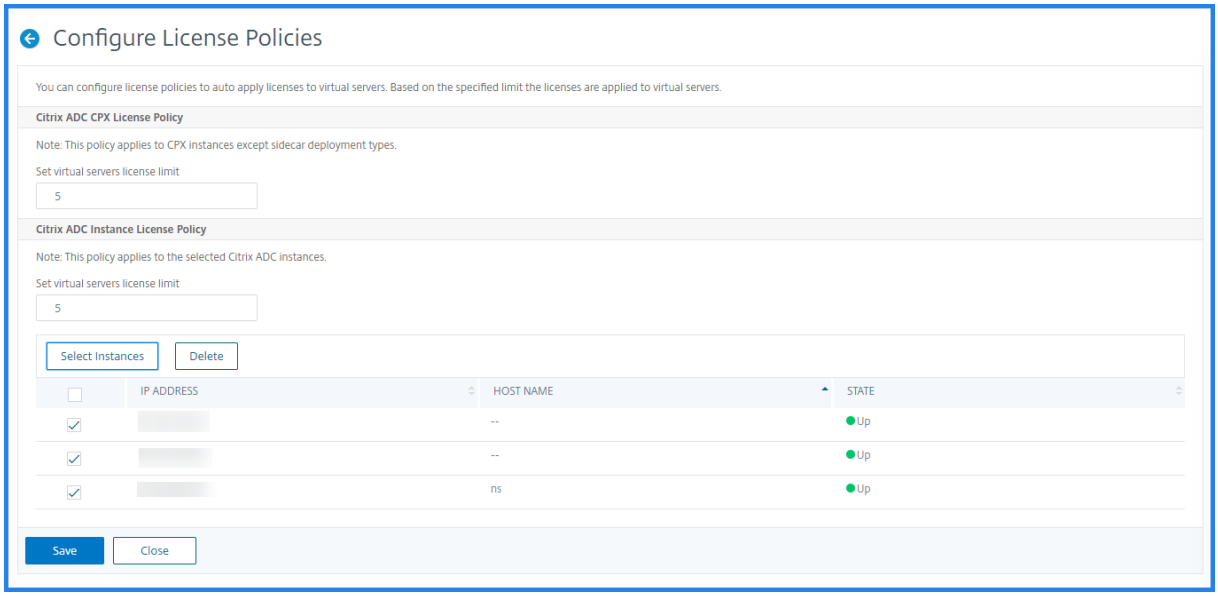
You can configure a policy to apply license to virtual servers. This policy controls the number of virtual servers that you want to auto-license. It also applies licenses to selected instances' virtual servers only.

Click **Edit Policies** and you can specify the following:

- Set virtual servers limit on CPX instances separately to apply licenses. The ADM applies license to virtual servers on CPX instances up to a specified limit.

  > **Important**
  >
  > This limit applies to CPX instances except sidecar deployment types.
  >
  > To view CPX instances of sidecar deployment types, filter the virtual servers using the property: `License Type: Freely Managed`.

- Set virtual servers limit on selected ADC instances (MPX/VPX/BLX) to apply licenses. The ADM applies licenses to virtual servers on ADC instances up to a specified limit.
- Select the priority ADC instances to apply virtual server licenses. Therefore, the ADM can apply license to selected instances' virtual servers only.



View the licensed virtual servers

After the licenses are applied to the virtual servers, you can view the licensed virtual servers or third-party virtual servers.

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Click the virtual server type in the **Total Licensed** section in the **Virtual Servers License Summary**.

Configure auto license support for non-addressable virtual servers

NetScaler ADM, by default, does not automatically apply licenses to non-addressable virtual servers. For licensing non-addressable virtual servers, you must disable the auto-license option and manually select the non-addressable virtual servers. This increases your effort to manually select the non-addressable servers initially when you apply the licenses. You also need to manually select the new non-addressable virtual servers whenever they are added to your network.

NetScaler ADM provides an option in NetScaler ADM under **Virtual Server License Allocation**. If you enable the **Auto-select non addressable Virtual Servers** option, automatically apply licenses non-addressable virtual servers.

> **Note**
>
> - NetScaler ADM, by default, still does not automatically select non-addressable virtual servers for licensing.

> - Application analytics (App Dashboard) is the only analytics supported currently on licensed non-addressable virtual servers.

Expiry Checks for virtual server licenses

You can now view the status of and set alerts for virtual server license expiry in NetScaler ADM.

To view the status of the licenses:

1. Navigate to **Infrastructure > Pooled Licensing > System Licenses.**
2. In the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
    - **Feature:** Type of license that is going to expire.
    - **Count:** Number of virtual servers or instances that are affected.
    - **Days to expiry:** Number of days remaining before expiry.

To configure the notification settings of licenses:

1. Navigate to **Infrastructure > Pooled Licensing > Settings**.
2. In the **Notification Settings** section, click the pencil icon and edit the parameters.
    - **Email profile:** Email profile or distribution list for sending notifications when licenses reach the threshold, or going to expire.
    - **SMS (Text Message):** SMS profile or distribution list for sending notifications when licenses reach the threshold, or going to expire.
    - **Slack** - Specify Slack profile details.
    - **PagerDuty alerts** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
    - **Notify me:** Set the percentage of pooled licenses to notify administrators by Email or SMS.
    - **License Expiry Threshold:** Number of days before the number of licenses determined by Alert Threshold expire.
    - **Expiry of licenses:** Number of days remaining before expiry.

System requirements

June 18, 2024

Before you install NetScaler Application Delivery Management (ADM), you must understand the software requirements, browser requirements, port information, license information, and limitations.

Requirements for NetScaler ADM

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs **Note:** Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.
Storage space	The default storage space required is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation. Use the sizing calculator mentioned in the **Maximum limits** section (page number 7) in the NetScaler ADM HA Deployment Guide. This guide is available at our download site, under **NetScaler MAS Release 12.1 > Earlier Versions**. **Note**: you need a Citrix account to access the deployment guide and sizing calculator. If your NetScaler ADM storage requirement exceeds 120 GB, you to have to attach an additional disk. You can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps

Requirements for NetScaler ADM on-prem agent

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual network interfaces	1
Throughput	1 Gbps

> **Note**
>
> AMD processor is supported in:
>
> - **NetScaler ADM 13.1 build 4.43 or later**.
> - **NetScaler agent 13.1 build 17.42 or later**.

Minimum NetScaler version required for NetScaler ADM features

> **Important**
>
> The NetScaler ADM version and build should be **equal to or higher** than your NetScaler version and build. For example, if you have installed NetScaler ADM 12.1 Build 50.39, then ensure you have installed NetScaler 12.1 Build 50.28/50.31 or earlier.

NetScaler ADM Feature	NetScaler Software Version
StyleBooks	10.5 and later
OpenStack/CloudStack Support	11.0 and later, if a partition is required
	11.1 and later, if partition on shared virtual LAN is required
NSX Support	11.1 Build 47.14 and later (VPX)
Mesos/Marathon Support	10.5 and later
Backup/Restore	For NetScaler, 10.1 and later
	For NetScaler SDX, 11.0 and later
Monitoring/Reporting and Configuration using Jobs	10.1 and later
Analytics Features	

NetScaler ADM Feature	NetScaler Software Version
Web Insight	10.5 and later
HDX Insight	10.1 and later
WAF Security Violations	11.0.65.31 and later
Gateway Insight	11.0.65.31 and later
Cache Insight	10.5 and later*
SSL Insight	12.0 and later

* Integrated Cache Metrics are not supported in NetScaler ADM with NetScaler instances running version 11.0 build 66.x.

Requirements for NetScaler ADM analytics

Minimum Citrix Virtual Apps and Desktops versions required for NetScaler ADM features

NetScaler ADM Feature	Citrix Virtual Apps and Desktops Version
HDX Insight	Citrix Virtual Apps and Desktops 7.0 and later

> **Note**
>
> The NetScaler Gateway feature (branded as Access Gateway Enterprise for versions 9.3 and 10.x) must be available on the NetScaler instance. NetScaler ADM does not support standalone Access Gateway Standard appliances.

NetScaler ADM can generate reports for applications that are published on Citrix Virtual Apps or Citrix Virtual Desktops and accessed through Citrix Workspace. However, this capability depends on the operating system on which Workspace is installed. Currently, a NetScaler does not parse ICA traffic for applications or desktops that are accessed through Citrix Workspace running on iOS or Android operating systems.

Thin clients supported for HDX insight

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux based Thin Clients

- Dell Wyse ThinOS based Thin Clients
- 10ZiG Ubuntu based Thin Clients
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

NetScaler instance license required for HDX insight

The data collected by NetScaler ADM for HDX Insight depends on the version and licenses of the NetScaler instances being monitored. HDX Insight reports are displayed only for NetScaler Premium and Advanced appliances running release 10.5 and later.

NetScaler License/Duration	5 Minutes	1 Hour	1 Day	1 Week	1 Month
Standard	No	No	No	No	No
Advanced	Yes	Yes	No	No	No
Premium	Yes	Yes	Yes	Yes	Yes

Supported hypervisors

The following table lists the hypervisors supported by NetScaler ADM.

Hypervisor	Versions
Citrix Hypervisor	7.1 and 7.4
VMware ESX	6.0, 6.5, 6.7, and 7.0
Microsoft Hyper-V	2012 R2 and 2016
Generic KVM	RHEL 7.4, RHEL 8.0, Ubuntu 16.04, and Ubuntu 18.04

Supported operating systems and Workspace versions

The following table lists the operating systems supported by NetScaler ADM, and the Citrix Workspace versions currently supported with each system:

Operating System	Workspace Version
Windows	4.0 Standard Edition
Linux	13.0.265571 and later
Mac	11.8, build 238301 and later
HTML5	1.5
Chrome App	1.5

Supported browsers

The following table lists the web browsers supported by NetScaler ADM:

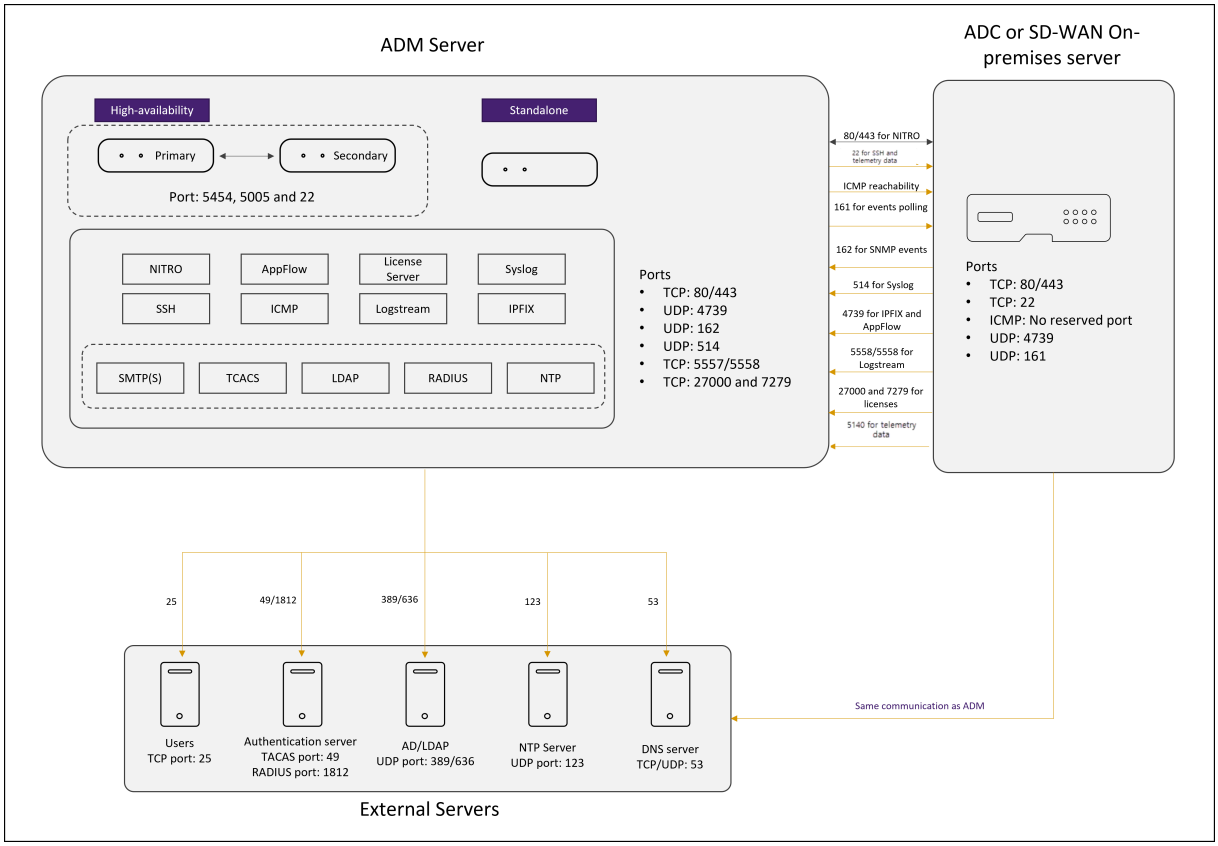
Web Browser	Version
Microsoft Edge	79 and later
Google Chrome	51 and later
Safari	10 and later
Mozilla Firefox	52 and later

Supported ports

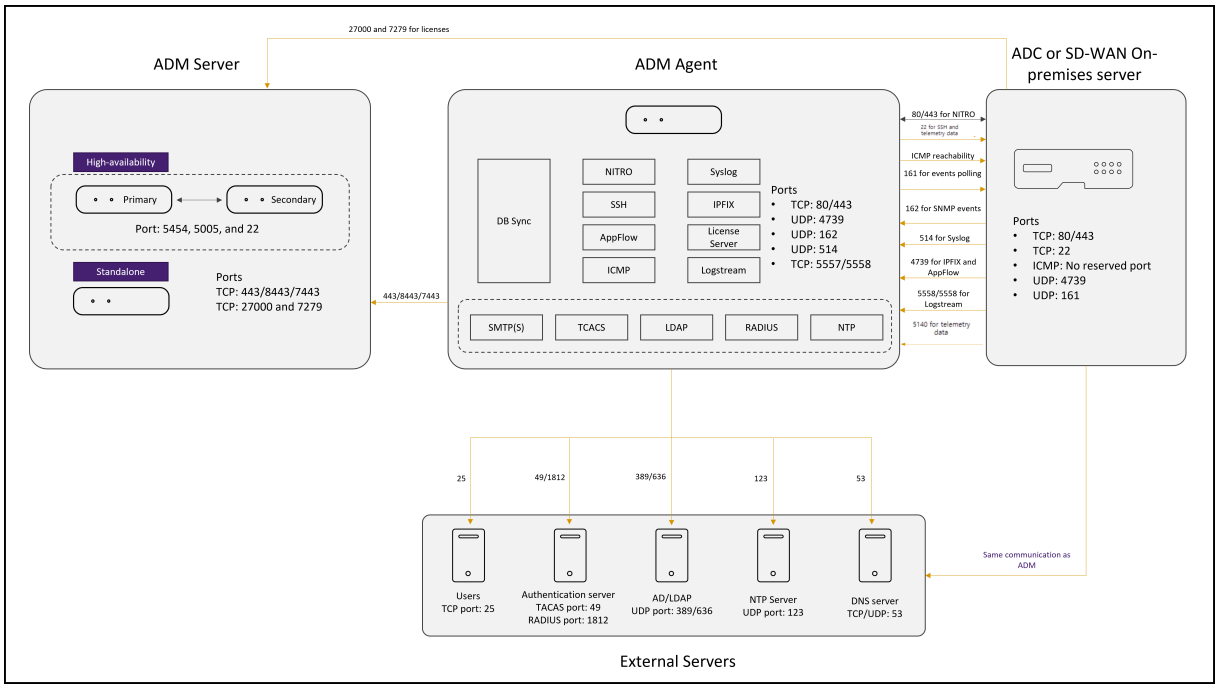
NetScaler ADM uses the NetScaler IP (known as NSIP) address to communicate with NetScaler. You can use ADM agent as an intermediary between the ADC instance and ADM. To establish a communication with these servers, open the required ports.

> **Note**
>
> If you have configured NetScalers in High Availability mode, NetScaler ADM uses NSIP to communicate with NetScaler and the required ports remain the same.

Network port diagram for agentless deployment:



Network port diagram for the deployment that includes ADM agent:



The following sections explain the required ports and their purpose:

- ADM server

- ADM agent
- ADC instance
- External servers

Ports for the ADM server

The following table explains the required ports that must be open on the ADM server.

Port	Type	Details	Direction of communication
80/443/5454/22	TCP	Default port for communication, and database synchronization in between NetScaler ADM nodes in high availability mode. **Note:** This port is also used for NetScaler telemetry.	NetScaler ADM primary node to NetScaler ADM secondary node
443/8443/7443	TCP	Port for communication between NetScaler agent and NetScaler ADM.	NetScaler agent initiates the communication with NetScaler ADM. Then, NetScaler ADM and agent interact with each other.
27000 and 7279	TCP	License ports for communication between NetScaler ADM license server and ADC instance. These ports are also used for ADC pooled licenses.	NetScaler to NetScaler ADM

Port	Type	Details	Direction of communication
5005	UDP	Port to exchange heartbeats between HA nodes.	NetScaler ADM primary node to secondary node. NetScaler ADM secondary node to primary node.
5140	UDP	Port to receive NetScaler Gateway telemetry data.	NetScaler to NetScaler Console

If the ADM and ADC instances are not using an agent for communication, ensure to open the following ports on the ADM server:

Port	Type	Details	Direction of communication
80/443	TCP	For NITRO communication from NetScaler ADM to NetScaler instance.	NetScaler agent to NetScaler and NetScaler to NetScaler agent
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent

Port	Type	Details	Direction of communication
5557/5558	TCP	For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from NetScaler to NetScaler ADM.	NetScaler to NetScaler ADM
5563	TCP	To receive ADC metrics (counters), system events, and Audit Log messages from NetScaler instance to NetScaler ADM	NetScaler to NetScaler ADM

Ports for the ADM agent

The following table explains the required ports that must be open on the ADM agent.

Port	Type	Details	Direction of communication
80/443	TCP	For NITRO communication from NetScaler ADM to NetScaler instance.	NetScaler agent to NetScaler and NetScaler to NetScaler agent
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent

Port	Type	Details	Direction of communication
5557/5558	TCP	For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from NetScaler to NetScaler ADM.	NetScaler to NetScaler ADM

Ports for ADC instances

The following table explains the required ports that must be open on NetScaler instances.

Port	Type	Details	Direction of communication
80/443	TCP	For NITRO communication from NetScaler ADM to NetScaler instance. For NITRO communication between NetScaler ADM servers in high availability mode.	NetScaler ADM to NetScaler and NetScaler to NetScaler ADM
22	TCP	For SSH communication from NetScaler ADM to NetScaler instance. For synchronization between NetScaler ADM servers deployed in high availability mode. And, this port is required for the SSH communication between the ADM agent and NetScaler.	NetScaler ADM to NetScaler. Or, NetScaler agent to NetScaler.

Port	Type	Details	Direction of communication
No reserved port	ICMP	To detect network reachability between NetScaler ADM and NetScaler instances, or the secondary NetScaler ADM server deployed in high availability mode.	NetScaler ADM to NetScaler
161	UDP	To poll events from ADC instances.	NetScaler ADM to NetScaler

Ports for ADC built-in agent

The following table explains the required ports that must be open for NetScaler built-in agent.

Port	Type	Details	Direction of communication
443	TCP	For all communication from NetScaler ADM to NetScaler built-in agent	NetScaler ADM to NetScaler built-in agent and NetScaler built-in agent to NetScaler ADM

> **Note:**
>
> In ADM high-availability deployment, all communications from ADM use the primary node IP address.

Ports for external servers

The following table explains the required ports that must be open on external servers:

Port	Type	Details	Direction of communication
25	TCP	To send SMTP notifications from NetScaler ADM to users.	NetScaler ADM to users.
389/636	TCP	Default port for authentication protocol. For communication between NetScaler ADM and LDAP external authentication server.	NetScaler ADM to LDAP external authentication server
123	UDP	Default NTP server port for, synchronizing with multiple time sources.	NetScaler ADM to NTP server
1812	RADIUS	Default port for authentication protocol. For communication between NetScaler ADM and RADIUS external authentication server.	NetScaler ADM to RADIUS external authentication server
49	TACACS	Default port for authentication protocol. For communication between NetScaler ADM and TACACS external authentication server.	NetScaler ADM to TACACS external authentication server

Limitations

From NetScaler ADM 12.1 or later, the following features support IPv6 format of IP addresses:

1. Management access for NetScaler ADM GUI
2. Management access for NetScaler
3. Registration and inventory
4. Network dashboard
5. SSL dashboard
6. Config jobs
7. Config audit
8. Network functions
9. Network reporting
10. Backup and restore of ADC instances
11. SNMP events from NetScalers

The following features do not support IPv6:

1. High availability floating IP
2. Syslogs received from ADCs that support IPv6
3. StyleBooks on ADCs that support IPv6
4. Analytics
5. Pooled licensing

Getting started

March 11, 2024

This document walks you through how to get started with deploying and setting up NetScaler Application Delivery Management (ADM) for the first time. This document is intended for network and application administrators who manage Citrix network devices (NetScaler and NetScaler Gateway). Follow the steps in this document irrespective of the type of device you plan to manage using NetScaler ADM.

If you are an existing user of NetScaler ADM, you are recommended to review the release notes, system requirements, and licensing details before upgrading your server to the latest release of NetScaler ADM.

Step 1 - Review the system requirements

Before you begin deploying NetScaler ADM in your data center, review the software requirements, browser requirements, port information, license information, and limitations.

- **License information**. You can manage and monitor any number of instances and entities without a license. However, you can only manage 30 discovered apps and view analytics information for only two virtual servers without applying a license. To manage more than 30 apps or to view analytics for more than two virtual servers, you must purchase appropriate licenses. Learn More.
- **Operating system and receiver requirements**. Review this information to make sure you have the correct receiver version for the supported operating systems. Learn More.
- **Browser requirements**. To access NetScaler ADM GUI, you must make sure you have the required browser and the correct version. Learn More.
- **Ports**. Make sure that the required ports are open for NetScaler ADM to communicate with NetScaler instances. Learn More.
- **NetScaler instance requirements**. Different NetScaler ADM features are supported on different NetScaler software versions. Review this information to make sure you have upgraded your NetScaler instances to the correct version. Learn More.

Step 2 - Deploy NetScaler ADM

To manage and monitor the applications and network infrastructure, you must first install NetScaler ADM on one of the hypervisors. You can deploy NetScaler ADM either as a single server or in a high availability mode. If you are using NetScaler Insight Center, you can migrate to NetScaler ADM and avail of the management, monitoring, orchestration, and application management features in addition to the analytics features.

- **Single-server deployment**. In a NetScaler ADM single server deployment, the database is integrated with the server and a single server processes all the traffic. You can deploy NetScaler ADM with Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, and Linux KVM. See:
  - NetScaler ADM with Citrix Hypervisor
  - NetScaler ADM with Microsoft Hyper-V
  - NetScaler ADM with VMware ESXi
  - NetScaler ADM with Linux KVM server
- **High availability deployment.** A high availability deployment (HA) of two NetScaler ADM servers provides uninterrupted operations. In a high availability setup, both the NetScaler ADM

nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have the same configurations. With HA deployment the ability to configure the floating IP address on the NetScaler ADM primary node eliminates the need of a separate NetScaler load balancer. To learn more, see Configure in high availability deployment.

Step 3 - Add instances to NetScaler ADM

Instances are NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler ADM. You must add instances to the NetScaler ADM server if you want to manage and monitor these instances. You can add the following instances to NetScaler ADM:

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

When you add an instance to the NetScaler ADM server, the server implicitly communicates with the instances and collects an inventory of these instances.

Learn More

Step 4 - Enable analytics on virtual servers

To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.

Learn More

Step 5 - Configure NTP server on NetScaler ADM

You have to configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

Learn More

Step 6 - Configure system settings for optimal NetScaler ADM performance

Before you start using NetScaler ADM to manage and monitor your instances and applications, it is recommended that you configure a few system settings that ensure optimal performance of your NetScaler ADM server.

- **Configure system alarms**. Configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server.
- **Configure system notifications**. You can send notifications to select groups of users for various system-related functions. You can set up a notification server in NetScaler ADM, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. This ensures that you are notified of any system-level activities such as user login or system restart.
- **Configure system prune settings**. To limit the amount of reporting data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).
- **Configure system backup settings**. NetScaler ADM automatically backs up the system every day at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system.
- **Configure instance backup settings**. If you back up the current state of a NetScaler instance, you can use the backup files to restore stability in case the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.
- **Configure instance event prune settings**. To limit the amount of event messages data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).
- **Configure instance syslog purge settings**. To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler ADM:
  - Generic Syslog data
  - AppFirewall data
  - NetScaler Gateway data.

  Learn More

What's next

After you have deployed and set up NetScaler ADM, you can start managing and monitoring your instances and applications.

Managing NetScaler instances and applications. All NetScaler ADM features are supported on NetScaler instances. You can start using any of the features.

Deploy

December 31, 2023

Before using NetScaler Console to manage and monitor your applications and network infrastructure, you must first install it on one of the hypervisors or on a Kubernetes cluster. If you deploy NetScaler Console on a hypervisor, you can deploy it either as a single server or in a high-availability mode. High availability mode not is applicable on a Kubernetes cluster. If you are using NetScaler Insight Center, you can migrate to it NetScaler Console and avail of the management, monitoring, orchestration, and application management features in addition to the analytics features.

- **Single-server deployment**: For a standalone ADM deployed on a hypervisor, the database is integrated with the server and a single server processes all the traffic. You can deploy NetScaler Console with Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, and Linux KVM. See:
  - NetScaler Console on Citrix Hypervisor
  - NetScaler Console on Microsoft Hyper-V
  - NetScaler Console on VMware ESXi
  - NetScaler Console on Linux KVM server
  - NetScaler Console on Kubernetes Cluster
- **High availability (HA) deployment**: An HA deployment of two NetScaler Console servers provides uninterrupted operations. In an HA setup, both the NetScaler Console nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have same configurations. With HA deployment the ability to configure the floating IP address on the NetScaler Console primary node eliminates the need for a separate NetScaler load balancer. See: Configure in high availability deployment.

> Note
>
> High availability is not applicable for ADM deployed on a Kubernetes cluster.

- **Migrate from NetScaler Insight Center to NetScaler Console**: You can migrate your NetScaler Insight Center deployment to NetScaler Console without losing the existing configuration, settings, or data. With NetScaler Console you can not only view the various analytics generated by the NetScaler, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console. See: Migrating from NetScaler Insight Center to NetScaler Console
- **Integrate NetScaler Console with Director**: Director integrates with NetScaler Console for network analysis and performance management. See: Integrate NetScaler Console with Director

Prerequisites for installing NetScaler ADM

March 11, 2024

You can download and install NetScaler Application Delivery Management (ADM) for Microsoft HyperV, VMware ESXi, Linux KVM, and Citrix Hypervisor platforms as a virtual appliance. Before you install NetScaler ADM, you must understand the software requirements, browser requirements, port information, license information, and limitations on all these platforms.

For specific platform requirements and detailed steps to install NetScaler ADM, see the following topics:

- NetScaler ADM with Citrix Hypervisor
- NetScaler ADM with Microsoft HyperV
- NetScaler ADM with VMware ESXi
- NetScaler ADM with Linux KVM server

General requirements for NetScaler ADM

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	Citrix recommends using Solid State Drive (SSD) technology for NetScaler ADM deployments.

Component	Requirement
	The default storage space required is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation. Use the sizing calculator mentioned in the **Maximum limits** section (page number 7) in the NetScaler ADM HA Deployment Guide. This guide is available at our download site, under **NetScaler MAS Release 12.1 > Earlier Versions**. **Note**: you need a Citrix account to access the deployment guide and sizing calculator If your NetScaler ADM storage requirement exceeds 120 GB, you to have to attach an extra disk. Citrix recommends you to estimate storage and attach an extra disk at the time of initial deployment. You can add only one extra disk. For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps

> Note:
>
> Citrix recommends you to host the NetScaler ADM VHD on a local storage. When hosted on storage devices in a SAN, NetScaler ADM might not work as expected. So, ADM deployment on SAN is not supported.

NetScaler ADM on Citrix Hypervisor

March 11, 2024

To install NetScaler ADM on Citrix Hypervisor (formerly known as XenServer), you need to first download the NetScaler ADM .xva image file to your local computer. You need to use Citrix XenCenter to perform the NetScaler ADM installation.

> **Note:**
>
> NetScaler ADM does not support XenMotion.

Prerequisites

Before installing NetScaler ADM, verify that the following requirements have been met:

- Citrix Hypervisor version 7.1 or later is installed on hardware that meets the minimum requirements.
- XenCenter is installed on a management workstation that meets the minimum requirements. You have to use XenCenter to install NetScaler ADM on Citrix Hypervisor.
- You have downloaded the NetScaler ADM .XVA image file.

XenCenter system requirements

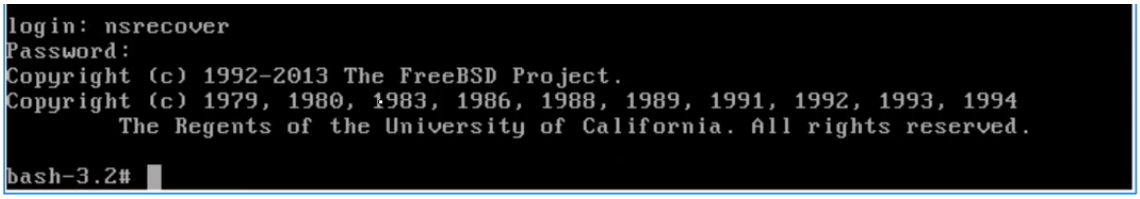
XenCenter is a Windows client application. It cannot run on the same machine as the Citrix Hypervisor host. The following table describes the minimum system requirements.

Component	Requirement
Operating System	Windows 7, Windows Server 2003, or Windows 10
.NET framework	Version 2.0 or later
CPU	750 MHz (MHz), Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB, Recommended: 2 GB
NIC	100 megabits per second (Mbps) or faster NIC

Install NetScaler Application Delivery Management

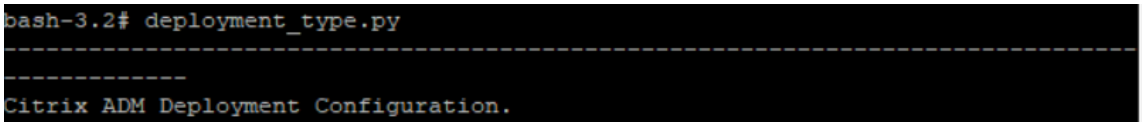
1. Import the XVA image file to your Citrix Hypervisor, and from the **Console** tab configure the initial network configuration options.

2. After specifying the required IP addresses, save the configuration settings.
3. When prompted, log on using nsrecover/nsroot credentials.

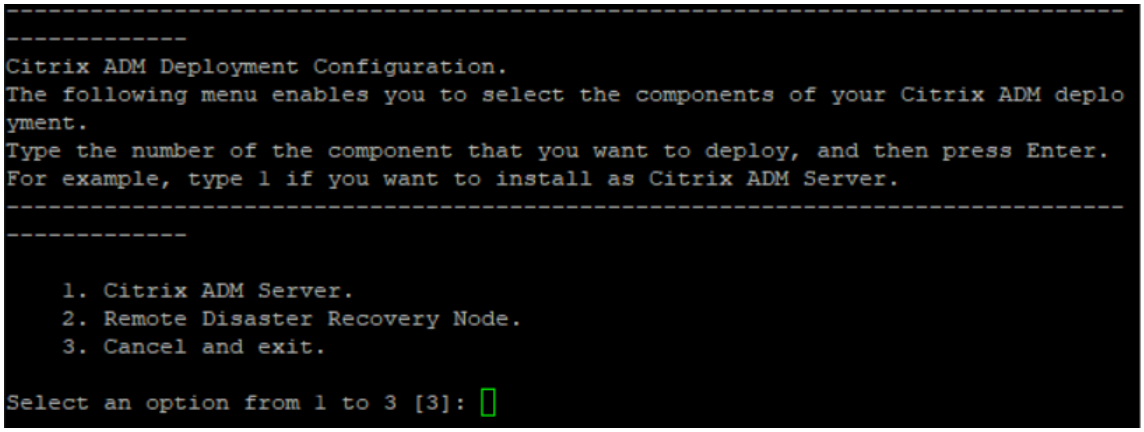


> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

4. Run the deployment script by typing the command at the shell prompt: `/mps/deployment_type.py`



5. Select the deployment type as **NetScaler ADM Server**. If you do not select any option, by default, it is deployed as a server.



6. Type **Yes** to deploy NetScaler ADM as a standalone deployment.
7. Type **Yes** to restart the NetScaler ADM server.

> **Note**
>
> After you install NetScaler ADM, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler ADM server in the web browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler ADM configuration utility.

NetScaler ADM on Microsoft Hyper-V

March 11, 2024

To install NetScaler ADM on Microsoft Hyper-V, you must first download the NetScaler ADM image file to your local computer. Also, ensure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available.

Prerequisites

Before installing the NetScaler ADM virtual appliance, verify that the following requirements have been met:

- Microsoft Hyper-V version 6.2 or later is installed on hardware that meets the minimum requirements.
- Install Microsoft Hyper-V Manager on a management workstation that meets the minimum system requirements.
- You have downloaded the NetScaler ADM image file.

Microsoft Hyper-V system requirements

Microsoft Hyper-V is a Windows client application. The following table describes the minimum system requirements.

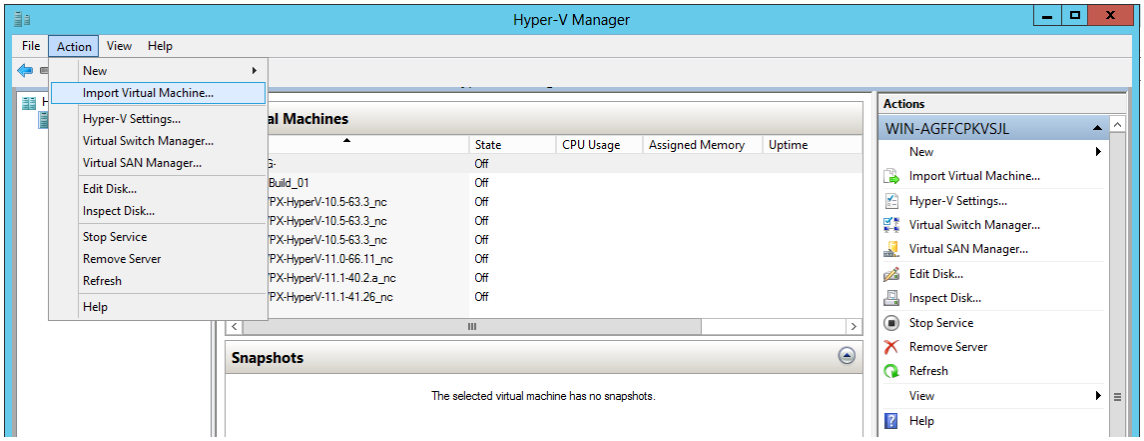
Component	Requirement
Operating System	Windows Server 2012 R2
.NET framework	Version 2.0 or later
CPU	750 MHz (MHz), Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB, Recommended: 2 GB
NIC	100 megabits per second (Mbps) or faster NIC

Installing NetScaler Application Delivery Management

The number of NetScaler ADM servers that you can install depends on the memory available on the Hyper-V server.

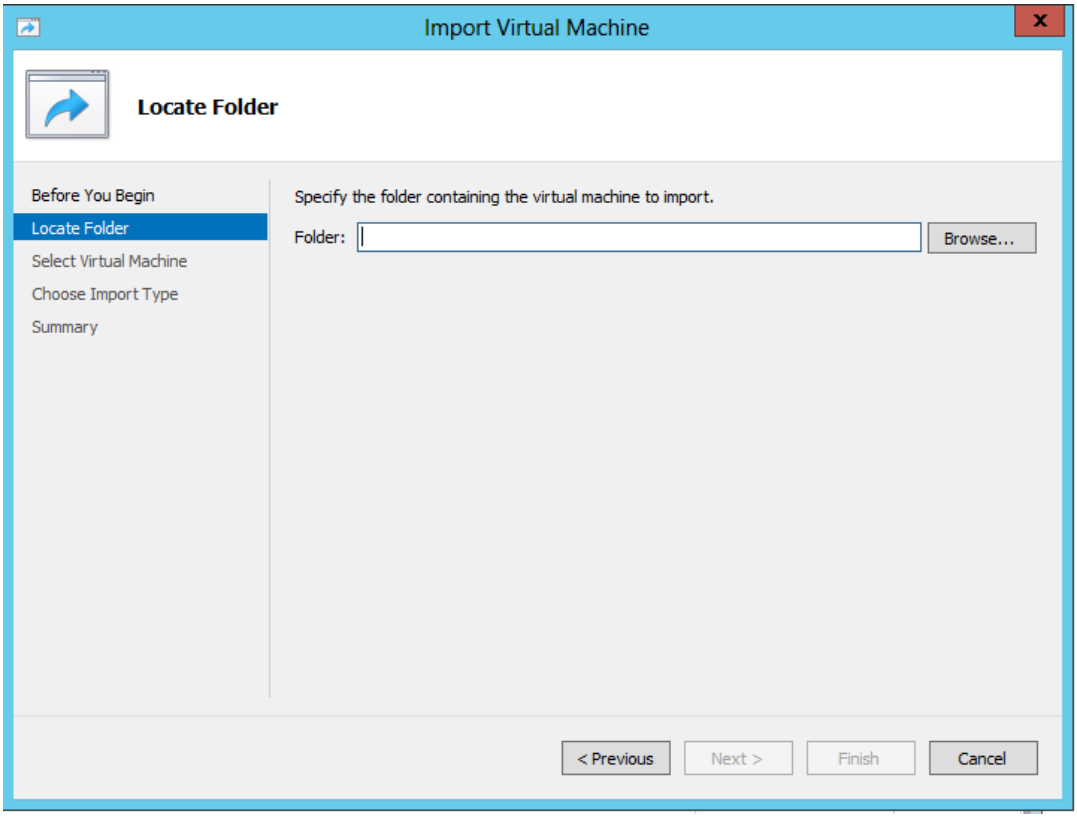
To install NetScaler ADM:

1. Start the Hyper-V Manager client on your workstation.
2. On the **Action** menu, click **Import Virtual Machine**.



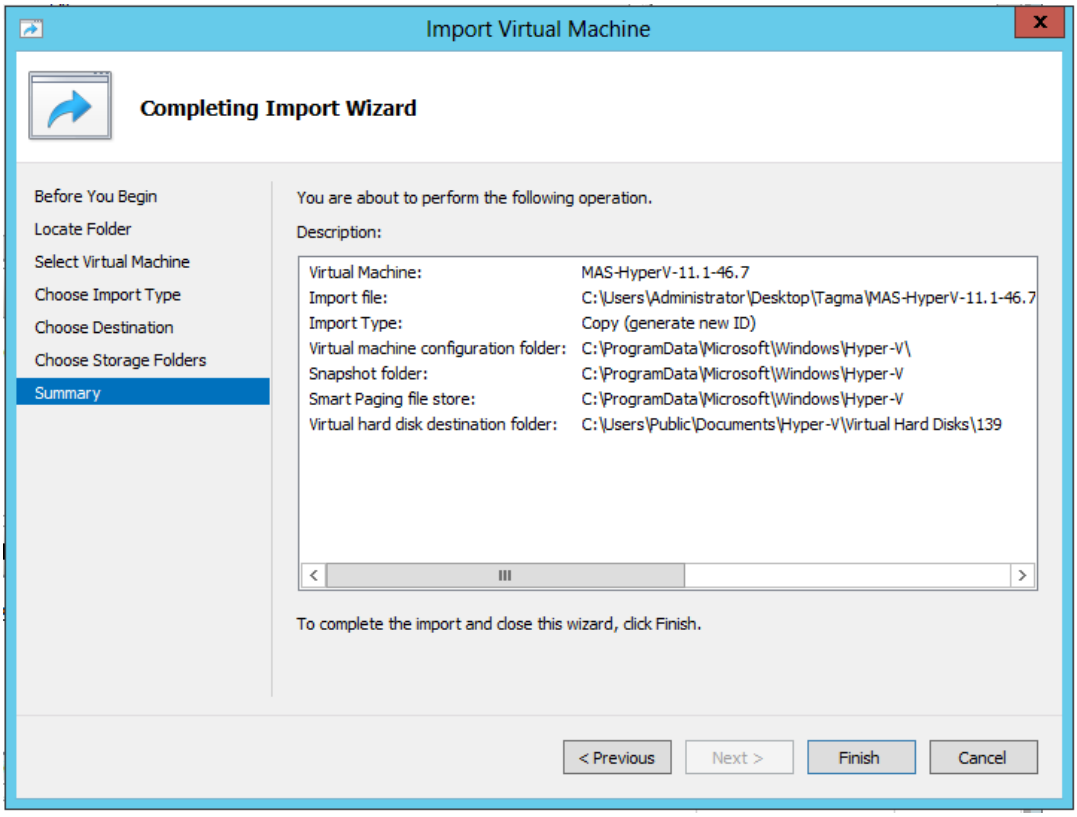
3. Import the Hyper-V image, and do the following:
   a) In the Import Virtual Machine dialog box, in **Locate Folder** section, browse to the folder in which you saved the NetScaler ADM Hyper-V image, select the folder, and click **Next**.
   b) In the Select virtual machine section, select the appropriate virtual machine name.
   c) In the **Choose Import Type** section, select Copy the virtual machine (create a new unique ID) option and click Next.
   d) In the **Choose Destination** section, you can specify the folders to store the virtual machine files.

> **Note**
>
> By default the wizard imports the virtual machine files to default Hyper-V folders on your local host.



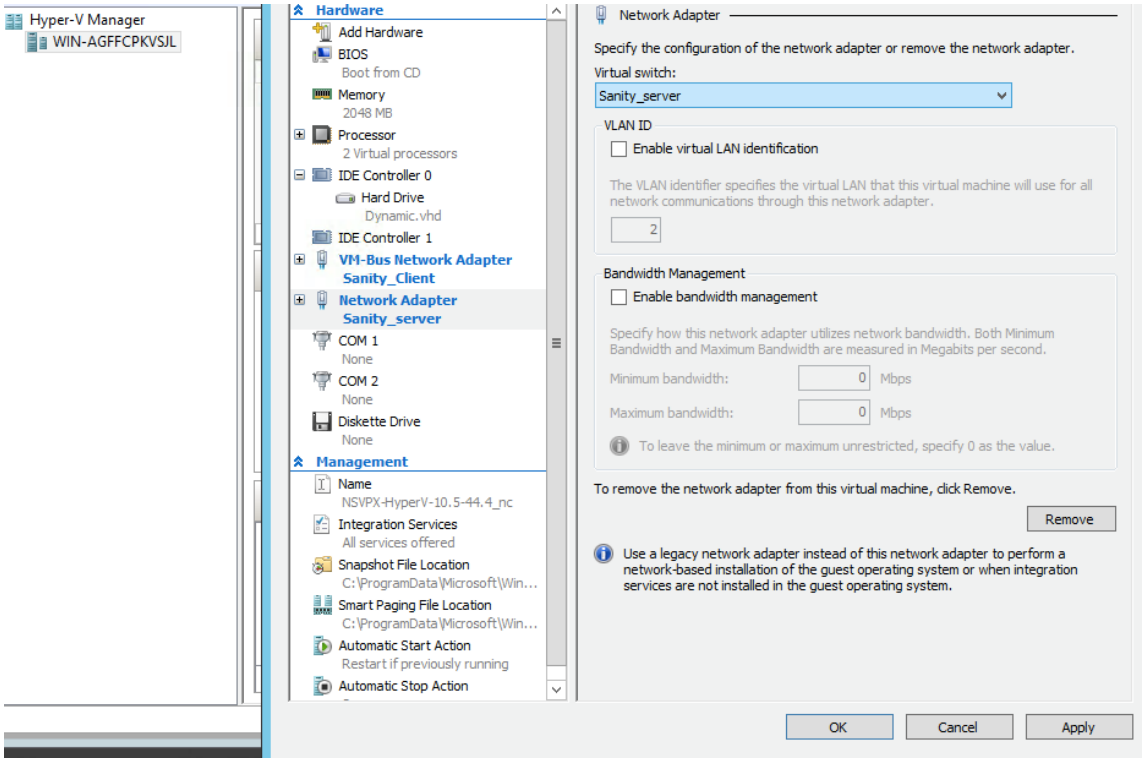
e) In the **Choose Storage Folders** section, you can select the location in which you want to store the virtual hard disks, and then click **Next**.

f) You can verify the Virtual Machine details in the summary pane, click **Finish**.

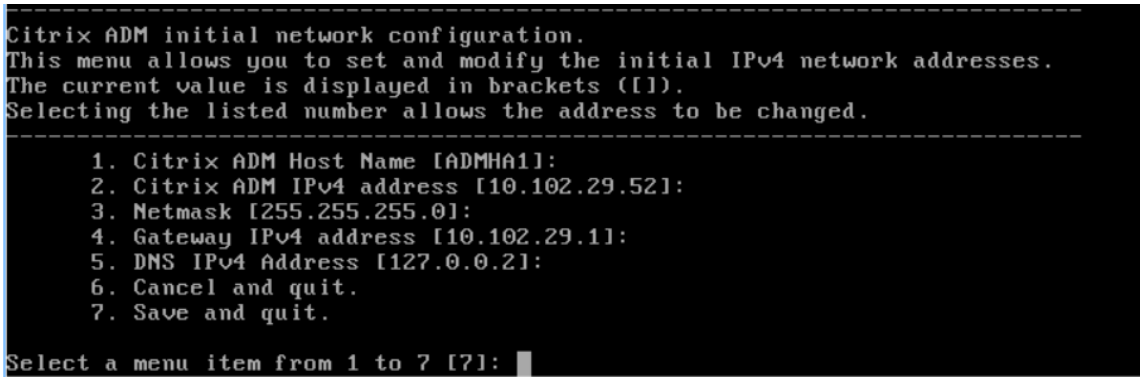


The NetScaler ADM Hyper-V image is displayed in the right pane.

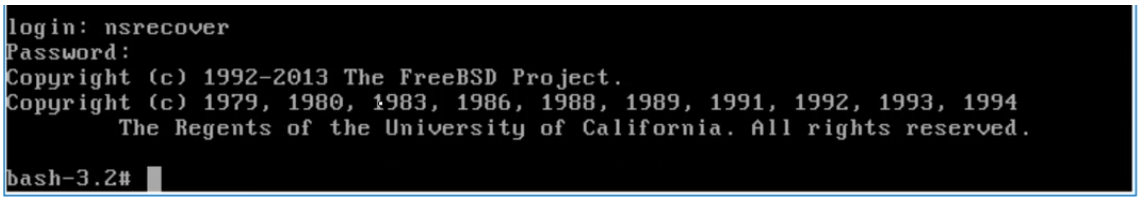
4. Right-click the NetScaler ADM Hyper-V image, and then click **Settings**.
5. In the left pane of the dialog box that appears, navigate to **Hardware** > **VM_Bus Network Adaptor**, and in the right pane, from the Network list, select the appropriate network.



6. Click **Apply**, and then click **OK**.
7. Right-click the NetScaler ADM Hyper-V image and click **Connect**.
8. On the Console window, click **Start** button.
9. Configure the initial network configuration options.



10. After specifying the required IP addresses, save the configuration settings.
11. When prompted, log on using nsrecover/nsroot credentials.



> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

12. Run the deployment script by typing the command at the shell prompt:

```
deployment_type.py
<!--NeedCopy-->
```

```
bash-3.2# deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. Select the deployment type as **NetScaler ADM Server**. If you do not select any option, by default, it is deployed as a server.

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. Type **Yes** to deploy NetScaler ADM as a standalone deployment.
15. Type **Yes** to restart the NetScaler ADM server.

> **Note**
>
> After you install NetScaler ADM, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler ADM server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler ADM configuration utility.

NetScaler ADM on VMware ESXi

March 11, 2024

This document describes how to install NetScaler ADM virtual appliances on VMware ESXi, using the VMware vSphere client.

Prerequisites

Before you begin installing a virtual appliance, verify that the following requirements:

- Install a supported VMware ESXi version (6.0, 6.5, 6.7, and 7.0).
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Download the NetScaler ADM setup files.

> Note
>
> - VMotion is supported only from **NetScaler ADM 13.0 Build 47.22 or later**. You can schedule and automate migration of the ADM server deployed on an ESXi hypervisor, including vSphere high availability and vSphere DRS setups.
> - VMware Tools for NetScaler ADM are delivered as part of the software build and they cannot be upgraded or modified separately.

To install NetScaler ADM

Follow these steps to install an ADM virtual appliance on VMware ESXi.

> **Note**
>
> The steps and screen captures are based on VMware ESXi version 6.0. The GUI might differ in other ESXi versions. VMware ESXi version 7.0.1c build number 17325551 with VMXNET3 adapter is supported in **NetScaler ADM 13.0 71.40 or later**. Refer to the VMware documentation for version-specific steps.

1. Start the VMware vSphere client on your workstation.
2. In the **IP address / Name** text box, type the IP address of the VMware ESXi server that you want to connect to.
3. In the **User Name** and **Password** text boxes, type the administrator credentials, and then click **Login**.

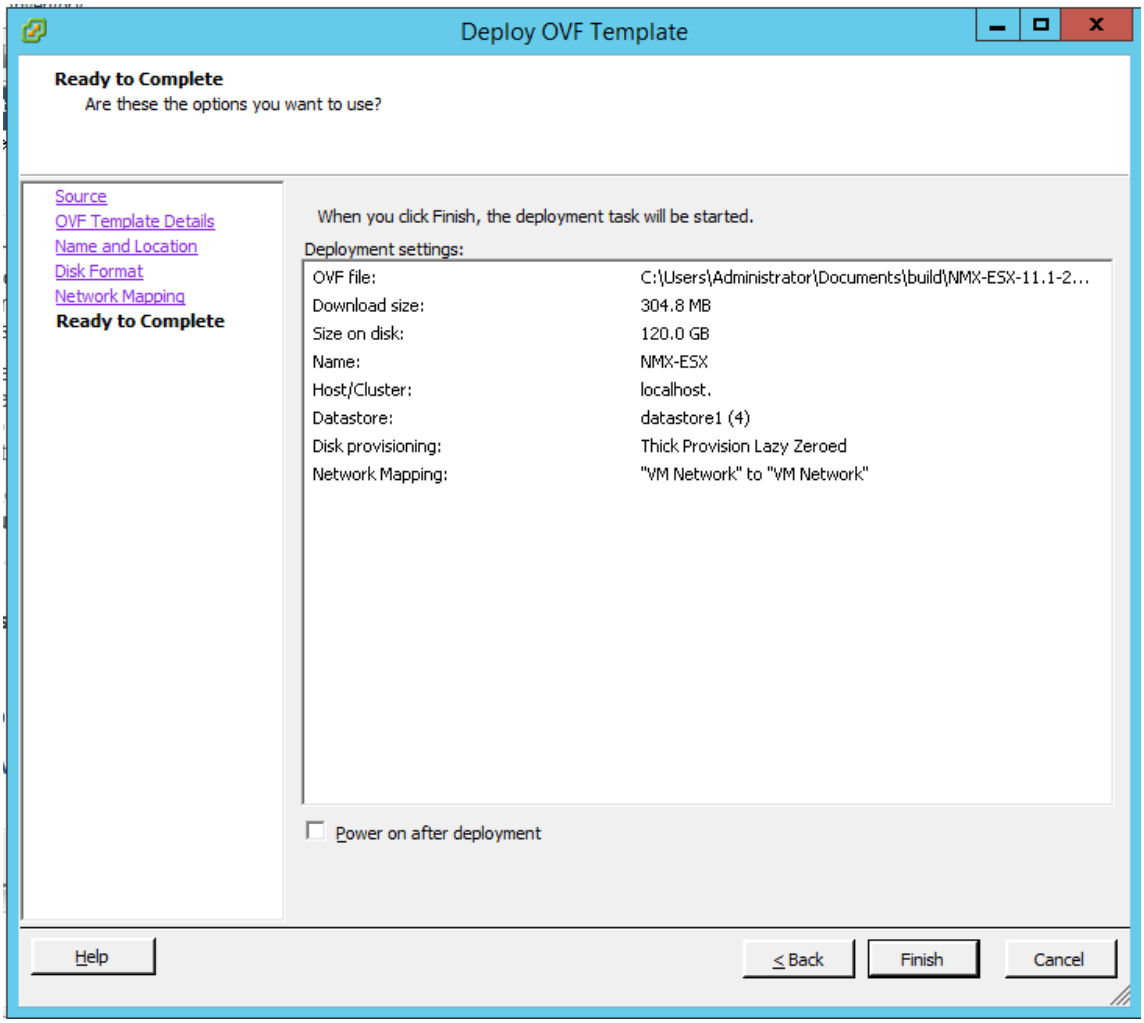
4. On the **File** menu, click **Deploy OVF Template**.
5. In the **Deploy OVF Template** dialog box, in **Deploy from a file or URL**, select the .ovf file, and click **Next**.

   > **Note**
   >
   > If a warning message appears with the following text: "The operating system identifier is not supported on the selected host, check to see if the VMware server supports the FreeBSD operating system."Click **Yes**.

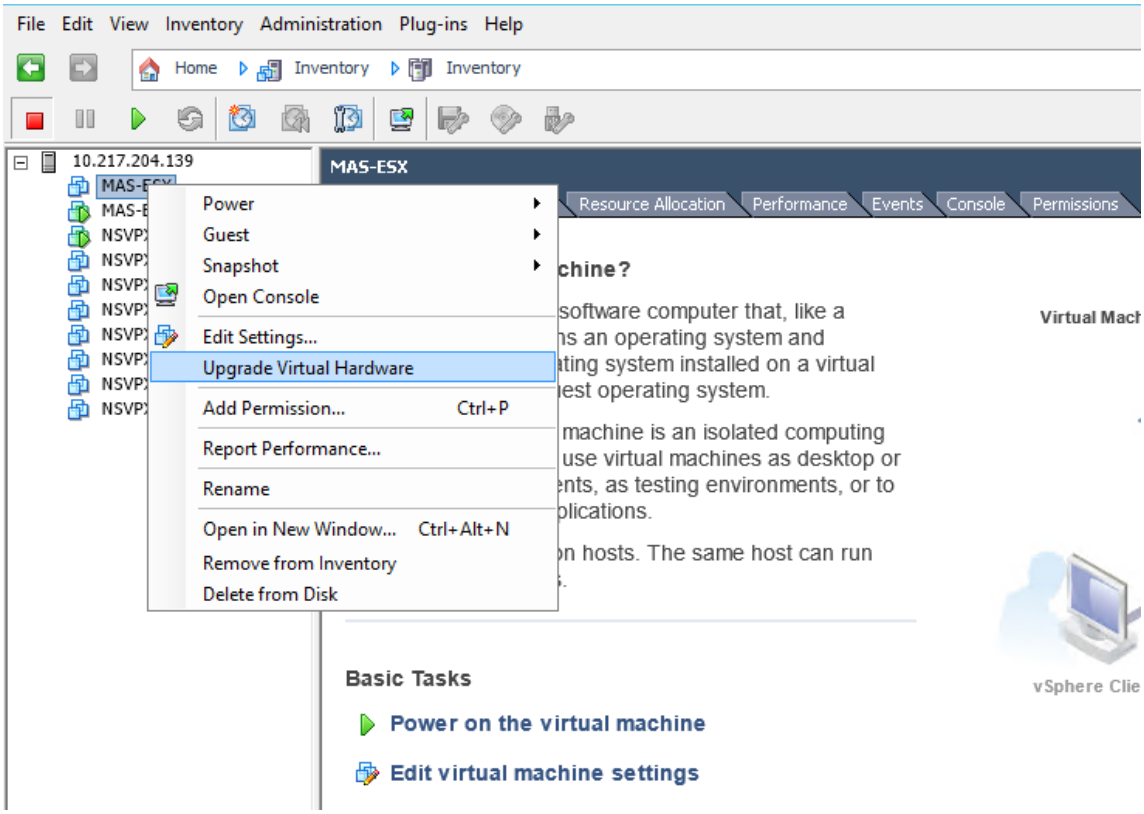
6. On the **OVF Template Details** page, click **Next**.
7. Type a name for the NetScaler ADM virtual appliance, and then click **Next**.
8. Specify the Disk Format by selecting either Thin provisioned format or Thick provisioned format.

   > **Note**
   >
   > Citrix recommends that you select **Thick provisioned format**.

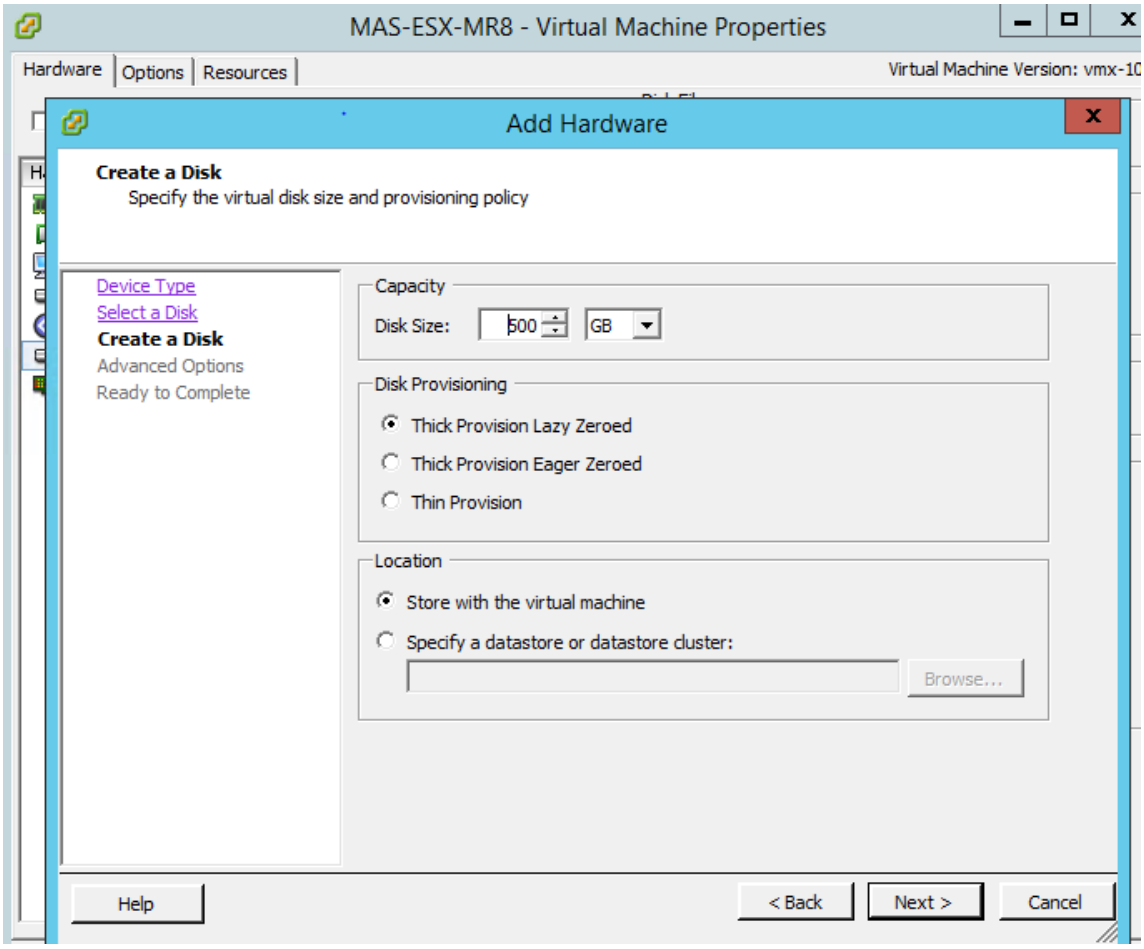
9. Click **Finish** to start the installation process.



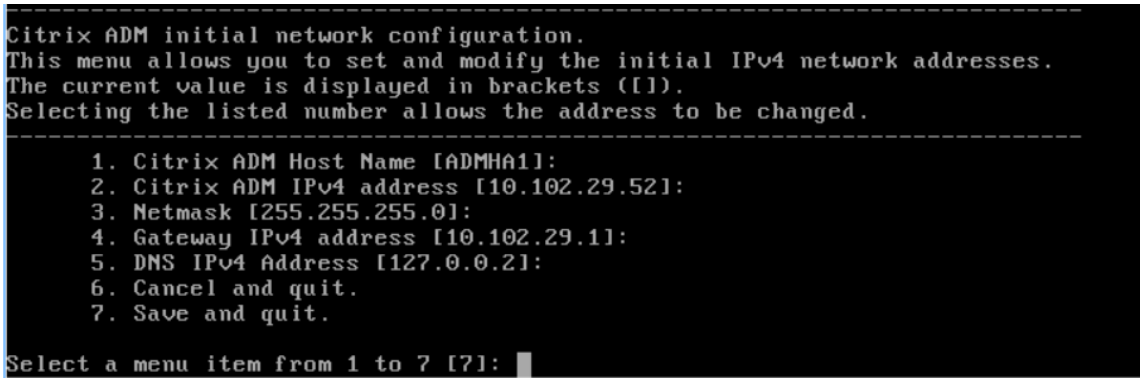
10. You are now ready to start the NetScaler ADM virtual appliance.
11. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, right-click on the **Virtual Machine**, and then click **Upgrade Virtual Hardware**. In the **Confirm Virtual Machine** dialog box, click **Yes**.



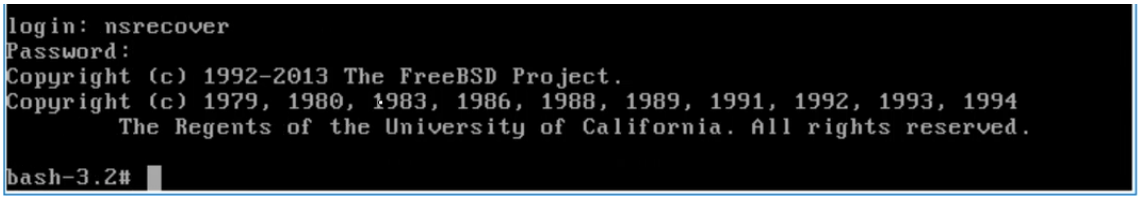
12. In the **Inventory** menu, click **Virtual Machine**, and then click **Edit Settings**.
13. In the **Virtual Machine Properties** dialog box, on the **Hardware** tab, click **Memory**, and then in the right pane specify the **Memory Size** as 32 GB.
14. Click **CPUs**, and then in the right pane, specify the CPUs as 8. Click **OK**.
15. Add an extra disk as per your requirement.



16. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, click **Virtual Machine**, click **Power**, and then click **Power On**.
17. Click the **Console** tab to display the NetScaler ADM Initial Network Configuration options.



18. After specifying the required IP addresses, save the configuration settings.
19. When prompted, log on using nsrecover/nsroot credentials.



> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

20. Run the deployment script by typing the command at the shell prompt:

```
deployment_type.py
<!--NeedCopy-->
```

21. Select the deployment type as **NetScaler ADM Server**. If you do not select any option, by default, it is deployed as a server.

22. Type **Yes** to deploy NetScaler ADM as a standalone deployment.
23. Type **Yes** to restart the NetScaler ADM server.

> **Note**
>
> After you install NetScaler ADM, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler ADM server in the browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler ADM configuration utility.

> **Note**
>
> Typical ADM installation time is around 10 minutes on VMware ESXi but might take longer on some systems.

Automate deployment of NetScaler agent on VMware ESXi

March 11, 2024

NetScaler ADM allows you to automate the deployment of NetScaler agents on VMware ESXi.

As an admin, you can automate the following actions:

- Configure the NetScaler agent
- Register the NetScaler agent and change the default password of the agent.

Configure the NetScaler agent

To automate the configuration of the agent, add the values for the following parameters in the .ovf file:

1. IPAddress
2. Netmask
3. Gateway
4. Nameserver
5. Hostname

> **Note**
>
> The .ovf file is available in the agent image file. To download the NetScaler agent file, go to https://www.citrix.com/downloads/citrix-application-management/. The naming pattern of the agent image file is as follows, **MASAGENT-ESX-releasenumber-buildnumber.zip**

Register the NetScaler agent and change the default password

> **Note**
>
> Before registering and changing the default password, make sure that you have added the parameters specified in Configure the NetScaler agent.

To automate the registering of the NetScaler agent and changing of the default password, add the values for the following parameters in the same .ovf file:

1. ADM Server IP
2. ADM Username
3. ADM Password
4. Agent New Password

Prerequisites

Before you begin installing a virtual appliance, make sure you:

- Install VMware vSphere 8.x on a management workstation that meets the minimum system requirements.
- Download the NetScaler ADM setup files.

How to configure and register a NetScaler agent

1. Download and edit the .OVF file
2. Install NetScaler ADM virtual appliance on VMware ESXi
3. Verify

Download and edit the .OVF file

1. Extract the files from the MASAGENT-ESX-releasenumber-buildnumber.zip to the desired location. The following files are available:
    - .ovf file
    - .vmdk file
    - .ova file
    - .mf file
2. Open the .ovf file in any editor and add the following <ProductSection>..</ProductSection> sample code after the </VirtualHardwareSection> tag

```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
```



```
7       ovf:key="eth0.ip">
8       <Label>IPAddress</Label>
9       </Property>
10
11      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
12      ovf:key="eth0.netmask">
13      <Label>Netmask</Label>
14      </Property>
15
16      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
17      ovf:key="eth0.gateway">
18      <Label>Gateway</Label>
19      </Property>
20
21      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
22      ovf:key="eth0.nameserver">
23      <Label>Nameserver</Label>
24      </Property>
25
26      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
27      ovf:key="eth0.hostname">
28      <Label>Hostname</Label>
29      </Property>
30
31      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
32      ovf:key="eth0.ServerIP">
33      <Label>ADM Server IP</Label>
34      </Property>
35
36      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
37      ovf:key="eth0.ServerUname">
38      <Label>ADM Username</Label>
39      </Property>
40
41      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
42      ovf:type="string" ovf:key="eth0.ServerPassword">
43      <Label>ADM Password</Label>
44      </Property>
45
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
```

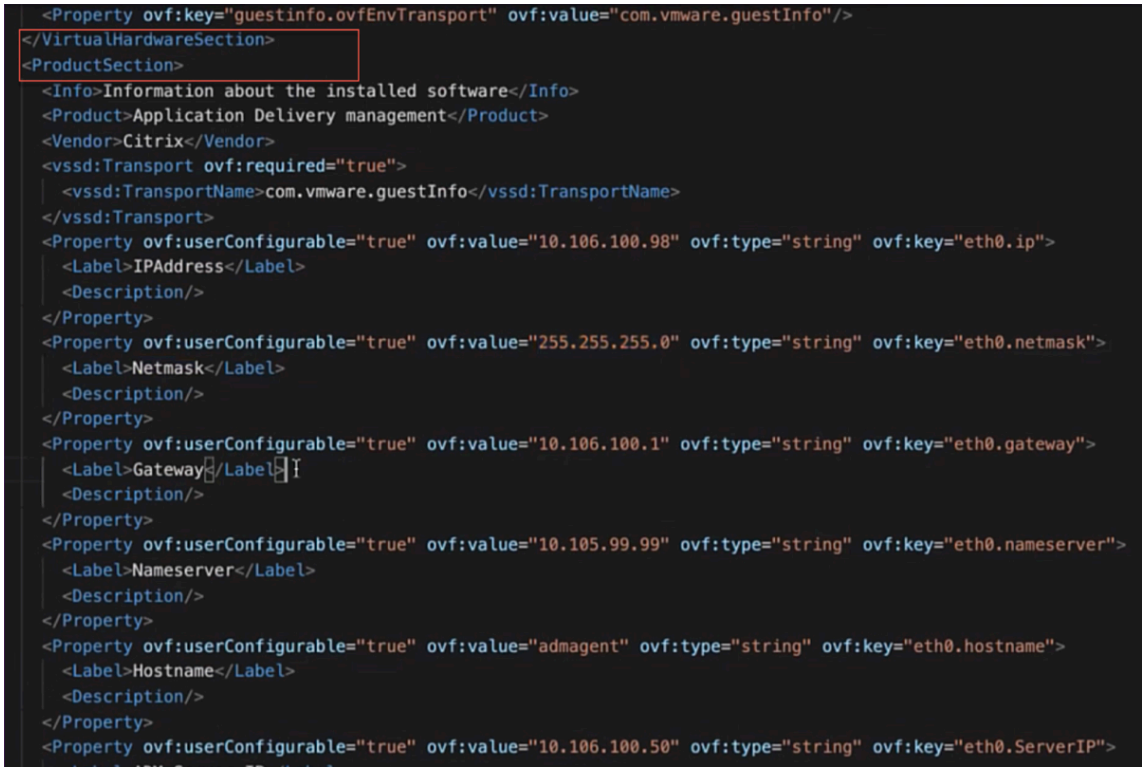


```
52  <!--NeedCopy-->
```

1. For parameters which you want to configure, add their corresponding values in ovf:value=" VALUE"

   - To configure the NetScaler agent, add the values to the following parameters:
     - IPAddress
     - Netmask
     - Gateway
     - Nameserver
     - Hostname
   - To register and change the default password of the NetScaler agent, add the values to the following parameters:
     - ADM Server IP
     - ADM Username
     - ADM Password
     - Agent New Password

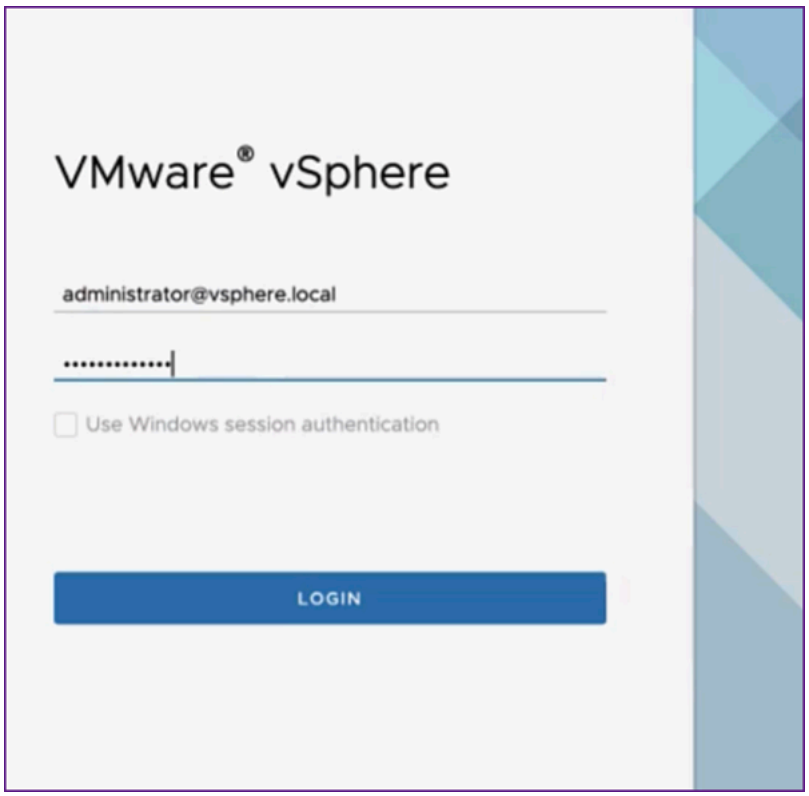
   > **Note**
   >
   > - You must configure the NetScaler agent before you register and change the default password of the agent.
   > - If you do not register and change the default password in the .ovf file, you must perform these actions manually after the VM is deployed.



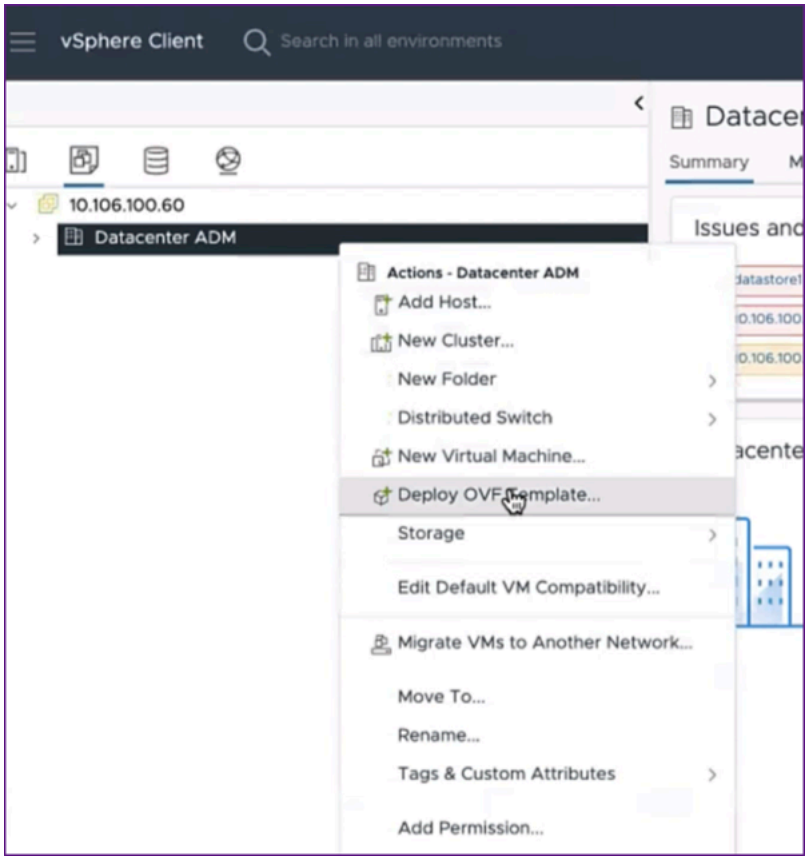
2. After adding the parameters and their values, save the .ovf file.

Install NetScaler ADM virtual appliance on VMware ESXi

1. Log in to the **VMWare vSphere Client** and type the administrator credentials. Click **Login**.

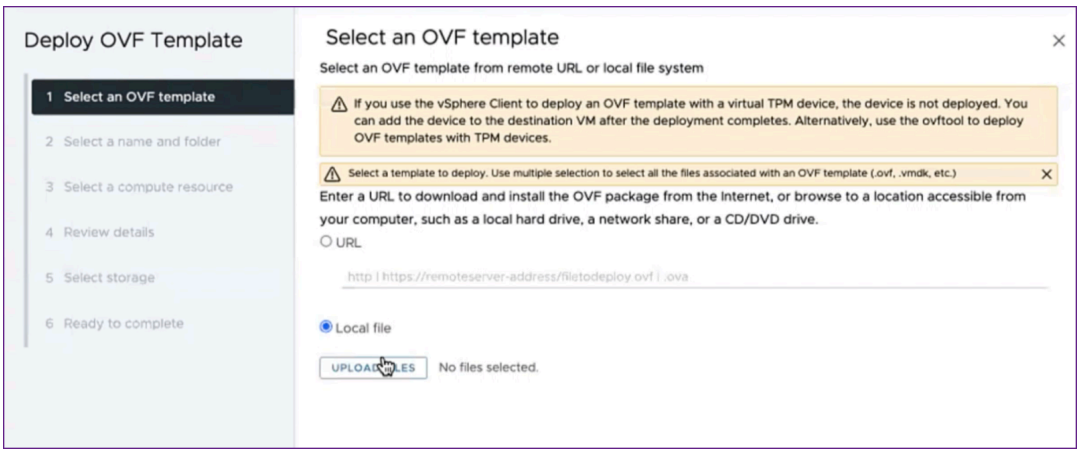


2. Select your ESXi server, and right-click to select **Deploy OVF Template**.

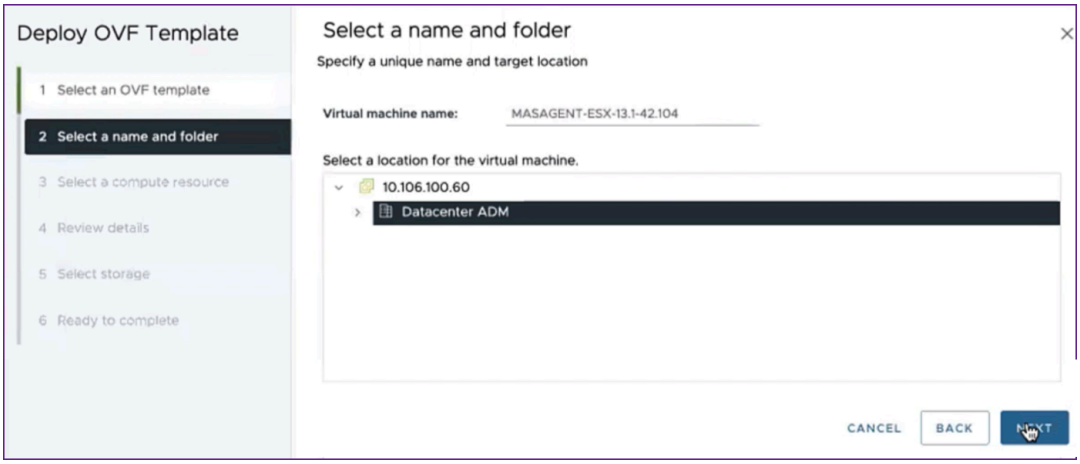


3. In the **Deploy OVF Template** page:

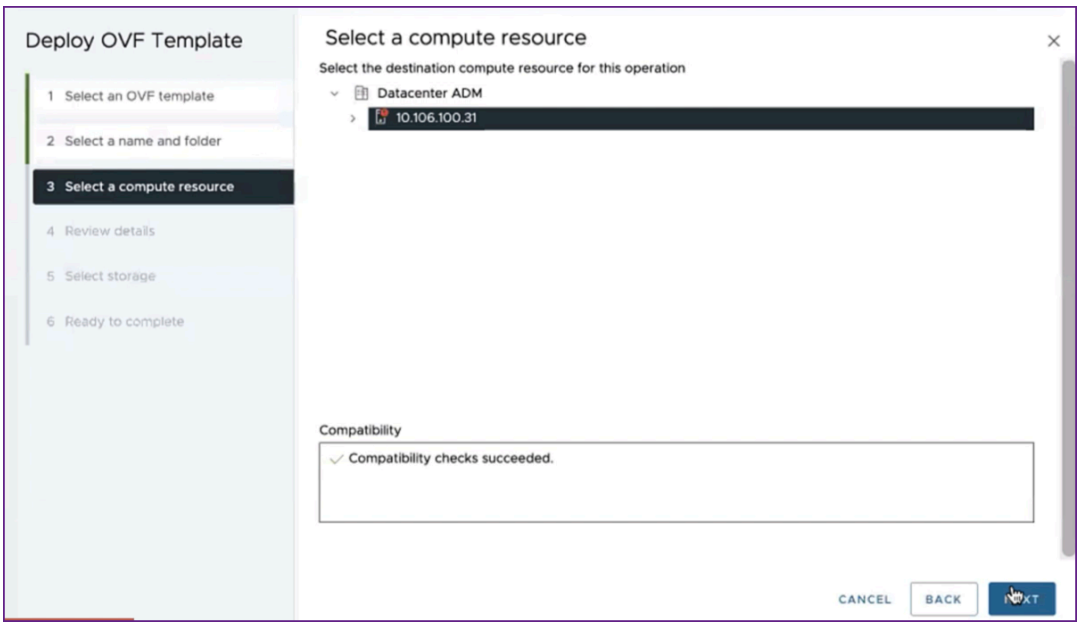
   a) **Select an OVF template**: Select **Local file** and navigate to where you have saved the edited .ovf file and the .vmdk file. Select the files and click **Open** to upload them. Click **Next**.



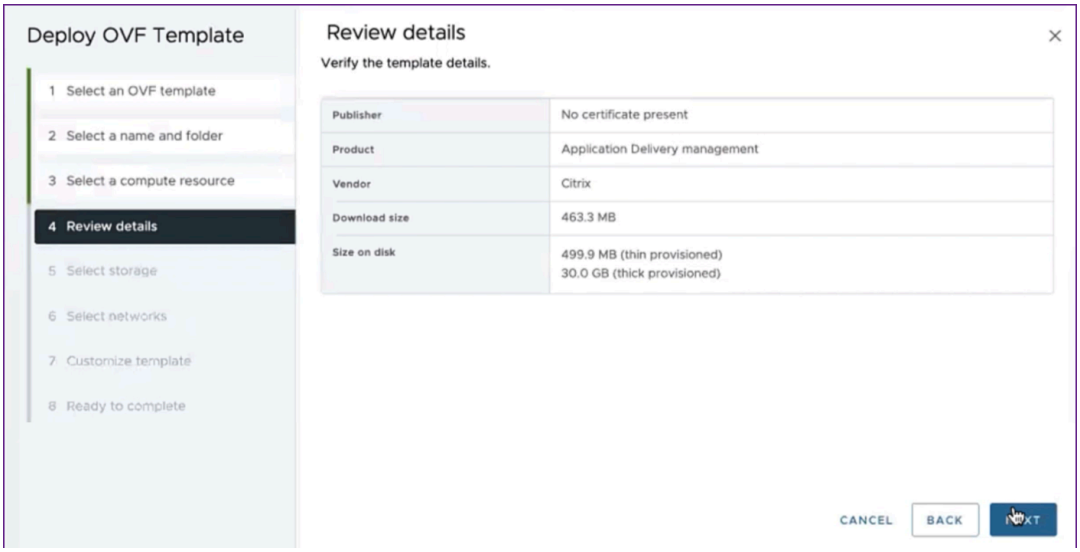
   b) **Select a name and folder**: Add a name for the virtual appliance and select the location on the ESXi where you want to deploy the virtual machine. Click **Next**.



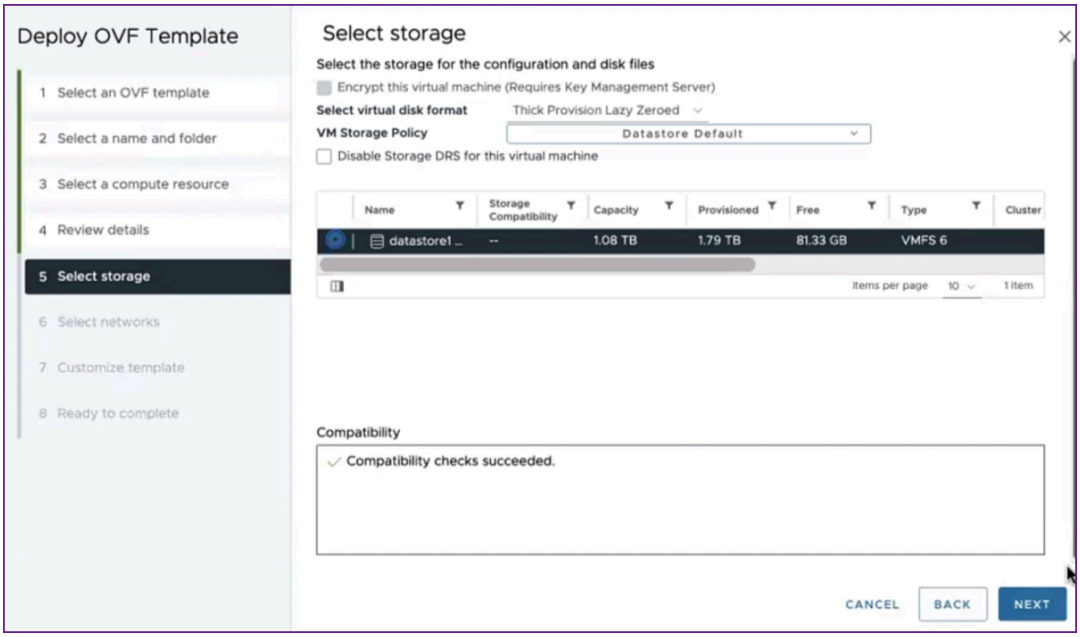
   c) **Select a compute resource**: Select a resource on which to run the template after it is deployed. Click **Next**.



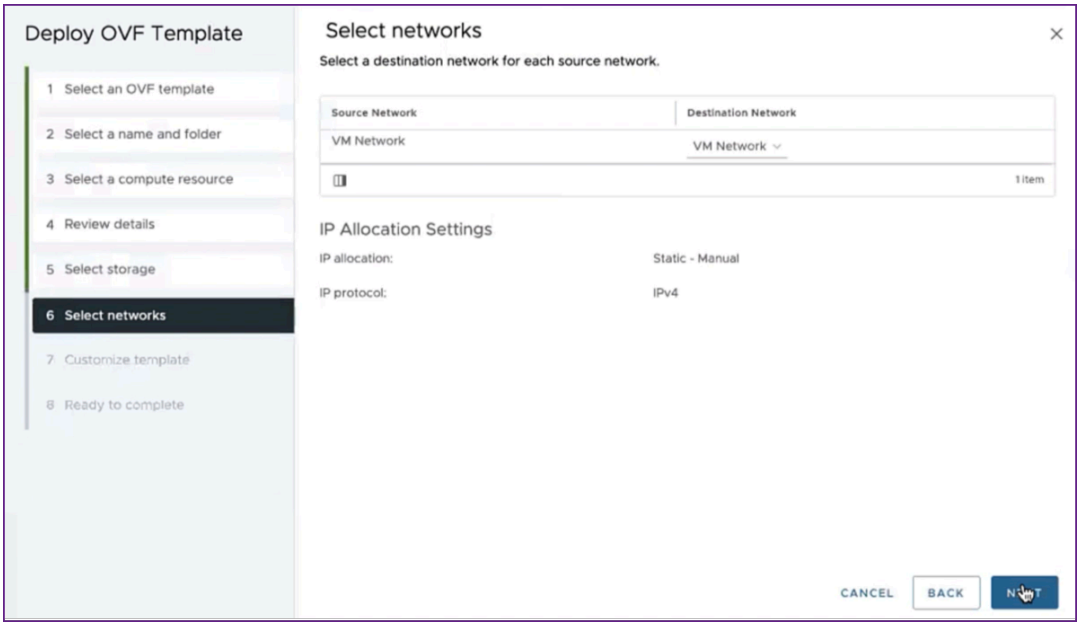
d) **Review details**: Verify the OVF template details. Click **Next**.



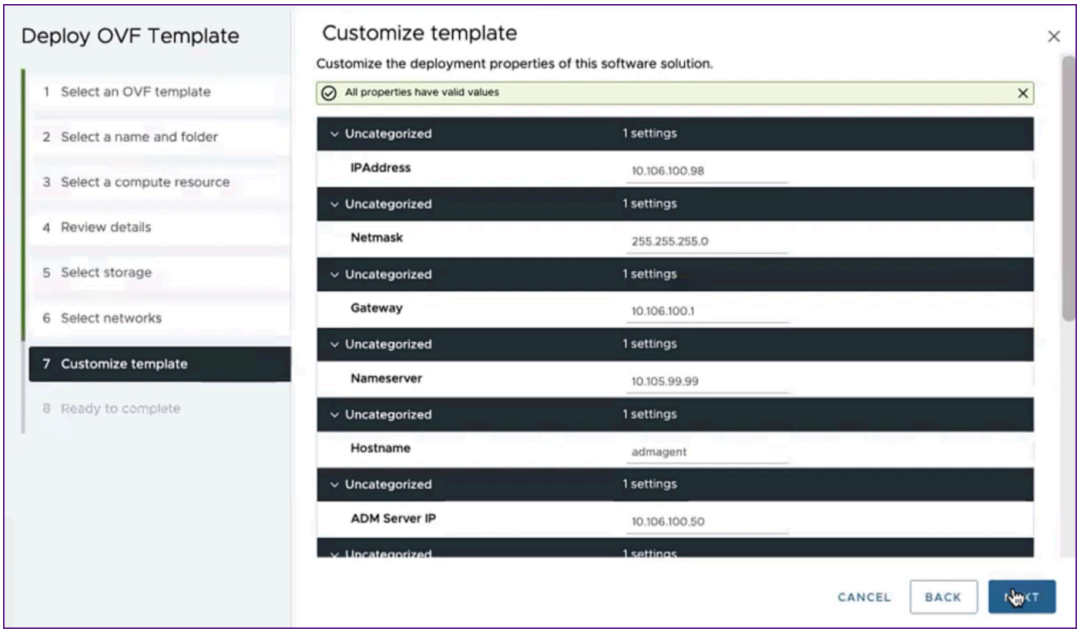
e) **Select storage**: Select a datastore to store the OVF template. Click **Next**.



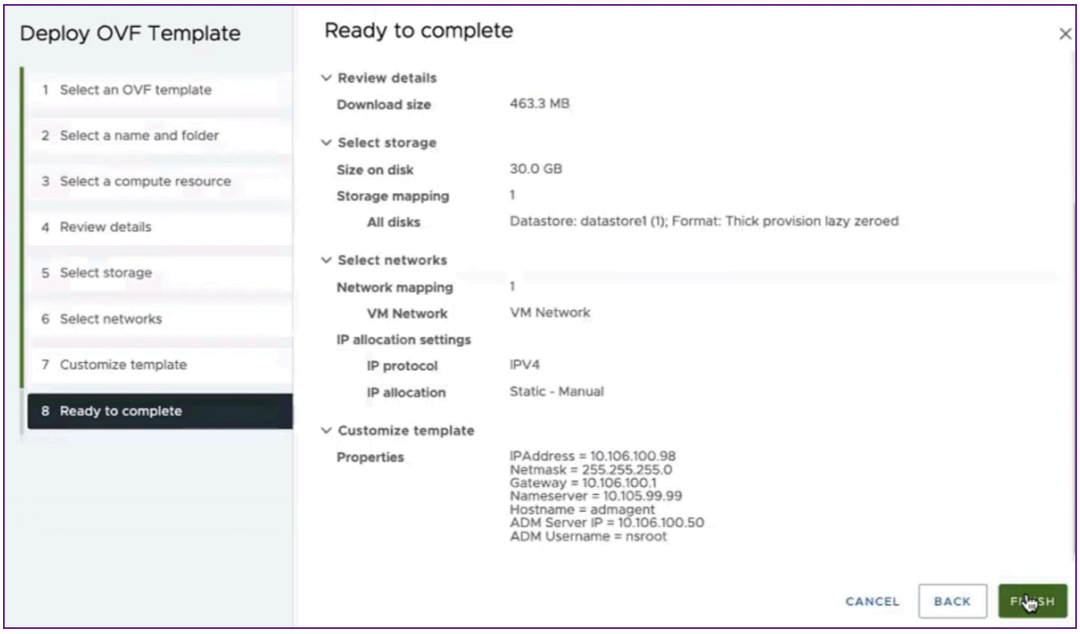
f) **Select networks**: Proceed with the default settings. Click **Next**.



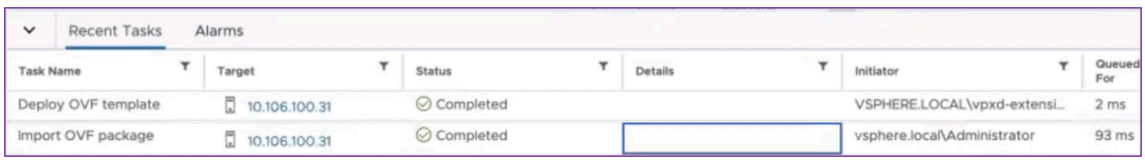
g) **Customize template**: Review all the properties of the OVF template. All the parameters and values you added in the .ovf file in the Download and edit the .OVF file section are displayed.



h) **Ready to complete**: To save the settings and start the deployment process, click **Finish**.

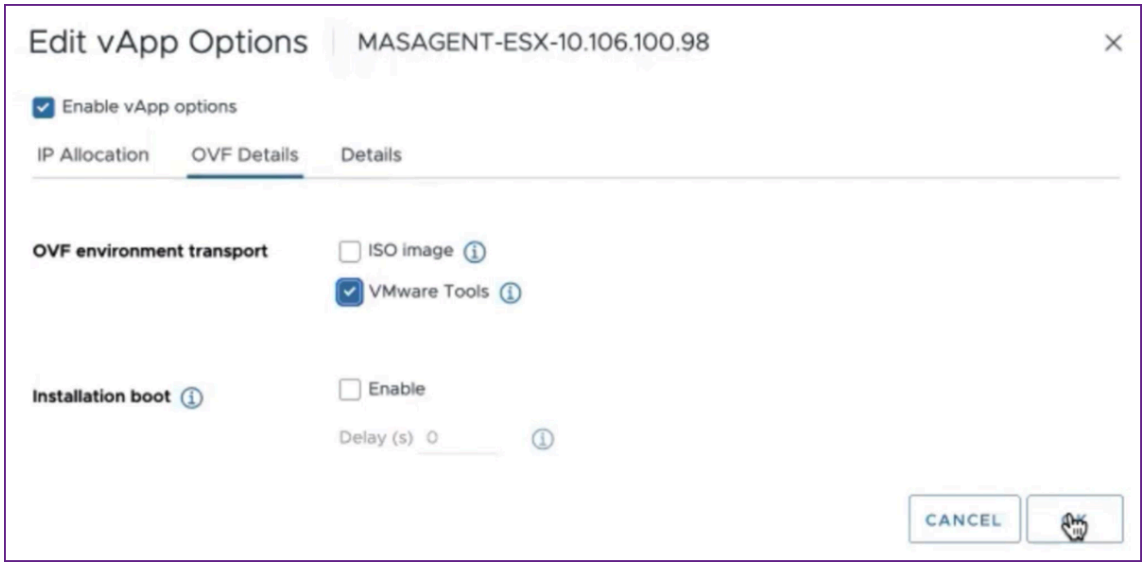


Wait for the deployment to complete. After the status of the **Deploy OVF template** operation is 100% complete, your agent is deployed.

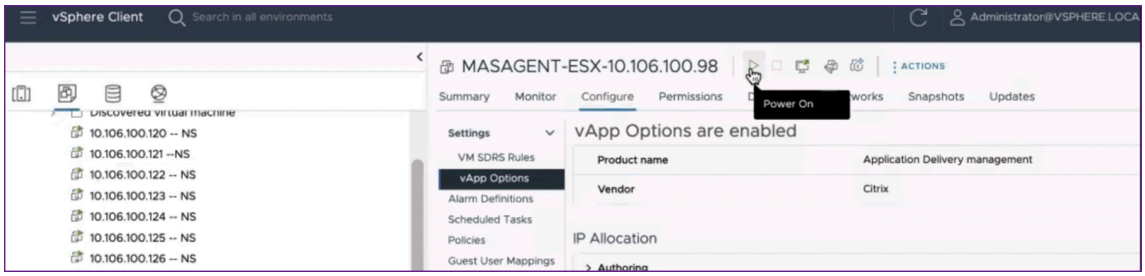


> **Important**
>
> Do not power on the virtual appliance before you edit the settings.

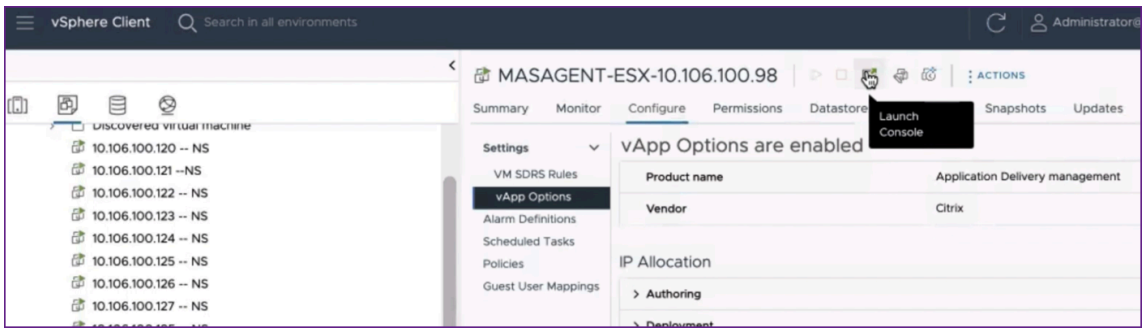
4. Click the new virtual appliance that you installed and navigate to **Configure > Settings > vApp Options > Edit**.
5. In the **Edit vApp Options** window, navigate to **In OVF Details > OVF environment transport**, and select **VMware Tools**. Click **OK**.

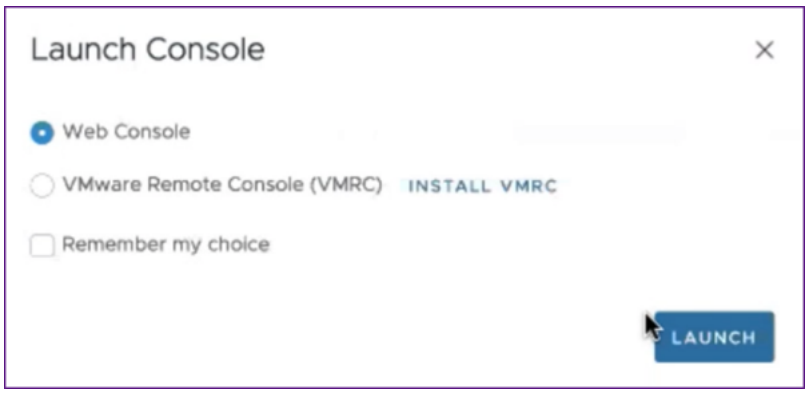


6. Right-click on the virtual machine and click **Power On**. As an alternative, you can select the virtual machine's **Summary** tab and click **Power On**.

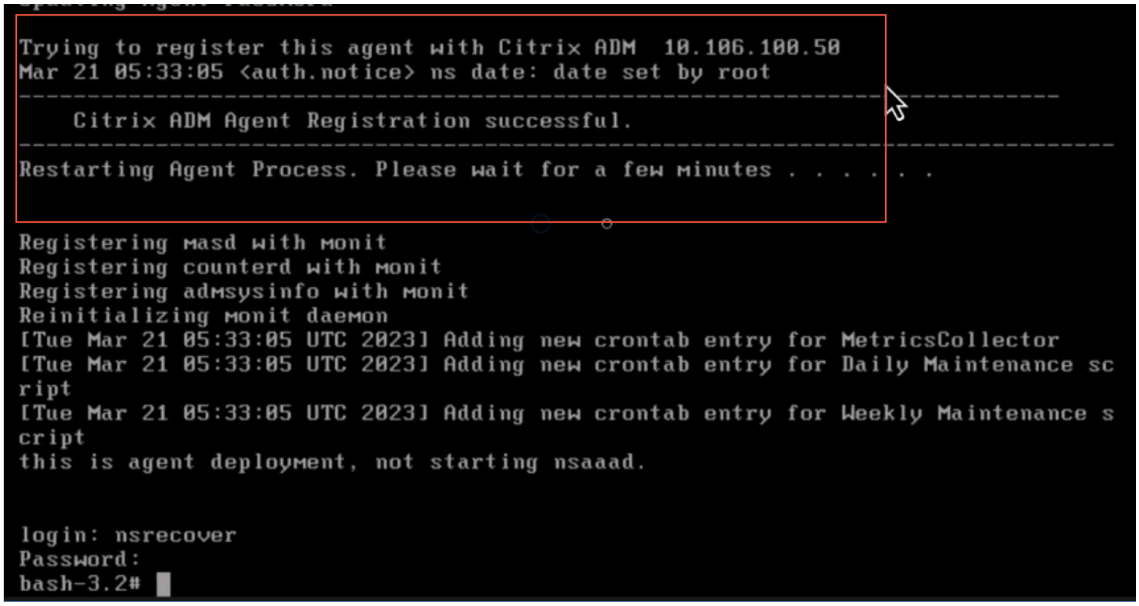


7. In the **Summary** tab, select **Launch Web Console**.
   In the **Launch Console** window, select **Web Console**. Click **Launch**.





8. In the console, a successful registration message is displayed after the NetScaler agent is registered to the NetScaler ADM server. To verify that the NetScaler agent has been deployed and the default password has been changed, log in with the NetScaler agent user name and the new password.



Verify

To verify that the NetScaler agent is deployed:

1. After the NetScaler agent is deployed, access the NetScaler ADM GUI by typing the IP address of the NetScaler ADM server in the browser.
2. Log in to the server with your credentials.
3. Navigate to **Infrastructure > Instances > Agents**.
   The newly deployed agent is displayed in the ESX Platform.

NetScaler ADM on Kubernetes cluster

March 11, 2024

Before you install NetScaler ADM virtual appliances on a Kubernetes cluster, read the prerequisites section.

Prerequisites

Ensure the following prerequisites are met before you install ADM.

Kubernetes cluster

- The Kubernetes cluster must be of the following version or above:
  - Server version v1.20
  - Client version v1.20

  Type the command `kubectl version` to check the version.
- The Helm application installed on the cluster must have the Client version v3.4.0 or above.

  Use the command `helm version` to check the version.
- Kubernetes cluster CNI (Container Network Interface) must be Calico version v3.21.1 or above.
- All the subordinate nodes in the cluster must have an NFS client installed on them. This is because the ADM application persists the data and configuration on volumes mounted on a Network File Server. To install an NFS client on an Ubuntu-based subordinate, type the following commands:

```
apt-get update
apt install nfs-common
```

- The ADM application needs 32 GB memory and 8 vCPUs across the cluster and 120 GB space on NFS.

NFS share

The ADM application needs persistent volumes to store data such as configuration, certificates, images, and others. For this purpose, ADM requires NFS mounts. The application requires two folders from the shared network mounts:

- One for storing files such as certificates, images, and others
- The other one for database

> Note
>
> It's recommended to have an NFS with an SSD.

These two folders can be different or the same. Both the folders must have 777 permissions. The first folder must have minimum 10 GB pace. The second folder's size depends upon the amount of data that needs to be persistent in the database. Minimum size is 100 GB.
For the production environment, we recommend having a production grade NFS solution.

NetScaler appliance

The NetScaler appliance is required as the ingress device. ADC makes the required application services available outside the Kubernetes
cluster. The NetScaler appliance must be outside the Kubernetes cluster, and the worker nodes must be reachable from the ADC. Perform the following steps:

- Configure a SNIP on the ADC. ADC uses this SNIP to reach the worker nodes of the Kubernetes cluster.
- Identify a free IP address to be used as virtual server IP address to make the required application services available outside the Kubernetes cluster.

Install ADM on Kubernetes cluster

Follow these steps to install an ADM appliance on a Kubernetes cluster:

1. Go to the NetScaler site and download the file for the NetScaler ADM Helm Chart for Kubernetes.
2. Extract the downloaded Helm Chart tarball into the /var directory of the main node of the Kubernetes cluster.
3. Open the `values.yaml` file under the `/var/citrixadm` directory.
4. Enter a password for the database in the `dbpasswd` field in the file.
5. Change the following values. The ADM application uses these values to configure the NetScaler appliance so that the services are exposed to the external world:
    - `ingressIP`: a Virtual IP configured in the NetScaler for accessing the application.
    - `applicationID`: a unique ID to distinguish the ingress configuration from the rest of the configuration on the NetScaler appliance.

- `ingressADCIP`: NetScaler IP address (NSIP), which is used as an ingress for the ADM application.
- `ingressADCUsername`: a user name to access the NetScaler appliance. This user must have write privileges.
- `ingressADCPassword`: Password for the user name.

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. Change the following values in the **storage** section. These values specify the persistence required to store files required by the ADM application.

   - `nfsServer`: Host name or IP address of the NFS server
   - `path`: mount the path for the folder to store application files.
   - `size`: at least 10 GB.

   > Note
   >
   > The unit for this value is Gi. For example, 10Gi, 20Gi.

7. Go to **storage** section under `pg-datastore` and change the following values. These values specify the persistence used for creating a database.

   - `nsfServer`: Host name or IP address of the NFS server.
   - `size`: mount a path for the folder used for the datastore.
   - `path`: at least 100 GB.

   > Note
   >
   > The unit for this value is Gi. For example, 100Gi, 200Gi.

8. Go to the /var/citrix directory in the main node and run the following command to install an ADM application:
   `helm install -n citrixadm --namespace <name> ./citrixadm`

   > Note

> This helm command is not supported in helm version 3.x.

This command also installs the required pods in your cluster. Namespace argument is optional. If namespace is not provided, Helm installs ADM in the default namespace. For ease of management, install ADM under a separate namespace.

9. Open your browser and type `http://< virtual server IP address >` and log in to the ADM using `nsroot`/`nsroot` as credentials. For secure access type `https://< virtual server IP address >`.

> Note
>
> During deployment, the ADM application creates tables in the datastore, which can take a while. Depending upon the resources allocated by Kubernetes to various pods of the ADM application, it can take 5- 15 mins for the service to come up.

NetScaler ADM on Linux KVM server

March 11, 2024

Virtualization platforms on which the NetScaler Application Delivery Management (ADM) can be provisioned include Linux-KVM.

Before you install NetScaler ADM on Linux-KVM, make sure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available. Verify that `virsh` (a command-line tool for managing virtual machines) is available on the hypervisor.

Use your administrator credentials to log on to Citrix.com website, access the latest NetScaler ADM setup files, and download them onto your computer. Then, install the NetScaler ADM on your Linux-KVM platform and configure it for your network.

Prerequisites

Before installing the NetScaler ADM virtual appliance, verify that Linux-KVM version 3.6.11-4 and later is installed on hardware that meets the minimum requirements.

Hardware requirements

Component	Requirement
CPU	A 64-bit x86 processor with the hardware virtualization features that are included in the Intel VT-X processor. Provide at least 2 CPU cores to host Linux-KVM. **Note** To test whether your CPU supports Linux host, enter the following command at the host Linux shell prompt: `*. egrep'^flags.\* ( vmx | svm )' /proc/cpuinfo*` If the BIOS settings for the extension are disabled, you must enable them in BIOS. There is no specific recommendation for processor speed, but higher the speed, the better is the performance of the NetScaler ADM.
Memory (RAM)	Minimum 4 GB for the host Linux kernel. Add additional memory as required by the VMs.
Hard Disk	Calculate the space for Host Linux kernel and VM requirements. A single NetScaler ADM VM requires 120 GB of disk space.

> **Note**
>
> The memory and hard disk requirements specified are for deploying NetScaler ADM on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depend on the number of virtual machines running on it.

Software requirements

Citrix recommends newer kernels, such as the 64-bit version of the 3.6.11-4 kernel or later.

Network requirements NetScaler ADM supports only one virtIO para-virtualized network interface. Ensure to connect this interface to the management network of the Linux-KVM host, so that the NetScaler ADM and Linux-KVM can communicate.

Download NetScaler ADM setup files

To download the NetScaler ADM setup files from `www.citrix.com`:

1. Open a web browser and type www.citrix.com in the address bar.

2. Hover over the **Sign In** option and click **My Account**, enter your Citrix credentials, and then again click **Sign In**.
3. Navigate to **Downloads** section.
4. From the **Downloads** list, select **NetScaler Application Delivery Management**.
5. On the **NetScaler Application Delivery Management** page, select the release. For example, select **Release 13.0**.
6. Click **Product Software** to expand it, and click the latest build. For example, select **NetScaler MAS Release (Feature Phase) 13.0 Build 36.27**.

   The selected build page is displayed.
7. On the **Jump to Download** list, select **NetScaler MAS image for KVM, 13.0 Build xx.xx**
8. Click **Download File**, accept the EULA, and download the compressed image file to any folder on your local machine.

Install the NetScaler Application Delivery Management on Linux-KVM

1. Using SSH, log on to the KVM host.
2. At the CLI prompt, by using any of the file transfer programs, copy the image to a folder on the server.
3. Navigate to the directory where you have saved the downloaded image.
4. Perform these at the command line:

   a) List the files in the directory verify the presence of the image file.

   b) Use the tar command to untar the NetScaler Application Delivery Management image file. The unzipped package contains the following components:

      i. A domain XML file that specifies the NetScaler ADM attributes

      ii. A text file that specifies the check sum of the domain disk image

      iii. A domain disk image

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



```
root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build#
```

iv. Create a copy of MAS-KVM.xml as MAS1-KVM.xml, as a back-up option. Open the MAS1-KVM.xml file by using the vi editor.

v. Edit MAS1-KVM.xml for the following networking attributes:

A. `name` - Specify the name.

B. `mac` - Specify the MAC address.

C. `source file` - Specify the absolute disk-image source path. The file path has to be absolute.

> **Note**
>
> The domain name and the MAC address must be unique.

D. `mode` - Specify the mode.

E. `model type` - Set to virtIO.

F. `source dev` - Specify the interface.

```
1 <name> MAS1-KVM</name>
2 <mac address='52:54:00:29:74:b3'/>
3 <source file='/var/ MAS-KVM.qcow2'/>
4 <source dev='eth0' mode='bridge'/>
5 <model type='virtio'/>
6 <!--NeedCopy-->
```

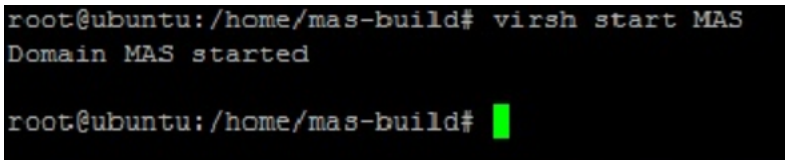
vi. Define the VM attributes in the MAS1-KVM.xml file by using the following command: `virsh define \<FileName\>.xml`

```
1 virsh define MAS-KVM.xml
2 Domain MAS defined from MAS-KVM.xml
3 <!--NeedCopy-->
```

```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

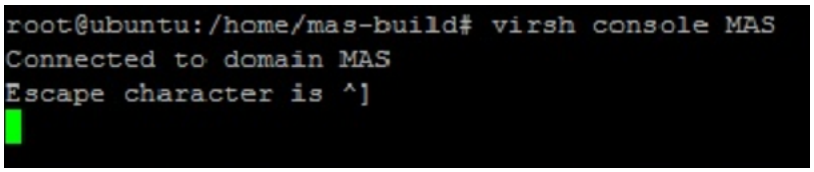
vii. Start the NetScaler ADM by entering the following command: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`


```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



viii. You can connect to the NetScaler ADM virtual machine by using the following command: `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```



Configure the NetScaler Application Delivery Management

> **Note**
>
> On some Linux KVM hosts, FreeBSD guests fail to restart properly if they have more than one CPU. When The NetScaler ADM virtual appliance is restarted, the NetScaler ADM CLI and GUI become unresponsive. For details, see https://bugs.launchpad.net/qemu/+bug/1329956
>
> To avoid the NetScaler ADM CLI and GUI from becoming unresponsive when the NetScaler ADM virtual appliance is restarted, shut down all the virtual machines on the KVM host, and perform the following on the KVM host:
>
> 1. Remove the kvm_intel module using the following command:
>   `rmmod kvm\\_intel`
> 2. Disable **APICv** and reload kvm_intel module using the following command:
>   `modprobe kvm\\_intel enable\\_apicv=N`
> 3. Start the virtual machines on the KVM host.

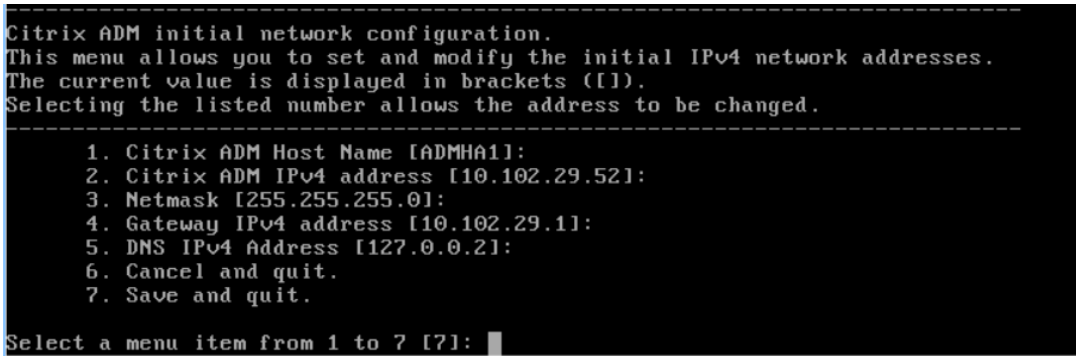
After installing the NetScaler ADM, allow about 10 minutes for the services to become available, and then log on to the NetScaler ADM.

1. At the command line, use the default system administrator credentials to log on to the system:

- User name: `nsroot`
- Password: `nsroot`

> **Note**
>
> After logging on for the first time, change the administrative password. Then, configure the MAS to function in your network. You can change the password from the NetScaler ADM user interface. From the NetScaler ADM home page, navigate to **Settings > User Administration > Users**. Select the user and click **Edit**, and then update the password in the Password field.

2. At the prompt, type: *shell*
3. Type **networkconfig** to enter the NetScaler ADM initial network configuration menu. Configure the management IP address.
4. To complete the initial network configuration of NetScaler ADM, follow the prompts. The console displays the NetScaler ADM initial network configuration options for setting the following parameters for the NetScaler ADM. The host name is populated by default.
   a) Enter **2** to update NetScaler ADM IPv4 address - management IP address at which you access a NetScaler ADM
   b) Enter **3** to update Netmask - subnet mask associated with the Management IP address
   c) Enter **4** to update Gateway IPv4 address - default gateway IP address for the subnet of the Management IP address of the NetScaler ADM
   d) Enter **7** to save and quit - saves your configuration changes and exits the system.



5. Run the deployment script by typing the command at the shell prompt: `deployment_type.py`
6. In the deployment screen that appears, select the deployment type as **NetScaler ADM server**.

7. Type **Yes** to deploy NetScaler ADM as a standalone deployment.
8. Type **Yes** to restart the NetScaler ADM server.
9. After NetScaler ADM server restarts, log on to NetScaler ADM by using the default administrator credentials as nsroot/nsroot through the command line or the GUI.

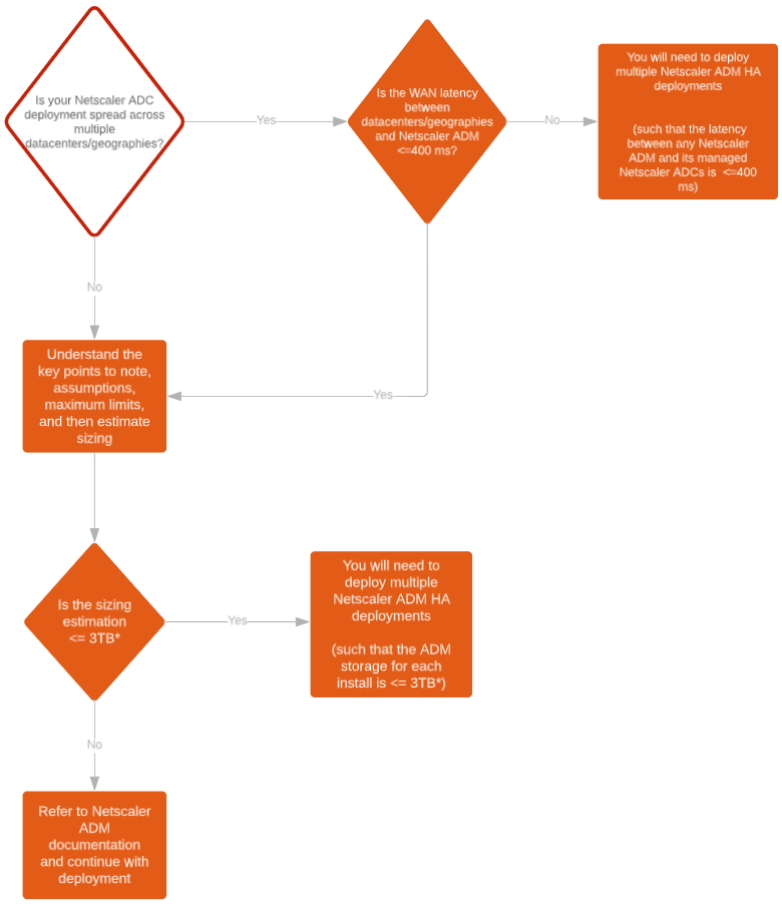
   You can later access the NetScaler ADM by typing the IP address of the NetScaler ADM server in the address bar of your browser. The default administrator credentials to log on to the server are *nsroot/nsroot*.

Configure high availability deployment

March 11, 2024

High Availability (HA) refers to a system that is always available to a user without any interruption to the services. High availability setup is crucial during system downtime, network or application failures, and is a key requirement to any enterprise. A high availability deployment of two NetScaler ADM nodes in active-passive mode with same configurations provides uninterrupted operations.

Deployment scenario



> **Note**
>
> The validated maximum storage limit for a single NetScaler ADM HA deployment is 3 TB. For more information, see the deployment guide.
>
> **Important**
>
> **To access NetScaler ADM 12.1 build 48.18 or later versions using HTTPS:**
>
> If you have configured a NetScaler instance to load balance NetScaler ADM in a high availability mode, first remove the NetScaler instance. Then, configure a floating IP address to access NetScaler ADM in high availability mode.

The following are the benefits of high availability deployment in NetScaler ADM:

- An improved mechanism to monitor heartbeats between the primary and secondary node.
- Provides physical streaming replication of database instead of a logical bi-directional replication.

- Ability to configure the floating IP address on the primary node to eliminate the need of separate NetScaler load balancer.
- Provides easy access to the NetScaler ADM user interface using the floating IP address.
- NetScaler ADM user interface is provided only on the primary node. By using the primary node, you can eliminate the risk of accessing and making changes to the secondary node.
- Configuring the floating IP address handles the failover situation and reconfiguring the instances is not required.
- Provides built in ability to detect and handle split-brain situation.

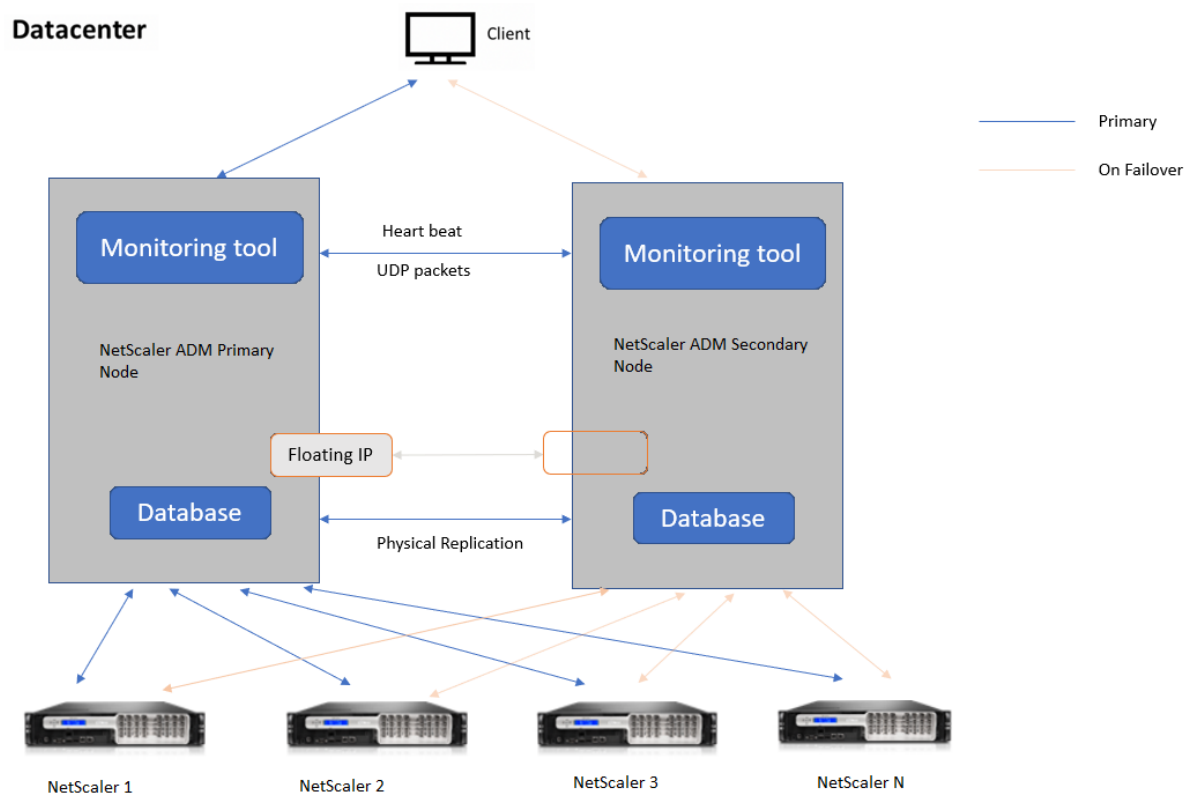
The following table describes the terms used in high availability deployment.

Terms	Description
Primary node	First node registered in the high availability deployment.
Secondary node	Second node registered in the high availability deployment.
Heartbeat	A mechanism used to exchange messages between primary and secondary node in the high availability setup. The messages determine status and health of the application on each individual node.
Floating IP address	A floating IP is an IP address that can be instantly moved from one node to another in the same subnet. Internally it is set up as an alias on the network interface of the primary node. If there is a failover, the floating IP address is seamlessly moved from the old primary to the new one. It is useful in high availability setup because it allows clients to communicate with the high availability nodes using a single IP address.

> **Note**
>
> For more information on port and protocol details, see Ports.

Components of high availability architecture

The following figure displays the architecture of two NetScaler ADM nodes deployed in high availability mode.



In high availability deployment, one NetScaler ADM node is configured as the primary node (MAS 1) and the other as the secondary node (MAS 2). If the primary node goes down due to any reason, the secondary node takes over as the new primary node.

Monitoring tool

Monitoring tool is an internal process used to monitor, alert, and handle failover situations. The tool is active and running on each node in high availability. It is responsible for starting subsystems, initiating database on both the nodes, deciding on the primary, or secondary node if there is a failover, and so on.

Primary node

The primary node accepts connections and manages the instances. All processes such as AppFlow, SNMP, LogStream, syslog, and so on is managed by the primary node. The NetScaler ADM user interface access is available on primary node. The floating IP address is configured on the primary node.

Secondary node

The secondary node listens to the heartbeat messages sent from the primary node. Database on the secondary node is in read-replica mode only. None of the processes are active in the secondary node and the NetScaler ADM user interface is not accessible on the secondary node.

Physical streaming replication

The primary and secondary nodes synchronize through heartbeat mechanism. With the physical streaming replication of database, the secondary node starts in read-replica mode. The secondary node listens to the heartbeat messages received from the primary node. If the secondary node does not receive any heartbeats for a time period of 180 seconds, the primary node is considered to be down. Then, the secondary node takes over as the primary node.

Heartbeat messages

Heartbeat messages are User Datagram Packets (UDP) that are sent and received between primary and secondary node. It monitors all subsystems of NetScaler ADM and database to exchange information about the node state, health, processes, and so on. The information is shared between the high availability nodes every second. Notifications are sent as alerts to the administrator if there is a failover or break up of high availability states.

Floating IP address

The floating IP address is associated with the primary node in the high availability setup. It is an alias given to the primary node IP address, that the client can use to connect to NetScaler ADM in the primary node. Since the floating IP address is configured on the primary node, the instance reconfiguration is not required in case of failover. The instances reconnect to the same IP address to reach the new primary.

Key points to note

- In a high availability setup, both the NetScaler ADM nodes are deployed in active-passive mode. They must be on the same subnets using the same software version and build, and have same configurations.
- Floating IP address:
  - Floating IP address is configured on the primary node.

  - Instances need not be reconfigured if there is a failover.
  - You can access a high availability node from the user interface, either by using the primary node IP or floating IP address.

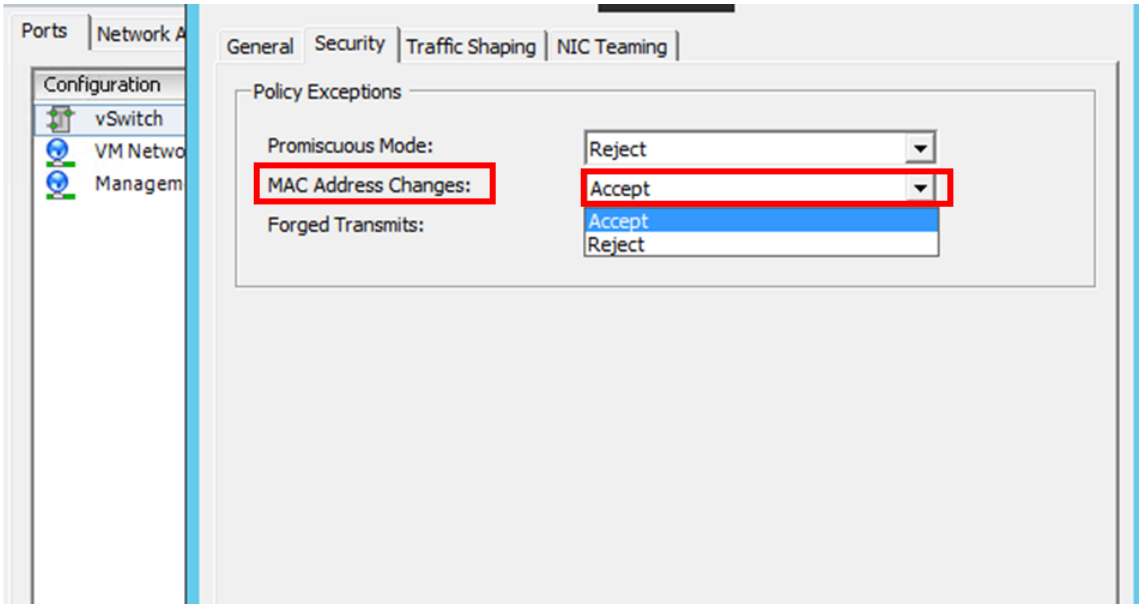
    > **Note**
    >
    > Citrix recommends that you use the floating IP address to access the user interface.

- Database:
  - In a high availability setup, all configuration files are synchronized automatically from the primary node to the secondary node at an interval of one minute.
  - Database synchronization happens instantly by physical replication of database.
  - Database on secondary node is in read-replica mode.
- NetScaler ADM upgrade:
  - Internal processes implicitly upgrade NetScaler ADM from the earlier versions.

    > **Note**
    >
    > After the upgrade is successful, you must configure the floating IP address.

- UDP default port 5005 is available on both the nodes for heartbeats to be sent and for messages to be received.
- MAC address
  The setting for the "MAC Address Changes"option in a hypervisor affects the traffic that a virtual machine receives. Allow MAC address changes to be enabled on the virtual switch so that the floating IP address moves seamlessly to the new primary node after failover.
  For example, when deploying NetScaler ADM on a high availability on VMware ESXi, ensure you accept changes to MAC address. ESXi now allows requests to change the active MAC address to other than the initial MAC address.

  > **Note**
  >
  > For NetScaler ADM deployed on ESXI version 6.7, you can set the **MAC Address Changes** option to **Reject** also. After failover, the traffic flows to new primary node seamlessly irrespective of the **MAC Address Changes** setting. Therefore, accept changes to MAC address is not mandatory.
  >
  > If the NetScaler ADM is deployed on the ESXI version lower than 6.7, ensure the **MAC Address Changes** option is set to **Accept** only.



Prerequisites

Before you set up high availability for NetScaler ADM nodes, note the following prerequisites:

- The NetScaler ADM high availability deployment is supported from NetScaler ADM version 12.0 build 51.24.
- Download the NetScaler Application Delivery Management image file (.xva) from the NetScaler site: https://www.citrix.com/downloads/

Citrix recommends that you set CPU priority (in virtual machine properties) at the highest level to improve scheduling behavior and network latency.

The following table lists the minimum requirements for the virtual computing resources:

Component	Requirement
RAM	**32 GB**
Virtual CPU	**8 CPUs**

Component	Requirement
Storage Space	Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation. If your NetScaler ADM storage requirement exceeds 120 GB, you have to attach an additional disk. **Note** You can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu and Fedora

To set up NetScaler ADM in high availability mode

1. Register and deploy the first server (primary node).
2. Register and deploy the second server (secondary node).
3. Deploy the primary and secondary node for high availability setup.

Register and deploy the first server (primary node)

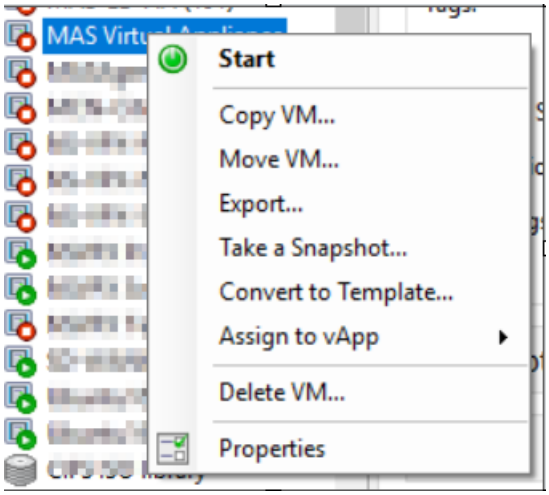
To register the first node:

1. Use the .xva image file downloaded from the NetScaler site and import it in to your hypervisor.

   > **Note**
   >
   > It might take a few minutes for the .xva image file to import and get started. You can see

> the status on the bottom of the screen.
>
>
>

2. After the import is successful, right-click and click **Start**.



3. From the **Console** tab, configure NetScaler ADM with the initial network configurations.

4. After the initial network configuration is complete, the system prompts for login. Log on using following credentials –*nsrecover/nsroot*.

> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

5. To deploy the primary node, enter **/mps/deployment_type.py**. The NetScaler ADM deployment configuration menu is displayed.


```
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

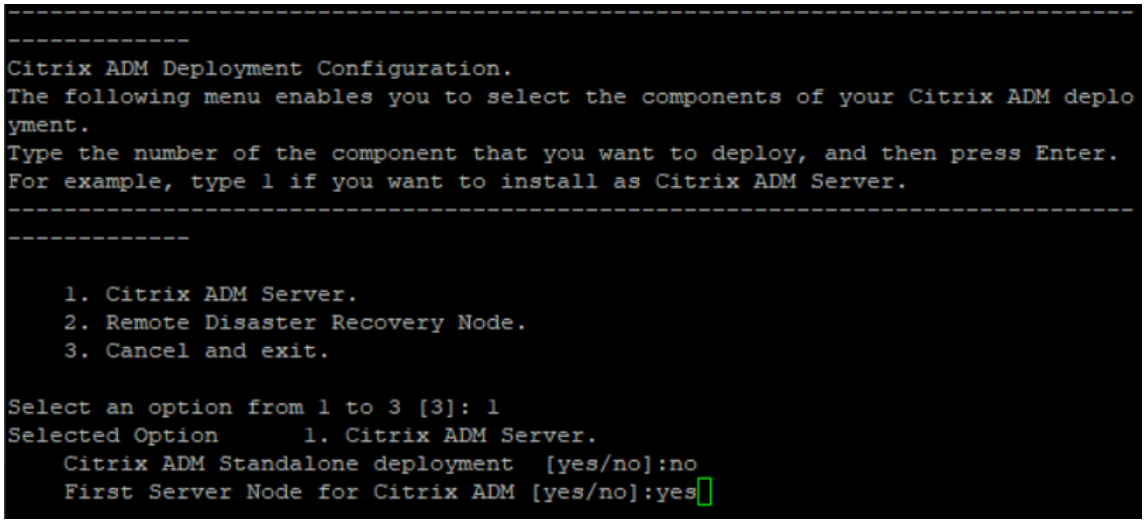
6. Select **1** to register NetScaler ADM server as primary node.

```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

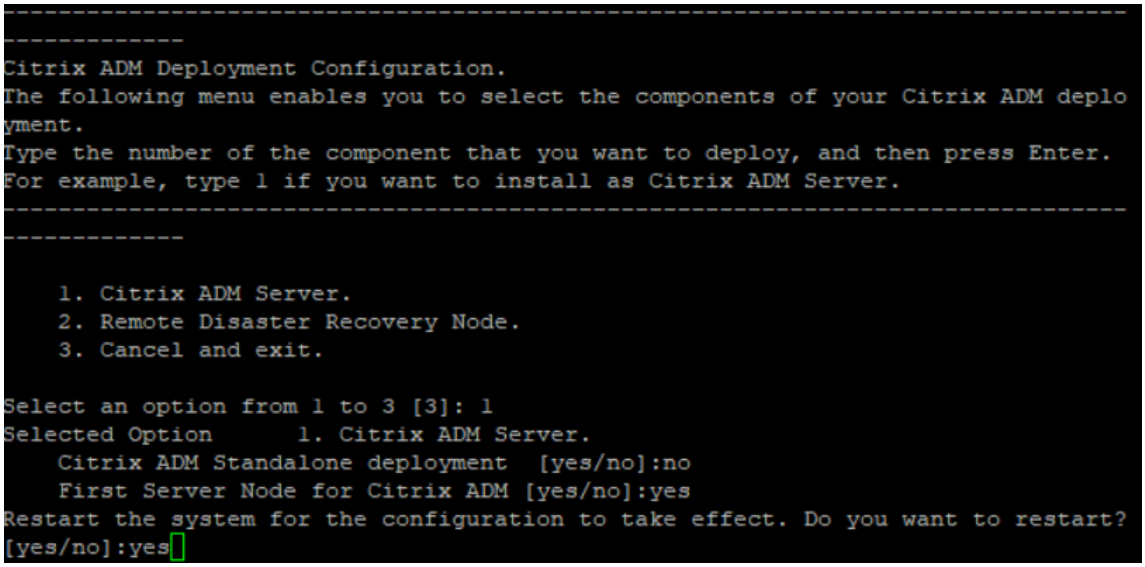
7. The console prompts you to select the NetScaler ADM standalone deployment. Enter **No** to confirm the deployment as high availability.

```
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

8. The console prompts you to select the First Server Node. Enter **Yes** to confirm the node as the first node.



9. The console prompts you to restart the system. Enter **Yes** to restart.



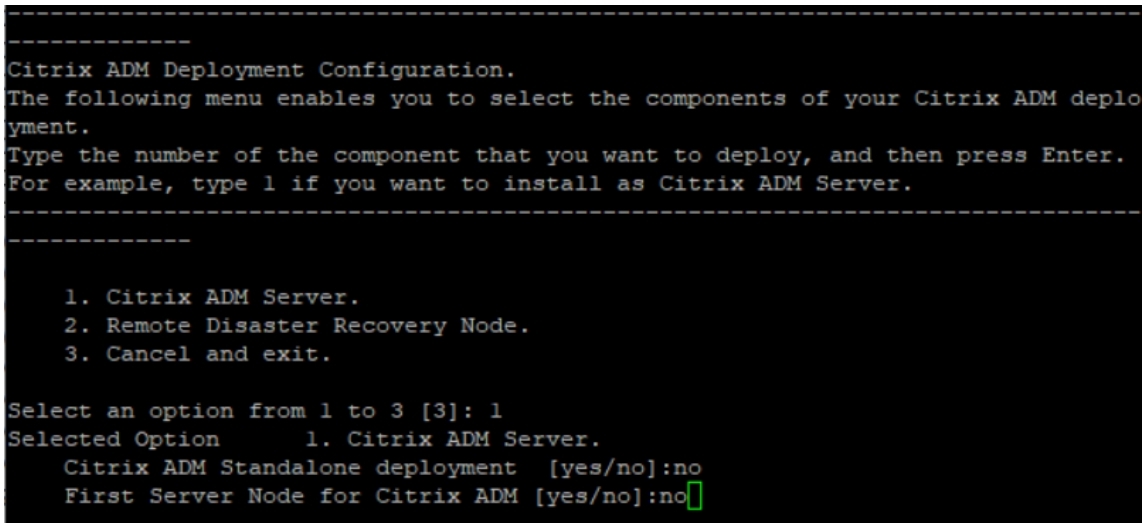
The system restarts and is displayed as the primary node in the NetScaler ADM user interface.

Register and deploy the second server (secondary node)

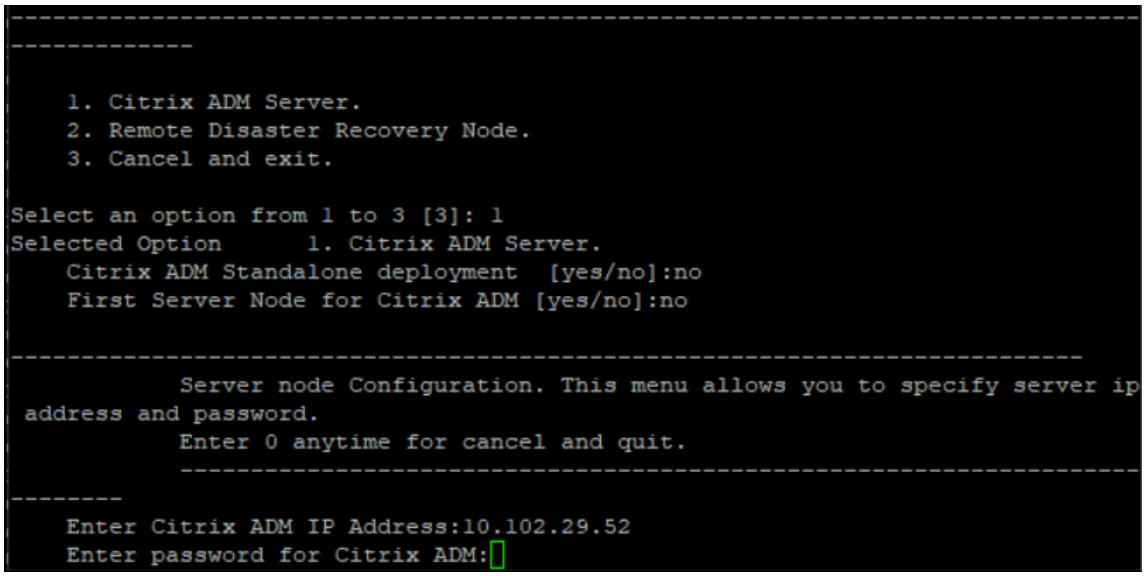
1. Use the **.xva** image file downloaded from the NetScaler site and import it in to your hypervisor.
2. From the **Console** tab, configure NetScaler ADM with the initial network configurations as displayed in the following image.
3. After the initial network configuration is completed, the system prompts for login. Log on using following credentials –*nsrecover/nsroot*.

> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

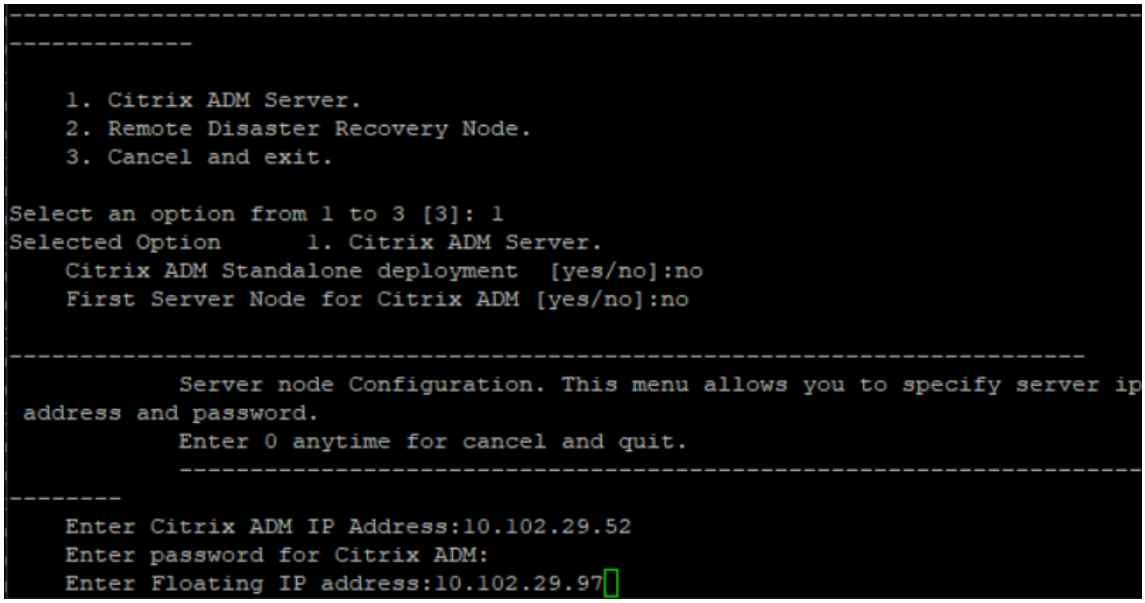
4. To deploy the secondary node, enter **/mps/deployment_type.py**. The NetScaler ADM deployment configuration menu is displayed.
5. Select **1** to register NetScaler ADM server as secondary node.
6. The console prompts you to select the NetScaler ADM as standalone deployment. Enter **No** to confirm the deployment as high availability.
7. The console prompts you to select the first server node. Enter **No** to confirm the node as the second server.



8. The console prompts you to enter the IP address and password of the primary node.



9. The console prompts you to enter the floating IP address.



10. The console prompts you to restart the system. Enter **Yes** to restart.

> **Note**
>
> - Floating IP address is mandatory for high availability deployment of nodes.
> - The system will show error messages if there are any issues in the configuration.
> - The system reboots and takes a few minutes for the configurations to take effect.

Deploy the primary and secondary node as a high availability pair

After the registration both primary and secondary nodes are displayed on the NetScaler ADM user interface. Deploy these nodes into a high availability pair.

> **Note**
>
> - Before deploying the nodes into a high availability pair, ensure that the secondary node is completed with a reboot, after the initial network configuration.
> - After the high availability deployment is complete, use the floating IP address to access the NetScaler ADM user interface.

To deploy nodes as a high availability pair:

1. Open a web browser and enter the IP address of the first NetScaler ADM server node.
2. In the **user Name** and **password** fields, enter the administrator credentials.
3. Click **Get Started** in the home page.

4. Select the deployment type as **Two Servers deployed in High Availability Mode**, and click **Next**.
5. On the Deployment page, click **Deploy**.
6. A confirmation message is displayed. Click **Yes**.

   The NetScaler ADM restarts and takes approximately 10 minutes for the configuration to take effect.

   > **Note**
   >
   > You can now start using the Floating IP address.

7. Log on to NetScaler ADM using administrator credentials, click **Get Started** in the home page, and optionally, complete the following:

   a) Add NetScaler instances

   b) Configure Customer Identity

   > **Note**
   >
   > You can also click **Skip** to complete it later and click **Finish**.

8. Navigate to **Settings > Deployment** to validate the deployment.

   For more information, see the Frequently Asked Questions.

Disable high availability

You can disable high availability on a NetScaler ADM high availability pair and convert the nodes to standalone NetScaler ADM servers.

> **Note**
>
> Disable high availability from the primary node.

To disable the high availability:

1. In a web browser, enter the IP address of the NetScaler ADM server primary node.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **System** tab, navigate to **Deployment** and click **Break HA**.

   A dialogue box is displayed. Click **Yes** to break the high availability deployment.

Redeploy high availability

After you disable the high availability to a standalone deployment, you can redeploy it to high availability mode again. Redeploying high availability is similar to the first time deployment of high availability. For more details see Deploy the primary and secondary node as a high availability pair.

High availability failover scenarios

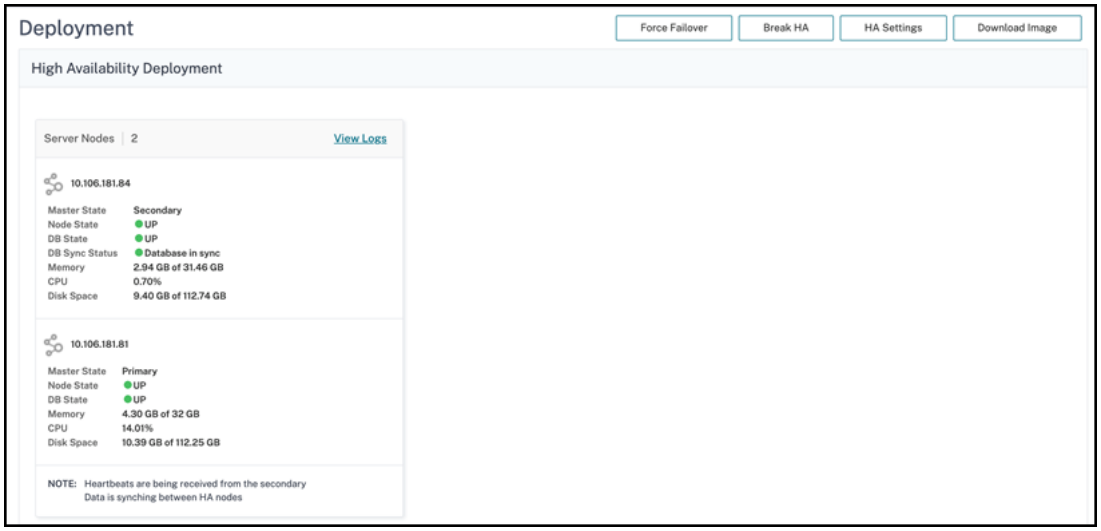
A failover occurs if one of the following conditions is encountered:

- **Node failure**: Primary node goes down, no heartbeat is detected from primary node for 180 seconds.
- **Application health failure**: Primary node is up and running but one of the NetScaler ADM processes is down.

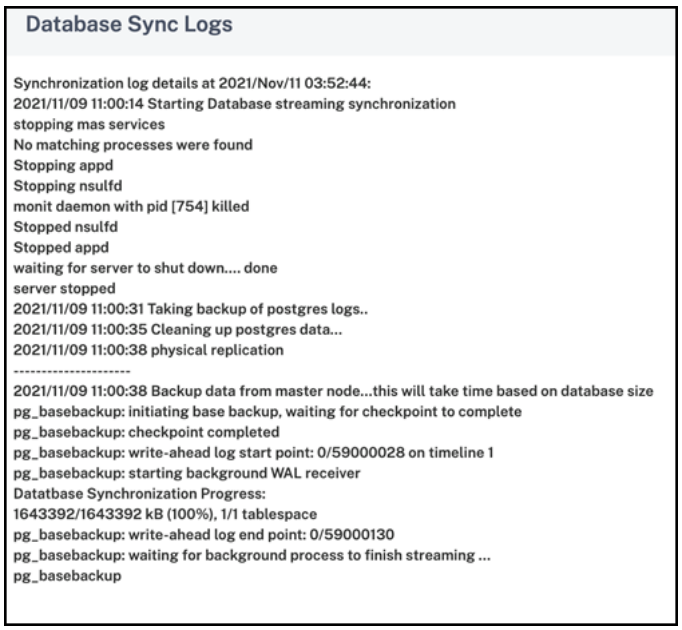
View Database Synchronization Log messages

In the NetScaler ADM HA pair, the configuration files are synchronized automatically from the primary node to the secondary node and the physical streaming replication of database happens.

However, if there is a streaming replication error, the **Sync Database** button appears. You can click the **Sync Database** button to start the database synchronization process.



To view the progress of the database synchronization, click **View Logs**. The **Database Sync Logs** message appears and you can view the details of the synchronization progress real-time.



Split-brain scenario

When there is no communication between both the nodes due to downtime in network link, then:

- Primary node continues to operate as primary
- Secondary node takes over as primary because of the failure to receive heartbeats
- Both the nodes would run their individual database instances

For example, in an enterprise two NetScaler ADM nodes have been deployed as primary and secondary. Due to a possible network link downtime, the communication between the two NetScaler ADM nodes breaks completely. Since there is no heartbeat exchange for over 180 seconds, both the nodes consider themselves to be the primary node. Both nodes act as active nodes and run their own instances of database.

From NetScaler ADM 12.1 or later release, this split-brain situation is handled gracefully after the network link and heartbeat is restored. High availability synchronization is restored automatically. The recovery time depends on the data and speed of the link between the nodes.

> **Note**
>
> During the split-brain condition, changes that occurred on the old primary node is reset with the new primary when it is rejoined in high availability. The changes that happened on new primary node during split-brain remains intact.

Configure disaster recovery for high availability

March 11, 2024

Disaster is a sudden disruption of business functions caused by natural calamities or human caused events. Disasters affect data center operations, after which resources and the data lost at the disaster site must be fully rebuilt and restored. The loss of data or downtime in the data center is critical and collapses the business continuity.

The NetScaler ADM disaster recovery (DR) feature provides full system backup and recovery capabilities for NetScaler ADM deployed in high availability mode. At the time of recovery, certificates, configuration files, and a complete backup of the database is available in the recovery site.

The following table describes the terms used while configuring disaster recovery in NetScaler ADM.

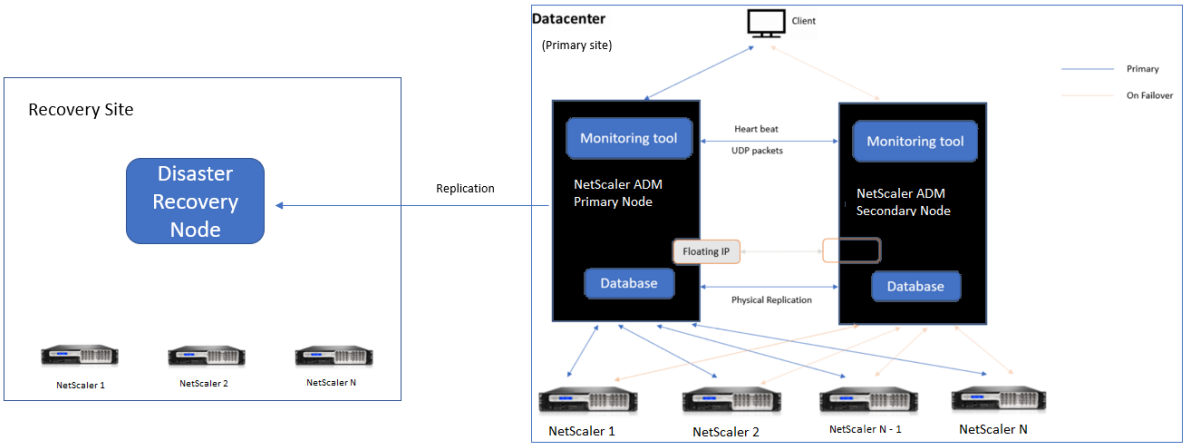
Terms	Description
Primary site (Data center A)	The primary site has NetScaler ADM nodes deployed in high availability mode.
Recovery site (Data center B)	The recovery site has a disaster recovery node deployed in standalone mode. This node is in read-only mode and is not operational until the primary site is down.
Disaster recovery node	The recovery node is a standalone node deployed in the recovery site. This node is made operational (to the new primary) in case a disaster occurs at the primary site and it is nonfunctional.

> **Note**
>
> The primary site and DR site communicate with each other through ports 5454 and 22, and these ports are enabled by default.
>
> For more information on port and protocol details, see Ports.

Disaster recovery workflow

The following image shows the disaster recovery workflow, the initial setup before disaster, and the workflow after the disaster.

Initial setup before disaster



The image shows the disaster recovery setup before disaster.

The primary site has NetScaler ADM nodes deployed in the high availability mode. To learn more, see High availability deployment

The recovery site has a standalone NetScaler ADM disaster recovery node deployed remotely. The disaster recovery node is in read-only mode and receives data from the primary node to create data backup. NetScaler instances in the recovery site are also discovered but, they do not have any traffic flowing through them. During the backup process, all data, files, and configurations are replicated on the disaster recovery node from the primary node.

Prerequisites

Before you set up the disaster recovery node, note the following the prerequisites:

- To enable disaster recovery settings, the primary site must have NetScaler ADM nodes configured in high availability mode.
- The standalone deployment of NetScaler ADM in the primary site does not support the disaster recovery feature.
- The NetScaler ADM HA pair (in primary site) and the standalone node (in DR site) must have same software version, build, and configurations.

Citrix recommends that you set CPU priority (in virtual machine properties) at the highest level to improve scheduling behavior and network latency.

The following table lists the minimum requirements to configure the Disaster Recovery node:

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage Space	Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation. If your NetScaler ADM storage requirement exceeds 120 GB, you have to attach an extra disk. **Note** You can add only one more disk. Citrix recommends you to estimate storage and attach more disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu and Fedora

First time disaster recovery setup

- Deploy NetScaler ADM in high availability mode
- Deploy and register the NetScaler ADM disaster recovery node
- Enable and disable disaster recovery settings from the user interface

Deploy NetScaler ADM in high availability mode

To set up the disaster recovery settings, ensure that NetScaler ADM is deployed in high availability mode. For information on deploying the NetScaler ADM in high availability, see High availability deployment

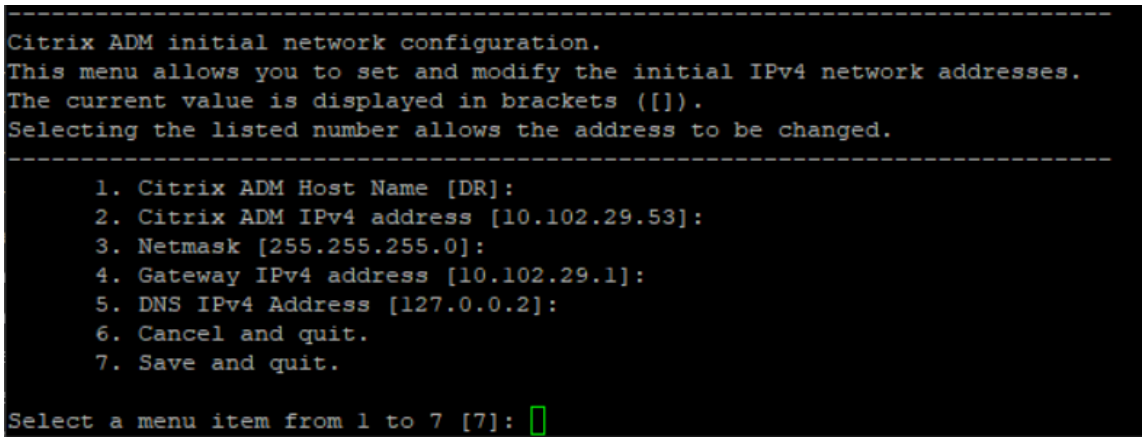
> **Note**
>
> - NetScaler ADM deployed in high availability mode must be upgraded to NetScaler ADM release version 13.1.
> - **Floating IP address is mandatory** to register disaster recovery node with the primary node.

Deploy and register the NetScaler ADM disaster recovery node using DR console

To register the NetScaler ADM disaster recovery node:

1. Download the `.xva` image file from the NetScaler site and import it into your hypervisor.
2. From the **Console** tab, configure NetScaler ADM with the initial network configurations.

   > **Note**
   >
   > The disaster recovery node can be on a different subnet.

3. After the initial network configuration is complete, the system prompts for login. Log on using the following credentials –`nsrecover`/`nsroot`.

   > **Important**
   >
   > Do not change the DR node credentials (`nsrecover`/`nsroot`) during registration. You can change the DR node credentials after you register DR node successfully.

4. To deploy the disaster recovery node, type **/mps/deployment_type.py** and press enter. The NetScaler ADM deployment configuration menu is displayed.


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. Select **2** to register disaster recovery node.

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. The console prompts for floating IP address of the high availability node and password.
7. Enter the floating IP address and password to register the disaster recovery node to the primary node.

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

The disaster recovery node is now registered successfully.

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
    ------------------------------------------------------------------------
```


> **Note**
>
> - The disaster recovery node does not have a GUI.
> - After registration is successful, the default administrator credentials to log on to the server are `nsroot`/`nsroot`.

8. If you want to change the DR node password, run the following script:

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Example:

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

Deploy the disaster recovery node using NetScaler ADM GUI

After the disaster recovery node is registered successfully using DR console, deploy the DR node from the NetScaler ADM GUI. This step enables the disaster recovery settings from the NetScaler ADM primary site.

1. Navigate to **System > System Administration > Disaster Recovery Settings.**
2. On the **Disaster Recovery** page, select **Deploy DR Node**.
3. A confirmation dialogue box is displayed. Click **Yes** to continue.

> **Note**
>
> The time taken for system backup depends on the data size and the WAN link speed.

After you deploy the DR node successfully in the NetScaler ADM GUI, you can monitor database state, memory, CPU, and disk usage of the DR node.

To disable the disaster recovery settings, select **Remove DR Node**. A confirmation dialogue box is displayed. Click **Yes** to continue.

To enable the DR node again, reconfigure the DR node for your high availability pair:

1. Log on to the DR node using a hypervisor or an SSH console.
2. Configure the DR node, by following the procedure available at Deploy and register the NetScaler ADM disaster recovery node using DR console.
3. Deploy the disaster recovery node using NetScaler ADM GUI.

For more information, see the FAQs.

> **Important**
>
> - It is the responsibility of the administrator to detect that a disaster has occurred on the primary site.
> - The disaster recovery workflow is manually initiated by the administrator after the primary site goes down.
> - An administrator must manually initiate the process by running a recovery script on the disaster recovery node at the recovery site.
> - If you upgrade the HA pair in primary site, you must also manually upgrade the standalone node in the DR site.

Workflow after the disaster

When the primary site goes down after a disaster, the disaster recovery workflow must be initiated as follows:

1. The administrator identifies that a disaster has struck the primary site and it is not operational.
2. The administrator initiates the recovery process.
3. The administrator must manually run one of the following recovery scripts on the disaster recovery node based on your requirement(at the recovery site):

   - Cofigure SNMP, Syslog, and Analytics on the DR node:

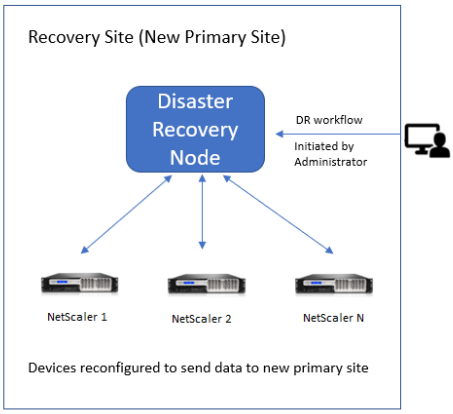
     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh

     <!--NeedCopy-->
     ```

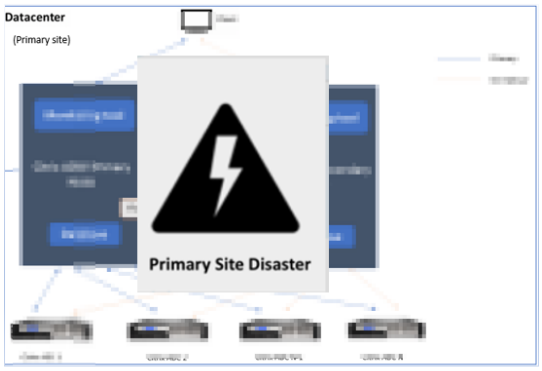
   - Configure the DR node as a license server also:

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -
        reconfig-ls <IP-address-of-the-primary-site>

     <!--NeedCopy-->
     ```

4. Internally, NetScaler instances are automatically reconfigured to send the data to the disaster recovery node that has now become the new primary site.

   The following image shows that the disaster recovery workflow after the primary site is struck with a disaster.





> **Note:**
>
> After you initiate the script at the DR site, the DR site now becomes the new primary site. You can also access the DR user interface.

Post disaster recovery

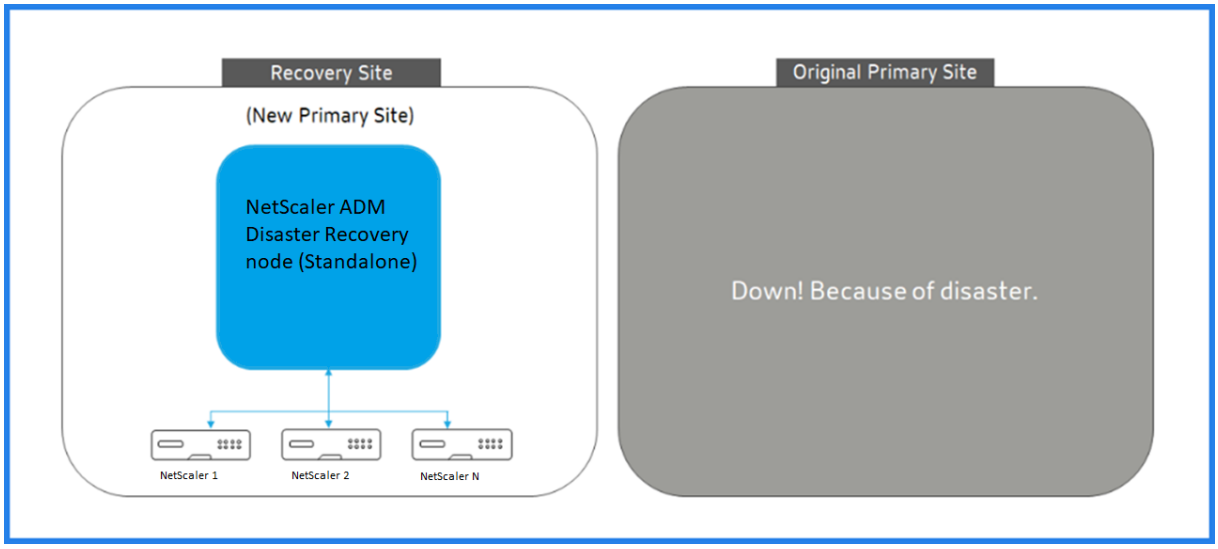
After the disaster has occurred and the administrator initiates the recovery script, the DR site now becomes the new primary site.

If you want to revert the configurations to the original site later, see Revert configurations to the original primary site.

> **Important**
>
> - If you have installed NetScaler ADM 12.1.49.x or earlier releases, you get a grace period of 30 days to contact Citrix to rehost the original license on the NetScaler ADM (at the DR site).
> - For 12.1.50.x or later releases, the NetScaler ADM license is automatically synchronized to the DR site (Not a requirement to contact Citrix for the license).
> - If you have applied pooled licenses for the instances, NetScalers with version **11.1 65.x or later**, **12.1 58.x or later**, **13.0 47.x or later**, and NetScaler SDX **13.0 76.x or later** have the support for auto-license server update in the DR site. All other versions, you must manually reconfigure the instances to the DR site.

Revert configurations to the original primary site

Post disaster the configured disaster recovery (DR) node becomes the new primary site and the client traffic flows through this node.



For more information, see Workflow after the disaster.

When your original primary site is free from disaster and you decide to move all operations to the primary site, reconfigure the original primary site to match the configurations from the DR node.

Before you begin, ensure both primary site and DR site are active.

To revert the changes to the original primary site from the DR site, perform the following steps:

1. Log in to the original primary site and run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password> &
<!--NeedCopy-->
```

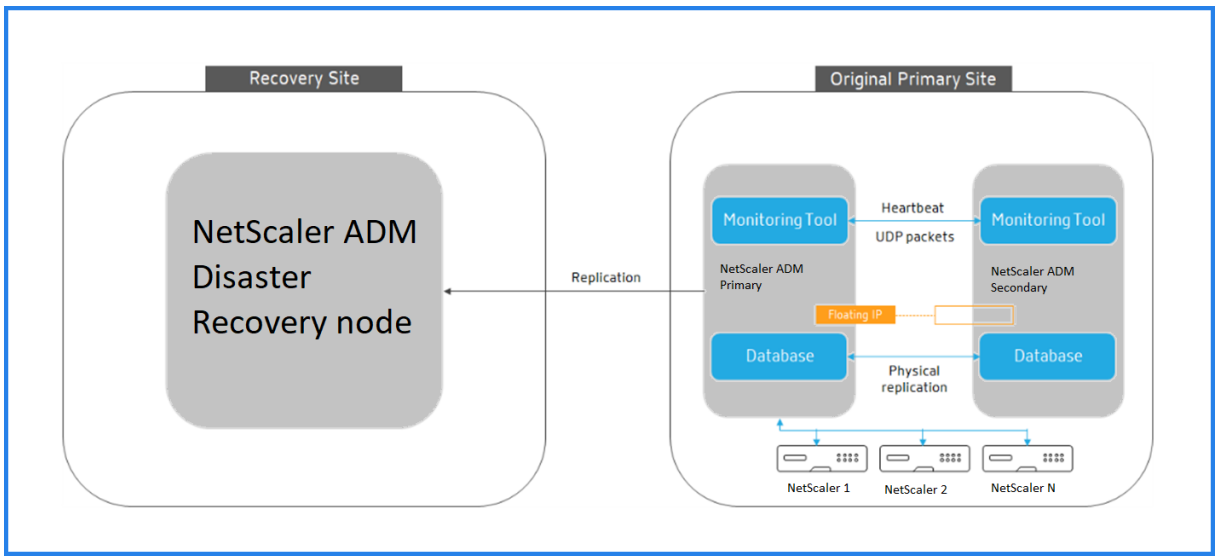
   This command configures only Syslog, SNMP, and Analytics to the primary site.

   If you want to configure the primary site as a pooled license server for ADC instances, run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

   The `-O` command fetches the DR site IP address and reconfigures the primary site as pooled license server.

2. Reconfigure the DR site. See, Deploy disaster recovery setup.



After you successfully revert the configurations from the DR site to the original primary site, the client traffic flows through the NetScaler ADM primary node.

Configure on-prem agents for multisite deployment

March 11, 2024

In the earlier versions of NetScaler ADM, NetScaler instances deployed in remote data centers can be managed and monitored from NetScaler ADM running in a primary data center. NetScaler instances sent data directly to the primary NetScaler ADM that resulted in consumption of WAN bandwidth. Also, processing of analytics data utilizes CPU and memory resources of the primary NetScaler ADM.

You can have data centers located across the globe. Agents play a vital role in the following scenarios:

- To install agents in remote data centers so that there is reduction in WAN bandwidth consumption.
- To limit the number of instances directly sending traffic to primary NetScaler ADM for data processing.

> **Note**
>
> - Installing agents for instances in remote data center is recommended but not mandatory. If necessary, users can directly add NetScaler instances to primary NetScaler ADM.
> - If you have installed agents for one or more remote data centers, then the communication between the agents and the primary site is through floating IP address. For more informa-

> tion, see port.
>
> - You can install agents and apply pooled licenses to the instances at one or more remote data centers. In this scenario, the communication between the primary site and one or more remote data centers is through the floating IP address.
> - NetScaler ADM on-premises agent doesn't support pooled licensing.

From NetScaler ADM 12.1 or later, instances can be configured with agents to communicate with the primary NetScaler ADM located in a different data center.

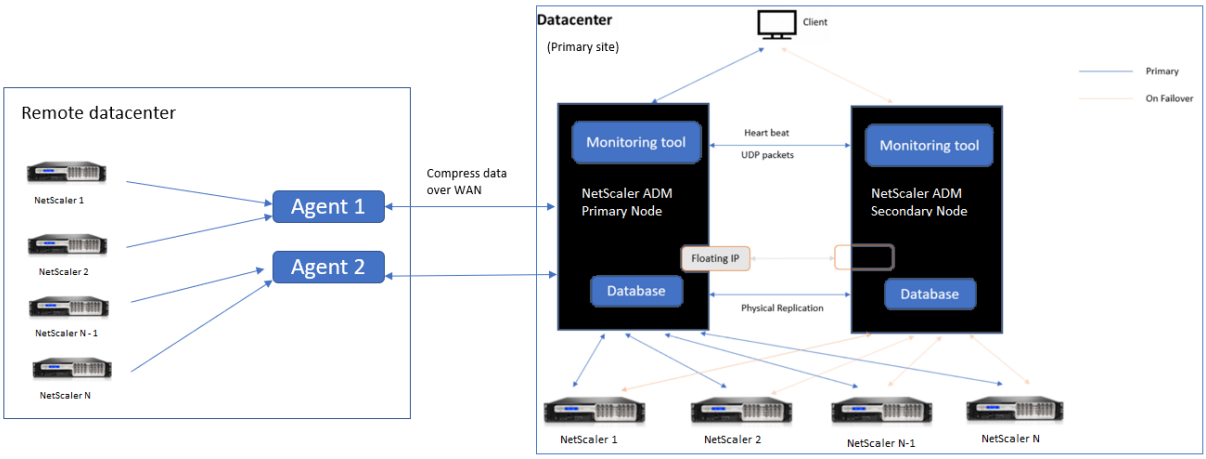
Agents work as an intermediary between the primary NetScaler ADM and the discovered instances across different data centers. Following are the benefits of installing agents:

- The instances are configured to agents so that the unprocessed data is sent directly to agents instead of primary NetScaler ADM. Agents do the first level of data processing and send the processed data in compressed format to the primary NetScaler ADM for storage.
- Agents and instances are co-located in the same data center so that the data processing is faster.
- Clustering the agents provides redistribution of NetScaler instances on agent failover. When one agent in a site fails, traffic from NetScaler instances is switched to another available agent in the same site.

> **Note**
>
> The number of agents to be installed per site depends on the traffic being processed.

Architecture

The following figure shows NetScaler instances in two data centers and NetScaler ADM high availability deployment using multisite agent-based architecture.



The primary site has the NetScaler ADM nodes deployed in a high availability configuration. The NetScaler instances in the primary site are directly registered with the NetScaler ADM.

In the secondary site, agents are deployed and registered with the NetScaler ADM server in the primary site. These agents work in a cluster to handle continuous flow of traffic in case an agent failover occurs. The NetScaler instances in the secondary site are registered with the primary NetScaler ADM server through agents located within that site. The instances send data directly to agents instead of primary NetScaler ADM. The agents process the data received from the instances and send it to the primary NetScaler ADM in a compressed format. Agents communicate with the NetScaler ADM server over a secure channel and the data sent over the channel is compressed for bandwidth efficiency.

Get started

- Install the agent in a data center
  - Register the agent
  - Attach the agent to a site
- Add NetScaler instances
  - Add new instance
  - Update an existing instance

Install the agent in a data center

You can install and configure the agent, to enable communication between the primary NetScaler ADM and the managed NetScaler instances in another data center.

You can install an agent on the following hypervisors in your enterprise data center:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM Server

> **Note**
>
> On-prem agents for multisite deployment are supported only with NetScaler ADM high availability deployment.

Before you begin installing the agent, ensure you have the required virtual computing resources that the hypervisor must provide for each agent.

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

Ports

For communication purposes, the following ports must be open between the agent and NetScaler ADM on-prem server.

Type	Port	Details	Direction of communication
TCP	8443, 7443, 443	For outbound and inbound communication between agent and the NetScaler ADM on-prem server.	NetScaler agent to NetScaler ADM

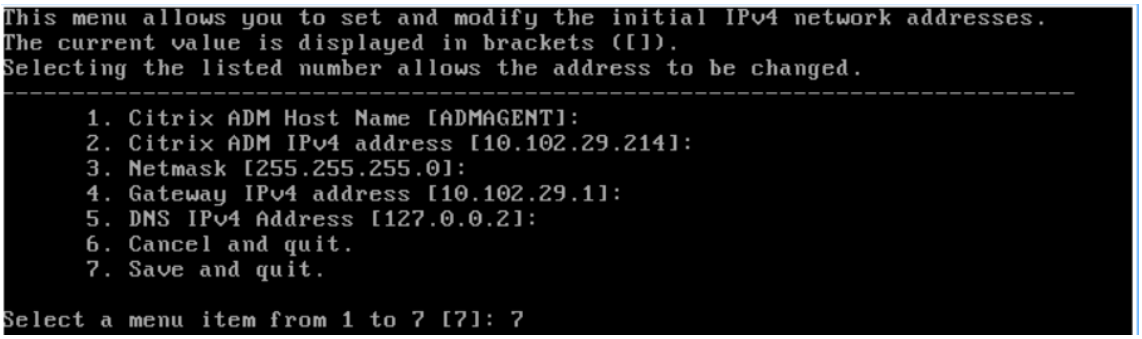
The following ports must be open between the agent and NetScaler Instances.

Type	Port	Details	Direction of communication
TCP	80	For NITRO communication between agent and NetScaler instance.	NetScaler ADM to NetScaler and NetScaler to NetScaler ADM

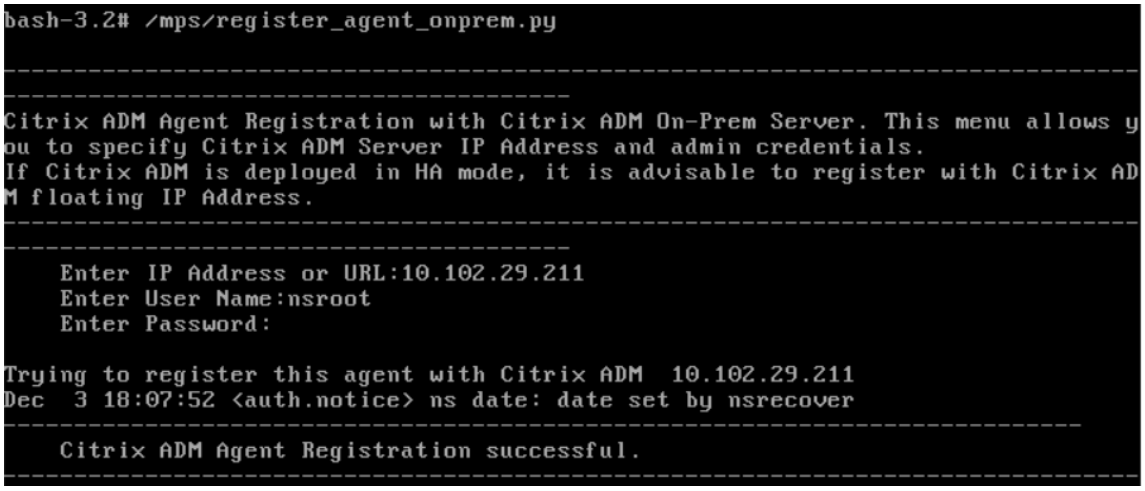
Type	Port	Details	Direction of communication
TCP	22	For SSH communication between agent and NetScaler instance. For synchronization between NetScaler ADM servers deployed in high availability mode.	NetScaler ADM to NetScaler and NetScaler agent to NetScaler
UDP	4739	For AppFlow communication between agent and NetScaler instance.	NetScaler to NetScaler ADM
ICMP	No reserved port	To detect network reachability between NetScaler ADM and NetScaler instances, or the secondary NetScaler ADM server deployed in high availability mode.	
UDP	161, 162	To receive SNMP events from NetScaler instance to agent.	Port 161 - NetScaler ADM to NetScaler Port 162 - NetScaler to NetScaler ADM
UDP	514	To receive syslog messages from NetScaler instance to agent.	NetScaler to NetScaler ADM
TCP	5557	For Logstream communication between agent and NetScaler instances.	NetScaler to NetScaler ADM

Register the agent

1. Use the agent image file downloaded from the NetScaler site and import it in to your hypervisor. The naming pattern of the agent image file is as follows, **MASAGENT-<HYPERVISOR>-<Version.no>.** For example: **MASAGENT-XEN-13.0-xy.xva**
2. From the **Console** tab, configure NetScaler ADM with the initial network configurations.
3. Enter the NetScaler ADM host name, IPv4 address, and gateway IPv4 address. Select option 7 to save and quit the configuration.



4. After the registration is successful, the console prompts to log on. Use *nsrecover/nsroot* as the credentials.
5. To register the agent, enter **/mps/register_agent_onprem.py**. The NetScaler agent registration credentials are displayed as shown in the following image.
6. Enter the NetScaler ADM floating IP address and the user credentials.



After the registration is successful, the agent restarts to complete the installation process.

After the agent restarts, access the NetScaler ADM GUI, from the main menu go to the **Infrastructure > Instances > Agents** page to verify the status of the agent. The newly added agent is displayed in **Up** state.

> **Note**
>
> The NetScaler ADM displays the version of the agent and also checks if the agent is on the latest version. The download icon signifies that the agent is not on the latest version and needs to be upgraded. Citrix recommends that you upgrade the agent version to the NetScaler ADM version.

Attach an agent to a site

1. Select the agent and click **Attach Site.**
2. In the **Attach site** page, select a site from the list, or create a site using the plus (+) button.
3. Click **Save.**

> **Note**
>
> - By default, all newly registered agents are added to the default data center.
> - It is important to associate the agent with the correct site. In the event of an agent failure, the NetScaler instances assigned to it are automatically switched to other functioning agents in the same site.

Agent actions

You can apply various actions to an agent under **Infrastructure > Agents > Select Actions**.

Under **Select Action**, you can use the following features:

Install a new certificate: if you need a different agent certificate to meet your security requirement, you can add one.

Change the default password: to ensure security of your infrastructure, change the default password of an agent.

Generate a technical support file: generate a technical support file for a selected NetScaler agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

Add NetScaler instances

Instances are NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler ADM through agents. You can add the following NetScaler ADC appliances and virtual appliances to NetScaler ADM or agents:

- NetScaler MPX
- NetScaler VPX

- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Citrix SSL Forward Proxy

For more information, see Add instances to NetScaler ADM.

Attach an existing instance to the agent

If an instance is already added to the primary NetScaler ADM, you can attach it to an agent by editing an agent.

1. Navigate to **Infrastructure > Instances** and select the instance type. For example, NetScaler.
2. Click **Edit** to edit an existing instance.
3. Click to select the agent.
4. From the **Agent** page, select the agent with which you want to associate the instance and then click **OK**.

> **Note**
>
> Ensure to select the **Site** with which you want to associate the instance.

Access the GUI of an instance to validate events

After the instances are added and agent is configured, access the GUI of an instance to check if the trap destination is configured.

In NetScaler ADM, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instance you want to access (for example, NetScaler VPX), and then click the IP address of a specific instance.

The GUI of the selected instance is displayed in a pop-up window.

By default, the agent is configured as the trap destination on the instance. To confirm, log on to the GUI of the instance and check the trap destinations.

> **Important**
>
> Adding an agent for NetScaler instances in remote data centers is recommended but not mandatory.

> In case you want to add the instance directly to the primary MAS, do not select **an agent** while adding instances.

NetScaler agent failover

The agent failover can occur in a site that has two or more registered agents. When an agent becomes inactive (DOWN state) in the site, the NetScaler ADM redistributes the ADC instances of the inactive agent with other active agents.

> **Important**
>
> - Ensure the **Agent Failover** feature is enabled on your account. To enable this feature, see Enable or disable ADM features.
> - If an agent is running a script, ensure that script is present on all the agents in the site. Therefore, the changed agent can run the script after agent failover.

To attach a site to an agent in the ADM GUI, see Attach an agent to a site.

To achieve an agent failover, select NetScaler agents one by one and attach to the same site.

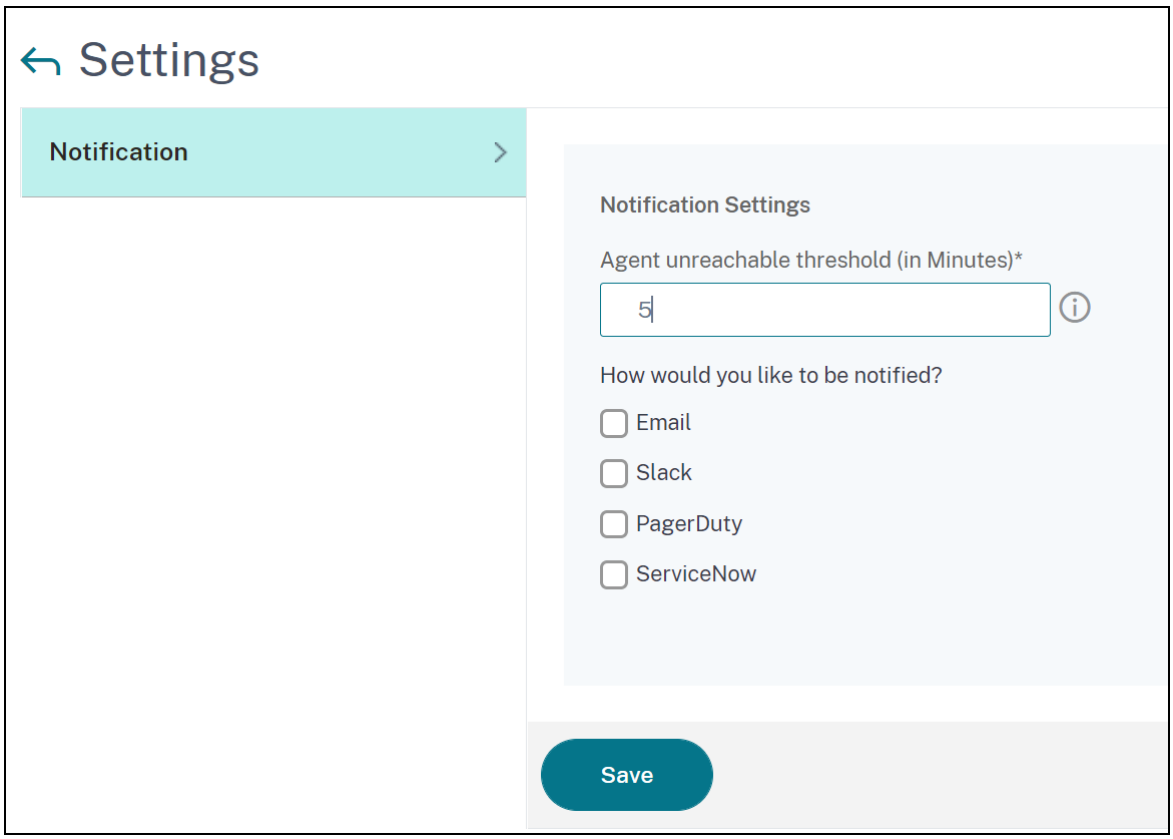
For example, two agents 10.106.1xx.2x and 10.106.1xx.3x are attached and operational in the Bangalore site. If one agent becomes inactive, NetScaler ADM detects it and displays the state as down.

When a NetScaler agent becomes inactive (Down state) in a site, NetScaler ADM waits for five minutes for the agent to become active (Up state). If the agent remains inactive, NetScaler ADM automatically redistributes the instances among available agents in the same site.

NetScaler ADM triggers instance redistribution every 30 minutes to balance the load among active agents in the site.

Configure agent unreachable threshold and notification

If an agent is down or not reachable for a certain duration, you can get notification on the agent status through email, slack, PagerDuty, and ServiceNow. In **Infrastructure > Instances > Agents**, click **Settings**, specify the duration between 5 minutes and 60 minutes, and select the notification method that you want to get notified.



Install an ADM agent as a microservice on a Kubernetes cluster

March 11, 2024

Deploying a NetScaler agent as a microservice is useful for managing your NetScaler CPX. The procedures available in this document are applicable only if the NetScaler ADM and Kubernetes cluster are configured on a different network. In this scenario, you can configure an ADM agent as a microservice, where the Kubernetes cluster is hosted.

> Note
>
> You can also configure an on-prem agent and register the agent on the network, where the Kubernetes cluster is hosted.

Get started

1. In NetScaler ADM, navigate to **Infrastructure > Instances > Agents**.
2. From the **Select Action** list, select the **Download Agent Microservice** option.

3. In the **Download Agent Microservice** page, specify the following parameters:

   a) **Application ID** –A string id to define the service for the agent in the Kubernetes cluster and distinguish this agent from other agents in the same cluster.

   b) **Password** –Specify a password for CPX to use this password to onboard CPX to ADM through the agent.

   c) **Confirm Password** –Specify the same password for confirmation.

   > Note
   >
   > You must not use the default password (`nsroot`).

   d) Click **Download Yaml File**.

Install NetScaler agent in Kubernetes cluster

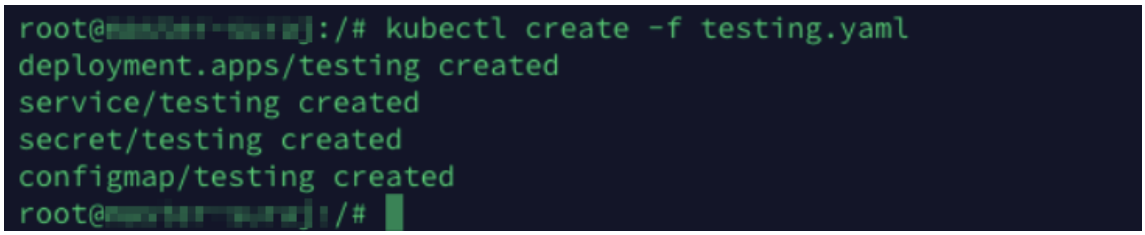
In the Kubernetes main node:

1. Save the downloaded YAML file
2. Run the following command:

   `kubectl create -f <yaml file>`

   For example, `kubectl create -f testing.yaml`

   The agent is successfully created.



In NetScaler ADM, navigate to **Infrastructure > Instances > Agents** to see the agent status.

After you configure the agent, you can add the NetScaler CPX instances and view analytics in service graph. For more information, see:

- Adding NetScaler CPX Instances to NetScaler ADM.
- Setting up service graph.

Migrate NetScaler ADM single-server deployment to a high availability deployment

March 11, 2024

You can upgrade your NetScaler ADM single server to a high availability deployment of two NetScaler ADM servers. A high availability pair of NetScaler ADM servers is in active-passive mode, and both the servers have the same configuration. In this type of active-passive deployment, one NetScaler ADM server is configured as the primary node and the other as the secondary node. If for any reason, the primary node goes down, the secondary node takes over.

To migrate a NetScaler ADM single server to a high availability pair, you need to provision a new NetScaler ADM server node, configure it as the second NetScaler ADM single server, and deploy both the NetScaler ADM servers as a high availability pair.

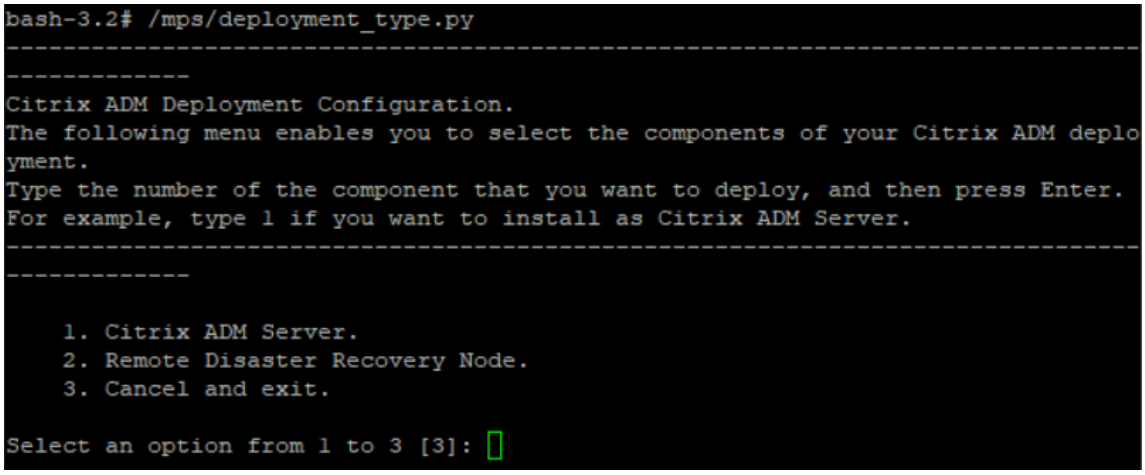
Migrating a NetScaler ADM single server to a high availability mode involves the following steps:

1. Modifying the existing server node
2. Provisioning the second server node
3. Deploying the two nodes in HA mode
4. Configuring the high availability pair

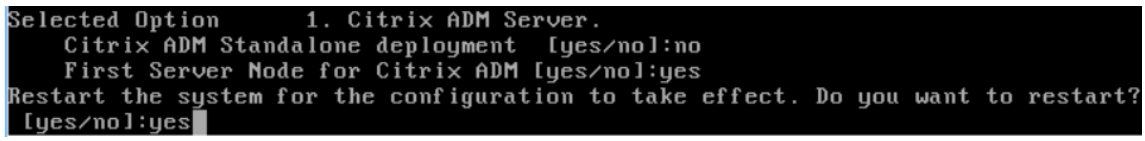
Modify the existing NetScaler ADM server node

To migrate the NetScaler ADM from single server to high availability mode, you have to change the initial deployment type of the server node to high availability mode.

1. On a workstation or laptop, open the console of the existing NetScaler ADM server node. For example, consider that you have deployed a NetScaler ADM with IP address as 10.106.171.17 as a standalone server.
2. Log on to NetScaler ADM. The default credentials are `nsroot` and `nsroot`.
3. In the shell prompt, type `/mps/deployment_type.py`, and press **Enter**.
4. Select the deployment type as NetScaler ADM server. If you do not select any option, by default, it is deployed as a server.



5. The deployment console prompts you to select the server deployment (as standalone). Type **No** to confirm the deployment as high availability pair.
6. The console prompts you to select the (first server node). Enter **Yes** to confirm the node as the first server node.
7. The console prompts you to restart the server.
8. Type **Yes** to restart.



Provision the second server node

You have to provision the second server on your hypervisor. Use the same image file that you used to install the first server, or obtain an image file of the same version from the NetScaler site.

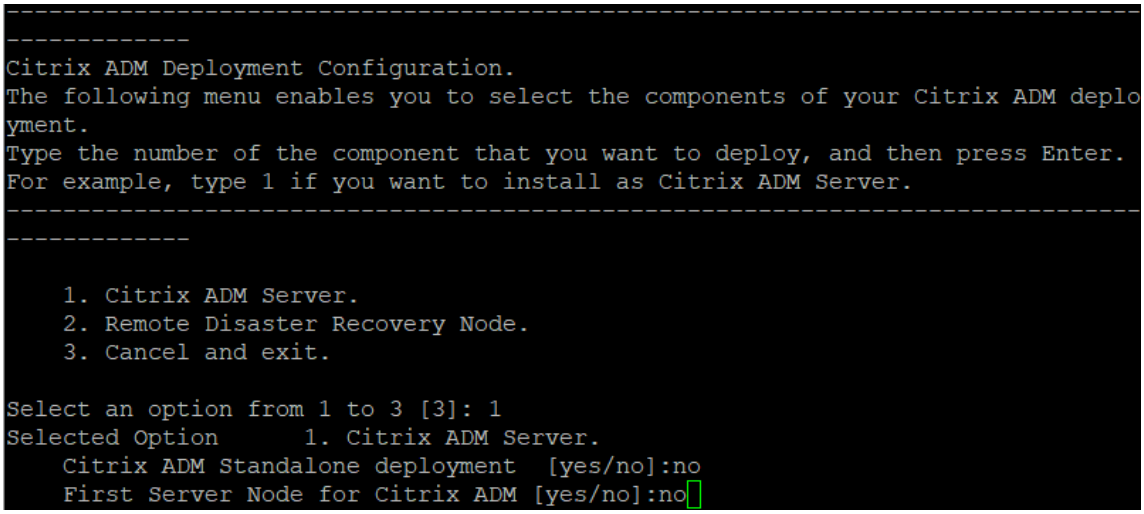
1. Import the image file to your hypervisor, and then from the Console tab configure the initial network configuration options as explained on the following screen:


```
--------------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Host Name [CitrixADM]:
      2. Citrix ADM IPv4 address [10.102.29.211]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

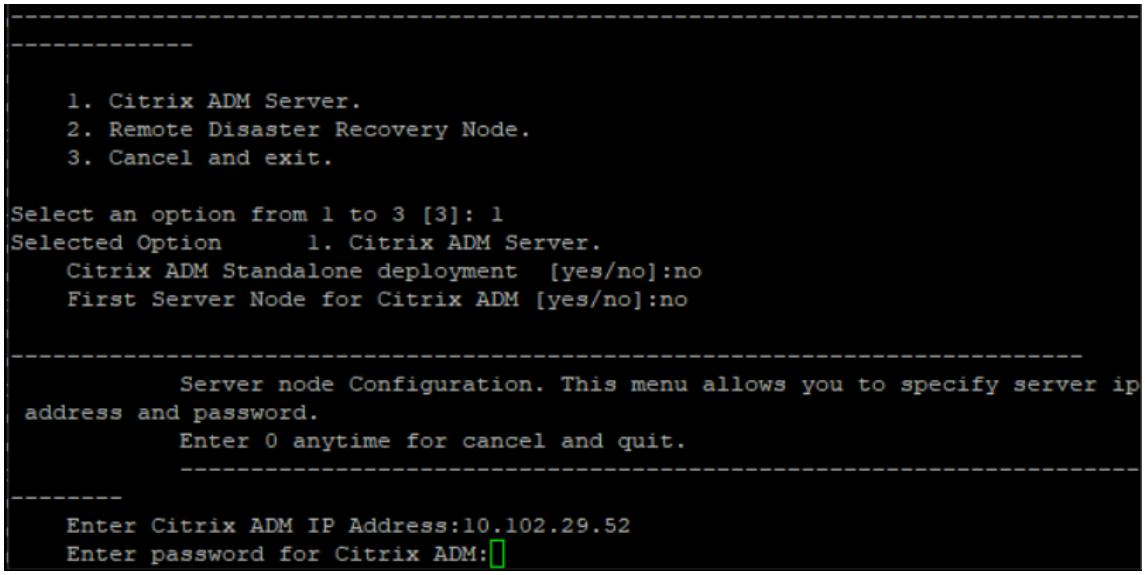
2. After specifying the required IP addresses, in the shell prompt, type /mps/deployment_type.py, and press enter.
3. Select the deployment type as **NetScaler ADM server**.
4. The deployment console prompts you to select the server deployment (as standalone). Type **No** to confirm the deployment as high availability pair.

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

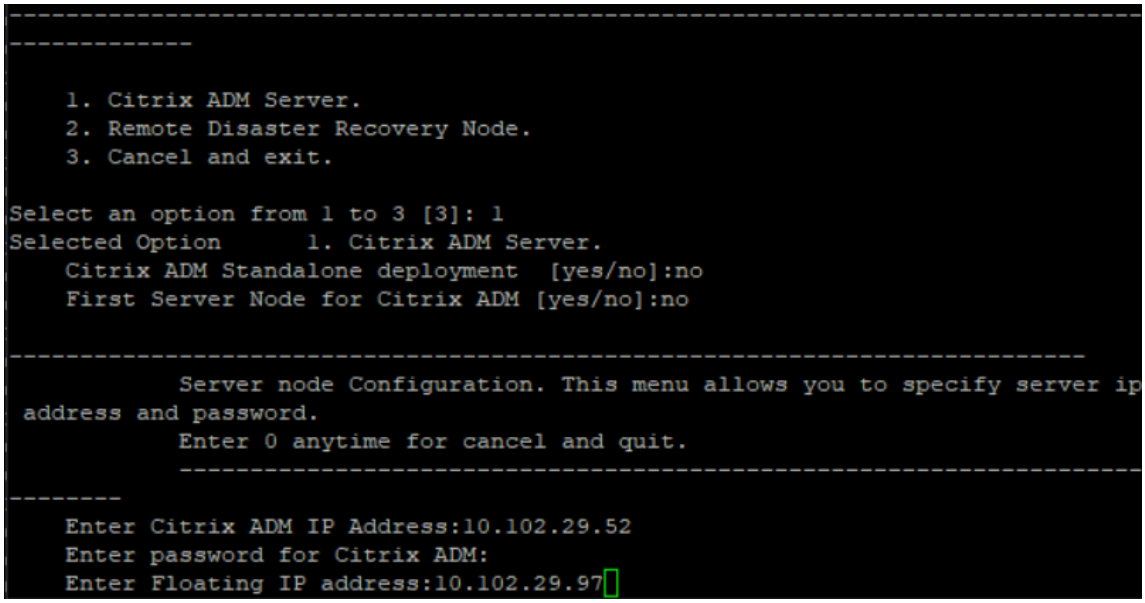
5. The console then prompts you to select the (first server node). Type **No** to confirm the node as the second server node.



6. Enter the first server's IP address and password.



7. Enter the floating IP address of the first node.



8. The console prompts you to restart the system. Enter **Yes** to restart.

Deploy the two servers in a high availability mode

To complete the installation process of the two server nodes as a high availability pair, you have to deploy these nodes from the GUI of the previously existing NetScaler ADM server node. Internal communication between the two servers starts when you deploy the two server nodes.

> **Important**
>
> Before deploying high-availability nodes, ensure to change the default password.

1. In a web browser, type the IP address of the previously existing NetScaler ADM server node.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **System** tab, navigate to **Deployment** and click **Deploy**.
4. A confirmation message appears. Click **Yes**.

   > **Note**
   >
   > After you deploy NetScaler ADM in high availability, you can either access the primary node or the floating IP address. You cannot access the secondary node from 12.1 release onwards.

5. Though you have entered the floating IP while configuring the second server node, you have an option to update the FIP on the **Systems** page. Click **HA Settings** > **Configure Floating IP Address for High Availability Mode**. You can view the floating IP address you configured earlier. You can enter a new IP address and click **OK**.

Migrate from NetScaler Insight Center to NetScaler ADM

March 11, 2024

You can now migrate your NetScaler Insight Center deployment to NetScaler ADM without losing the existing configuration, settings, or data. With NetScaler ADM you can not only view the various analytics generated by the NetScaler instances associated with an application, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

> **Note**
>
> Migration is currently supported only on NetScaler Insight Center Standalone instances.

Prerequisites

Before migrating the NetScaler Insight Center virtual appliance to NetScaler ADM, verify that the following requirements have been met:

- NetScaler Insight Center 11.1 Build 47.14 or later is installed.
- You have downloaded the NetScaler ADM 12.0 build 57.24 .tgz image file.

  > **Note**
  >
  > You must install NetScaler ADM 12.0 build 57.24 and then upgrade to the latest NetScaler ADM 13.1 build. For more information, see Upgrade.

- You have downloaded the NetScaler ADM 13.1 latest build .tgz image file.

Hardware requirement

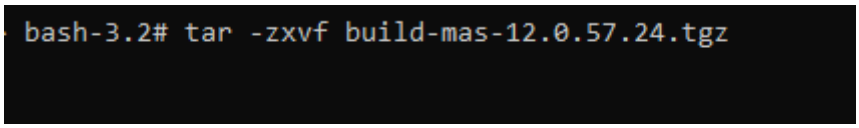
Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	120 GB **Note** Citrix recommends that you use **500 GB** for better performance. Also, Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.

Component	Requirement
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor Requirements	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Installation procedure

To migrate NetScaler Insight Center to NetScaler ADM:

1. Log on to the shell prompt of NetScaler Insight Center.
2. Download the NetScaler ADM 12.0 build 57.24 to the */var/mps/mps_images* folder.
3. Untar the TGZ file by using the **tar -zxvf build-mas-12.0-57.24.tgz** command.



4. Install NetScaler ADM by using the **./installmas** command.

5. After installing NetScaler ADM 12.0 build 57.24, you need to upgrade to the latest NetScaler ADM 13.1 build by performing the above steps.

After the migration, all the NetScaler instances that were discovered in the NetScaler Insight Center inventory appear in the **Infrasturcture > Instances** section of NetScaler ADM. However, for the first time you need to manually poll the virtual servers hosted in the discovered appliances.

> **Note**
>
> In NetScaler ADM, by default, there is no licensing cost to manage and monitor two virtual servers created within the discovered NetScaler instances. To monitor and manage more than two vir-

> tual servers, install the required NetScaler ADM licenses. For more details, see NetScaler ADM Licensing.

Integrate NetScaler ADM with Citrix Director

March 11, 2024

Director integrates with NetScaler ADM for network analysis and performance management.

- Network analysis obtains HDX Insight reports from NetScaler ADM and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment.
- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you integrate NetScaler ADM with Director, HDX Insight reports provide you with the following information in Director:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Prerequisites

Hardware requirements for HDX Insight to NetScaler ADM Migration

Component	Requirement
RAM	32 GB
Virtual CPU	8
Storage Space	500 GB. Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps

Minimal requirements

Before you configure the network integration, ensure that you create an RBAC user with HDX Insights access.

Software requirements

Before migrating to the NetScaler ADM virtual appliance, verify that the following requirements have been met:

- Director version 1811 is installed
- NetScaler HDX Insight version 10.1 or later is installed
- HDX Insight and NetScaler ADM support Citrix VDA version 7.0 and later
- Citrix Workspace is supported on Citrix Virtual Apps and Desktops version 7.0 and later
- Ensure that MAC Citrix Workspace for Mac version 11.8 and later, and Windows Citrix Workspace for Windows 14.0 and later are available to display accurate ICA RTT metrics
- NetScaler ADM version 11.0 and later is installed. For more information on how to install NetScaler ADM, see Deploy NetScaler ADM.

Limitations

- The availability of this feature depends on your organization's license and your administrator permissions.
- ICA session Round Trip Time (RTT) shows data correctly for Citrix Workspace for Windows 3.4 or later and for Citrix Workspace for Mac 11.8 or later. For earlier versions of these Workspaces, the data does not display correctly.
- In the Trends view, HDX connection logon data is not collected for VDAs earlier than version 7. For earlier VDAs, the chart data is displayed as 0.
- For deployments that already have an external hard disk with storage space less than 500 GB, you cannot add another hard disk.

> **Note**
>
> - For more information on Director and for steps to integrate NetScaler ADM with Director, see https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html.
> - For more information on HDX Insight, see http://docs.citrix.com/en-us/xenapp-and-

> xendesktop/7-11/director/hdx-insight.html.

Attach an extra disk to NetScaler ADM

March 11, 2024

NetScaler Application Delivery Management (ADM) storage requirement is determined based on your NetScaler ADM sizing estimation. By default, NetScaler ADM provides you a storage capacity of 120 GB. If you need more than 120 GB for storing your data, you can attach an extra disk.

> **Note**
>
> - Estimate storage requirements and attach an extra disk to the server at the time of initial deployment of NetScaler ADM.
> - For a NetScaler ADM single-server deployment, you can attach only one disk to the server in addition to the default disk.
> - For a NetScaler ADM high availability deployment, you must attach an extra disk to each node. The size of both disks must be identical.
> - If you had earlier attached an external disk of lower capacity, you must remove the disk before attaching a new disk.
> - You can attach an extra disk of capacity greater than 2 terabytes. If necessary, the size of the disk can be lower than 2 terabytes also.
> - Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.

This document explains the following scenarios about attaching an extra, new disk, creating partitions, and resizing the additional disks:

1. Attach a new, extra disk
2. Launch the disk partitioning tool
3. Create partitions in the new, extra disk
4. Resize the existing extra disk
5. Remove partitions on the additional disk

Attach an extra disk in a standalone NetScaler ADM

Perform the following steps to attach a disk to the virtual machine:

1. Shut down the NetScaler ADM virtual machine.
2. In the hypervisor, attach an extra disk of the required disk size to NetScaler ADM virtual machine.

   The newly attached larger disk stores the database data and NetScaler ADM log files. The existing 120-gigabytes default disk is now used to store the core files, operating system log files, and so on.
3. Start the NetScaler ADM virtual machine.

NetScaler ADM disk partition tool

NetScaler ADM now provides **NetScaler ADM disk partition tool**, a new command line tool. The functionalities of this tool are described in detail as follows:

1. Using the tool, you can create partitions in the newly added extra disk.
2. You can also resize existing extra disk using this tool. But the existing external disk must not be greater than 2 terabytes.

   > **Note**
   >
   > - It is not possible to resize existing disks beyond 2 terabytes without losing data. This is due to a known limitation on the platform.
   > - To create a storage capacity greater than 2 terabytes, you must remove the existing partitions and create partitions using this new tool.

3. Using this new tool, you can perform any partition action on the disk explicitly. The tool provides you with clear visibility and control over the disk and the associated data.

   > **Note**
   >
   > You can only use this tool on the additional disk that you have attached to the NetScaler ADM server. You cannot create partitions in the primary (default) 120-gigabytes disk using this tool.

Launch the disk partition tool

1. Open an SSH connection to the NetScaler ADM by using an SSH client, such as PuTTY.
2. Log on to the NetScaler ADM by using the `nsrecover`/`nsroot` credentials.
3. Switch to the shell prompt and type:

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```



```
bash-3.2# /mps/DiskPartitionTool.py

---------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
---------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> **Note**
>
> For NetScaler ADM in high availability deployment, you must launch the tool in both nodes and create or resize partitions after attaching disks to the respective virtual machines.

Create partitions in the new additional disk

The **create** command is used to create partitions whenever a new secondary disk is added. You can also use this command to create partitions on an existing secondary disk after the existing partitions are deleted using the “remove”command.

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> **Note**
>
> There is no 2 terabytes size limitation while creating partitions with the disk partition tool. The tool can create partitions larger than 2 terabytes. When you partition the disk, a swap partition of size 32 GB is automatically added. The primary partition then uses all the remaining space on the disk.

Once the command is run, a GUID partition table (GPT) partition scheme is created. Also a 32 GB swap partition and data partition are created to use rest of the space. A new file system is then created on the primary partition.

> **Note**
>
> This process can take a few seconds, and you must not interrupt the process.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```



```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Once the create command completes, the virtual machine is automatically restarted for the new partition to get mounted.

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

After the restart, the new partition is mounted at /var/mps.

```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

The swap partition added shows up as swap space in the output of the "create"command.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Note**
>
> The tool restarts the virtual machine after you have created the partition.

Resize the partitions in the existing additional disk

You can use the **resize** command to resize the attached (secondary) disk. You can resize a disk that has a `master boot record` (MBR) or GPT scheme. The size of the disk must be less than 2 terabytes in size to a maximum of 2 terabytes.

Note

- The “resize”command is designed to function without losing any existing data. But Citrix recommends that you back up critical data in this disk to external storage before attempting the resize. Data backup is helpful in cases where the disk data can get corrupted during the resize operation.
- Ensure to increase the disk space in increments of 100 GB of space while resizing the partitions. Such an incremental increase ensures that you would not have to resize more frequently.

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

The “resize”command checks for all preconditions and proceeds if all preconditions are met and after you have given consent to resizing. It stops the processes accessing the disk, which includes the NetScaler ADM subsystems, PostgreSQL DB processes, and NetScaler ADM monitor process. Once the processes are stopped, the disk is unmounted to prepare it for resizing. The resizing is done by extending the partition to occupy the complete available space and then growing the file system. If a swap partition exists on the disk, it is deleted and recreated at the end of the disk after resizing. The swap partition is discussed in the **Create** command section of the document.

Note

The “growing file system”process can take some to complete and take care that you do not interrupt the process while it is in progress. The tool restarts the virtual machine after you have resized the partition.

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```



```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

All the intermediate steps in the resize process (stopping applications, resizing disk, growing filesystem) are shown on the console. Once the process completes, the following message is seen.

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

After rebooting, the increase in size can be observed using the "df"command. Here is the before and after details after you increase the size:

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

Remove the partitions in the additional disk

An existing partition on the secondary disk can be resized up to 2 terabytes. This is due to a known limitation on the partition. If you want a disk larger than 2 terabytes, either attach a new disk and partition it by using the disk partition tool. You can also remove the existing partition by using the **remove** command, and then create a partition.

> **Note**
>
> Removing the existing partition deletes all existing data. So, any critical data must be backed up to external storage before using this command.


```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Running the "remove"command asks you for confirmation and once confirmed, it stops all processes (such as ADM subsystems, PostgreSQL processes, and ADM monitor) using the secondary disk. If a swap partition exists and swap is enabled on the partition, then the swap is disabled.

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

When you type "y,"the command unmounts the disk and removes all partitions on the disk.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

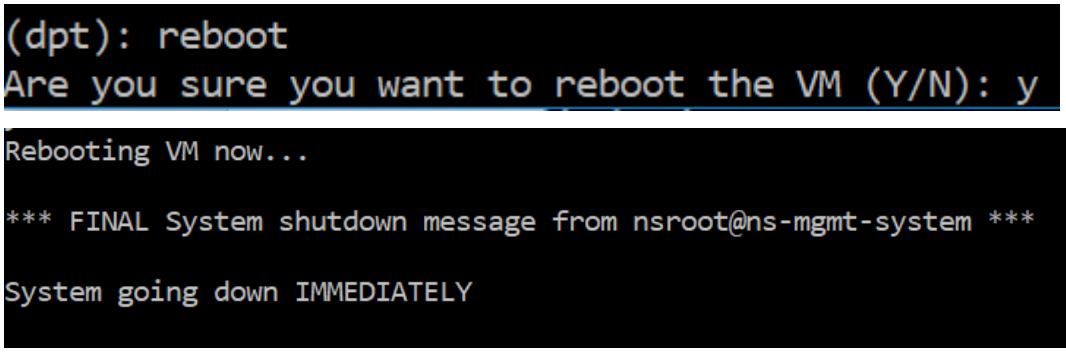
> **Note**
>
> The tool restarts the virtual machine after you have removed the partition.

Restart the virtual machine

When a partition is created or resized, or when a swap file is created, restart the virtual machine. The changes take effect only after restarting. For this purpose, a **reboot** command is provided in the tool.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

You are prompted for confirmation and once confirmed, it stops all processes (such as ADM subsystems, PostgreSQL processes, and ADM monitor.) The virtual machine is then restarted.



Create a backup file of the disk data

Here are the steps to follow to backup NetScaler ADM data before resizing or removing the partitions.

> **Note**
>
> Creating a backup file requires disk space. Citrix recommends that you ensure there is sufficient disk space available (50% or more) before backup commands are run.

1. Stop ADM.

```
/mps/masd stop
<!--NeedCopy-->
```

2. Stop PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. Stop ADM Monitor.

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. Create a tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> **Note**
>
> The operation takes time depending on the size of the data to be backed up.

5. Generate checksum.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```


6. Copy the tarball and checksum files to a remote server.
7. Validate the correctness of the copied tarball. Generate a checksum of the transferred file and compare with the source checksum.
8. Remove the tarball from the ADM virtual machine.

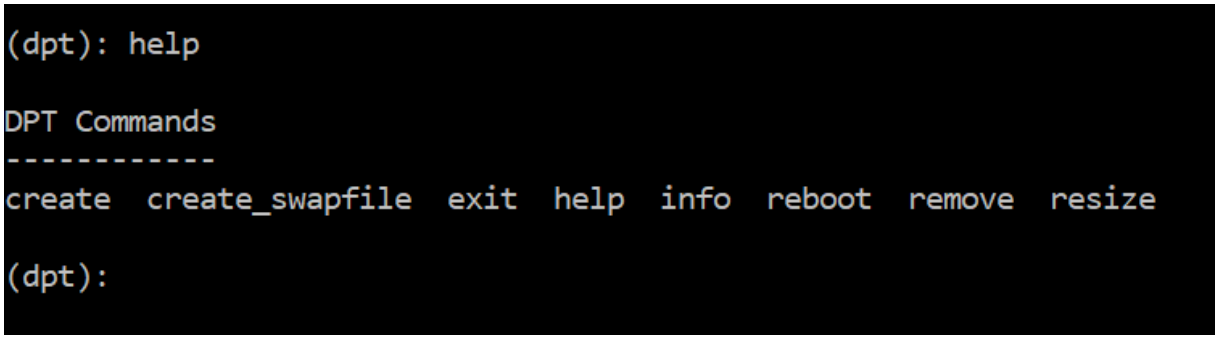
```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

Additional commands

In addition to the commands listed earlier, you can also use the following commands in the tool:

Help command:

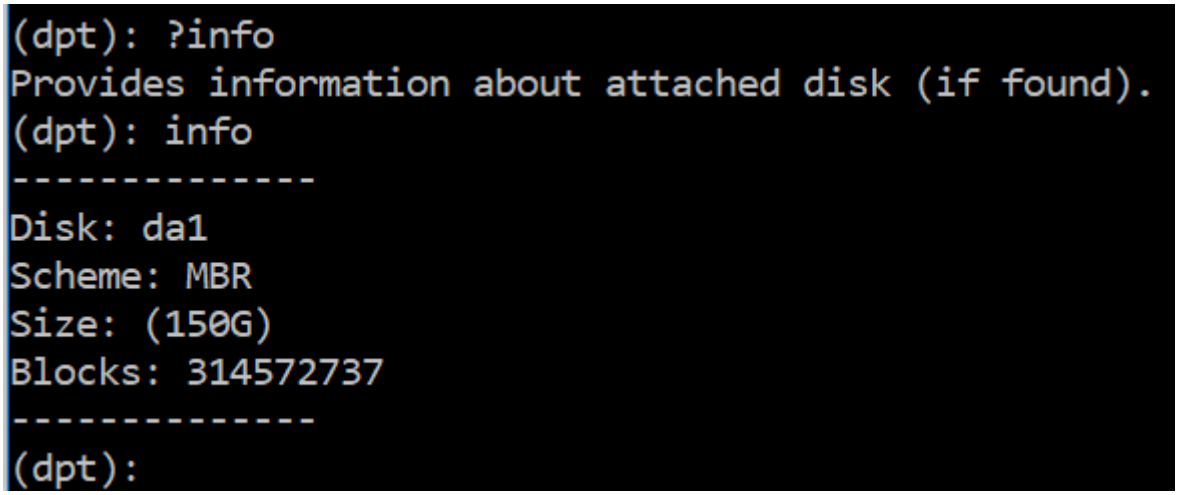
To list the supported commands, type **help** or **?** and press enter. To get further help on each of the command press **help** or **?** followed by the command name and press the **Enter** key.



Info command:

The **info** command provides information about the attached secondary disk if the disk exists. The command provides the device name, the partition scheme, size in human-readable form, and the number of disk blocks. The scheme can be MBR or GPT. An MBR scheme means the disk was partitioned using an earlier version of NetScaler ADM version. The MBR/GPT based partition can be resized but not beyond 2 terabytes. GPT partition scheme means that the disk was partitioned using NetScaler ADM 12.1 or later.

> **Note**
>
> A GPT partition can be greater than 2 terabytes but when it is created. But you cannot resize the disk to a size greater than 2 terabytes after creating a disk with a smaller size. This is a known limitation of the platform.



Create_swapfile command:

The default swap partition on the primary disk of NetScaler ADM is 4 GB and therefore, the default swap space is 4 GB. For the default memory configuration of NetScaler ADM which is 2 GB, this swap space is sufficient. However, when you run NetScaler ADM with a higher memory configuration, you need to have more swap space allocated on the disk.

> **Note**
>
> Swap partition is usually a dedicated partition that is created on a hard disk drive (HDD) during the installation of the operating system. Such a partition is also referred to as a swap space. Swap partition is used for virtual memory that simulates the additional main memory.

Secondary disks that were added in the earlier versions of NetScaler ADM do not have a swap partition created by default. The "create_swapfile"command is meant for secondary disks created using older NetScaler ADM versions which don't have a swap partition. The command checks for the following:

- Presence of a secondary disk
- Disk being mounted
- Size of the disk (at least 500 GB)
- The existence of the swap file

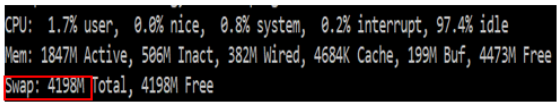
The "create_swapfile"command is useful only when the memory is greater or equal to 16 GB and not when memory is low. Therefore, this command also checks for memory before proceeding with swap file creation.

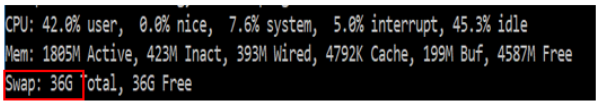

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

If all the conditions are met, and the user consents to proceed, a 32 GB swap file is created on the secondary disk. The swap file creation process takes a few minutes to complete and take care that you do not interrupt the process while in progress. After successful completion, a restart is done for the swap file to take effect.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

After reboot, the increase in swap can be observed using the top command.





Exit command:

To exit from the tool, type exit and press the **Enter** key.

```
(dpt): exit
bash-3.2#
```

Attach additional disks to NetScaler ADM deployed in high availability

Consider that you have configured a pair of NetScaler ADM servers in a high availability set up without any secondary disks. Also, consider that you have added 2 or more NetScaler instances, checked and ensured all processes are running. You might want to add secondary disks to the virtual machines in this setup. In a high availability set up, you must add additional disks to both nodes as detailed in this task:

1. Shut down the secondary node.
2. Add an additional disk through the hypervisor.

> **Note**
>
> Ensure not to extend the secondary node main disk.

3. Start the secondary node.
4. Run the partition tool on the secondary node.
5. After the disk is added, the secondary node restarts.
6. Shut down the secondary node after it restarts.
7. Shut down the primary node.
8. Add an additional disk through the hypervisor.

> **Note**
>
> Ensure not to extend the primary node main disk.

9. Start the primary node.
10. Run the partition tool on the primary node.
11. After the disk is added, the primary node restarts.
12. After the primary node is up and running, start the secondary node.
13. Ensure that the secondary node is up and running and the databases have synchronized.
14. Confirm that all data still exists.

To increase the capacity of RAM on both the nodes:

1. Shutdown ADM_Secondary and increase the RAM size as required. Don't restart the node.
2. Shutdown ADM_Primary and increase the RAM size as required.

   Ensure that you increase the RAM size equally on both nodes. For example, if you increase the RAM size on the primary node to 16 GB, do the same on the secondary node as well.
3. Restart the ADM_Primary.
4. After the ADM_Primary reboots, check that it is the primary node.
5. Now start the ADM_Secondary node. After it restarts, ensure that it has come up as secondary and the DB sync is working.
6. Now confirm that all data still exists.

> **Note**
>
> After you add the secondary disk, the primary node takes some time to come up. Also, the entire process of adding secondary disks to both nodes and increasing RAM capacity

> requires both nodes to be down for some time. Consider this downtime while planning this maintenance activity.

Configure

March 11, 2024

You can access a NetScaler ADM server only by using the GUI. You have to access the GUI to add instances, manage, and monitor your instances and apps, view analytics, and configure the NetScaler ADM server.

Your workstation must have a supported web browser to access the configuration utility and Dashboard.

The following browsers are supported.

Web Browser	Version
Internet Explorer	11.0 and later
Google Chrome	Chrome 19 and later
Safari	Safari 5.1.1 and later
Mozilla Firefox	Firefox 3.6.25 and later

To access the NetScaler ADM GUI:

Log on to NetScaler ADM using the administrator credentials.

After you log on to NetScaler ADM, you have to do the following to get started:

- Add instances to NetScaler ADM. You must add instances to the NetScaler ADM server if you want to manage and monitor these instances.
- Enable analytics on virtual servers. To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.
- Configure NTP server on NetScaler ADM. You have to configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize its clock with the NTP server.
- Configure system settings for optimal NetScaler ADM performance. Before you start using NetScaler ADM to manage and monitor your instances and applications, it is recommended that you configure a few system settings that ensure optimal performance of your NetScaler ADM server.

Add instances to NetScaler ADM

March 11, 2024

Instances are NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler ADM. You must add instances to the NetScaler ADM server if you want to manage and monitor these instances. You can add the following NetScaler ADC appliances and virtual appliances to NetScaler ADM:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

You can add instances either while setting up the NetScaler ADM server for the first time or later. You must then specify an instance profile that NetScaler ADM can use to access the instance.

> **Note**
>
> - NetScaler ADM uses the NetScaler IP (NSIP) address of the NetScaler instances for communication. For information about the ports that must be open between the NetScaler instances and NetScaler ADM, see Ports.
> - To learn how NetScaler ADM discovers instances, see Discover instances.

How to create a NetScaler profile

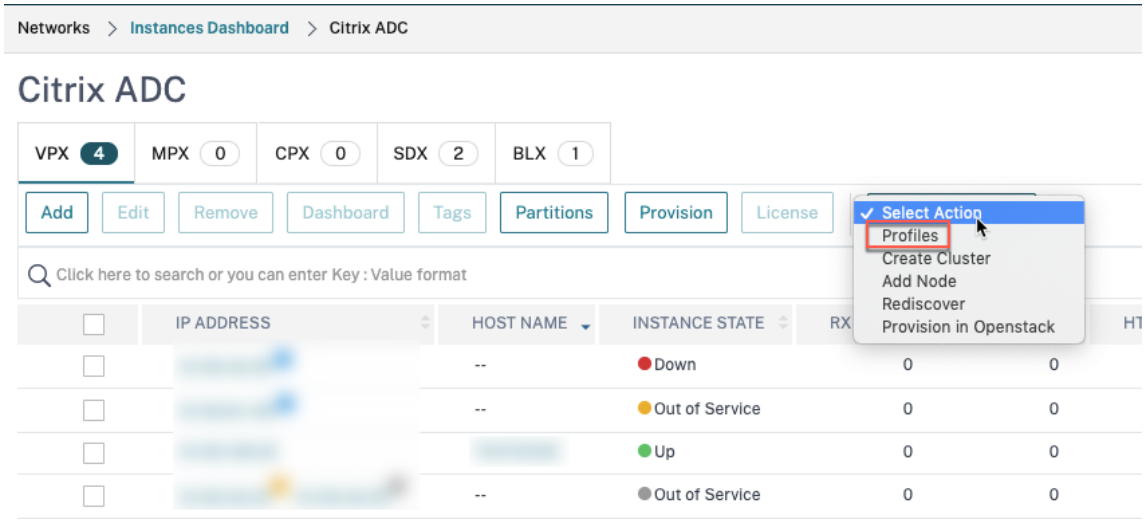
NetScaler profile contains the user name, password, communication ports, and authentication types of the instances that you want to add to NetScaler ADM. For each instance type, a default profile is available. For example, the `nsroot` is the default profile for NetScaler instances. The default profile is defined by using the default NetScaler administrator credentials. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a profile, and then rediscover the instance.

You can create a NetScaler profile from the **Instance** page or while adding or changing an instance.

> **Note**
>
> Ensure to use the super administrator account to create an instance profile.

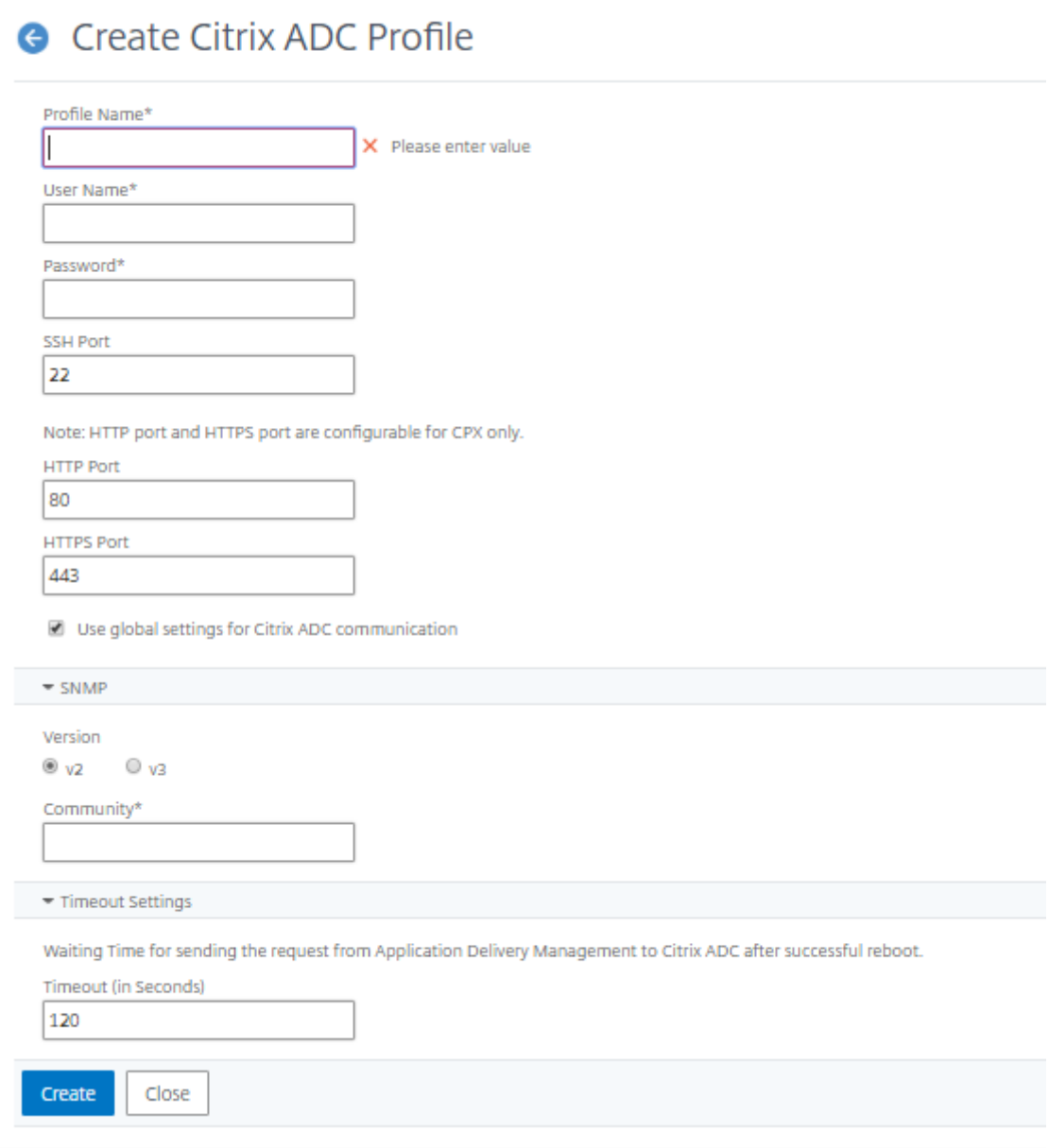
To create a NetScaler profile from the Instance page:

1. Navigate to **Infrastructure > Instances**.
2. Select an Instance. For example, NetScaler.
3. On the NetScaler page, under **Select Action** select **Profiles**.



4. On the **Admin Profiles** page, select **Add**.

5. On the **Create NetScaler Profile** page, do the following:



a) **Profile Name**: Specify a profile name for the NetScaler instance.

b) **User Name**: Specify a user name to log on to the NetScaler instance.

c) **Password**: Specify a password to log on to the NetScaler instance.

d) **SSH Port**: Specify the port for SSH communication between NetScaler ADM and the NetScaler instance.

e) **HTTP Port**: Specify the port for HTTP communication between NetScaler ADM and the NetScaler instance.

> **Note**
>
> The default HTTP port is 80. You can also specify the non-default or customized HTTP port that you might have configured in your NetScaler CPX instance. The customized HTTP port can be used for communication only between NetScaler ADM and NetScaler CPX.

f) **HTTPS Port**: Specify the port for HTTPS communication between NetScaler ADM and the NetScaler instance.

> **Note**
>
> The default HTTPS port is 443. You can also specify the non-default or customized HTTPS port that you might have configured in your NetScaler CPX instance. The customized HTTPS port can be used for communication only between NetScaler ADM and NetScaler CPX.

g) **Use global settings for NetScaler communication**: Select this option if you want to use the system settings for communication between NetScaler ADM and NetScaler instance, otherwise select either HTTP or https.

h) **SNMP Version**: Select either **SNMPv2** or **SNMPv3** and do the following:

   i. If you select SNMPv2, specify the **Community** name for authentication.

   ii. If you select SNMPv3, specify the **Security Name** and **Security Level**. Based on the security level, select the **Authentication Type** and **Privacy Type**.

   > **Note**
   >
   > For NetScaler SDX, only **SNMPv2** is supported.

i) **Timeout Settings**: Specify the time that NetScaler ADM must wait before sending a connection request to the NetScaler instance after a restart.

j) Select **Create**.

Add ADC instances to NetScaler ADM

You can add instances either while setting up the NetScaler ADM server for the first time or later.

To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

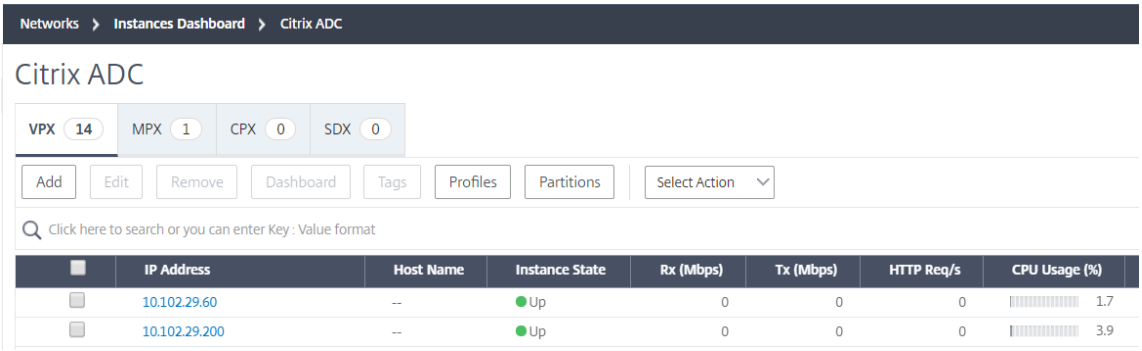
> **Note**
>
> - To add NetScaler instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on NetScaler ADM, the cluster is represented by the cluster IP address only.
> - For NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

If two NetScaler ADM servers are set up in high availability mode, when an instance is added, the traffic source is through the ADM floating IP address.

When you add an instance from a remote data that is configured with an on-prem agent, the traffic source is through the ADM agent.

To add an instance to NetScaler ADM:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Infrastructure > Instances > NetScaler**. Select the type of instance you want to add (for example, NetScaler VPX) and click **Add**.



3. Select one of the following options:

   - **Enter Device IP address** - For NetScaler instances, specify either the host name or IP address of each instance, or a range of IP addresses.

     If you want to discover an ADC HA pair using SNIP, ensure the Independent Network Configuration (INC) mode is enabled. And, specify the SNIP addresses in the following format:

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     For example, `10.10.10.11#10.10.10.12`

   - **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.

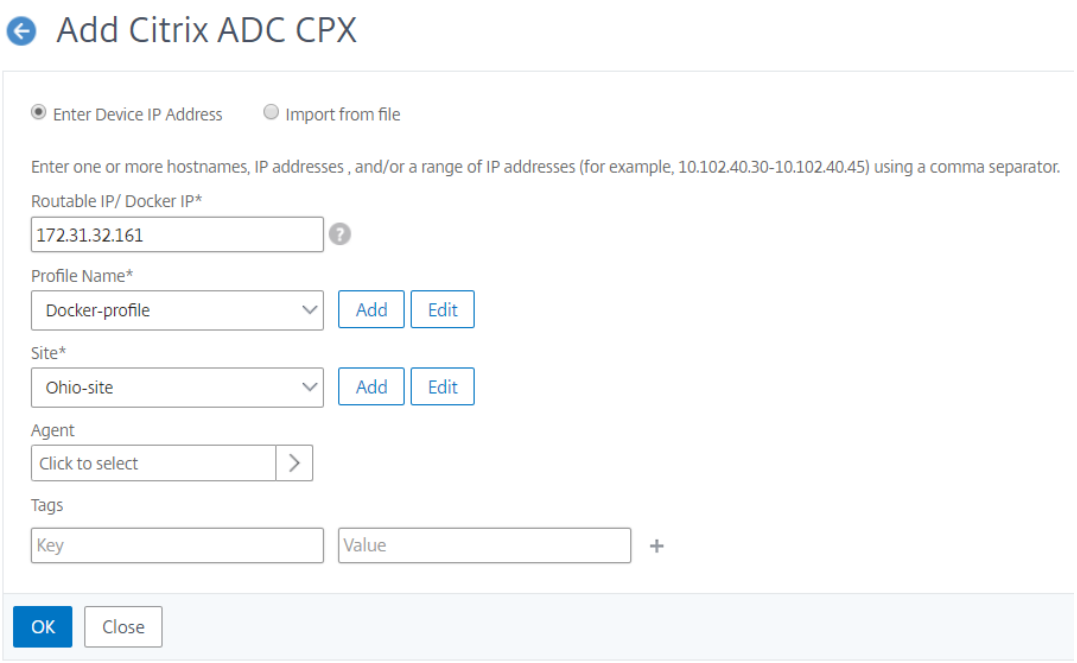
4. From **Profile Name**, select the appropriate instance profile, or create a new profile by clicking the + icon.
5. From **Site**, select the location where you want to add the instance, or create a new location by clicking the **+** icon.
6. Click **OK** to initiate the process of adding instances to NetScaler ADM.

> **Note**
>
> If you want to rediscover an instance, navigate to **Infrastructure > Instances > NetScaler**. Select the instance type (for example, VPX) and select the instance you want to rediscover, and then from the **Select Action** list, click **Rediscover**.

Add NetScaler CPX instances to NetScaler ADM

NetScaler ADM has been enhanced to provide support to the improvements that has been accomplished in CPX functionalities. NetScaler CPX instance is now added in NetScaler ADM by providing an IP address for the CPX along with a device profile. The process of addition of a CPX instance is now similar to how other ADC types such as VPX or MPX is added in ADM. Also, the registration of CPX in ADM has been enhanced. When a CPX starts, NetScaler ADM automatically discovers and registers the CPX instance. A CPX instance is no longer discovered through Docker host.

1. Navigate to **Infrastructure > Instances > NetScaler** and click **CPX** tab.
2. Click **Add** to add new CPX instances in NetScaler ADM.
3. The **Add NetScaler CPX** page opens. Enter the values for the following parameters:
    a) You can add CPX instances by providing either the reachable IP address of the CPX instance or the IP address of the Docker container where the CPX instance is hosted.
    b) Select the profile of the CPX instance.
    c) Select the site where the instances are to be deployed.
    d) Select the agent.
    e) As an option, you can enter the key-value pair to the instance. Adding key-value pair makes it easy for you to search for the instance later.



> **Note**
>
> For NetScaler CPX instances, you must specify the **HTTP, HTTPS, SSH**, and **SNMP** port details of the host while creating the CPX instance profile. You can also specify the range of ports that were published by the host in the **Start Port** and **Number of ports** field.

4. Click **OK**.

Add a standalone NetScaler BLX instance in NetScaler ADM

A standalone NetScaler BLX instance is a single instance that is running on the dedicated host Linux server.

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **BLX** tab, click **Add**.
3. Select the **Standalone** option from the **Instance Type** list.
4. In the **IP address** field, specify the IP address of the BLX instance.
5. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
6. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

> **Important**
>
> Ensure you have specified the correct host user name and password of the Linux server in the profile.

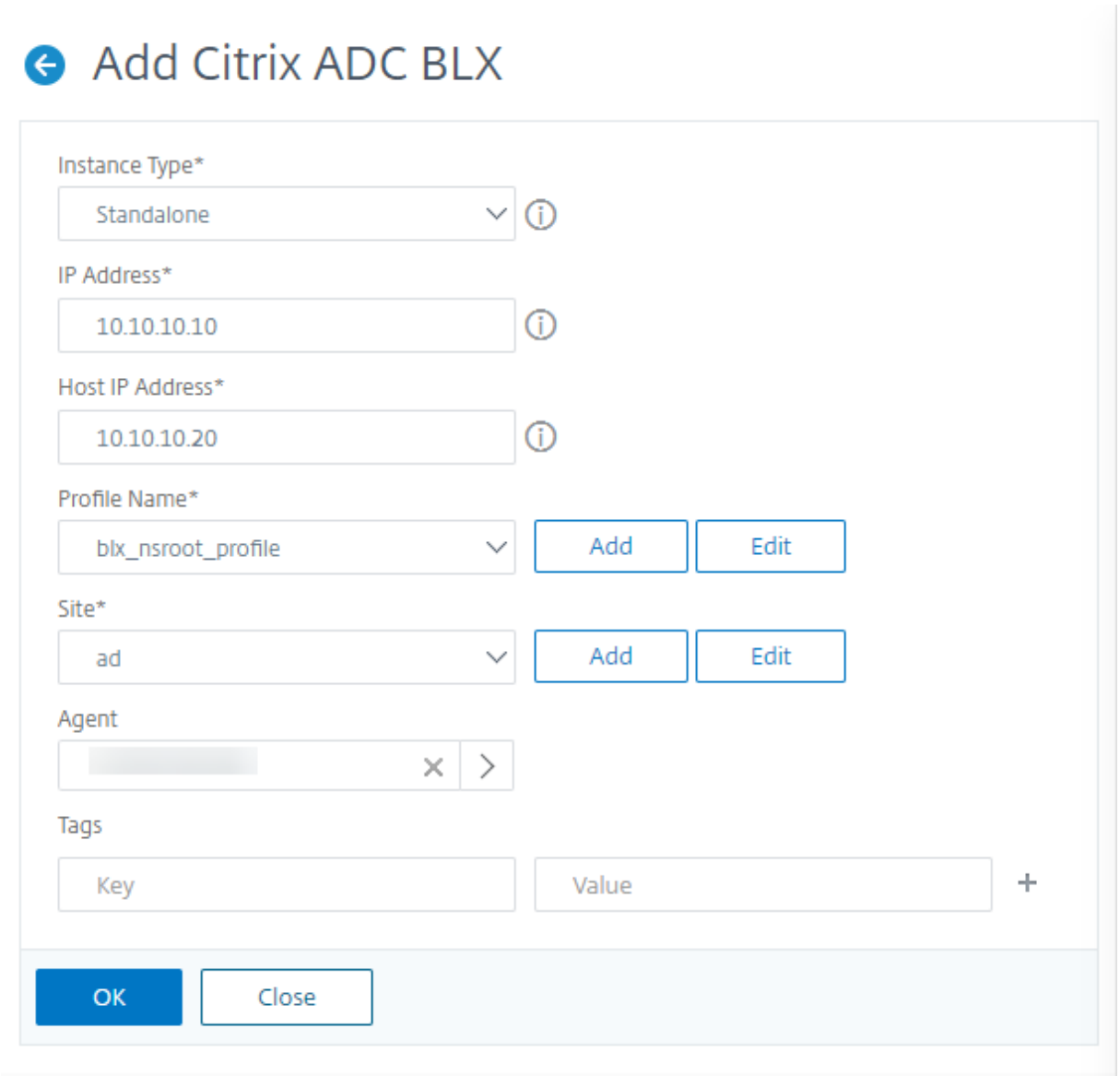
7. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.

8. In the **Agent** list, select the NetScaler agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler ADM, that agent is selected by default.

9. Click **OK**.



Add high-availability NetScaler BLX instances in NetScaler ADM

The high-availability NetScaler BLX instances that run on different host Linux servers. A Linux server cannot host more than one BLX instances.

1. In the **BLX** tab, click **Add**.
2. Select the **High Availability** option from the **Instance Type** list.
3. In the **IP address** field, specify the IP address of the BLX instance.
4. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
5. In the **Peer IP address** field, specify the IP address of the peer BLX instance.
6. In the **Peer Host IP address** field, specify the IP address of the Linux server where the peer BLX instance is hosted.
7. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

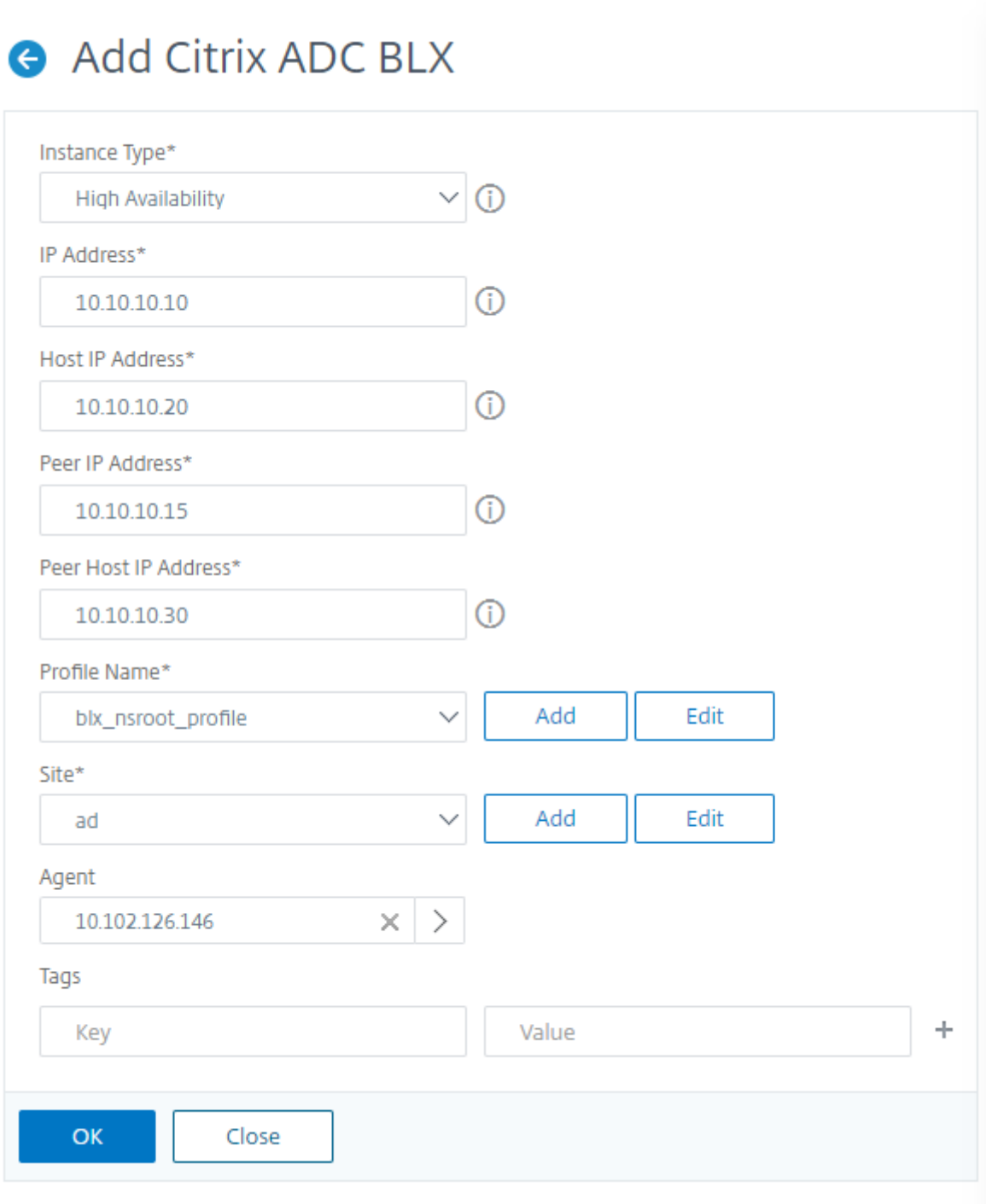
   To create a profile, click **Add**.

   > **Important**
   >
   > Ensure you have specified the correct host user name and password of the Linux server in the profile.

8. In the **Site** list, select the site where you want to add an instance.

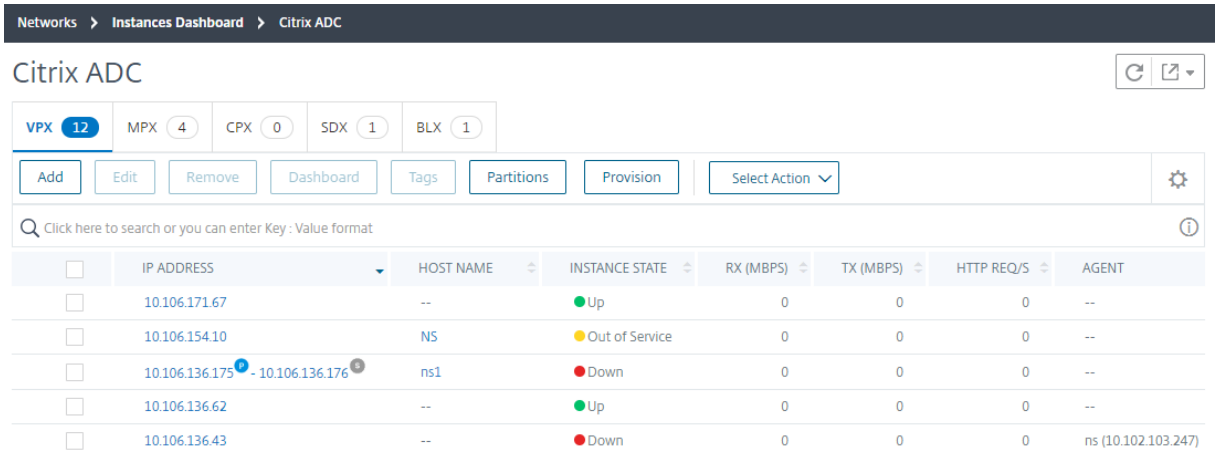
   If you want to add a site, click **Add**.
9. In the **Agent** list, select the NetScaler agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler ADM, that agent is selected by default.
10. Click **OK**.



Access an instance GUI from the NetScaler ADM

1. Navigate to **Infrastructure > Instances** > **NetScaler**.
2. Select the type of instance you want to access (for example, VPX, MPX, CPX, SDX, or BLX).
3. Click the required NetScaler IP address or host name.



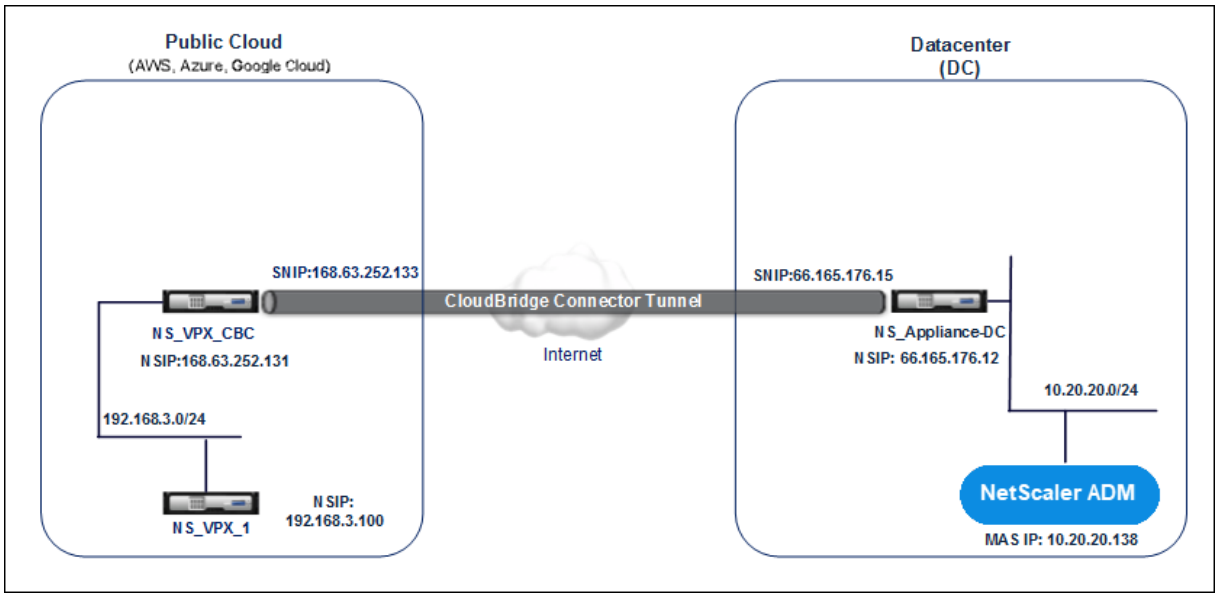
The GUI of the selected instance appears in a pop-up window.

Add NetScaler VPX instances deployed in cloud to NetScaler ADM

March 11, 2024

You can use NetScaler ADM to manage and monitor the NetScaler VPX instances deployed on a public cloud such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. You need to establish Layer 3 connectivity between NetScaler ADM and the NetScaler VPX instances deployed on the public cloud. To establish the Layer 3 connectivity, you can use solutions such as Direct Connect to AWS, VPN in Azure, or third-party connectors such as Equinix and so on.

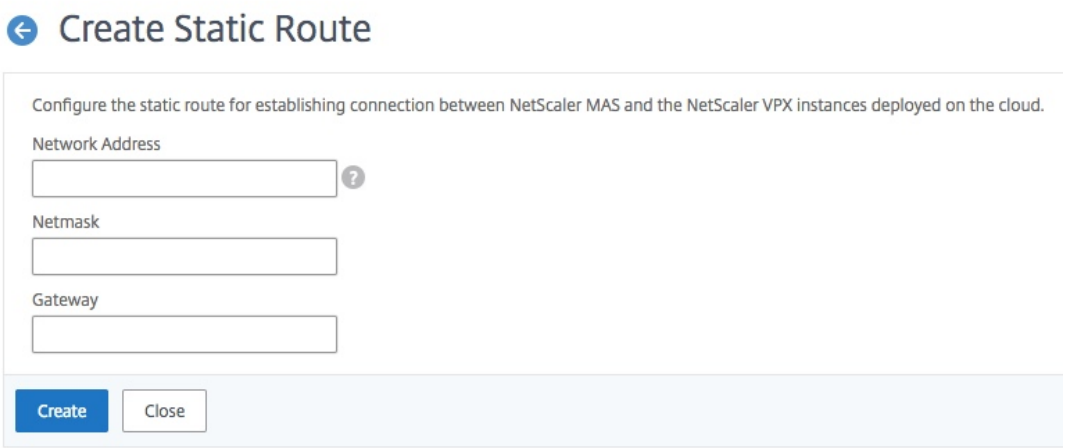
The following sample topology uses Citrix CloudBridge Connector for Layer 3 connectivity between NetScaler ADM and the NetScaler VPX instances deployed in the cloud.



A Citrix CloudBridge Connector tunnel is set up between NetScaler appliance NS_Appliance-DC, in a data center DC, and NetScaler virtual appliance (VPX) NS_VPX_CBC in the public cloud. NS_Appliance-DC and NS_VPX_CBC enable the communication between NetScaler ADM and the NetScaler VPX instance, NS_VPX_1, deployed in the public cloud. After the communication is established, you can discover NS_VPX_1 in NetScaler ADM.

To configure this topology:

1. Install, configure, and start a NetScaler VPX instance in the public cloud.
    - For instructions, see Install NetScaler VPX on AWS.
    - For instructions, see Install NetScaler VPX on Microsoft Azure.
    - For instructions, see Install NetScaler VPX on Google Cloud.
2. Deploy and configure a NetScaler physical appliance, or provision and configure a NetScaler virtual appliance (VPX) on a virtualization platform in the data center.
    - For instructions, see Install a NetScaler VPX instance on Citrix Hypervisor.
    - For instructions, see Install Citrix virtual appliances on VMware ESXi.
    - For instructions, see Install NetScaler virtual appliances on Microsoft Hyper-V.
3. Configure the Citrix CloudBridge Connector between the data center and the public cloud. For instructions, see Configuring Citrix CloudBridge Connector.
4. Configure the static route for establishing connection between NetScaler ADM and the NetScaler VPX instances deployed on the cloud, as follows:
    a) Log on to NetScaler ADM.
    b) Navigate to **System > Static Routes** and click **Add**.



c) In the **Network Address** field, enter the address of the network that you want to establish a static route from NetScaler ADM through the connector.

d) In the **Netmask** field, enter the netmask for the network.

e) In the **Gateway** field, enter the address of the gateway.

5. Add the NetScaler VPX cloud instances to the NetScaler ADM by specifying the range of IP addresses of NetScaler VPX instances in the public cloud. For detailed instructions, Add Instances to NetScaler ADM.

Provision NetScaler VPX instances on VMware ESX

March 18, 2024

You can use ADM to automate an NetScaler VPX instance deployment and management in VMware ESX. When you use NetScaler ADM to provision an NetScaler VPX instance on VMware ESX, the instance is readily available to manage in the ADM GUI.

The NetScaler ADM uses ADC templates of the already deployed instances to provision a new instance in VMware ESX. It stores the required VMware ESX server details in a site. Also, it uses Cloud Access Profile to access the server.

Prerequisites

Before you provision an NetScaler VPX instance in VMware ESX, ensure to complete the following:

1. Install a supported VMware ESXi version (6.0, 6.5, and 6.7).
2. Install VMware Client on a management workstation that meets the minimum system requirements.
3. Downloading the NetScaler VPX setup files.
4. Convert NetScaler VPX files into templates in ESX.
5. Create a site in ADM.

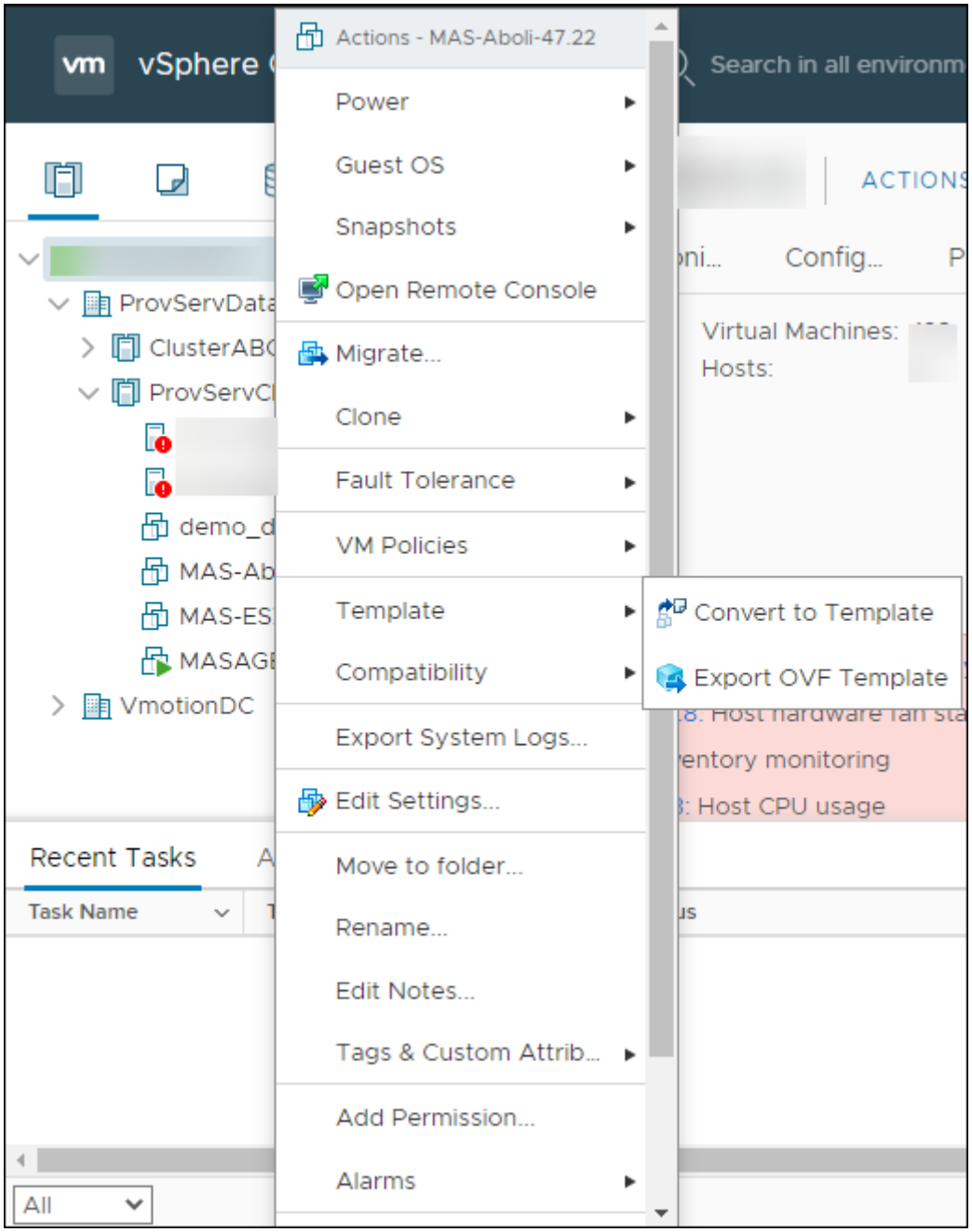
Convert NetScaler VPX files into templates

The NetScaler ADM uses the ADC template in ESX converted by an NetScaler VPX file. Perform the following steps to convert VPX files into templates.

1. Deploy a NetScaler VPX instance on VMware using the ADC setup files.

   For the first time, use ADC setup files to deploy the VPX instance. For more information, see Install NetScaler VPX instance on VMware.

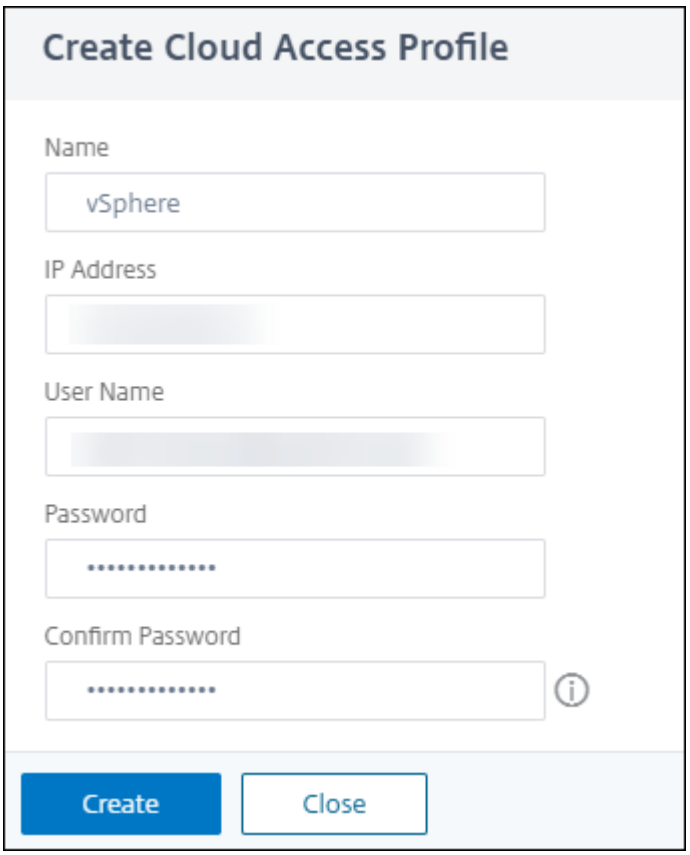
2. Right-click the deployed VM and select **Template**.
3. Click **Convert to Template**.



Create a site in ADM

Create a site in NetScaler ADM and add the VMware ESX details.

1. In NetScaler ADM, navigate to **Infrastructure > Instances > Sites**.
2. Click **Add**.
3. In the **Select Cloud** pane,
    a) Select **Data Center** as a **Site** type.
    b) Choose **VMware vCenter** from the **Type** list.
    c) Click **Next**.
4. In the **Choose Region** pane,
    a) In the **Cloud Access Profile** pane, select the profile created for your VMware ESX. If there are no profiles, create a profile.
    b) To create a cloud access profile, click **Add** and specify the following:
        - **Name** –Specify a name to identify your cloud access profile in NetScaler ADM.
        - **IP address** –Specify the IP address of the VMware vCenter server where you want to provision VPX instances.
        - **Username** –Specify the user name to access the VMware vCenter server.
        - **Password** –Specify the password to access the VMware vCenter server and confirm the password.

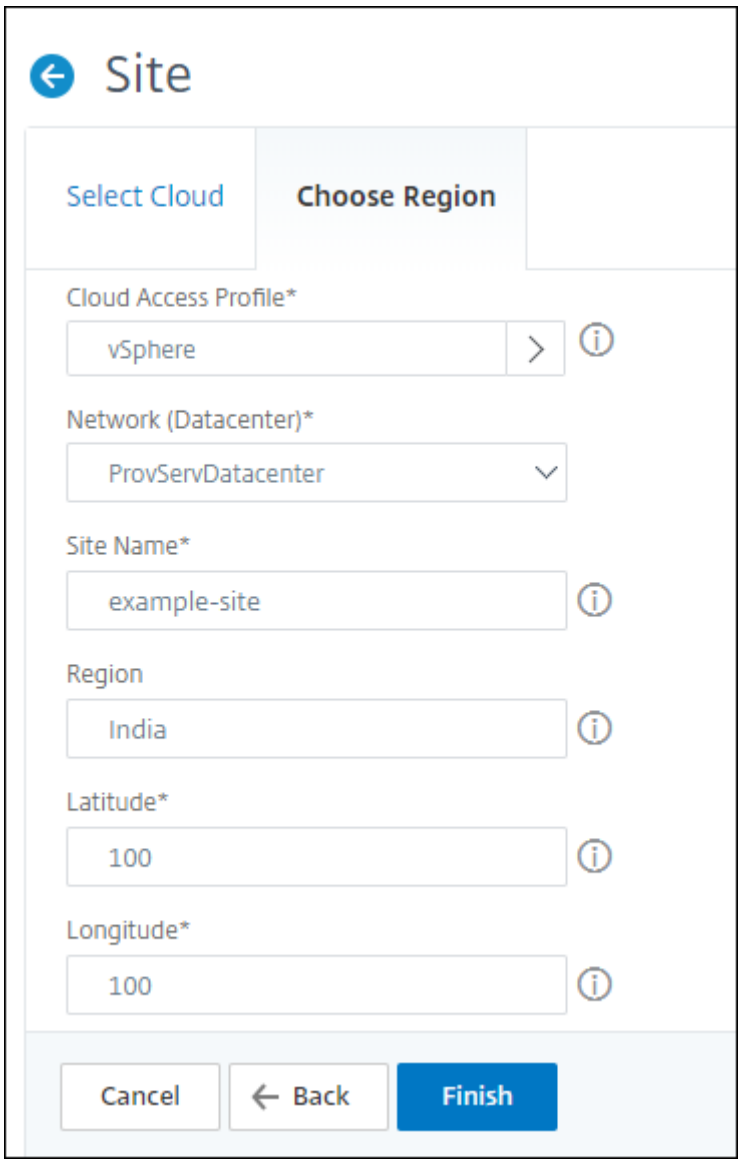


c) In **Network (Datacenter)**, select the data center where you have the ADC templates.

d) Specify the **Site Name**.

e) Specify the **Region**, **Latitude**, and **Longitude** to identify the geo-location of your data center.

f) Click **Finish**.



Provision an instance on VMware ESX

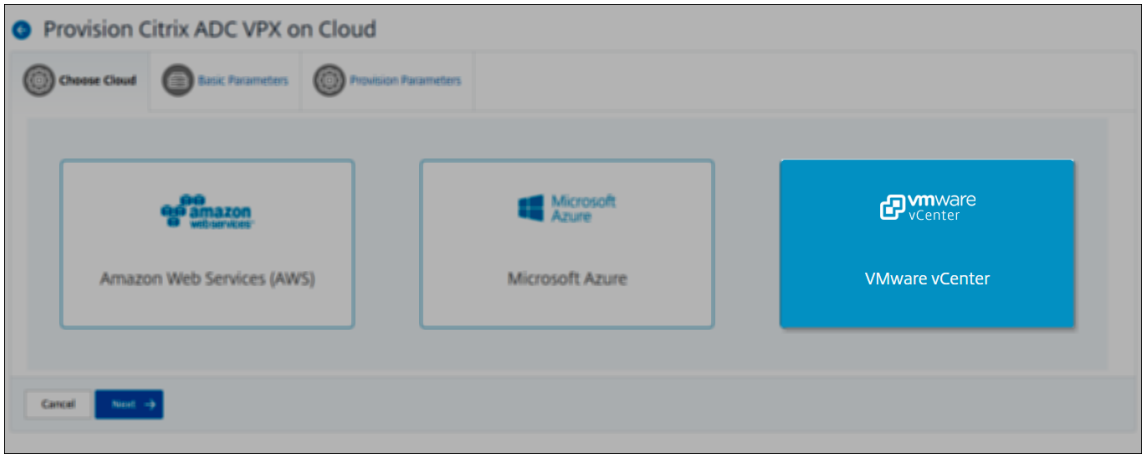
Use the site that you have associated with your VMware ESX to provision the NetScaler VPX instances.

> **Note:**
>
> Currently, the NetScaler ADM supports only to provision standalone ADC instances.

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

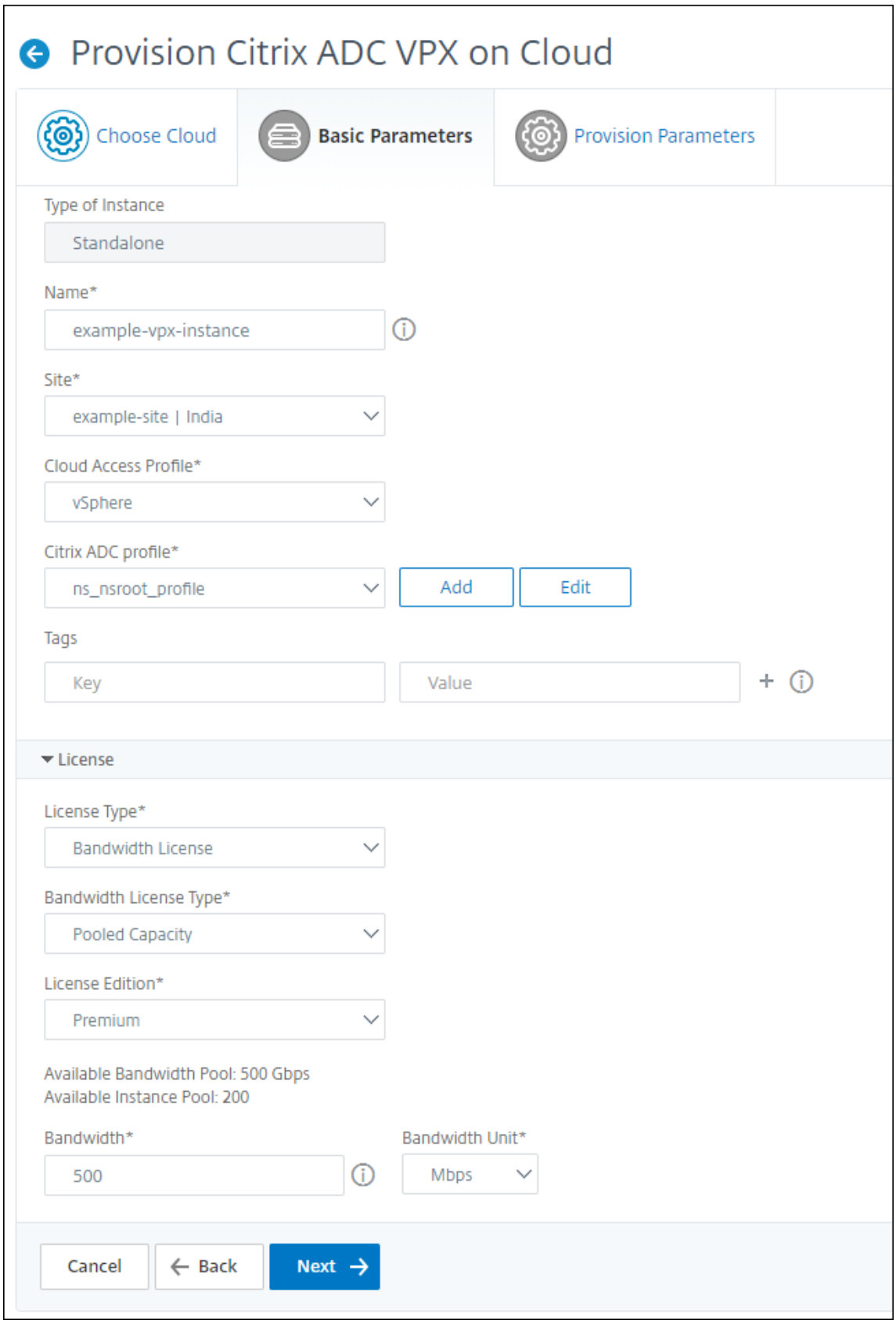
   This option displays the **Provision NetScaler VPX on Cloud** page.

3. Select **VMware vCenter** and click **Next**.

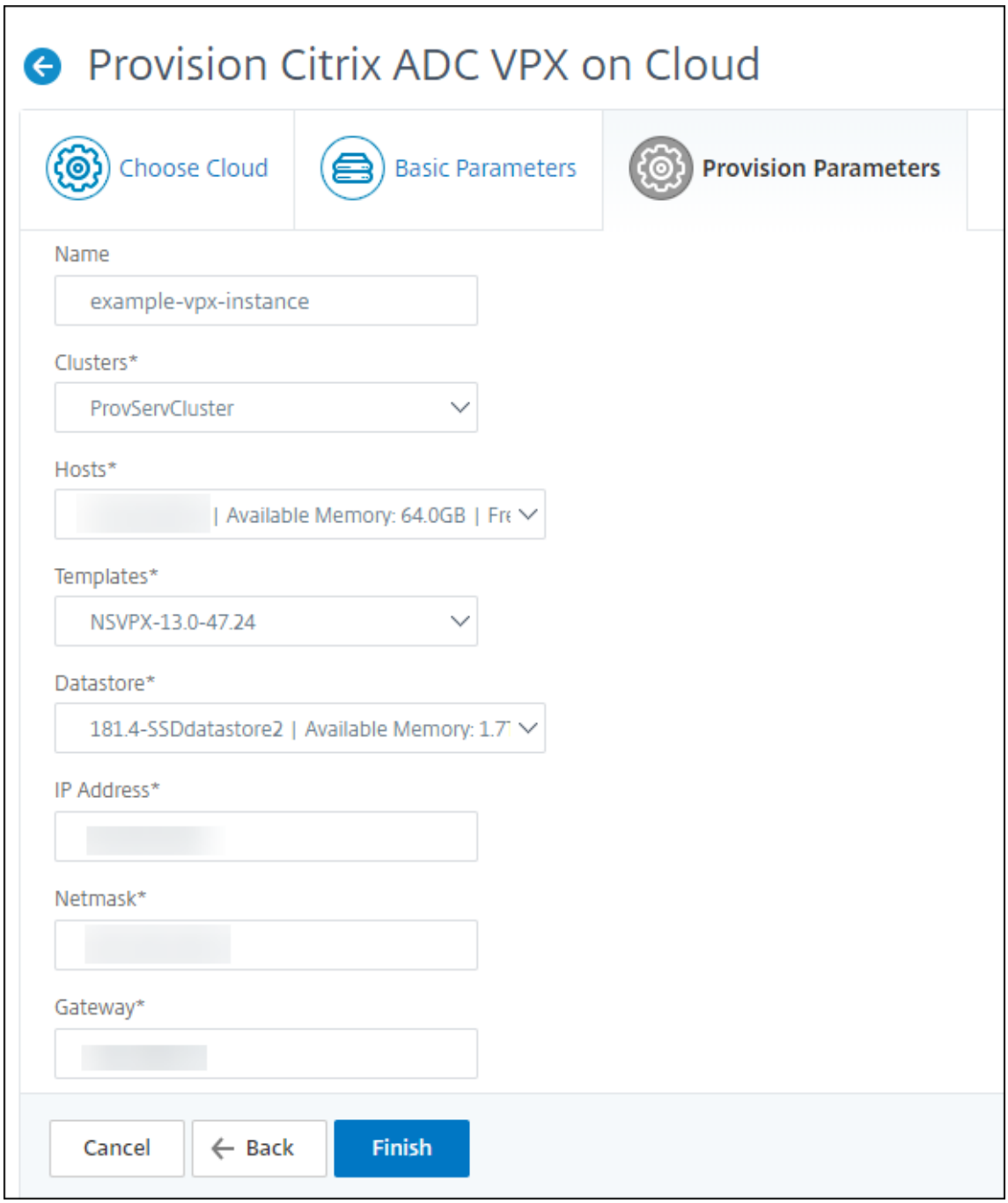


4. In **Basic Parameters**, specify the following:

   - **Name** –Specify the name of an instance.
   - **Site** –Select the site that you have created earlier.
   - **Cloud Access Profile** –Select the cloud access profile created during site creation.
   - **NetScaler profile** –Select the ADC profile to provide authentication.
   - **License** –Use pooled capacity licensing to apply licenses to an instance.



5. Click **Next**.
6. In **Provision Parameters**, specify the following details:
    - **Clusters** –Select the cluster where you want to provision an instance.
    - **Hosts** –Select the required host from the list.
    - **Templates** –Select the template from the list that you want to apply to an instance.
    - **Datastore** –Select the datastore from the list.
    - **IP address** –Specify an IP address to an instance.
    - **Net mask** –Specify a net mask to an instance.
    - **Gateway** –Specify a gateway to an instance.



7. Click **Finish**.

Manage licensing and enable analytics on virtual servers

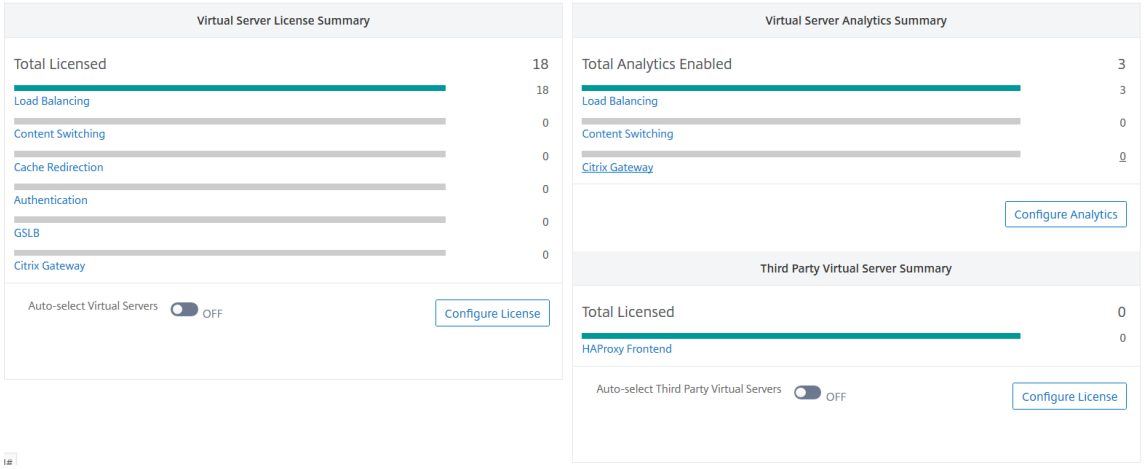
March 11, 2024

> **Note**
>
> - By default, the **Auto Licensed Virtual Servers** option is enabled. You must ensure to have sufficient licenses to license the virtual servers. If you have limited licenses and want to license only the selective virtual servers based on your requirement, disable the **Auto Licensed Virtual Servers** option. Navigate to **Settings > Licensing & Analytics Configuration** and disable the **Auto Licensed Virtual Servers** option under **Virtual Server License Allocation**.

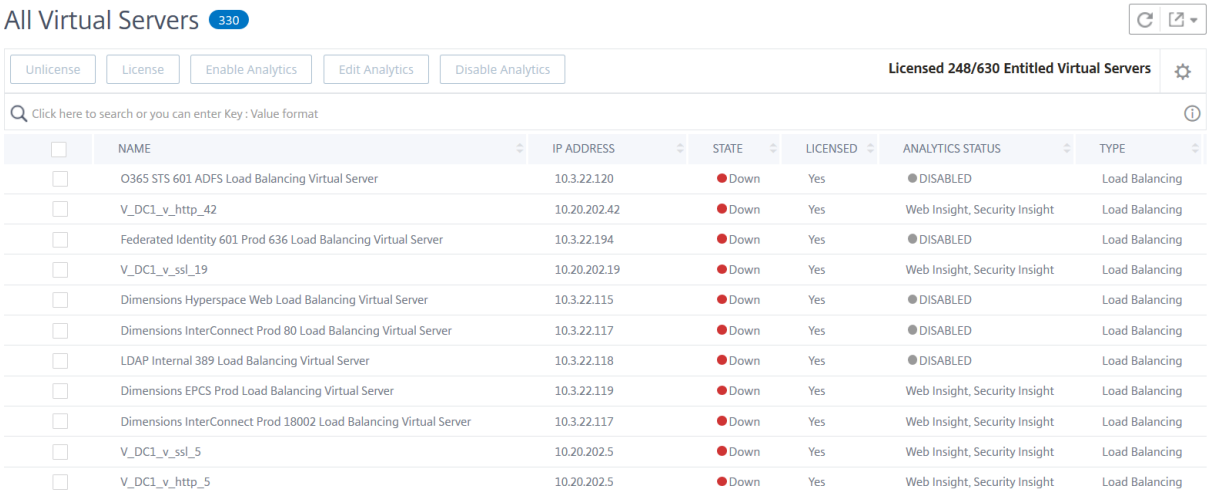
The process of enabling analytics is simplified. You can license the virtual server and enable analytics in a single workflow.

Navigate to **Settings > Licensing & Analytics Configuration** to:

- View the **Virtual Server Licence Summary**
- View the **Virtual Server Analytics Summary**



When you click **Configure License** or **Configure Analytics**, the **All Virtual Servers** page is displayed.



On the **All Virtual Servers** page, you can:

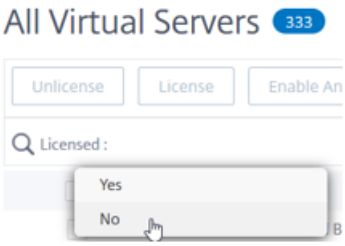
- Apply license for unlicensed virtual servers
- Remove license for licensed virtual servers
- Enable analytics on licensed virtual servers
- Edit analytics
- Disable analytics

> **Note**
>
> The supported virtual servers to enable analytics are Load Balancing, Content Switching, and NetScaler Gateway.

Manage licensing on virtual servers

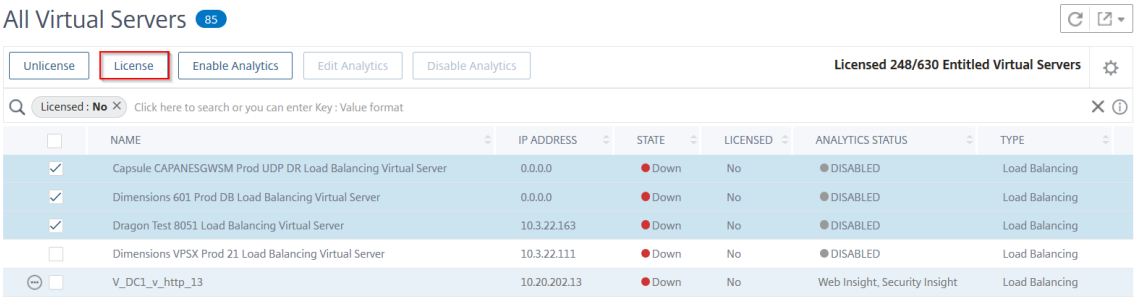
To license the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **No**.



   The filter is now applied and only the unlicensed virtual servers are displayed.

2. Select the virtual servers and then click **License**.



To unlicense the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **Yes**.
2. Select the virtual servers and click **Unlicense**.

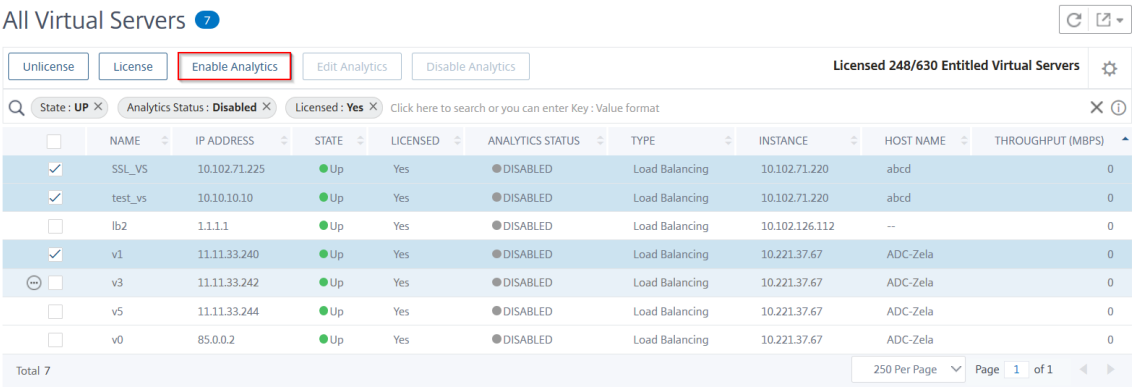
Enable analytics

The following are the prerequisites to enable analytics for virtual servers:

- Ensure that virtual servers are **licensed**
- Ensure that analytics status is **Disabled**
- Ensure that virtual servers are in **UP** status

You can filter the results to identify the virtual servers that are mentioned in the prerequisites.

1. Click the search bar and select **State** and then select **UP**.
2. Click the search bar and select **Licensed**, and then select **Yes**.
3. Click the search bar and select **Analytics Status**, and then select **Disabled**.
4. After applying the filters, select the virtual servers, and then click **Enable Analytics**.



> **Note**
>
> Alternatively, you can enable analytics for a particular instance:
>
> a) Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.
>
> b) Select the instance and from **Select Action** list, select **Configure Analytics**
>
> c) On the Configure Analytics on Virtual Servers page, select the Virtual Server and click **Enable Analytics**.

5. On the **Enable Analytics** window:
   a) Select the insight types (Web Insight or WAF Security Violations)
   b) Select **Logstream** as Transport Mode

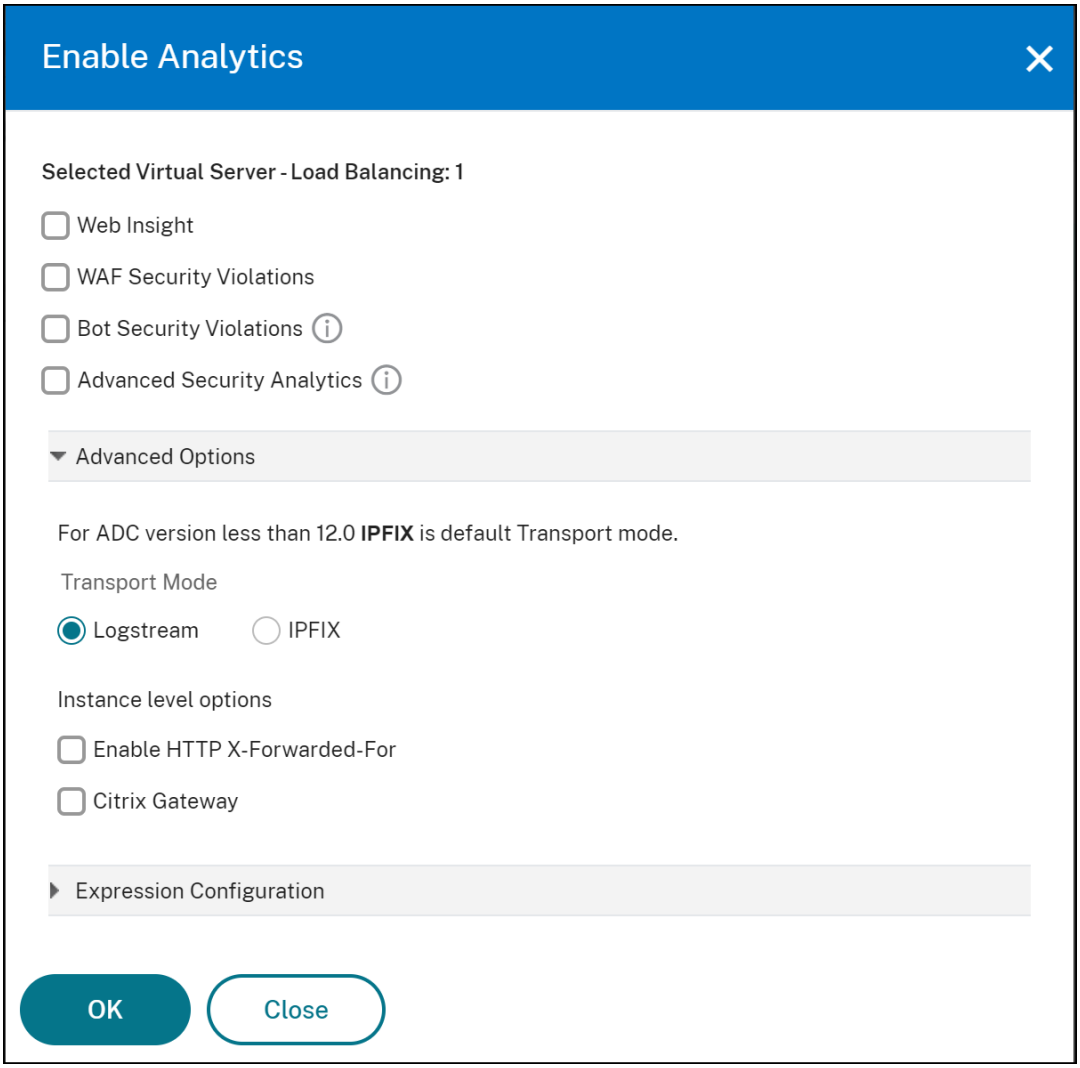
> **Note**
>
> For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.
>
> For more information about IPFIX and Logstream, see Logstream overview.

c) Under **Instance level options**:

- **Enable HTTP X-Forwarded-For** - Select this option to identify the IP address for the connection between client and application, through HTTP proxy or load balancer.
- **NetScaler Gateway** - Select this option to view analytics for NetScaler Gateway.

d) The Expression is true by default

e) Click **OK**



> **Note**
>
> - If you select virtual servers that are not licensed, then NetScaler ADM first licenses those virtual servers and then enables analytics
> - For admin partitions, only **Web Insight** is supported
> - For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

After you click **OK**, NetScaler ADM processes to enable analytics on the selected virtual servers.

> **Note**
>
> NetScaler ADM uses NetScaler SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between NetScaler agent and NetScaler instance, ensure you open the following port to enable NetScaler ADM to collect AppFlow traffic:

Transport Mode	Source IP	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

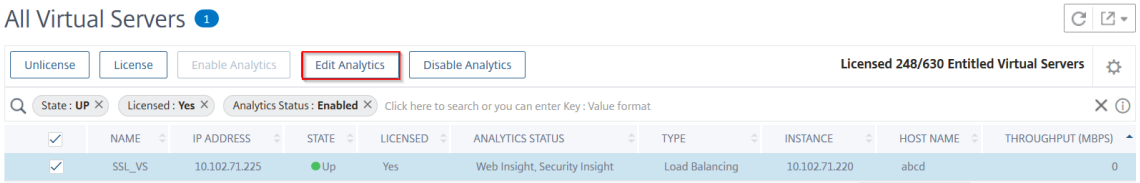
Edit analytics

To edit analytics on the virtual servers:

1. Select the virtual servers

   > Note
   >
   > Alternatively, you can also edit analytics for a particular instance:
   >
   > a) Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.
   >
   > b) Select the instance and click **Edit Analytics**.

2. Click **Edit Analytics**



3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window

4. Click **OK**.

Disable analytics

To disable analytics on the selected virtual servers:

1. Select the virtual servers
2. Click **Disable Analytics**

NetScaler ADM disables the analytics on the selected virtual servers

The following table describes the features of NetScaler ADM that supports IPFIX and Logstream as the transport mode:

Feature	IPFIX	Logstream
Web Insight	•	•
WAF Security Violations	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

A unified process to enable analytics on virtual servers

March 11, 2024

Apart from the existing process to enable analytics, you can also use a single-pane workflow to configure analytics on:

- All the existing licensed virtual servers
- The subsequent licensed virtual servers

After configuration, this feature eliminates the necessity to manually enable analytics on the existing and subsequent virtual servers.

Points to note:

Before you configure analytics, you must understand the following behaviors of NetScaler ADM:

- When you configure this feature for the first time, you must ensure that the prerequisites mentioned in this document are met.
- Modify the analytics settings later.

  Consider that you have configured the analytics settings for the first time by selecting Web Insight, HDX Insight, and Gateway Insight. If you want to modify the analytics settings later and deselect Gateway Insight, the changes do not impact the virtual servers that are already enabled with analytics.
- The virtual servers that are already enabled with analytics.

  Consider that you have 10 licensed virtual servers and two of them are already enabled with analytics. In this scenario, this feature enables analytics only for the remaining eight virtual servers.
- The virtual servers that are manually disabled with analytics.

  Consider that you have 10 licensed virtual servers and you have manually disabled analytics for two virtual servers. In this scenario, this feature enables analytics only for the remaining eight virtual servers and skips the virtual servers that are manually disabled with analytics.
- **Bot Security Violations** and **WAF Security Violations** options are supported only in premium licensed virtual servers. If the virtual servers are not premium licensed, then **Bot Security Violations** and **WAF Security Violations** are not enabled.

Prerequisites

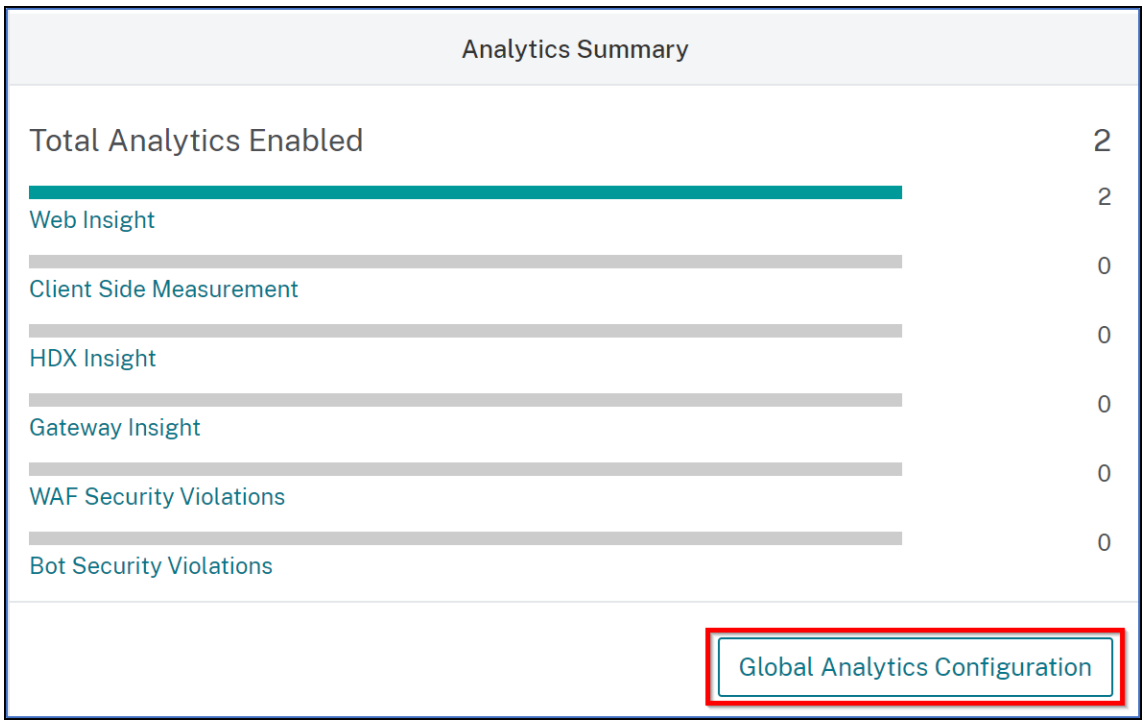
Ensure that:

- All existing virtual servers are licensed.
- Auto-licensed option is enabled to license all the subsequent virtual servers. Navigate to **Settings > Licensing & Analytics Config** and under **Virtual Server License Allocation**, turn on the **Auto Licensed Virtual Servers** option.

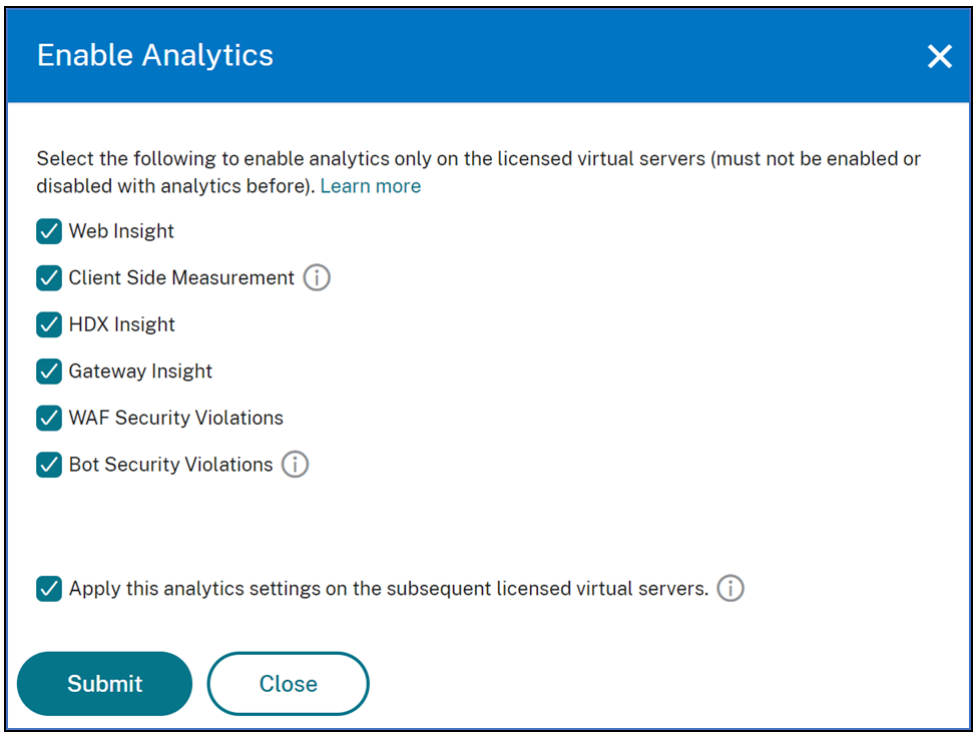
Enable analytics

1. Navigate to **Settings > Licensing & Analytics Config**.

2. Under **Analytics Summary**, click **Global Analytics Configuration**.



3. Select the analytics features that you want to enable analytics on the virtual servers.
4. To enable analytics on the subsequent virtual servers, select the **Apply this analytics settings on the subsequent licensed virtual servers** check box.
5. Click **Submit**.



Configure NTP server

March 11, 2024

You can configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server on NetScaler ADM:

1. From the ADM GUI, navigate to **Settings > Administration**. In the **System Administration** page, under **Network Configurations**, click **NTP Servers**. Then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
    - **Server Name/IP Address** –Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
    - **Minimum Poll Interval** –Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2^6, enter 6
    - **Maximum Poll Interval** –Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll

interval to be 256 seconds, which can be expressed as 2^8, enter 8.

- **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.
- **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
- **Preferred** –Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

To enable NTP synchronization on NetScaler ADM:

1. Navigate to **System** > **NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** check box.
3. Click **OK**.

Configure system settings

March 11, 2024

Before you start using NetScaler ADM to manage and monitor your instances and applications, it is recommended that you configure a few system settings ensure optimal performance of your NetScaler ADM server.

Configure system alarms

Configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, loginFailure), a message is recorded in the system and you can view the message as a syslog message.

To configure system alarms:

1. Navigate to **Settings > SNMP**, and then click the **Alarms** tab on the upper-right corner.

2. Select the alarm you want to configure, and click **Edit**.
3. On the **Configure Alarm** page, select the alarm severity, and set the Threshold.
4. To view the alarms that have breached the threshold or for which an event has occurred, navigate to **Settings > Auditing** and click **Syslog Messages**.

Configure system notifications

You can send notifications to select groups of users for various system-related functions. You can set up a notification server in NetScaler ADM, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. Setting notification ensures that you are notified of any system-level activities such as user login or system restart.

To configure system notifications:

1. Navigate to **Settings > Administration**. In the **System Administration** page, under **Event Notifications**, click **Configure Event Notification and Digest > Event Notification**.
2. On the **Configure System Notification Settings** page, select the category or category of events generated by NetScaler ADM.
3. Then, configure either the email server or the SMS server to receive notification through email or SMS or both.

Configure system prune settings

To limit the amount of reporting data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

To configure system prune setting:

1. Navigate to **Settings > System Administration**. Under **Data Pruning**, click **System and Instance Data Pruning**.
2. In the **System** page, specify the number of days for which to retain data, and click **Save**.

Configure instance syslog prune settings

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the generic syslog data is deleted from NetScaler ADM.

To configure instance syslog purge settings:

1. Navigate to **Settings > Administration > Data Pruning**.
2. Click **System and Instance Data Pruning > Instance Syslog**.
3. In **Configure Instance Syslog Prune Settings page**, specify the number of days between 1 and 180 in **Retain Syslog Generic Data** field.
4. Click **Save**.

Configure instance event prune settings

To limit the amount of event messages data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).

To configure instance event prune settings:

1. Navigate to **Settings > Administration**.
2. From the **System Administration** page, under **Data Pruning**, click **System and Instance Data Pruning**.
3. In the **Data Pruning** page, click **Instance Events**.
4. In the **Data to keep (days)** field, enter the time interval, in days, for which you want to retain data on the NetScaler ADM server and click **Save**.

Configure system backup settings

NetScaler ADM automatically backs up the system every day at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system. You can also encrypt the backup file. You can also choose to save the backup on an external server.

To configure system backup settings:

1. Navigate to **Settings > Administration**.
2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **System** and on the **Configure System Backup Settings** page, specify the required values.

Configure instance backup settings

If you back up the current state of a NetScaler instance, you can use the backup files to restore stability if the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.

To configure instance backup settings:

1. Navigate to **Settings > Administration**.
2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **Instance**, under **Configure Instance Backup Settings**, and specify the required values.

Enable or disable ADM features

As an administrator, you can enable or disable the following features in the **Settings > Administration > Configurable Features** page:

- **Agent failover** - The agent failover can occur on a site that has two or more active agents. When an agent becomes inactive (DOWN state) in the site, the NetScaler ADM service redistributes the ADC instances of the inactive agent with other active agents. For more information, see Configure on-prem agents for multisite deployment.
- **Entity polling network function** - An entity is either a policy, virtual server, service, or action attached to an ADC instance. By default, NetScaler ADM automatically polls configured network function entities every 60 minutes. For more information, see Polling overview.
- **Instance backup** - Back up the current state of a NetScaler instance and later use the backed-up files to restore the ADC instance to the same state. For more information, see Back up and restore NetScaler instances.
- **Instance configuration audit** - Monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations. For more information, see Create audit templates.
- **Instance events** - Events represent occurrences of events or errors on a managed NetScaler instance. Events received in NetScaler ADM are displayed on the **Events Summary** page (**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**). For more information, see Events.
- **Instance network reporting** - You can generate reports for instances at a global level. Also, for entities such as the virtual servers and network interfaces. For more information, see Network Reporting.
- **Instance SSL certificates** - NetScaler ADM provides a centralized view of SSL certificates installed across all managed NetScaler instances. For more information, see SSL Dashboard.
- **Instance Syslog** - You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler ADM.

To enable a feature, perform the following steps:

1. Select the feature from the list that you want to enable.
2. Click **Enable**.

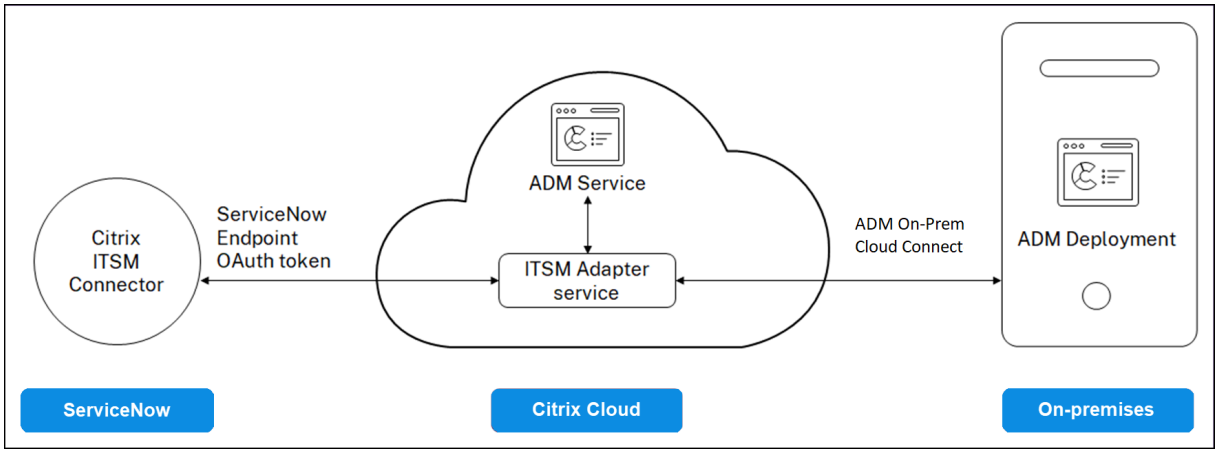
> **Important**
>
> If a feature is disabled, the user cannot perform the operations associated with that feature.

Integrate NetScaler ADM with the ServiceNow instance

March 11, 2024

When you want to enable ServiceNow notifications for NetScaler and ADM events, integrate NetScaler ADM with the ServiceNow instance. This integration uses Citrix ITSM connector to communicate between NetScaler ADM and the ServiceNow instance.

The ServiceNow integration with ADM uses the ITSM Adapter service for token based authentication. To do so, it creates an endpoint instance in ServiceNow. For more information, see How ITSM Adapter works.



To connect your ADM on-premises deployment with an ITSM adapter, ensure to configure customer identity. For more information, see, Configure customer identity.

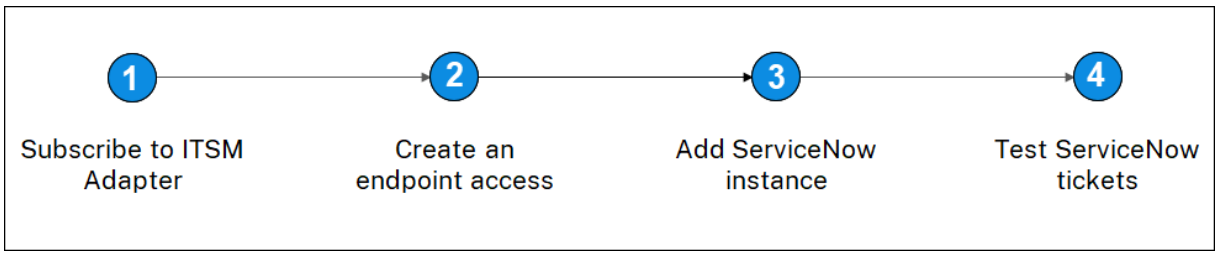
Prerequisites

Before you integrate ADM with ServiceNow, ensure the following:

1. Sign Up for Citrix Cloud. Make sure you have access to manage Citrix Cloud administrators. For more information, see Manage Citrix Cloud administrators.

How to integrate ADM with ServiceNow?

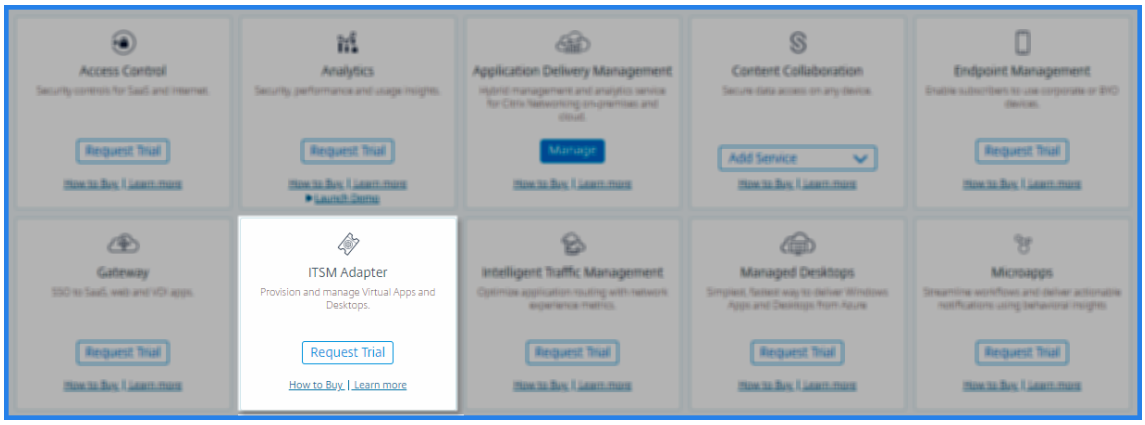
Perform the following steps to integrate NetScaler ADM with ServiceNow using the ITSM connector:



1. Subscribe to ITSM Adapter service in Citrix Cloud.
2. Create an endpoint access in the ServiceNow instance.
3. Add a ServiceNow instance.
4. Test auto-generation of ServiceNow tickets in ADM.

Step 1 - Subscribe to ITSM Adapter service in Citrix Cloud

1. On the **ITSM Adapter** tile, click **Request Trial**.

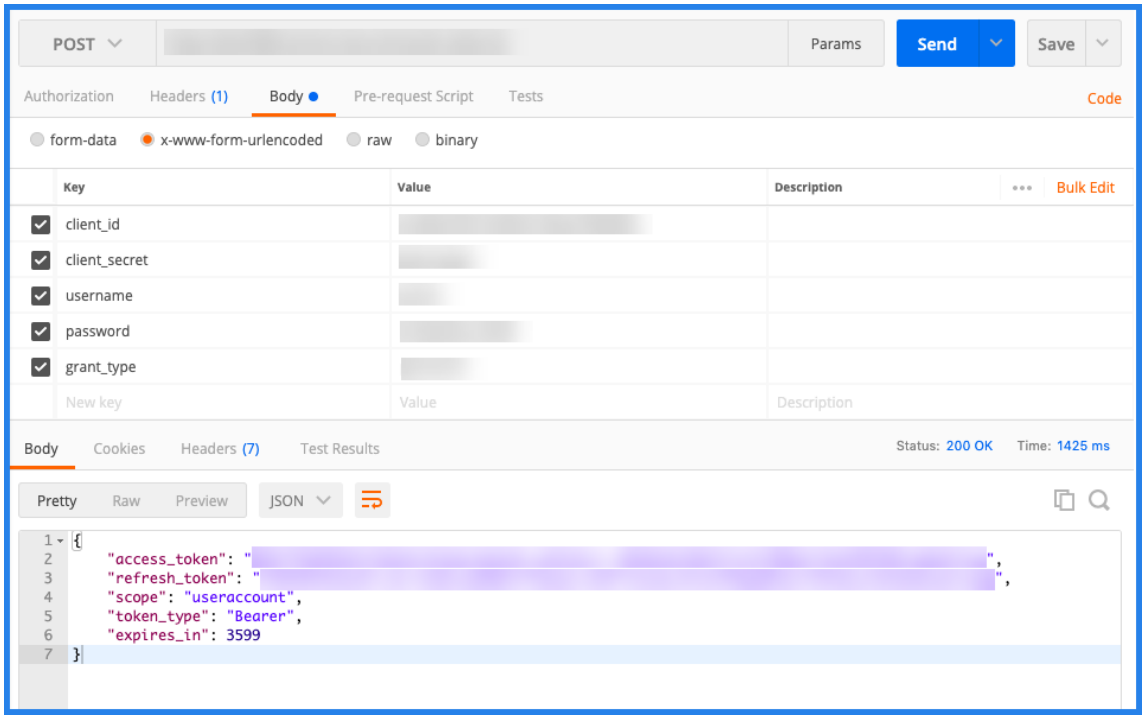


2. Navigate to **Identity Access and Management** > **API Access** and note the **Client ID** and **Client Secret** information.

Step 2 - Create an endpoint access in the ServiceNow instance

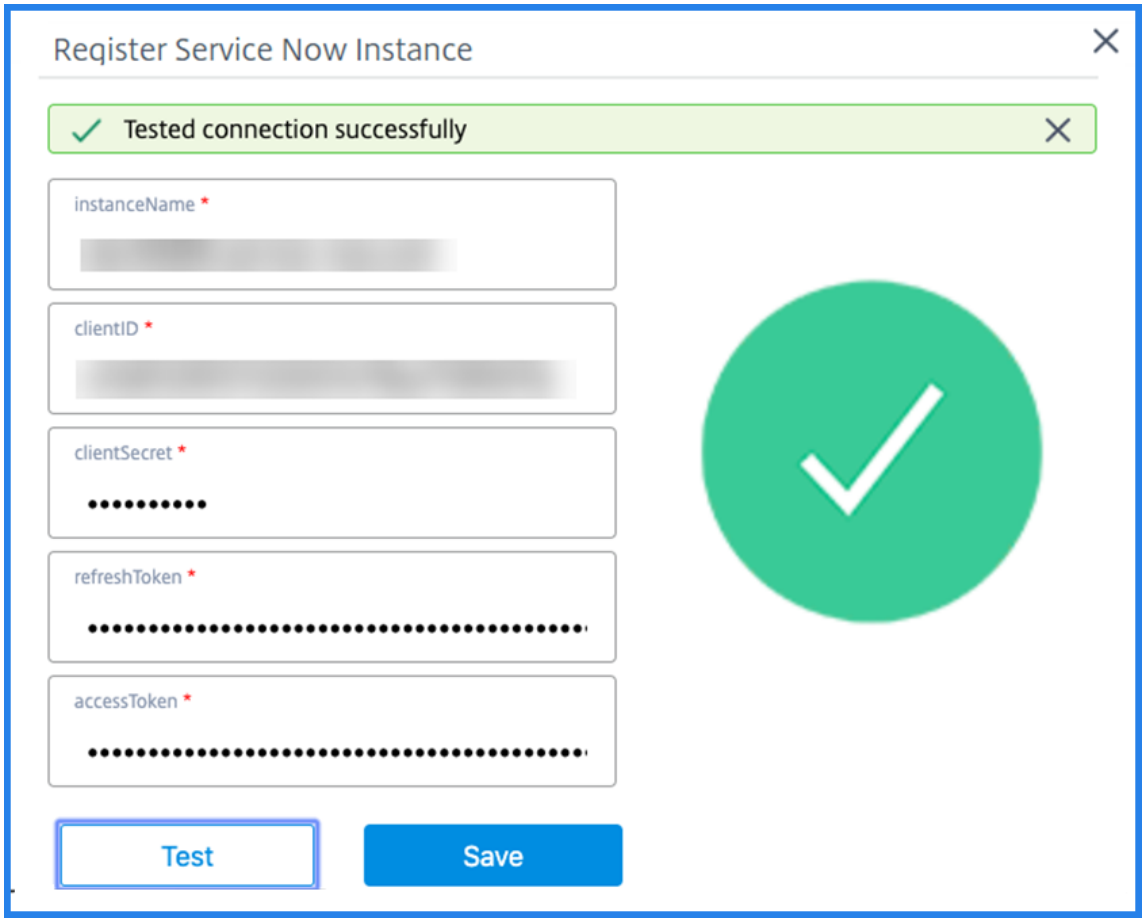
1. Log in to your ServiceNow instance with an administrator credentials.
2. Go to ServiceNow store. Download and install the **Citrix ITSM connector**.
3. On the **Citrix ITSM Connector** pane, select **Home** and then click **Authenticate**. Type the Client ID and Secret that you have noted from Citrix Cloud.
4. Test the connection.
5. Save the configuration. An acknowledgment from ServiceNow appears indicating that the connection is active.

6. Create an endpoint to access a ServiceNow instance. See Create an endpoint for clients to access the instance.
7. Obtain the Access and Refresh tokens using the Client ID and Client Secret. See OAuth tokens.



Step 3 - Add a ServiceNow instance

1. In the **Manage** tab, select Add ServiceNow Instance.
2. Specify the **Instance Name**, **Client ID**, **Client Secret**, **Refresh Token**, and **Access Token**.
3. Click **Test**.



The ServiceNow instance is now connected to the ITSM Adapter service.

4. After testing the connection successfully, click **Save** to add a ServiceNow instance.

Step 4 - Test auto-generation of ServiceNow tickets in ADM

1. Log in to NetScaler ADM.
2. Navigate to **Account > Notifications** and select **ServiceNow**.
3. Select the ServiceNow profile from the list.
4. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   If you want to view ServiceNow tickets in the NetScaler ADM GUI, select **ServiceNow Tickets**.

Set ServiceNow notifications in ADM

After the ServiceNow instance is registered on the ITSM adapter, you can set up ServiceNow notifications for the following events in the NetScaler ADM GUI:

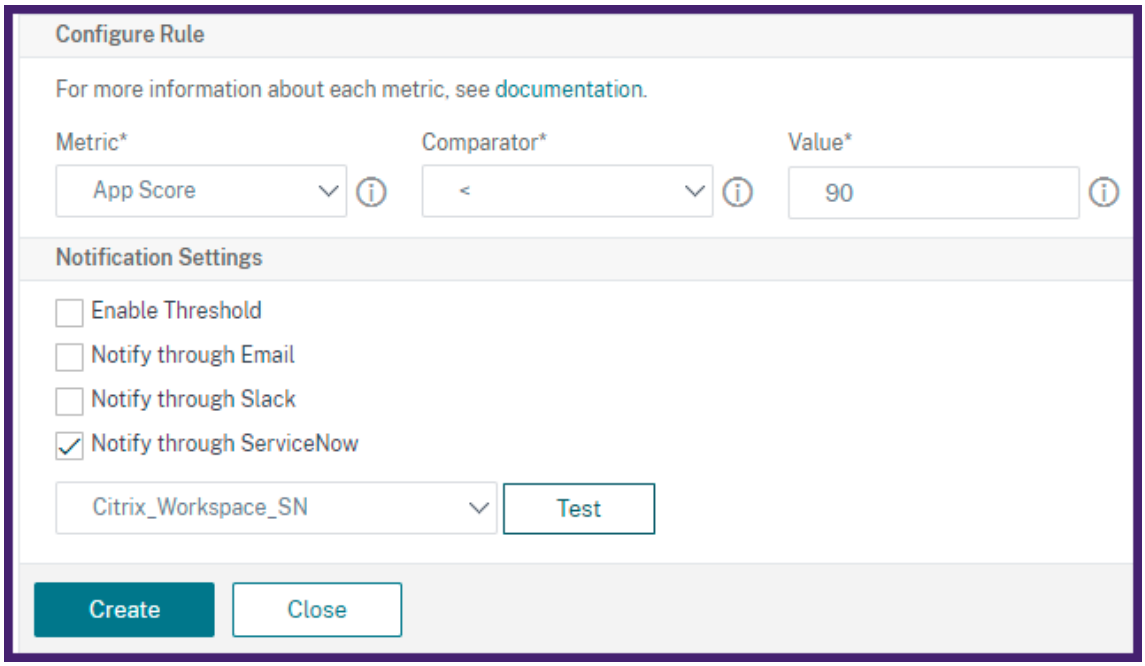
> **Important**
>
> This feature is supported on ServiceNow Cloud.

- **NetScaler events**: NetScaler ADM can generate the ServiceNow incidents for the selected set of NetScaler events from selected managed NetScaler instances.

  To send ServiceNow notifications for NetScaler events from the managed instances, you must configure an event rule and assign the rule action as **Send ServiceNow Notifications**.

  Create an event rule on the ADM by navigating to **Infrastructure > Events > Rules**. For more information, see Send ServiceNow notifications.

- **Application Analytics**: NetScaler ADM can generate ServiceNow incidents for the applications that breach the specified threshold.



  In this example, a ServiceNow incident is generated when the App score of applications falls under 90.

- **The SSL certificate and ADM license events**: NetScaler ADM can generate the ServiceNow incidents for the SSL certificate expiry and ADM license expiry events.

  To send ServiceNow notifications for an SSL certificate expiry, see The SSL certificate expiry.

  To send ServiceNow notifications for an ADM license expiry, see The NetScaler ADM license expiry.

Export or schedule export reports

March 11, 2024

In NetScaler ADM, you can export a comprehensive report for the selected NetScaler ADM feature. This report provides you an overview of the mapping between the instances, partitions, and corresponding details.

NetScaler ADM displays feature-specific scheduled export reports under individual ADM features, which you can view, edit, or delete. For example, to view the export reports of NetScaler instances, navigate to **Network > Instances > NetScaler** and click the export icon. You can export these reports in PDF, JPEG, PNG, and CSV file format.

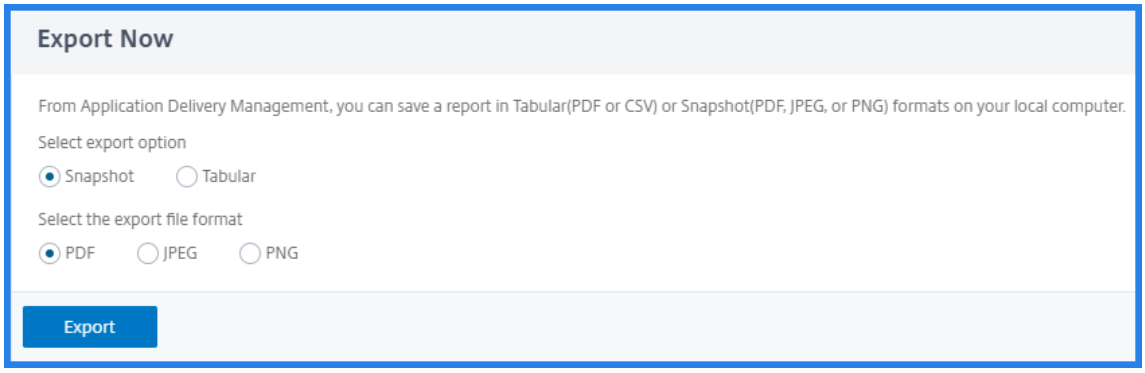
In **Export Reports**, you can perform the following actions:

- Export a report to a local computer
- Schedule export reports
- View, edit, or delete the scheduled export reports

Export a report

To export a report from the ADM to the local computer, perform the following steps:

1. Click the export icon at the top-right corner of the page.
2. Select **Export Now**.
3. Select one of the following the export options:
    - **Snapshot** - This option export ADM reports as a snapshot.
    - **Tabular** - This option export ADM reports in a tabular format. You can also choose how many data records to export in a tabular format

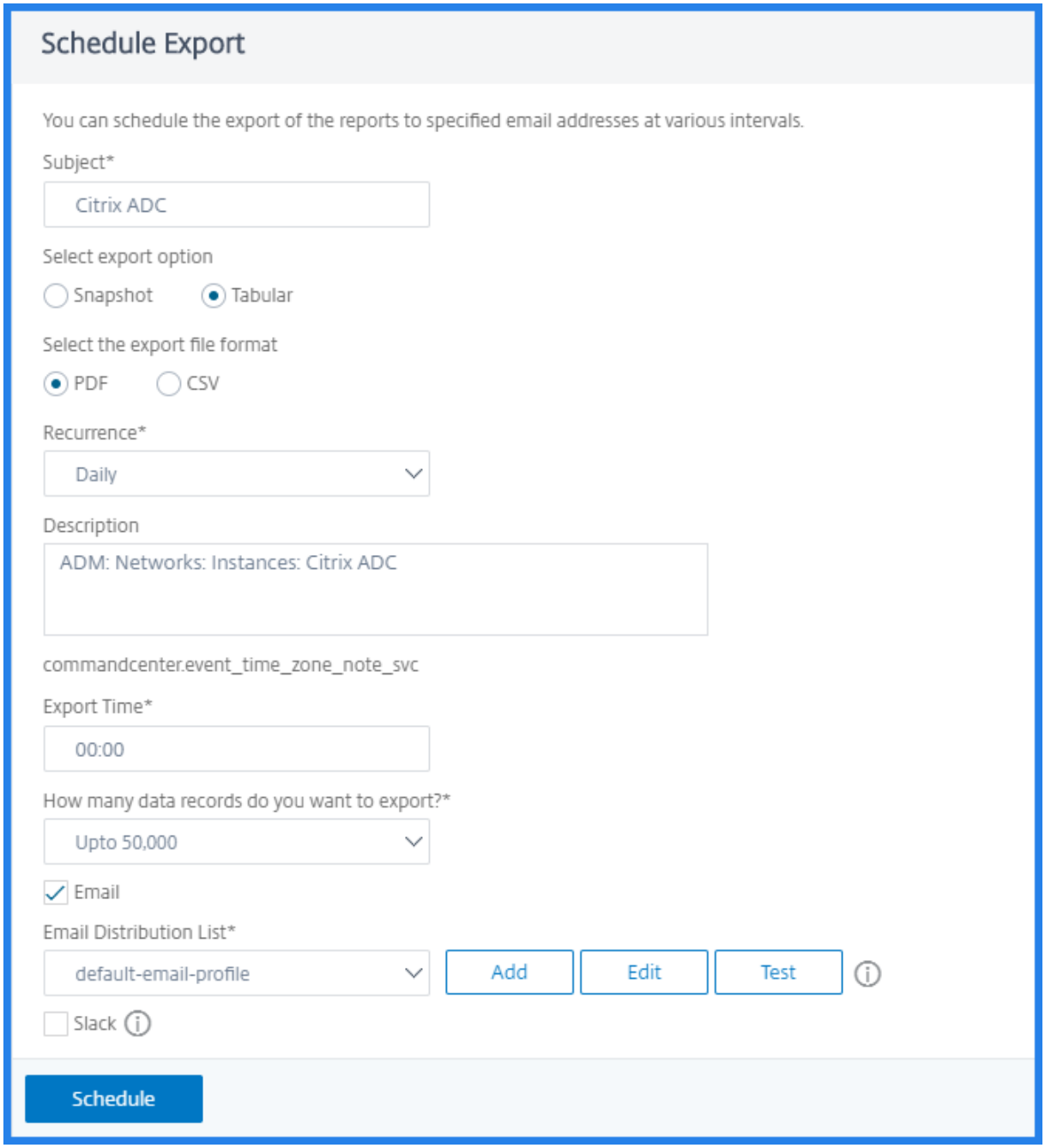


4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

Schedule export report

To schedule the export report at regular intervals, specify the recurrence interval. NetScaler ADM sends the exported report to the configured email or slack profile.

1. Click the export icon at the top-right corner of the page.
2. Select **Schedule Export** and specify the following:
    - **Subject** - By default, this field auto-populates the selected feature name. However, you can rewrite it with a meaningful title.
    - **Export option** - Export ADM reports in a snapshot or a tabular format. You can also choose how many data records to export in a tabular format
    - **Format** - Select the file format that you want to receive the report on the configured email or slack profile.
    - **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the list.
    - **Description** - Specify the meaningful description to a report.
    - **Export Time** - Specify at what time you want to export the report.
    - **Email** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
    - **Slack** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
3. Click **Schedule**.



View and edit the scheduled export reports

To view the export reports, perform the following:

1. Click the export icon at the top-right corner of the page.

   The **Export Report** page displays all the feature-specific export reports .

2. Select the report that you want to edit and click **Edit**.

Upgrade

March 11, 2024

Each NetScaler ADM release offers new and updated features with increased functionality. Citrix recommends you upgrade NetScaler ADM to the latest release to avail of the new features and bug fixes. A comprehensive list of enhancements, known issues, and bug fixes is included in the release notes accompanying every release announcement. It is also important to understand the licensing framework and the types of licenses that can be used before you start to upgrade. For NetScaler ADM licensing information, see Licensing.

The Upgrade path information is also available in the Citrix Upgrade Guide.

Before you upgrade

Download the upgrade package from the NetScaler ADM Downloads page and follow the instructions in this article to upgrade your system to the latest 13.1 build. After the upgrade process begins, ADM restarts and the existing connections are terminated and reconnected when the upgrade completes. The existing configuration is preserved, but NetScaler ADM does not process any data until the upgrade completes.

> **Important**
>
> The NetScaler ADM version and build should be **equal to or higher** than your NetScaler version and build. For example, if you have installed NetScaler ADM 12.1 Build 50.39, then ensure you have installed NetScaler 12.1 Build 50.28/50.31 or earlier.

Points to note before upgrading to 13.1:

- If you upgrade from version 11.1 or version 12.0 56.x and previous builds, perform the following steps:
  1. Upgrade from the existing version to 12.0 build 57.24.
  2. Upgrade to the latest build of version 12.1.
  3. Upgrade to version 13.1.
- If you upgrade from 12.0 build 57.24 and higher, first upgrade to 12.1 and then to 13.1.
- If you upgrade from 12.1, you can directly upgrade to 13.1.
- If you upgrade from versions lower than 13.0 64.xx, for better user experience, first upgrade to 13.0 64.xx and then to 13.1.

Important points to note before upgrading to 13.1 xx.xx and later

When you upgrade the ADM software to version 13.1 xx.xx, your ADM database is also migrated. This data migration happens because ADM now uses PostgreSQL version 10.11.

> **Note**
>
> Downgrading the ADM software is unsupported. Do not attempt to downgrade.

Recommended precautions:

- Take a snapshot of the NetScaler ADM server if you are upgrading to 13.1 xx.xx and later.
- Back up the NetScaler ADM server before you upgrade.
- After the upgrade, you might have to reestablish connections between the NetScaler ADM server and the managed instances. A confirmation prompt warns you that connections can fail if you proceed.
- If you upgrade to any version between 13.1.9.x and 13.1.30.x, NetScaler ADM rolls back the existing StyleBooks ConfigPacks to its earlier version.

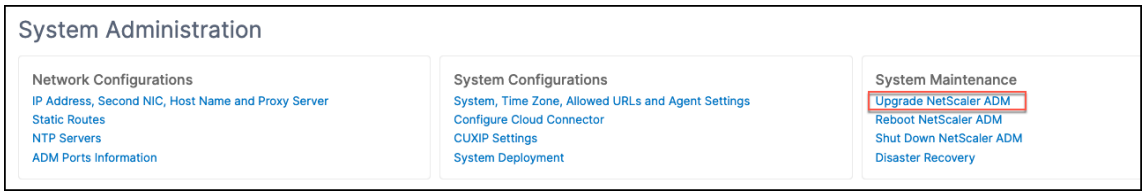
  To avoid this issue, upgrade to 13.1.33.50 build.
- For NetScaler ADM servers in high availability setup, when upgrading, do not make any configuration changes on either of the nodes.

  > **Warning**
  >
  > Do not refresh the browser until the upgrade process is successfully completed. Check the GUI for the approximate time for the upgrade to complete.

- After upgrade, the active node can change in a high availability pair.

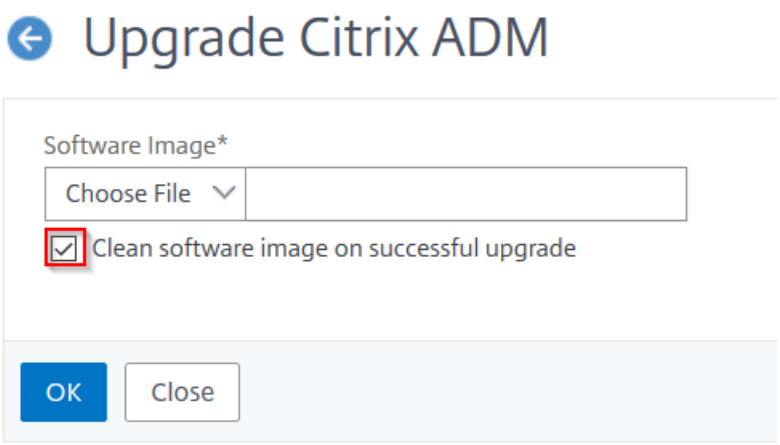
Upgrade a single NetScaler ADM server to 13.1-12.x

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Settings > Administration**. Under **System Maintenance**, click **Upgrade NetScaler ADM**.

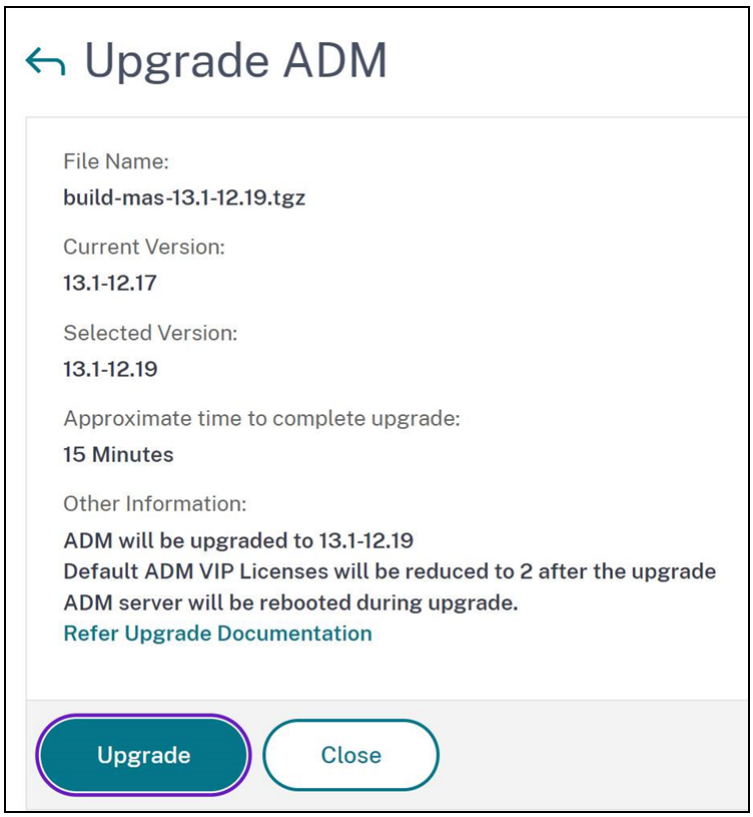


3. On the **Upgrade NetScaler ADM** page, select the **Clean software image on successful upgrade** check box to delete image files after upgrade. Selecting this option removes the NetScaler ADM image files automatically upon upgrade.

> **Note**
>
> This option is selected by default. If you do not select this check box before starting the upgrade process, you must manually delete the images.

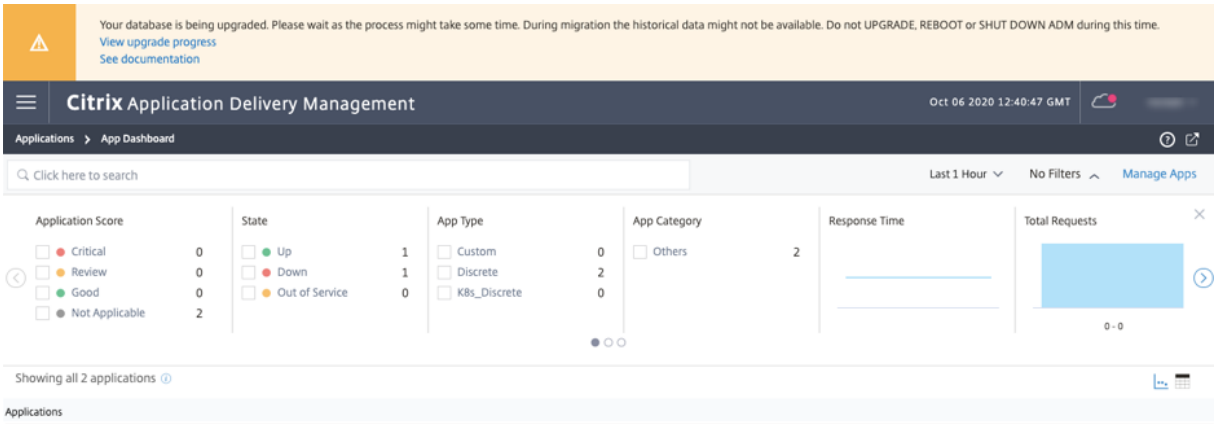


4. You can then upload a new image file by selecting either **Local** (your local machine) or **Appliance**. The build file must be present on the NetScaler ADM virtual appliance.
5. Click **OK**.
6. The **Upgrade ADM** page displays few details such as file name, selected version, estimated time to complete. Click **Upgrade**.



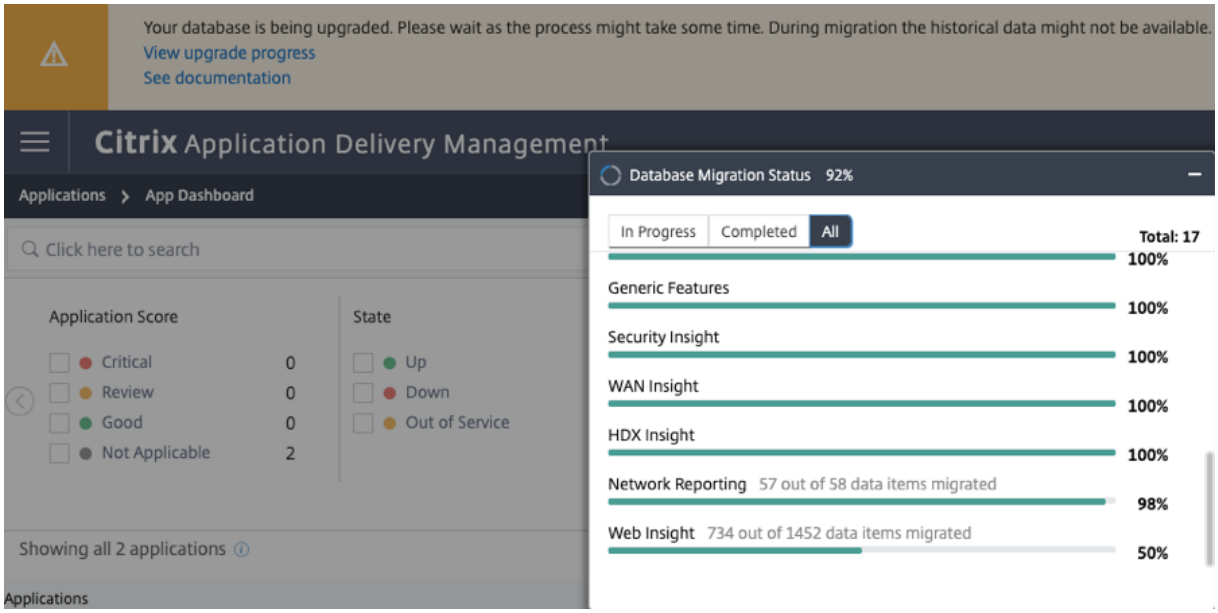
The upgrade process starts.

After your configuration is migrated, you can log on to the ADM GUI. Upon logon, the historical data starts to migrate at the background while you can continue to work on ADM.

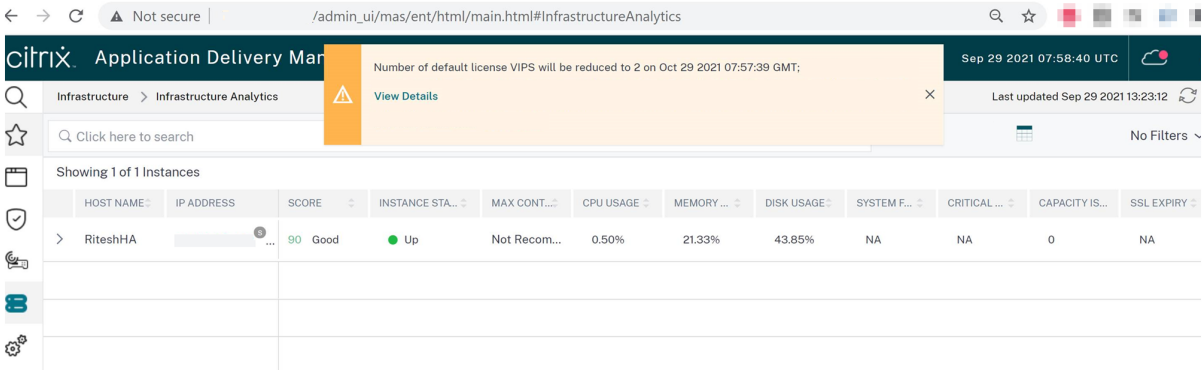


During historical data migration, some of the old data might not be available. The time taken to migrate your database depends on the size of data and the number of tables.

You can monitor the database migration using the ADM GUI. Click **View upgrade progress** and the **Database Migration Status** appears.

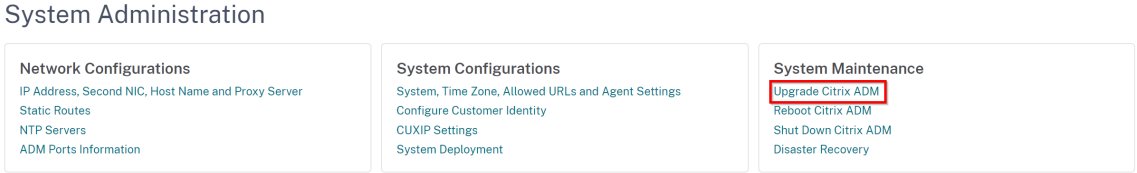


After the upgrade is complete, you can view the message that the default free licenses get reduced to two. Click **View Details** for more information.



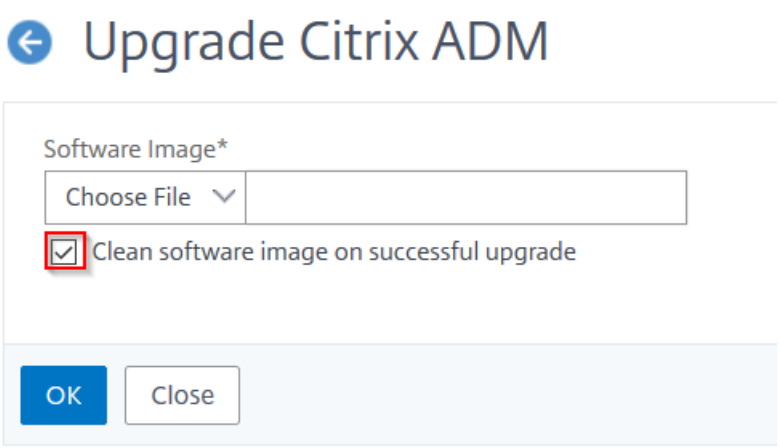
Upgrade a single NetScaler ADM server to 13.1-4.x or 13.1-9.x

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **System** > **System Administration**. Under the **System Administration** subheading, click **Upgrade NetScaler ADM**.

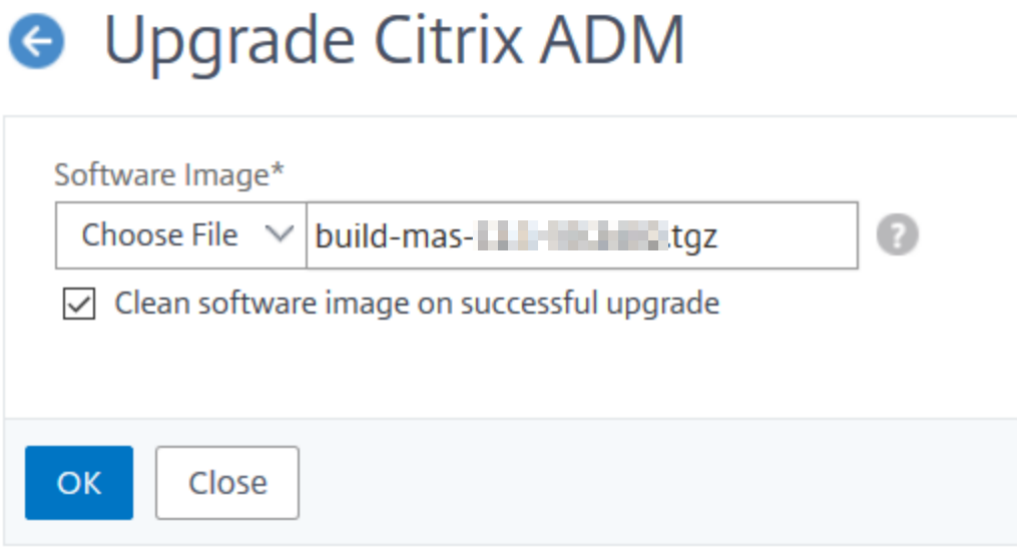
   

3. On the **Upgrade NetScaler ADM** page, select the **Clean software image on successful upgrade** check box to delete image files after upgrade. Selecting this option removes the NetScaler ADM image files automatically upon upgrade.

> **Note**
>
> This option is selected by default. If you do not select this check box before starting the upgrade process, you must manually delete the images.



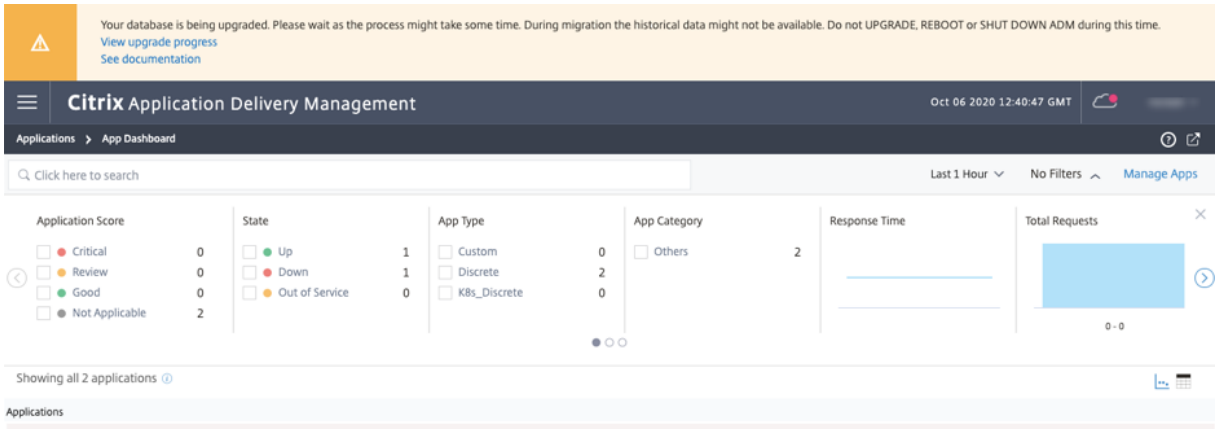
4. You can then upload a new image file by selecting either **Local** (your local machine) or **Appliance**. The build file must be present on the NetScaler ADM virtual appliance.



5. Click **OK**.
   The Confirm dialog box is displayed. Click **Yes**.

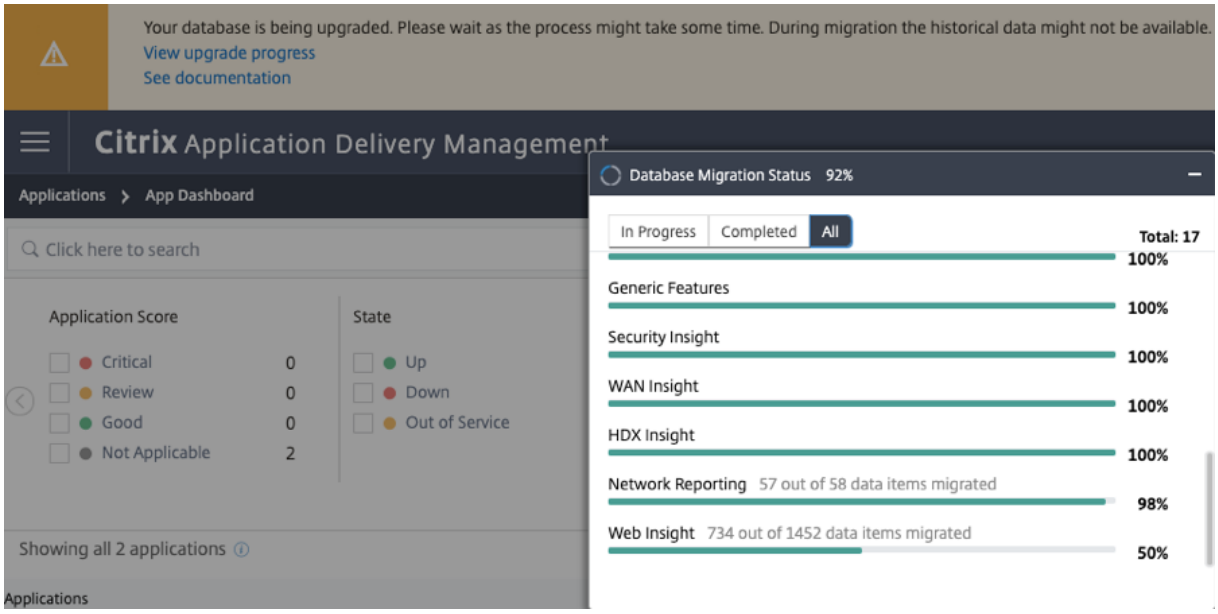
   The upgrade process starts.

After your configuration is migrated, you can log on to the ADM GUI. Upon logon, the historical data starts to migrate at the background while you can continue to work on ADM.



During historical data migration, some of the old data might not be available. The time taken to migrate your database depends on the size of data and the number of tables.

You can monitor the database migration using the ADM GUI. Click **View upgrade progress** and the **Database Migration Status** appears.



Troubleshooting database migration issues

During the upgrade process to 13.1 xx.xx and later, sometimes the migration of Web Insight historical data might appear to be stuck. In such cases, to check details of data migration, do the following.

Log on to the ADM shell prompt and run the following command to see the granular details of the progress.

```
1     cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
2
3 <!--NeedCopy-->
```


Here's an example output

```
    bash-3.2# cat /var/mps/log/db_upgrade/
       web_insight_mapping_migration_status
    Tue Oct  6 07:41:55 GMT 2020
    157 out of 127346 done in 54 seconds
    File
     /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
        af_app_client_server_resp_second_l3p_d7_dump
    bash-3.2#

<!--NeedCopy-->
```

In this example, `af_app_client_server_resp_second_l3p_d7` is the entry that is being upgraded. And 157 entries out of 127,346 is migrated in 54 seconds.

Upgrade a high availability pair from 12.1 release to 13.1 release

For NetScaler ADM servers in a high availability mode, you can upgrade by either accessing the active node or the floating IP address. Both the NetScaler ADM servers are automatically upgraded to the latest build once you initiate the upgrade process in either of the servers.

> **Note**
>
> If you are upgrading a high availability pair from 12.0 or earlier releases, see NetScaler ADM 12.1 Upgrade

Upgrade NetScaler ADM disaster recovery deployment

Upgrading NetScaler ADM disaster recovery deployment is a two-step process:

- Upgrade the NetScaler ADM nodes configured in high availability mode in the primary site. Later you must upgrade the disaster recovery node.
- Ensure that you have upgraded the NetScaler ADM servers that are deployed in high availability, before upgrading the disaster recovery node.

Upgrade the NetScaler ADM disaster recovery node

1. Download NetScaler ADM upgrade image file from NetScaler site.
2. Upload this file to the disaster recovery node using `nsrecover` credentials.
3. Log on to the disaster recovery node using the `nsrecover` credentials.
4. Navigate to the folder where you placed the image file and unzip the file.

5. Run the following script:

   ./installmas

```
bash-3.2# ./installmas
```

Upgrade on-prem agents for multisite deployment

Upgrading NetScaler agent deployment is a three-step process.
Ensure that you have completed the following tasks before upgrading the on-prem agents:

1. Upgrade the NetScaler ADM servers that are deployed in high availability.
2. Upgrade the NetScaler ADM disaster recovery node.

   For more information, see Upgrade NetScaler ADM disaster recovery deployment.

Upgrade the on-prem agent

1. Download NetScaler agent upgrade image file from NetScaler site.
2. Upload this file to the agent node using `nsrecover` credentials.
3. Ensure that you download the correct agent upgrade image.
4. Log on to the on-prem agent using the `nsrecover` credentials.
5. Navigate to the folder where you placed the image file and unzip the file.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Run the following script:

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

Add an extra disk to the NetScaler ADM server

If your NetScaler ADM storage requirement exceeds the default disk space (120 GB), you can attach an extra disk. You can attach more disk in both single-server and high availability deployments.

When you upgrade NetScaler ADM from release version 12.1–13.1Œ, the partitions that you had created on the additional disk in the earlier version remain the same. The partitions are not removed or resized.

The procedure to attach more disk remains the same in the upgraded build. You can now use the new disk partitioning tool in NetScaler ADM to create partitions in the newly added disk. You can also use the tool to resize the partitions in the existing more disk. For more information on how to attach more disks and to use the new disk partitioning tool, see How to attach an extra disk to NetScaler ADM.

Provision NetScaler instances in OpenStack using StyleBooks

From NetScaler ADM 12.1 build 49.23 onwards, the architecture of an OpenStack orchestration workflow has been updated. The workflow now uses NetScaler ADM StyleBooks to configure NetScaler instances. If you upgrade to NetScaler ADM 13.1 from version 12.0 or 12.1 build 48.18, you must run the following migration script:

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

For more information about the `os-cs-lb-mon` StyleBook and the migration script, see Provisioning of NetScaler VPX instance on OpenStack using StyleBook

Authentication

March 11, 2024

Users can be authenticated either internally by NetScaler ADM, externally by an authenticating server, or both. If local authentication is used, the user must be in the NetScaler ADM security database. If the user is authenticated externally, the user "external name"must match the external user identity registered with the authenticating server, depending on the selected authentication protocol.

NetScaler ADM supports external authentication by RADIUS, LDAP, and TACACS servers. This unified support provides a common interface to authenticate and authorize all the local and external Authentication, Authorization, and Accounting server users who are accessing the system. NetScaler ADM can authenticate users regardless of the actual protocols they use to communicate with the system. When a user attempts to access a NetScaler ADM implementation that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. If the authentication is successful, the user is granted access to NetScaler ADM.

External authentication servers

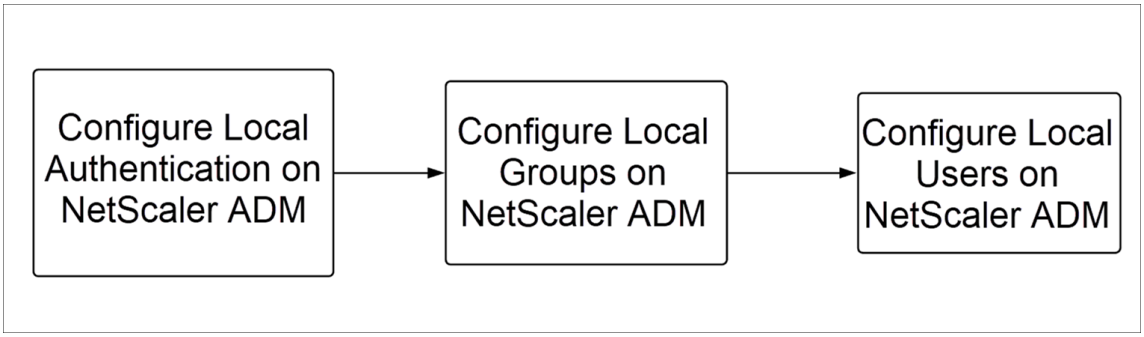
NetScaler ADM sends all authentication, authorization, and auditing service requests to the remote RADIUS, LDAP, or TACACS server. The remote authentication, authorization, and auditing server receive the request, validates the request, and sends a response to NetScaler ADM. When configured to use a remote RADIUS, TACACS, or LDAP server for authentication, NetScaler ADM becomes a RADIUS, TACACS, or LDAP client. In any of these configurations, authentication records are stored in the remote host server database. The account name, assigned permissions, and time-accounting records are also stored on the authentication, authorization, and auditing server for each user.

Also, you can use the internal database of NetScaler ADM to authenticate users locally. You create entries in the database for users and their passwords and default roles. You can also select the authentication order for specific types of authentication. The list of servers in a server group is an ordered list. The first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers to include the internal database as a fallback authentication backup to the configured list of authentication, authorization, and auditing servers.

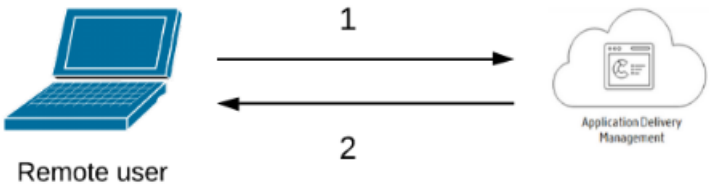
Authenticate users in NetScaler ADM

You can authenticate your users in NetScaler ADM in two ways:

- Local users configured in NetScaler ADM



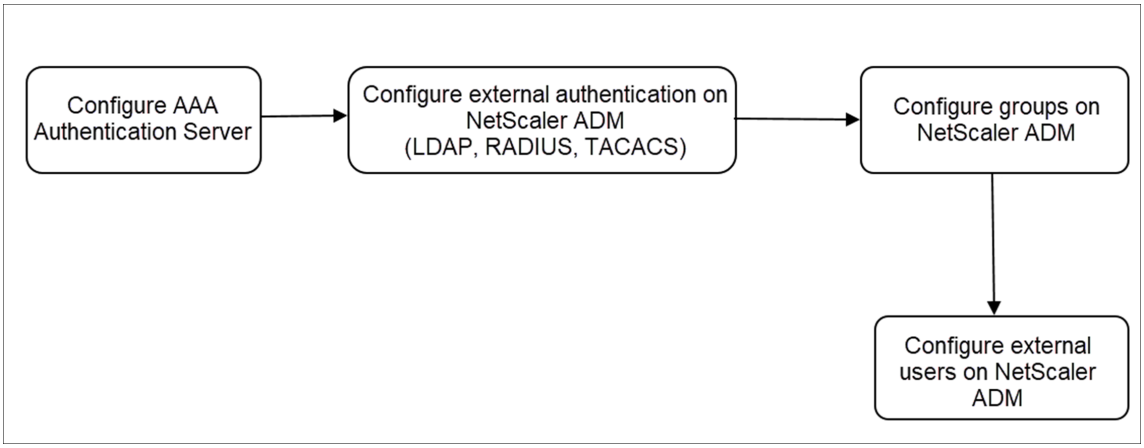
After configuration, the following is the workflow for user authentication in the local server.



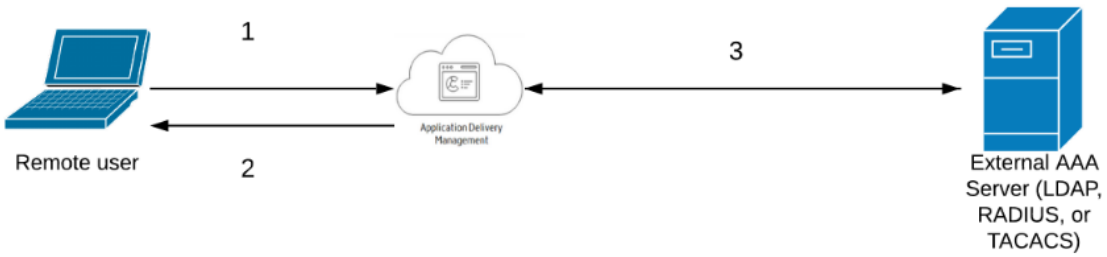
1 –The user logs on to NetScaler ADM

2 –NetScaler ADM prompts the users for credentials for authentication and checks if the credentials match in the ADM database.

- Using external authentication servers



After configuration, the following is the workflow for user authentication in the external authentication, authorization, and auditing server:



1 –The user connects with NetScaler ADM

2 –NetScaler ADM prompts the user for credentials

3 –NetScaler ADM validates the user credentials with the external authentication, authorization, and auditing server. If the validation is successful, the user can continue to log on

Configure external authentication servers in NetScaler ADM

March 11, 2024

After you configure the LDAP, RADIUS, or TACACS server, you can add these servers in NetScaler ADM.

Add LDAP authentication server

March 11, 2024

When you integrate LDAP protocol with RADIUS and TACAS authentication servers, you can use ADM to search and authenticate user credentials from distributed directories.

1. Navigate to **Settings > Authentication**.
2. Select the **LDAP** tab and then click **Add**.
3. On the **Create LDAP Server** page, specify the following parameters:

    a) **Name** –Specify the LDAP server name

    b) **Server Name/IP address** –Specify the LDAP IP address or server name

    c) **Security Type** –Type of communication required between the system and the LDAP server. Select from the list. If plain text communication is inadequate, you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL

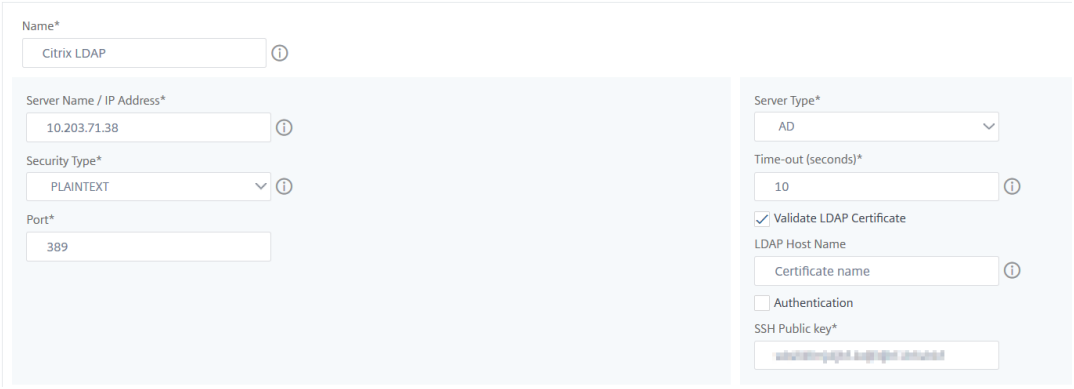
    d) **Port** –By default, port 389 is used for PLAINTEXT. You can also specify port 636 for SSL/TLS

    e) **Server Type** –Select Active Directory (AD) or Novell Directory Service (NDS) as the type of LDAP server

    f) **Time-out (seconds)** –Time in seconds for which the NetScaler ADM system waits for a response from the LDAP server

    g) **LDAP Host Name** –Select Validate LDAP Certificate check box and specifying the host name to be entered on the certificate

    Clear the **Authentication** option and specify the SSH Public Key. With key-based authentication, you can now fetch the list of public keys that are stored on the user object in LDAP server through SSH.

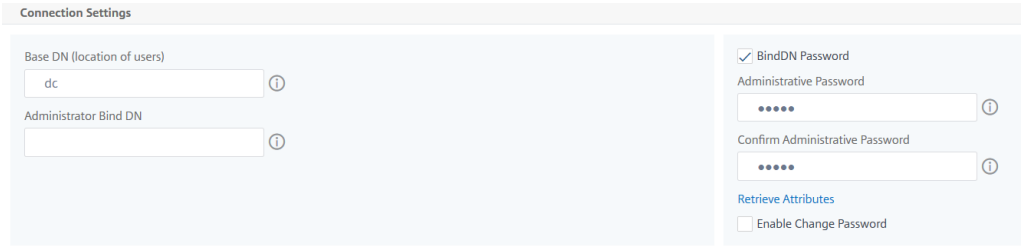
    Under Connection Settings, specify the following parameters:

    i. **Base DN** –The base node for LDAP server to start the search

    ii. **Administrator Bind DN** –User name to it bind to LDAP server. For example, admin@aaa.local.

iii. **Bind DN password** –Select this option to provide a password for authentication

iv. **Enable Change Password** –Select this option to enable password change



Under **Other Settings**, specify the following parameters

i. **Server Log on Name Attribute** –Name attribute used by the system to query the external LDAP server or an Active Directory. Select **samAccountname** from the list.

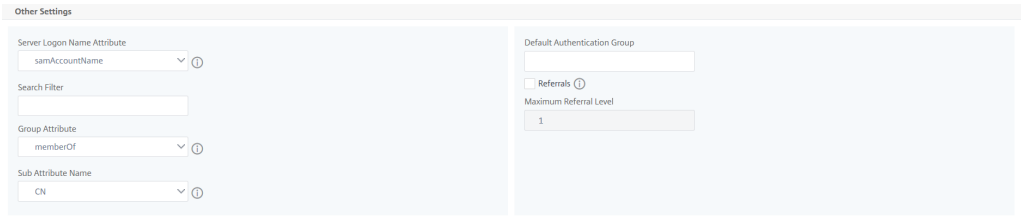
ii. **Search Filter** –Configure external users for two-factor authentication according to the search filter configured in LDAP server. For example, vpnallowed=true with ldaploginame `samaccount` and the user-supplied user name bob would yield an LDAP search string of: &(`vpnallowed`=**`true`**)(`samaccount`=`bob`).

> Note
>
> By default, the values in the search filter are enclosed in brackets.

iii. **Group Attribute** –Select memberOf from the list.

iv. **Sub Attribute Name** –The Sub attribute name for group extraction from the LDAP server.

v. **Default Authentication Group** –Default group to choose when the authentication succeeds in addition to extracted groups.



4. Click **Create**.

The LDAP server is now configured.

> **Note**:
>
> If the users are Active Directory group members, the group and the users'names on NetScaler ADM must have the same names of Active Directory group members.

5. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add RADIUS authentication server

March 11, 2024

1. Navigate to **Settings > Authentication**.
2. Select the **RADIUS** tab and then click **Add**.

   On the **Create RADIUS Server** page, specify the following parameters:

   a) **Name** –Specify a RADIUS server name

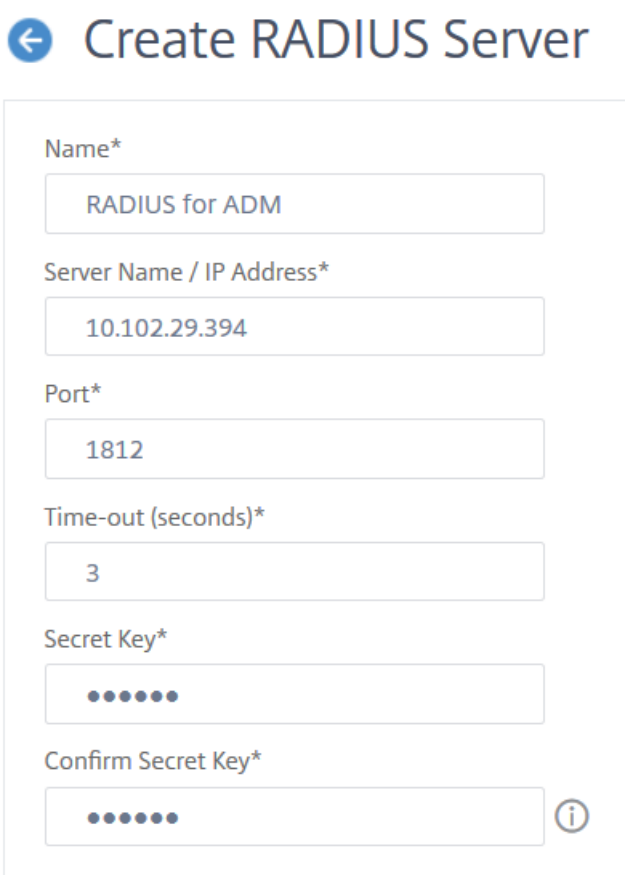
   b) **Server Name / IP address** –Specify the RADIUS server IP address

   c) **Port** –Specify the port number on which the RADIUS server is hosted. The default port is 1812

   d) **Time-out (seconds)** –Time in seconds for which the NetScaler ADM system waits for a response from the RADIUS server

   e) **Secret Key** –Specify the RADIUS secret key for authentication

   f) **Confirm Secret Key** –Specify the key again for confirmation



Under **Details**, specify the following parameters:

i. **NAS ID** –Specify the ID to send the identifier to RADIUS server

ii. **Group Vendor Identifier** –Specify the vendor ID for using RADIUS group extraction

iii. **Group Prefix** - A string that precedes group names within a RADIUS attribute for RADIUS group extraction

iv. **Group Attribute Type** –Specify the attribute type for RADIUS group extraction

v. **Group Separator** –A string that delimits group names within a RADIUS attribute for RADIUS group extraction

vi. **IP Address Vendor Identifier** –Vendor ID in RADIUS denotes the intranet IP. A value of 0 denotes that the attribute is not vendor encoded

vii. **Password Vendor Identifier** –Vendor ID password in RADIUS response to extract the user password

viii. **IP Address Attribute Type** –Remote IP address attribute for the RADIUS to respond

ix. **Password Attribute Type** –The password attribute for the RADIUS to respond

x. **Password encoding** –Select pap, chap, mschapv1, or mschapv2 from the list. This

denotes how passwords should be encoded in the RADIUS packets traveling from the system to the RADIUS server.

xi. **Default Authentication Group** –Default group to choose when the authentication succeeds in addition to extracted groups

Select Accounting if you want the appliance to log audit information with RADIUS server.

3. Click **Create**.

   The RADIUS server is now configured.

4. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add TACACS authentication server

March 11, 2024

1. Navigate to **Settings > Authentication**.
2. Select the **TACACS** tab and then click **Add**.
3. On the **Create TACACS** page, specify the following parameters:

   a) **Name** –Specify a TACACS server name

   b) **IP address** –Specify the TACACS IP address

   c) **Port** –Specify the port number on which the TACACS server is hosted. The default port is 49

   d) **Time-out (seconds)** –Time in seconds for which the NetScaler ADM system waits for a response from the LDAP server

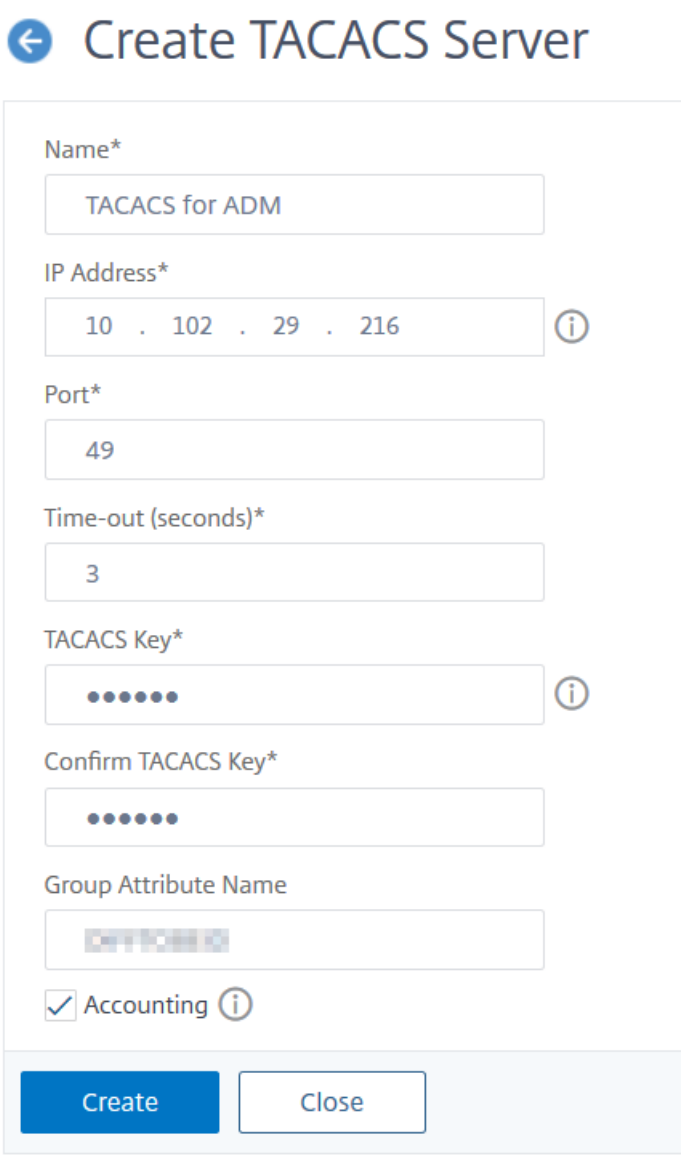
   e) **TACACS Key** –Specify the TACACS key for authentication

   f) **Confirm TACACS Key** –Specify the TACACS key again for confirmation

   g) **Group Attribute Name** –Specify the group name

   Select **Accounting** if you want the appliance to log audit information with TACACS server.

4. Click **Create**.



5. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Users in NetScaler ADM

March 11, 2024

You can create user accounts locally on NetScaler ADM to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server.

For more information on configuring users, see Configure Users.

> Note
>
> If the users are on Active Directory, ensure that the group name in NetScaler ADM is same as the one for the Active Directory group on the external server.

User Groups in NetScaler ADM

NetScaler ADM allows you to authenticate and authorize your users by creating groups and adding the users to the groups. A group can have either “admin”or “read-only”permissions and all users in that group will receive equal permissions.

In NetScaler ADM:

- A group is defined as a collection of users having similar permissions
- A group can have one or multiple roles
- A user is defined as an entity that can have access based on the permissions assigned
- A user can belong to one or more groups

You can create local groups in NetScaler ADM and use local authentication for the users in the groups. If you are using external servers for authentication, configure the groups on NetScaler ADM to match the groups configured on authentication servers in the internal network. When a user logs on and is authenticated, if a group name matches a group on an authentication server, the user inherits the settings for the group on NetScaler ADM.
If you are using local authentication, create users and add them to groups configured on NetScaler ADM. The users then inherit the settings for those groups.

For more information on configuring groups and assigning group permissions, see Configure Groups.

Extract an authentication server group

March 11, 2024

> **Note**
>
> TACACS server extraction is supported from **NetScaler ADM 13.0**.

NetScaler ADM enables you to:

- Extract the list of groups that a user belongs to on the external authentication server.

- Assign them to the group settings that match with the groups configured on the external server.

Advantages:

- You do not have to create users in NetScaler ADM, as they are managed on the external server.
- NetScaler ADM performs the authorization of users by assigning group permissions to access specific load balancer virtual servers, and for specific applications on the system.

Enable external authentication servers and fallback options

March 11, 2024

Fallback option enables local authentication to take over if the external server authentication fails. A user configured on both NetScaler ADM and external authentication server can log on to NetScaler ADM, even if the configured external authentication servers are down or not reachable. To ensure fallback authentication work:

- Non-nsroot users must be able to access NetScaler ADM if external server is down or not reachable
- You must add at least one external server

NetScaler ADM also supports a unified system of authentication, authorization, and accounting (AAA) protocols (LDAP, RADIUS, and TACACS), along with local authentication. This unified support provides a common interface to authenticate and authorize all users and external AAA clients accessing the system.

NetScaler ADM can authenticate users regardless of the actual protocols they to communicate with the system.
Cascading external authentication servers provides a continuous non-failing process for authenticating and authorizing external users. If authentication fails on the first authentication server, NetScaler ADM attempts to authenticate the user by using the second external authentication server, and so on. To enable cascade authentication, you must add the external authentication servers in NetScaler ADM. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS).

For example, consider that you want to add four external authentication servers and configured two RADIUS servers, one LDAP server, and one TACACS server. NetScaler ADM attempts to authenticate with the external servers, based on the configurations. In this example scenario, NetScaler ADM attempts to:

- Connect with the first RADIUS server
- Connect with the second RADIUS server, if the authentication has failed with first RADIUS server

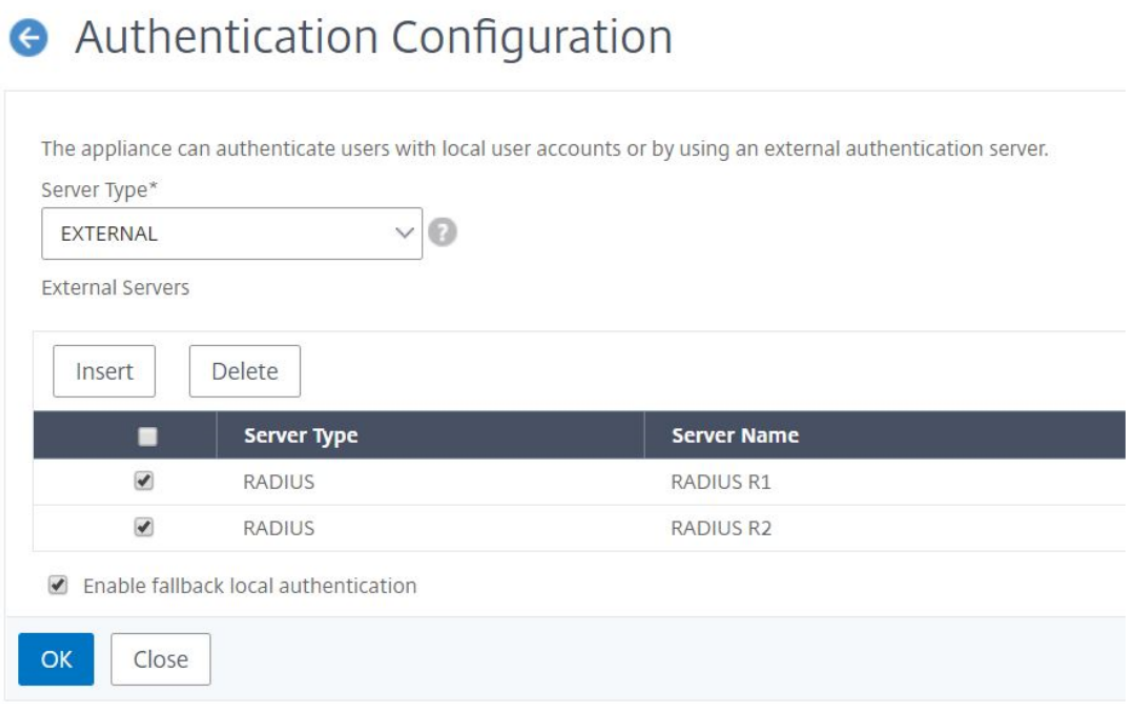
- Connect with the LDAP server, if the authentication has failed with both RADIUS servers
- Connect with the TACACS server, if the authentication has failed with both RADIUS servers and LDAP server.

> Note
>
> You can configure up to 32 external authentication servers in NetScaler ADM.

Configure fallback and cascade external servers

1. Navigate to **Settings > Authentication**.
2. On the **Authentication** page, click **Settings**
3. On the **Authentication Configuration** page, select **EXTERNAL** from the **Server Type** list (only external servers can be cascaded).
4. Click **Insert**, and on the **External Servers** page, select one or multiple authentication servers to cascade.
5. Select the **Enable fallback local authentication** check box if you want the local authentication to take over if the external authentication fails.
6. Select the **Log external group information** check box if you want to capture the external user group information in the system audit log.
7. Click **OK** to close the page.

   The selected servers are displayed under External Servers:



You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.

Access Control

March 11, 2024

Authentication is a process by which you verify that someone is who they claim they are. To perform authentication, a user must already have an account created in a system which can be interrogated by the authentication mechanism, or an account must be created as part of the process of the first authentication. NetScaler Application Delivery Management (ADM) provides a method for authenticating both local users and external users. While local users are authenticated internally, NetScaler ADM supports external authentication with RADIUS, LDAP, and TACACS protocols. When a user attempts to access NetScaler ADM that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. Once authenticated, the required protocol is used to identify the user on NetScaler ADM.

Access Control is the process of enforcing the required security for a particular resource. It is a security technique that can be used to regulate who can view or use resources in a computing environment. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, and what programs running on behalf of the users are allowed to do. In this way access control seeks to prevent

activity that can lead to a breach of security. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control through a reference monitor. NetScaler ADM allows fine-grained, role-based access control (RBAC) by which the administrators can provide access permissions to users based on the roles of individual users within an enterprise. RBAC in NetScaler ADM is achieved by creating access policies, roles, groups, and users.

Role-based access control

March 11, 2024

NetScaler ADM provides fine-grained, role based access control (RBAC), with which you can grant access permissions based on the roles of individual users within your enterprise. In this context, access is the ability to perform a specific task, such as view, create, modify, or delete a file. Roles are defined according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and help creating configuration templates.

Roles are determined by in policies. After creating policies, you create roles, bind each role to one or more policies, and assign roles to users. You can also assign roles to groups of users.

A group is a collection of users who have permissions in common. For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users or groups based on specific conditions. In NetScaler ADM, creating roles and policies are specific to the RBAC feature in NetScaler. Roles and policies can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

Roles can be feature based or resource based. For example, consider an SSL/security administrator and an application administrator. An SSL/security administrator must have complete access to SSL Certificate management and monitoring features, but must have read-only access for system administration operations. An application administrator must be able to access only the resources within the scope.

Example:

Chris, the ADC group head, is the super administrator of NetScaler ADM in his organization. Chris creates three administrator roles: security administrator, application administrator, and network administrator.

David, the security admin, must have complete access for SSL Certificate management and monitoring but also have read-only access for system administration operations.

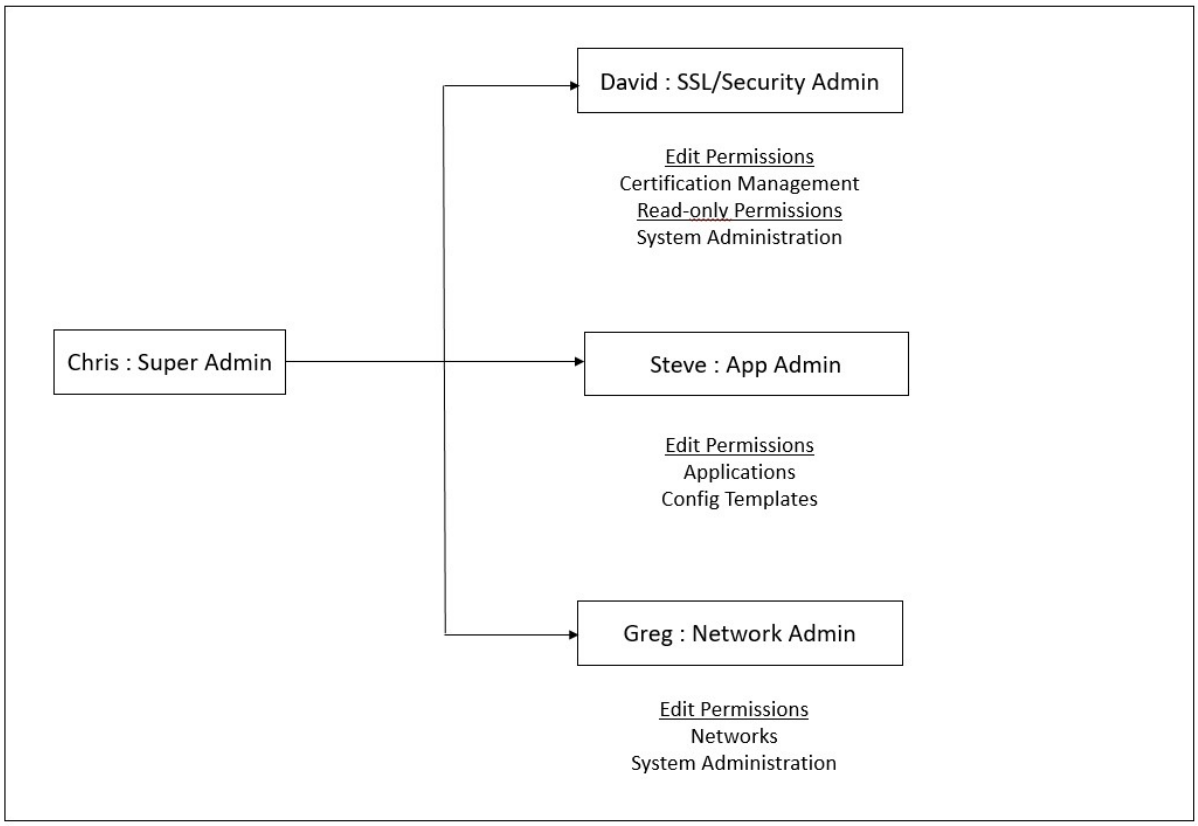
Steve, an application admin, needs access to only specific applications and only specific configuration templates.

Greg, a network admin, needs access to system and network administration.

Chris also must provide RBAC for all users, irrespective of the fact that they are local or external.

NetScaler ADM users can be locally authenticated or can be authenticated through an external server (RADIUS/LDAP/TACACS). RBAC settings must be applicable to all users irrespective of the authentication method adopted.

The following image shows the permissions that the administrators and other users have and their roles in the organization.



Limitations

RBAC is not fully supported for the following NetScaler ADM features:

- **Analytics** - RBAC is not supported fully in the analytics modules. RBAC support is limited to instance level, and it is not applicable at application level in the Web Insight, SSL Insight, Gateway Insight, HDX Insight, and WAF Security Violations analytics modules. For example:

Example 1: Instance based RBAC (Supported)

An administrator who has been assigned a few instances can see only those instances under **Web Insight** > **Instances**, and only the corresponding virtual servers under **Web Insight** > **Applications**,

because RBAC is supported at instance level.

Example 2: Application based RBAC (Not Supported)

An administrator who has been assigned a few applications can see all virtual servers under **Web Insight** > **Applications** but cannot access them, because RBAC is not supported at applications level.

- **StyleBooks** –RBAC is not fully supported for StyleBooks.
  - In NetScaler ADM, StyleBooks and configuration packs are considered as separate resources. Access permissions, either view, edit, or both, can be provided for StyleBook and configuration packs separately or concurrently. A view or edit permission on configuration packs implicitly allows the user to view the StyleBooks, which is essential for getting the configuration pack details and creating configuration packs.
  - Access permission for specific StyleBook or configuration packs is not supported
    Example: If there is already a configuration pack on the instance, users can modify the configuration on a target NetScaler instance even if they don't have access to that instance.
- **Orchestration** - RBAC is not supported for Orchestration.

Configure access policies

March 11, 2024

Access policies define permissions. A policy can be applied to a single user or group, or to multiple users and multiple groups. NetScaler Application Delivery Management (ADM) provides four predefined access policies:

1. **adminpolicy**. Grants access all NetScaler ADM features. The user has both view and edit permissions, can view all NetScaler ADM content, and can perform all edit operations. That is, the user can perform add, modify, and delete operations on the resources.
2. **readonlypolicy**. Grants read-only permissions. The user can view all content on NetScaler ADM, but is not authorized to perform any operations.
3. **appAdminPolicy**. Grants administrative permissions for accessing the application features in NetScaler ADM. A user bound to this policy can add, modify, and delete custom applications, and can enable or disable the services, service groups, and the various virtual servers, such as content switching, cache redirection, and HAProxy virtual servers.
4. **appReadOnlyPolicy**. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.

> **Note:**
>
> The predefined policies cannot be edited.

You can also create your own (user-defined) policies.

To create user-define access policies:

1. In NetScaler ADM, navigate to **Settings > Users & Roles > Access Policies**.
2. Click **Add**.
3. In the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.

   The **Permissions** section lists of all NetScaler ADM features, with options for specifying read-only, enable-disable, or edit access.
4. Click the (+) icon to expand each feature group into multiple features.

   a) Select the permission check box next to the feature name to grant permissions to the users.

   - **View:** This option allows the user to view the feature in NetScaler ADM.
   - **Enable-Disable:** This option is available only for the **Network Functions** features that allow enable or disable action on NetScaler ADM. User can enable or disable the feature. And, user can also perform the **Poll Now** action.

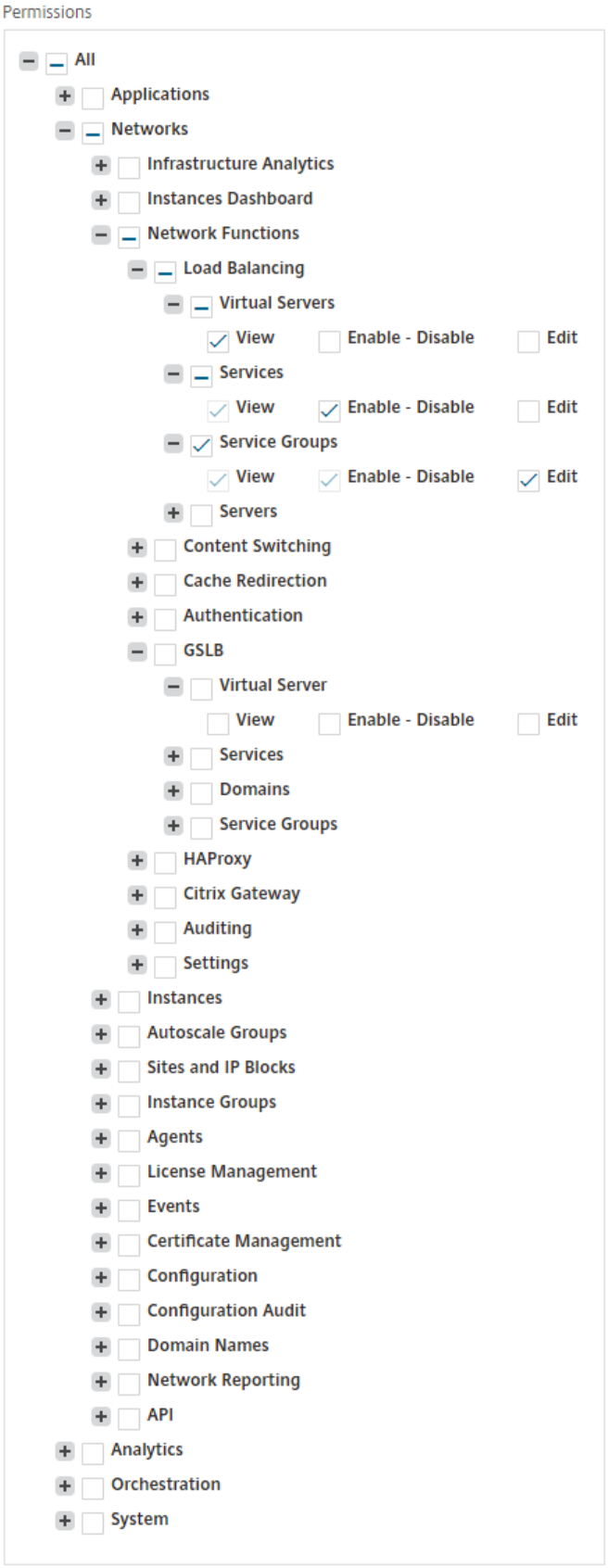
     When you grant the **Enable-Disable** permission to a user, the **View** permission is also granted. You cannot deselect this option.
   - **Edit:** This option grants the full access to the user. User can modify the feature and its functions.

     If you grant the **Edit** permission, both **View** and **Enable-Disable** permissions are granted. You cannot deselect the auto-selected options.

   If you select the feature check box, it selects all the permissions for the feature.

   > **Note:**
   >
   > Expand Load Balancing and GSLB to view more configuration options.

   In the following image, the configuration options of the Load Balancing feature have different permissions:



The **View** permission is granted to a user for the **Virtual Servers** feature. User can view the load balancing virtual servers in NetScaler ADM. To view virtual servers, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Virtual Servers** tab.

The **Enable-Disable** permission is granted to a user for the **Services** feature. This permission also grants the **View** permission. User can enable or disable the services bound to a load balancing virtual server. Also, user can perform **Poll Now** action on services. To enable or disable services, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Services** tab.

> **Note:**
>
> If a user has the **Enable-Disable** permission, the enable or disable action on a service is restricted in the following page:
>
> a) Navigate to **Infrastructure > Network Functions**.
>
> b) Select a virtual server and click **Configure**.
>
> c) Select the **Load Balancing Virtual Server Service Binding** page.
> This page displays an error message if you select **Enable** or **Disable**.

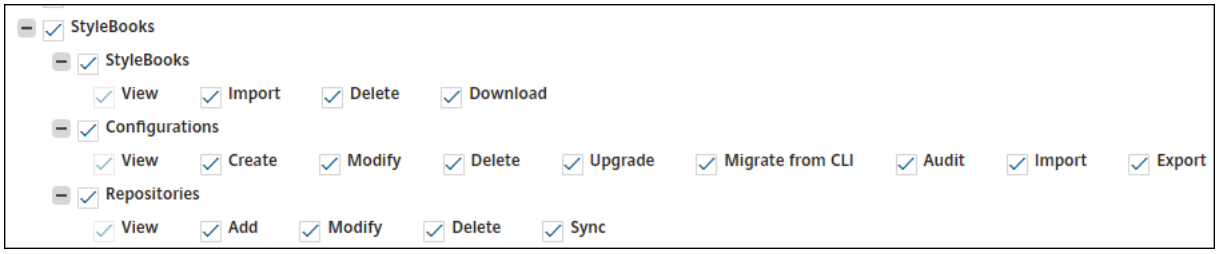
The **Edit** permission is granted to a user for the **Service Groups** feature. This permission grants the full access where **View** and **Enable-Disable** permissions are granted. User can modify the service groups that are bound to a load balancing virtual server. To edit service groups, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Service Groups** tab.

5. Click **Create**.

Grant StyleBook permissions to users

You can create an access policy to grant StyleBook permissions such as import, delete, download, and more.

> **Note:**
>
> The View permission is automatically enabled when you grant other StyleBook permissions.



Configure groups

March 11, 2024

In NetScaler ADM, a group can have both feature-level and resource-level access. For example, one group of users might have access to only selected NetScaler instances; another group with only a selected few applications, and so on.

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. All users in that group are assigned the same access rights in NetScaler ADM.

You can manage a user access in NetScaler ADM at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.

NetScaler ADM treats virtual server, services, service groups, and servers as network function entities.

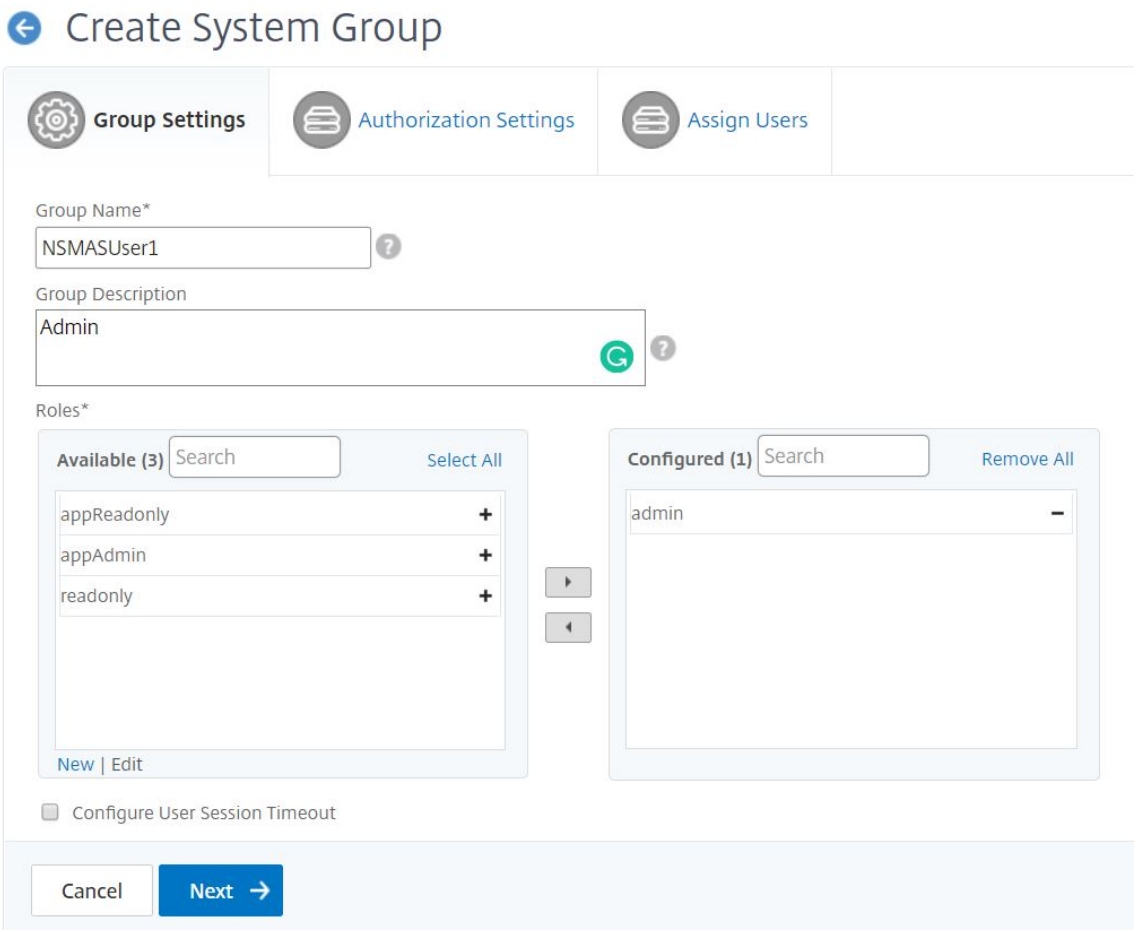
- **Virtual server (Applications)** - Load Balancing(lb), GSLB, Context Switching (CS), Cache Redirection (CR), Authentication (`Auth`), and NetScaler Gateway (VPN)
- **Services** - Load balancing and GSLB services
- **Service Group** - Load balancing and GSLB Service groups
- **Servers** - Load balancing Servers

Create a user group

1. In NetScaler ADM, navigate to **Settings > Users & Roles > Groups**.
2. Click **Add**.

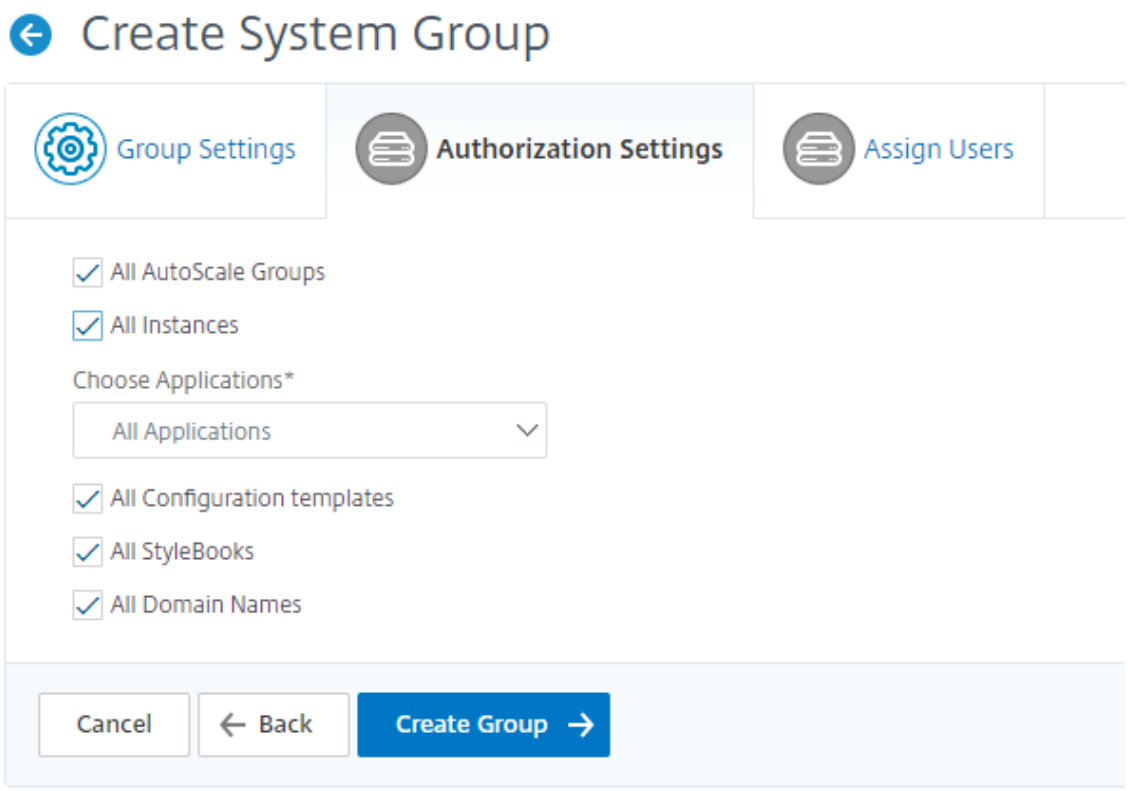
   The **Create System Group** page is displayed.
3. In the **Group Name** field, enter the name of the group.
4. In the **Group Description** field, type in a description of your group. Providing a good description of the group helps you to understand the role and function of the group in a better way at a later point.
5. In the **Roles** section, add or move one or more roles to the **Configured** list.

   > **Note:**
   >
   > Under the **Available** list, you can click **New** or **Edit** and create or modify roles. Alternatively, you can navigate to **Settings > Users & Roles > Users** and create or modify users.



6. Click **Next**. On the **Authorization Settings** tab, you can provide authorization settings for the following resources:

   - Autoscale Groups
   - Instances
   - Applications
   - Configuration Templates
   - StyleBooks
   - Configpacks
   - Domain Names



You might want to select specific resources from the categories to which users can have access.

Autoscale Groups:

If you want to select the specific Autoscale groups that a user can view or manage, perform the following steps:

a) Clear the **All AutoScale Groups** check box and click **Add AutoScale Groups**.

b) Select the required Autoscale groups from the list and click **OK**.

Instances:

If you want to select the specific instances that a user can view or manage, perform the following steps:

a) Clear the **All Instances** check box and click **Select Instances**.

b) Select the required instances from the list and click **OK**.

Applications:

The **Choose Applications** list allows you to grant access to a user for the required applications.

You can grant access to applications without selecting their instances. Because applications are independent of their instances to grant user access.

When you grant a user access to an application, the user is authorized to access only that application regardless of instance selection.

This list provides you the following options:

- **All Applications:** This option is selected by default. It adds all the applications that are present in the NetScaler ADM.
- **All Applications of selected instances:** This option appears only if you select instances from the **All Instances** category. It adds all the applications present on the selected instance.
- **Specific Applications:** This option allows you to add the required applications that you want users to access. Click **Add Applications** and select the required applications from the list.
- **Select Individual Entity Type:** This option allows you to select a specific type of network function entity and corresponding entities.

  You can either add individual entities or select all entities under the required entity type to grant access to a user.

  The **Apply on bound entities also** option authorizes the entities that are bound to the selected entity type. For example, if you select an application and select **Apply on bound entities also**, NetScaler ADM authorizes all the entities that are bound to the selected application.

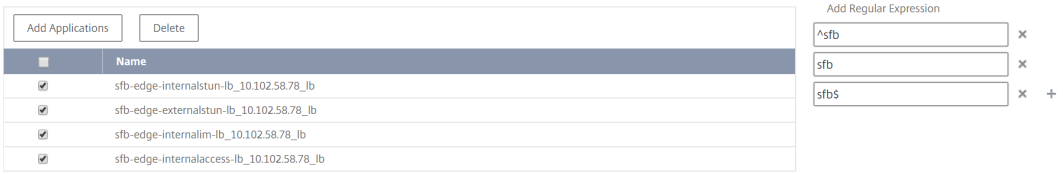
  > **Note:**
  >
  > Ensure you have selected only one entity type if you want to authorize bound entities.

You can use regular expressions to search and add the network function entities that meet the regex criteria for the groups. The specified regex expression is persisted in NetScaler ADM. To add regular expression, perform the following steps:

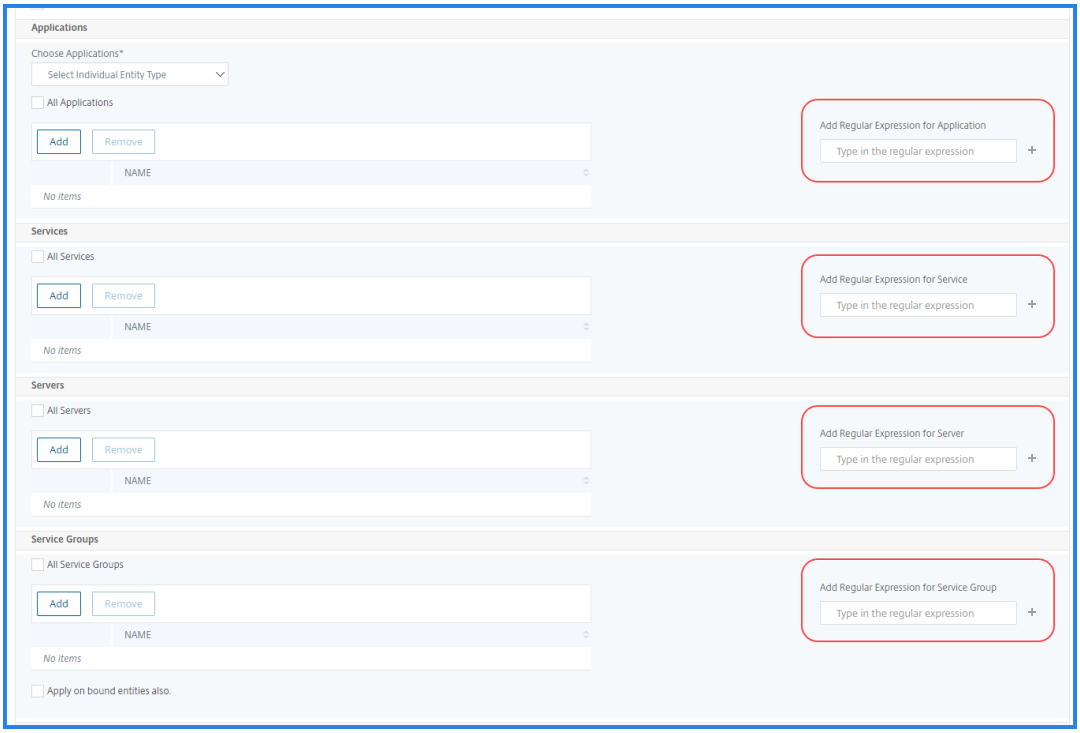
a) Click **Add Regular Expression**.

b) Specify the regular expression in the text box.

   The following image explains how to use regular expression to add an application when you select the **Specific Applications** option:



The following image explains how to use regular expression to add network function entities when you choose the **Select the Individual Entity Type** option:



If you want to add more regular expressions, click the **+** icon.

> **Note:**
>
> The regular expression only matches the server name for the **Servers** entity type and not the server IP address.

If you select the **Apply on bound entities also** option for a discovered entity, a user can automatically access the entities that are bound to the discovered entity.

The regular expression is stored in the system to update the authorization scope. When the new entities match the regular expression of their entity type, NetScaler ADM updates the authorization scope to the new entities.

Configuration Templates:

If you want to select the specific configuration template that a user can view or manage, perform the following steps:

a) Clear the **All Configuration templates** check box and click **Add Configuration Template**.

b) Select the required template from the list and click **OK**.

StyleBooks:

If you want to select the specific StyleBook that a user can view or manage, perform the following steps:

a) Clear the **All StyleBooks** check box and click **Add StyleBook to Group**. You can either select individual StyleBooks or specify a filter query to authorize StyleBooks.

If you want to select the individual StyleBooks, select the StyleBooks from the **Individual StyleBooks** pane and click **Save Selection**.

If you want to use a query to search StyleBooks, select the **Custom Filters** pane. A query is a string of key-value pairs where keys are `name`, `namespace`, and `version`.

You can also use regular expressions as values to search and add StyleBooks that meet regex criteria for the groups. A custom filter query to search StyleBooks supports both `And` and `Or` operation.

Example:

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
<!--NeedCopy-->
```

This query lists the StyleBooks that meet the following conditions:

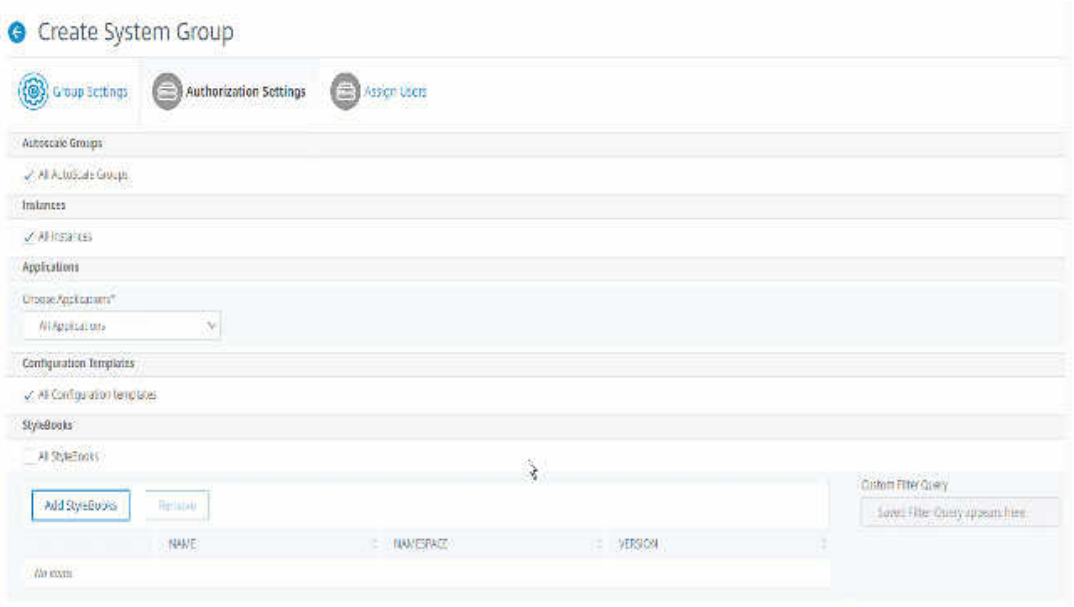
- StyleBook name is either `lb-mon` or `lb`.
- StyleBook namespace is `com.citrix.adc.stylebooks`.
- StyleBook version is `1.0`.

Use an `Or` operation between value expressions that is defined to the key expression.

Example:

- The `name=lb-mon|lb` query is valid. It returns the StyleBooks having a name either `lb-mon` or `lb`.
- The `name=lb-mon | version=1.0` query is invalid.

Press `Enter` to view the search results and click **Save Query**.



The saved query appears in the **Custom Filters Query**. Based on the saved query, the ADM provides user access to those StyleBooks.

b) Select the required StyleBooks from the list and click **OK**.

You can select the required StyleBooks when you create groups and add users to that group. When your user selects the permitted StyleBook, all dependent StyleBooks are also selected.

Configpacks:

In **Configpacks**, select one of the following options:

- **All Configrations**: This option is selected by default. It adds all the configuration packs that are in ADM.
- **All Configrations of the selected StyleBooks**: This option adds all the configuration packs of the selected StyleBook.
- **Specific Configurations**: This option allows you to add the required cofiguration packs.

  You can select the required configuration packs when you create groups and add users to that group.

Domain Names:

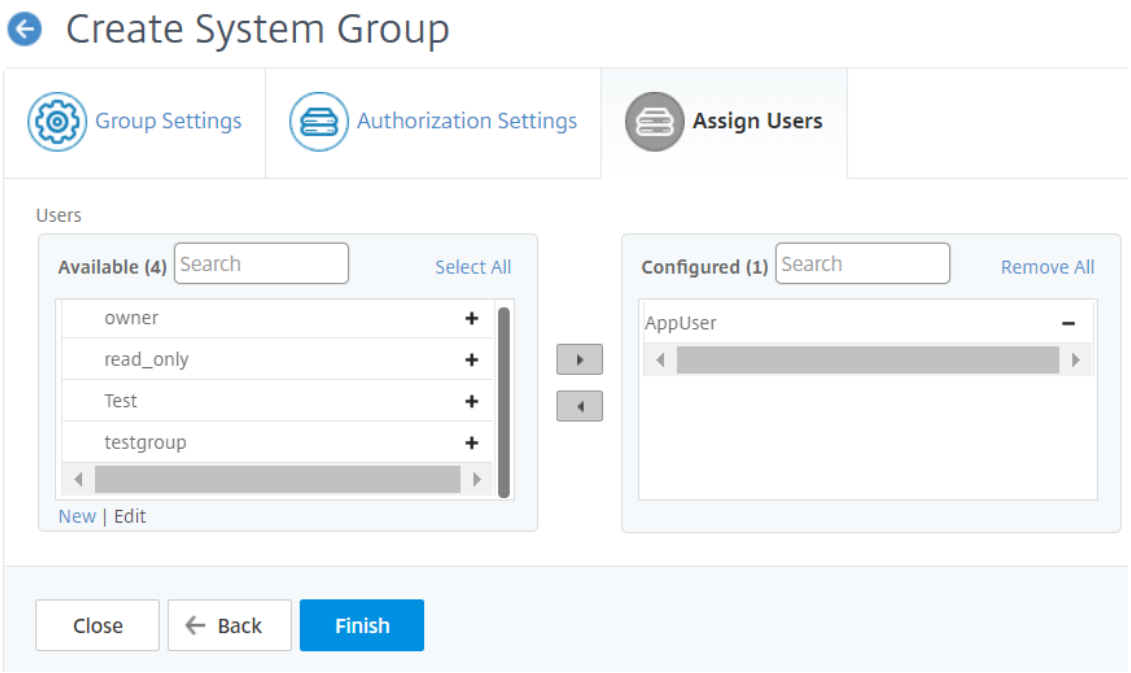
If you want to select the specific domain name that a user can view or manage, perform the following steps:

a) Clear the **All Domain Names** check box and click **Add Domain Name**.

b) Select the required domain names from the list and click **OK**.

7. Click **Create Group**.
8. In the **Assign Users** section, select the user in the **Available** list, and add the user to the **Configured** list.

   > **Note:**
   >
   > You can also add users by clicking **New**.



9. Click **Finish**.

Manage user access across multiple network function entities

As an administrator, you can manage user access at the individual level of network function entities in NetScaler ADM. And, you can dynamically assign specific permissions to the user or a group at the entity level by using the regular expression filter.

This document describes how to define user authorization at the entity level.

Before you begin, create a group. See Configure groups on NetScaler ADM for more information.

Usage scenario:

Consider a scenario where one or more applications (virtual servers) are hosted on the same server. A super administrator (George) wants to grant Steve (an application administrator) access only to App1 and not to the hosting server.

The following table illustrates this environment, where Server-A hosts applications App-1 and App-2.

Host Server	Application (virtual server)	Service	Service group
Server A	App1	App-service-1	App-service-group-1
Server A	App2	App-service-2	App-service-group-2

> **Note**
>
> NetScaler ADM treats virtual server, services, service groups, and servers as network function entities. The entity type virtual server is referred as an application.

To assign user permissions to network function entities, George defines the user authorization as follows:

1. Navigate to **Account > User Administration > Groups** and add a group.
2. In the **Authorization Settings** tab, select Choose Applications.
3. Choose **Select Individual Entity Type**.
4. Select the **All Applications** entity type and add the App-1 entity from the available list.
5. Click **Create Group**.
6. In **Assign users**, select the users who require the permission. For this scenario, George selects Steve's user profile.
7. Click **Finish**.

With this authorization setting, Steve can manage only App-1 and not other network function entities.

> **Note:**
>
> Ensure the **Apply on bound entities also** option is cleared. Otherwise, NetScaler ADM grants access to all network function entities that are bound to App-1. As a result, grants access to the hosting server as well.

A super administrator can specify the regular expressions (regex) for each entity type. The regular expression is stored in the system to update the user authorization scope. When new entities match the regular expression of their entity type, NetScaler ADM can dynamically grant users access to the specific network function entities.

To grant user permissions dynamically, the super administrator can add regular expressions in the **Authorization Settings** tab.

In this scenario, George adds App* as a regular expression for the Applications entity type and the applications that match the regex criteria appear in the list. With this authorization setting, Steve can access all the applications that match the App* regex. However, his access is limited only to the applications not to the hosted server.

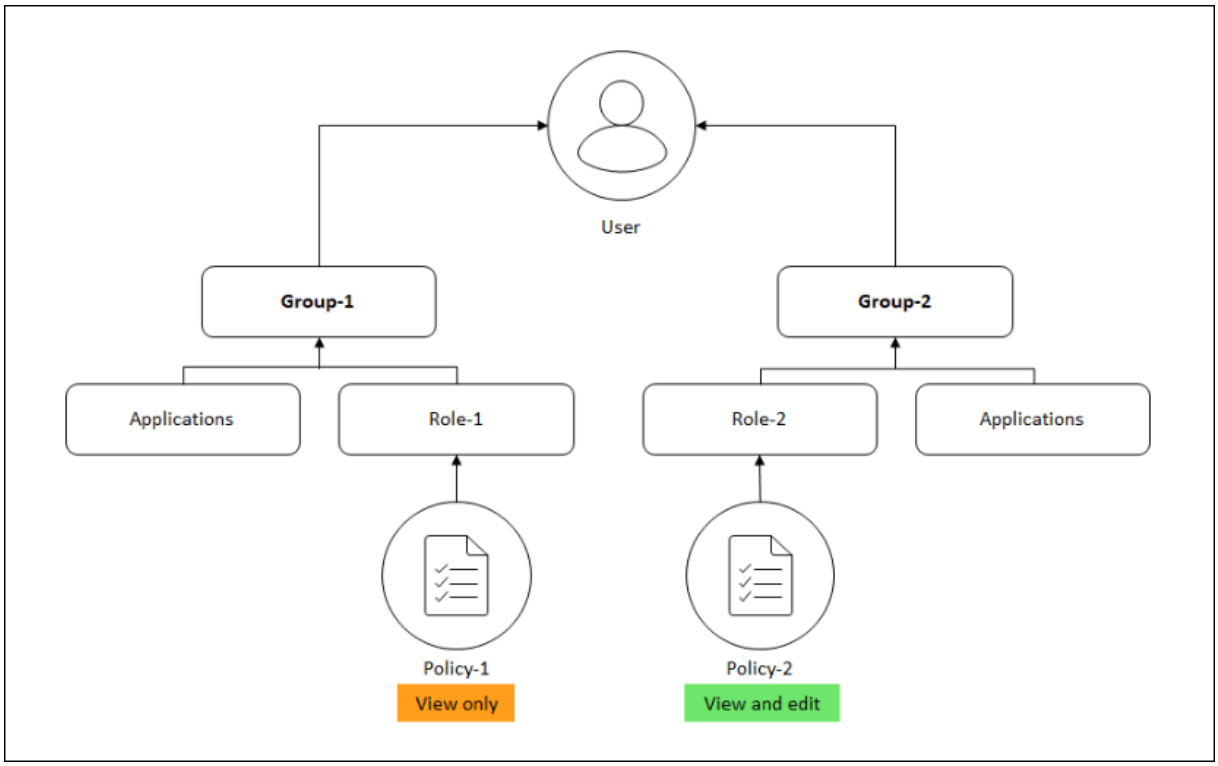
How user access changes based on the authorization scope

When an administrator adds a user to a group that has different access policy settings, the user is mapped to more than one authorization scopes and access policies.

In this case, the ADM grants the user access to applications depending on the specific authorization scope.

Consider a user who is assigned to a group that has two policies Policy-1 and Policy-2.

- **Policy-1** –View only permission to applications.
- **Policy-2** –View and Edit permission to applications.



The user can view the applications specified in Policy-1. Also, this user can view and edit the applications specified in Policy-2. The edit access to Group-1 applications are restricted as it is not under Group-1 authorization scope.

Mapping of RBAC when upgrading NetScaler ADM from 12.0 to later releases

When you upgrade NetScaler ADM from 12.0 to 13.1, you do not see the options to provide "read-write"or "read"permissions while creating groups. These permissions have been replaced by "roles and access policies,"which give you more flexibility to provide role-based permissions to the users. The following table shows how the permissions in release 12.0 are mapped to release 13.1:

12.0	Allow Applications Only	13.1
admin read-write	False	`admin`
admin read-write	True	`appAdmin`
admin read-only	False	`readonly`
admin read-only	True	`appReadonly`

Configure roles

March 11, 2024

In NetScaler Application Delivery Management (ADM), each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add NetScaler instances in NetScaler ADM, and the other policy might grant permission to create and deploy StyleBooks and to configure NetScaler instances.

When multiple policies define edit and read-only permissions for a single feature, the edit permissions have priority.

NetScaler ADM provides four predefined roles:

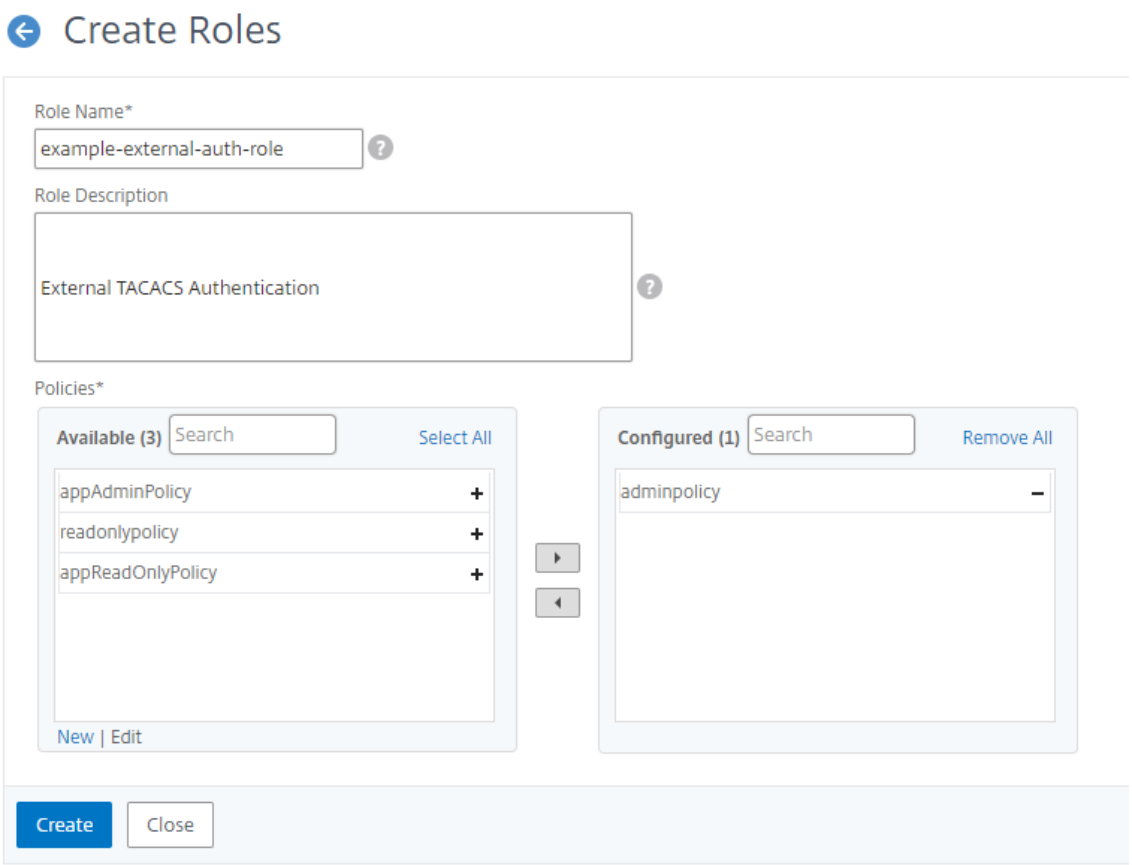
- **admin**. Has access to all NetScaler ADM features. (This role is bound to adminpolicy.)
- **readonly**. Has read-only access. (This role is bound to readonlypolicy.)
- **appAdmin**. Has administrative access to only the application features in NetScaler ADM. (This role is bound to appAdminPolicy).
- **appReadonly**. Has read-only access to the application features. (This role is bound to appReadOnlyPolicy.)

> **Note:**
>
> The predefined roles cannot be edited.

You can also create your own (user-defined) roles.

To create roles and assign policies to them:

1. In NetScaler ADM, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. In the **Role Name** field, enter the name of the role, and provide the description in the **Role Description** field (optional.)
4. In the **Policies** section, add or move one or more policies to the **Configured** list.



5. Click **Create**.

Configure users

March 11, 2024

By default, NetScaler Application Delivery Management (ADM) has one user:

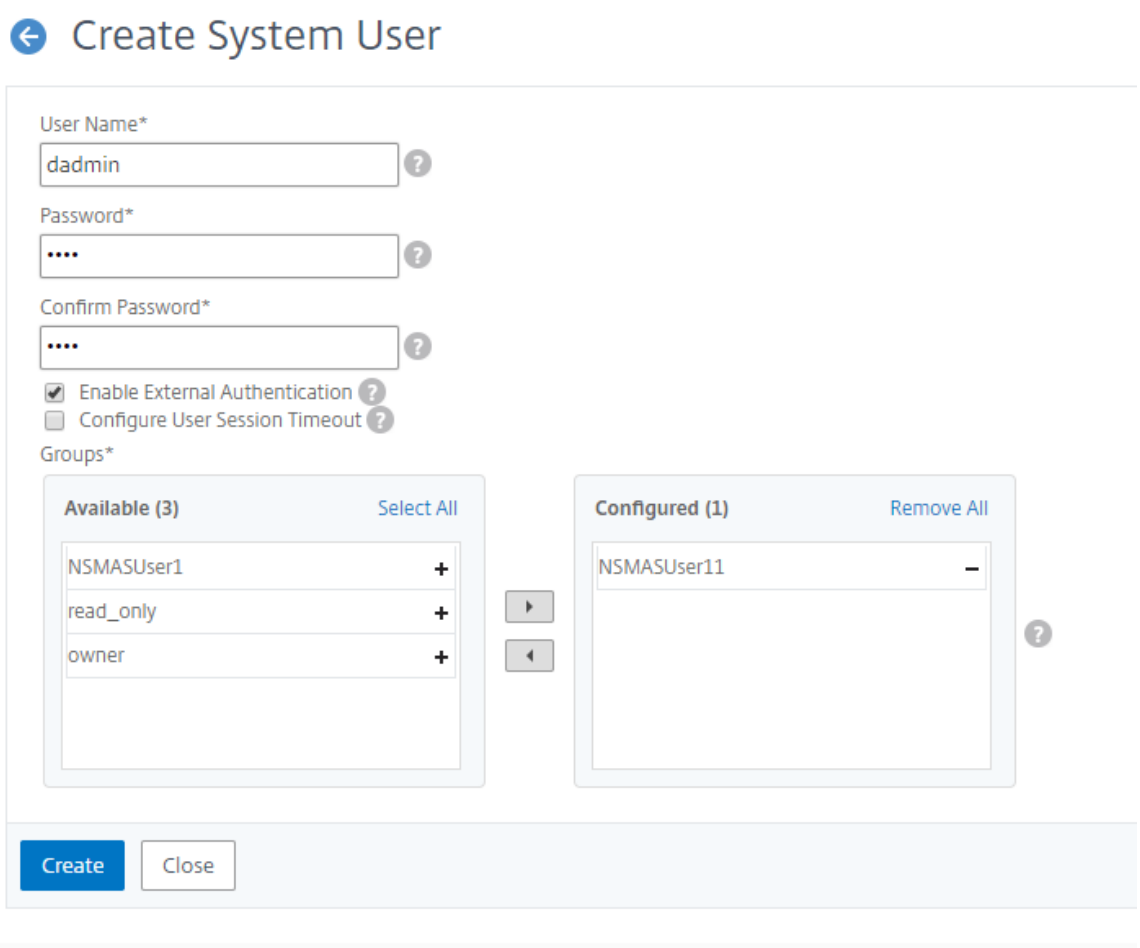
nsroot - The root user (nsroot) has full administrative privileges on the appliance. The nsroot user is the super admin of NetScaler ADM.

You can create additional users by configuring accounts for them. When you add new users to NetScaler ADM, you can define their permissions by assigning the appropriate groups, roles, and policies.

You can assign a user to a group and bind the group to roles. You can define one-to-one, one-to-many, or many-to-many relationship between users, groups, roles, and access policies. A user can be assigned to multiple groups. A group can have multiple roles, and multiple groups can have identical roles.

To configure users in NetScaler ADM:

1. In NetScaler ADM, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. Enter the following details:
    a) **User Name**. Name of the user
    b) **Password**. Password with which the user logs on to NetScaler ADM
4. Optionally, select **Enable External Authentication**, so that the user can be authenticated through an external authentication server.
5. If you have created groups and want to assign the user to a group, in the **Groups** section, move one or more groups from the **Available** list to the **Configured** list.



6. Click **Create**.

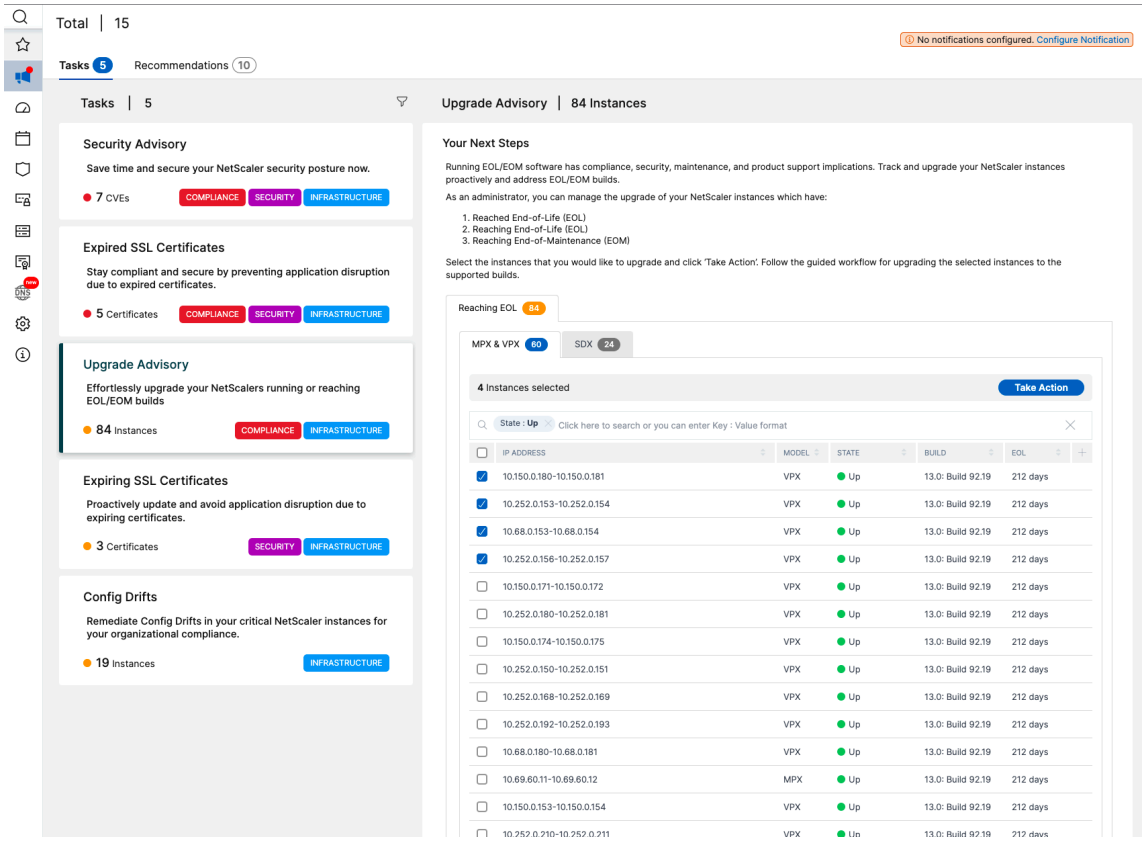
View recommendations and manage your ADCs and applications efficiently

March 11, 2024

You might have hundreds of discovered NetScaler instances and configured multiple virtual servers (applications) from each ADC instance. As an administrator, you must ensure that all the NetScaler instances and your applications are efficiently managed to get insights for better prioritizing and troubleshooting.

As you scale-up your infrastructure more, you might also need to focus on instances and apps that need immediate attention. The Tasks feature in NetScaler ADM provides recommendations based on the subscription and current utilization that:

- Help the admins to know how NetScaler ADM can provide an efficient deployment, by using the actionable Guide me workflows.
- Reduce the crucial time and effort of admins by either completing the tasks or acknowledging them to complete later.
- Ensure the admins are making use of all the capabilities of NetScaler ADM, enable product discovery and functionalities recommended by the product for efficient administration of the deployment.



In the **Set-up tasks** page, you can view the following tabs:

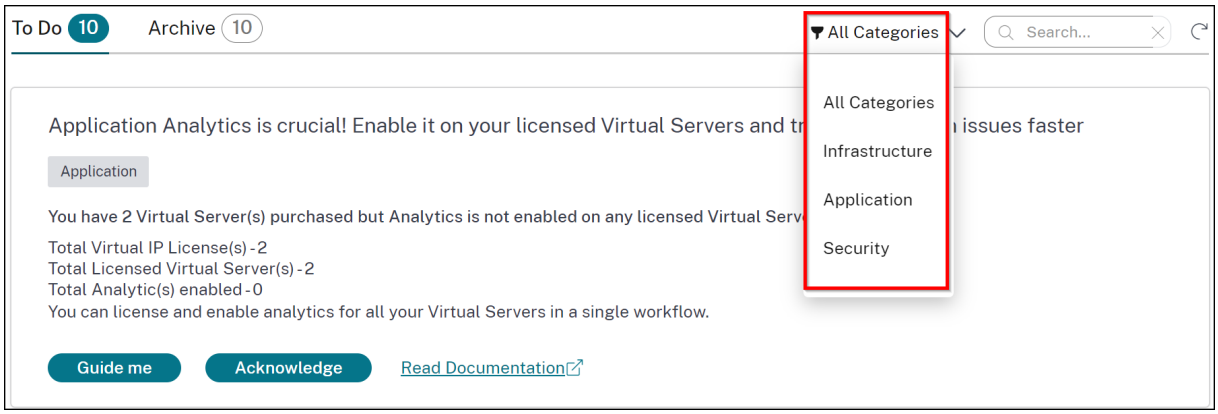
- **To Do** –Enables you to view a list of recommendations. You can review and click **Guide Me** to complete the task or click **Acknowledge** to skip this task.
- **Archive** –Enables you to view the list of all completed or acknowledged tasks. You can also use the Guide Me option to complete the recurring requirements.

The following table describes the tasks or recommendations that you can view in the NetScaler ADM GUI:

Recommendation name	When the task is visible in the GUI?
Add an ADC	After you onboard to NetScaler ADM and if no ADC instance is discovered.
Application Analytics is crucial! Enable it on your licensed Virtual Servers and triage application issues faster	If you have multiple licensed virtual servers but are not enabled with analytics.
Want to reallocate bandwidth on your ADC? It's simple!	If the pooled licenses are allocated in the ADC GUI and those ADC instances are discovered in NetScaler ADM, you can make the reallocation using NetScaler ADM.
Get more value from your Virtual IP entitlement! Enable more Virtual IP licenses on your remaining discovered Virtual Servers	If you have the required licenses, but not licensed to all the virtual servers.
Enable Granular Role based access for your key enterprise users	If role-based access control (RBAC) is not yet configured in NetScaler ADM.
Configure rules and never miss any critical events on your ADC instances	If a custom event rule is not configured yet.
Need to monitor multiple applications and their performance? Just create a Custom Application	If the custom app is not configured yet.
Avoid application outages and never miss expiring SSL certificates in an application	If no alerts or notifications configured for the expiring SSL certificates
Security Advisory - Keep your ADCs up-to-date with CVEs and mitigations	If the ADC instances have any CVE impact.
Configure an enterprise policy and monitor for any deviations	If the SSL enterprise settings are not changed or still in default.
Repeating tasks manually? Create Configuration Jobs and apply them to multiple ADCs	If **Config Job** task is not configured yet.
Manage and monitor your instance score by selecting custom indicators of your choice	If the default settings and thresholds in **Instance Score Settings** are not modified.
Track your application score by selecting custom indicators of your choice	If the App Score components in the App Dashboard are used in default and no customization is made.
Add private IP blocks to visualize client requests in the Geo Map	If IP blocks are not configured. You can create IP Blocks for mapping and visualizing client requests on a Geo Map based on their private IPs/range.
Save time! Simplify Application deployment and management with StyleBooks	If default stylebook is not yet configured.

Recommendation name	When the task is visible in the GUI?
Subscribe and export your AppSec violations to Splunk in realtime	If Splunk integration in NetScaler ADM is not yet configured.
Customize the default threshold or create a new threshold for your Kubernetes services	If only default thresholds are used in service graph and no single or double threshold is applied to the services.
Proactively configure notification profiles and get notifications in your communication destinations	If a notification profile is not yet configured.
Schedule recurring exports and get notifications on the infrastructure details	If no export schedules configured yet in **Infrastructure > Instances**.
Having ServiceNow and looking to integrate with ADM?	If ServiceNow integration in NetScaler ADM is not yet configured.

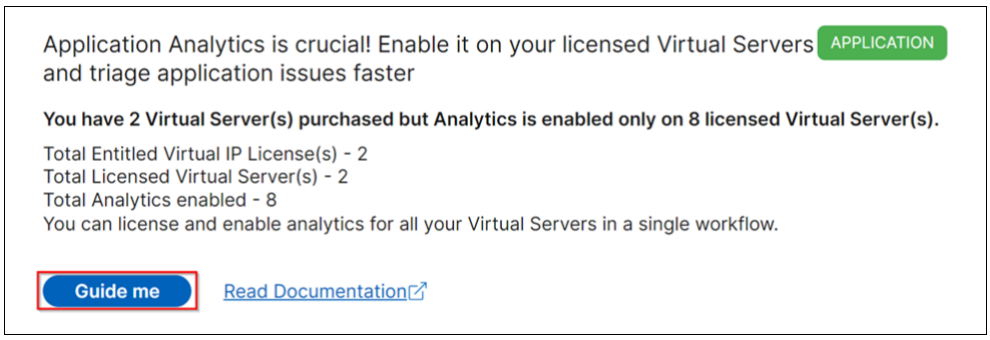
By default, you can view the top 5 recommendations. Click **Show All** to view all recommendations. You can use the category list and select a category to filter specific recommendations based on the selection.



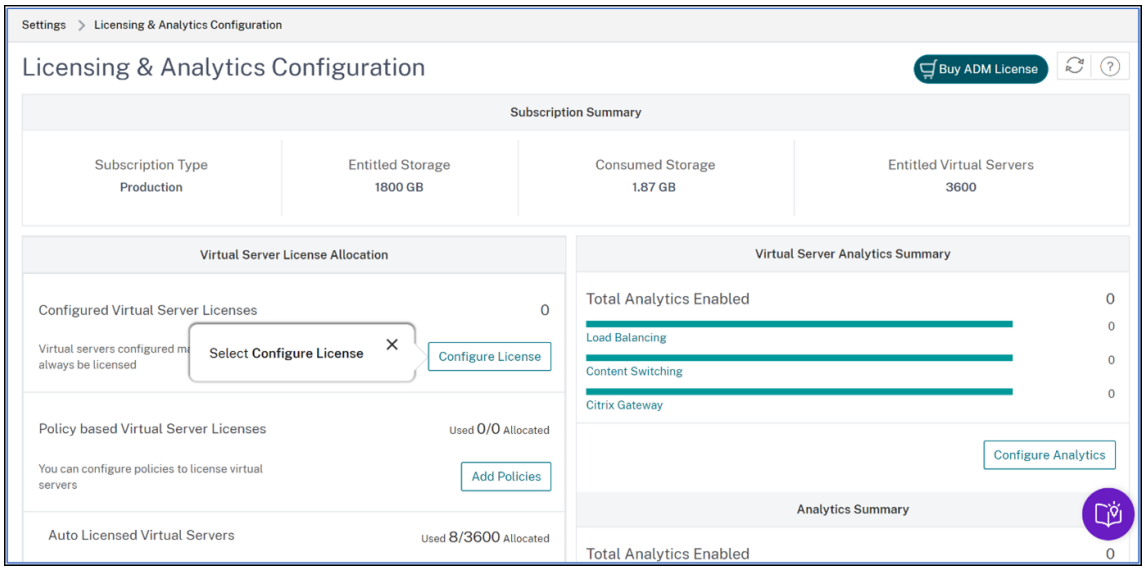
Alternatively, you can also use the Search bar, type in the first few characters to drill down to the task.

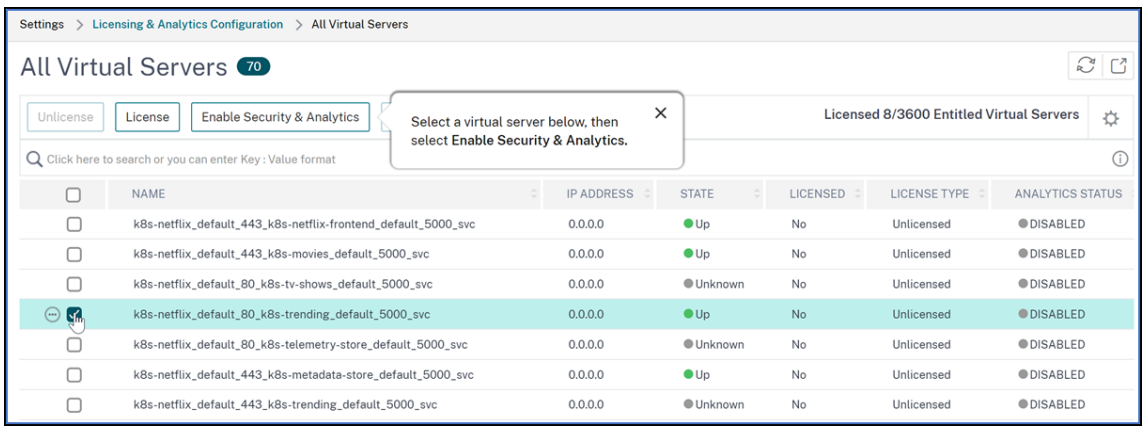
How to use the Guide me workflow and complete the task?

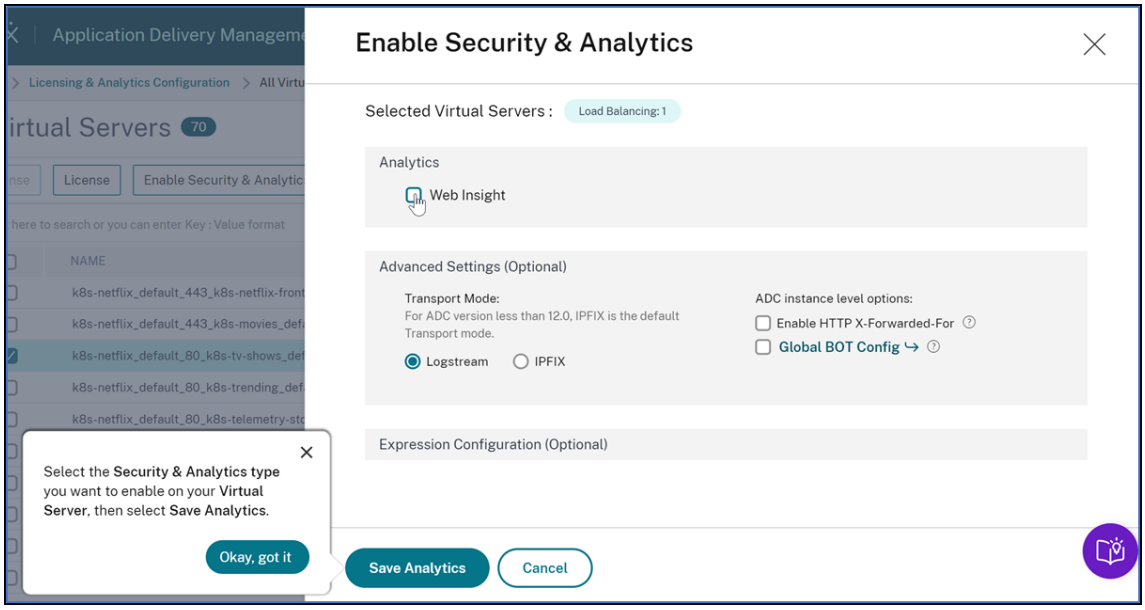
Consider that you want to enable analytics for all the licensed virtual servers. Click **Guide me** for the following task:



The workflow provides the required suggestions to complete the task. In this example, after you click **Guide me**, follow the tool-tip suggestions provided:

1. 

2. 

3. 

After you select the analytics type and click **Save Analytics**, the task is complete. This task gets moved to the **Archived** tab.

Similarly, you can also use the same workflow for the recurring requirements in the **Archive** tab.

Under **Popular Features**, you can see the important features of NetScaler ADM and it enables you to explore these features by clicking a feature.

FAQs

1. **Guide me** does not show tool-tip and only does redirection of UI? What should I do to fix this?

   This issue can happen if your firewall is blocking Pendo FQDN. Refer to Enable Pendo for your enterprise and ensure that the FQDN is allowed in the firewall. Allowing Pendo FQDN enables the **Guide me** to show tool tips. You can experience the **Guide me** workflow at its best only when Pendo is available.

2. Why type of tasks is present for the administrators?

   Currently, the recommendations are specific to deployments that help the admins more on configurations and setup tasks for making the deployment efficient. It also enables better product discovery and admins can know what a task does and how it can help without any prior knowledge or knowing if the feature exists in ADM or not.

3. Can I bring back a task from **Archive** to **To Do** ?

   Any task in archive goes back to **To Do** only based on specific conditions. For example, if the event rules are all removed or all ADCs are removed, an archived task moves to To-Do tasks for the admins again, to get their attention.

4. Does the progress bar complete if I acknowledge?

   Yes! But it is recommended to complete these tasks. However, if you want to do it later, you can acknowledge that you are aware of the product recommendation and go back to Archive to complete it later.

5. Does the task go to Archive if I start a guide me and leave it in the middle?

   No, the task continues to be available in To Do unless the action is saved or completed.

6. Can I perform search or filtering?

   Yes! You can use the search bar or narrow down to specific tasks by selecting the category from the list.

7. Will I get tasks to take actions on dynamic events like ADC memory spike, App down, LB virtual server down, and so on?

   All these are part of enhancements and are planned to be available in the upcoming releases.

8. Will this be available for on-premises ADM?

   This feature is currently available only in ADM service.

9. Will all my 20+ tasks show up even if I do not have an ADC added in NetScaler ADM?

   No. You must have both ADC instance and virtual servers available in NetScaler ADM to show all these tasks.

10. How often will the tasks refresh?

```
When you click **Tasks** from the left navigation pane, they are refreshed and available at the latest status. The details for each task are fetched and updated. The tasks are automatically refreshed every 24 hours. For better administrative control, you can also do a manual refresh of tasks to get the latest status.
```

Applications

March 11, 2024

The application analytics and management feature of NetScaler ADM enables you to monitor the applications through application-centric approach. This approach helps you to:

- Check the score and analyze the overall performance of the applications
- Check for any issues that persist with server or client
- Detect anomalies in the application traffic flows and take corrective actions

> **Note**
>
> Applications refer to one or more virtual servers that are configured on the instances (NetScaler).

You can monitor the applications for the time duration such as 1 hour, 1 day, 1 week, and 1 month.

Prerequisites

- Ensure you have added NetScaler instances in NetScaler ADM
- Ensure you have valid license for your NetScaler instances. For more information, see Licensing
- Ensure you have applied license for virtual servers. For more information, see Manage licensing on virtual servers

Application overview

Applications can be:

- Discrete applications
- Custom applications
- Microservices applications (k8s_discrete)

Discrete applications

All virtual servers that are licensed are referred to as discrete applications.

Custom applications

The virtual servers under one category are referred to as custom applications. As an administrator, you must add custom applications based on a category. You can then manage and monitor the applications through the dashboard. You get an ease of monitoring specific applications that are grouped under one category.

For example, you can create a category for your data center1 and add its ADC instances. After you define a category and add the instance for your data center1, the application dashboard is displayed with a separate category, comprising all the applications related to your data center1.

Points to note

- The discrete applications that are added to the custom applications are removed from the discrete applications.
- All applications that are not added to any category are available as **"others"**.
- By default, NetScaler ADM enables you to add licenses for up to 2 applications. Depending upon your license, you can select and apply licenses for the applications that you want to monitor.

Microservices applications

In a Kubernetes cluster, NetScaler provides an Ingress Controller for NetScaler MPX (hardware), NetScaler VPX (virtualized), and NetScaler CPX (containerized). For more information, see NetScaler Ingress Controller.

The discrete applications that are configured using the NetScaler CPX instances are referred to as microservices applications.

Web Insight dashboard

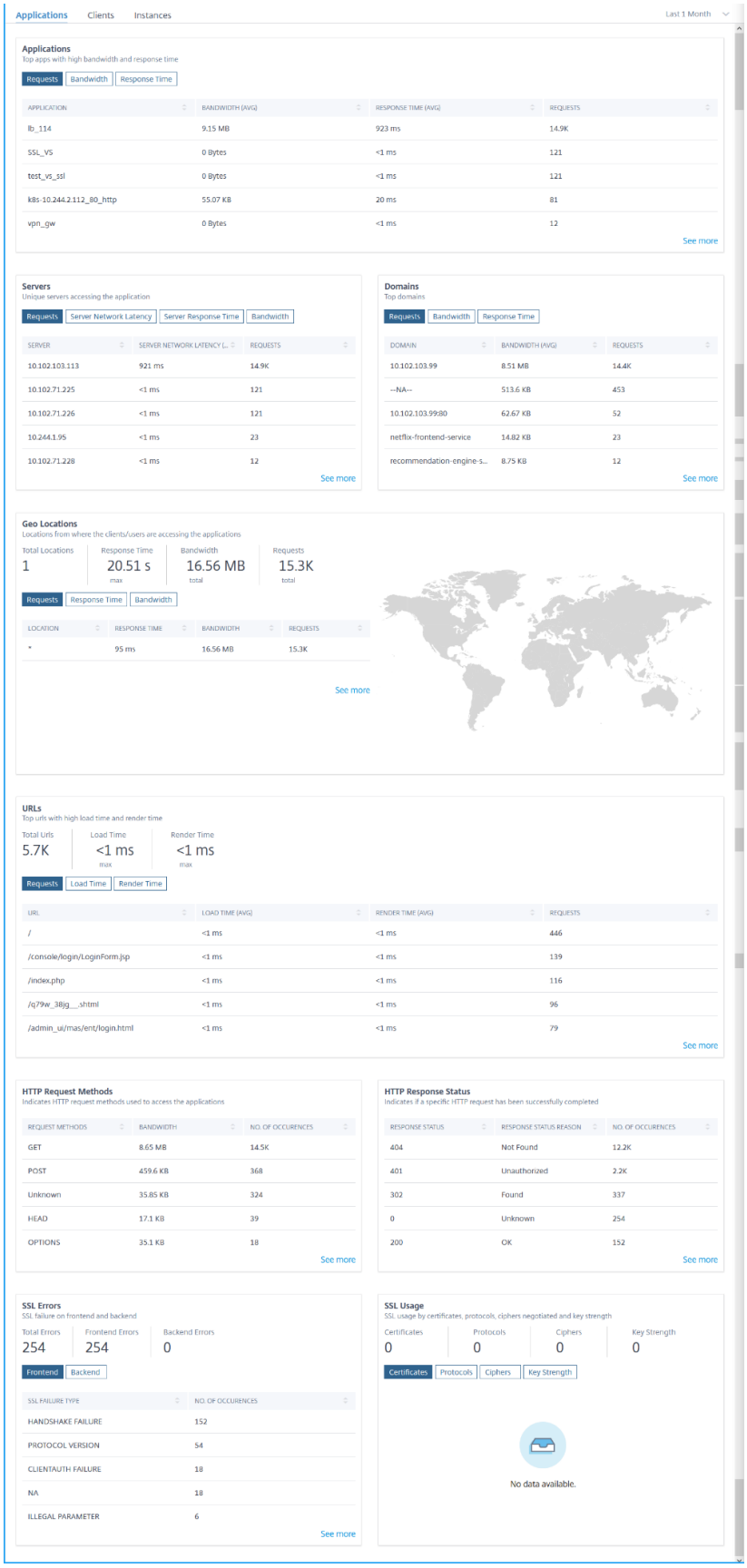
March 11, 2024

The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and NetScaler instances. This improved Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, you can view Web Insight for:

- An application. Navigate to **Applications > Dashboard**, click an application, and select **Web Insight** tab to view the detailed metrics. For more information, see Application Usage Analytics.
- All applications. Navigate to **Applications > Web Insight** and click each tab (Applications, Clients, Instances) to view the following metrics:

Applications	Clients	Instances
Applications	Clients	Instance Metrics
Servers	Geo Locations	Applications
Domains	HTTP Request Methods	Domains
Geo Locations	HTTP Response Status	URLs

Applications	Clients	Instances
URLs	URLs	HTTP Request Methods
HTTP Request Methods	Operating System	HTTP Response Status
HTTP Response Status	Browsers	Clients
SSL Errors	SSL Errors	Servers
SSL Usage	SSL Usage	Operating System
		Browsers

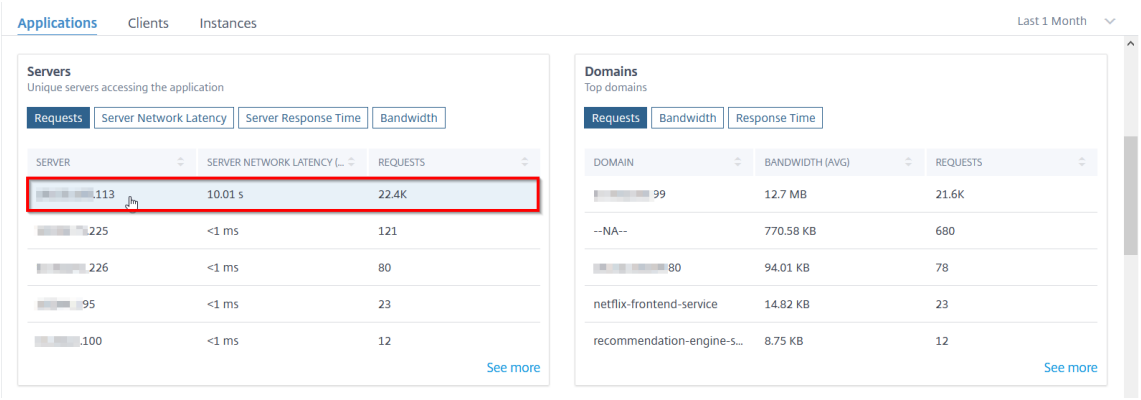


In each metric, you can view the top 5 results. You can click to drill down further to analyze the issue and take troubleshooting actions faster.

> Note
>
> In some scenarios, NetScaler might not be able to calculate the RTT values for some transactions. For such transactions, NetScaler ADM displays the RTT values as
>
> - **NA** –Displays when the ADC instance cannot calculate the RTT.
> - **< 1ms** –Displays when the ADC instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

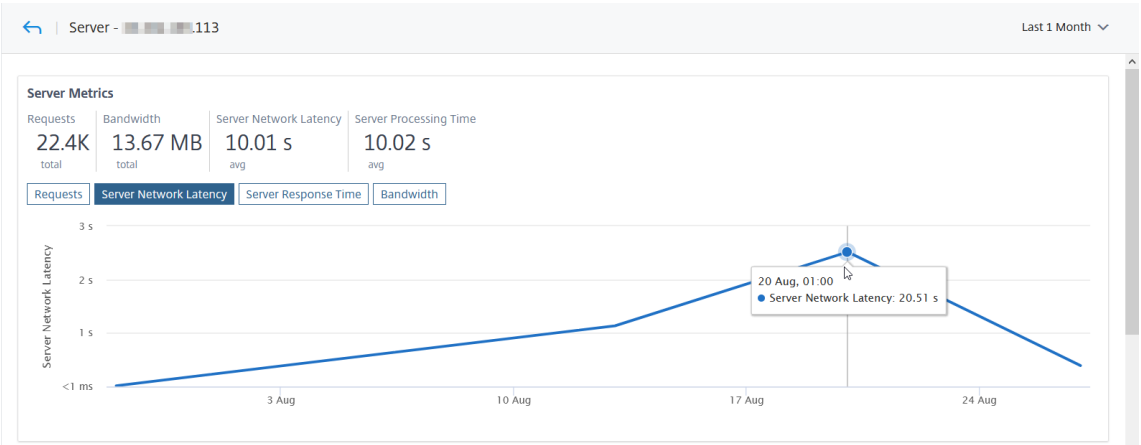
For example, consider that you want to analyze the server network latency for 1-month time duration and take decision whether to scale up or scale down the production environment. To analyze this:

1. Select Last 1 Month from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.



   The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.



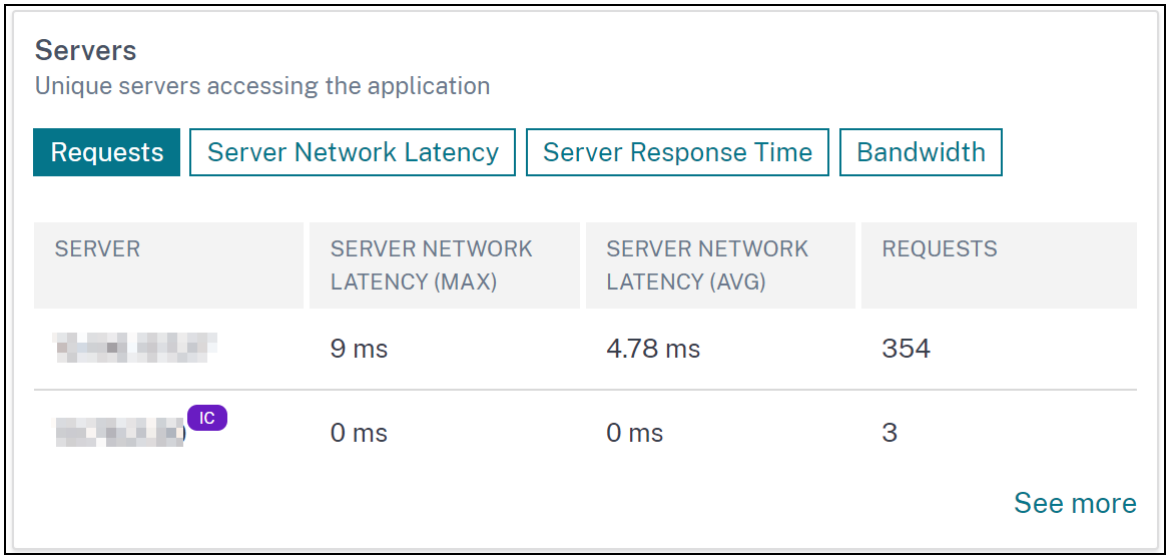
   The average latency indicates 10.01 s and from the graph, you can analyze that the server network latency for the last 1 month seems to be high. As an administrator, you can take decision

to scale up the production environment.

Integrated cache requests

The integrated cache provides in-memory storage on the NetScaler appliance and serves Web content to users without requiring a round trip to an origin server.

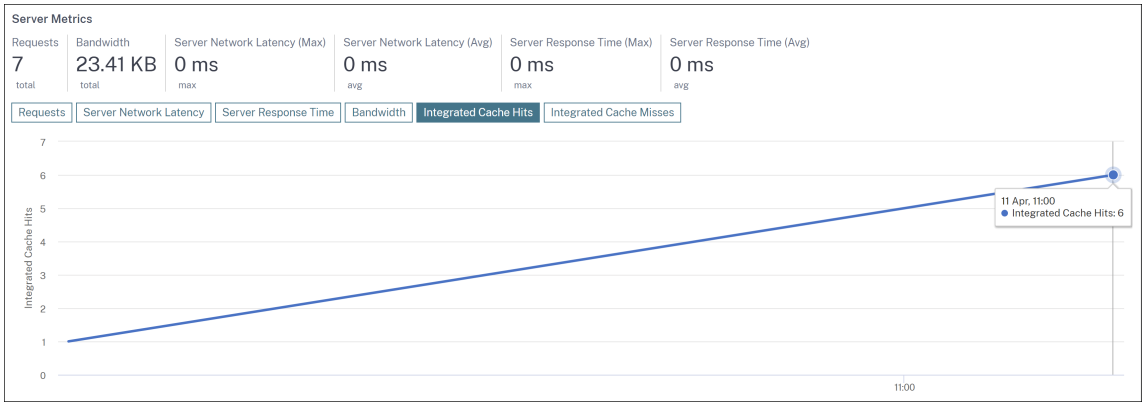
The integration cache requests are currently visible under **Servers** with an IC notification next to the ADC virtual server IP address. All other requests are visible with the origin server IP address.



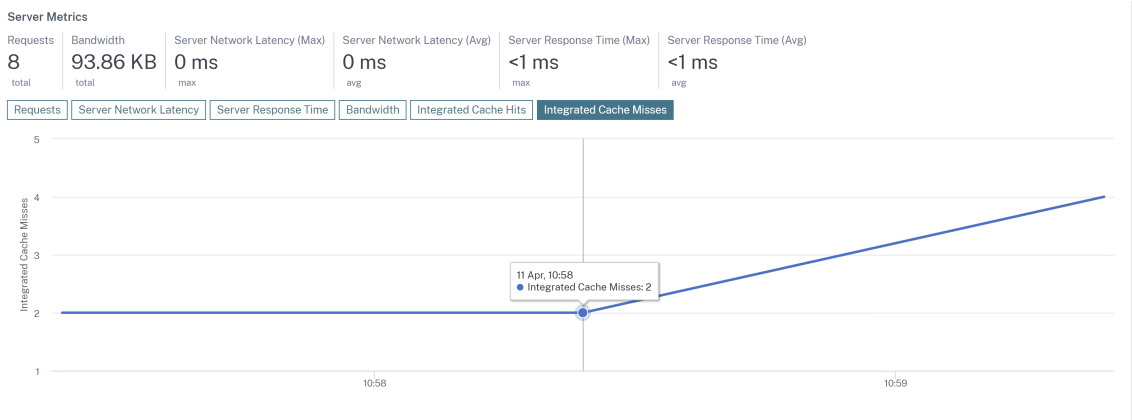
When you drill down a server to view more details, the **Server Metrics** display integrated cache hits and misses tabs.

The graph view in:

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.



- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.



Troubleshoot Web Insight issues

For details, see the troubleshooting document Troubleshoot Web Insight issues.

Service Graph

March 11, 2024

The service graph feature in NetScaler ADM enables you to monitor all services in a graphical representation. This feature also enables you to view a detailed analysis and actionable metrics of the services. You can view service graph for:

- Applications configured across all NetScaler instances
- Kubernetes applications
- 3-tier Web applications

Service graph for applications across all NetScaler instances

The global service graph feature enables you to get a holistic visualization of the `clients to infrastructure to application` view. From this single-pane service graph view, as an administrator, you can:

- Understand from which region the users are accessing the specific applications (3-tier Web apps and microservices app)
- Visualize the infrastructure (NetScaler instance) view that the client request is processed
- Understand if the issues are occurring from the client, infrastructure, or application
- Further drill down to troubleshoot the issue

Navigate to **Applications > Service Graph** and click the **Global** tab to view:

- End-to-end details of all applications connected from client to back-end servers
- All NetScaler instances that are connected to its respective data centers

  > **Note**
  >
  > You can view data centers only if you have GSLB apps.

- The client metrics information
- The NetScaler metrics information
- All NetScaler instances that have discrete applications, custom applications, and discrete microservice applications
- The top 4 low-scored applications that belong to custom apps, discrete apps, and microservices apps
- The metrics information for the top 4 low-scored virtual servers
- The applications (discrete apps, custom apps, and microservices apps) status such as **Critical**, **Review**, **Good**, and **Not Applicable**.

For more information, see Holistic view of applications in service graph.

Service graph for Kubernetes applications

Navigate to **Applications > Service Graph** and click the **Microservices** tab to view:

- Ensure end-to-end application overall performance
- Identify bottlenecks created by inter-dependency of different components of your applications
- Gather insights into the dependencies of different components of your applications
- Monitor services within the Kubernetes cluster
- Monitor which service has issues
- Check the factors contributing to performance issues
- View detailed visibility of service HTTP transactions
- Analyze the HTTP, TCP, and SSL metrics

By visualizing these metrics in NetScaler ADM, you can analyze the root cause of issues and take necessary troubleshooting actions faster. Service graph displays your applications into various component services. These services running inside the Kubernetes cluster can communicate with various components within and outside the application. To get started, see Setting up service graph.

Service graph for 3-tier Web applications

Navigate to **Applications > Service Graph** and click the **Web Apps** tab to view:

- Details on how the application is configured (with content switching virtual server and load balancing virtual server)

  For GSLB applications, you can view data center, ADC instance, CS, and LB virtual servers.
- End-to-end transactions from client to service
- The location from where the client is accessing the application
- The data center name where the client requests are processed and the associated data center NetScaler metrics (only for GSLB applications)
- Metrics details for client, service, and virtual servers
- If the errors are from the client or from the service
- The service status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the service status based on service response time and error count.
  - **Critical (red)** - Indicates when average service response time > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average service response time > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average service response time < 200 ms
- The client status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the client status based on client network latency and error count.
  - **Critical (red)**- Indicates when average client network latency > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average client network latency > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average client network latency < 200 ms
- The virtual server status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the virtual server status based on the app score.
  - **Critical (red)** - Indicates when app score < 40
  - **Review (orange)** - Indicates when app score is between 40 and 75
  - **Good (green)** - Indicates when app score is > 75

Points to note:

- Only Load Balancing, Content Switching, GSLB virtual servers are displayed in service graph.
- If no virtual server is bound to a custom application, the details are not visible in service graph for the application.
- You can view metrics for clients and services in service graph only if active transactions occur between virtual servers and web application.
- If no active transactions available between virtual servers and web application, you can only view details in service graph based on the configuration data such as load balancing, content switching, GSLB virtual servers, and services.
- If any changes made in the application configuration, it may take 10 minutes to reflect in service graph.

For more information, see Service graph for applications.

StyleBooks

March 11, 2024

StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations. You can create a StyleBook for configuring a specific feature of NetScaler, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Lync.

StyleBooks fit in well with the principles of Infrastructure-as-code that is practiced by DevOps teams, where configurations are declarative and version-controlled. The configurations are also repeated and are deployed as a whole. StyleBooks offer the following advantages:

- **Declarative**: StyleBooks are written in a declarative rather than imperative syntax. Stylebooks allow you to focus on describing the outcome or the "desired state"of the configuration rather than the step-by-step instructions on how to achieve it on a particular NetScaler instance. NetScaler Application Delivery Management (ADM) computes the diff between existing state on a NetScaler and the desired state you specified, and makes the necessary edits to the infrastructure. Because StyleBooks use a declarative syntax, written in YAML, components of a StyleBook can be specified in any order, and NetScaler ADM determines the correct order based on their computed dependencies.
- **Atomic**: When you use StyleBooks to deploy configurations, the full configuration is deployed or none of it is deployed and this ensures that the infrastructure is always left in a consistent state.

- **Versioned**: A StyleBook has a name, namespace, and a version number that uniquely distinguishes it from any other StyleBook in the system. Any modification to a StyleBook requires an update to its version number (or to its name or namespace) to maintain this unique character. The version update also allows you to maintain multiple versions of the same StyleBook.
- **Composable**: After a StyleBook is defined, the StyleBook can be used as a unit to build other StyleBooks. You can avoid repeating common patterns of configuration. It also allows you to establish standard building blocks in your organization. Because StyleBooks are versioned, changes to existing StyleBooks results in new StyleBooks, therefore ensuring that dependent StyleBooks are never unintentionally broken.
- **App-Centric**: StyleBooks can be used to define the NetScaler configuration of a full application. The configuration of the application can be abstracted by using parameters. Therefore, users who create configurations from a StyleBook can interact with a simple interface consisting of filling a few parameters to create what can be a complex NetScaler configuration. Configurations that are created from StyleBooks are not tied to the infrastructure. A single configuration can thus be deployed on one or multiple NetScalers, and can also be moved among instances.
- **Auto-Generated UI**: NetScaler ADM auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the NetScaler ADM GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.
- **API-driven**: All configuration operations are supported by using the NetScaler ADM GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

You can use one StyleBook to create multiple configurations. Each configuration is saved as a config pack. For example, consider that you have a StyleBook that defines a typical HTTP load balancing application configuration. You can create a configuration with values for the load balancing entities and execute it on a NetScaler instance. This configuration is saved as a config pack. You can use the same StyleBook to create another configuration with different values and execute it on the same or a different NetScaler instance. A new config pack is created for this configuration. A config pack is saved both on NetScaler ADM and on the NetScaler instance on which the configuration is executed.

You can either use default StyleBooks, shipped with NetScaler ADM, to create configurations for your deployment, or design your own StyleBooks and import them to NetScaler ADM. You can use the StyleBooks to create configurations either by using the NetScaler ADM GUI or by using APIs.

This document includes the following information:

- How to view StyleBooks
- Default StyleBooks
- Stylebooks developed for business applications

- Custom StyleBooks
- APIs in StyleBooks
- StyleBooks grammar

Application Security Dashboard

March 11, 2024

The **App Security** dashboard provides you the overview of security metrics for the discovered/licensed applications. This dashboard displays the security attack information for the discovered/licensed applications, such as sync attacks, small window attacks, DNS flood attacks, and so on.

To view the security metrics on app security dashboard:

1. Navigate to **Security** > **Security Dashboard**.
2. Select the instance IP address from the Instance list.

   The reports include the following information for each application:

   - **Threat index**. A single-digit rating system that indicates the criticality of attacks on the application. The more critical the attacks on an application, the higher the threat index for that application. The values range from 1 through 7.

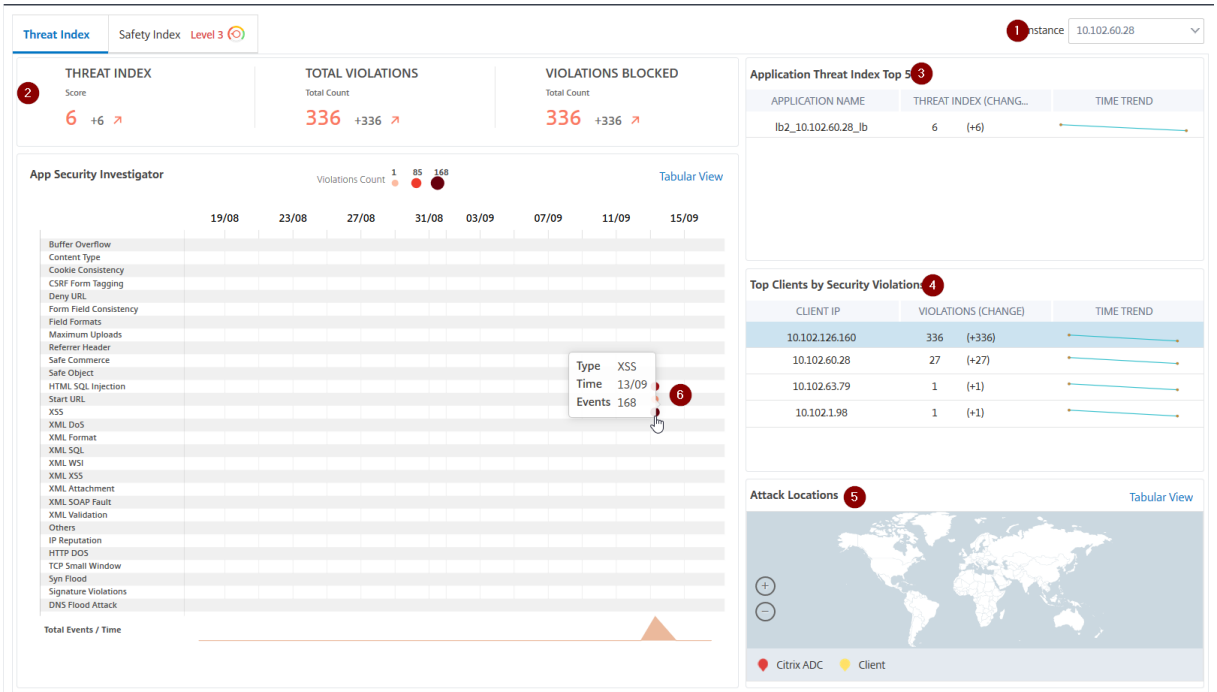
     The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives an insight into the attacks on the application. Violation information is sent to NetScaler ADM only when a violation or attack occurs. A large number of breaches and vulnerabilities lead to a high threat index value.

   - **Safety index**. A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. The values range from 1 through 7.

     The safety index considers both the application firewall configuration and the NetScaler system security configuration. For a high safety index value, both configurations must be strong. For example, if rigorous application firewall checks are in place, but NetScaler system security measures, such as a strong password for the `nsroot` user is not provided, then applications are assigned a low safety index value.

You can view the discrepancies reported on the **App Security Investigator**.

Threat index details



1 - Displays the NetScaler instance IP address for which you can view details.

2 - Displays details such as threat index score, total violations occurred, and total violations blocked.

3 - Displays the virtual server of the selected instance.

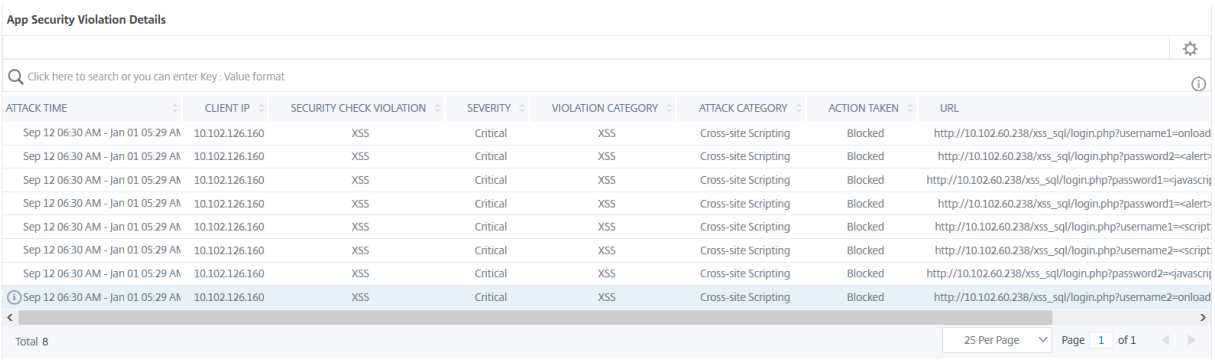
4 - Displays the security violations based on clients. The App Security Investigator graph is displayed for each client. You can click each client IP to view the results.

5 - Displays the violations in map view and tabular view.

6 - Displays the violation details. When you hover the mouse pointer on the graph, the details such as violation type, time of the attack, and total events are displayed.

When you click a bubble graph, the details are displayed in the **App Security Violation Details** page. For example, if you want to further view details for cross-site scripting (cross-site script) violation, click the graph populated for **XSS** in **App Security Investigator**.

The **App Security Violation Details** is displayed with violation details such as attack time, attack category, severity, URL, and so on.



You can also click the **Settings** option to select the options that you want to get it displayed.

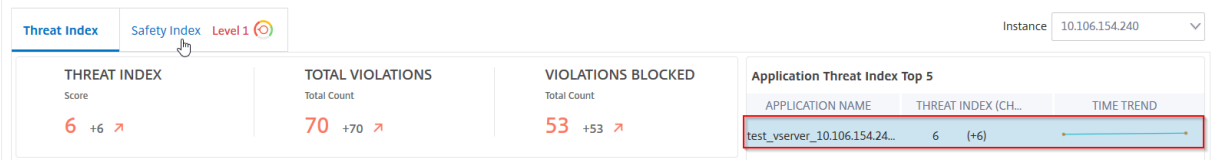
Safety index details

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application safety index summary.

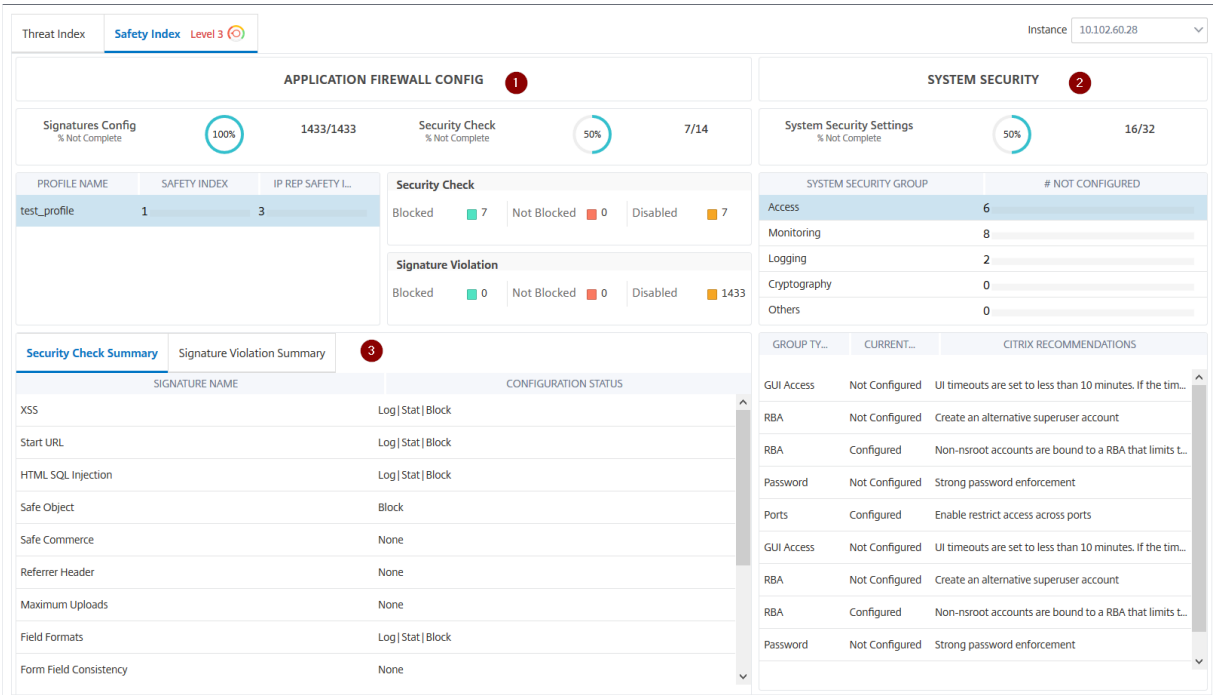
The safety index summary gives you information about the effectiveness of the following security configurations:

- **Application Firewall Configuration**. Shows how many signature and security entities are not configured.
- **NetScaler ADM System Security**. Shows how many system security settings are not configured.

To view the **Safety Index** details, select a virtual server/application and click the **Safety Index** tab.



The details are displayed.



1 - Displays the detailed information for Application Firewall configurations.

2 - Displays the detailed information for System Security. Click each security group to get details on current status and Citrix recommendations.

3 - Displays the summary for Security Check and Signature Violation.

You can also view summary of the threat environment by enabling the **WAF Security Violations** for virtual servers and then navigating to **Security** > **Security Violations**.

View application security violation details

March 11, 2024

Web applications that are exposed to the internet have become vulnerable to attacks drastically. NetScaler ADM enables you to visualize actionable violation details to protect applications from attacks. Navigate to **Security** > **Security Violations** for a single-pane solution to:

- Visualize applications with full visibility into the threat details associated in both WAF Security Violations and Bot Security Violations
- Access the application security violations based on its categories such as **Network**, **Bot**, and **WAF**
- Take corrective actions to secure the applications

The **Security Violations** page has the following options:

- **Application Overview** –Displays an overview with applications that have total violations, total WAF and Bot violations, violation by country, and so on. For more information, see Application overview.
- **All Violations** –Displays the application security violation details. For more information, see All violations.

Prerequisite

Ensure if **Metrics Collector** is enabled. By default, **Metrics Collector** is enabled on the NetScaler instance. For more information, see Configure Intelligent App Analytics.

Integration with Splunk

March 11, 2024

You can now integrate NetScaler ADM with Splunk to view analytics for:

- WAF violations
- Bot violations
- SSL Certificate Insights

Splunk add-on enables you to:

- Combine all other external data sources.
- Provide greater visibility of analytics in a centralized place.

NetScaler ADM collects Bot, WAF, SSL events, and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an administrator, using the CIM compatible data, you can view the events in the Splunk dashboard.

For a successful integration, you must:

- Configure Splunk to receive data from NetScaler ADM
- Configure NetScaler ADM to export data to Splunk
- View dashboards in Splunk

Configure Splunk to receive data from NetScaler ADM

In Splunk, you must:

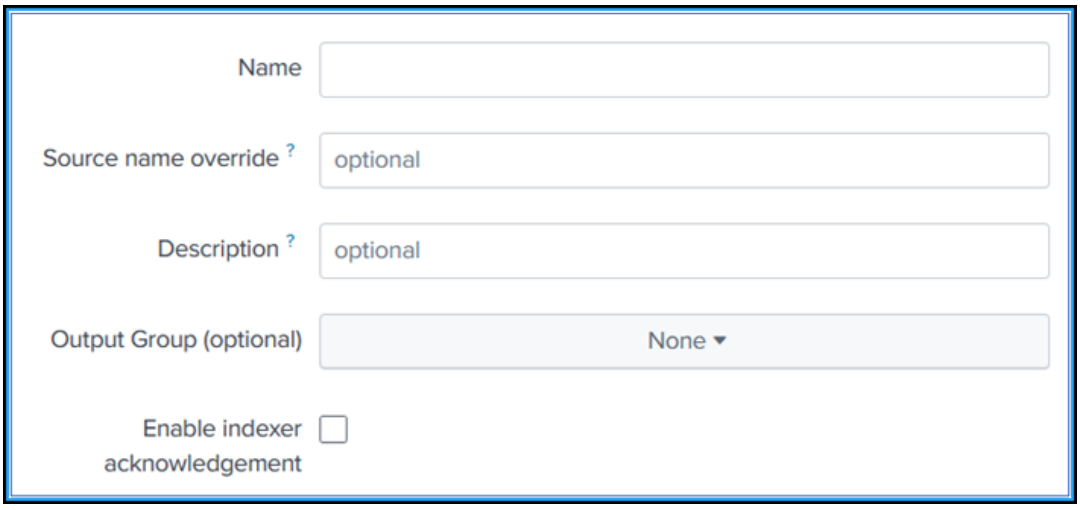
1. Setup the Splunk HTTP event collector endpoint and generate a token
2. Install the Splunk Common Information Model (CIM) add-on
3. Prepare a sample dashboard in Splunk

Setup the Splunk HTTP event collector endpoint and generate a token

You must first setup the HTTP event collector in Splunk. This setup enables the integration between the ADM and Splunk to send the data. Next, you must generate a token in Splunk to:

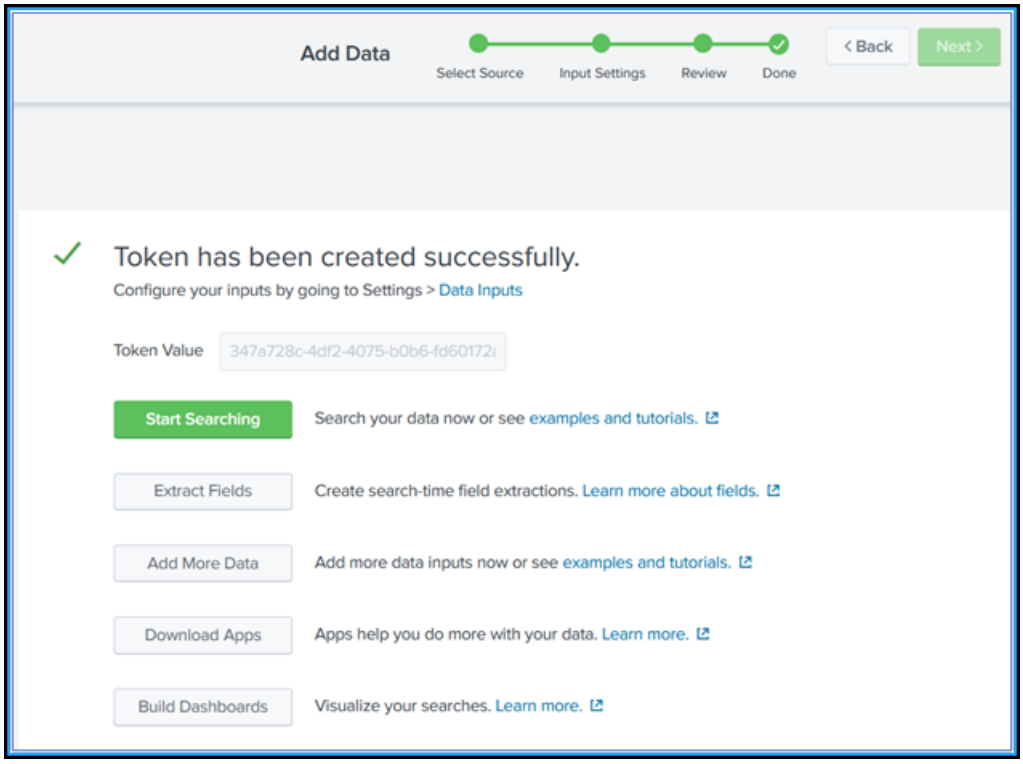
- Enable authentication between ADM and Splunk.
- Receive data through the event collector endpoint.

1. Log on to Splunk.
2. Navigate to **Settings > Data Inputs > HTTP event collector** and click **Add new**.
3. Specify the following parameters:
    a) **Name**: Specify a name of your choice.
    b) **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector.
    c) **Description (optional)**: Specify a description.
    d) **Output Group (optional)**: By default, this option is selected as None.
    e) **Enable indexer acknowledgement**: By default, this option is not selected.



4. Click **Next**.
5. Optionally, you can set additional input parameters in the **Input Settings** page.
6. Click **Review** to verify the entries and then click **Submit**.

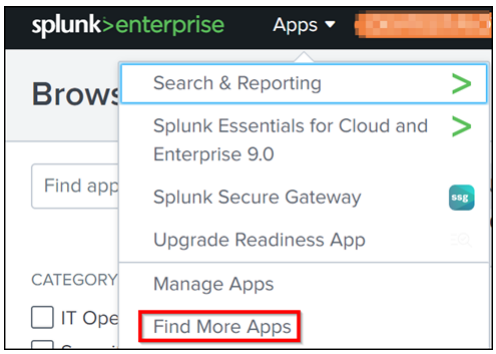
   A token gets generated. You must use this token when you add details in NetScaler ADM.



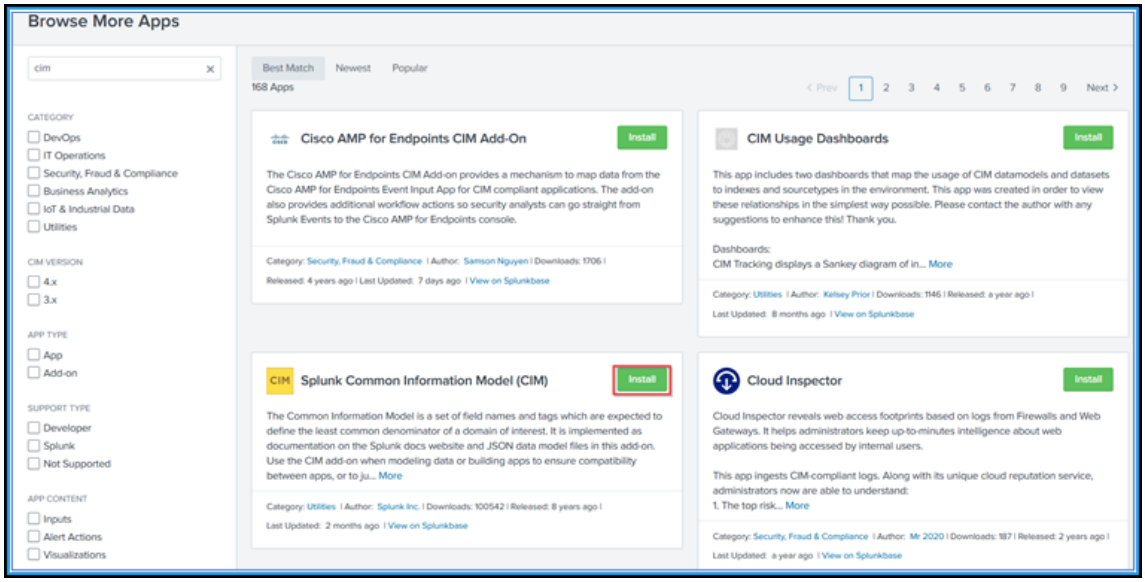
Install the Splunk Common Information Model

In Splunk, you must install the Splunk CIM add-on. This add-on ensures that the data received from NetScaler ADM to normalize the ingested data and match a common standard using the same field names and event tags for equivalent events.

1. Log on to Splunk.
2. Navigate to **Apps > Find More Apps**.



3. Type **CIM** in the search bar and press **Enter** to get the **Splunk Common Information Model (CIM)** add-on, and click **Install**.



Prepare a sample dashboard in Splunk

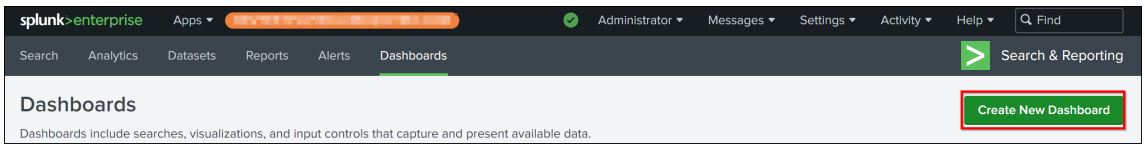
After you install the Splunk CIM, you must prepare a sample dashboard using a template for WAF and Bot, and SSL Certificate Insights. You can download the dashboard template (`.tgz`) file, use any editor (for example, notepad) to copy its contents, and create a dashboard by pasting the data in Splunk.

> **Note:**
>
> The following procedure to create a sample dashboard is applicable for both WAF and Bot, and SSL Certificate Insights. You must use the required `json` file.

1. Log on to Citrix downloads page and download the sample dashboard available under Observability Integration.
2. Extract the file, open the `json` file using any editor, and copy the data from the file.

> **Note:**
>
> After you extract, you get two `json` files. Use `adm_splunk_security_violations.json` to create the WAF and Bot sample dashboard, and use `adm_splunk_ssl_certificate.json` to create the SSL certificate insight sample dashboard.

3. In the Splunk portal, navigate to **Search & Reporting > Dashboards** and then click **Create New Dashboard**.



4. In the **Create New Dashboard** page, specify the following parameters:

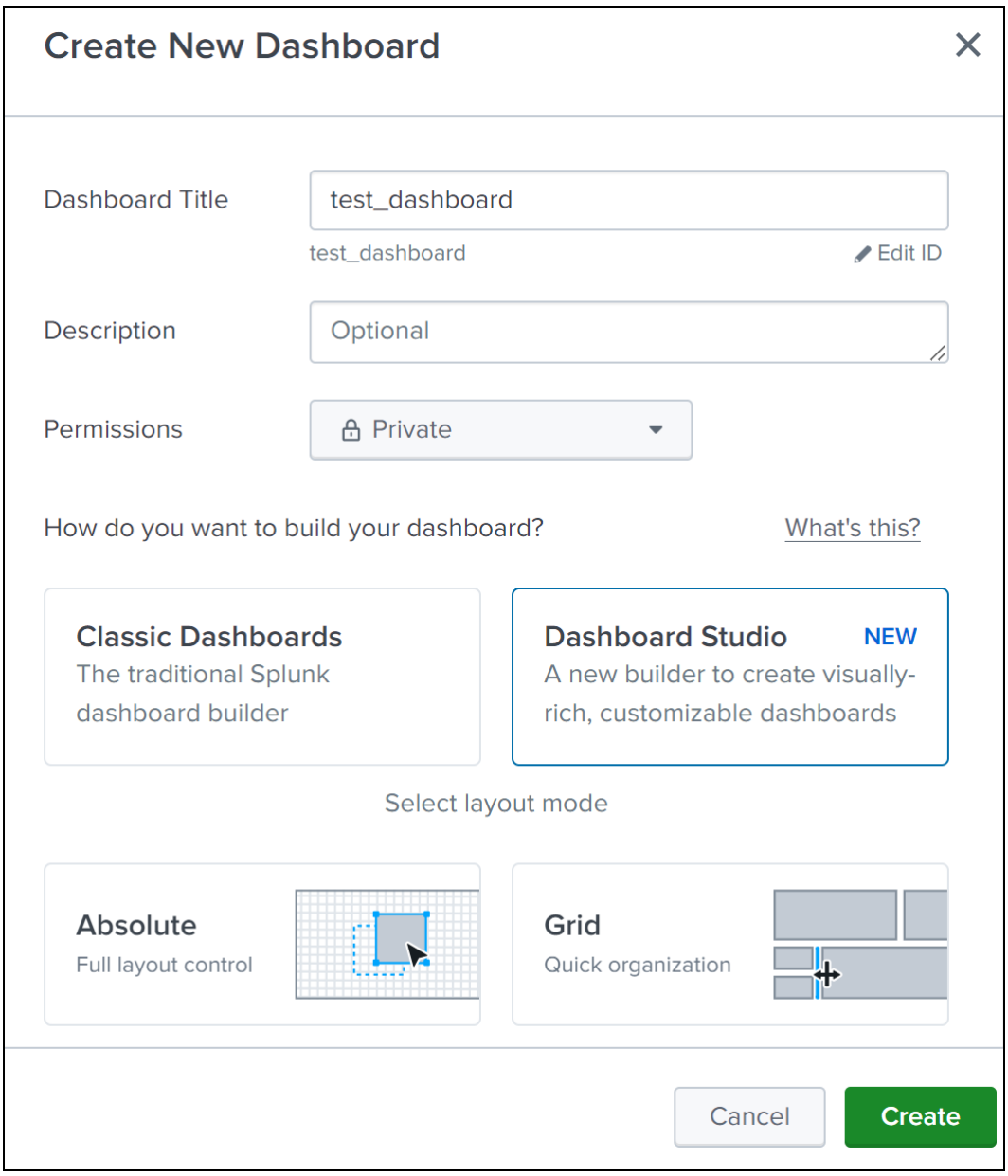
   a) **Dashboard Title** - Provide a title of your choice.

   b) **Description** - Optionally, you can provide a description for your reference.

   c) **Permission** - Select **Private** or **Shared in App** based on your requirement.

   d) Select **Dashboard Studio**.

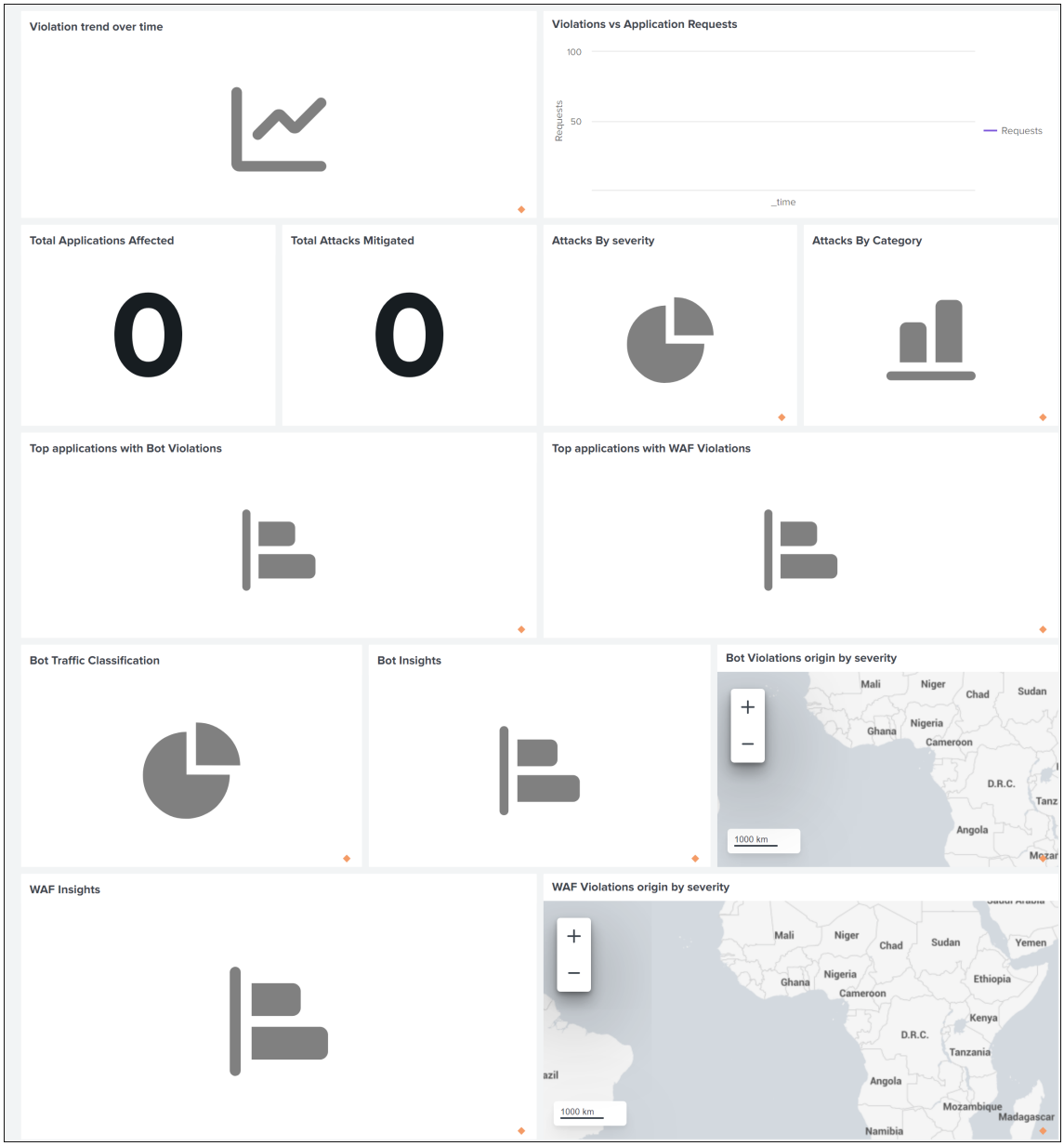
   e) Select any one layout (**Absolute** or **Grid**), and then click **Create**.



After you click **Create**, select the **Source** icon from the layout.

5. Delete the existing data, paste the data that you copied in step 2, and click **Back**.
6. Click **Save**.

   You can view the following sample dashboard in your Splunk.



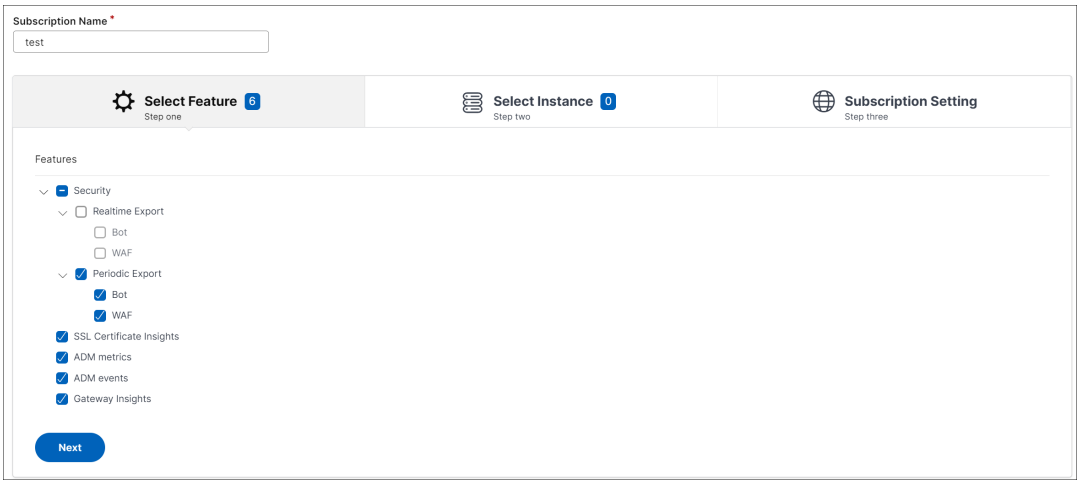
Configure NetScaler ADM to export data to Splunk

You now have everything ready in Splunk. The final step is to configure NetScaler ADM by creating a subscription and adding the token.

Upon completion of the following procedure, you can view the updated dashboard in Splunk that is currently available in your NetScaler ADM:

1. Log on to NetScaler ADM.
2. Navigate to **Settings > Ecosystem Integration**.

3. In the **Subscriptions** page, click **Add**.
4. In the **Select features to subscribe** tab, select the features that you want to export and click **Next**.
   - **Realtime Export** - The selected violations are exported to Splunk immediately.
   - **Periodic Export** - The selected violations are exported to Splunk based on the duration you select.

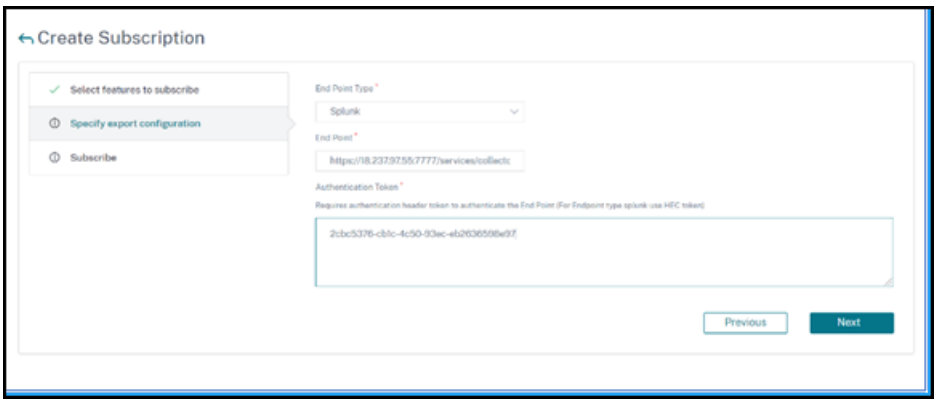


5. In the **Specify export configuration** tab:
   a) **End Point Type** –Select **Splunk** from the list.
   b) **End Point** –Specify the Splunk end point details. The end point must be in the https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event format.

      > **Note**
      >
      > It is recommended to use HTTPS for security reasons.

      - **SPLUNK_PUBLIC_IP** –A valid IP address configured for Splunk.
      - **SPLUNK_HEC_PORT** –Denotes the port number that you have specified during the HTTP event endpoint configuration. The default port number is 8088.
      - **Services/collector/event** –Denotes the path for the HEC application.

   c) **Authentication token** –Copy and paste the authentication token from the Splunk page.
   d) Click **Next**.



6. In the **Subscribe** page:

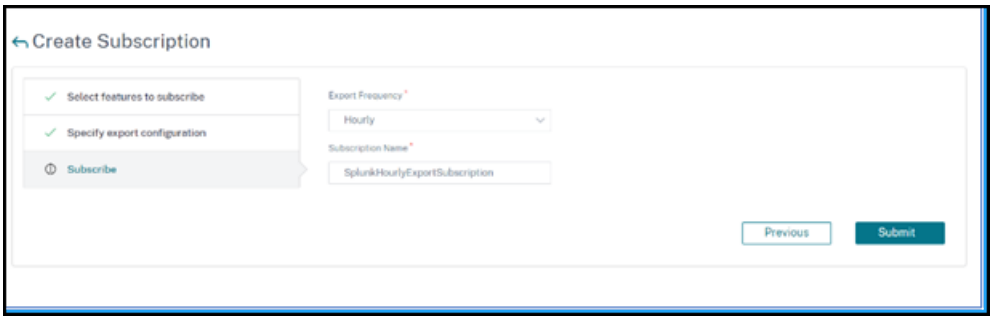
   a) **Export Frequency** –Select Daily or Hourly from the list. Based on the selection, NetScaler ADM exports the details to Splunk.

   > **Note:**
   >
   > Applicable only if you have selected violations in **Periodic Export**.

   b) **Subscription Name** –Specify a name of your choice.

   c) Select the **Enable Notifications** check box.

   d) Click **Submit**.



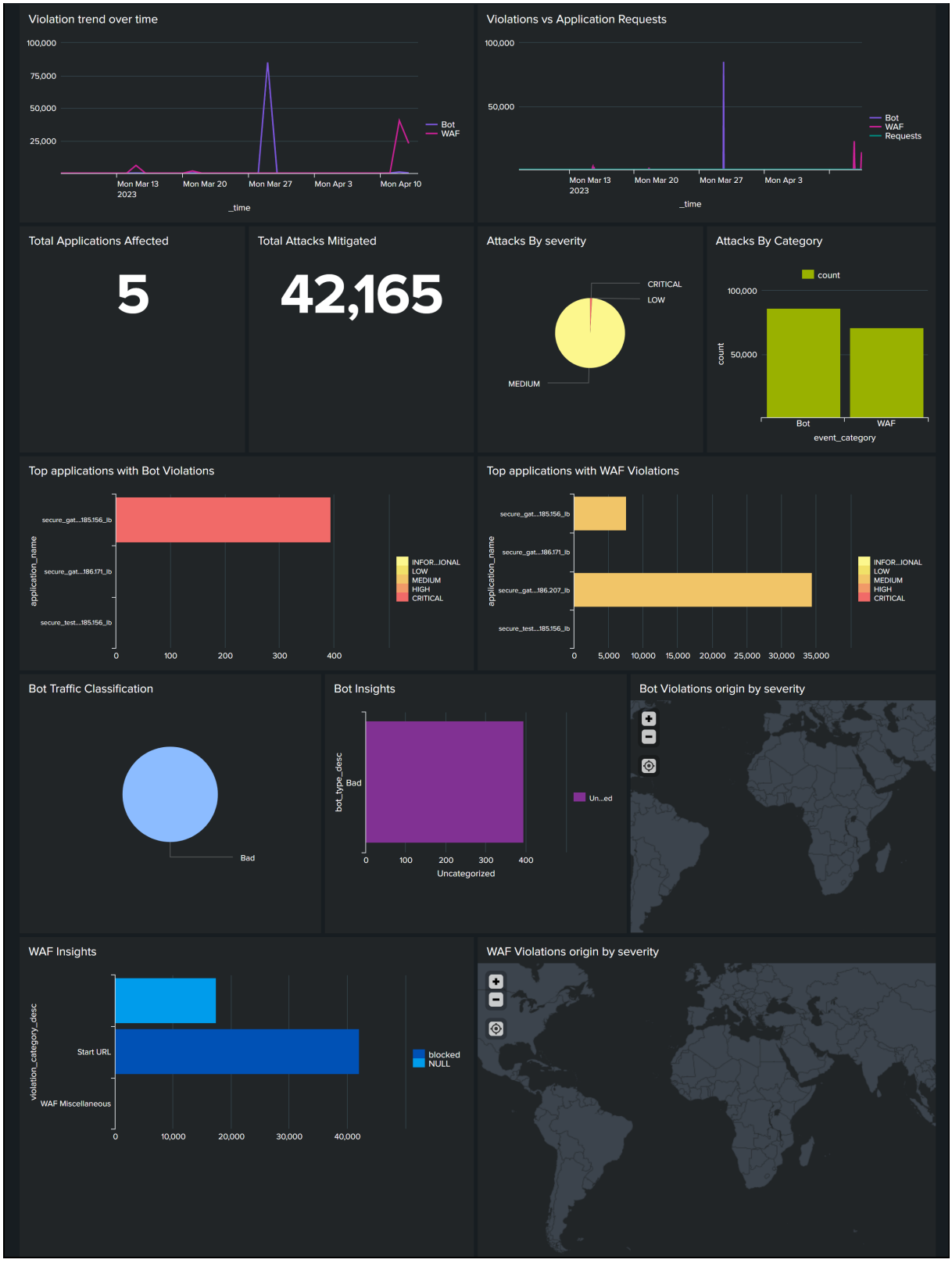
> **Note**
>
> - When you configure with **Periodic Export** option for the first time, the selected features data get pushed to Splunk immediately. The next export frequency happens based on your selection (daily or hourly).
> - When you configure with **Realtime Export** option for the first time, the selected features data pushed to Splunk immediately when the violations are detected in NetScaler ADM.

View dashboards in Splunk

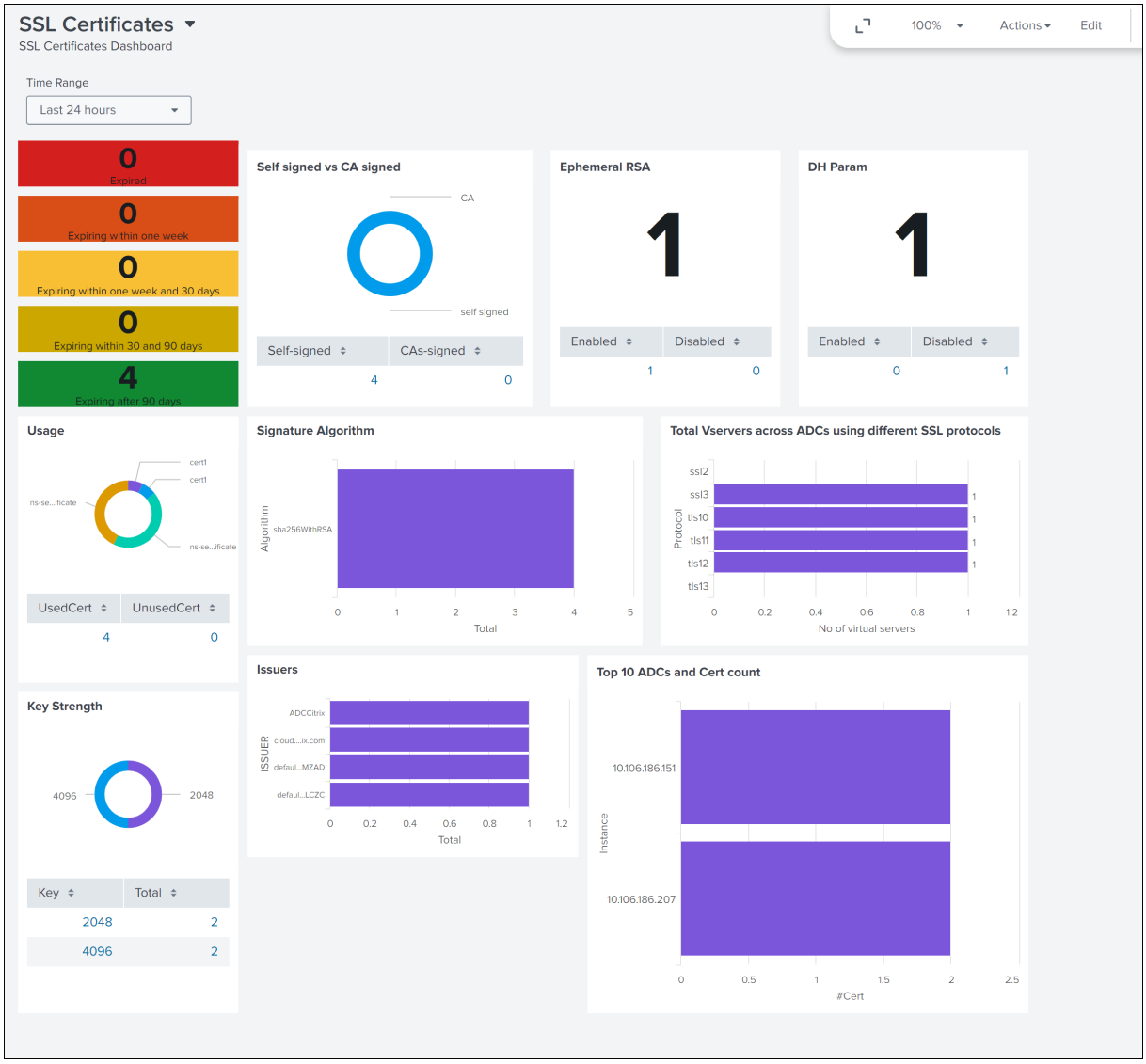
After you complete the configuration in NetScaler ADM, the events appear in Splunk. You are all set to view the updated dashboard in Splunk without any additional steps.

Go to Splunk and click the dashboard that you have created to view the updated dashboard.

The following is an example for the updated WAF and Bot dashboard:



The following dashboard is an example for the updated SSL Certificate Insights dashboard.



Integration with New Relic

March 11, 2024

You can now integrate NetScaler ADM with New Relic to view analytics for WAF and Bot violations in your New Relic dashboard. With this integration, you can:

- Combine all other external data sources in your New Relic dashboard.
- Get visibility of analytics in a centralized place.

NetScaler ADM collects Bot and WAF events, and sends them to New Relic either in real time or periodically based on your choice. As an administrator, you can also view the Bot and WAF events in your

New Relic dashboard.

Prerequisites

For a successful integration, you must:

- Obtain a New Relic event endpoint in the following format:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

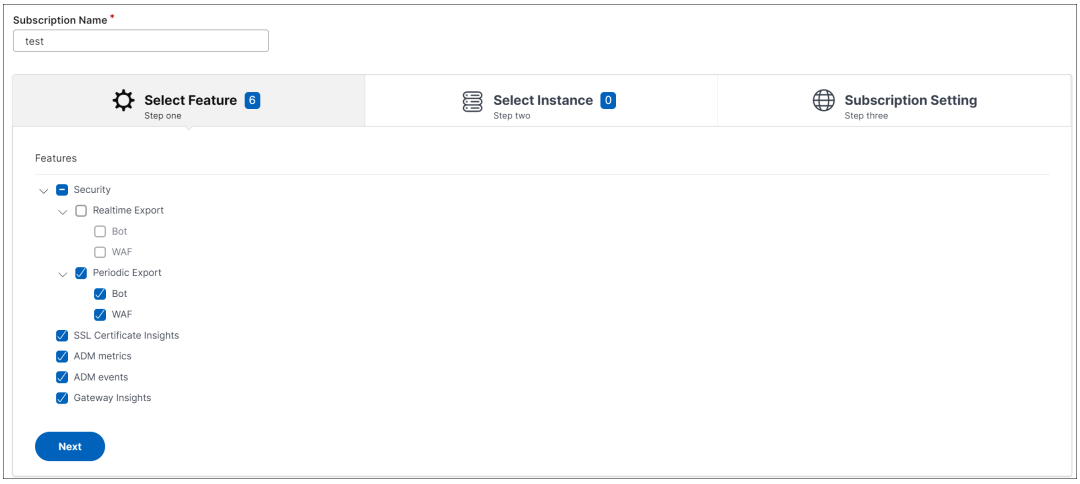
  For more information on configuring an event endpoint, see New Relic documentation.

  For more information on getting an account ID, see New Relic documentation.
- Obtain a New Relic key. For more information, see New Relic documentation.
- Add the key details in NetScaler ADM

Add the key details in NetScaler ADM

After you generate a token, you must add details in NetScaler ADM to integrate with New Relic.

1. Log on to NetScaler ADM.
2. Navigate to **Settings > Ecosystem Integration**.
3. In the **Subscriptions** page, click **Add**.
4. In the **Select features to subscribe** tab, select the features that you want to export and click **Next**.
   - **Realtime Export** - The selected violations are exported to New Relic immediately.
   - **Periodic Export** - The selected violations are exported to New Relic based on the duration you select.



5. In the **Specify export configuration** tab:

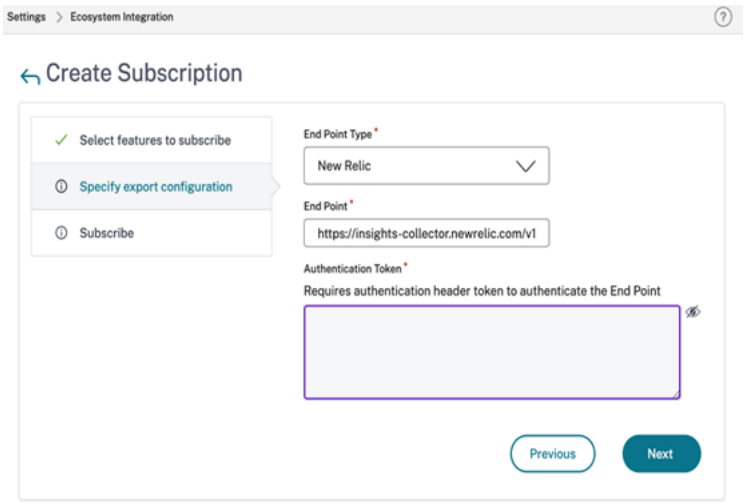
   a) **End Point Type** –Select **New Relic** from the list.

   b) **End Point** –Specify the New Relic end point details. The end point must be in the `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` format.

   > **Note**
   >
   > It is recommended to use HTTPS for security reasons.

   c) **Authentication token** –Copy and paste the authentication token from the New Relic page.

   d) Click **Next**.



6. In the **Subscribe** page:

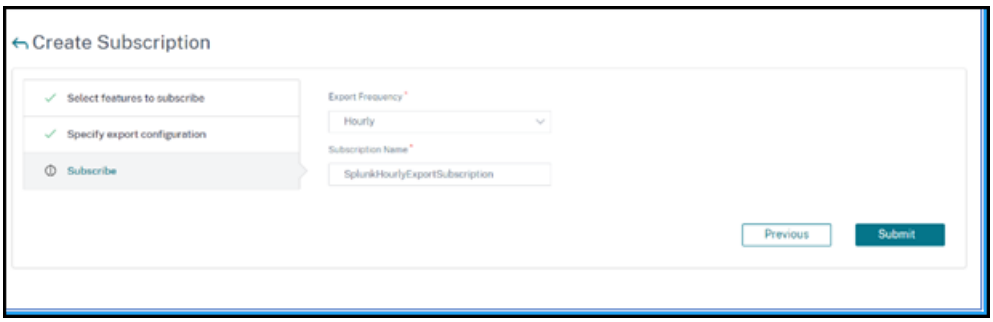
   a) **Export Frequency** –Select Daily or Hourly from the list. Based on the selection, NetScaler ADM exports the details to New Relic.

   > **Note**
   >
   > Applicable only if you have selected violations in **Periodic Export**.

   b) **Subscription Name** –Specify a name of your choice.

   c) Select the **Enable Notifications** check box.

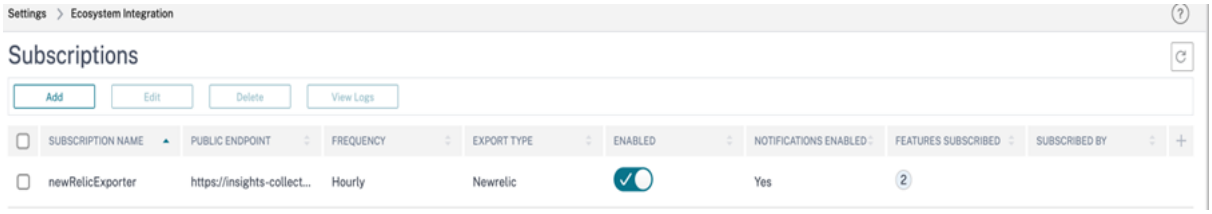
   d) Click **Submit**.



Note

- When you configure with **Periodic Export** option for the first time, the selected features data get pushed to New Relic immediately. The next export frequency happens based on your selection (daily or hourly).
- When you configure with **Realtime Export** option for the first time, the selected features data pushed to New Relic immediately as soon as the violations are detected in NetScaler ADM.

The configuration is complete. You can view details in the **Subscriptions** page.

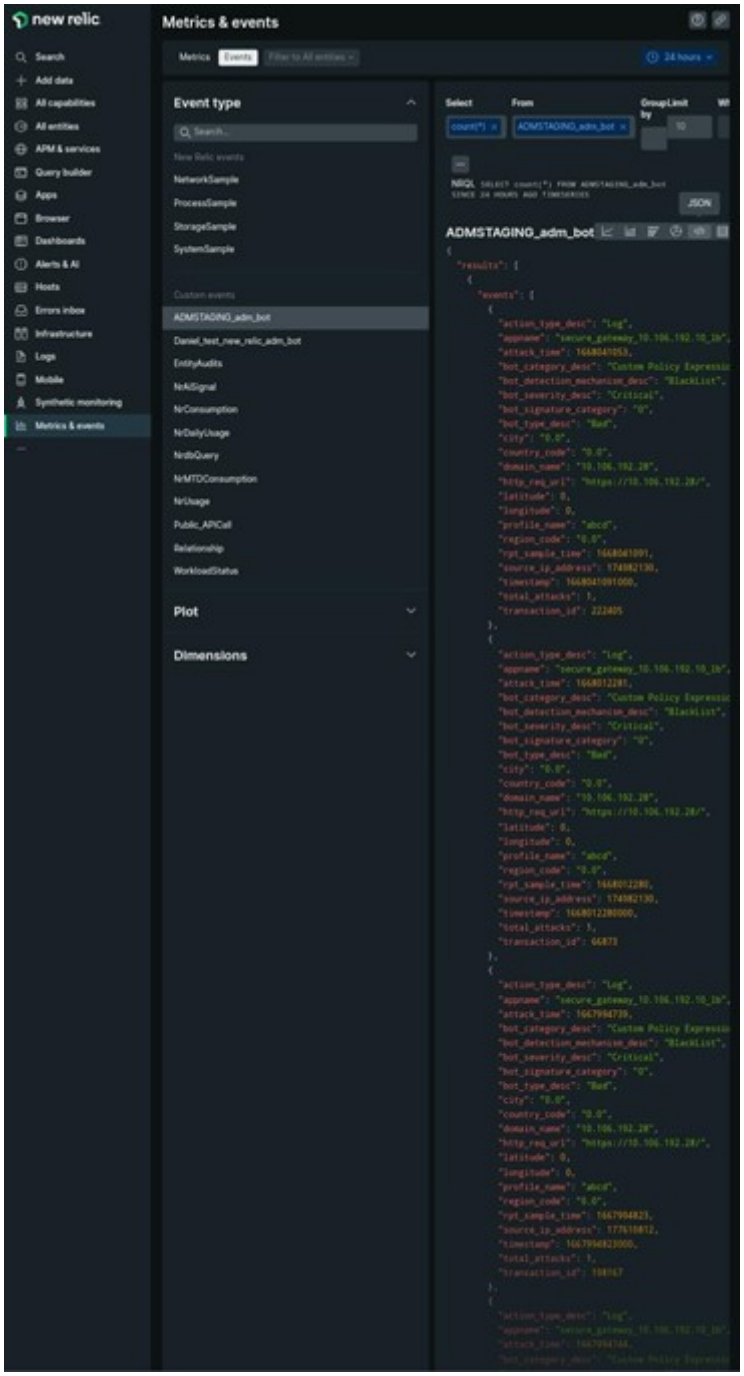


New Relic dashboard

When the events are exported in New Relic, you can view event details under **Metrics & events** in the following JSON format:

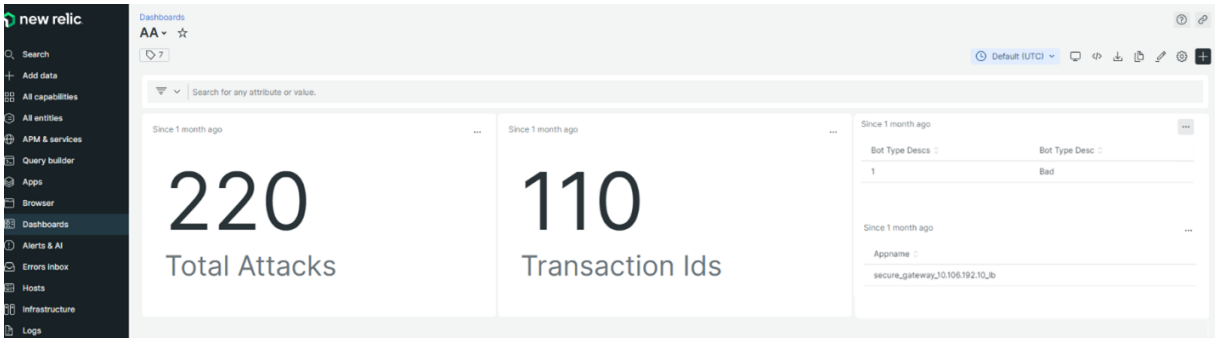
<subsription_name>_adm_<event name> where event name can be Bot, WAF, and so on.

In the following example, ADMSTAGING is the <subscription_name> and bot is the <event_name>.



Once you get the JSON data ingested into your New Relic dashboard, as an administrator, you can use the NRQL (New Relic Query Language) and create a custom dashboard with facets and widgets based on your choice by constructing queries around the ingested data. For more information, see https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/

The following is an example dashboard created using the NRQL:



To create this dashboard, the following queries are required:

- Widget 1: Total Unique Attacks in events table

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- Widget 2: Unique Transaction IDs in event table

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days
   ago
  ```

- Widget 3: Total Unique Bot Types and their counts

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <
  event_name> since 30 days ago
  ```

- Widget 4: Total unique App Names seeing Bot Violations

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

Gateway Insight

March 11, 2024

In a NetScaler Gateway deployment, visibility into a user's access details is essential for troubleshooting access failure issues. As a network administrator, you want to know when a user is not able to log on to NetScaler Gateway, and you want to know the user activity and the reasons for logon failure. This information is typically not available unless the user sends a request for resolution.

Gateway Insight provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway. You can view a list of all available users, number of active users, number of active sessions, and bytes and licenses used by all users at any given time. You can view the end-point analysis (EPA), authentication, single sign-on (SSO), and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

Gateway Insight also provides visibility into the reasons for application launch failure for virtual applications. This enhances your ability to troubleshoot any kind of logon or application launch failure issues. You can view the number of applications launched, the number of total and active sessions, the number of total bytes, and the bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

All log messages are stored in the NetScaler ADM database, so you can view error details for any time period. You can also view a summary of the logon failures and determine at what stage of the logon process a failure has occurred.

Points to note

- Gateway Insight is supported on the following deployments:
  - Access Gateway
  - Unified Gateway
- The NetScaler ADM release and build must be the same or later than that of the NetScaler Gateway appliance.
- One hour of Gateway Insight reports can be viewed for NetScaler instances with Advanced license. A Premium license is a must view Gateway Insight reports beyond one hour.

Limitations

- NetScaler Gateway does not support Gateway Insight when the authentication method is configured as certificate-based authentication.
- For Gateway Insight reporting, geo location information is not provided from the NetScaler appliance.
- Successful user logons, latency, and application-level details for virtual ICA applications and desktops are visible only on the HDX Insight Users dashboard.
- In a double-hop mode, visibility into failures on the NetScaler Gateway appliance in the second DMZ is not available.
- Remote Desktop Protocol (RDP) desktop access issues are not reported.

- Gateway Insight is supported for the following authentication types. If other authentication type is used other than these, you might see some discrepancies in Gateway Insight.
  - Local
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Native OTP
  - OAuth-OpenID Connect

    For the OAuth-OpenID Connect authentication, NetScaler can act as an OAuth-OpenID connect relying party (RP) or OAuth-OpenID connect identity provider (IdP). When the authentication succeeds, the user name is reported under the Users tab in the Gateway Insight report. However, you cannot identify whether the session was created at IdP or RP.

    Note: OAuth-OpenID Connect authentication is supported from NetScaler ADM release 13.1 build 4.xx and later.

Enable Gateway Insight

To enable Gateway Insight for your NetScaler Gateway appliance, you must first add the NetScaler Gateway appliance to NetScaler ADM. You must then enable AppFlow for the virtual server representing the VPN application. For information about adding device to NetScaler ADM, see Adding Devices.

> **Note**
>
> To view end-point analysis (EPA) failures in NetScaler ADM, you must enable AppFlow authentication, authorization, and auditing user name logging on the NetScaler Gateway appliance.

The following procedure to enable gateway insight is applicable if your NetScaler ADM is **13.0 Build 36.27**:

1. Navigate to **Infrastructure > Instances**, and select the instance for which you want to enable AppFlow.
2. From the **Select Action** list, select **Configure Analytics**.
3. In the **Configure Insight** page, under **Configure Analytics**, select **NetScaler Gateway**.
4. Select the virtual server and then click **Enable AppFlow**.

5. On the **Enable AppFlow** screen, in the **Select Expression** list, click true.
6. Next to **Transport Mode**, select the **Logstream** check box.

   > **Note**
   >
   > You can choose either **IPFIX** or **Logstream** as transport mode.
   >
   > For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

7. Click **OK**.

For NetScaler ADM version 13.0 Build 41.x or later

1. Navigate to **Infrastructure > Instances**, and select the instance.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the virtual server and click **Enable Analytics**.
4. Under **Advanced Options**:
   a) Select **Logstream**
   b) Select **NetScaler Gateway**
5. Click **OK**.

Enable AppFlow authentication, authorization, and auditing user name logging on a NetScaler Gateway appliance by using the GUI

1. Navigate to **Configuration > System > AppFlow > Settings**, and then click **Change AppFlow Settings**.
2. In the **Configure AppFlow Settings** screen, select **AAA Username**, and then click **OK**.

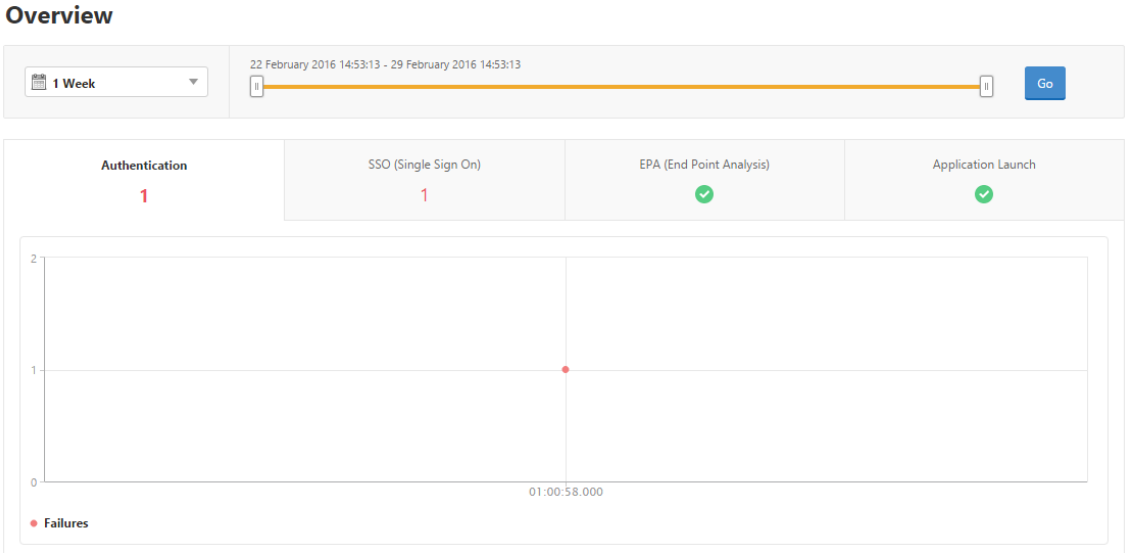
Viewing Gateway Insight reports

In NetScaler ADM, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the **Overview** section, you can view the EPA, SSO, Authentication, and Application Launch failures. You can also view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.

> **Note**
>
> When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

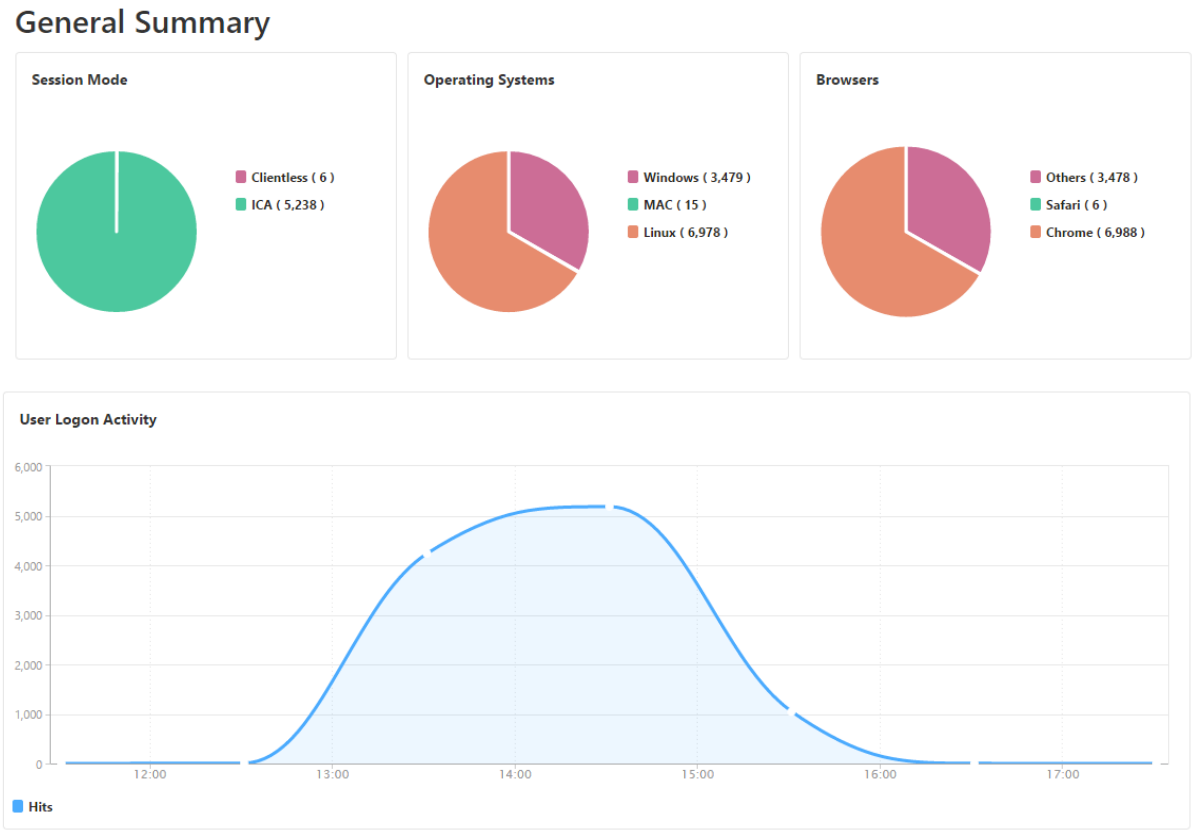
To view EPA, SSO, authentication, authorization, and application launch failures

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.



To view a summary of session modes, clients, and the number of users

In NetScaler ADM, navigate to **Gateway > Gateway Insight**, scroll down to view the reports.



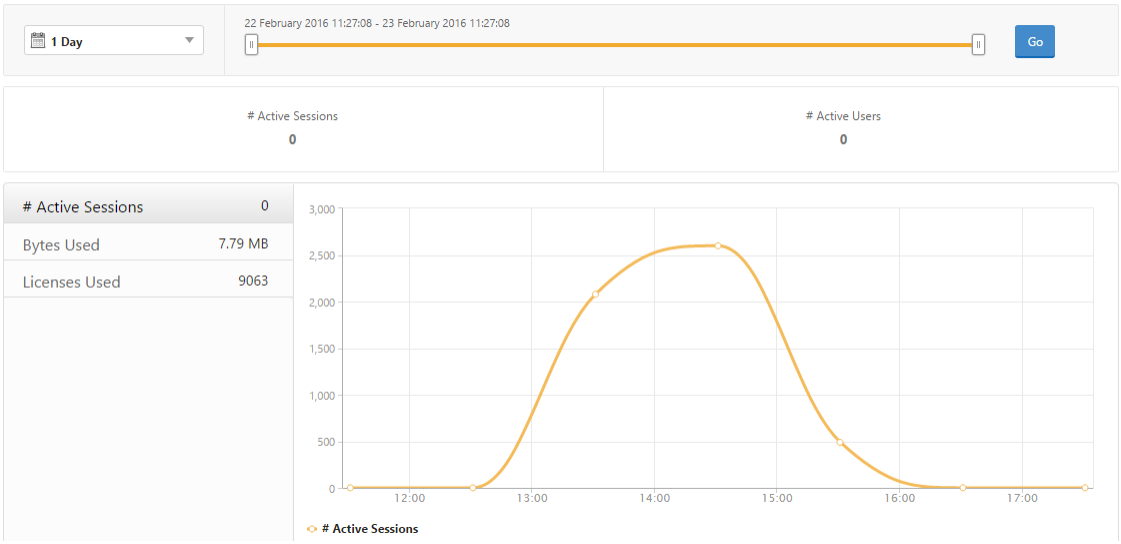
Viewing Gateway Insight reports for users

You can view the reports for:

- All users associated with the NetScaler Gateway appliances.
- The EPA, authentication, SSO, and application launch failures for a user.
- The details of active and terminated sessions for a user.
- The types of session modes such as Full Tunnel, clientless VPN, and ICA Proxy.

To view user details

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight > Users**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. You can view the number of active users, number of active sessions, bytes, and licenses used by all users during the time period.

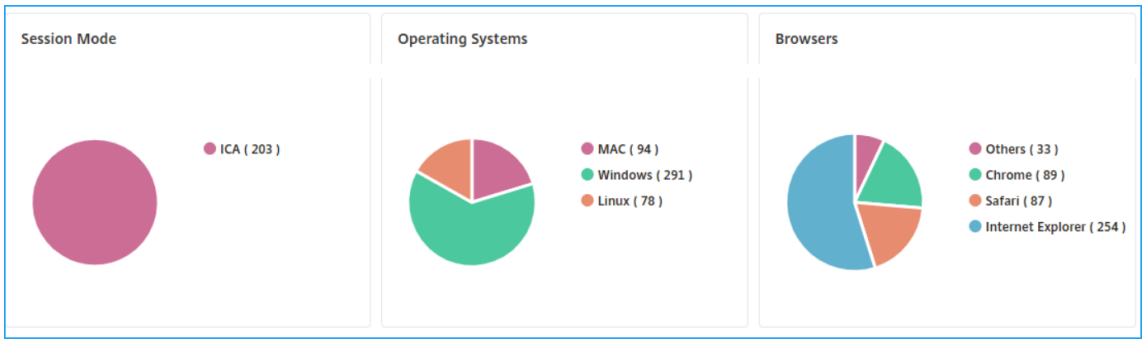


Scroll down to view a list of available users and active users.

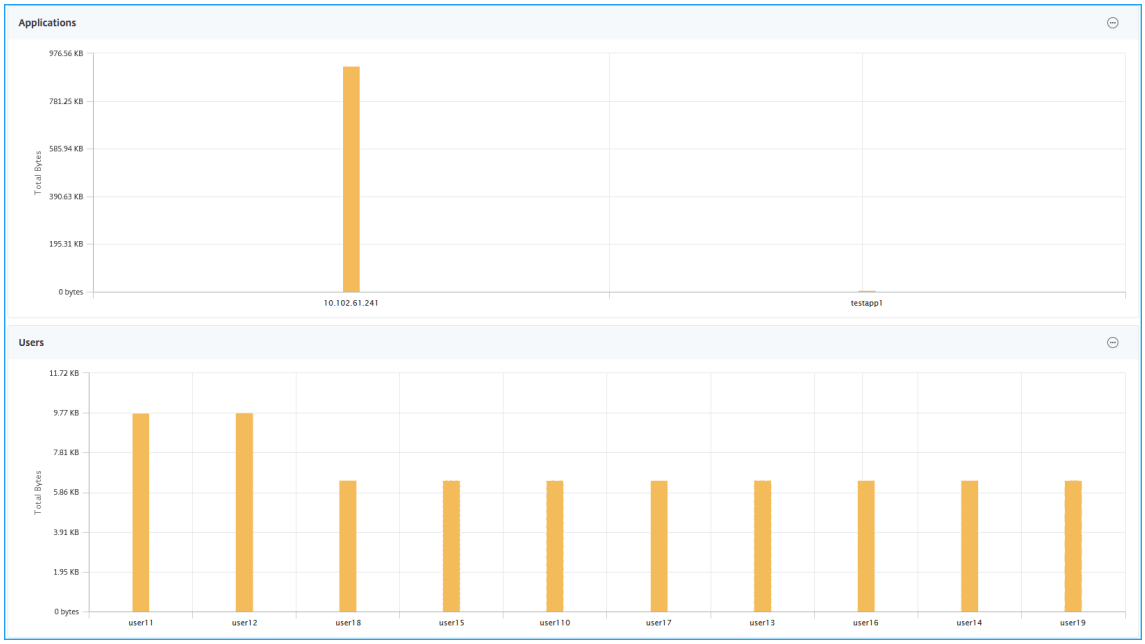
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

On the **Users** or **Active Users** tab, click a user to view the following user details:

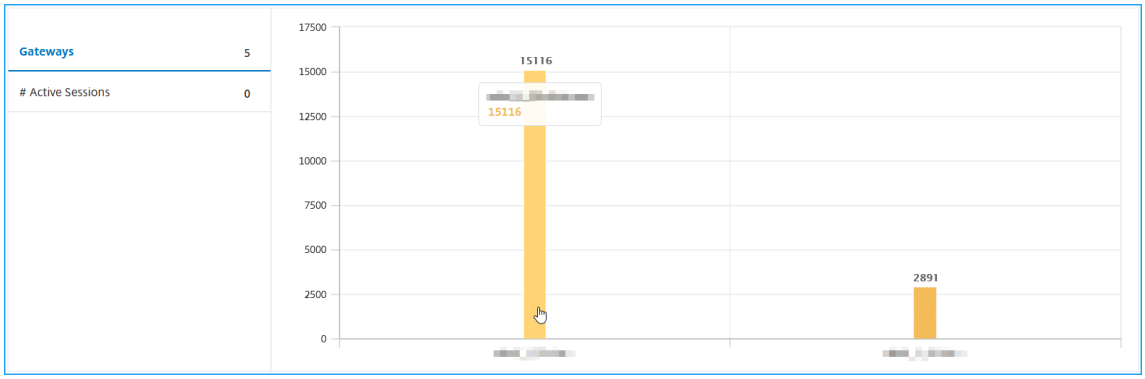
- **User details** - You can view insights for each user associated with the ADC Gateway appliances. Navigate to **Gateway** > **Gateway Insight** > **Users** and click a user to view insights for the selected user such as Session Mode, Operating System, and Browsers.



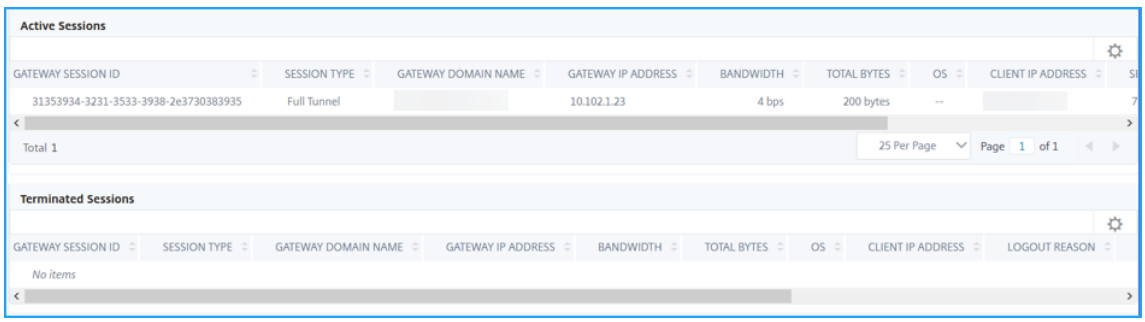
- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.



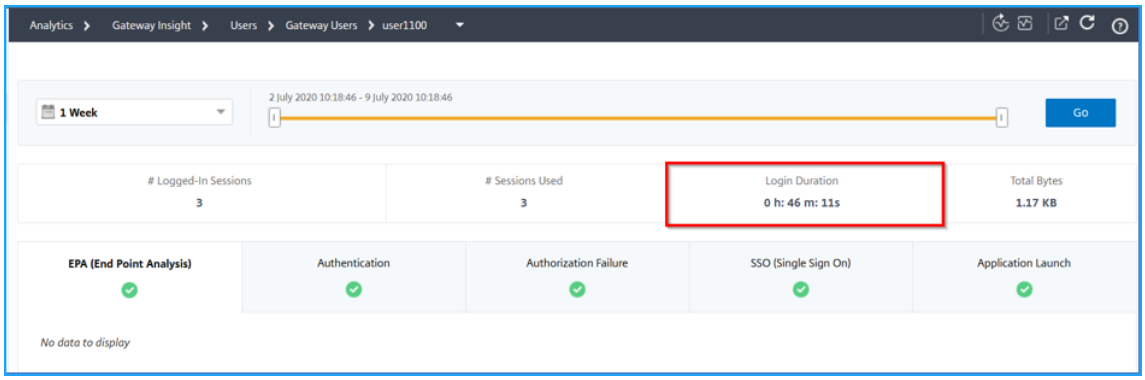
- **View more option for applications and users** –For more than 10 applications and users, you can click the more icon in Applications and Users to view all users and applications details that are associated with the selected gateway.
- **View details by clicking the bar graph** –When you click a bar graph, you can view the relevant details. For example, navigate to **Gateway > Gateway Insight > Gateway** and click the gateway bar graph to view the gateway details.



- The user **Active Sessions** and **Terminated Sessions**.



- The gateway domain name and gateway IP address in **Active Sessions**.
- The user login duration.



- The reason for the user logout session. The logout reasons can be:
  - Session timed out
  - Logged out because of internal error
  - Logged out because of inactive session timed out
  - User has logged out
  - Administrator has stopped the session

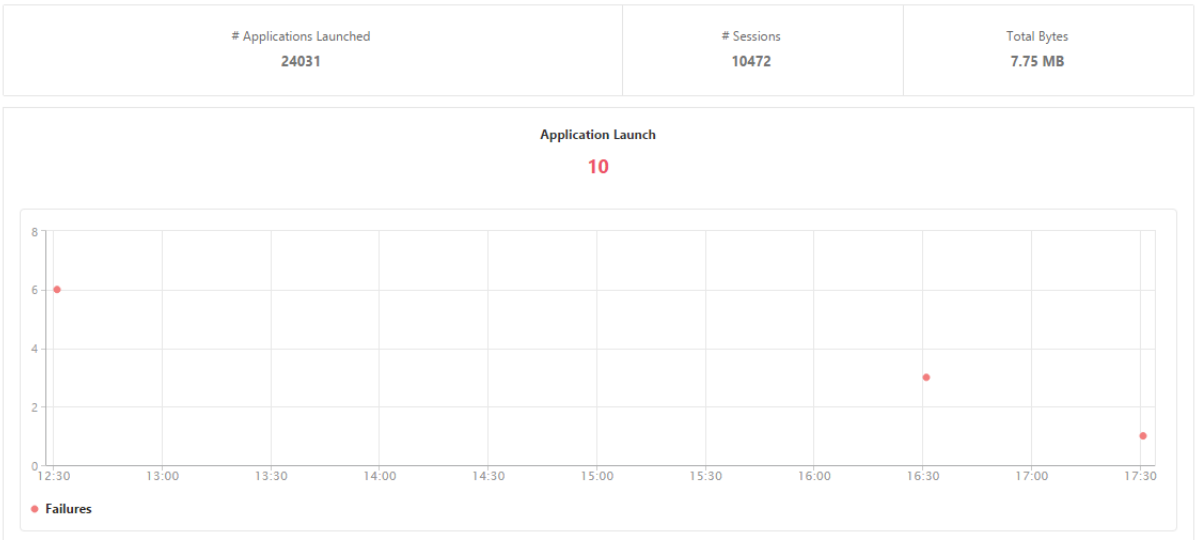
Viewing Gateway Insight reports for applications

You can view the number of applications launched, the number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

To view application details

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight > Applications**.
2. Select the time period for which you want to view the application details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of applications launched, the number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.



Scroll down to view the numbers of sessions, bandwidth, and total bytes consumed by ICA and other applications.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

On the **Other Applications** tab, you can click an application in the **Name** column to display details of that application.

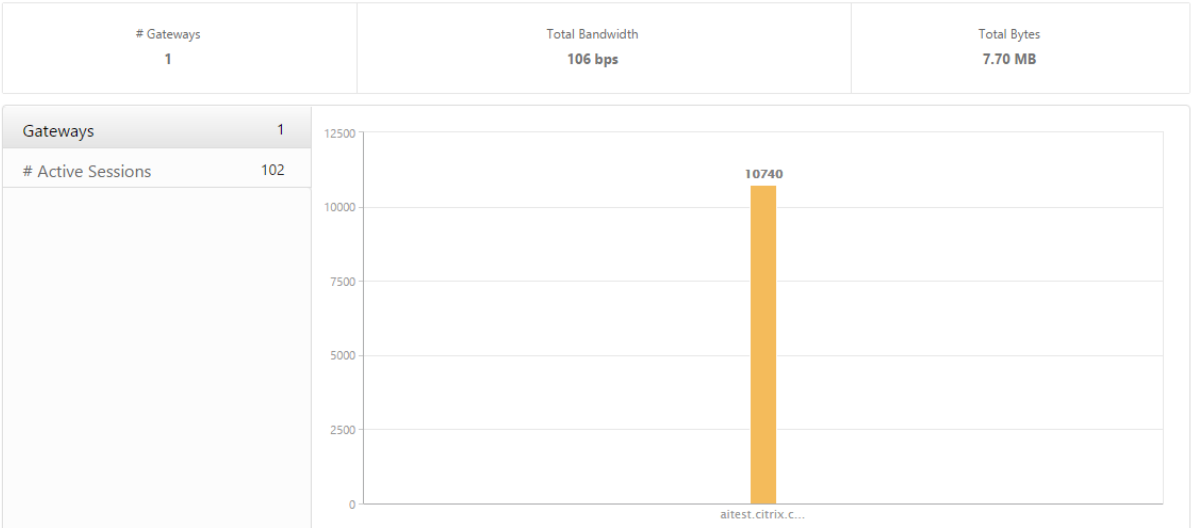
Viewing Gateway Insight reports for gateways

You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

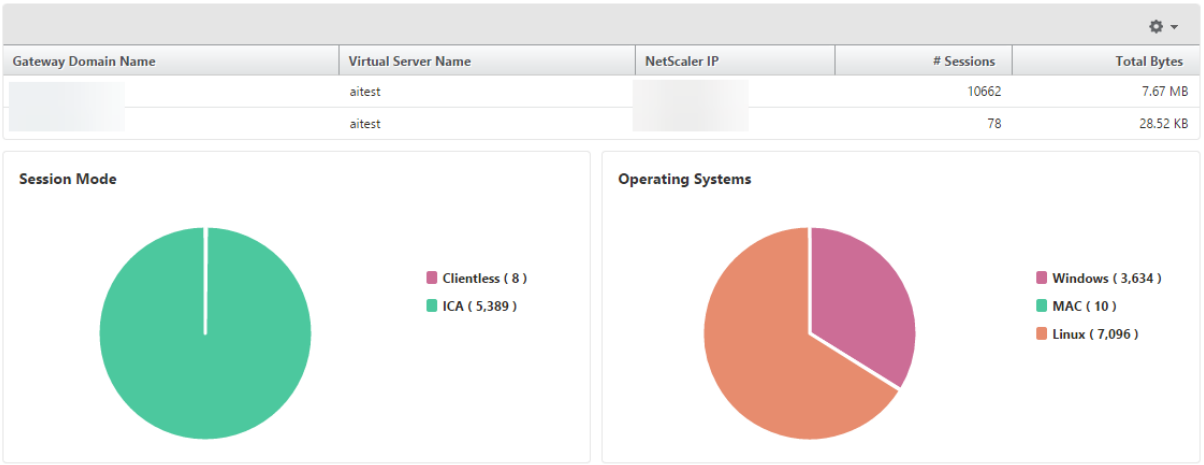
To view gateway details

1. In **NetScaler ADM**, navigate to **Gateway > Gateway Insight > Gateways**.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time.



Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, NetScaler IP address, session modes, and Total Bytes.



You can click a gateway in the **Gateway Domain Name** column to display the EPA, authentication, single sign-on, and application launch failures and other details for a gateway.

Exporting reports

You can save the Gateway Insight reports with all the details shown in the GUI in PDF, JPEG, PNG, or CSV format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.

> **Note**
>
> - Users with read only access cannot export reports.
> - Geo map reports are exported only if the NetScaler ADM has internet connectivity.

To export a report

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select the required format, and then click **Export**.

To schedule export:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Schedule Export**, specify the details and click **Schedule**.

To add an email server or an email distribution list:

1. On the **Configuration** tab, navigate to **Settings > Notifications > Email**.
2. In the right pane, select **Email Server**, to add an email server, or select **Email Distribution list** to create an email distribution list.
3. Specify the details and click **Create**.

To export the entire Gateway Insight dashboard:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select **PDF** format, and then click **Export**.

Gateway Insight use cases

The following use cases show how you can use Gateway Insight to gain visibility into users' access details, applications, and gateways on NetScaler Gateway appliances.

A user is not able to log in to the NetScaler Gateway appliance or to the internal web servers

You are a NetScaler Gateway administrator monitoring NetScaler Gateway appliances through NetScaler ADM, and you want to see why a user is unable to log in, or at what stage of the login process the failure has occurred.

NetScaler ADM enables you to view the user login error details in the following stages of the login process:

- Authentication
- End-point analysis (EPA)
- Single sign-on

In NetScaler ADM, you can search for a particular user and then view all the details for that user.

To search for a user:

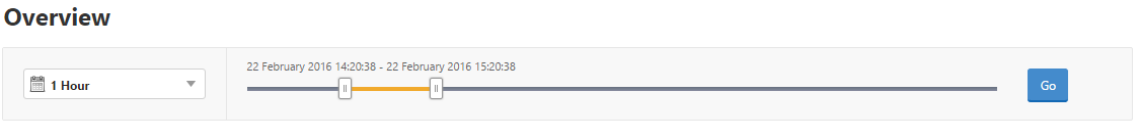
In NetScaler ADM, navigate to **Gateway > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

Authentication failures

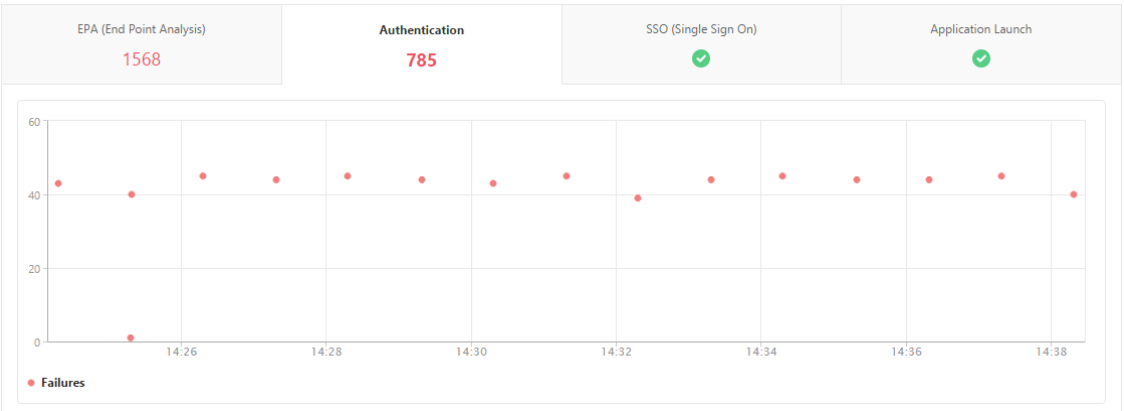
You can view authentication errors such as incorrect credentials or no response from the authentication server. You can also see the factor at which the authentication failed.

To view the authentication failure details:

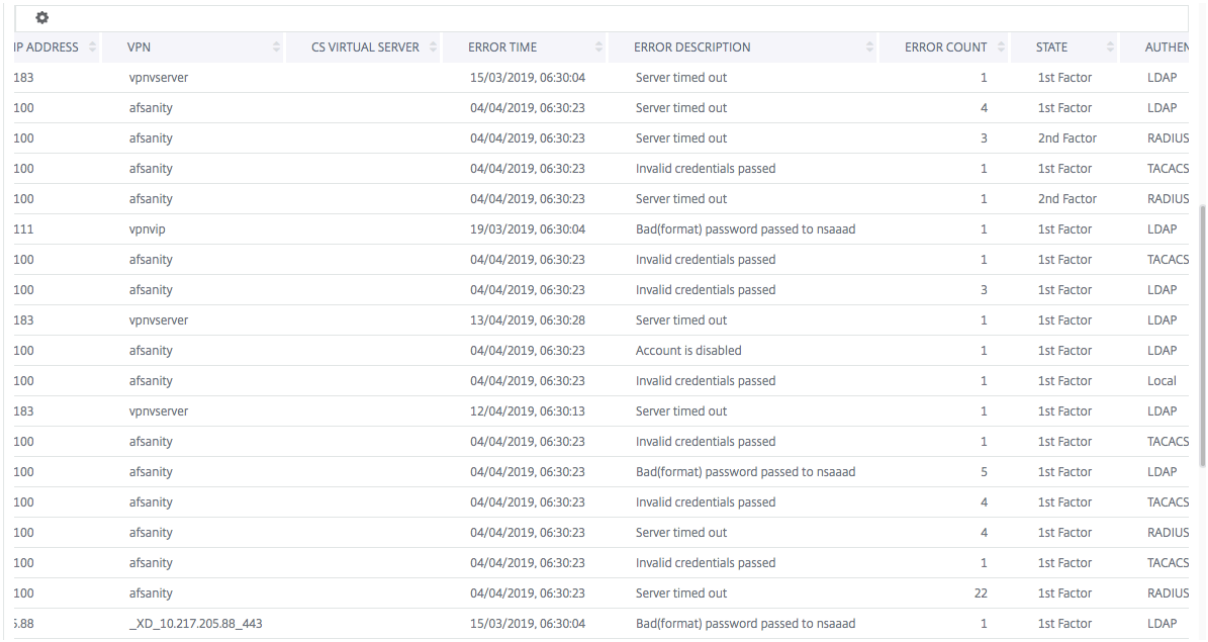
1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the authentication errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.



Scroll down to view details of each authentication error such as **Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address**, and more from the table on the same tab. The **Error Description** column in the table displays the reason for the logon failure, and the **State** column displays the nth factor at which the failure occurred.



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

You can click a user in the **Username** column to display the authentication errors and other details for that user. You can customize the table to add or delete columns by using the settings icon.

> **Important:**
>
> If OAuth-OpenID Connect authentication fails, the user name is displayed as **NA** in the Gateway Insight report for some of the failures, for example "Token verification failure". In this failure, the user names are not available for authentication failure due to "Token verification failure"at the OAuth-OpenID connect relying party.

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-				gitest.citrix.com		Relying party: Token verification failed
-NA-				gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token decryption failure

EPA failures

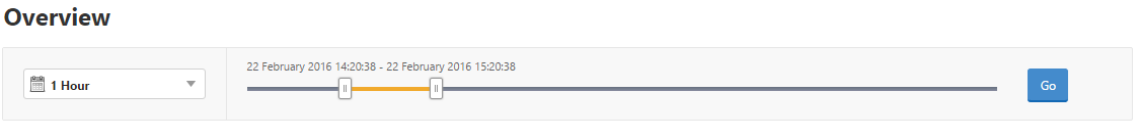
You can view EPA failures at the pre-authentication or post-authentication stage.

> **Important:**
>
> - EPA failures are reported only when classic expressions are configured.
> - EPA failures are not reported if advanced expression is configured in the pre-authentication or post-authentication policy.

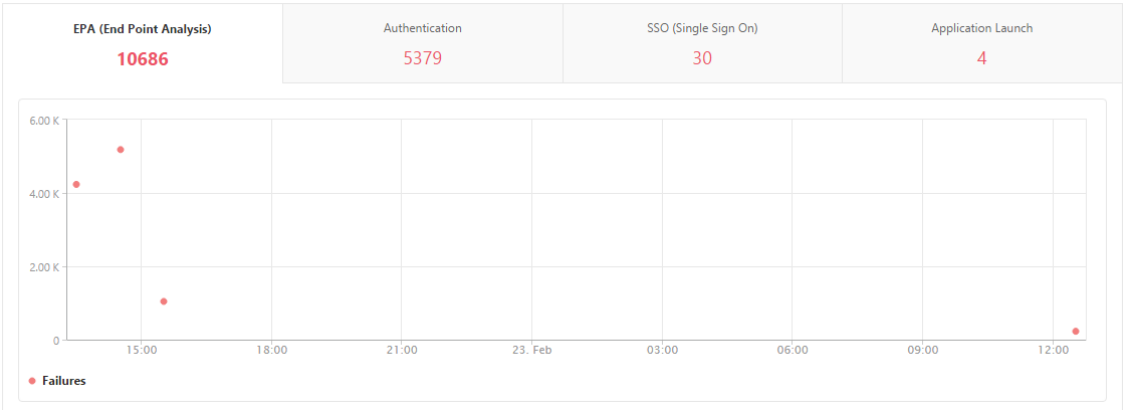
- EPA failures are not reported if EPA is configured as one of the factors in an nFactor authentication flow.

To view EPA failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **EPA (End Point Analysis)** tab. You can view the number of EPA errors at any given time in the **Failures** graph.



Scroll down to view details of each EPA error such as **Username, NetScaler IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name** and more from the table on the same tab. The **Error Description** column in the table displays the reason for the EPA failure, and the **Policy Name** column displays the policy that resulted in the failure.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

You can click a user in the **Username** column to display the EPA errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

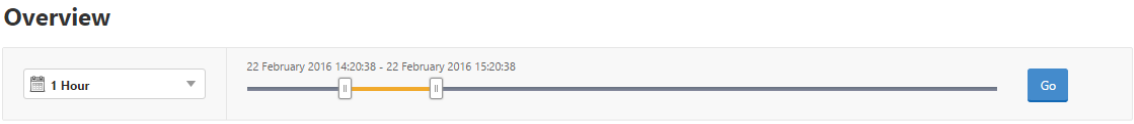
> **Note**
>
> NetScaler Gateway doesn't report the EPA failures when the "clientSecurity"expression is configured as a VPN session policy rule.

SSO failures

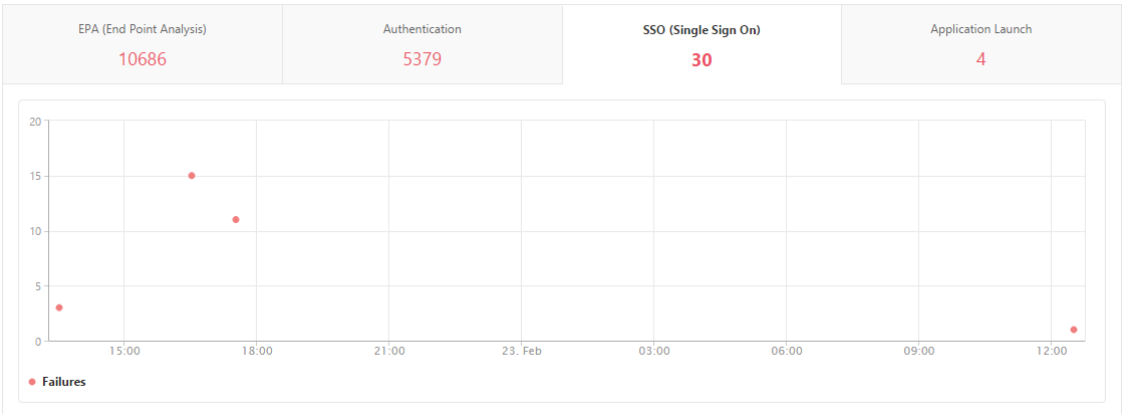
You can view the all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

To view the SSO failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.



Scroll down to view details of each SSO error such as **Username, NetScaler IP Address, Error Time, Error Description, Resource Name** and more from the table on the same tab.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

You can click a user in the **Username** column to display the SSO errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

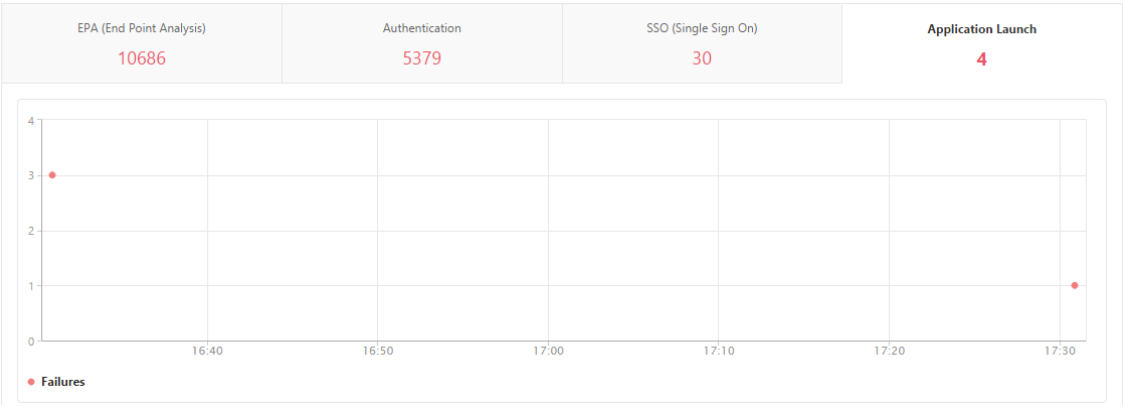
After successfully logging on to NetScaler Gateway, a user is not able to launch any virtual application

For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or Citrix Virtual App server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

To view the application launch failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.

3. Click the **Application Launch** tab. You can view the number of application launch failures at any given time in the **Failures** graph.



Scroll down to view details of each application launch error, such as **NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, and more, from the table on the same tab. The **Error Description** column in the table displays the IP address of the STA server and the **Resource Name** column displays the details of the resource for which the STA validation has failed.

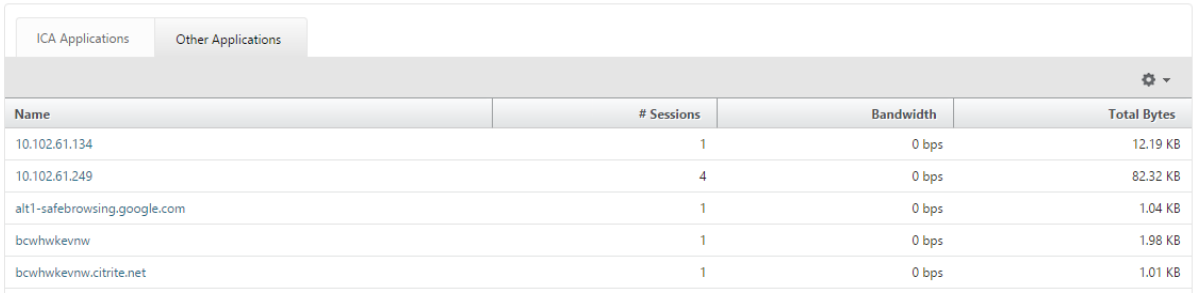
You can click a user in the **Username** column to display the application launch errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application

After you have successfully launched a new application, in NetScaler ADM, you can view the total bytes and bandwidth consumed by that application.

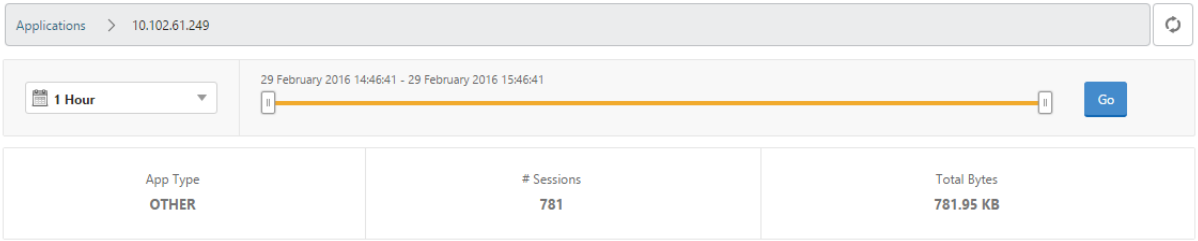
To view total bytes and bandwidth consumed by an application:

In NetScaler ADM, navigate to **Gateway > Gateway Insight > Applications**, scroll down and, on the **Other Applications** tab, click the application for which you want to view the details.

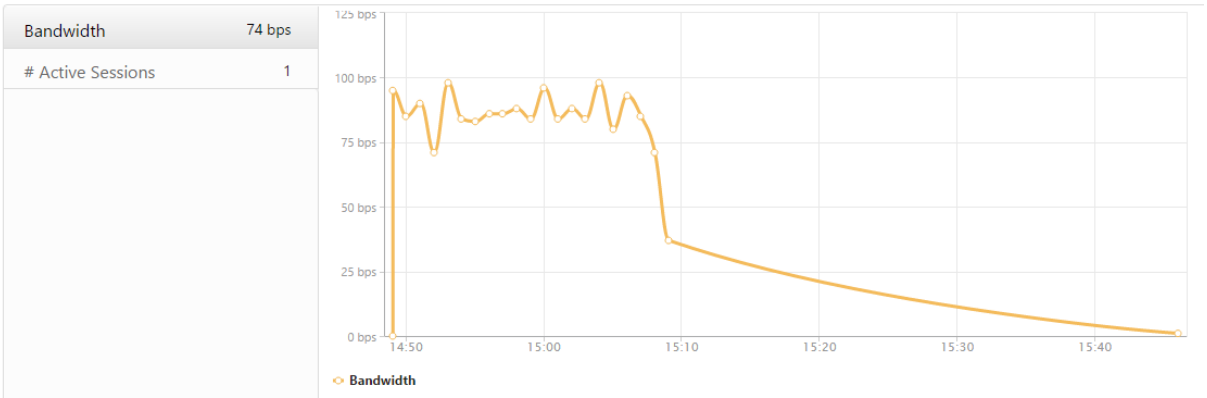


Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

You can view the number of sessions and the total number of bytes consumed by that application.



You can also view the bandwidth consumed by that application.

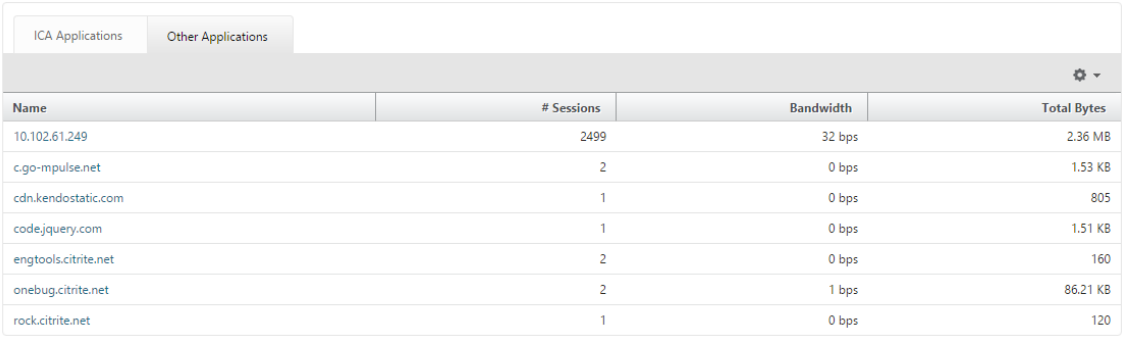


A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network

With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

To view user access for resources:

1. In NetScaler ADM, **navigate to Gateway > Gateway Insight > Applications**.
2. On the screen that appears, scroll down, and on the **Other Applications** tab, select the application to which the user was unable to log on.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

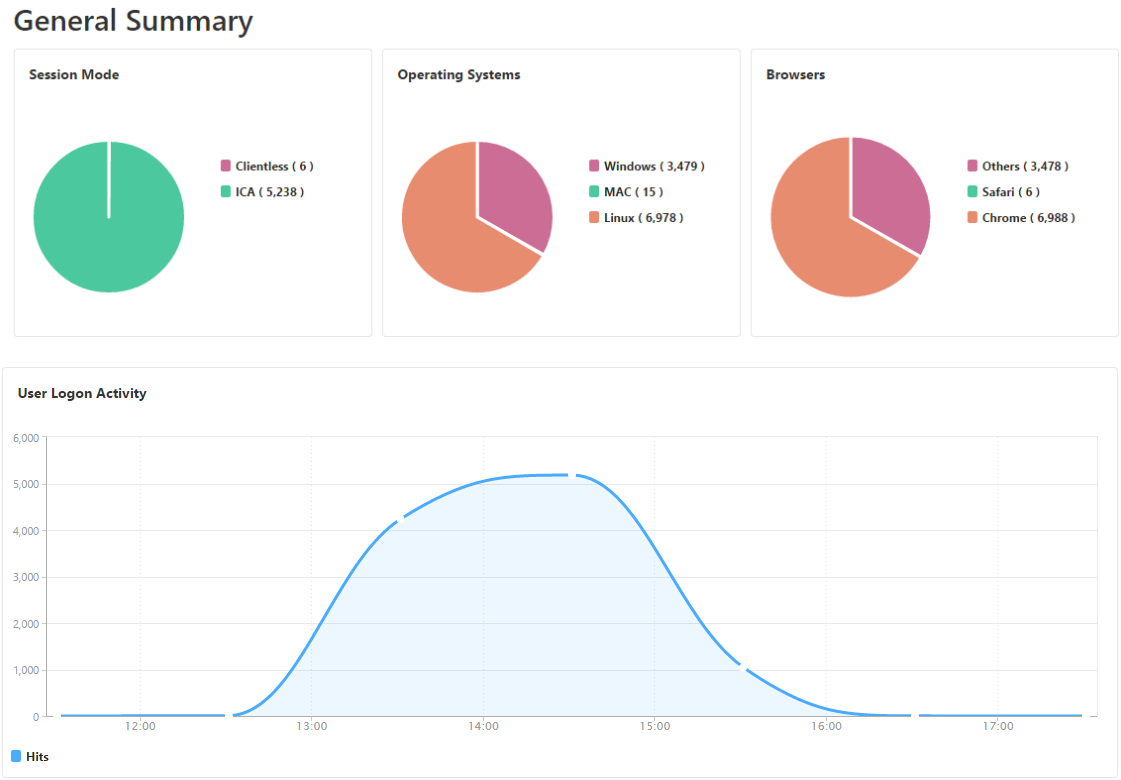
3. Scroll down and in the **Users** table, all the users that have access to that application are displayed.

Different users might be using different NetScaler Gateway deployments or might log on to NetScaler Gateway through different access modes. The administrator must be able to view details about the deployment types and access modes

With Gateway Insight, you can view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour. You can also determine whether a user's deployment is a unified gateway or classic NetScaler Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

To view the summary of session modes, type of clients, and number of users logged on:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, scroll down to view the **Session Mode, Operating Systems, Browsers**, and **User Logon Activity** charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.



Troubleshoot Gateway Insight issues

March 11, 2024

If the Gateway Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- Gateway Insight configuration.
- Connectivity issue between NetScaler and NetScaler ADM.
- Record generation in NetScaler.
- Validations in NetScaler ADM.

Gateway Insight configuration checklist

- Make sure that the AppFlow feature is enabled in the NetScaler appliance. For details, see Enabling AppFlow.
- Check the Gateway Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the Gateway Insight configuration. Make sure that the bind type is REQUEST. For example;


```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
<!--NeedCopy-->
```

Bind type OTHERTCP_REQUEST is also required for Gateway Insight.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

- For single-hop, Access Gateway, or Unified Gateway deployment, make sure that Gateway Insight AppFlow policy is bound to the VPN virtual server, where VPN traffic is flowing. For details, see Enabling HDX Insight data collection.
- For double-hop, Gateway Insight must be configured on both the hops.
- Check `appflowlog` parameter in NetScaler Gateway/VPN virtual server. For details, see Enabling AppFlow for Virtual Servers.

Connectivity between NetScaler and NetScaler ADM checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check Gateway Insight AppFlow policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation in NetScaler checklist

- Run the `nsconmsg -d stats -g ai_tot` command and check for the stats increments in NetScaler.
- Capture `nstrace logs` and check for CFLOW packets to confirm NetScaler exports AppFlow records.

  > **Note:**
  >
  > The `nstrace logs` are required only for IPFIX. For Logstream, nstrace logs do not confirm if the ADC appliance exported the AppFlow records.

Validation of records in NetScaler ADM

- Run the `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` command to check the logs to confirm NetScaler ADM is receiving AppFlow records.
- Make sure that the NetScaler instance is added to the NetScaler ADM.
- Make sure that the NetScaler Gateway/VPN virtual server is licensed in NetScaler ADM.

Validation of Logstream logs in NetScaler ADM

Validation of Logstream data received by NetScaler ADM can be done using the following methods:

- **Enabling data record logging in NetScaler ADM**

  Once enabled, the logs can be seen in the /var/mps/log/mps_afdecoder.log

- **Enabling ULFD library logging**

  Run the command `/mps/decoder_enable_debug`

  The logs are captured in `/var/ulflog/libulfd.log`

  You can disable logging by using the command `/mps/decoder_disable_debug`

Gateway Insight counters

The following Gateway Insight counters are available.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

AppFlow records in NetScaler log

Starting from release 13.0 build 71.x, you can check the NetScaler logs to confirm if the AppFlow records are exported. The default log level of `syslogparams` captures all the error and information logs. In case you do not find a clue about the errors, enable all log levels including DEBUG in `syslogparams` to capture even the DEBUG logs.

Sample logs

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
   GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
   =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
   Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
   vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
   AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
   CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
   =16777219 Deviceid=0 email="
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
   : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
   zero"
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
   : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
   =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
   CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
   =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```



```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

Contact Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler ADM versions.
- Tech support bundle for NetScaler and NetScaler ADM.
- `nstrace` capture during the issue.

Known Issues

Refer ADC release notes for known issues on Gateway Insight.

HDX Insight

March 11, 2024

HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktop passing through NetScaler. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables NetScaler Application Delivery Management (ADM) to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your NetScaler Gateway virtual servers. AppFlow can be delivered by the IPFIX protocol or the LogStream method.

> **Note**
>
> To allow ICA round trip time calculations to be logged, enable the following policy settings:

- ICA Round Trip Calculation
- ICA Round Trip Calculation Interval
- ICA Round Trip Calculation for Idle Connections

If you click an individual user, you can see each HDX session, active or terminated, that the user made within the selected time frame. Other information includes several latency statistics and bandwidth consumed during the session. You can also get bandwidth information from individual virtual channels such as audio, printer mapping, and client drive mapping.

> **Note**
>
> When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

You can also navigate to **Gateway > HDX Insight > Applications** and click **Launch Duration** to view the time taken for the application to launch. You can also view the user agent of all connected users by navigating to **Gateway > HDX Insight > Users.**

> **Note** HDX insight supports Admin Partitions configured in NetScaler instances running on software version 12.0.

The following Thin Clients support HDX Insight:

- WYSE Windows-based Thin Clients
- WYSE Linux-based Thin Clients
- WYSE ThinOS-based Thin Clients
- 10ZiG Ubuntu-based Thin Clients

Identifying the root cause of slow performance issues

Scenario 1

User is experiencing delays while accessing Citrix Virtual Apps and Desktops.

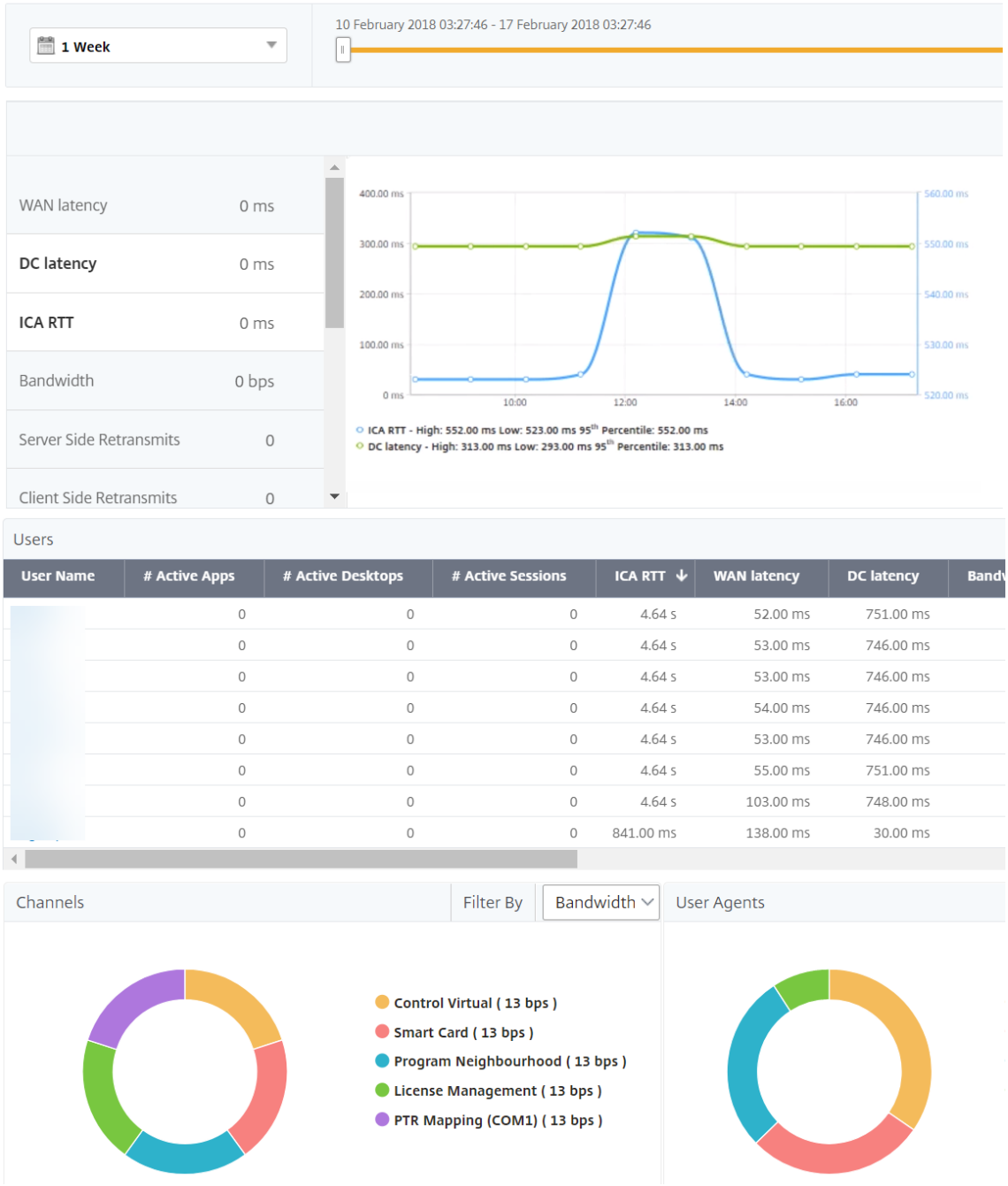
The delays might be due to latency on the server network, ICA traffic delays caused by the server network, or latency on the client network.

To identify the root cause of the issue, analyze the following metrics:

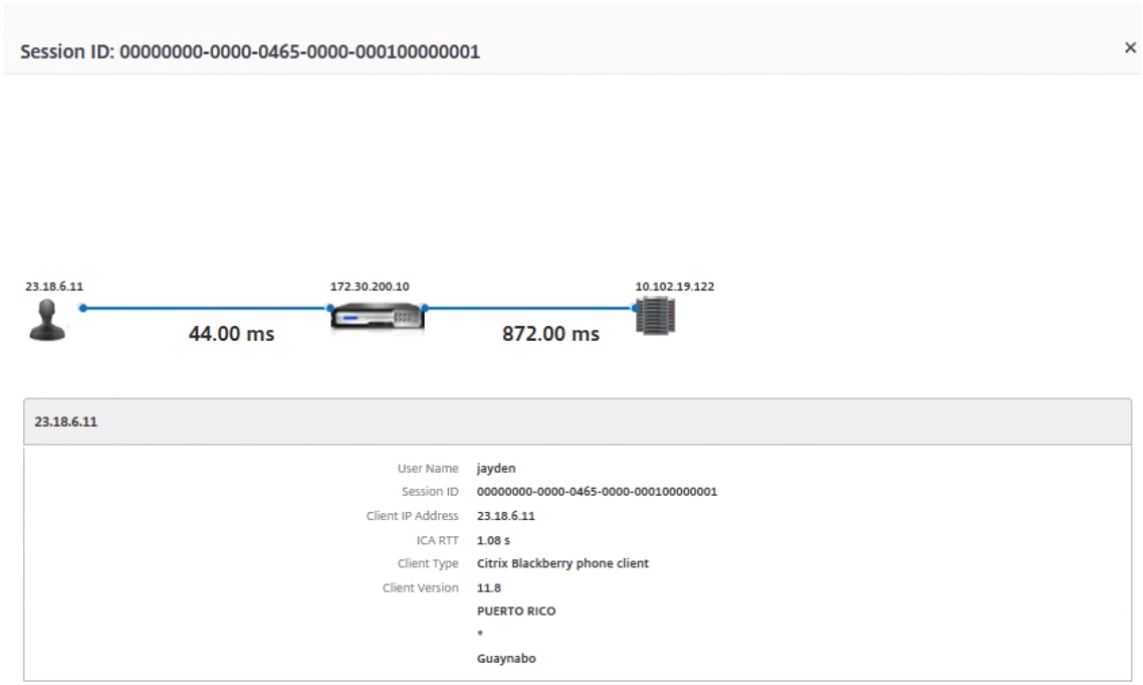
- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

1. Navigate to **Gateway > HDX Insight> Users**.
2. Scroll down and select the user name and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.



4. On the **Current Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.
5. On the **Current Sessions** table, click the hop diagram symbol to display information about the connection between the client and the server, including latency values.



Summary In this example, the **DC Latency** is 751 milliseconds, the **WAN latency** is 52 milliseconds, and **Host Delays** is 6 seconds. This indicates that the user is experiencing delay due to average latency caused by the server network.

Scenario 2

User is experiencing delay while launching an application on Citrix Virtual App or Desktop

The delay might be due to latency on the server network, ICA-traffic delays caused by the server network, latency on the client network, or time taken to launch an application.

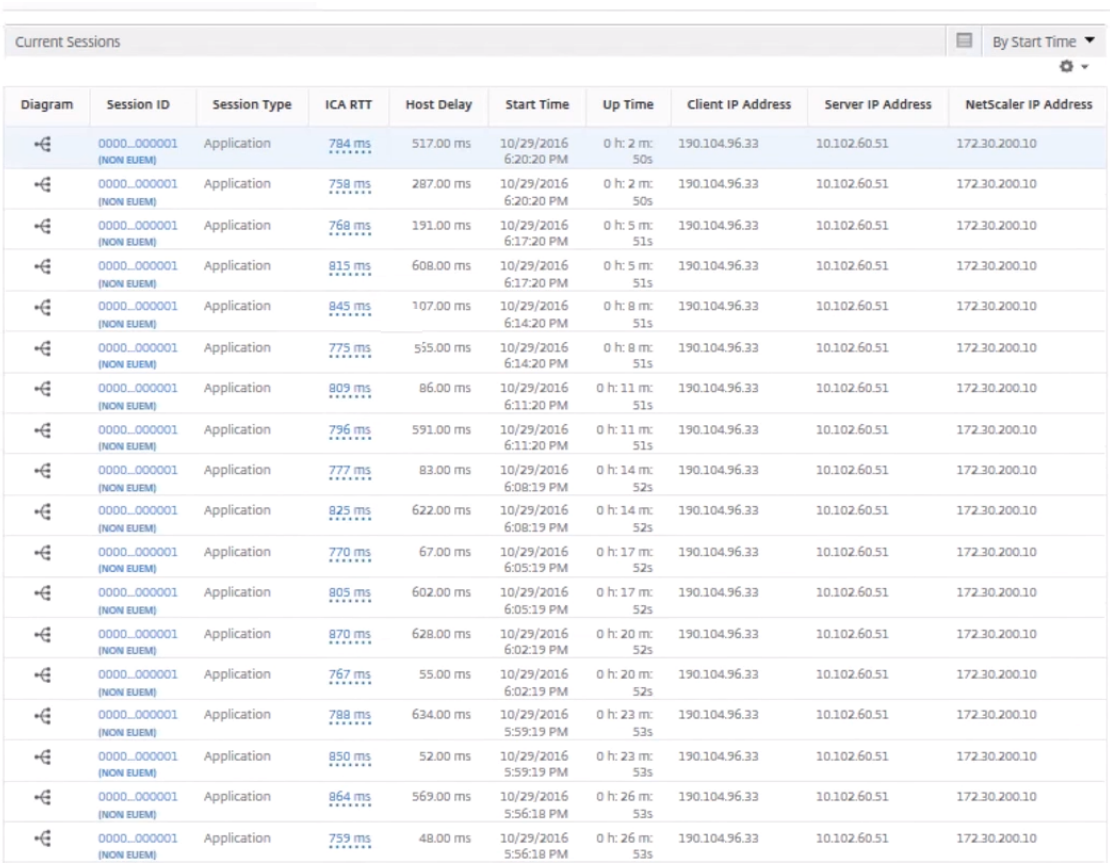
To identify the root cause of the issue, analyze the following metrics:

- WAN latency
- DC latency
- Host delay

To view the user metrics:

1. Navigate to **Gateway > HDX Insight > Users.**
2. Scroll down and click the user name.
3. In the graphical representation, note the WAN Latency, DC Latency, and RTT values for the particular session.

4. In the **Current Sessions** table, note that the host delay is high.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Summary In this example, the **DC Latency** is 1 millisecond, the **WAN latency** is 12 milliseconds, but the **Host Delay** is 517 milliseconds. High RTT with low DC and WAN latencies indicates an application error on the host server.

> **Note** HDX Insight also displays more user metrics, such as WAN jitter and Server Side Retransmits if you are using NetScaler ADM running software 11.1 build 51.21 or later. To view these metrics, navigate to **Gateway > HDX Insight > Users**, and select a user name. The user metrics appear in the table next to the graph.

Geomaps for HDX Insight

The NetScaler ADM geomaps functionality displays the usage of applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage across various geographical locations.

You can configure NetScaler ADM to display the geomaps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

You can also view the historical and active users' details from the geo location maps in HDX Insight. Navigate to **Gateway > HDX Insight**, and in the **World** section of the map, click the country or region for which you want to see the details. You can further drill down to view information by city and state.

To configure a geomap for data centers:

Navigate to **Settings > Analytics Settings > IP Blocks** to configure geomaps for a particular location.

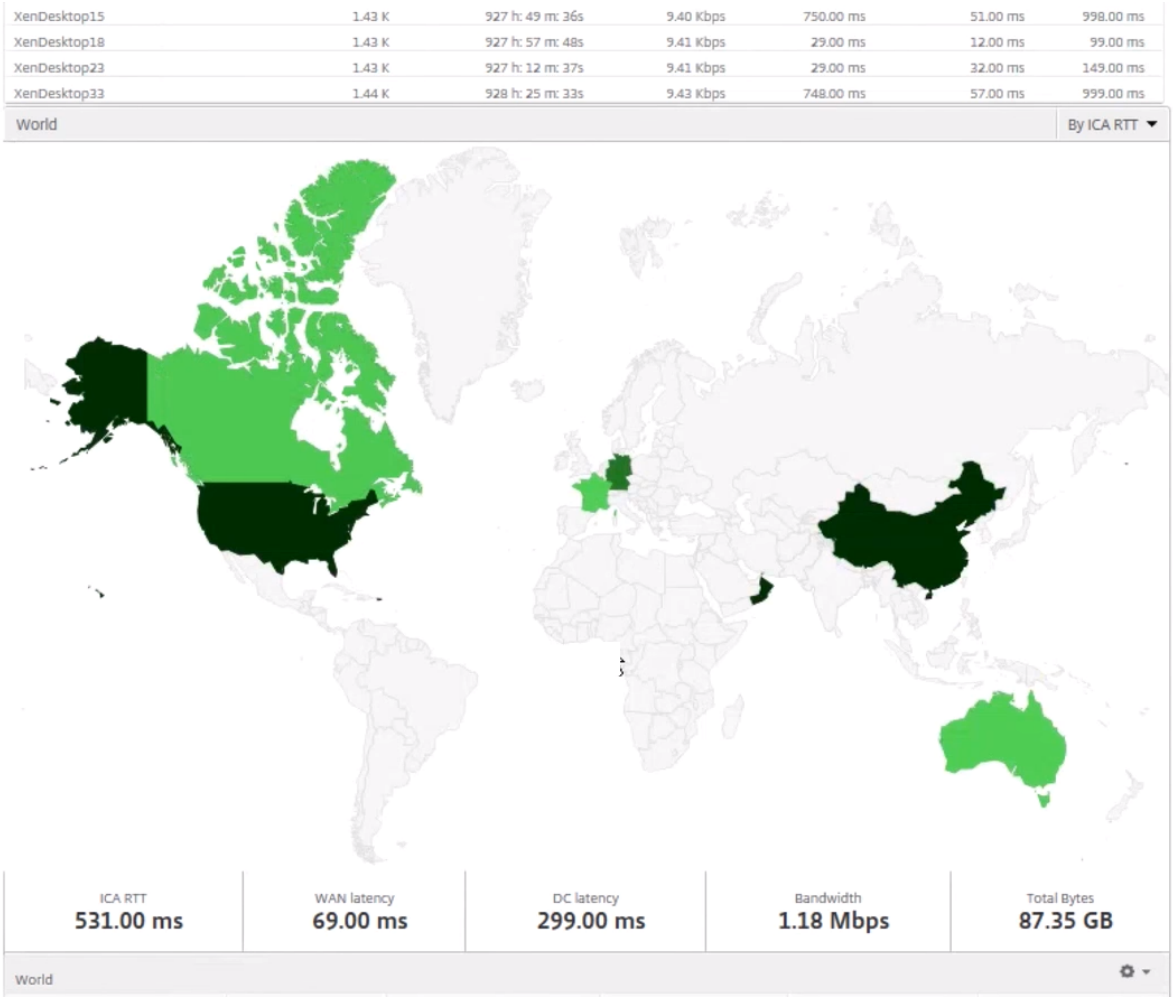
Use case

Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.

The Santa Clara users use the NetScaler Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the NetScaler Gateway appliance at India.x.com to access VPN traffic.

During a particular time-interval, say 10 AM to 5 PM, the users in Santa Clara connect to SClara.x.com to access VPN traffic. Most of the users access the same NetScaler Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

A NetScaler administrator analyzing the traffic can use the geo map functionality to show the traffic in Santa Clara office. The map shows that the response time in the Santa Clara office is high, because the Santa Clara office has only one NetScaler Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another NetScaler Gateway, so that users have two local NetScaler Gateway appliances through which to access the VPN.



Limitations

If NetScaler instances have Advanced license, thresholds set on NetScaler ADM for HDX Insight will not be triggered since analytical data is collected for only 1 hour.

Enabling HDX Insight data collection

March 11, 2024

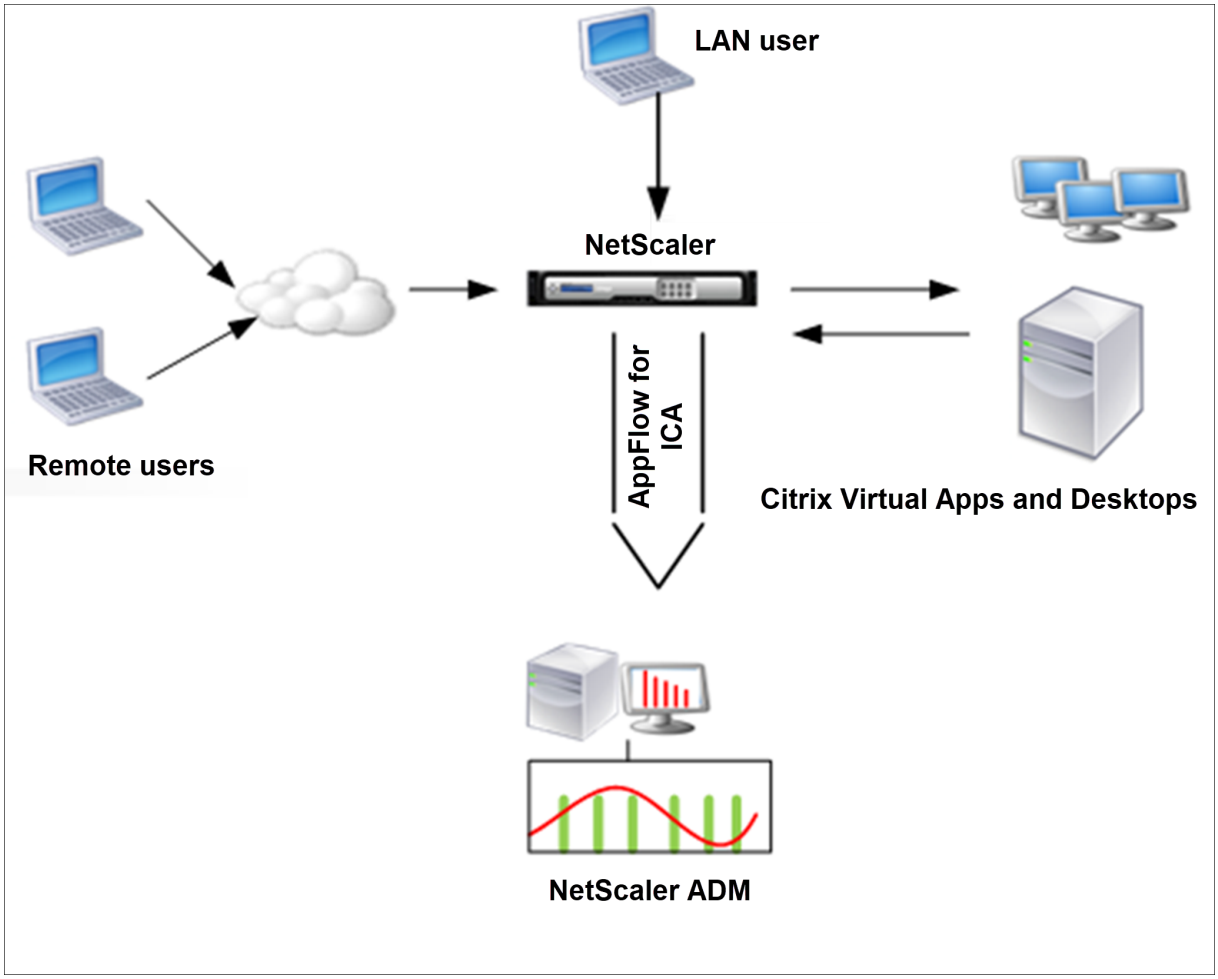
HDX Insight enables IT to deliver an exceptional user experience by providing unprecedented end-to-end visibility into the ICA traffic that passes through the NetScaler instances and is a part of NetScaler Application Delivery Management (ADM) Analytics. HDX Insight delivers compelling and powerful business intelligence and failure analysis capabilities for the network, virtual desktops, applications, and application fabric. HDX Insight can both instantly triage on user issues, collects data about virtual desktop connections, and generates AppFlow records and presents them as visual reports.

The configuration to enable data collection in the NetScaler differs with the position of the appliance in the deployment topology.

Enabling data collection for monitoring NetScalers deployed in LAN user mode

External users who access Citrix Virtual App and Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual App and Desktop applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.



> **Note** NetScaler ADM and NetScaler Gateway appliance reside in the same subnet.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow, and then view the reports on the dashboard.

After you add the NetScaler appliance to the NetScaler ADM inventory, you must enable AppFlow for data collection.

> **Note**
>
> - On an ADC instance, you can navigate to **Settings > AppFlow > Collectors**, to check if the collector (that is, NetScaler ADM) is up or not. NetScaler instance sends AppFlow records to NetScaler ADM using NSIP. But the instance uses its SNIP to verify connectivity with NetScaler ADM. So, ensure that the SNIP is configured on the instance.
> - You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler ADM configuration utility.
> - For detailed information about the commands and their usage, see Command Reference.
> - For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Example

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Note:** If you are accessing the LAN network by using a NetScaler Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Example

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Add NetScaler ADM as an AppFlow collector on the NetScaler appliance.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Create an AppFlow action and associate the collector with the action.

```
add appflow action <name> -collectors <string>
<!--NeedCopy-->
```

Example:


```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Example:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Example:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Note**
>
> The value of type must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Example:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Save the configuration. Type: `save ns config`

Enabling data collection for NetScaler Gateway appliances deployed in single-hop mode

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization.
In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler Application Delivery Management (ADM) inventory and enable AppFlow on ADM.

To enable the AppFlow feature from NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.
5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA**.
7. Click **OK**.

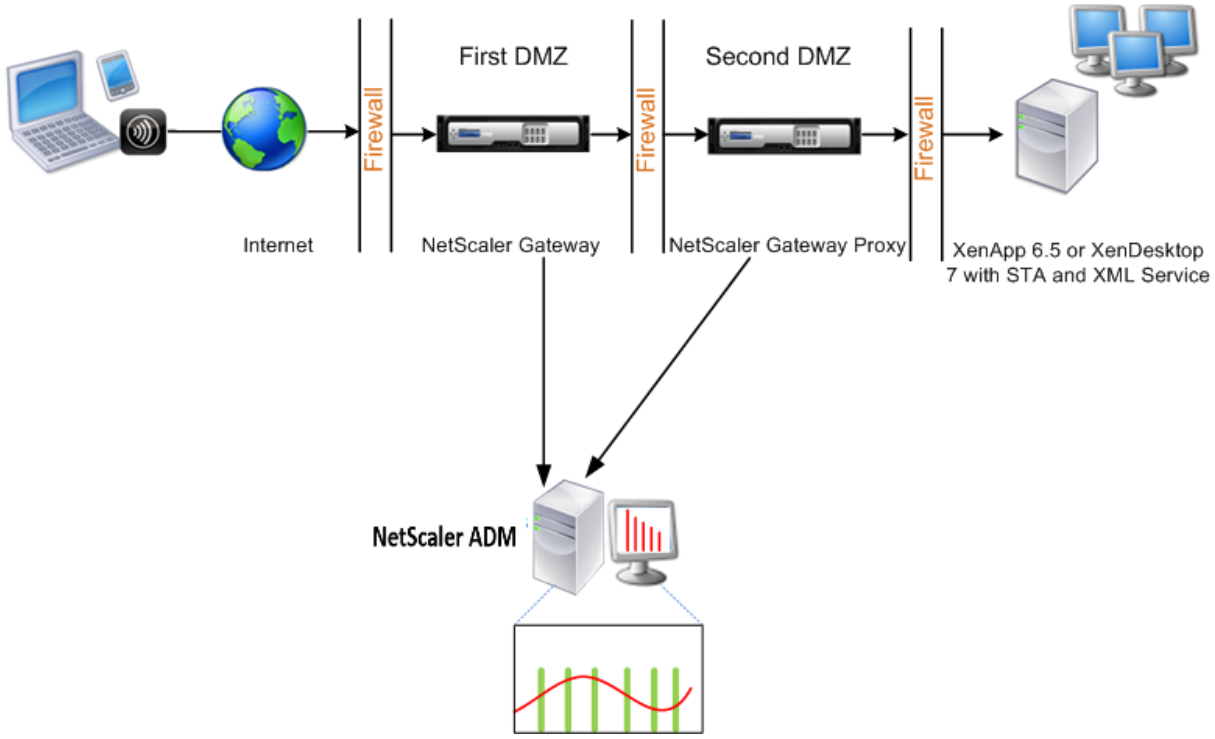
> **Note**
>
> when you enable AppFlow in single-hop mode, the following commands run in the background. These commands are explicitly specified here for troubleshooting purposes.

```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  enable ns feature AppFlow
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
20 <!--NeedCopy-->
```

EUEM virtual channel data is part of HDX Insight data that the NetScaler ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

Enabling data collection for NetScaler Gateway appliances deployed in double-hop mode

The NetScaler Gateway double-hop mode provides additional protection to an organization's internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler ADM so that the NetScaler Gateway appliances report these vital statistics.



The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler ADM can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler ADM and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler ADM collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler ADM inventory

and enable data collection, each of the appliances exports the reports by keeping track of the hop count and connection chain ID.

For NetScaler ADM to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of NetScaler Gateway appliances through which the traffic flows from a client to the servers. The connection chain ID represents the end- to end connections between the client and server.

NetScaler ADM uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler ADM inventory, enable AppFlow on NetScaler ADM, and then view the reports on the NetScaler ADM dashboard.

Configure HDX Insight on virtual servers used for Optimal Gateway

Steps to configure HDX Insight on virtual servers used for Optimal Gateway:

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the VPN virtual server configured for authentication, and click **Enable Analytics**.
4. Select **HDX Insight** and then select **ICA**.
5. Select other advanced options as required.
6. Click **OK**.
7. Repeat steps 3 through 6 on the other VPN virtual server.

Enable data collection on NetScaler ADM

If you enable NetScaler ADM to start collecting the ICA details from both the appliances, the details collected are redundant. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first NetScaler Gateway appliances, and then enable AppFlow for TCP on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow feature from NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, http://192.168.100.1).

2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.
5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA** or **TCP** for ICA traffic or TCP traffic respectively.

   > **Note**
   >
   > If AppFlow logging is not enabled for the respective services or service groups on the NetScaler appliance, the NetScaler ADM dashboard does not display the records, even if the Insight column shows Enabled.

7. Click **OK**.

Configuring NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler Gateway appliances to export the reports to NetScaler ADM:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

Configure NetScaler Gateway Using the Command Line Interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

```
1 add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
     ON or OFF)] [-imgGifToPng]
2
3 add vpn nextHopServer nh1 10.102.2.33 8443  – secure ON
4 <!--NeedCopy-->
```


2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1

<!--NeedCopy-->
```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 – doubleHop ENABLED – appFlowLog ENABLED
<!--NeedCopy-->
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 – type
    OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Enable the other NetScaler Gateway appliance to export ICA records:

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
<!--NeedCopy-->
```

7. Enable connection chaining on both the NetScaler Gateway appliances:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configure NetScaler Gateway using Configuration Utility:

1. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway

in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand **Published Applications**.

c) Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

2. Enable double hop on the NetScaler Gateway in the second DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand more, select **Double Hop** and click **OK**.

3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More**, and clear **Enable Authentication**.

4. Enable one of the NetScaler Gateway appliances to export TCP records.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.

c) Click the + icon and from the **Choose Policy** list, select **AppFlow**, and from the **Choose Type** list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

5. Enable the other NetScaler Gateway appliance to export ICA records:

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Advanced** group, expand **Policies**.

c) Click the + icon and from the **Choose Policy** list, select AppFlow, and from theChoose Type list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

6. Enable connection chaining on both the NetScaler Gateway appliances.

a) On the **Configuration** tab, navigate to **System** > **Appflow**.

b) In the right Pane, in the **Settings** group, double-click **Change Appflow Settings**.

c) Select **Connection Chaining** and Click **OK**.

7. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.

a) On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Advanced group**, expand **Published Applications**.

c) Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

8. Enable double hop on the NetScaler Gateway in the second DMZ.

a) On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand More, select **Double Hop**, and click **OK**.

9. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.

a) On the Configuration tab expand NetScaler Gateway and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More**, and clear **Enable Authentication**.

10. Enable one of the NetScaler Gateway appliances to export TCP records.

a) On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand **Policies**.

c) Click the **+** icon and from the Choose Policy list, select AppFlow, and from the **Choose Type** list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

11. Enable the other NetScaler Gateway appliance to export ICA records.

a) On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand **Policies**.

c) Click the **+** icon and from the **Choose Policy** list, select AppFlow, and from the **Choose Type** list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

12. Enable connection chaining on both the NetScaler Gateway appliances.

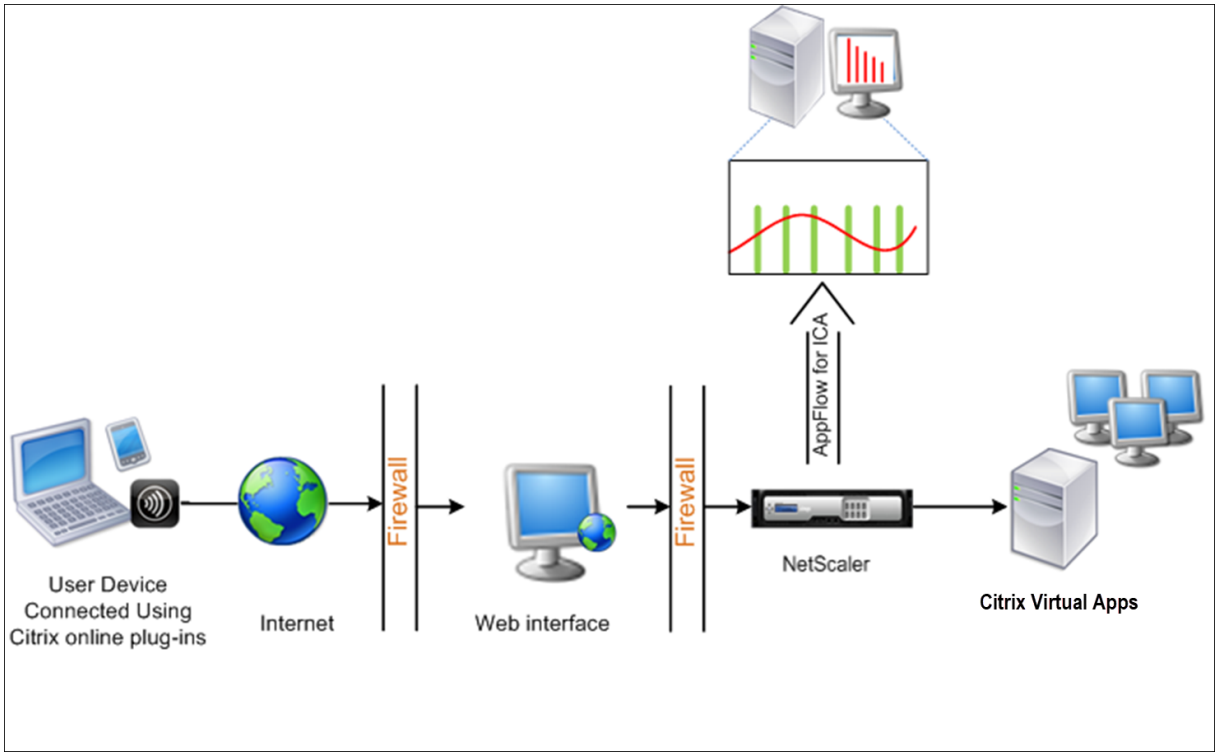
Enable data collection for monitoring NetScalers deployed in transparent mode

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a Citrix Virtual Apps and Desktop environment, the ICA traffic is not transmitted over a VPN.

After you add the NetScaler to the NetScaler ADM inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler ADM as an AppFlow collector on each NetScaler appliance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

> **Note**
>
> - You cannot enable data collection on a NetScaler deployed in transparent mode by using the NetScaler ADM configuration utility.
> - For detailed information about the commands and their usage, see Command Reference.
> - For information on policy expressions, see Policies and Expressions.

The following figure shows the network deployment of a NetScaler ADM when a NetScaler is deployed in a transparent mode:



To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

Example:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Note**
>
> - You can specify up to 10 ports with this command.
> - The default port number is 2598. You can modify the port number as required.

3. Add NetScaler Insight Center as an AppFlow collector on the NetScaler appliance.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Note** To view the AppFlow collectors configured on the NetScaler appliance, use the **show appflow collector** command.

4. Create an AppFlow action and associate the collector with the action.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Example:

add AppFlow action act-collectors MyInsight

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Example:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Example:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Note**
>
> The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Example:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

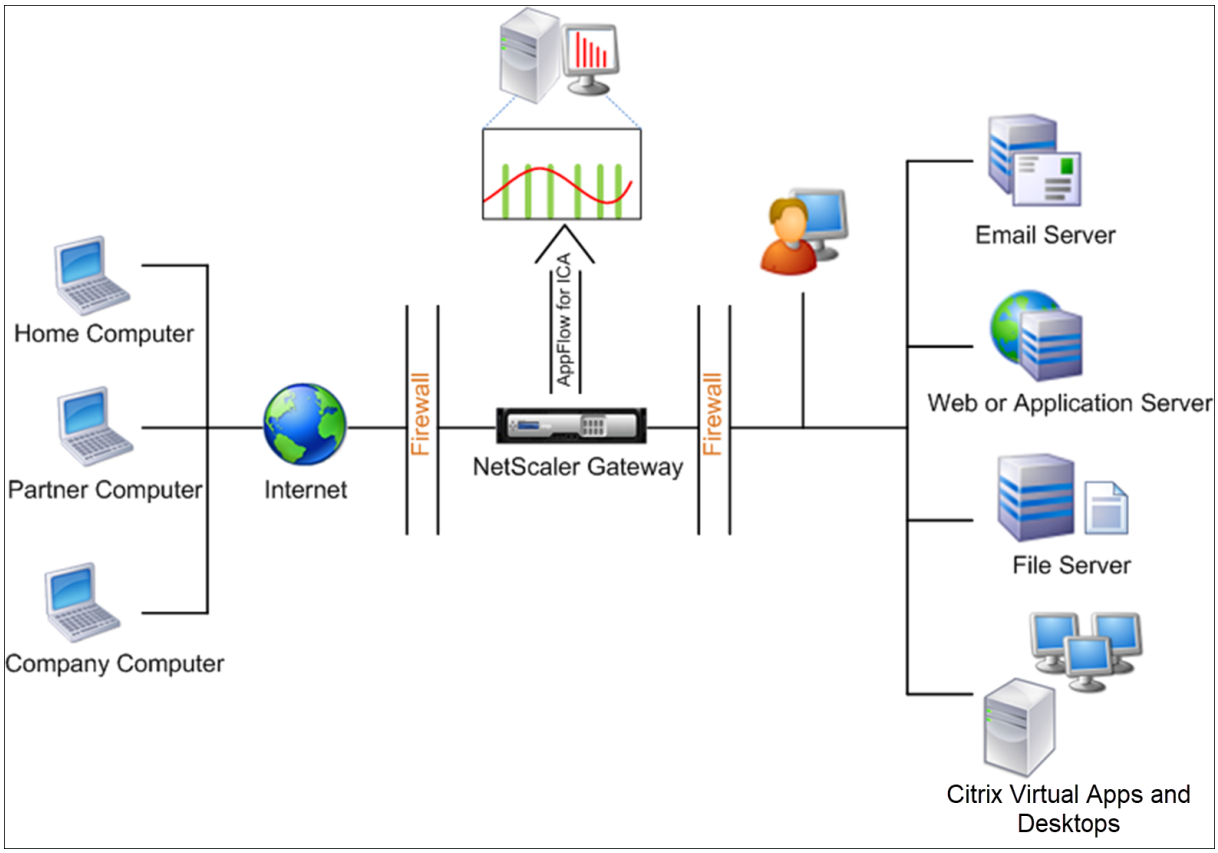
8. Save the configuration. Type: `save ns config`

Enable data collection for NetScaler Gateway appliances deployed in single-hop mode

March 11, 2024

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization.
In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler Application Delivery Management (ADM) inventory and enable AppFlow on ADM.



To enable the AppFlow feature from ADM:

1. Navigate to **Infrastructure** > **Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Action** list, select **Enable/Disable Insight**.
3. Select the **VPN virtual servers**, and click **Enable AppFlow**.

4. In the **Enable AppFlow** field, type **true**, and select **ICA**.
5. Click **OK**.

> **Note**
>
> When you enable AppFlow in single-hop mode, the following commands run in the background. These commands are explicitly specified here for troubleshooting purposes.
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`
> - `set appflow policy \<name\> -rule \<expression\>`
> - `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
> - `set vpn vserver \<name\> -appflowLog ENABLED`
> - `save ns config`

EUEM virtual channel data is part of HDX Insight data that the NetScaler ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

Enable data collection to monitor NetScalers deployed in transparent mode

March 11, 2024

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler is deployed in transparent mode in a Citrix Virtual Apps and Desktops environment, the ICA traffic is not transmitted over a VPN.

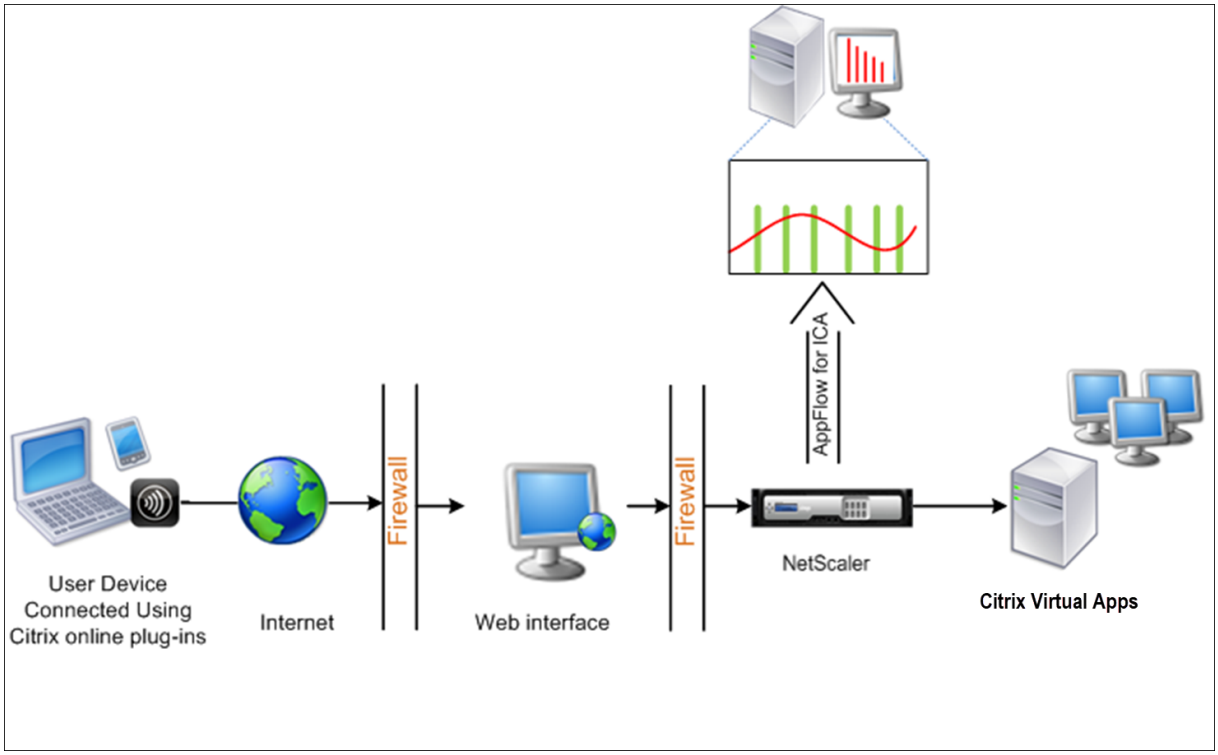
After you add the NetScaler to the NetScaler ADM inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler ADM as an AppFlow collector on each NetScaler instance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

> **Note**
>
> - You cannot enable data collection on a NetScaler deployed in transparent mode by using

the NetScaler ADM configuration utility.

- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

The following figure shows the network deployment of a NetScaler ADM when a NetScaler is deployed in a transparent mode:



To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

Example:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

Note

- You can specify up to 10 ports with this command.
- The default port number is 2598. You can modify the port number as required.

3. Add NetScaler Insight Center as an AppFlow collector on the NetScaler instance.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Note** To view the AppFlow collectors configured on the NetScaler instance, use the **show appflow collector** command.

4. Create an AppFlow action and associate the collector with the action.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Example:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Example:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Example:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Note**
>
> The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```


8. Save the configuration.

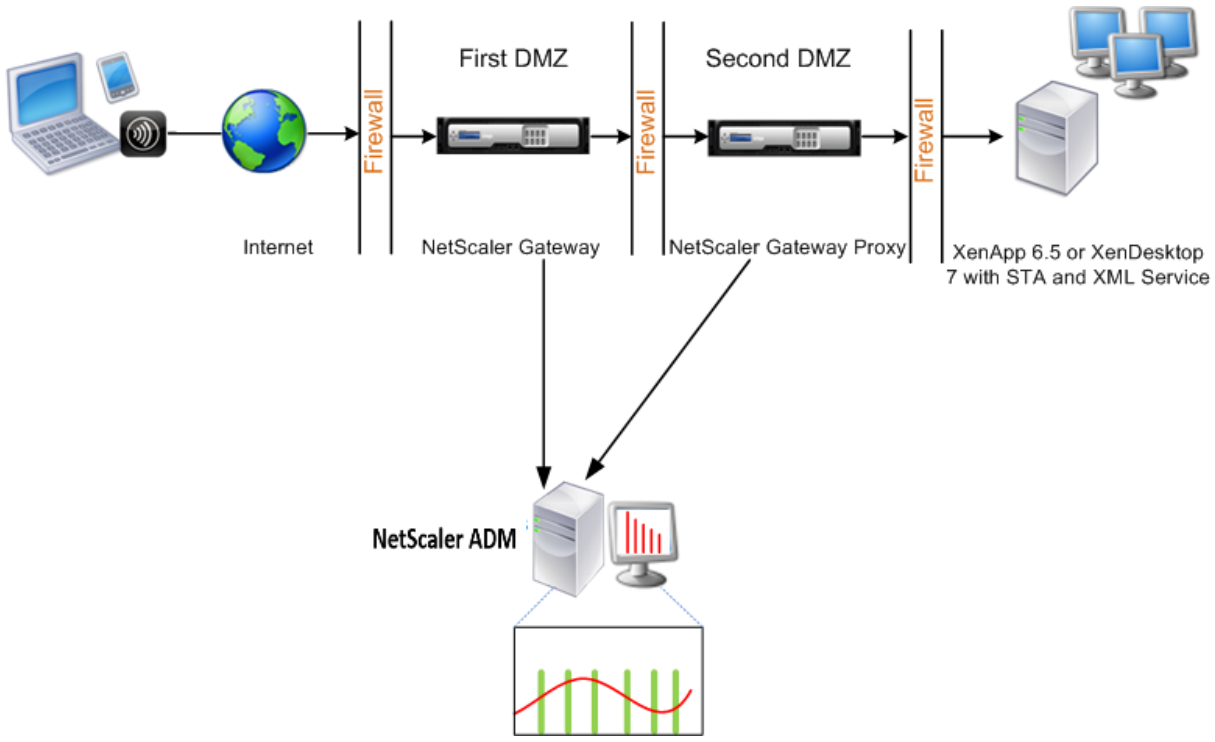
```
save ns config
<!--NeedCopy-->
```

Enable data collection for NetScaler Gateway appliances deployed in double-hop mode

March 11, 2024

The NetScaler Gateway double-hop mode provides extra protection to an organization's internal network, because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler ADM, so that the NetScaler Gateway appliances report these vital statistics.

Figure 3. NetScaler ADM deployed in double-hop mode



The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler ADM can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler ADM and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler ADM collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler ADM inventory and enable data collection, each appliance exports the reports by keeping track of the hop count and connection chain ID.

For NetScaler ADM to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of NetScaler Gateway appliances through which the traffic flows from a client to the servers. The connection chain ID represents the end- to end connections between the client and server.

NetScaler ADM uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler ADM inventory, enable AppFlow on NetScaler ADM, and then view the reports on the NetScaler ADM dashboard.

Enable data collection on NetScaler ADM

If you enable NetScaler ADM to start collecting the ICA details from both the appliances, the details collected are redundant. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for TCP on one of the first NetScaler Gateway appliances, and then enable AppFlow for ICA on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow feature from NetScaler ADM:

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Action** list, select **Enable/Disable Insight**.
3. Select the VPN virtual servers, and click **Enable AppFlow**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA/TCP** for ICA traffic a TCP traffic respectively.

> **Note**
>
> If AppFlow logging is not enabled for the services or service groups on the NetScaler appliance, the NetScaler ADM dashboard does not display the records, even if the Insight column shows Enabled.

5. Click **OK**.

Configure NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler Gateway appliances to export the reports to NetScaler ADM:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

Configure NetScaler Gateway using the command line interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
<!--NeedCopy-->
```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```


3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

set vpn vserver [**- doubleHop** (DISABLED)] [**- appflowLog** (DISABLED)] ENABLED ENABLED

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
<!--NeedCopy-->
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
<!--NeedCopy-->
```

6. Enable the other NetScaler Gateway appliance to export ICA records:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA\
   _REQUEST
<!--NeedCopy-->
```

7. Enable connection chaining on both the NetScaler Gateway appliances:

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configuring NetScaler Gateway using configuration utility:

1. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand **Published Applications**.

c) Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

2. Enable double hop on the NetScaler Gateway in the second DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More** , select **Double Hop** and click **OK**.

3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More**, and clear **Enable Authentication**.

4. Enable one of the NetScaler Gateway appliances to export TCP records.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.

c) Click the + icon and from the **Choose Policy** list, select **AppFlow**, and from the **Choose Type** drop-down list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

5. Enable the other NetScaler Gateway appliance to export ICA records:

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Advanced** group, expand **Policies**.

c) Click the + icon and from the **Choose Policy** drop-down list, select **AppFlow**, and from theChoose Type drop-down list, select **Other TCP Request**.

d) Click **Continue**.

e) Add a policy binding, and click **Close**.

6. Enable connection chaining on both the NetScaler Gateway appliances.

a) On the **Configuration** tab, navigate to **Settings > Appflow**.

b) In the right Pane, in the **Settings** group, click **Change Appflow Settings**.

c) Select **Connection Chaining** and Click **OK**.

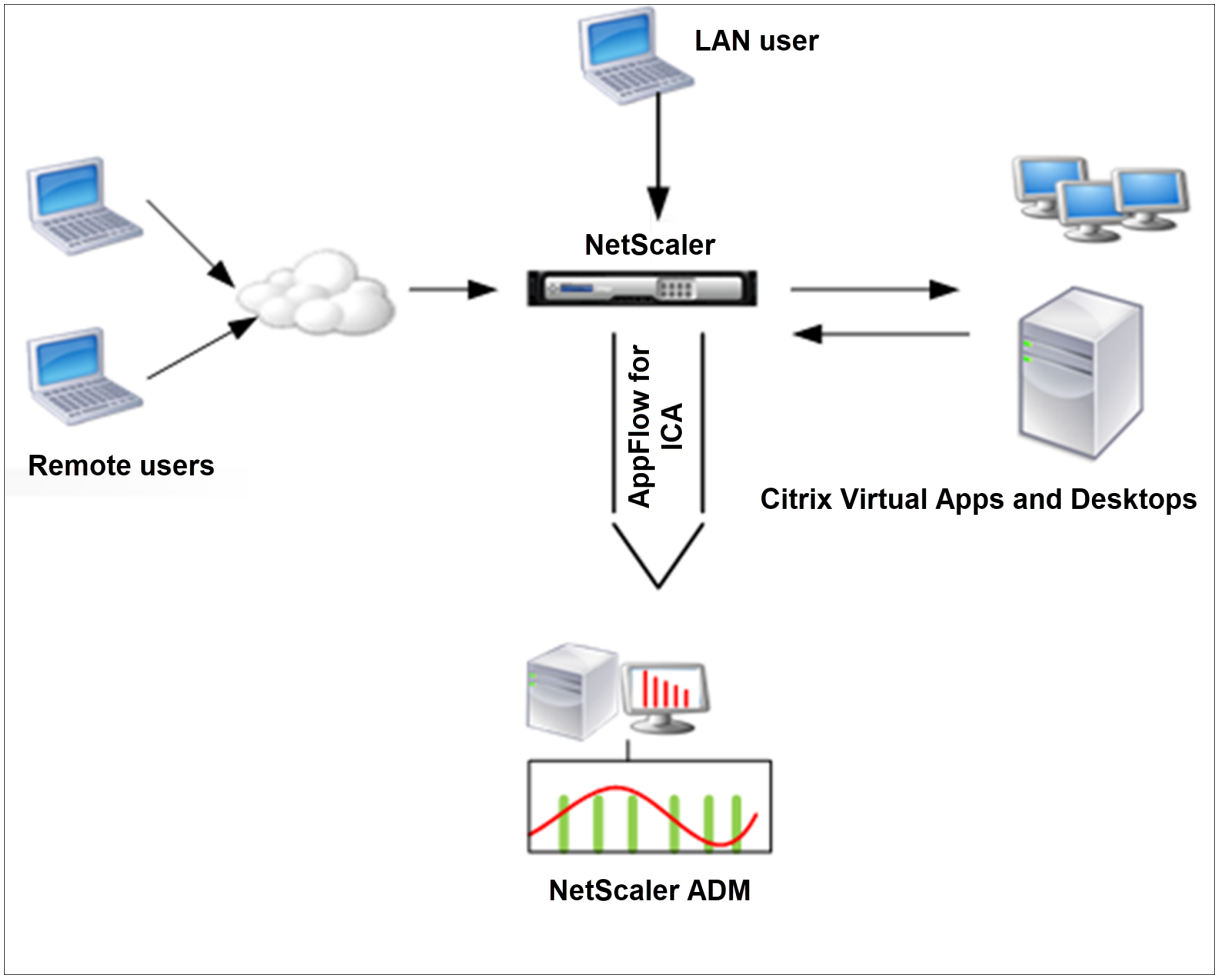
Enable data collection to monitor NetScalers deployed in LAN user mode

March 11, 2024

External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual Apps and Desktops applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

Figure 4. NetScaler ADM deployed in LAN User Mode



Note NetScaler ADM and NetScaler Gateway appliance reside in the same subnet.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow, and then view the reports on the dashboard.

After you add the NetScaler appliance to the NetScaler ADM inventory, you must enable AppFlow for data collection.

> **Note**
>
> - You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler ADM configuration utility.
> - For detailed information about the commands and their usage, see Command Reference.
> - For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.

2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Example:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Note** If you are accessing the LAN network by using a NetScaler Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

Example:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Add NetScaler ADM as an AppFlow collector on the NetScaler appliance.

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
<!--NeedCopy-->
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Create an AppFlow action and associate the collector with the action.

```
add appflow action** \<name\> **-collectors** \<string\> ...
<!--NeedCopy-->
```

Example:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```



```
<!--NeedCopy-->
```

Example:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type
    \>
<!--NeedCopy-->
```

Example:

```
bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
<!--NeedCopy-->
```

> **Note**
>
> The value of type must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Example:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Save the configuration.

```
save ns config
<!--NeedCopy-->
```

Create thresholds and configure alerts for HDX Insight

March 11, 2024

HDX Insight on NetScaler Application Delivery Management (ADM) allows you to monitor the HDX traffic passing through NetScaler instances. NetScaler ADM allows you to set thresholds on various counters used to monitor the Insight traffic. You can also configure rules and create alerts in NetScaler ADM.

HDX traffic type is associated with various entities such as applications, desktops, gateways, licenses, and users. Every entity can contain different metrics associated with them. For example, application entity is associated with various hits, bandwidth consumed by the application, and response time of the server. A user entity can be associated with WAN latency, DC latency, ICA RTT, and bandwidth consumed by a user.

The threshold management for HDX Insight in NetScaler ADM allowed you to proactively create rules and configure alerts whenever the thresholds set are breached. Now, this threshold management is extended to configure a group of threshold rules. You can now monitor the group instead of individual rules. A threshold rule group comprises one or more user-defined threshold rules for metrics chosen from entities such as users, applications, and desktops. Each rule is monitored against an expected value that you enter when you create the rule. In case of users entity, the threshold group can be associated with a geolocation as well.

An alert is generated on NetScaler ADM only if all the rules in the configured threshold group are breached. For example, you can monitor an application on total session launch count and also on application launch count as one threshold group. An alert is generated only if both rules are breached. This allows you to set more realistic thresholds on an entity.

A few examples are listed as follows:

- Threshold rule1: ICA RTT(metric) for users(entity) must be <= 100 ms
- Threshold rule2: WAN Latency (metric) for users(entity) must be <= 100 ms

An example of threshold group can be: {Threshold rule 1 + Threshold rule 2}

To create a rule, you must first select the entity that you want to monitor. Then choose a metric while creating a rule. For example, you can select applications entity and then select Total Session Launch count or App Launch Count. You can create one rule for every combination of an entity and a metric. Use the comparators provided (>, <, >=, and <=) and type a threshold value for each metric.

> **Note**
>
> If you do not want to monitor multiple entities in a single group, you must create a separate threshold rule group for each entity.

When the value of a counter exceeds the value of a threshold, NetScaler ADM generates an event to signify a threshold breach, and an alert is created for every event.

You must configure how you receive the alert. You can enable the alert to be displayed on NetScaler ADM and/or receive the alert as an email or as an SMS on your mobile device. For the last two actions, you must configure the email server or the SMS server on NetScaler ADM.

Threshold groups can also be bound to Geolocations for geo-specific monitoring for user entity.

Example Use cases

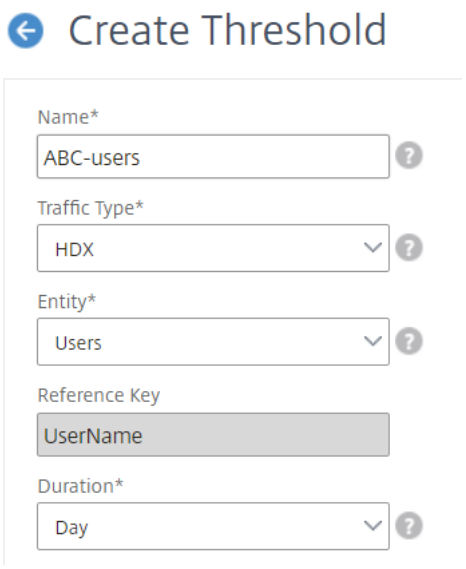
ABC Inc. is a global firm and has offices in over 50 countries. The firm has two data centers, one in Singapore and other in California that host the Citrix Virtual Apps and Desktops. Employees of the firm access the Citrix Virtual Apps and Desktops throughout the globe using NetScaler Gateway and Citrix GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc. wants to track the user experience for all their offices to optimize the apps and desktop delivery for anywhere, anytime access. Eric also wants to check the user-experience-metrics like ICA RTTs, latencies, and raise any deviations proactively.

The users of ABC Inc. have a distributed presence. Some users are located close to the data center, while a few are located at further away from the data center. As the user base is distributed widely, the metrics and the corresponding thresholds also vary among these locations. For example, the ICA RTT for a location near to the data center can be 5–10 ms whereas the same for a remote location can be around 100 ms.

With threshold rule group management for HDX Insight, Eric can set geo-specific threshold rule groups for each location and be alerted through email or SMS for breaches per area. Eric is also able to combine tracking of more than one metric within a threshold rule group and narrow down the root cause to capacity issues if any. Eric is now able to proactively track any deviation without having to worry about the complexity of manually looking through all Citrix Virtual Apps and Desktops portfolio metrics.

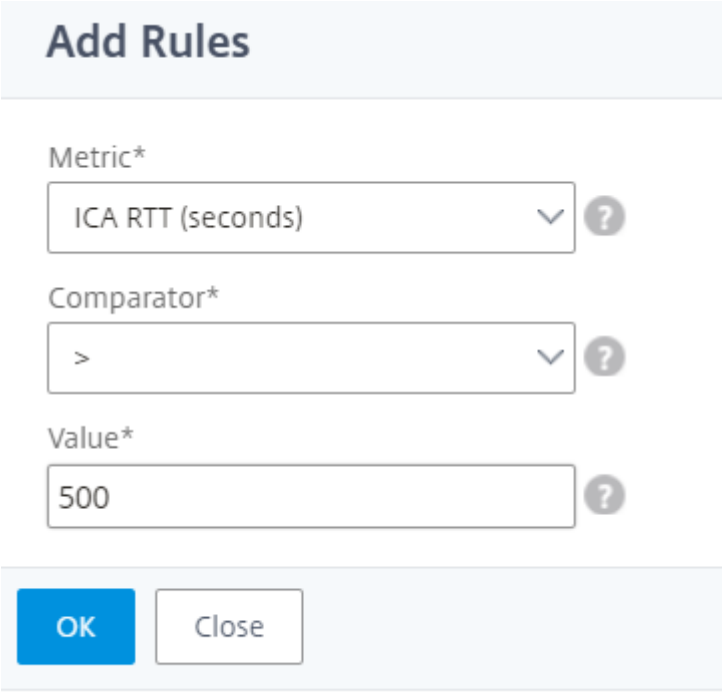
To create a threshold rule group and configure alerts for HDX Insight using NetScaler ADM:

1. In NetScaler ADM, navigate to **Settings > Analytics Settings > Thresholds**. On **Thresholds** page that opens, click **Add**.
2. On the **Create Thresholds and Alerts** page, specify the following details:
    a) **Name**. Type in a name for creating an event for which NetScaler ADM generates an alert.
    b) **Traffic Type**. From the list box, select HDX.
    c) **Entity**. From the list box, select the category or the resource type. The entities differ for each traffic type that you have selected earlier.
    d) **Reference Key**. A reference key is automatically generated based on the traffic type and entity that you have selected.
    e) **Duration**. From the list box, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.

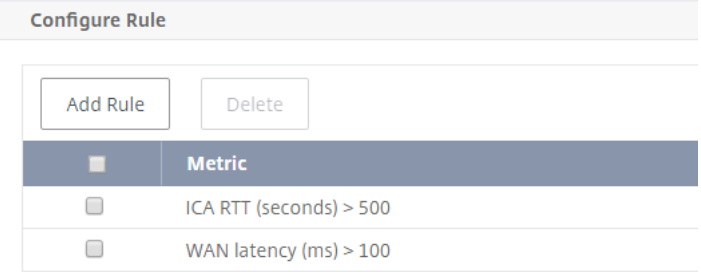


3. Creating threshold rules group for all entities:

   For HDX traffic, you must create a rule by clicking **Add Rule. E**nter the values in the **Add Rules** pop-up window that opens.

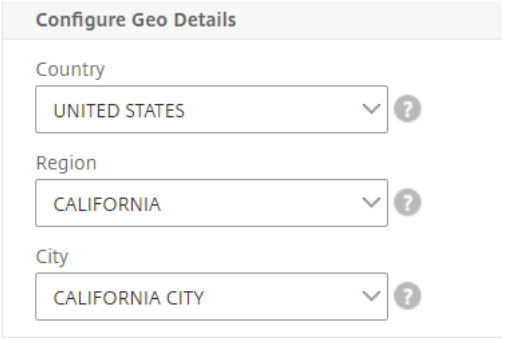


   You can create multiple rules to monitor each entity. Creating multiple rules in one single group allows you to monitor the entities as a group of threshold rules instead of individual rules. Click **OK** to close the window.



4. Configuring Geolocation tagging for Users entity

   Optionally, you can create a location-based alert for the user entity in the **Configure Geo Details** section. The following image shows an example of creating a geolocation based tagging to monitor WAN latency performance for users on the west coast of the United States.



5. Click **Enable Thresholds** to allow NetScaler ADM to start monitoring the entities.
6. Optionally, configure actions such as email notifications and SMS notifications.
7. Click **Create** to create a threshold rule group.

Viewing HDX Insight reports and metrics

March 11, 2024

HDX insight provides complete visibility of the reports and metrics pertaining to HDX traffic on your NetScaler instances.

You can view the HDX metrics for any selected entity. The views include the following categories of entities:

- **Users**: Displays the reports for all the users accessing the Citrix Virtual App or Desktop within the selected time interval.

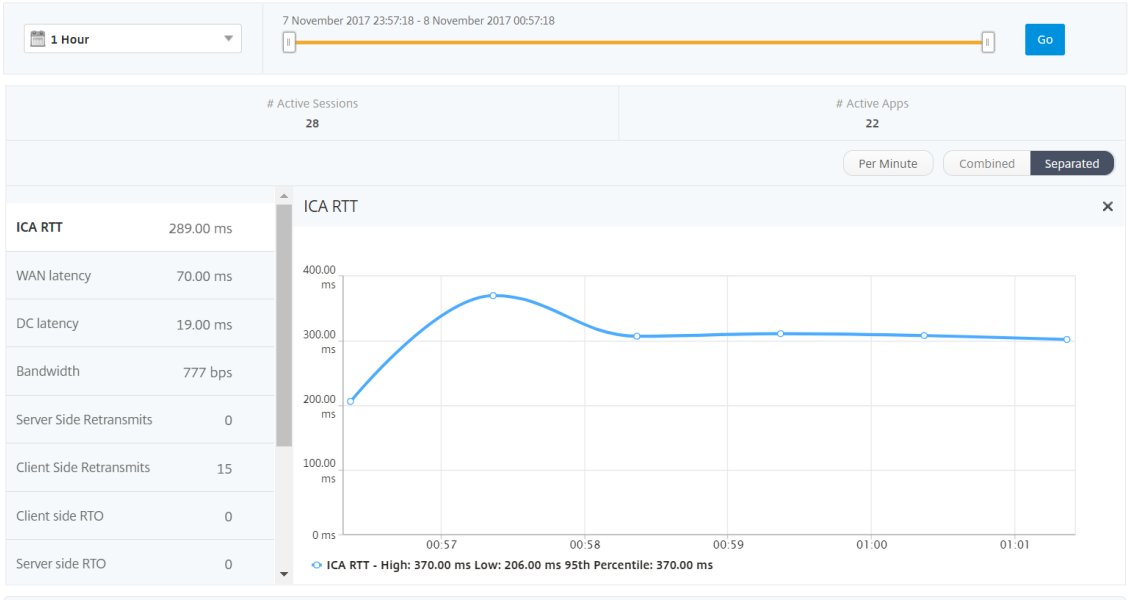
- **Applications:** Displays the reports for total number of applications, and all related relevant information like the total number of times the applications were launched within the specified time interval.
- **Instances**: Displays the reports on the NetScaler instances that act as gateways for incoming traffic.
- **Desktops**: Displays the reports for the desktops used in the selected time frame.
- **Licenses**: Displays the reports for total SSL VPN licenses used within the specified time slot.

User view reports and metrics

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktops user.

To navigate to the users view:

1. Navigate to **Gateway > HDX Insight > Users**



User view reports and metrics consist of the following sections:

- Summary View
- Per User View
- Per User Session View

Summary view

The summary view displays the reports for all the users that have logged in during the selected timeline. All the metrics/reports in this view display the values corresponding to them for the selected

time period unless specified otherwise.

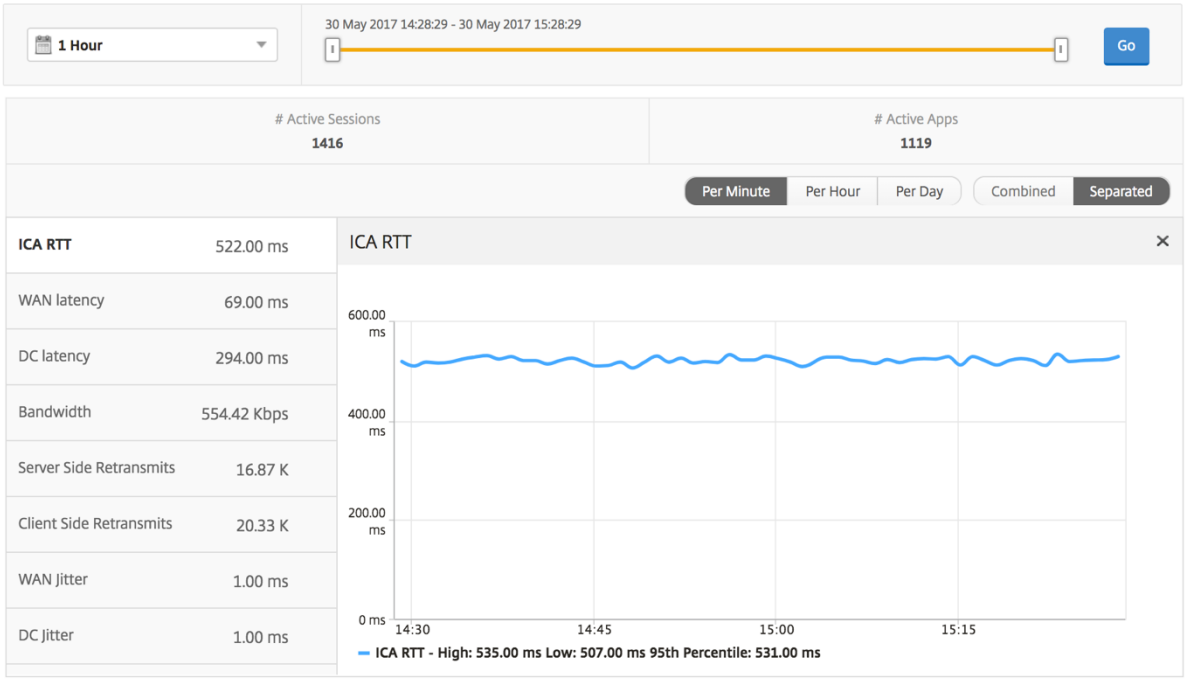
To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI OR CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

Metrics	Description
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



User summary report Following are the metrics that are specific to this report.

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

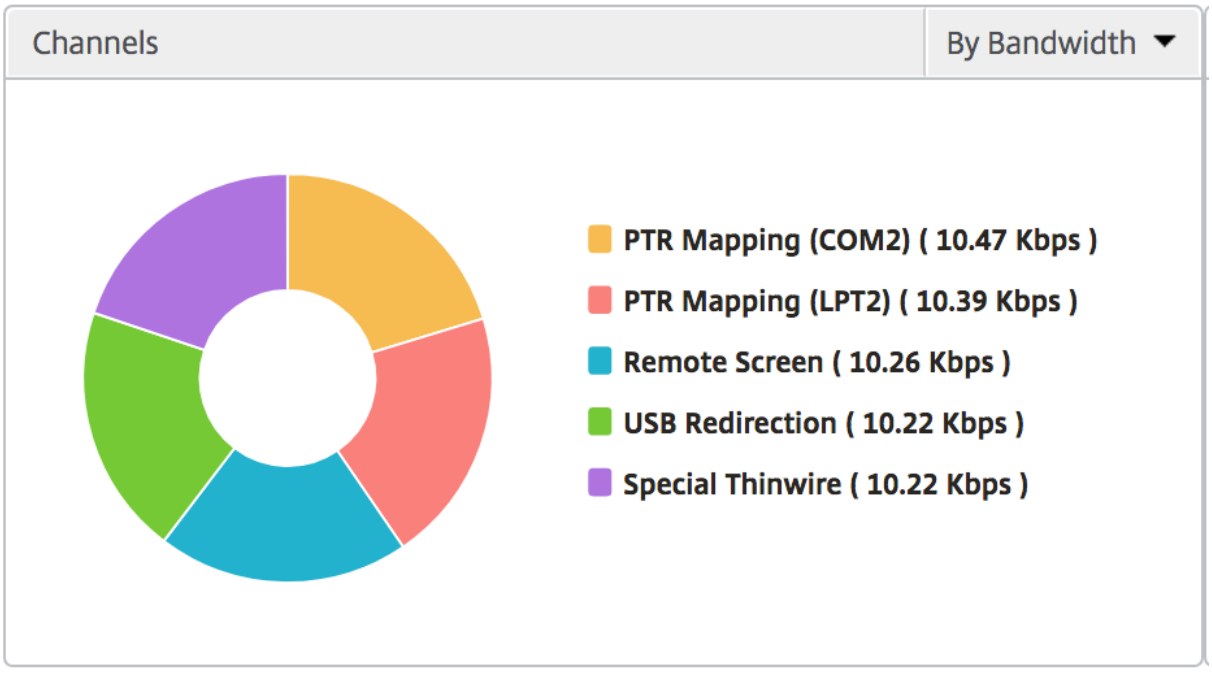
Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

Users

Search

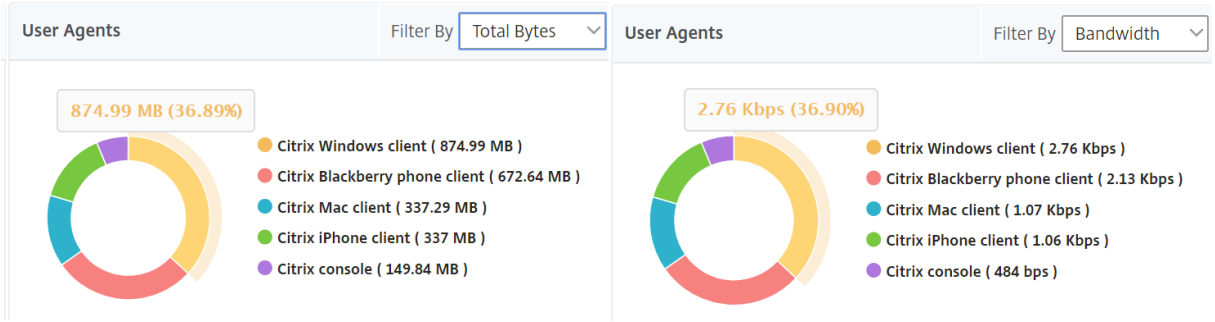
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

Channels Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

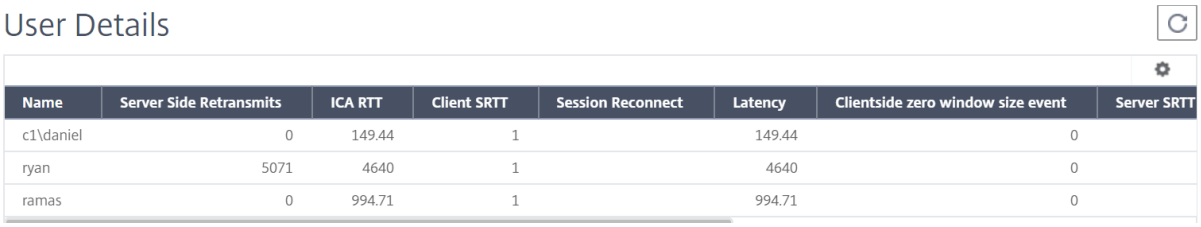


User agents User agents represent the overall bandwidth/total bytes consumed by each workspace client in the form of a doughnut chart. Each colored segment in the chart represents one workspace

client. The length of the segment depends on the number of users launching their applications on that workspace client. You can also sort the metrics by bandwidth, or total bytes.



Click each segment to view the details of the users using that workspace client.



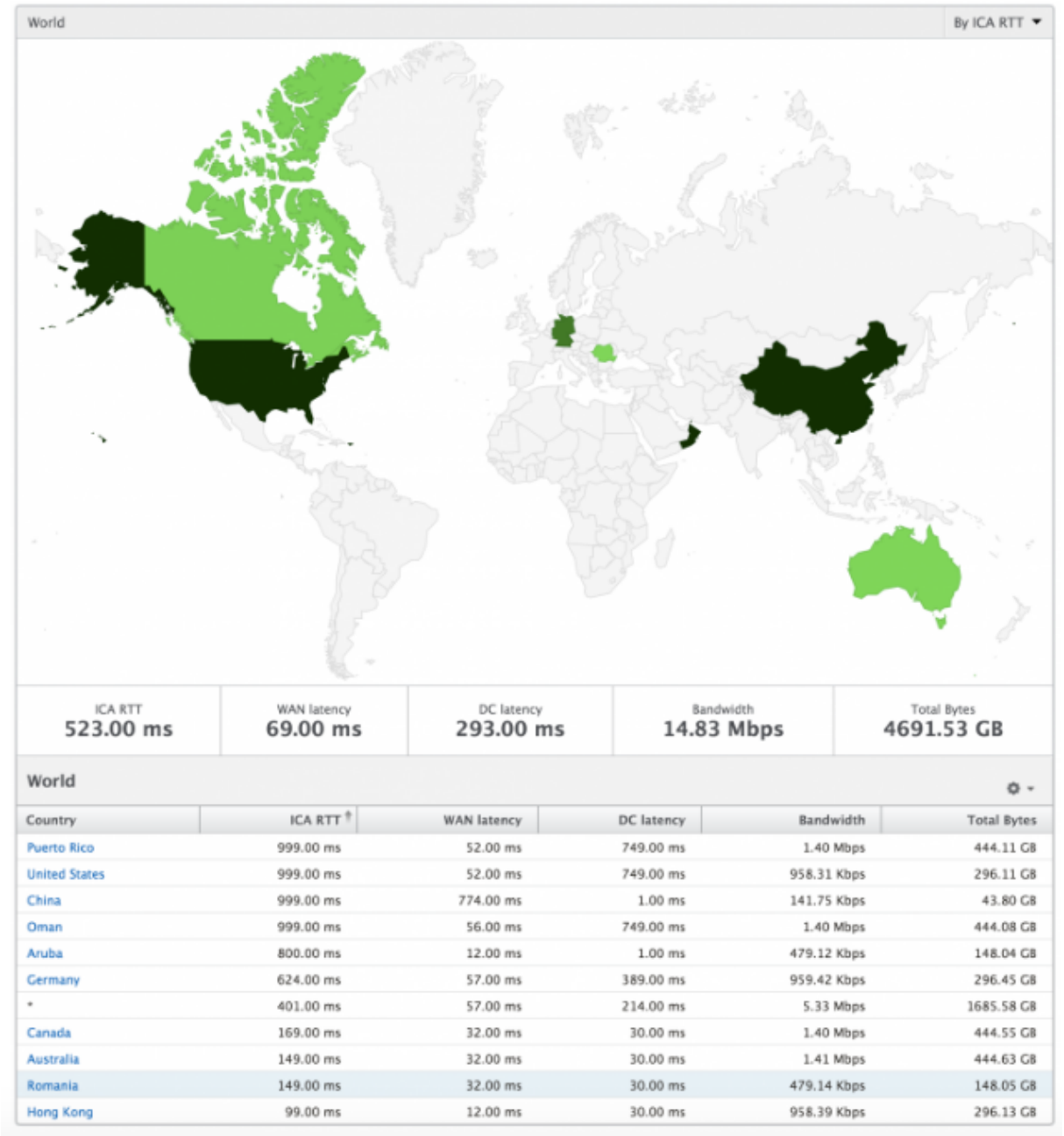
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

Thresholds breach count The Thresholds breach count metrics represent the count of thresholds breached in the selected time period.

World map The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per User view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the Users summary report.

Line chart Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.

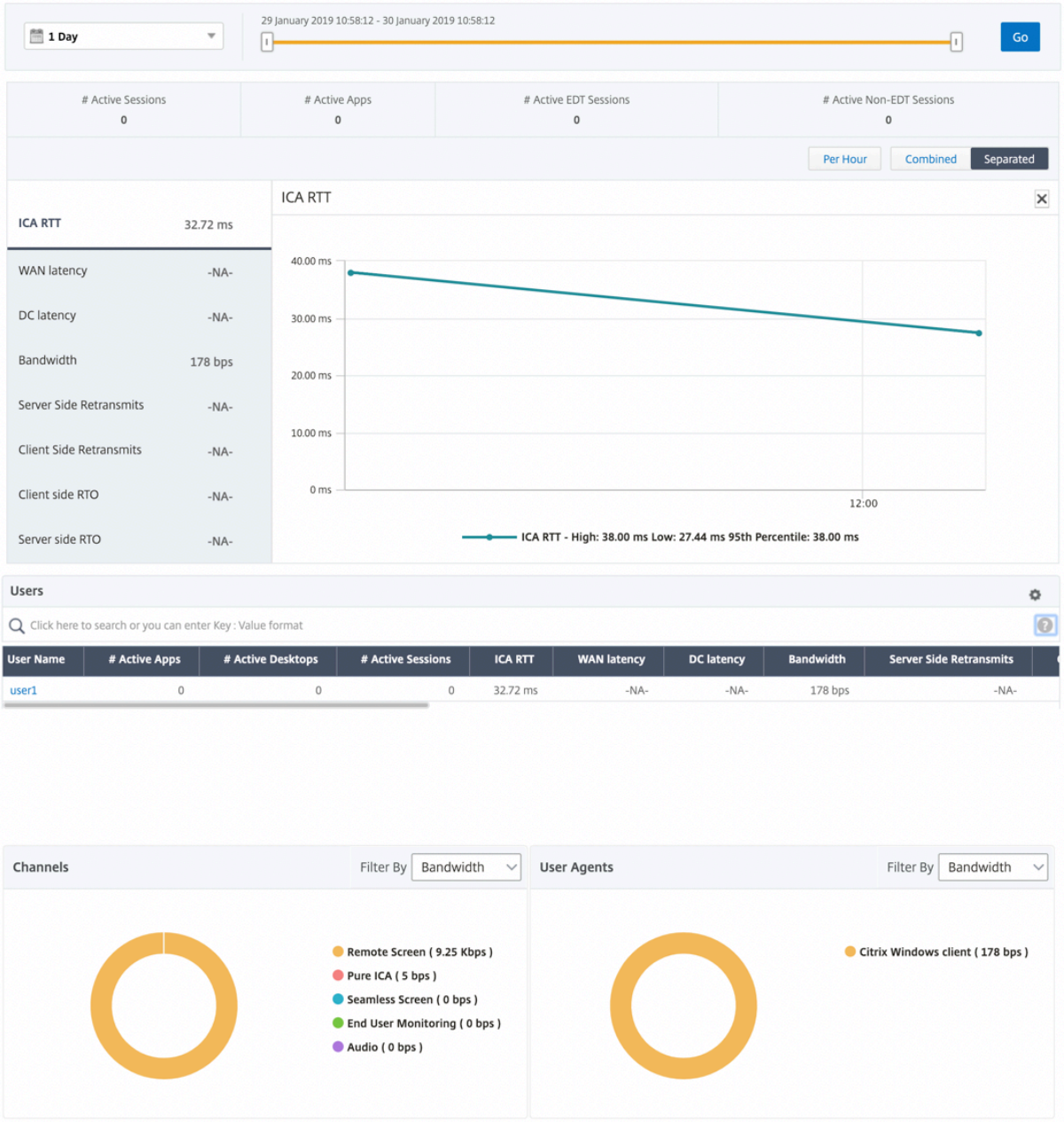
Metrics	Description
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

Metrics	Description
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.

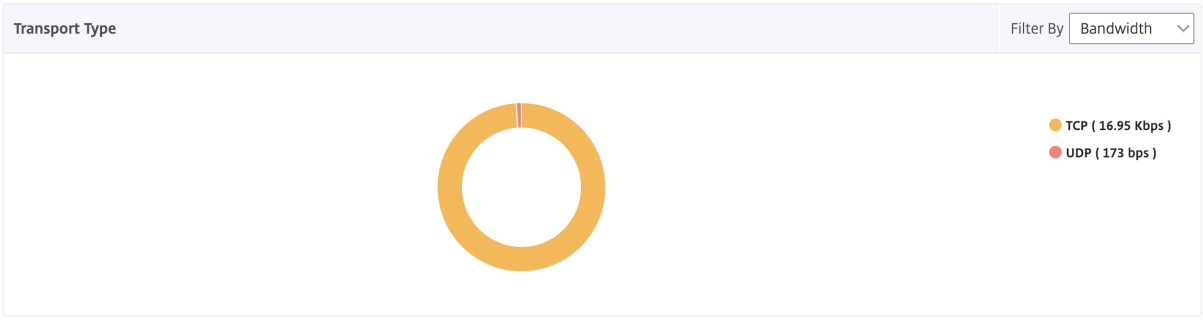
Support for EDT in HDX insight

NetScaler Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol. EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".



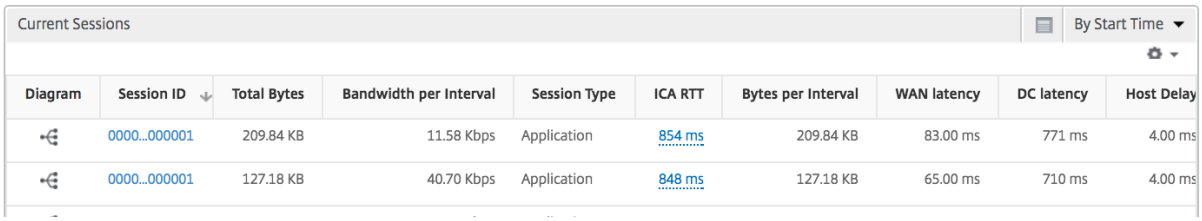
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.

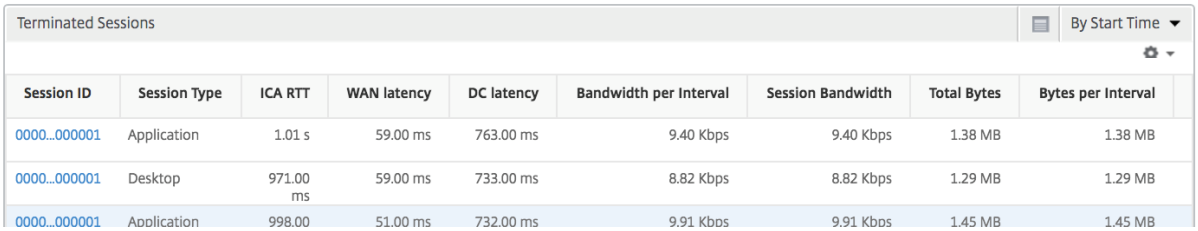


> **Note**
>
> EDT in HDX Insight is supported on NetScaler ADM from release 12.1 build 50.28 and is available on ADC instances from release 12.1 build 49.23.

HDX Insight metrics available from NetScaler ADM 12.0 and later:

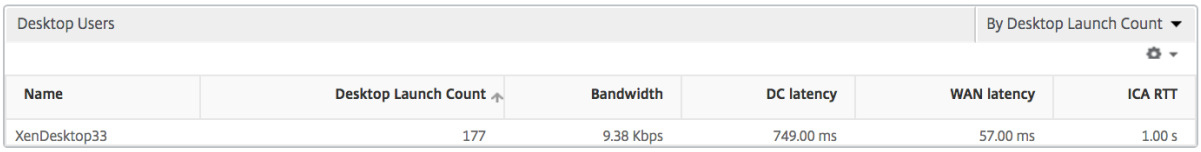
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.



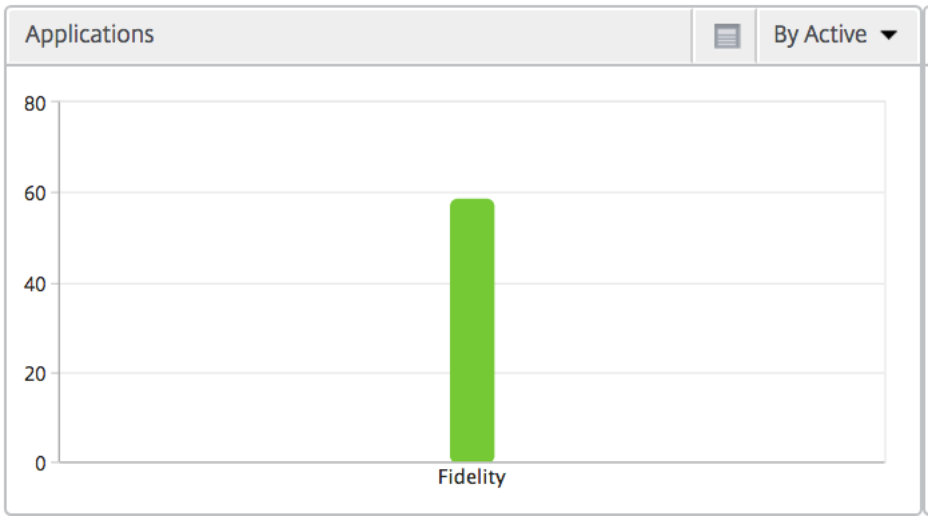


Desktop users This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

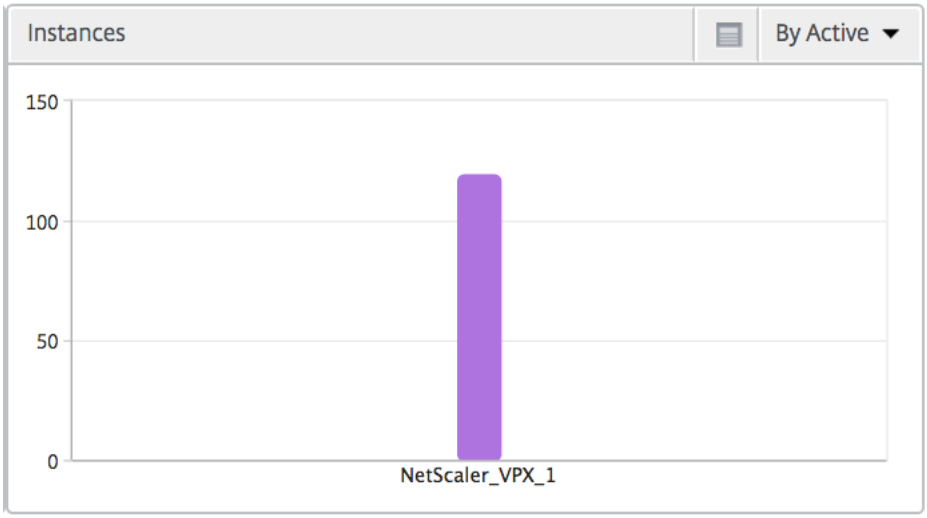
Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



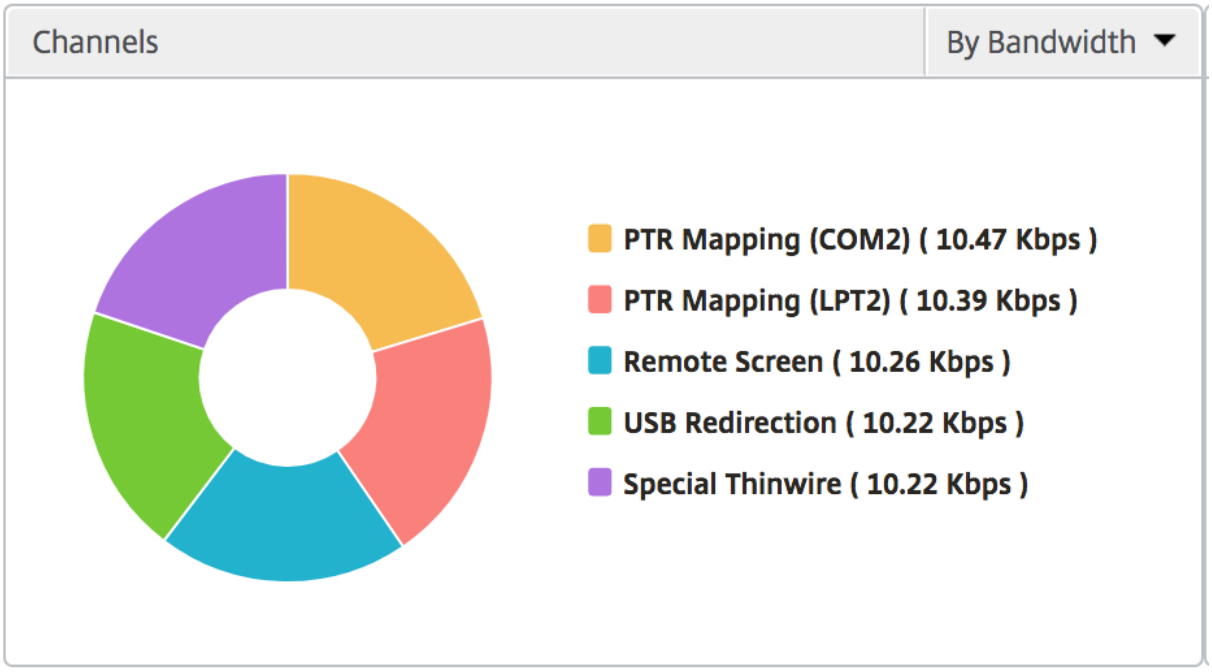
Applications A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.



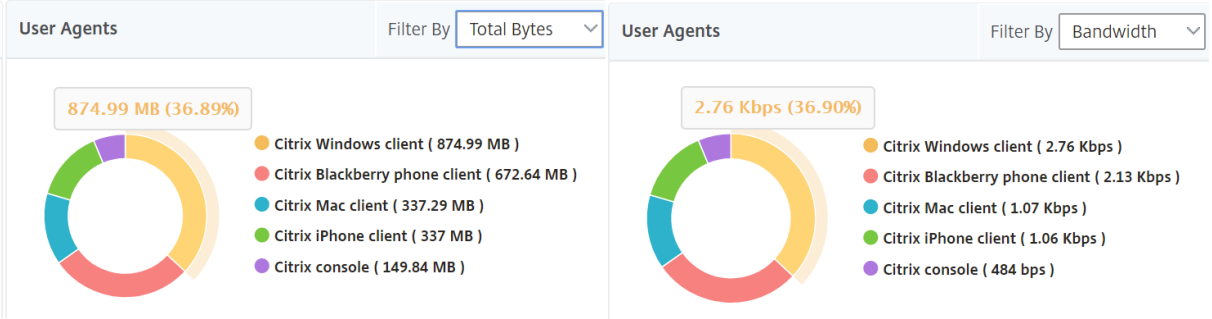
Instances A bar graph representing NetScaler instances sorted by Active and total apps



Channels Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



User agents User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



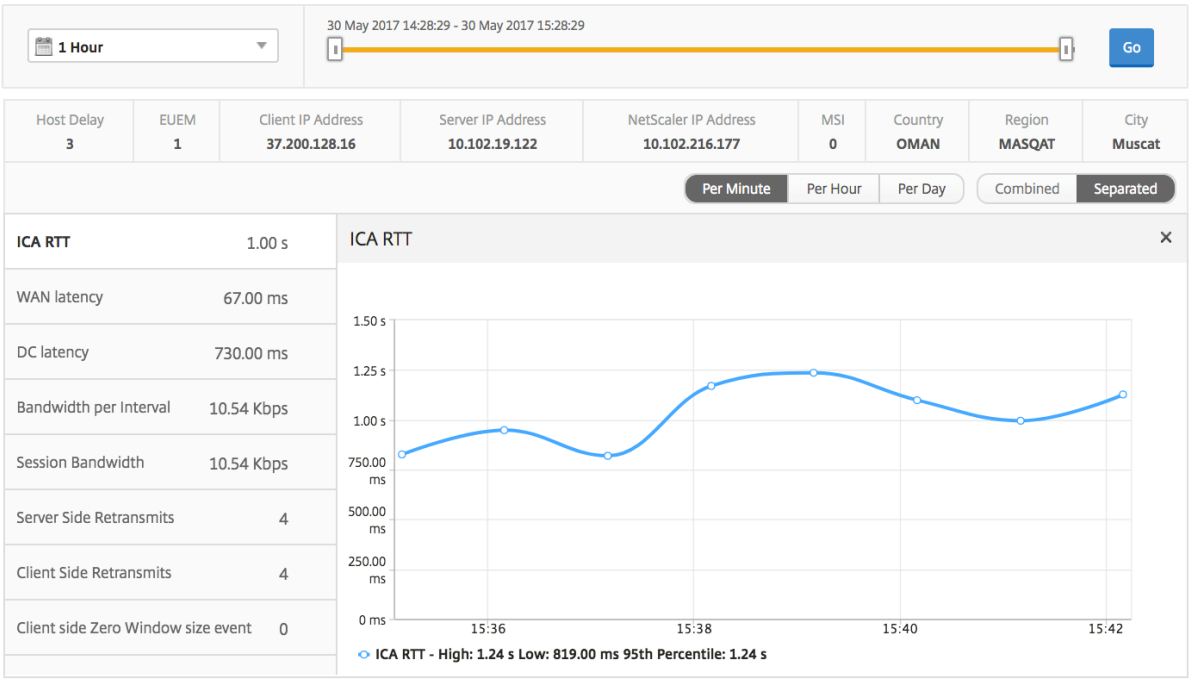
Per User session view The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

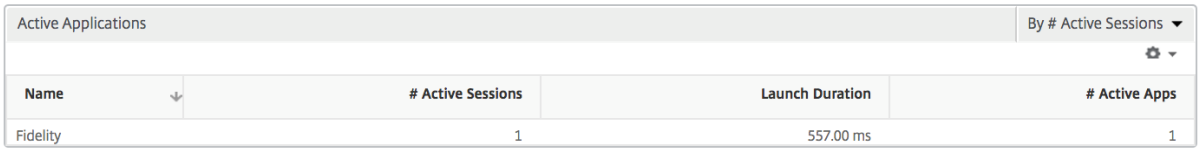
1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

Timeline chart

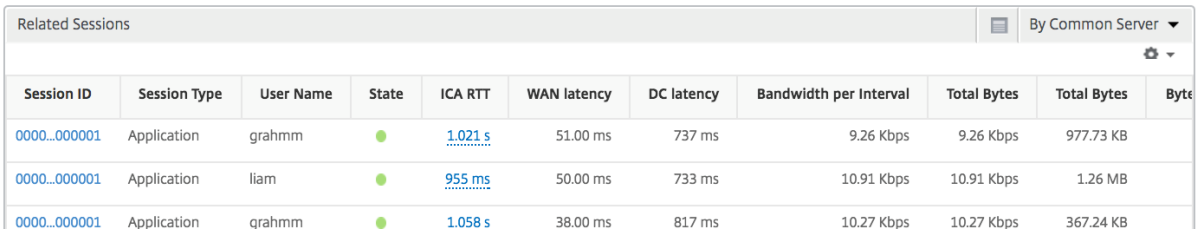
Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



Active application The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.



Application view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX Insight > Applications**.

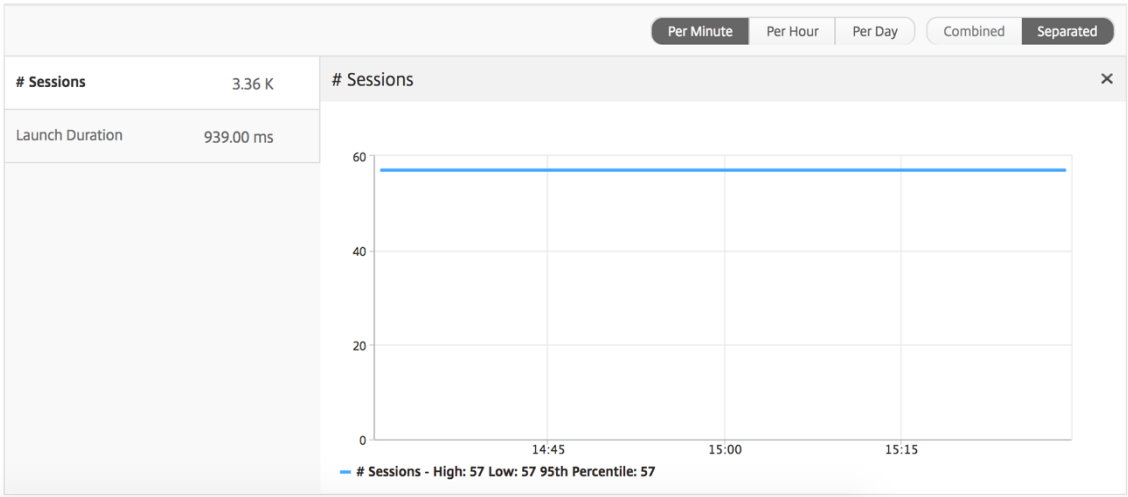
Summary view

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

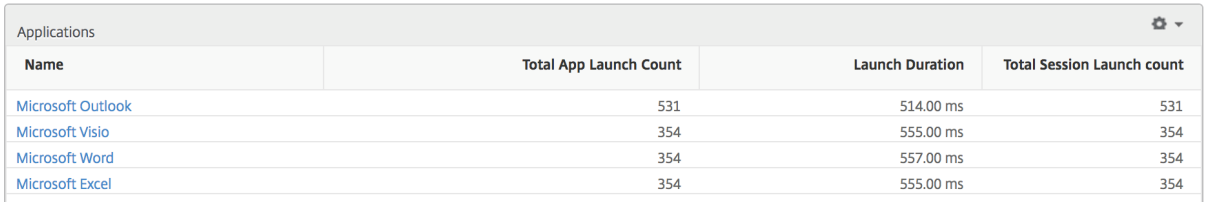
Line chart

Metrics	Description
Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.



Applications summary report

Metrics	Description
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.
Launch Duration	Average time taken to launch the Citrix Virtual App.

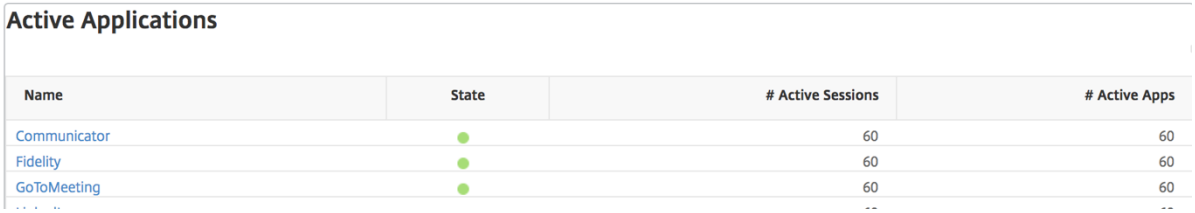


Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

Active application report

Metrics	Description
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.



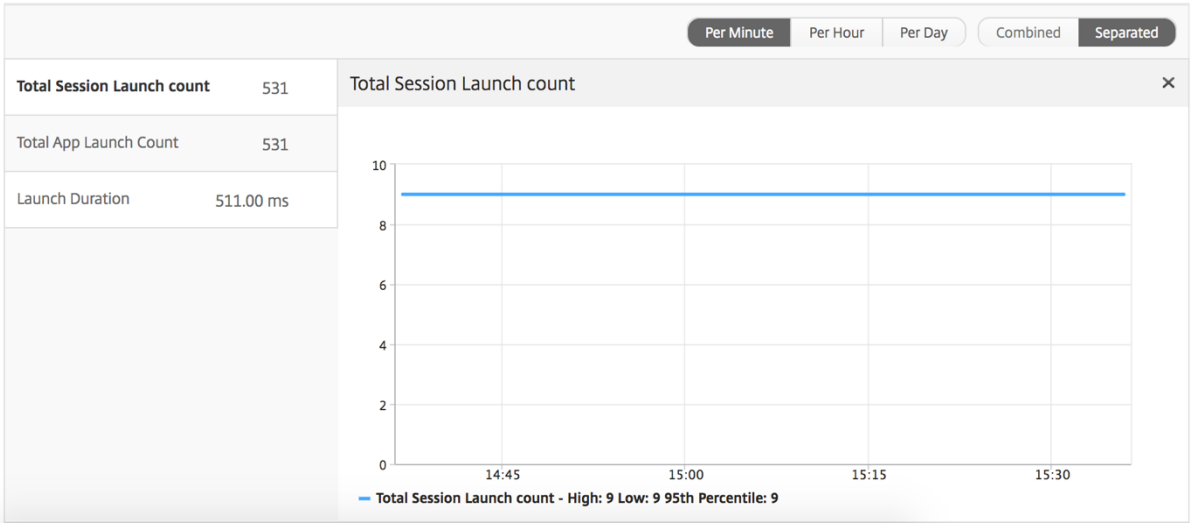
Active Applications

Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

Threshold report The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.

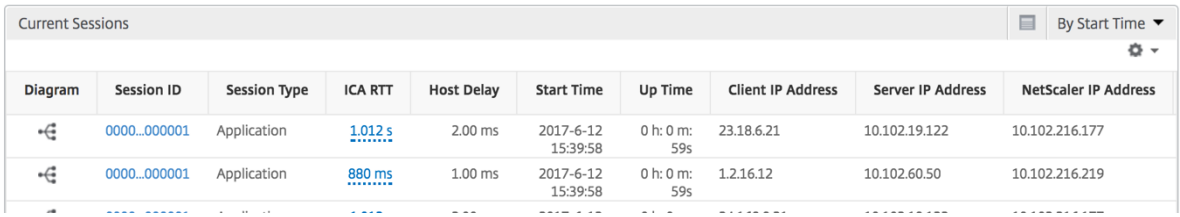


Current sessions report

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.

Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

Metrics	Description
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.



Per application session view

The per application session view displays reports for a particular selected application session.

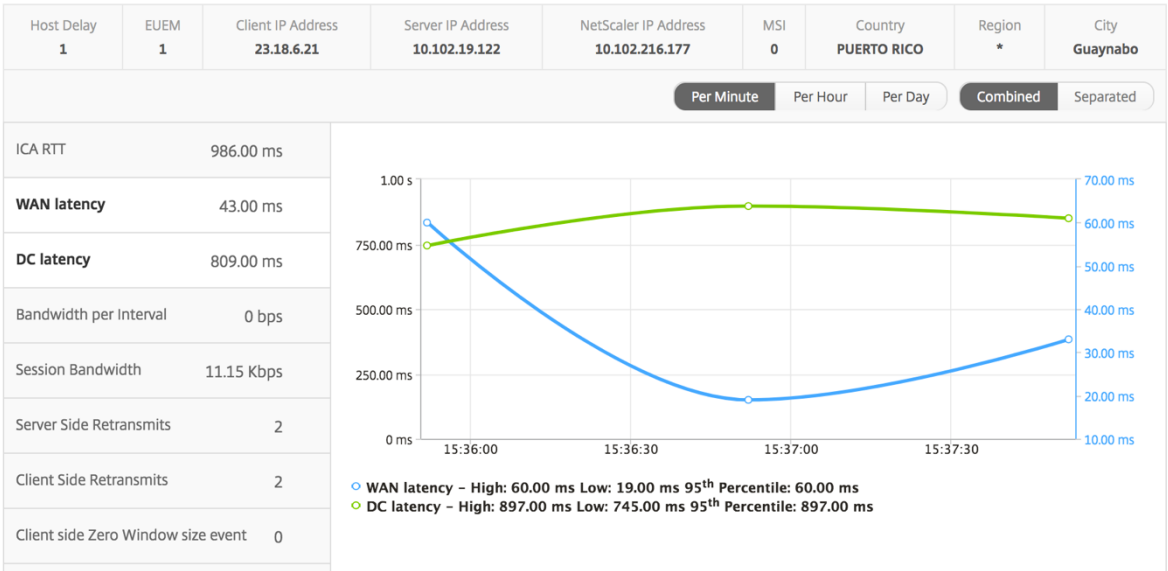
To view the Session reports:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Applications**.
3. Select a particular user from the Application Summary Report.
4. Selected a session from current sessions report.

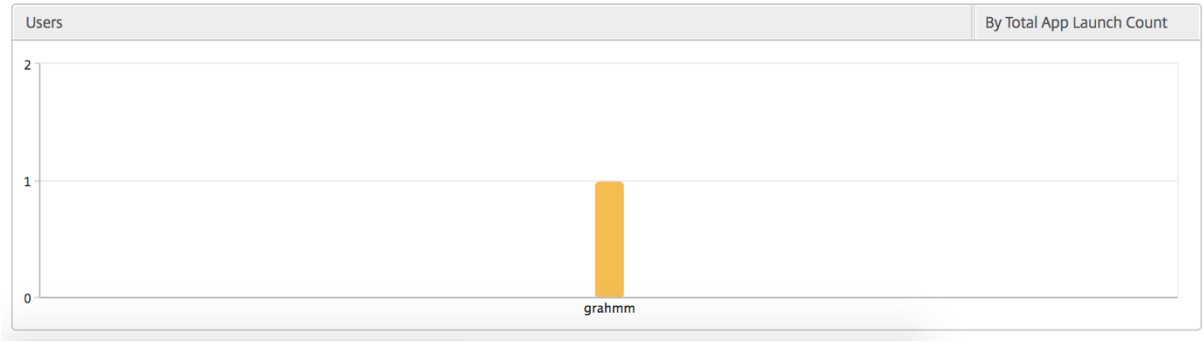
Line chart

Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

Metrics	Description
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



User bar graph The User's bar graph represents the users logged into this particular app.



Desktop view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Desktop**.

Summary view

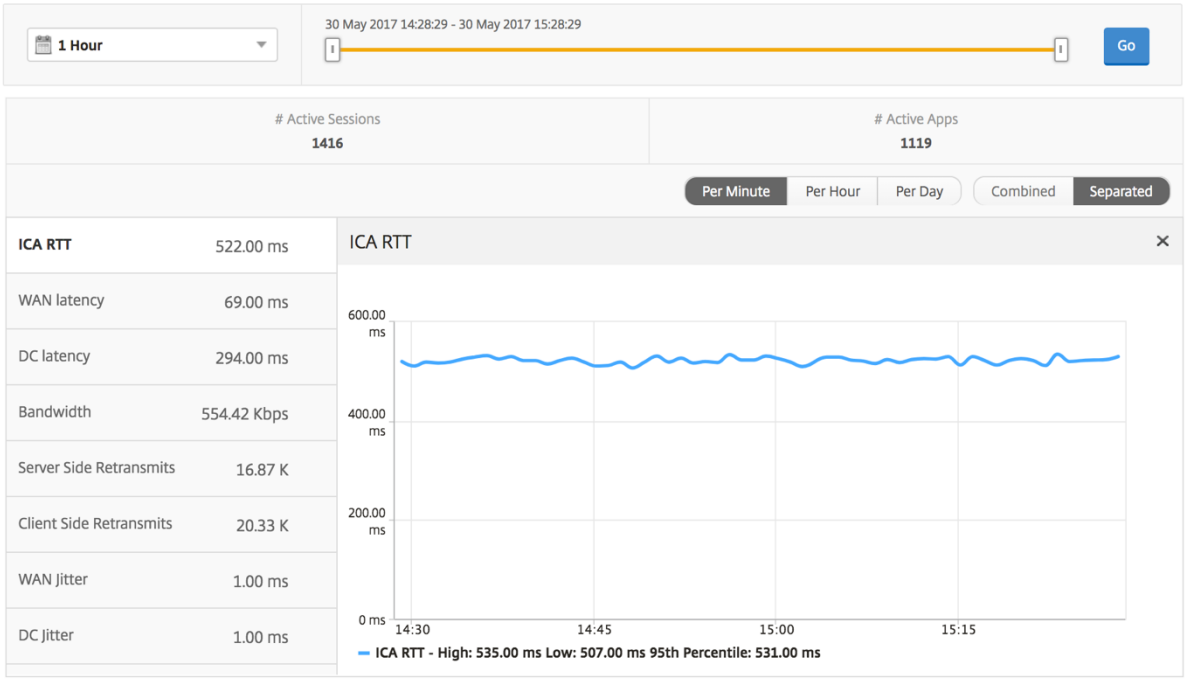
The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

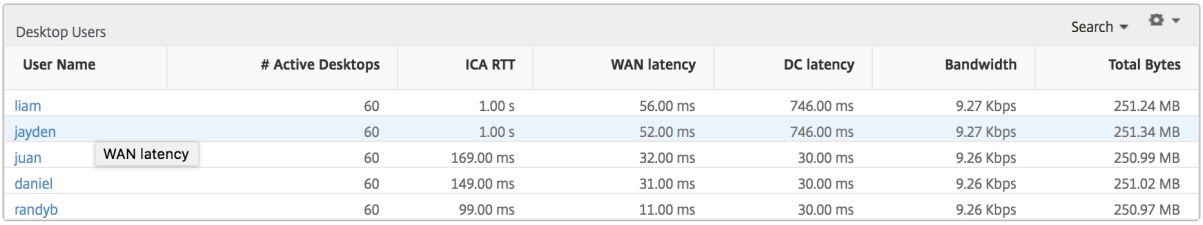
Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



Desktop summary report

Metrics	Description
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.



Threshold report The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period. For more information, see how to create thresholds.

Per Desktop view

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

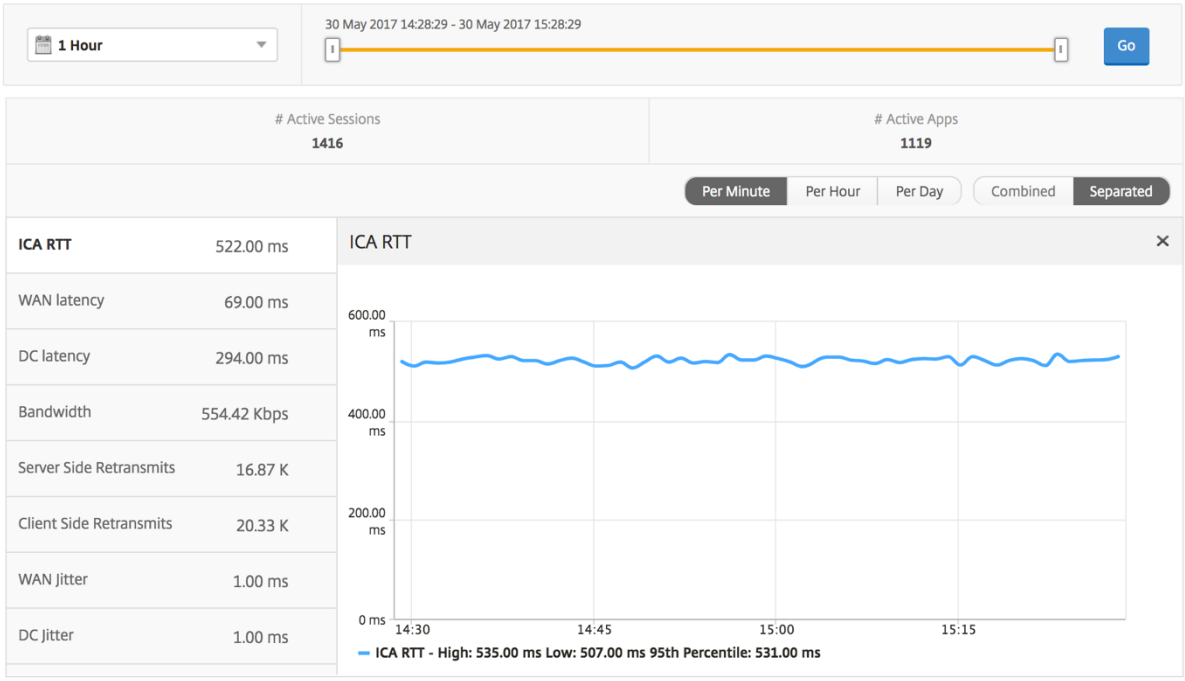
To navigate to the particular Desktop view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.
3. Select a particular **Desktop** from the **Desktop Summary Report**.

Line chart

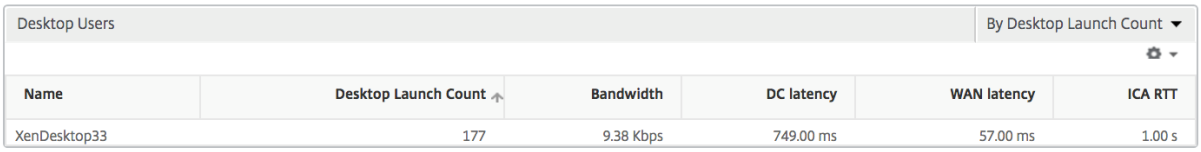
Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.

Metrics	Description
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



Desktop Users report This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

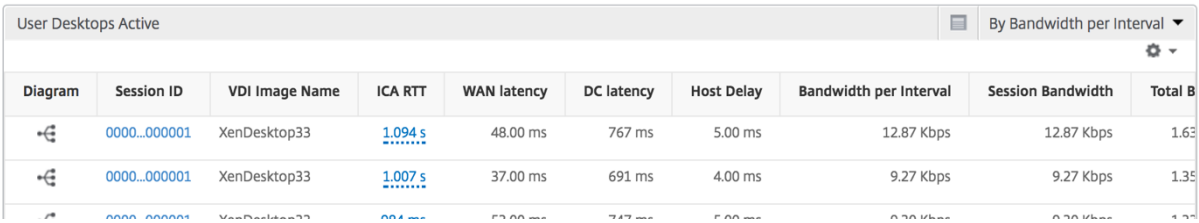


User Desktops Active/Inactive report These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.

Metrics	Description
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

Metrics	Description
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per Desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.
3. Select a particular desktop from the **Desktop Summary Report**.
4. Select a session from current sessions report.

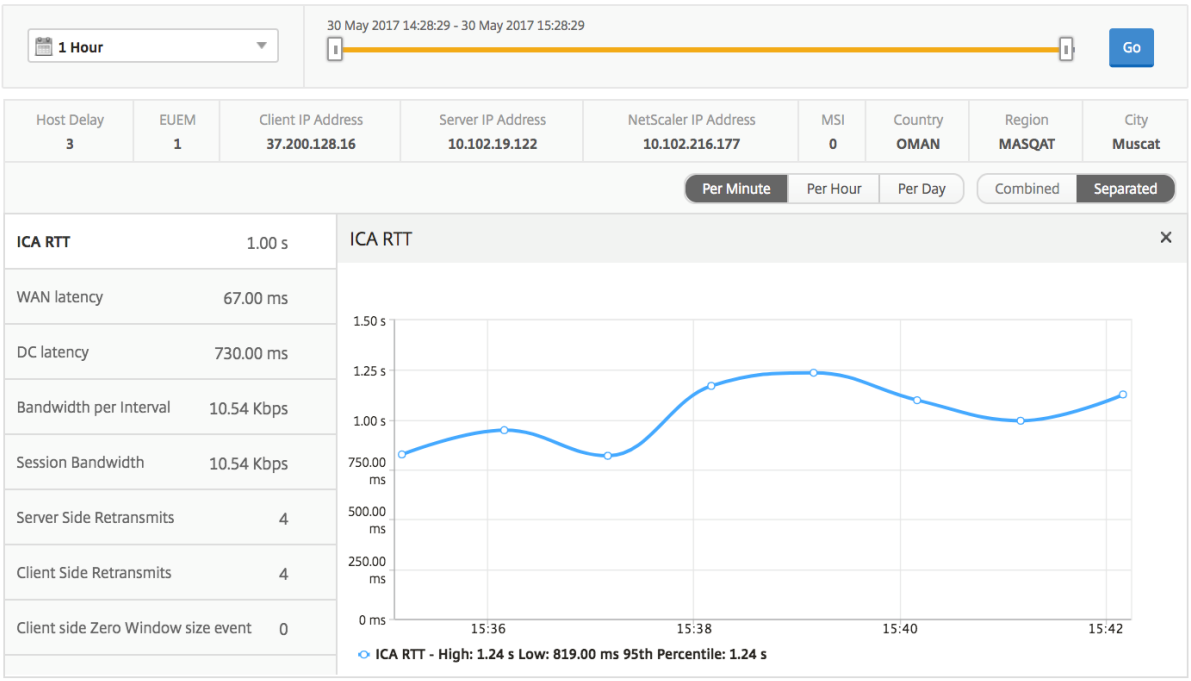
Timeline chart The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the **User Summary Report** section.

4. Select a session from **Current Sessions** or **Terminated Sessions** column.

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

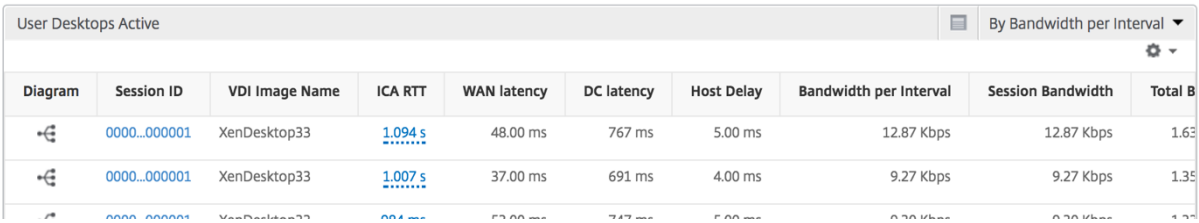


Related Desktop sessions report These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.

Metrics	Description
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.

Metrics	Description
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.



Instance view reports and metrics

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the Instance view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Instances**.

Instance view reports and metrics consist of the following sections:

- Instance Summary View
- Per Instance View

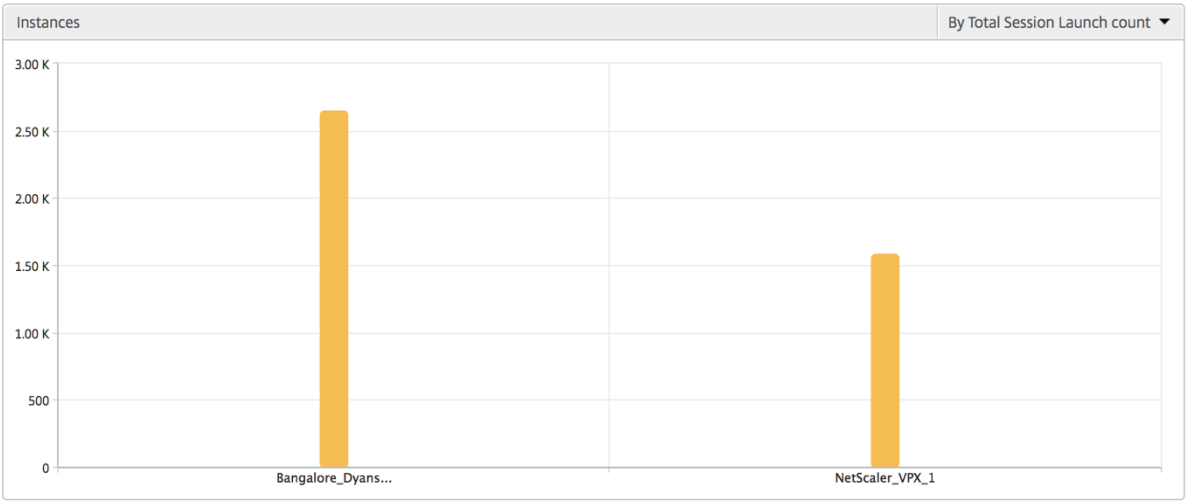
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler ADM.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

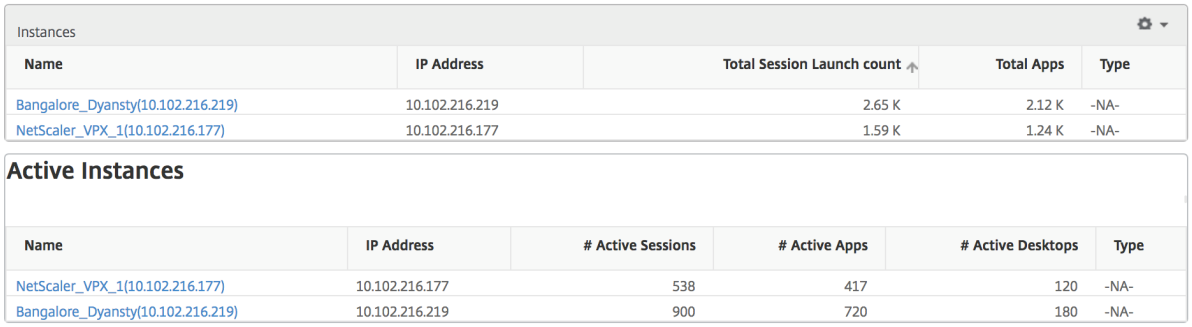
Instance bar graph

This graph displays the instance vs the Total Session Launch count	Total Apps which can be selected from the list on the top right on the graph canvas.



Instance/Active instances summary report

Metrics	Description
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A



Instances

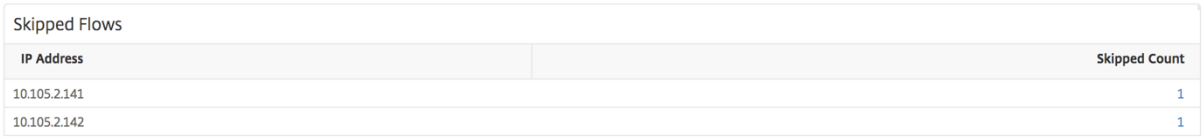
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Threshold report Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds.

Skipped flows A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type and so on This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.



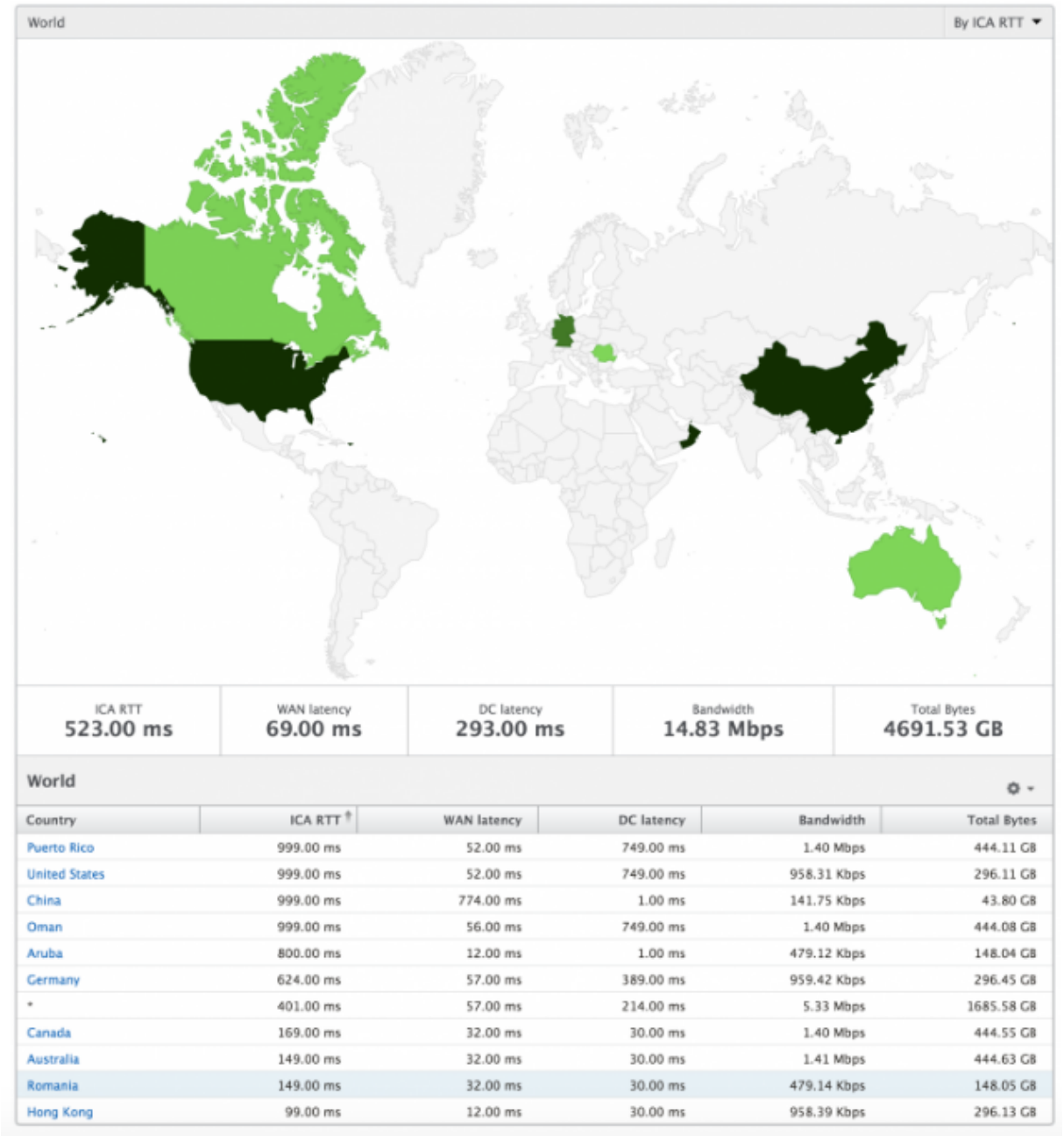
Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

World view The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per instance view

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

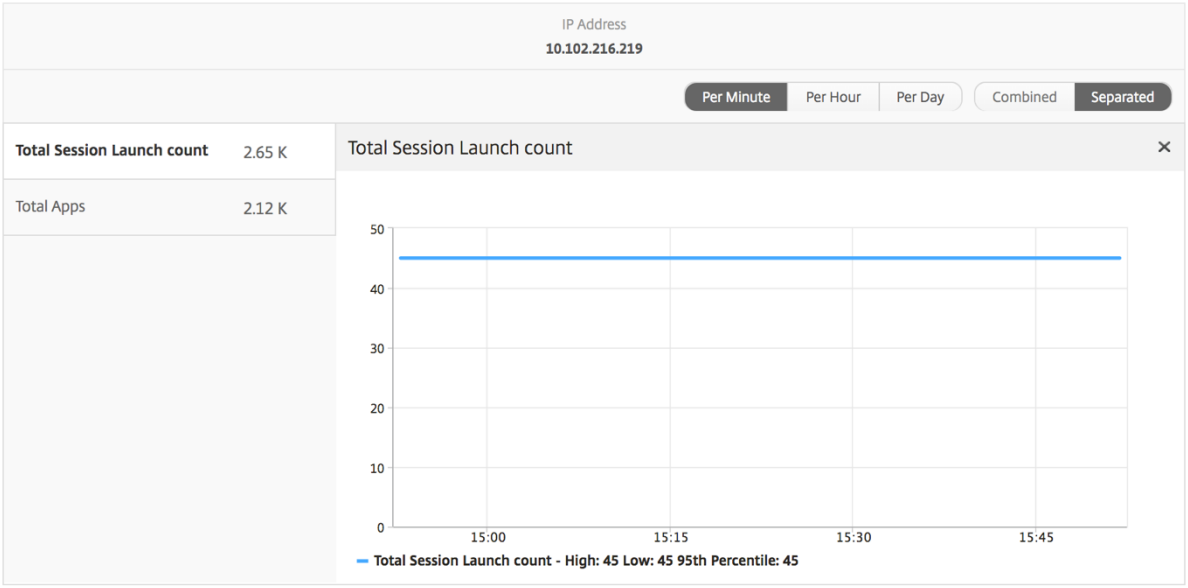
To navigate to the instance view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Instances**.

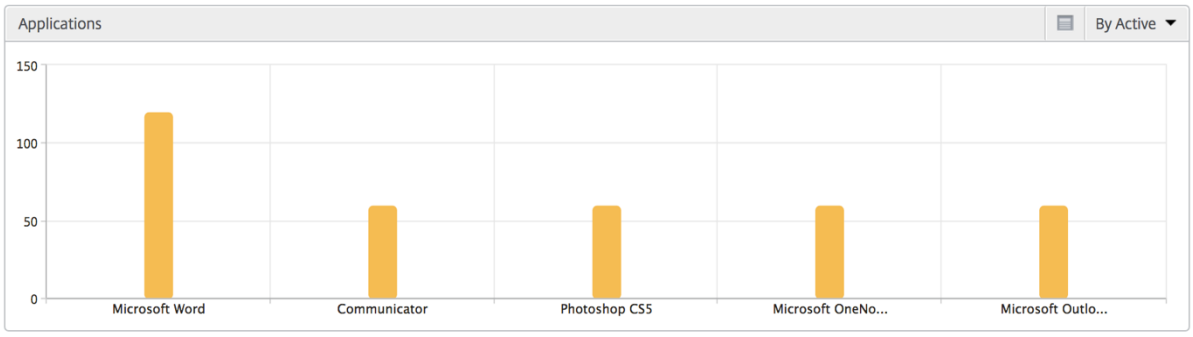
3. Select a particular instance from the **Instance Summary Report**.

Line chart

Metrics	Description
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.

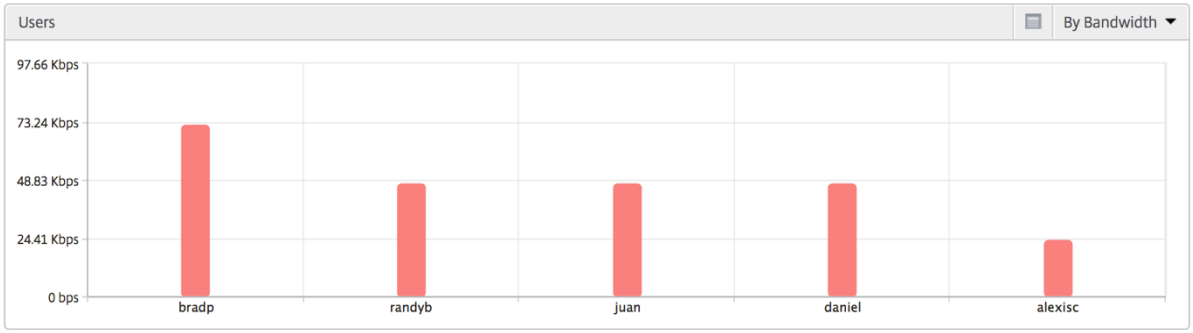


Applications bar graph Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.



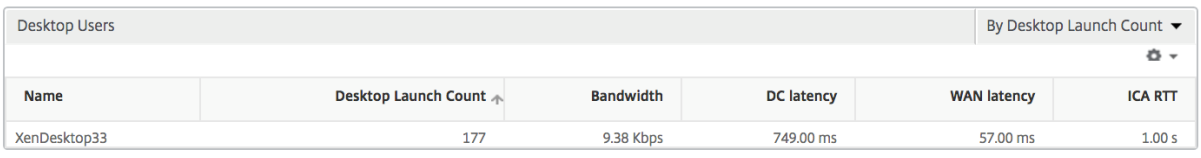
Users bar graph The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT



Desktop Users report This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

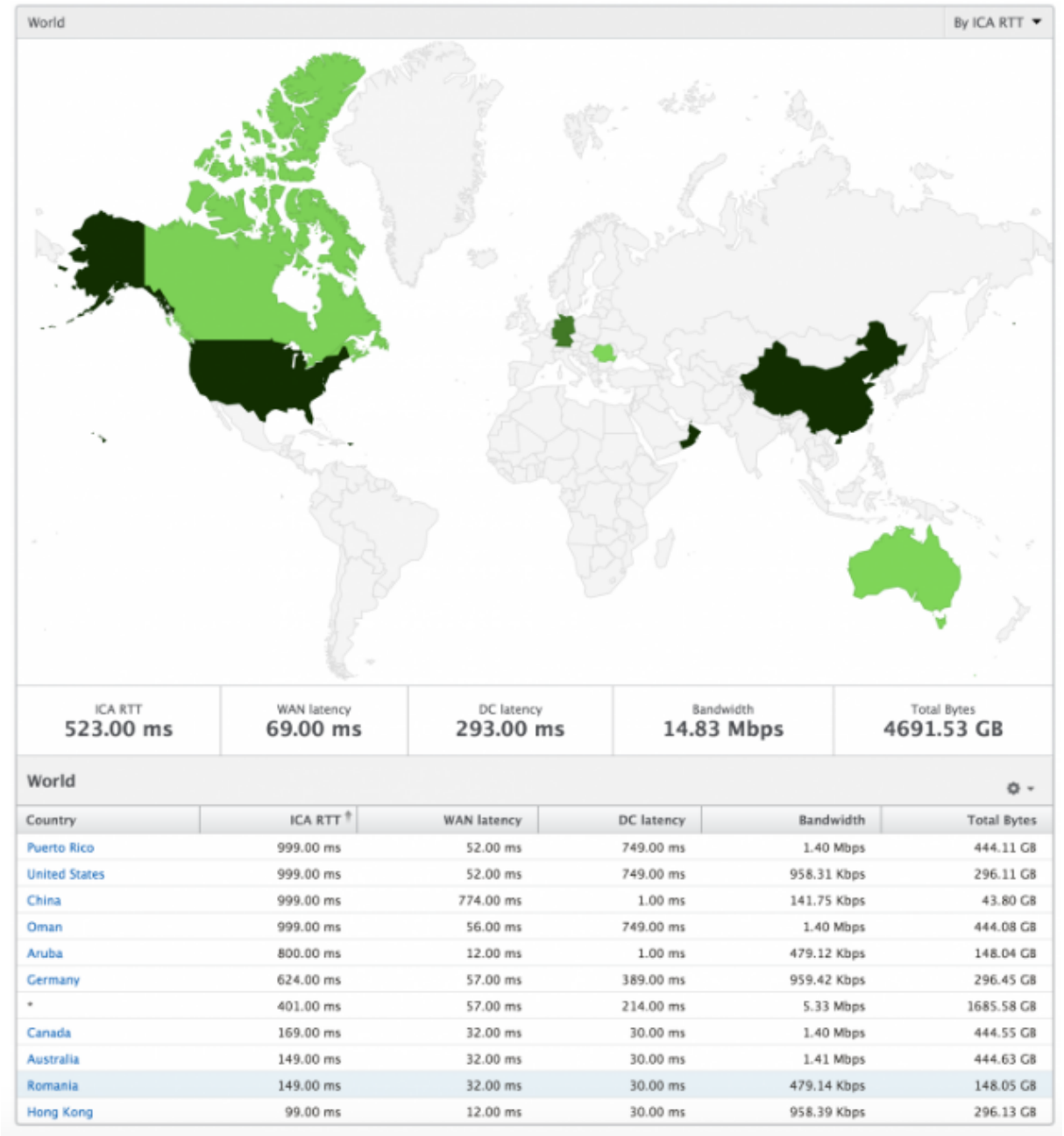
Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



World view The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License view reports and metrics

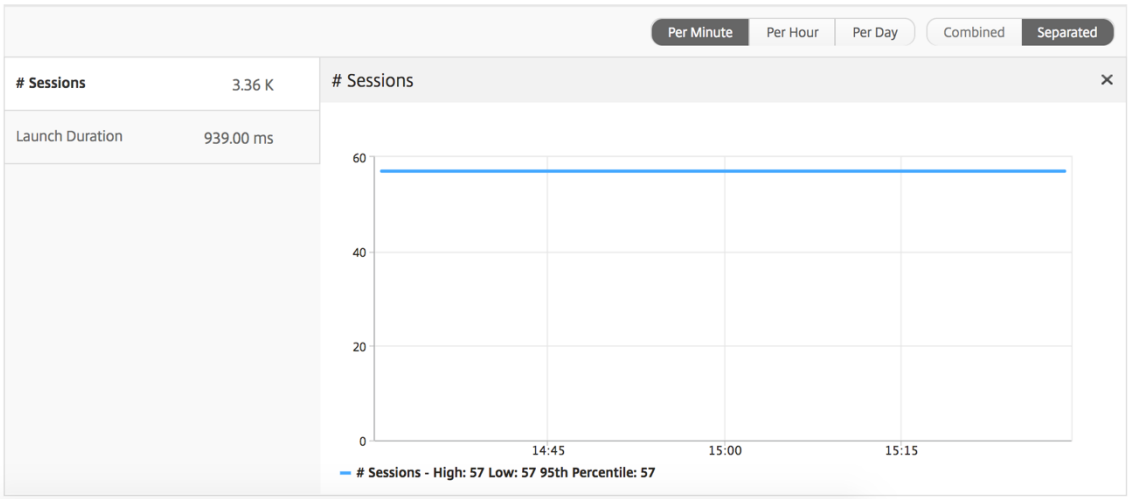
The license view gives details on the NetScaler Gateway license information.

To navigate to the License view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Licenses**.

Line chart

Metrics	Description
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds.

Application View Reports and Metrics

December 31, 2023

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX Insight > Applications**.

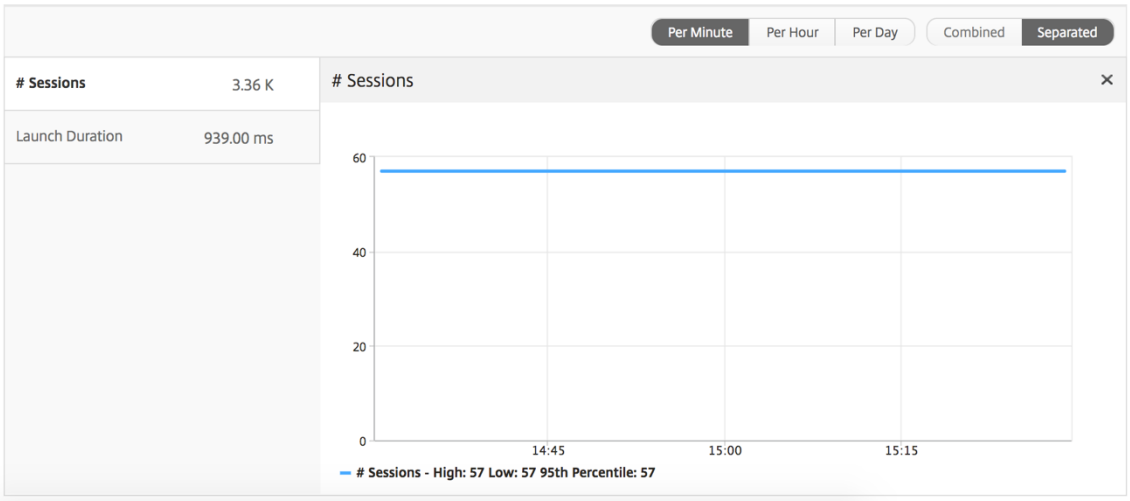
Summary view

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

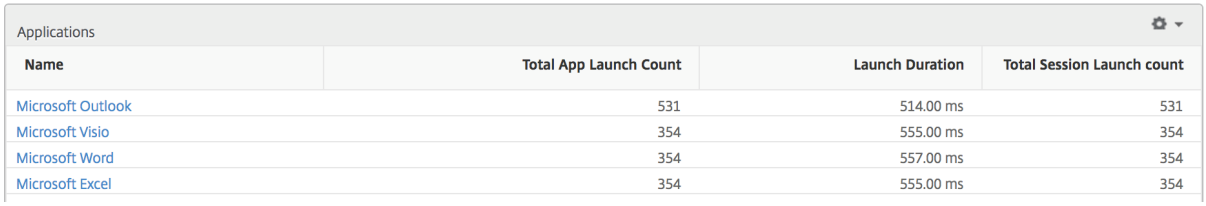
Metrics	Description
Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.



Applications summary report

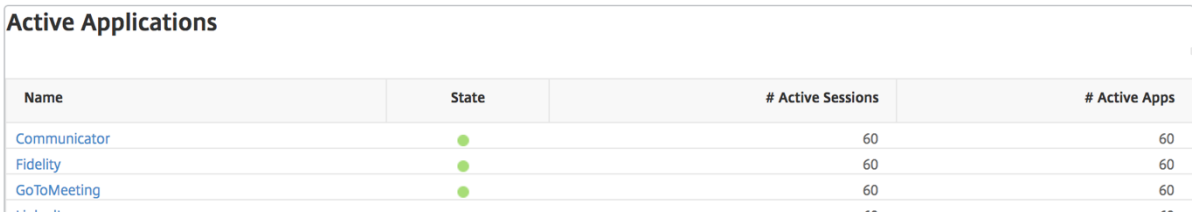
Metrics	Description
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.

Metrics	Description
Launch Duration	Average time taken to launch the Citrix Virtual App.



Active application report

Metrics	Description
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.

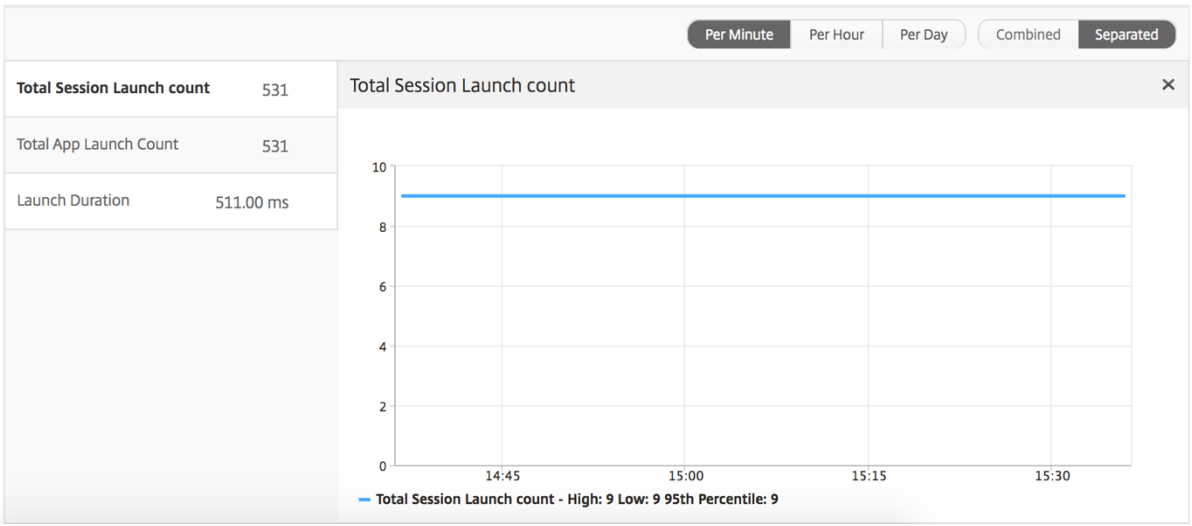


Threshold report

The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds and alerts.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.



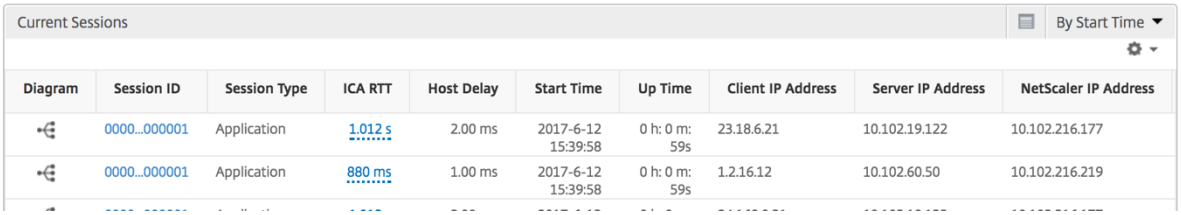
Current sessions report

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.

Metrics	Description
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.

Metrics	Description
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.

Metrics	Description
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in non-Citrix devices being present in the delivery path.



Per Application session view

The per application session view displays reports for a particular selected application session.

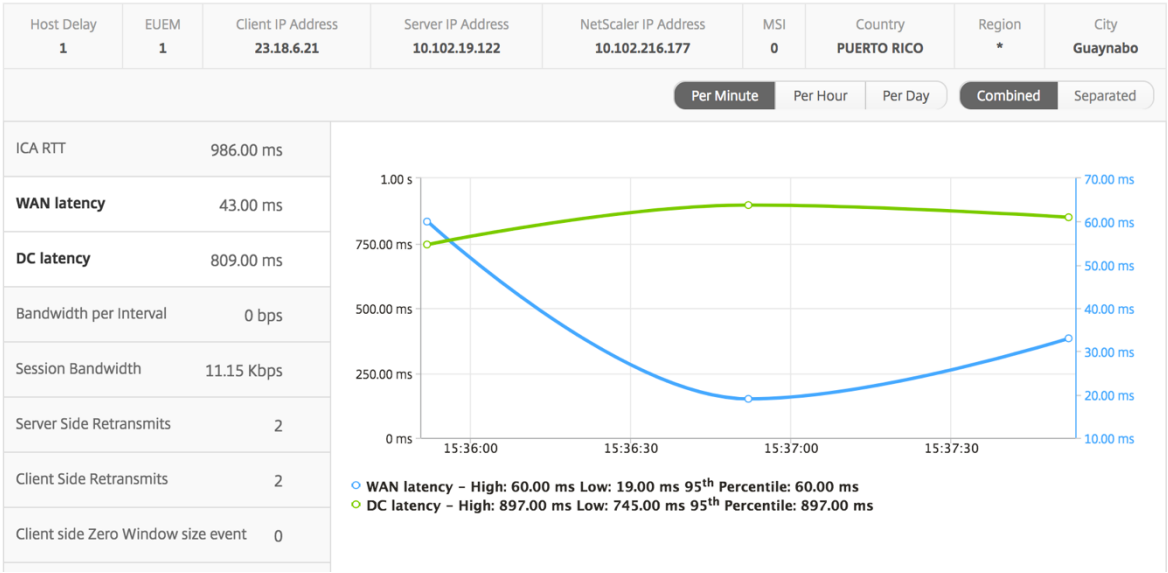
To view the Session reports:

1. Navigate to **Gateway > HDX Insight > Applications**.
2. Select a particular user from the Application Summary Report.
3. Selected a session from current sessions report.

Line chart

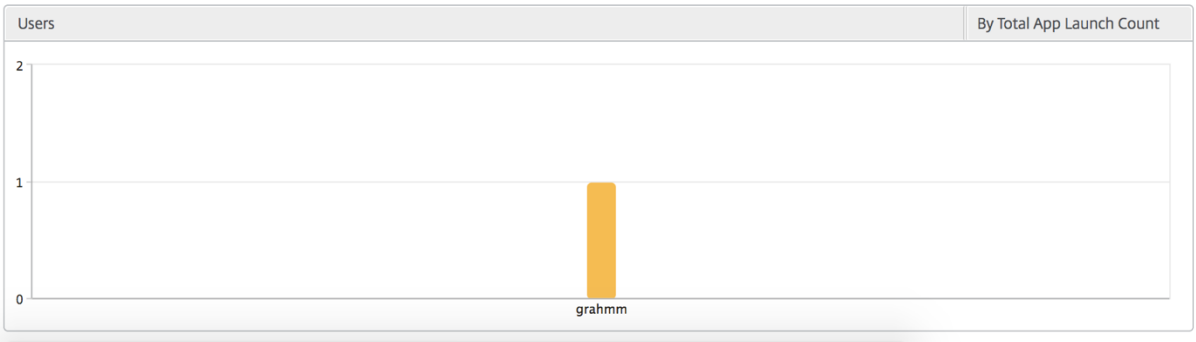
Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



User bar graph

The User's bar graph represents the users logged into this particular app.



Desktop View Reports and Metrics

December 31, 2023

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Navigate to **Gateway > HDX Insight > Desktop**.

Summary view

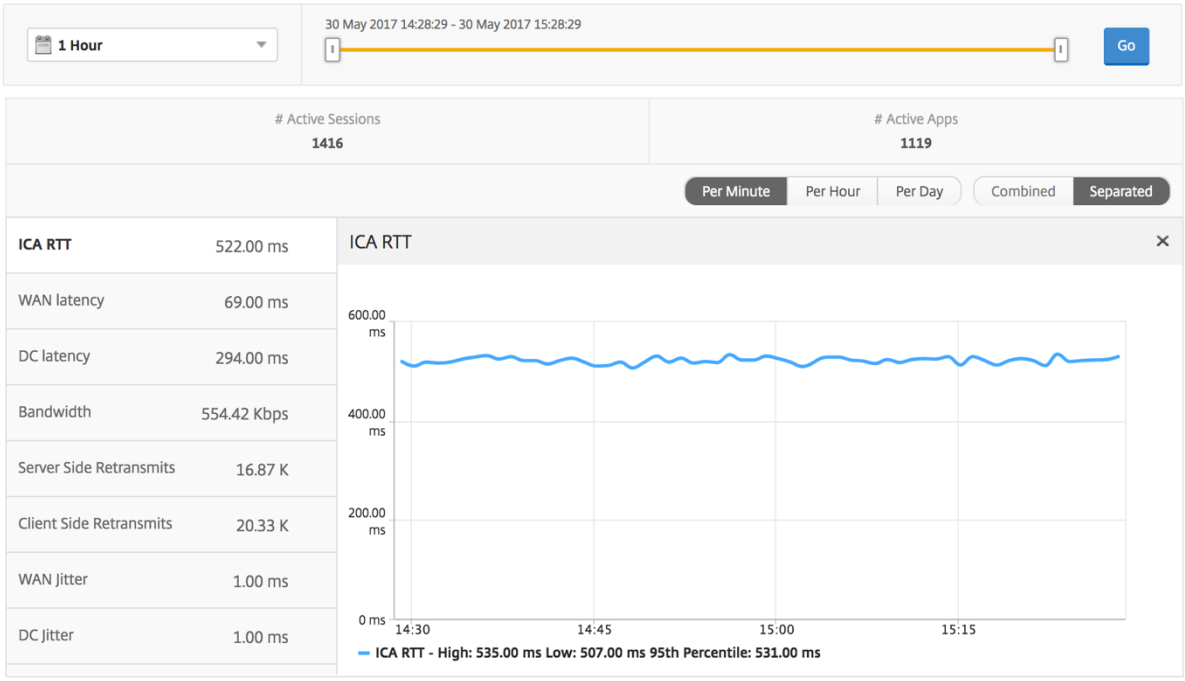
The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

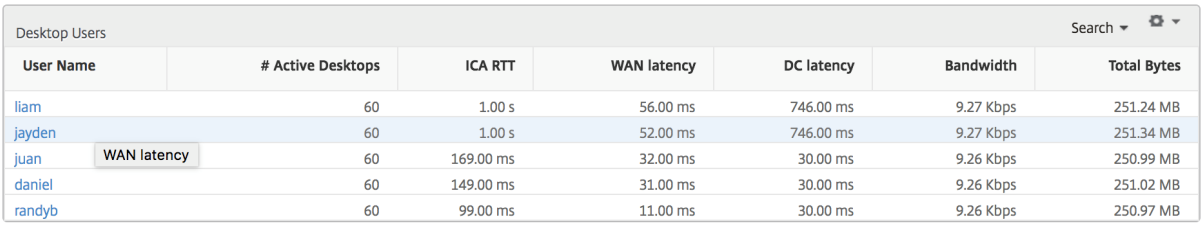
Metrics	Description
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



Desktop summary report

Metrics	Description
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period. For more information, see how to create thresholds and alerts.

Per desktop view

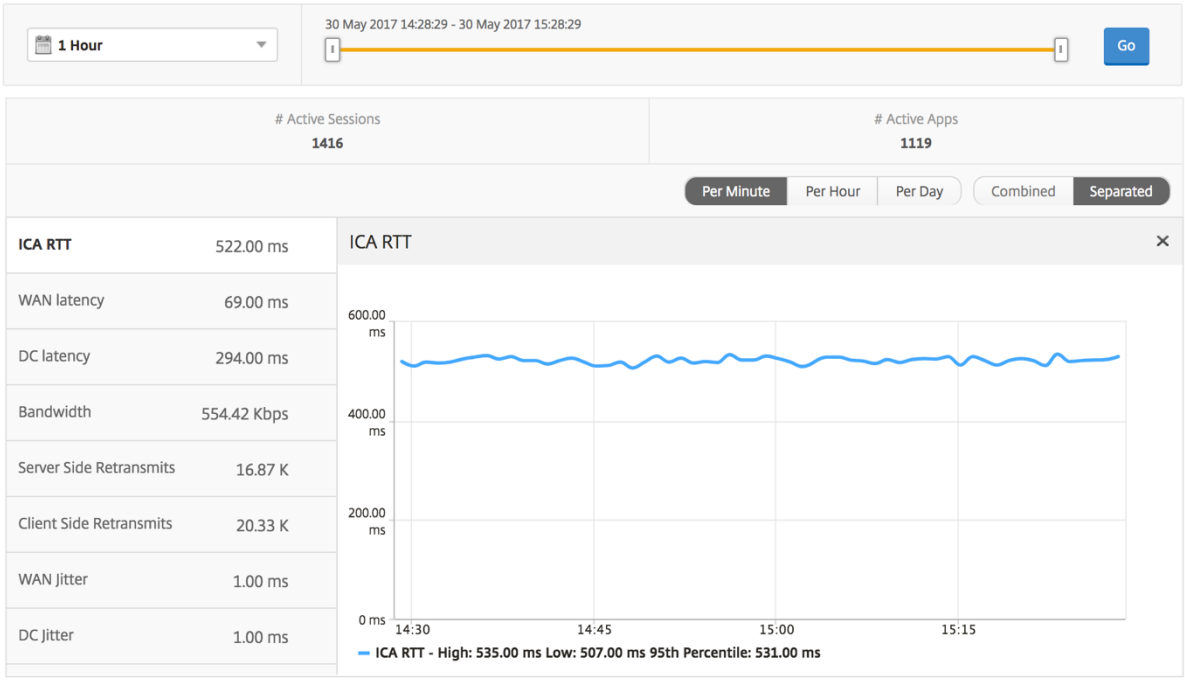
Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

To navigate to the particular Desktop view:

1. Navigate to **Analytics > HDX Insight > Desktop**.
2. Select a particular **Desktop** from the **Desktop Summary Report**.

Line chart

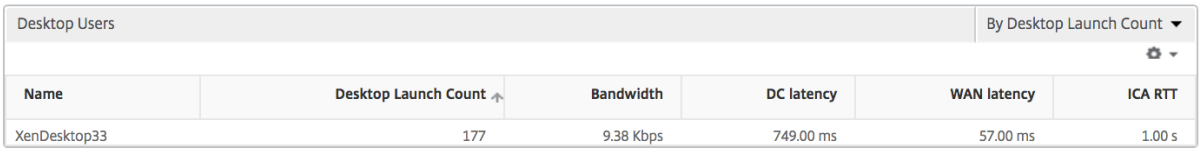
Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



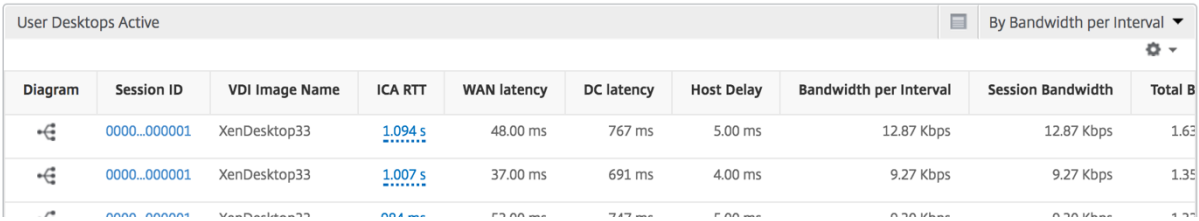
User desktops active/inactive report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.

Metrics	Description
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

Metrics	Description
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Navigate to **Gateway > HDX Insight > Desktop**.
2. Select a particular desktop from the **Desktop Summary Report**.
3. Select a session from current sessions report.

Timeline chart

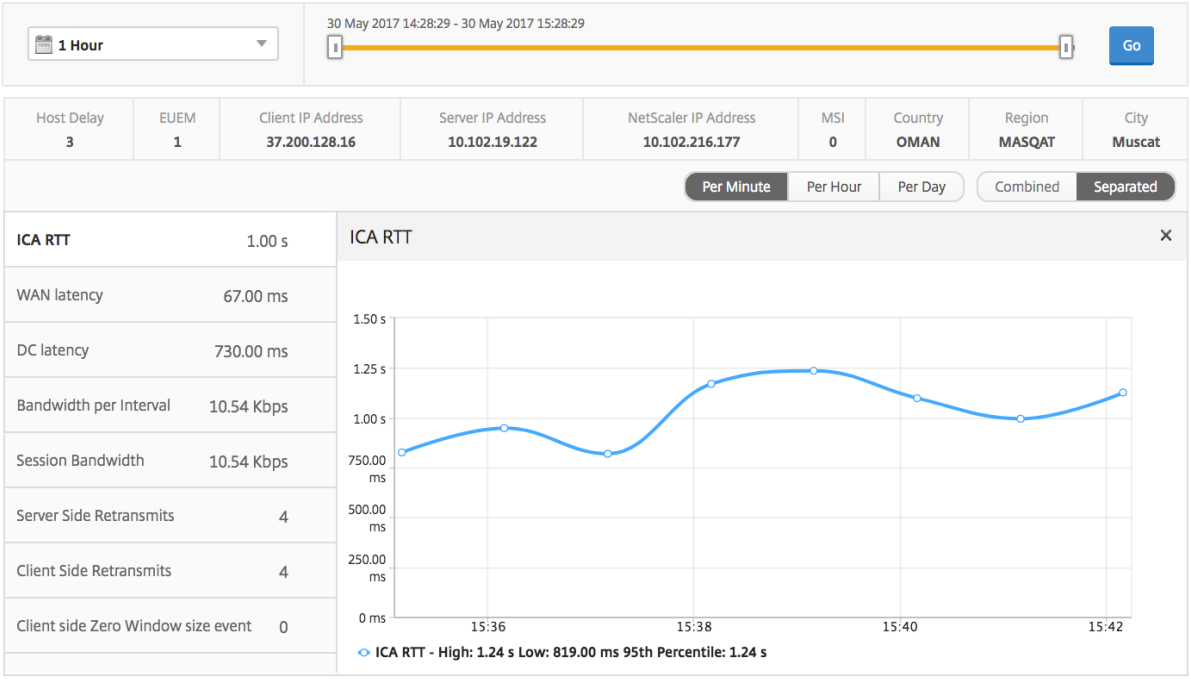
The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.

3. Select a session from **Current Sessions** or **Terminated Sessions** column.

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App and Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



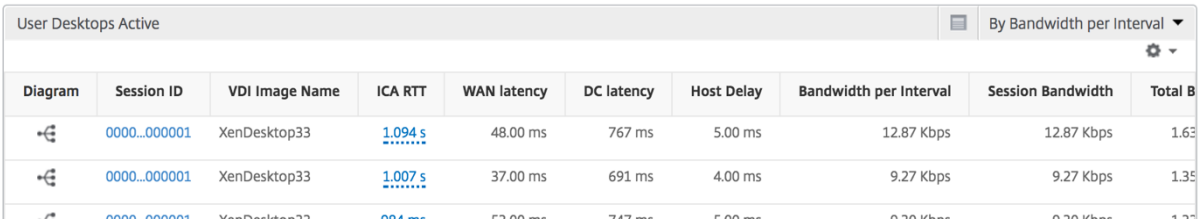
Related desktop sessions report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.

Metrics	Description
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Receiver type- Citrix Windows Client and so on
Client Version	Receiver version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.

Metrics	Description
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected



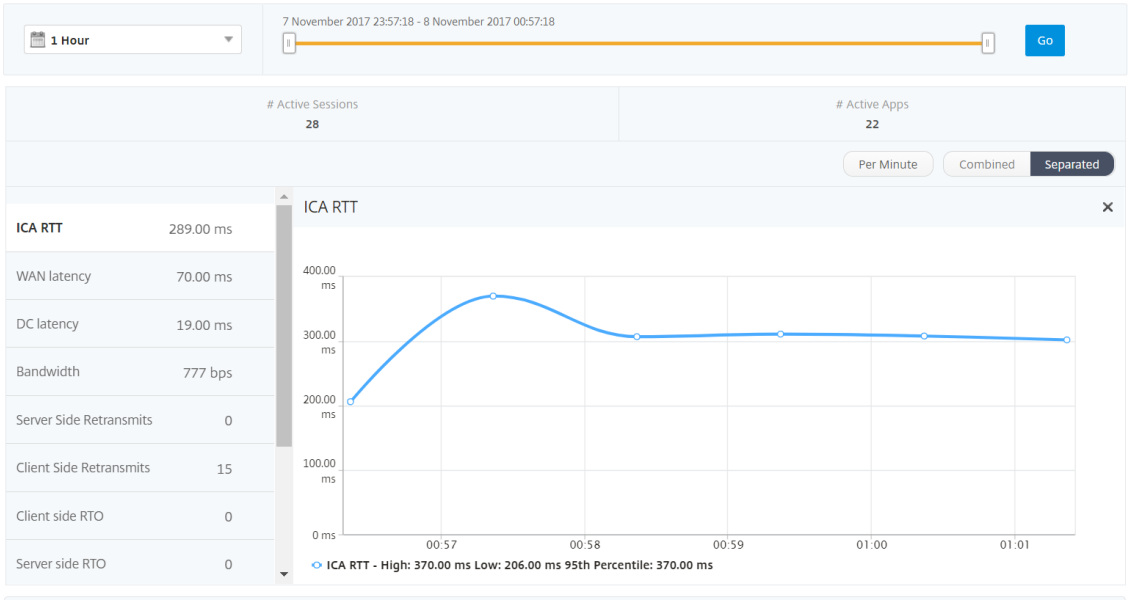
User View Reports and Metrics

March 11, 2024

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktop users.

To navigate to the Users view:

1. Navigate to **Gateway > HDX Insight > Users**



Summary view

The summary view displays the reports for all the users that have logged in during the selected time-line. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

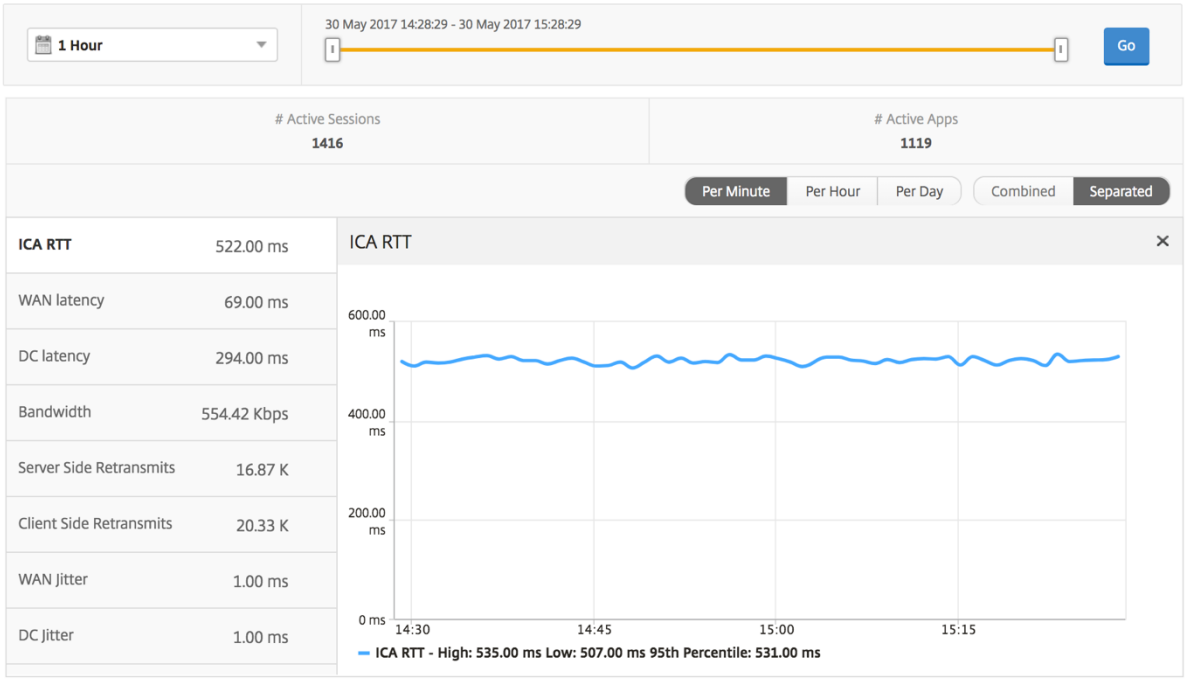
To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



User summary report

Following are the metrics that are specific to this report.

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.

Metrics	Description
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

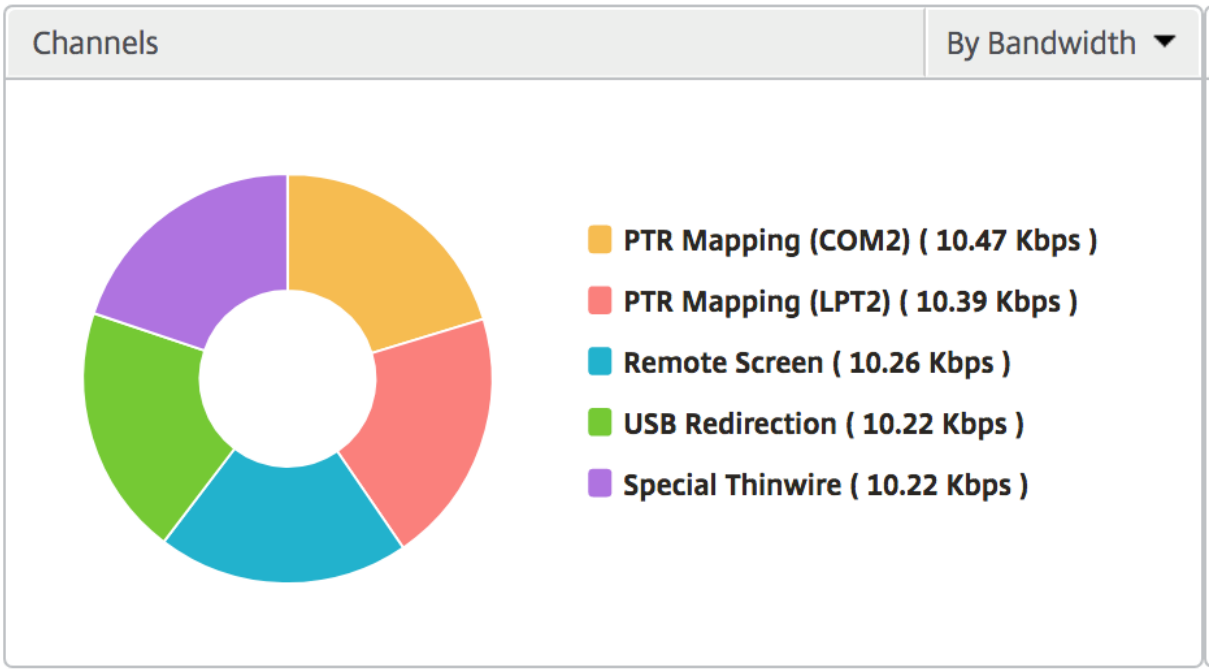
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

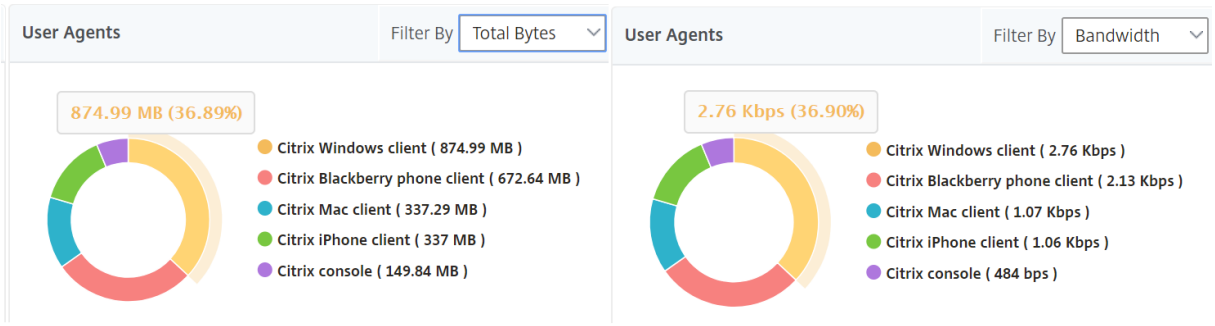
Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Thresholds breach count

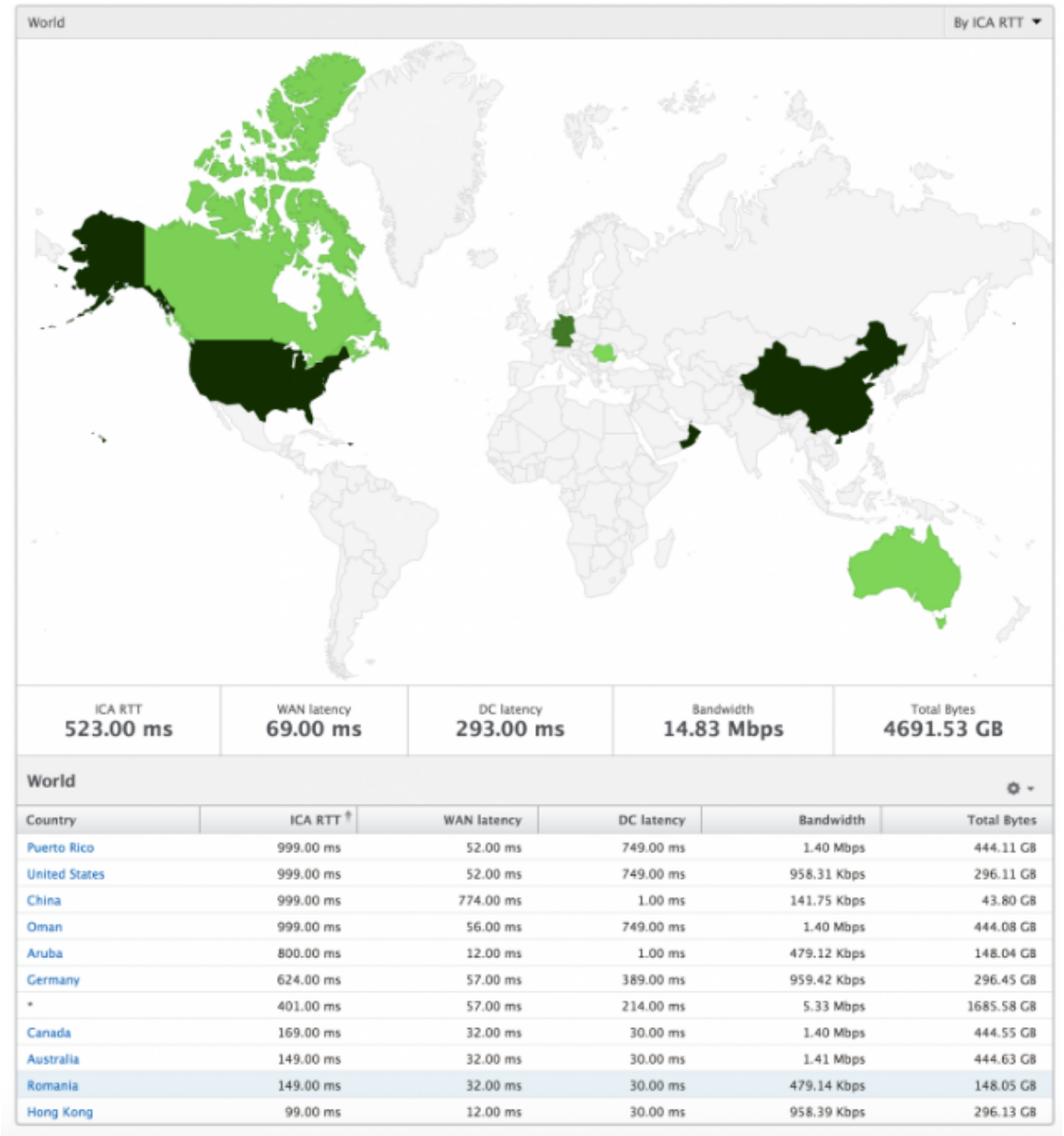
The Thresholds breach count metrics represent the count of thresholds breached in the selected time period. For more information, see how to create thresholds and alerts.

World map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Per user view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the Users summary report.

Line chart

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.

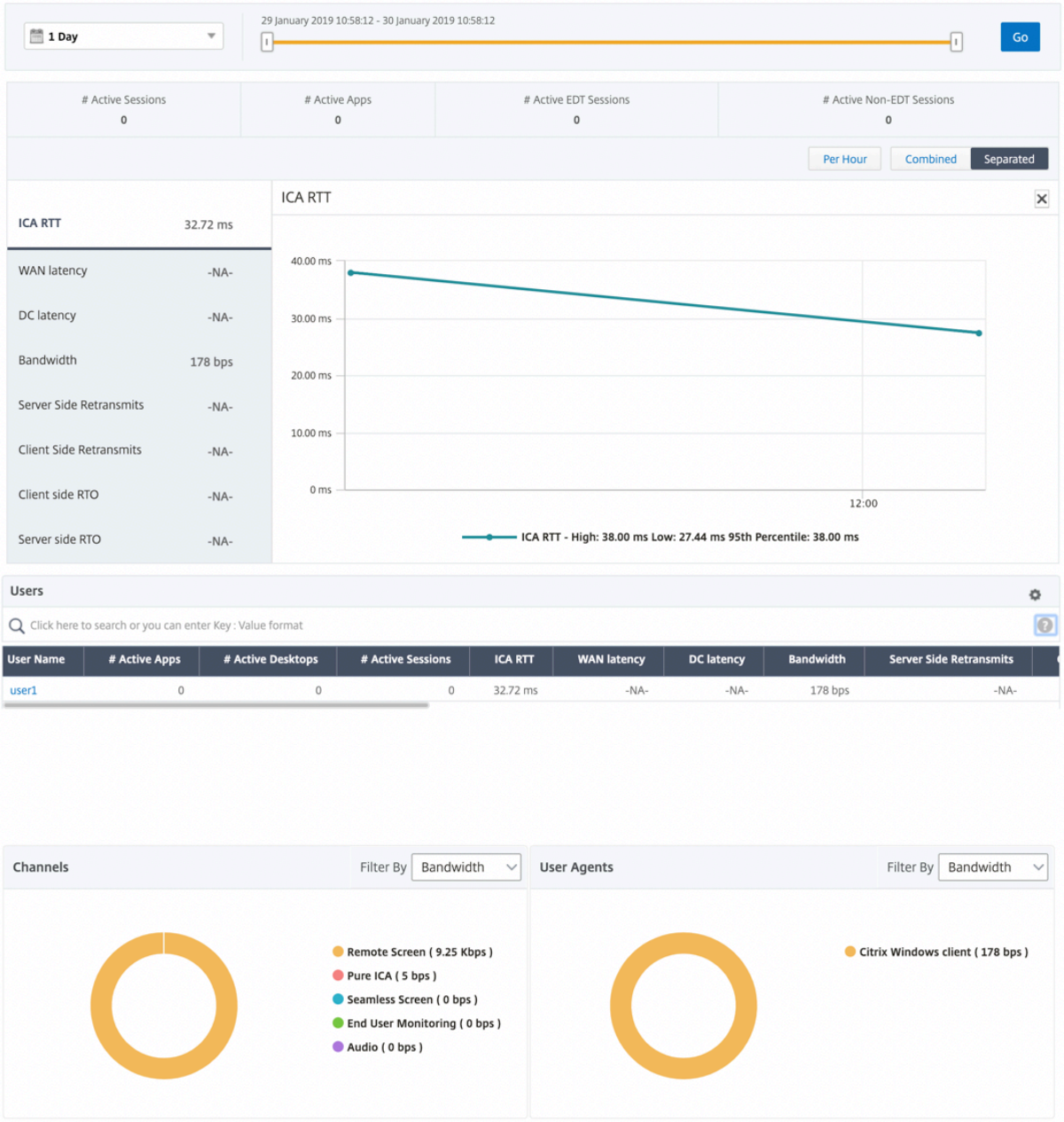
Metrics	Description
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

Metrics	Description
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

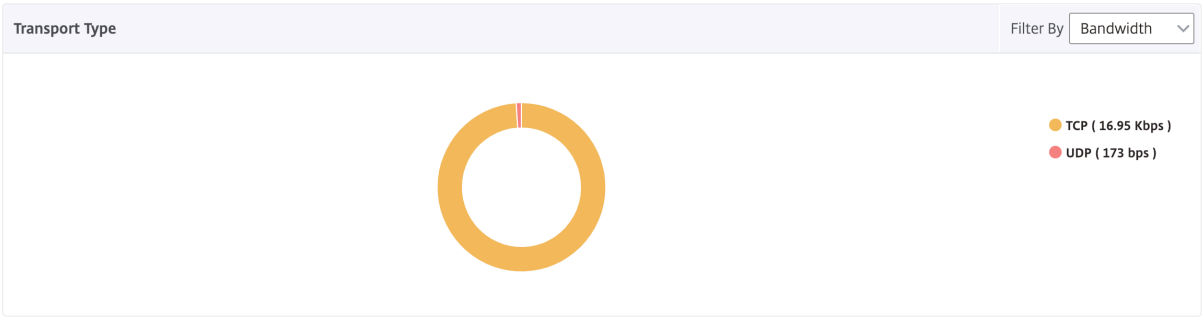
Support for EDT in HDX insight

NetScaler Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol. EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, and RTOs. Some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".

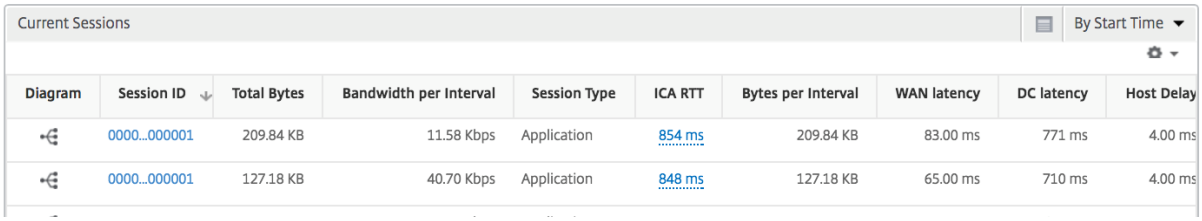


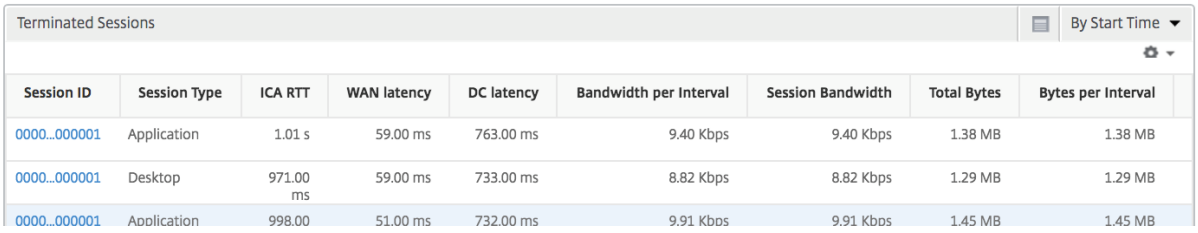
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.



HDX Insight metrics available from NetScaler ADM 12.0 and later:

L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.

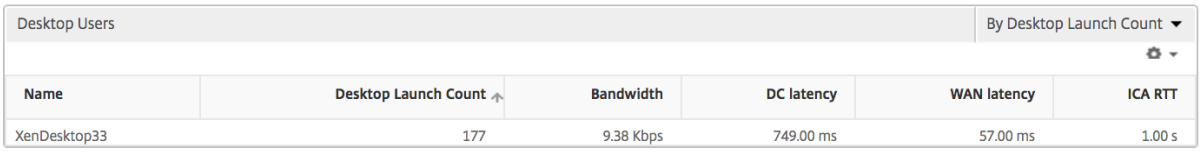




Desktop Users

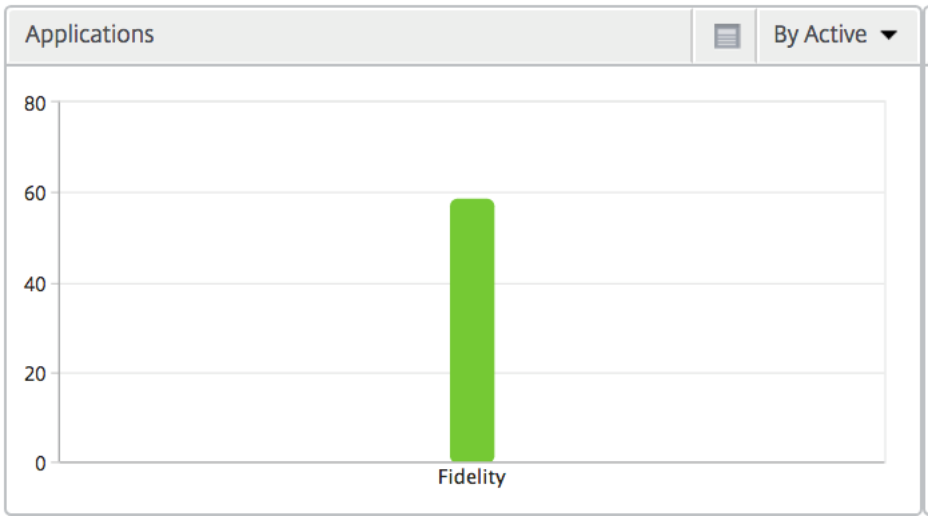
This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



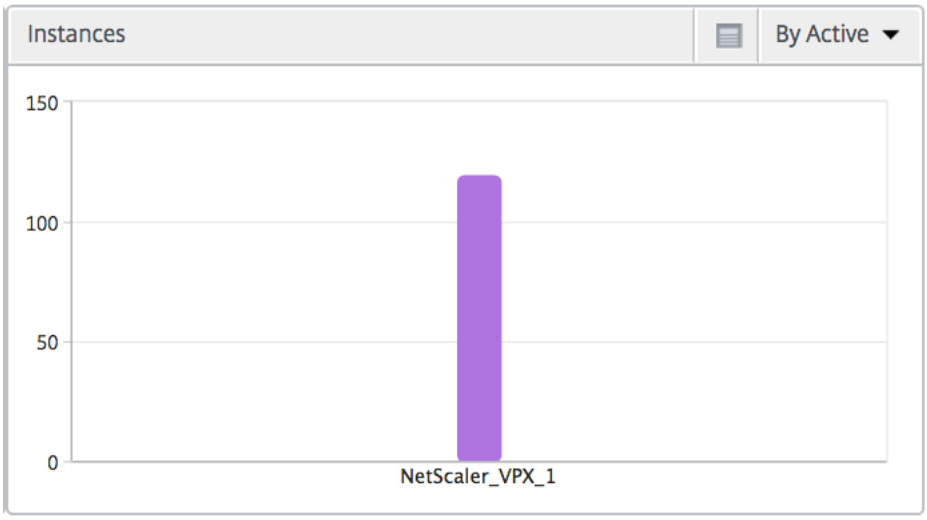
Applications

A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.



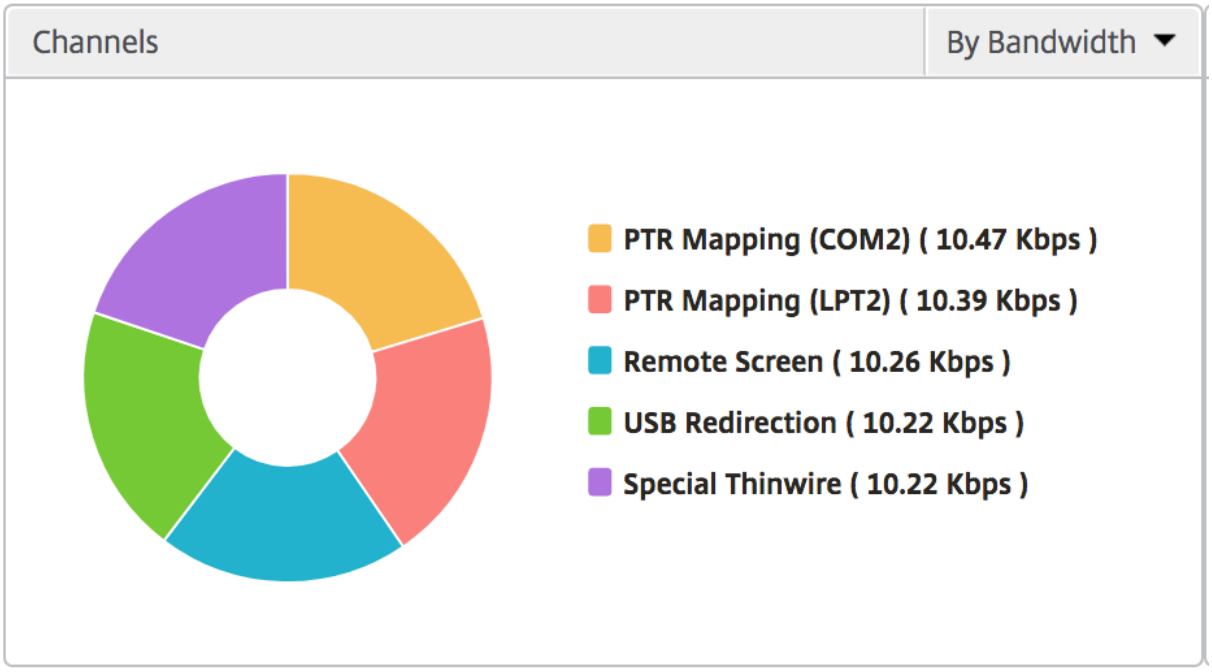
Instances

A bar graph representing NetScaler Instances sorted by Active and total apps



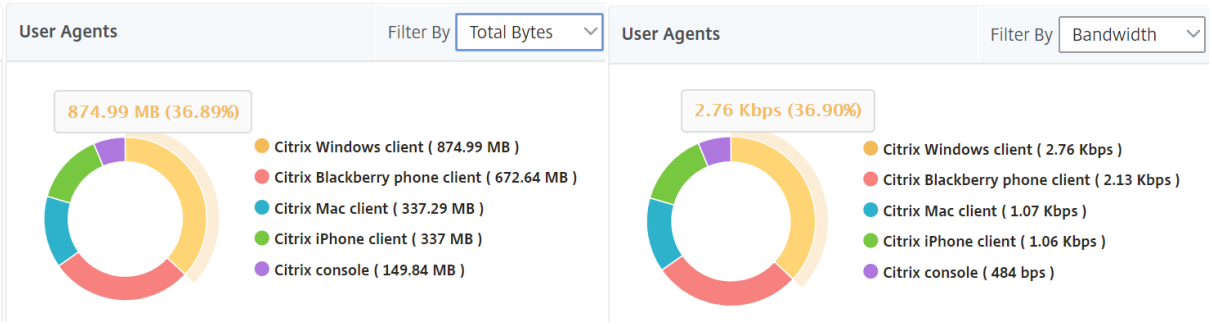
Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Per User session view

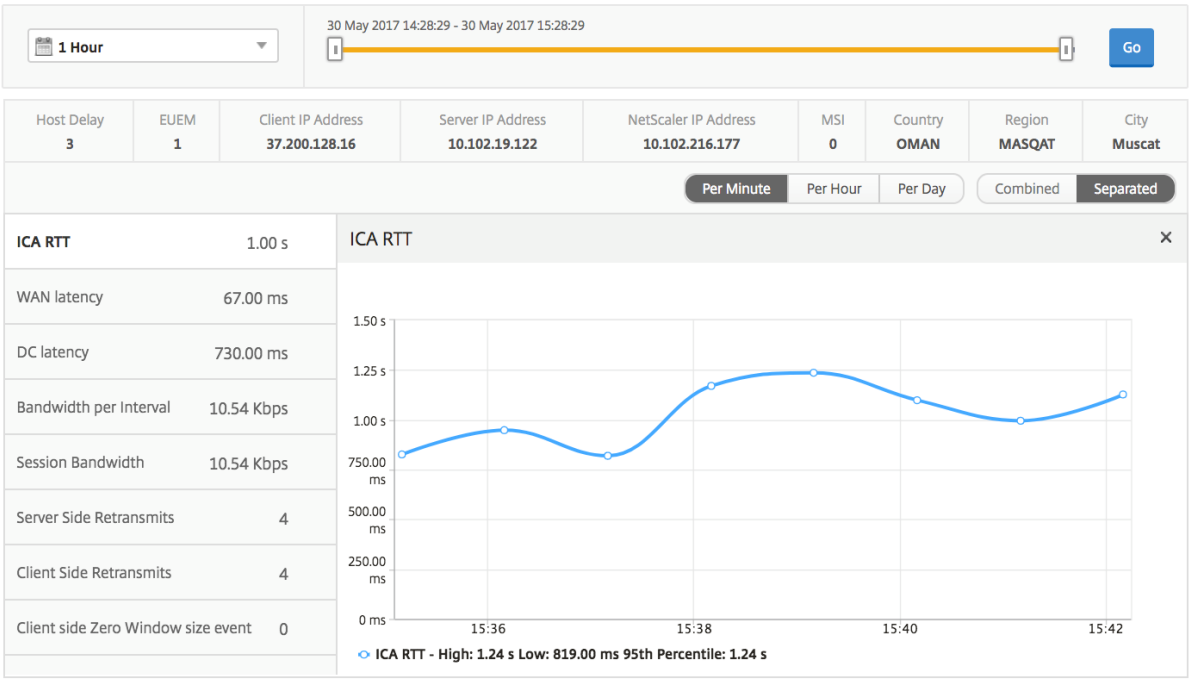
The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

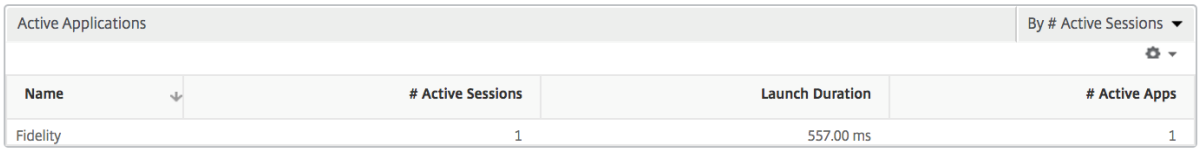
Timeline chart

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



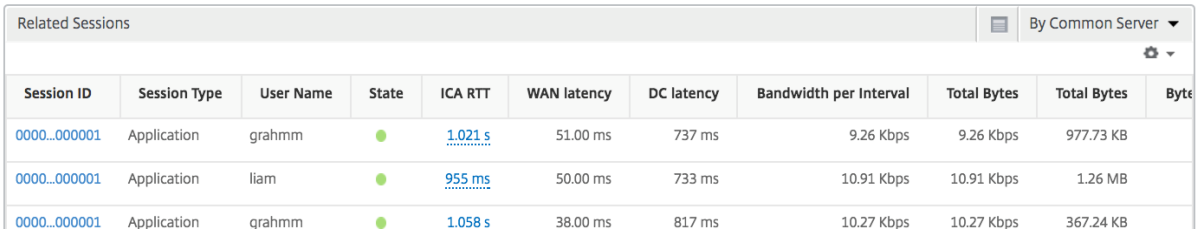
Active application

The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions

The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.



Instance View Reports and Metrics

March 11, 2024

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the instance view:

1. Navigate to **Gateway > HDX Insight > Instances**.

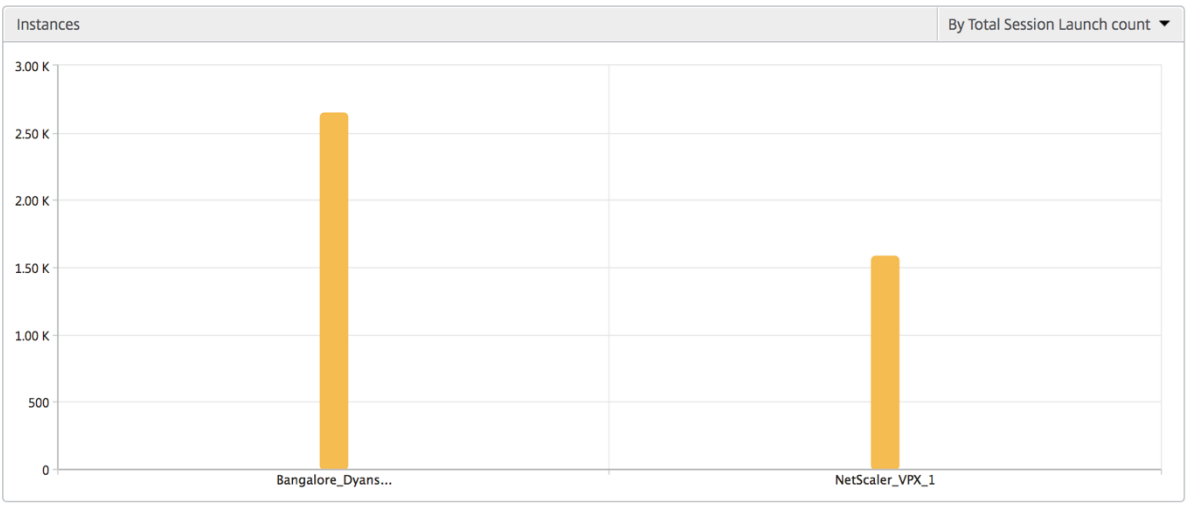
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler ADM.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

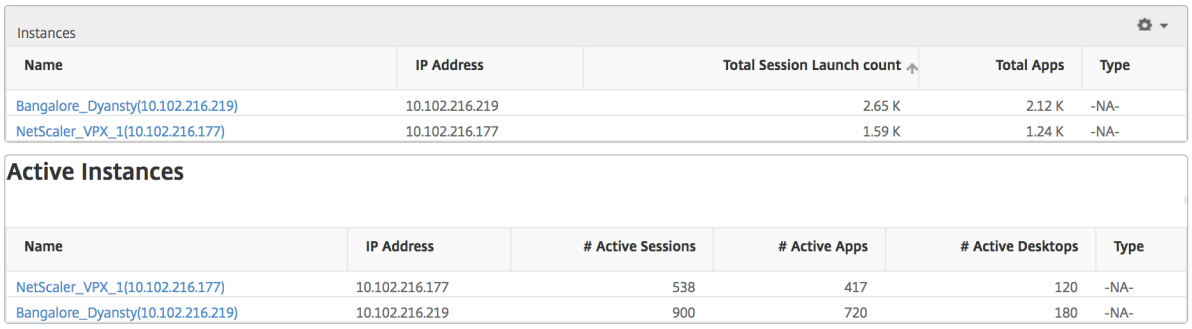
Instance bar graph

This graph displays the instance vs the Total Session Launch count and Total Apps which can be selected from the list on the top right on the graph canvas.



Instance/Active instances summary report

Metrics	Description
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A



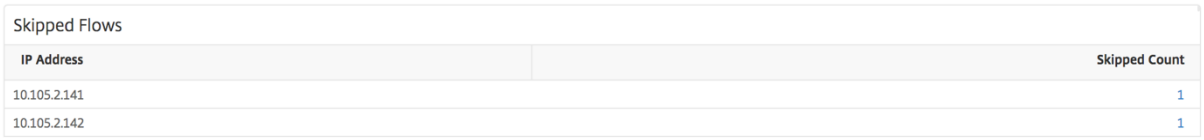
Threshold report

Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds and alerts.

Skipped flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type, and so on. This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.

See **Error! Hyperlink reference not valid** for more details on issues related to ICA parsing.

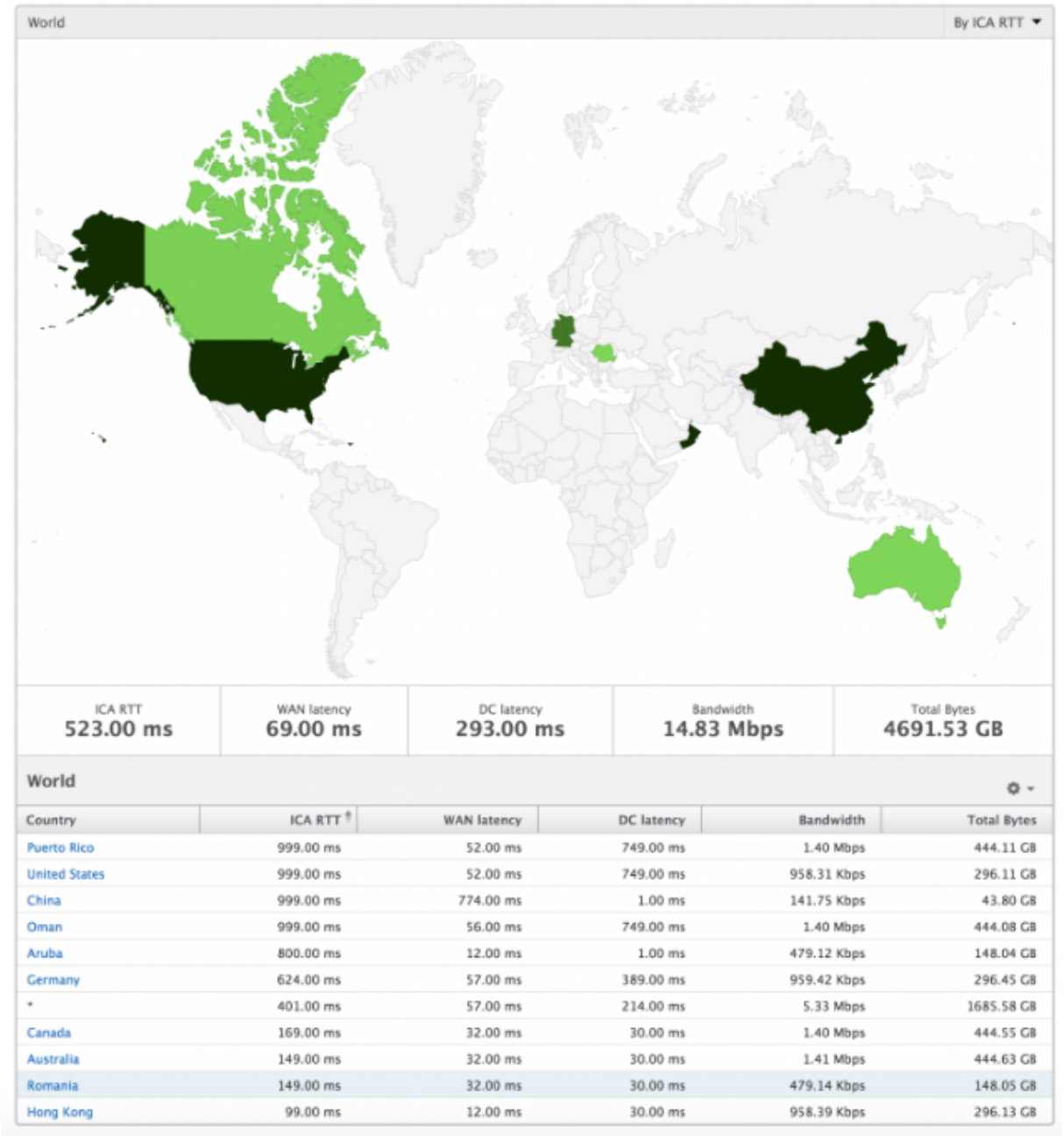


World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per instance view

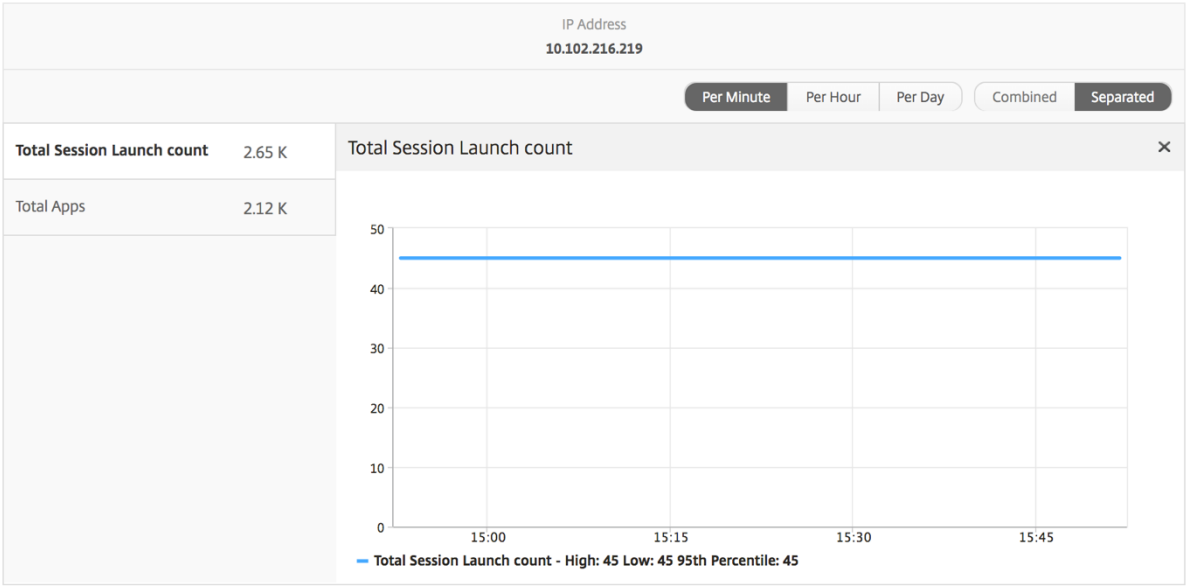
Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

To navigate to the instance view:

1. Navigate to **Gateway > HDX Insight > Instances**.
2. Select a particular instance from the **Instance Summary Report**.

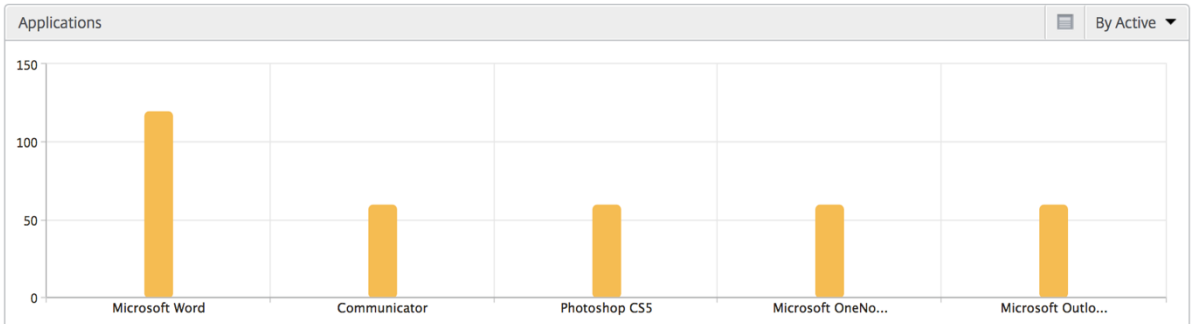
Line chart

Metrics	Description
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



Applications bar graph

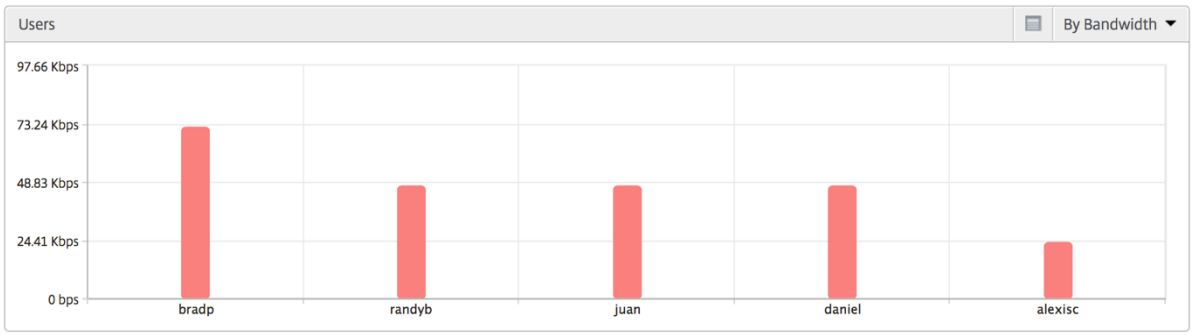
Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.



Users bar graph

The Users bar graph displays top 5 users based on the following criteria

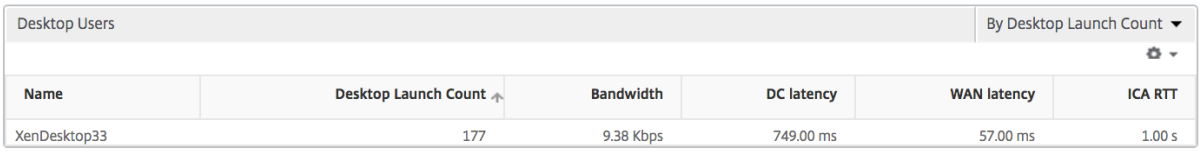
- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT



Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

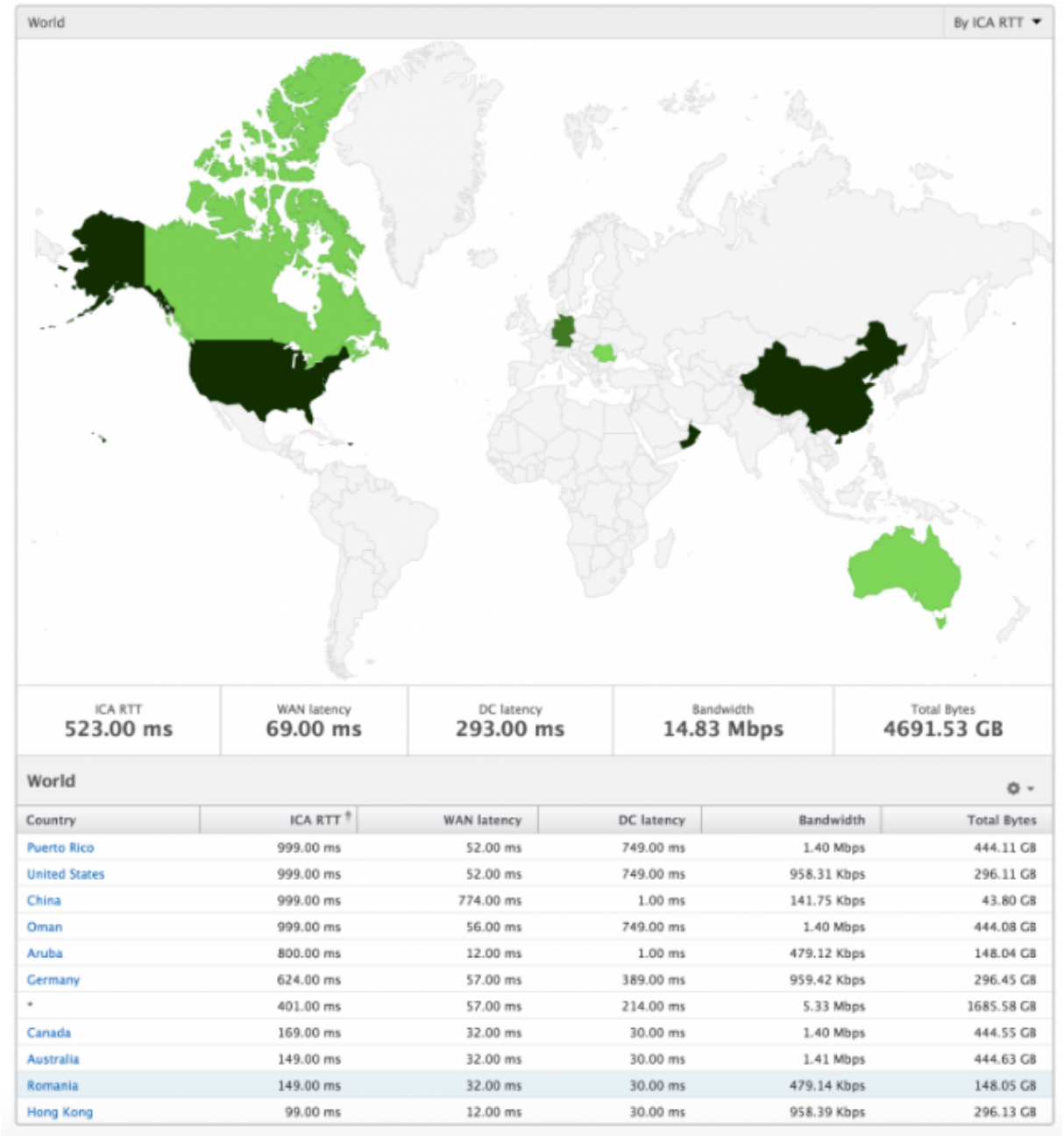


World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License View Reports and Metrics

December 31, 2023

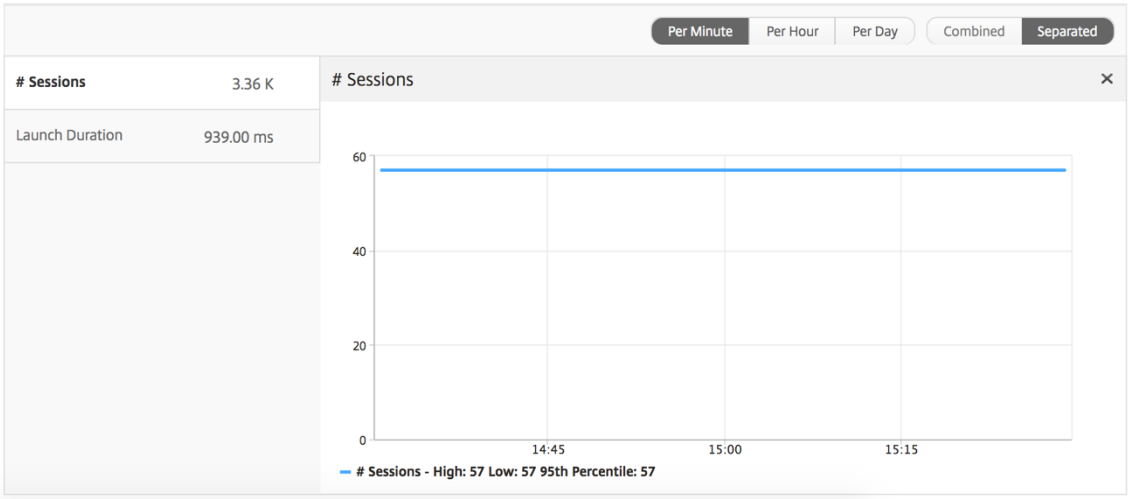
The license view gives details on the NetScaler Gateway license information.

To navigate to the license view:

1. Navigate to **Gateway > HDX Insight > Licenses**.

Line chart

Metrics	Description
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds and alerts.

Troubleshoot HDX Insight issues

March 11, 2024

If the HDX Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- HDX Insight configuration.
- Connectivity between NetScaler and NetScaler ADM.
- Record generation for HDX/ICA traffic in NetScaler.
- Population of records in NetScaler ADM.

HDX Insight configuration checklist

- Make sure that the AppFlow feature is enabled in NetScaler. For details, see Enabling AppFlow.
- Check HDX Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the HDX Insight configuration. Make sure that the bind type is ICA REQUEST. For example;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type ICA_REQUEST
  ```

  For transparent mode, the bind type must be ICA_REQ_DEFAULT. For example;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```
- For single-hop/Access Gateway or double-hop deployment, make sure that HDX Insight AppFlow policy is bound to the VPN virtual server, where HDX/ICA traffic is flowing.
- For Transparent mode or LAN user mode make sure the ICA ports 1494 and 2598 are set.
- Check `appflowlog` parameter in NetScaler Gateway or VPN virtual server is enabled for Access Gateway or double-hop deployment. For details, see Enabling AppFlow for Virtual Servers.
- Check "Connection Chaining"is enabled in double-hop NetScaler. For details see, Configuring NetScaler Gateway appliances to export data.
- After HA Failover if the HDX Insight details are Skip parsed, check ICA param "enableSRon-HAFailover"is enabled. For details, see Session Reliability on NetScaler High Availability Pair.

Connectivity between NetScaler and NetScaler ADM checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check HDX Insight AppFlow policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.

- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation for HDX/ICA traffic in NetScaler checklist

Run the command `tail -f /var/log/ns.log | grep -i "default ICA Message"` for log validation. Based on the logs that are generated, you can use this information for troubleshooting.

- Log: **Skipped parsing ICA connection - HDX Insight not supported for this host**

  Cause: Unsupported Citrix Virtual Apps and Desktops versions

  Workaround: Upgrade the Citrix Virtual Apps and Desktops servers to a supported version.

- Log: **Client type received 0x53, NOT SUPPORTED**

  Cause: Unsupported version of Citrix Workspace

  Solution: Upgrade Citrix Workspace to a supported version. For details, see Citrix Workspace app.

- Log: **Error from Expand Packet - Skipping all hdx processing for this flow**

  Cause: Issue with uncompressing ICA traffic

  Solution: No reports are available for this ICA session until a new session is established.

- Log: **Invalid transition: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**"

  Cause: Issue with parsing the ICA handshake

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Missing EUEM ICA RTT**

  Cause: Unable to parse End-User Experience Monitoring channel data

  Solution: Make sure End-User Experience Monitoring service in started on the Citrix Virtual Apps and Desktops servers. Make sure you are using the supported versions of Citrix Workspace App.

- Log: **Invalid Channel Header**

  Cause: Unable to identify channel header

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Skip code**

  If you see any of the following values for skip code, then the Insight details are skip parsed.

  > Skip code 0 indicates that the record is successfully exported from NetScaler.

Skip Code	Error message	Cause of error
100	NS_ICA_ERR_NULL_FRAG	Error handling ICA fragments, likely due to memory conditions
101	NS_ICA_ERR_INVALID_HS_CMD	Invalid handshake command received
102	NS_ICA_ERR_REDUC_PARAM_CNT	Invalid parameter specified for V3 expander initialization
103	NS_ICA_ERR_REDUC_INIT	Unable to initialize the V3 expander correctly
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Insufficient bytes to assign a coder to a channel
105	NS_ICA_ERR_INVALID_CHANNEL	Invalid ICA channel number
106	NS_ICA_ERR_INVALID_DECODER	Invalid decoder specified for a channel
107	NS_ICA_ERR_INVALID_TW_PARAM	Invalid parameter count specified on Thinwire channel
108	NS_ICA_ERR_INVALID_TW_DECODER	Invalid decoder for Thinwire channel
109	NS_ICA_ERR_REDUC_NO_DECODER	No decoder defined for channel
110	NS_ICA_ERR_REDUC_V3_EXPAND_FA	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_COR	Expander error: Bytes consumed more than bytes available
112	NS_ICA_ERR_REDUC_BYTES_OOR	Error: Uncompressed data overrun
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefined Expander command
114	NS_ICA_ERR_CGP_FILL_HOLE	Error while handling split CGP frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB allocation error –due to low memory conditions

Skip Code	Error message	Cause of error
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Memory allocation error for expander context
117	NS_ICA_ERR_ICA_OLD_SERVER	Old server, capability blocks not supported
118	NS_ICA_ERR_PIR_MANY_FRAG	Packet Init request is fragmented, unable to process
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA capability initialization error
120	NS_ICA_ERR_NO_MSI_SUPPORT	Host does not support MSI feature. Indicates for XenApp version lower than 6.5 or XenDesktop versions lower than 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Invalid CGP command encountered
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Insufficient bytes over channel
123	NS_ICA_ERR_CHANNEL_DATA	Incorrect data on EUEM, CONTROL, or SEAMLESS channel
124	NS_ICA_ERR_INVALID_PURE_CMD	Invalid command received while processing pure ICA channel data
125	NS_ICA_ERR_INVALID_PURE_LEN0	Invalid length encountered while processing pure ICA channel data
126	NS_ICA_ERR_INVALID_PURE_LEN	Invalid length encountered while processing PURE ICA channel data
127	NS_ICA_ERR_INVALID_CLNT_DATA	Invalid data length received from client
128	NS_ICA_ERR_MSI_GUID_SZ	Error in MSI GUID size
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Detected invalid channel header
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_VC	Retrieval of reconnected session failed
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Error in disabling SR

Skip Code	Error message	Cause of error
132	NS_ICA_ERR_REDUC_NOT_V3	Unsupported ICA Reducer version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression disabled, not honored by host
134	NS_ICA_ERR_IDENT_PROTO	Unable to identify ICA or CGP protocol, seen with incorrect workspaces
135	NS_ICA_ERR_INVALID_SIGNATURE	Incorrect ICA signature or magic string
136	NS_ICA_ERR_PARSE_RAW	Error while parsing the ICA handshake packet
137	NS_ICA_ERR_INCOMPLETE_PKT	Incomplete packet received in handshake
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA frame is too large, exceeds 1460 bytes
139	NS_ICA_ERR_FORWARD	Error while forwarding the ICA data
140	NS_ICA_ERR_MAX_HOLES	Unable to process CGP command as it is split beyond supported limit
141	NS_ICA_ERR_ASSEMBLE_FRAME	Unable to reassemble ICA frame correctly
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Skipped parsing for this workspace (client) as it is not in the allow list
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Unable to detect parsing state for client reconnect cookie
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Invalid reconnect cookie length detected post client reconnect
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects cookie missed the needed constraint
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Invalid workspace version string received from client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Invalid product ID received from client
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Invalid channel length post expansion

Skip Code	Error message	Cause of error
149	NS_ICA_ERR_SPECIAL_THINWIRE	Decompression error
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Encountered insufficient bytes for seamless command
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Encountered insufficient bytes for EUEM command
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Invalid event for seamless channel parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Invalid event for CTRL channel parsing
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Invalid event for EUEM channel parsing
155	NS_ICA_ERR_USB_INVALID_EVENT	Invalid event for USB channel parsing
156	NS_ICA_ERR_PURE_INVALID_EVENT	Invalid event for pure channel parsing
157	NS_ICA_ERR_VCP_INVALID_EVENT	Invalid event for virtual channel parsing
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Invalid event for ICA data parsing
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Invalid event for CGP data parsing
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Invalid state for a crypt command in basic encryption
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Invalid crypt command in basic encryption
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Invalid state for a crypt command in RC5 encryption
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Invalid crypt command in RC5 encryption
164	NS_ICA_ERR_ADVCRYPT_ENC	Error in RC5 encryption/decryption
165	NS_ICA_ERR_ADVCRYPT_DEC	Error in RC5 encryption/decryption
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA does not support Reducer Version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace does not support Reducer Version 3

Skip Code	Error message	Cause of error
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unexpected number of bytes in ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Higher CGP resumption sequence number from peer post reconnects
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Unable to restore ICA parsing state post reconnect
171	NS_ICA_ERR_NSAP_PARSING	Error while parsing Insight channel data
172	NS_ICA_ERR_NSAP_APP	Error while parsing app details from Insight channel data
173	NS_ICA_ERR_NSAP_ACR	Error while parsing ACR details from Insight channel data
174	NS_ICA_ERR_NSAP_SESSION_END	Error while parsing session end details from Insight channel data
175	NS_ICA_ERR_NON_NSAP_SN	Skipped ICA parsing on service node due to the absence of Insight channel support
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP is not supported by client
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP is not supported by VDA
178	NS_ICA_ERR_NSAP_NEG_FAIL	Error while NSAP data negotiation
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Error in fetching service reconnects ticket in service node
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Error when receiving higher reconnect sequence number in service node
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Error while disabling HDX Insight for non-NSAP connections

Sample logs:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
```



```
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"

Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Error counters

Various counters are captured ICA parsing. The following table lists the various counters for ICA parsing.
Run the command `nsconmsg –g hdx –d statswt0`for viewing the counter details.

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_tot_ica_conn	Indicates total number of Pure ICA connections detected by NS. Incremented whenever an ICA connection based on the ICA signature on a client PCB is detected.	Stats
hdx_tot_cgp_conn	Indicates total number of CGP connections detected by NS (Session Reliability ON). Incremented whenever a CGP connection based on the CGP signature on a client PCB is detected.	Stats
hdx_dbg_tot_udt_conn	Indicates total number of UDP ICA connections detected by NS	Stats

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_tot_nsap_conn	Indicates total number of NSAP supported connections detected by NS	Stats
hdx_tot_skip_conn	Indicates how many ICA connections were skipped by parser due to invalid ICA or CGP signature.	Stats
hdx_dbg_active_conn	Total Active EDT/CGP/ICA connections at that instant.	Stats
hdx_dbg_active_nsap_conn	Total Active EDT/CGP/ICA NSAP connections at that instant.	Stats
hdx_dbg_skip_appflow_disabled	Total number of instances where AppFlow was detached from a session because of disabling AppFlow	Stats/Diagnostics
hdx_dbg_transparent_user	Total number of transparent user access	Stats/Diagnostics
hdx_dbg_ag_user	Total number of Access Gateway user access	Stats/Diagnostics
hdx_dbg_lan_user	Total number of LAN user mode access	Stats/Diagnostics
hdx_basic_enc	Indicates the number of ICA connections using basic encryption	Stats/Diagnostics
hdx_advanced_enc	Indicates the number of ICA connections using advanced RC5 based encryption	Stats/Diagnostics
hdx_dbg_reconnected_session	Total number of reconnect requests from client without any NetScaler error	Stats/Diagnostics
hdx_dbg_host_rejected_ns_reconnect	Total number of hosts rejected reconnects requests by client	Stats/Diagnostics

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_euem_available	Indicates the number of connections having the End User Experience Monitoring channel available. End User Experience Monitoring channel is required to collect statistics such as ICA RTT.	Stats/Diagnostics
hdx_err_disabled_sr	Session Reliability is disabled using `nsapimgr` knob. Session does not work for this session.	Error
hdx_err_skip_no_msi	XA/XD server is Missing MSI capability. This indicates an older server version and HDX Insight skips this connection.	Error
hdx_err_skip_old_server	Old unsupported server version	Error
hdx_err_clnt_not_whitelist	Client workspace not in allow list, HDX Insight skips this connection	Error
hdx_sm_ica_cam_channel_disabled	Total number of NS_ICA_CAM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_usb_channel_disabled	Total number of NS_ICA_USB_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_clip_channel_disabled	Total number of NS_ICA_CLIP_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_ccm_channel_disabled	Total number of NS_ICA_CCM_CHANNEL disabled via SmartAccess policy	Diagnostics

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_sm_ica_cdm_channel_disabled	Total number of NS_ICA_CDM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com1_channel_disabled	Total number of NS_ICA_COM1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com2_channel_disabled	Total number of NS_ICA_COM2_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cpm_channel_disabled	Total number of NS_ICA_CPM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_lpt1_channel_disabled	Total number of NS_ICA_LPT1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_lpt2_channel_disabled	Total number of NS_ICA_LPT2_CHANNEL disabled via SmartAccess policy	Diagnostics
dx_dbg_sm_ica_msi_disabled	Total number of cases where MSI is disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_file_channel_disabled	Total number of NS_ICA_FILE_CHANNEL is disabled via SmartAccess policy	Diagnostics
hdx_dbg_usb_accept_device	Total number of USB devices accepted	Diagnostics
hdx_dbg_usb_reject_device	Total number of USB devices rejected	Diagnostics
hdx_dbg_usb_reset_endpoint	Total number of USB endpoints reset	Diagnostics

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_usb_reset_device	Total number of USB devices reset	Diagnostics
hdx_dbg_usb_stop_device	Total number of USB devices stopped	Diagnostics
hdx_dbg_usb_stop_device_response	Total number of responses from stopped USB devices	Diagnostics
hdx_dbg_usb_device_gone	Total number of USB devices gone	Diagnostics
hdx_dbg_usb_device_stopped	Total number of USB devices stopped	Diagnostics

nstrace validation

Check for CFLOW protocol to see all AppFlow records going out of NetScaler.

Population of records in NetScaler ADM checklist

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`and check logs to confirm NetScaler ADM is receiving AppFlow records.
- Confirm NetScaler instance is added to NetScaler ADM.
- Validate NetScaler Gateway/VPN virtual server is licensed in NetScaler ADM.
- Make sure multi-hop parameter setting is enabled for double-hop.
- Make sure NetScaler Gateway is cleared for second-hop in double-hop deployment.

Before contacting Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler ADM versions.
- Citrix Virtual Apps and Desktops server versions.
- Client Workspace versions.

- Number of Active ICA sessions when the issue occurred.
- Tech support bundle captured by running the `show techsupport` command at the NetScaler command prompt.
- Tech support bundle captured for NetScaler ADM.
- Packet traces captured on all NetScaler.
  To start a packet trace, type, `start nstrace -size 0'`
  To stop a packet trace, type, `stop nstrace`
- Collect entries in the system's ARP table by running the `show arp` command.

Known Issues

Refer ADC release notes for known issues on HDX Insight.

Infrastructure Analytics

March 11, 2024

A key goal for network administrators is to monitor NetScaler instances. ADC instances offer interesting insights into usage and performance of applications and desktops accessed through it. Administrators must monitor the ADC instance and analyze the application flows processed by each ADC instance. They can be able to remediate any probable issues in configuration, setup, connectivity, certificates, and others which might impact application usage or performance. For example, a sudden change in the application traffic pattern can be due to change in SSL configuration like disabling of an SSL protocol. Administrators must be able to quickly identify the correlation between these data points to ensure the following:

- Application availability is in an optimal state
- There are no resource consumption, hardware, capacity, or configuration change issues
- There are no unused inventories
- There are no expired certificates

Infrastructure Analytics feature simplifies the process of data analysis by correlating multiple data sources and quantifying it to a measurable score that defines the health of an instance. With this feature, the administrators get a single touch point to understand if there is a problem, the origin of the problem, and probable remediations that they can perform.

Infrastructure analytics

The NetScaler Application Delivery Management (ADM) Infrastructure analytics feature collates all the data gathered from the NetScaler instances and quantifies it into an **Instance Score** that defines the health of the instances. The instance score is summarized over a tabular view or as circle pack visualization. The Infrastructure Analytics feature helps you to visualize the factors that resulted or might result in an issue on the instances. This visualization also helps you to determine the actions that must be performed to prevent the issue and its recurrence.

Instance score

Instance score indicates the health of an ADC instance. A score of 100 means a perfectly healthy instance without any issues. Instance score captures different levels of potential issues on the instance. It is a quantifiable measurement of instance health and multiple "health indicators"contribute to the score.

Health indicators are the building blocks of the instance score, where the score is computed periodically for a predefined "monitoring period,"based on all detected indicators in that time window. Currently, Infrastructure analytics calculates the instance score once every hour based on the data collected from the instances.
An indicator can be defined as any activity (an event or an issue) that belongs to one of the following categories on the instances.

- System resource indicators
- Critical events indicators
- SSL configuration indicators
- Configuration deviation indicators

Health indicators

- System resources indicators

  The following are the critical system resource issues that might occur on NetScaler instances and monitored by NetScaler ADM.

  - **High CPU usage**. The CPU usage has crossed the higher threshold value in the NetScaler instance.
  - **High memory usage**. The memory usage has crossed the higher threshold value in the NetScaler instance.

- **High disk usage**. The disk usage has crossed the higher threshold value in the NetScaler instance.
- **Disk errors**. There are errors on hard disk 0 or hard disk 1 on the hypervisor where the ADC instance is installed.
- **Power failure**. The power supply has failed or disconnected from the ADC instance.
- **SSL card failure**. The SSL card installed on the instance has failed.
- **Flash errors**. There are Compact Flash Errors seen on the NetScaler instance.
- **NIC discards**. The packets discarded by the NIC card have crossed the higher threshold value in the NetScaler instance.

For more information on these system resources errors, see The instance dashboard.

- Critical events indicators

  The following critical events are identified by the events under event management feature of ADM that are configured with critical severity.

  - **HA sync failure**. Configuration sync between the ADC instances in high availability has failed on the secondary server.
  - **HA no heartbeats**. The primary server in a pair of ADC instances in high availability is not receiving heart beats form the secondary server.
  - **HA bad secondary state**. The secondary server in a pair of ADC instances in high availability is in Down, Unknown, or Stay secondary state.
  - **HA version mismatch**. The version of the ADC software images installed on a pair of ADC instances in high availability does not match.
  - **Cluster sync failure**. Configuration sync between the ADC instances in cluster mode has failed.
  - **Cluster version mismatch**. The version of the ADC software images installed on the ADC instances in cluster mode does not match.
  - **Cluster propagation failure**. Propagation of configurations to all instances in a cluster has failed.

    > **Note**
    >
    > You can have your list of critical SNMP events by changing the severity levels of the events. For more information on how to change the severity levels, see Modify the reported severity of events that occur on NetScaler instances.

  For more information on events in NetScaler ADM, see Events.

- SSL configuration indicators
  - **Not recommended key strength**. The key strength of the SSL certificates is not as per NetScaler standards
  - **Not recommended issuer**. The issuer of the SSL certificate is not recommended by Citrix.
  - **SSL certs expired**. The SSL certificate installed in the ADC instance has expired.
  - **SSL certs expiry due**. The SSL certificate installed in the ADC instance is about to expire in the next one week.
  - **Not recommended algorithms**. The signature algorithms of SSL certificates installed in the ADC instance are not as per NetScaler standards.

For more information on SSL certificates, see SSL dashboard.

- Configuration deviation indicators
  - **Config drift template**. There is a drift (unsaved changes) in configuration from the audit templates that you have created with specific configurations you want to audit on certain instances.
  - **Config drift default**. There is a drift (unsaved changes) in configuration from the default configuration files.

For more information on configuration deviations and how to run audit reports to check configuration deviation, see View audit reports.

View ADC Capacity issues

When an ADC instance has consumed most its available capacity, packet-drop may occur while processing the client traffic. This issue causes low performance in an ADC instance. By understanding such ADC capacity issues, you can allocate additional licenses proactively to steady the ADC performance.

To view ADC capacity issues,

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Expand the instance for which you want to view capacity issues.

The ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters:

- **Throughput Limit Reached** –The number of packets dropped in the instance after the throughput limit is reached.

- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** –The number of packets dropped in the instance after PPS limit is reached.
- **SSL Throughput Rate Limit** –The number of times the SSL throughput limit reached.
- **SSL TPS Rate Limit** –The number of times the SSL TPS limit reached.

The ADM calculates the instance score on the defined capacity threshold.

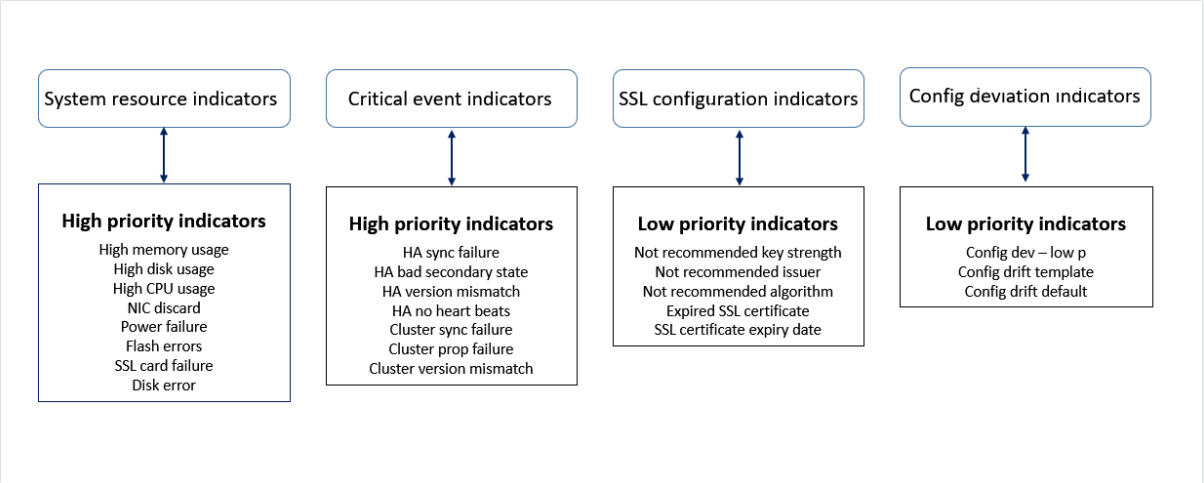
- Low threshold –1 packet drop or rate-limit counter increment
- High threshold –10000 packets drop or rate-limit counter increment

Therefore, when an ADC instance breaches the capacity threshold the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the `ADCCapacityBreach` category. To view these events, navigate to **Accounts > System Events**.

Value of health indicators

The indicators are classified into high priority indicators and low-priority indicators based on their values as follows:



The health indicators within the same group of indicators have different weights assigned to them. One indicator might contribute more to lowered instance score than another indicator. For example, high memory usage brings down the instance score more than high disk usage, high CPU usage, and NIC discard. If an instance has a greater number of indicators detected on it, the lesser is the instance score.

The value of an indicator is calculated based on the following rules. The indicator is said to be detected in one of the following three ways:

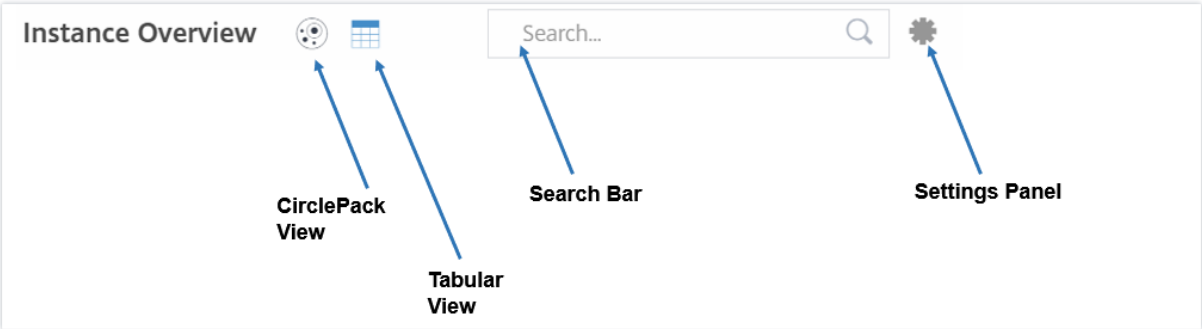
1. **Based on an activity**. For example, a System resource indicator is triggered whenever there is a power failure on the instance, and this indicator reduces the value of the instance score. When the indicator is cleared the penalty is cleared, and the instance score increases.
2. **Based on the threshold value breach**. For example, a System resource indicator is triggered when the NIC card discards packets and the threshold level is breached.
3. **Based on the low and high threshold value breach**. Here, an indicator can be triggered in two ways:
    - When the value of the indicator is between low and high thresholds, in which case a partial penalty is levied on the instance score.
    - When the value crosses the high threshold, in which case a full penalty is levied on the instance score.
    - No penalty is levied on the instance score if the value falls below a low threshold.

For example, CPU usage is a system resource indicator triggered when the usage value crosses the low threshold and also when the value crosses the high threshold.

Infrastructure analytics dashboard

Navigate to **Infrastructure > Infrastructure Analytics**.

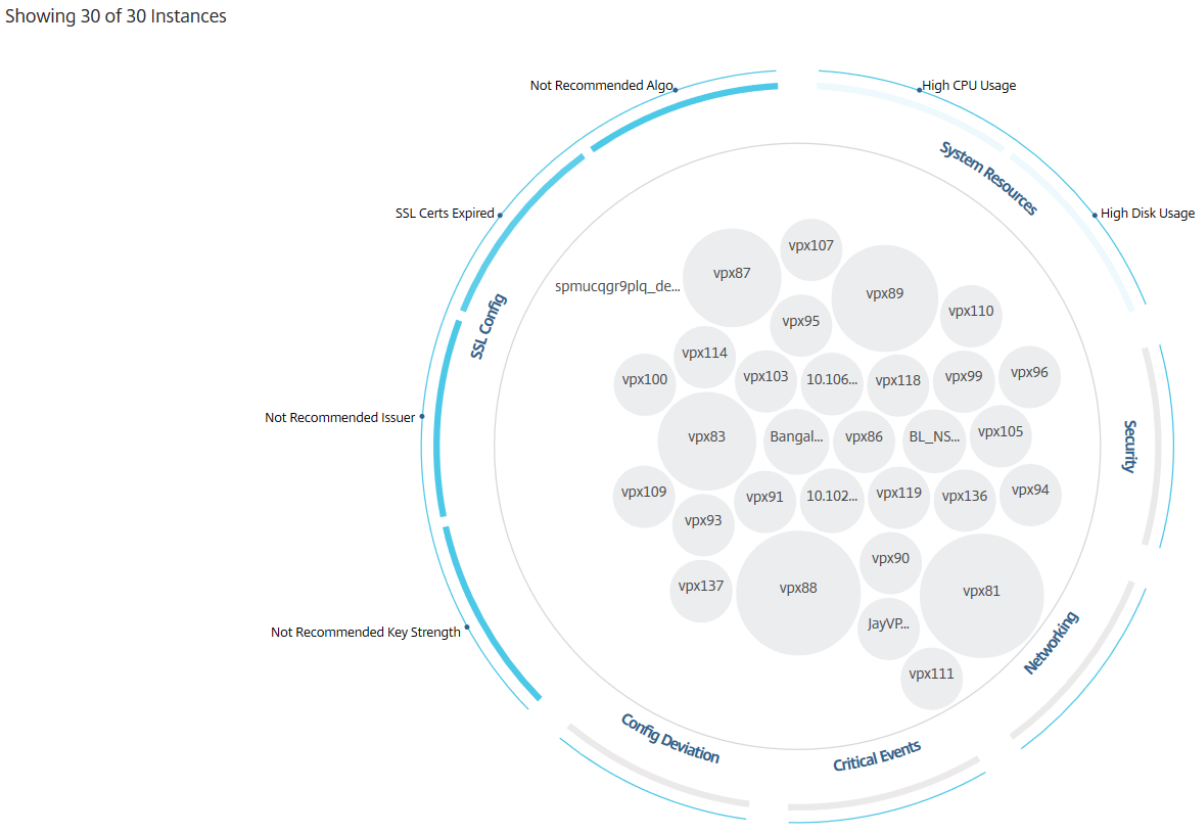
The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.



- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view formats, the Summary Panel displays details of all the instances in your network.

Circle pack view

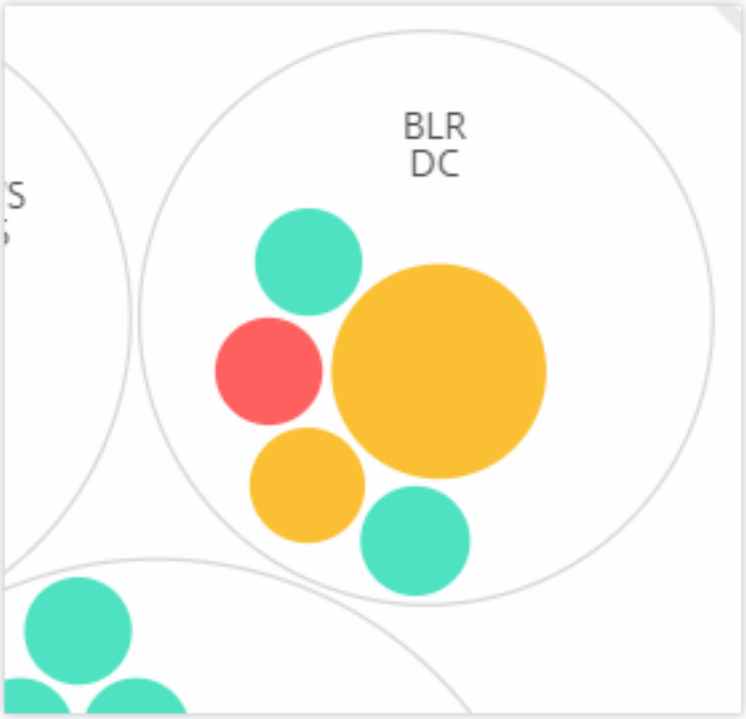
Circle packing diagrams show instance groups as tightly organized circles. They often show hierarchies where smaller instance groups are either colored similarly to others in the same category, or nested within larger groups. Circle packs represent hierarchical data sets and shows different levels in the hierarchy and how they interact with each other.



Instance circles

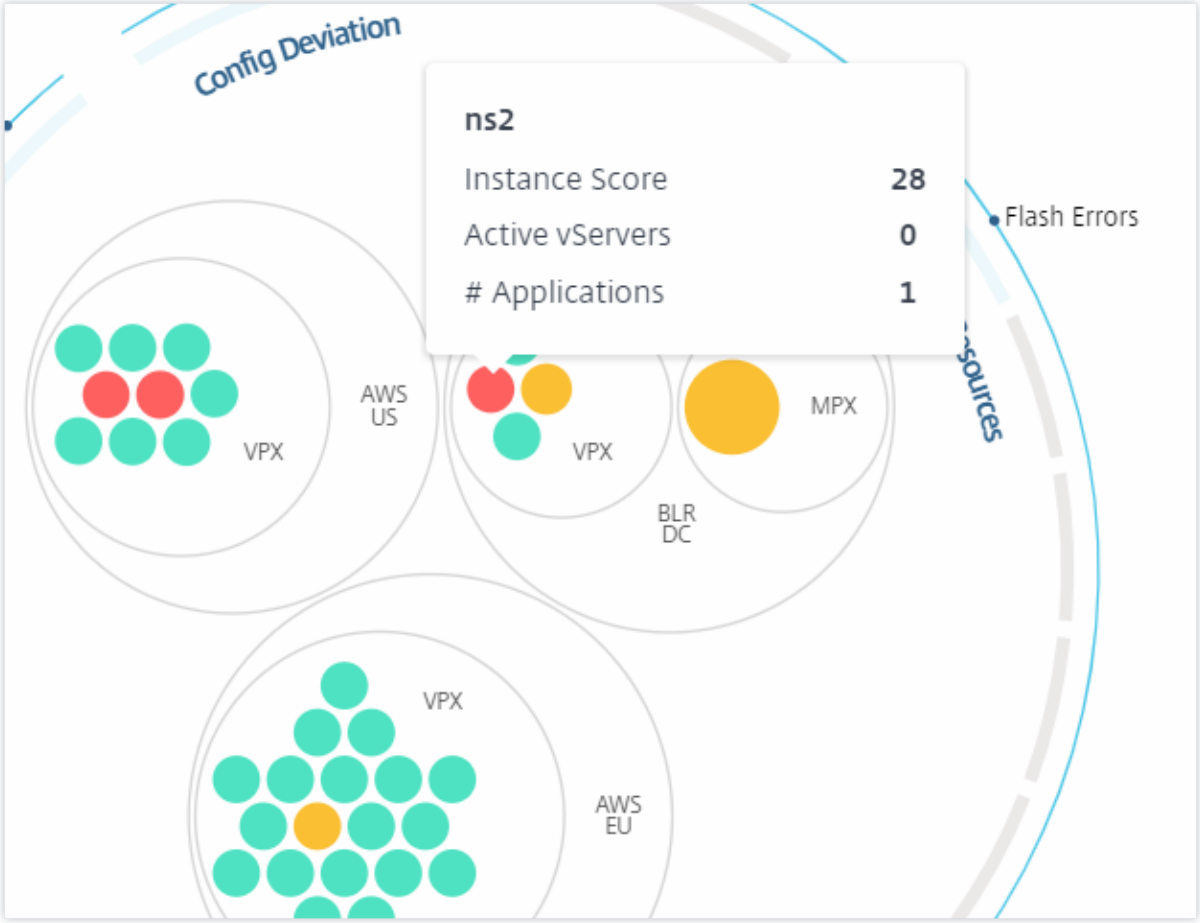
Color. Each instance is represented in Circle Pack as a colored circle. The color of the circle indicates the health of that instance.

- **Green** - instance score is between 100 and 80. The instance is healthy.
- **Yellow** - instance score is between 80 and 50; some issues have been noticed and in need of review.
- **Red** - instance score is below 50. The instance is in a critical stage as there are multiple issues noticed on that instance.



Size. The size of these colored circles indicates the number of virtual servers configured on that instance. A bigger circle indicates that there are a greater number of virtual servers.

You can hover the mouse pointer on each of the instance circles (colored circles) to view a summary. The hover tool tip displays the host name of the instance, the number of active virtual servers and the number of applications configured on that instance.

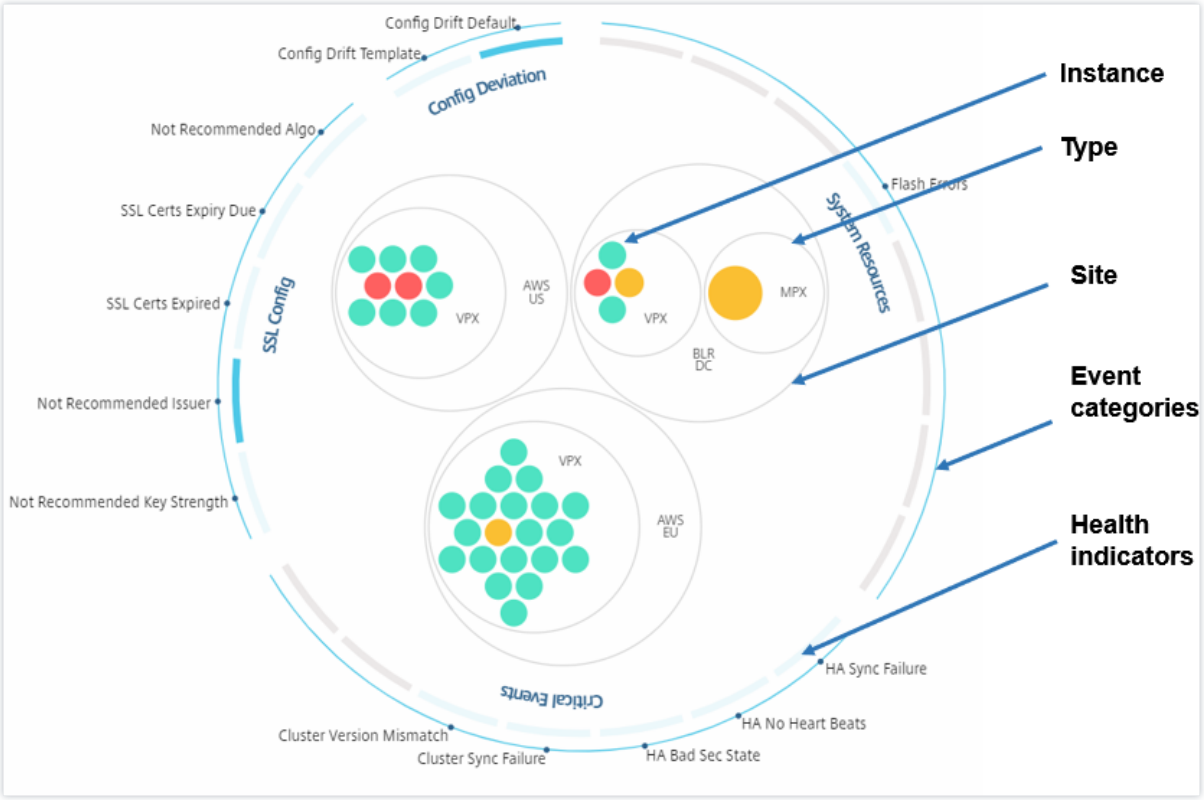


Grouped instance circles

The Circle Pack at the outset, comprises instance circles that are grouped, nested, or packed inside another circle based on the following criteria:

- the site where they are deployed
- the type of instances deployed - VPX, MPX, SDX, and CPX
- the virtual or physical model of the ADC instance
- the ADC image version installed on the instances

The following image shows a Circle Pack where the instances are first grouped by the site or data center where they are deployed, and then they are further grouped based on their type, VPX, and MPX.

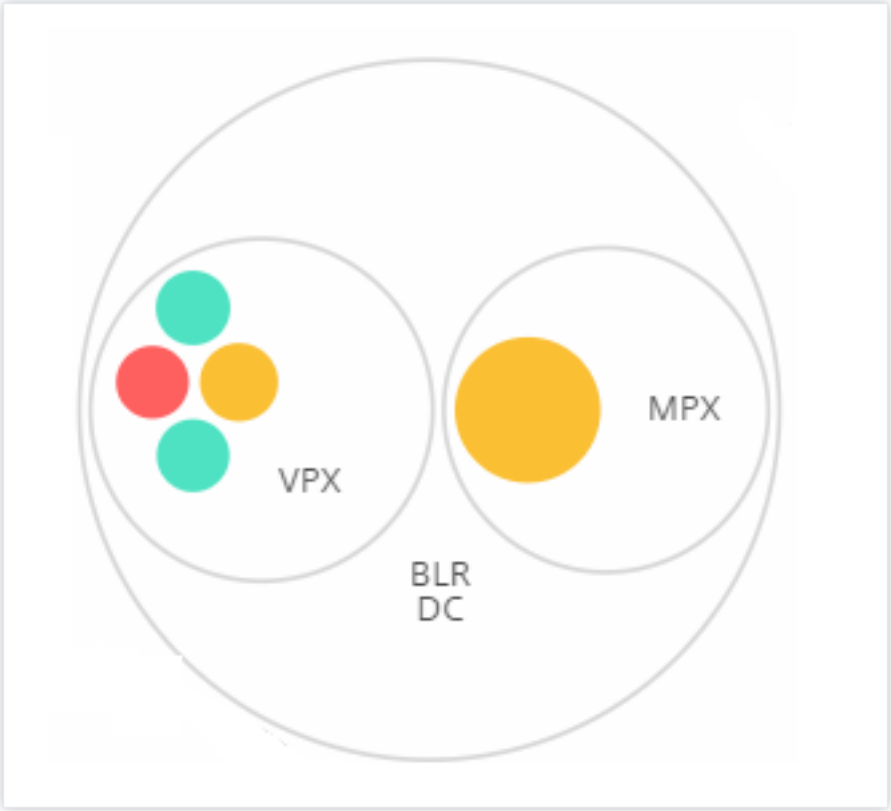


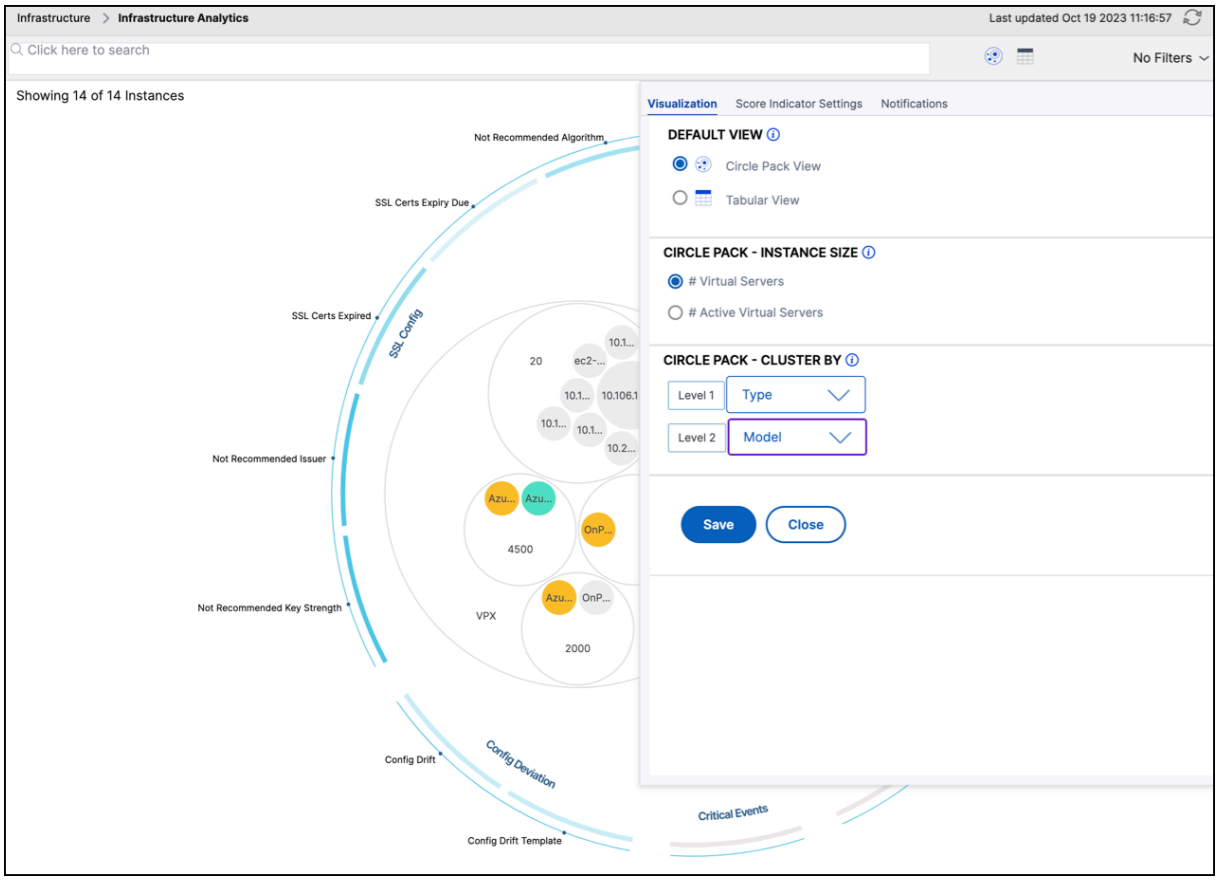
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the NetScaler ADM (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

Clustered instance circles

NetScaler ADM monitors many instances. To ease the monitoring and maintenance of these instances, Infrastructure Analytics allows you to cluster them at two levels. That is, the instance groupings can be nested within another grouping.

For example, the BLR data center has two types of ADC instances - VPX and MPX, deployed in it. You can first group the ADC instances by their type and then group all instances by the site where they are grouped. You can now easily identify how many types of instances are deployed in the sites that you are managing.

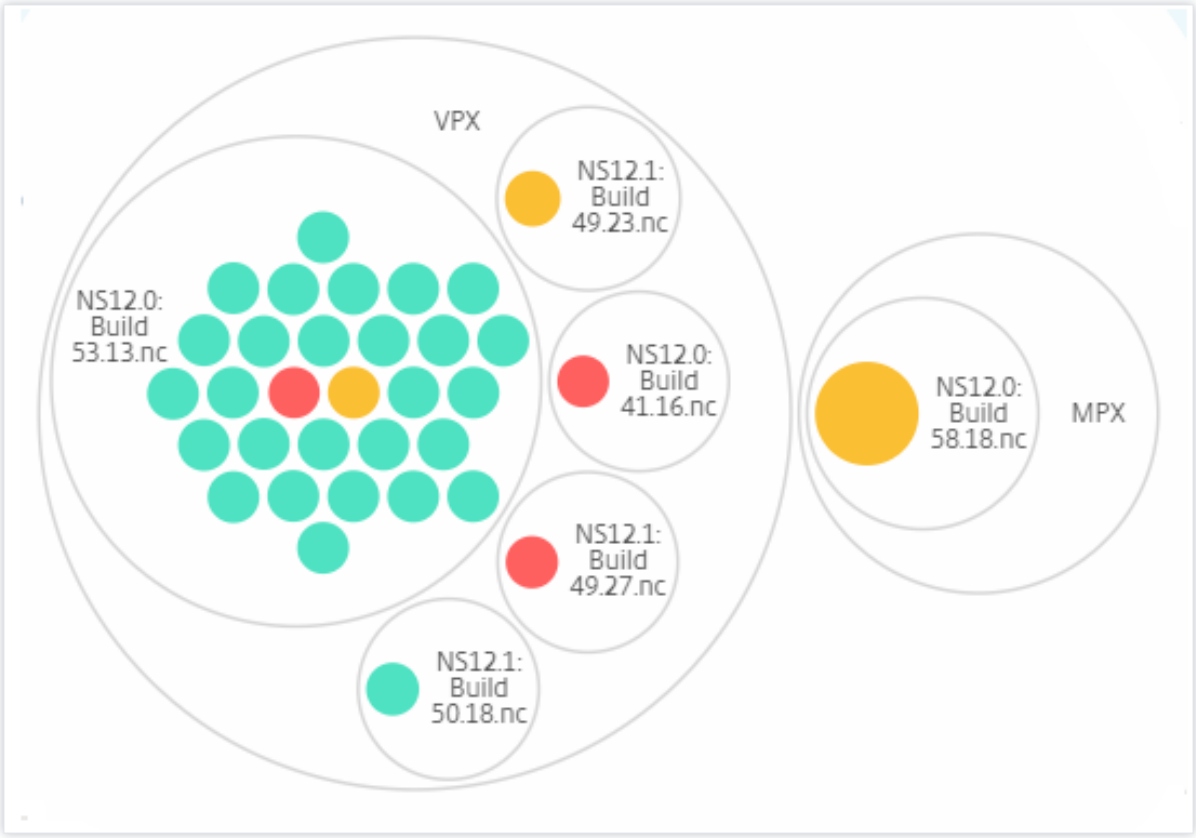




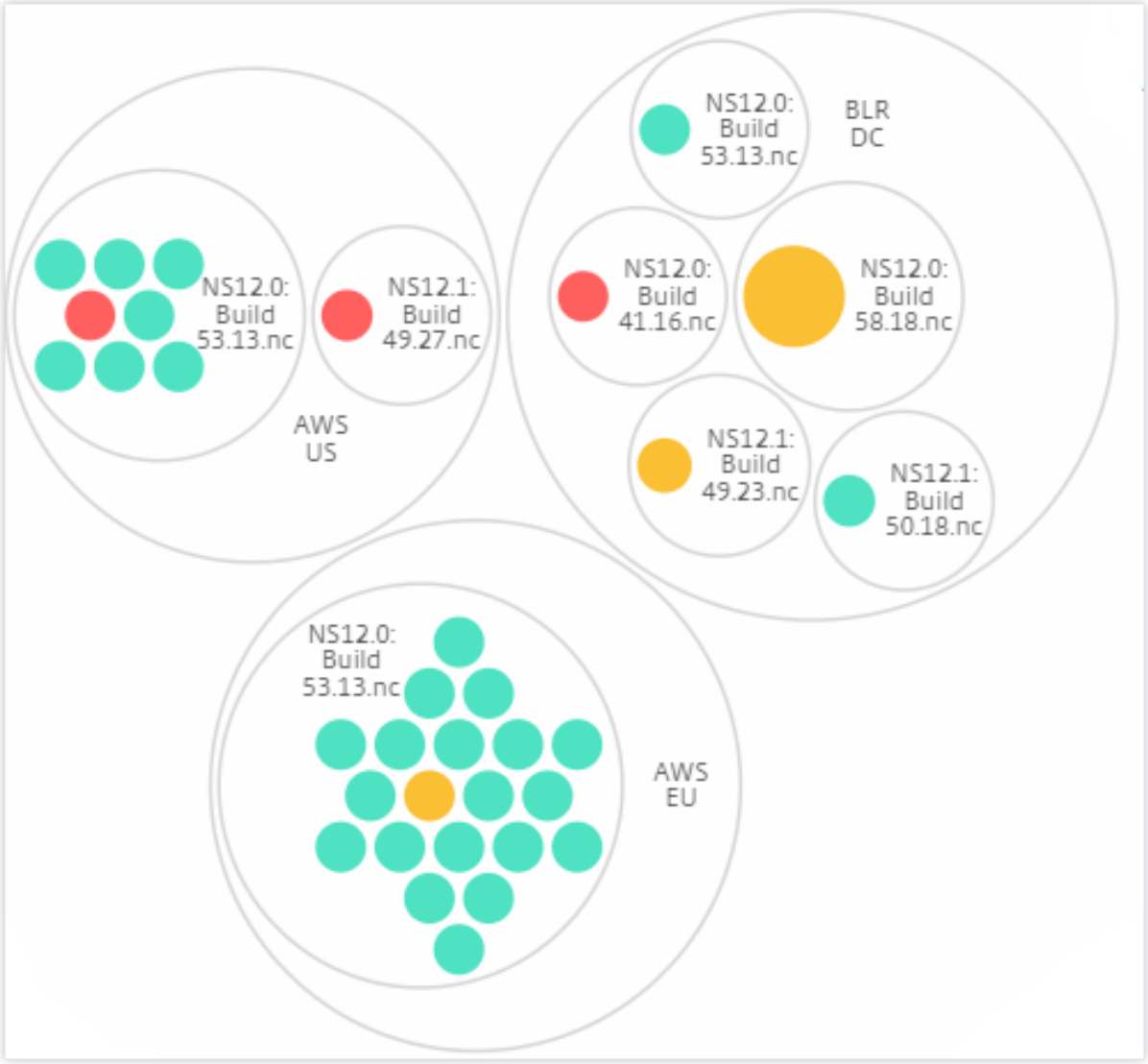
A few more examples of two-level clustering are as follows:

Site and model:

Type and version:

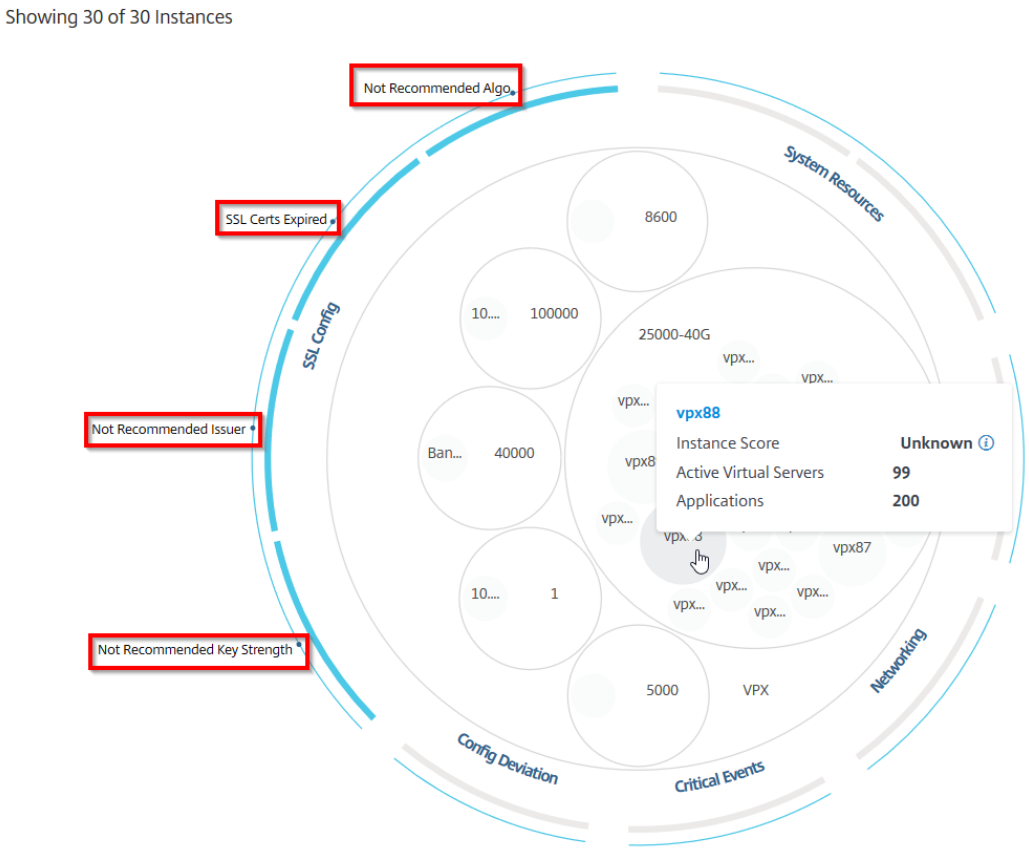


Site and version:



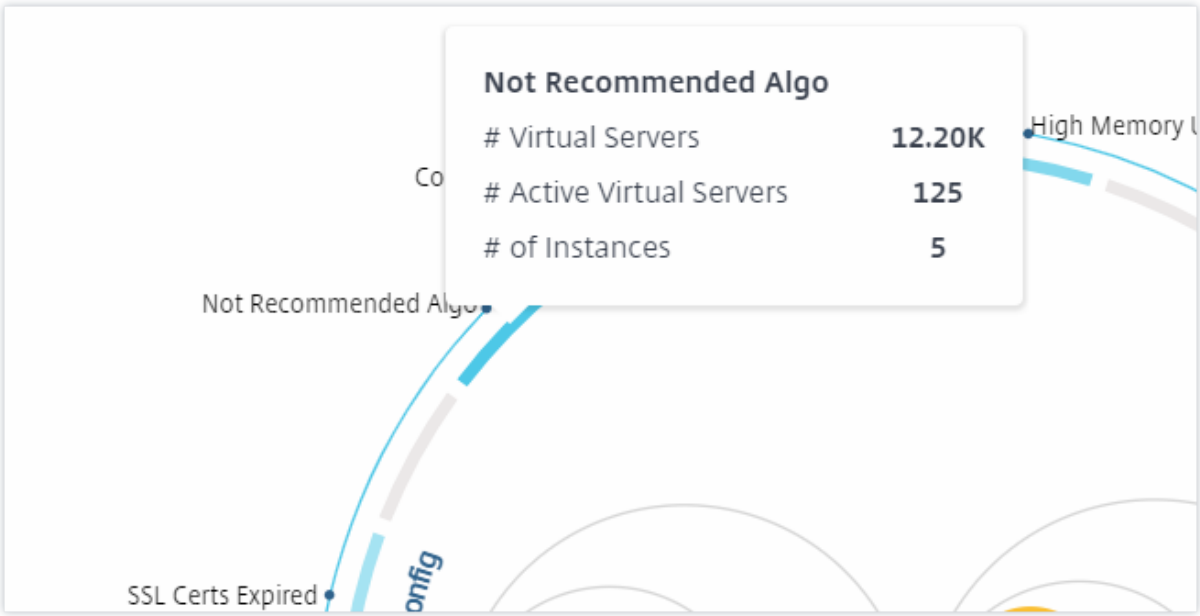
How to use Circle Pack

Click each of the colored circle to highlight that instance.



Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.

You can also click the health indicators to get more details on the number of instances that have reported that risk indicator. For example, click `Not recommended Algo` to view the summary report of that risk indicator.

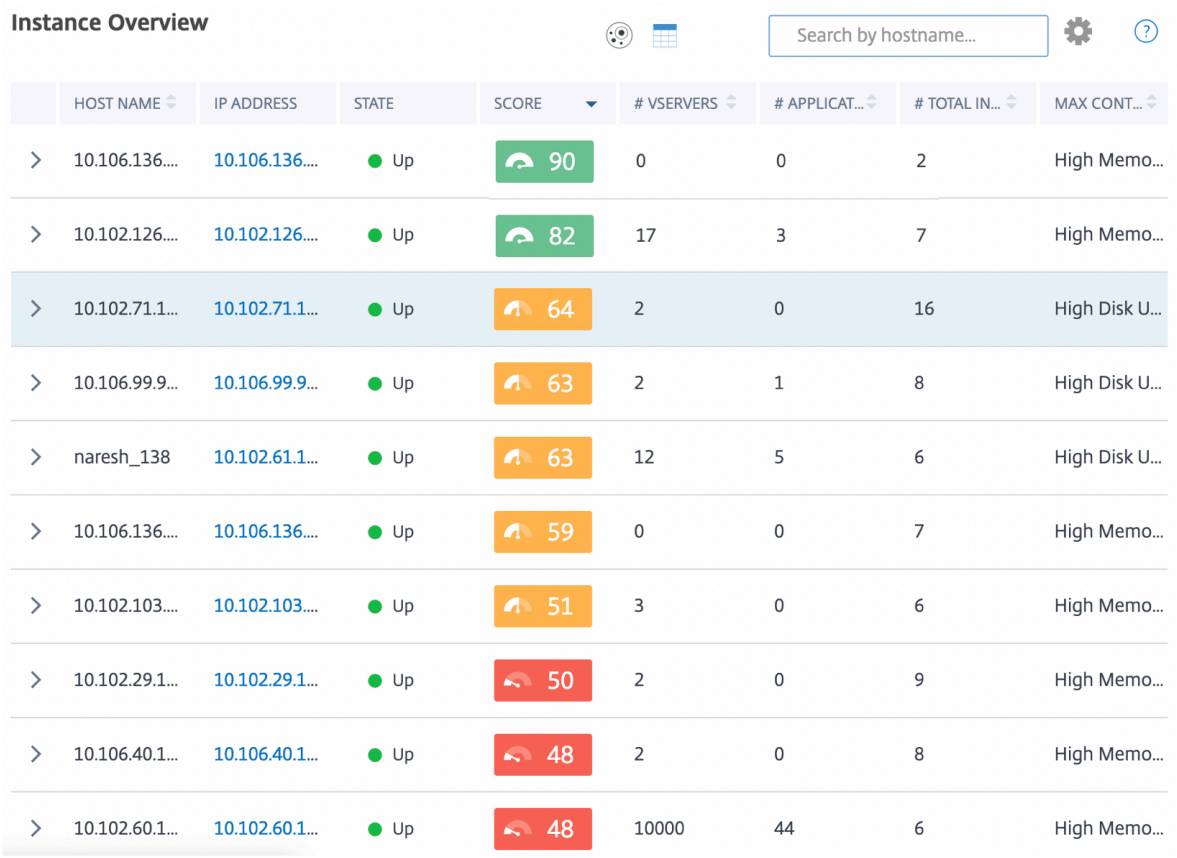


Tabular view

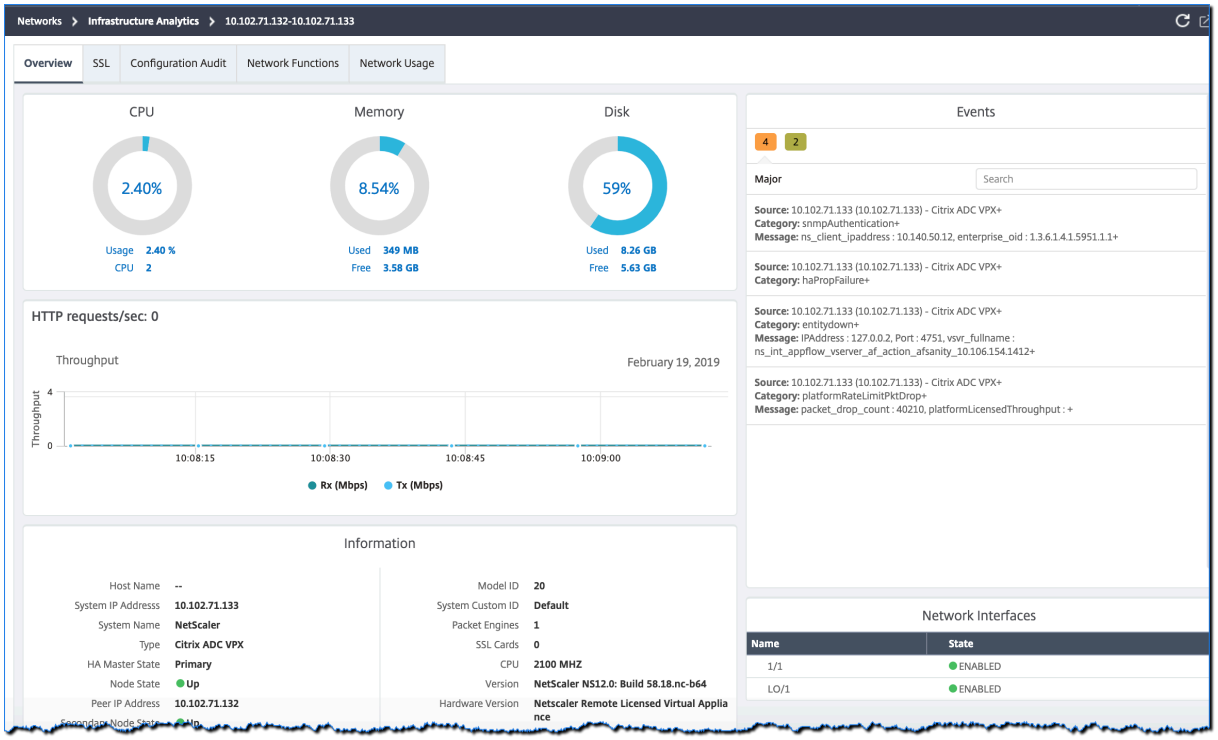
The tabular view displays the instances and the details of those instances in a tabular format. The details that are displayed are as follows:

- Host name of the instance
- The IP address of the instance
- State of the instance
- Instance score
- Number of virtual servers configured on that instance
- Number of applications configured on that instance
- Total number of risk indicators
- The event that is contributing more to a lowered instance score

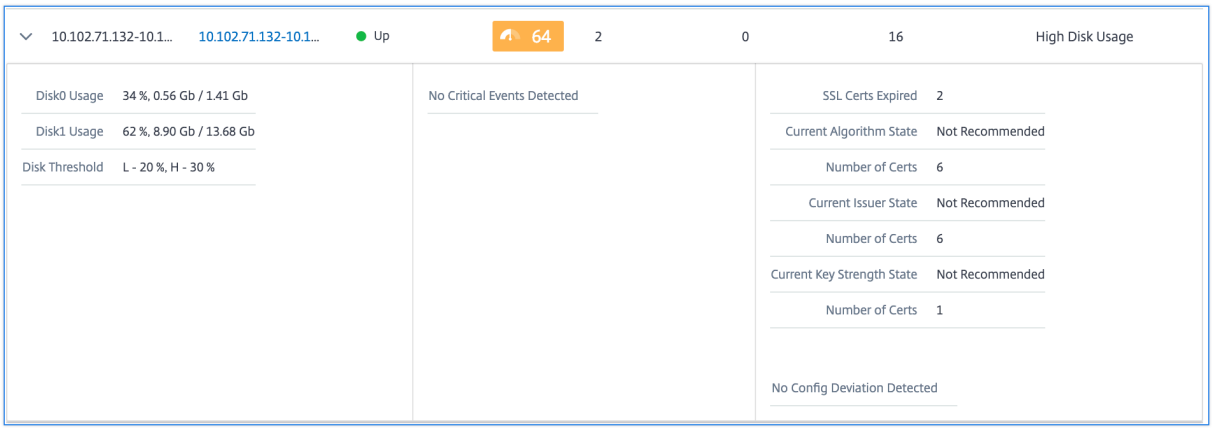
The instances that are in the critical state are at the top of the table, followed by the instances that need to be reviewed and then the healthier instances.



Click the instance IP address in the tabular view to see more details of that instance as a dashboard display. The instance dashboard presents an overview of the instance where you can see the CPU, memory, and the disk usage of the instance. You can also see details related to SSL certificate management, config audit, network functions, and a network report that shows detailed network usage of the instance. Scroll down further to see the list of the features and the modes enabled on this instance.



You can also click the arrow at the beginning of each row to expand the row for more details.



The expanded table row displays the errors that have occurred on the instance for all the categories. In the example above, you can view that there have been errors in system resources, SSL configuration, and deviations in configuration files. But there are no critical events reported from the instance.

How to use the summary Panel

The **Summary Panel** assists you in efficiently and quickly focuses on the instances that are in need of review or critical state. The panel is divided into three tabs - overview, instance info, and traffic profile. The changes you make in this panel modifies the display in both Circle Pack and Tabular view formats. The following sections describe these tabs in more detail. The examples in the following

sections assist you to use the different selection criteria efficiently to analyze the issues reported by the instances.

Overview:

The **Overview** tab allows you to monitor the instances based on the hardware errors, usage, expired certificates and similar indicators that can occur in the instances. The indicators that you can monitor here are as follows:

- CPU usage
- Memory usage
- Disk usage
- System failures
- Critical events
- SSL certificates expiry

The following examples illustrate how you can interact with the **Overview** panel to isolate those instances that are reporting errors.

Example 1: View instances that are in a review state:

Select **Review** check box to view only those instances that are not reporting critical errors, but still needs attention.

The Histograms in the **Overview** panel represent an aggregated number of instances based on high CPU usage, high memory usage, and high disk usage events. The Histograms are graded at 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, and 100%. Hover your mouse pointer on one of the bar charts. The legend at the bottom of the chart displays the usage range and the number of instances in that range. You can also click the bar chart to display all the instances in that range.

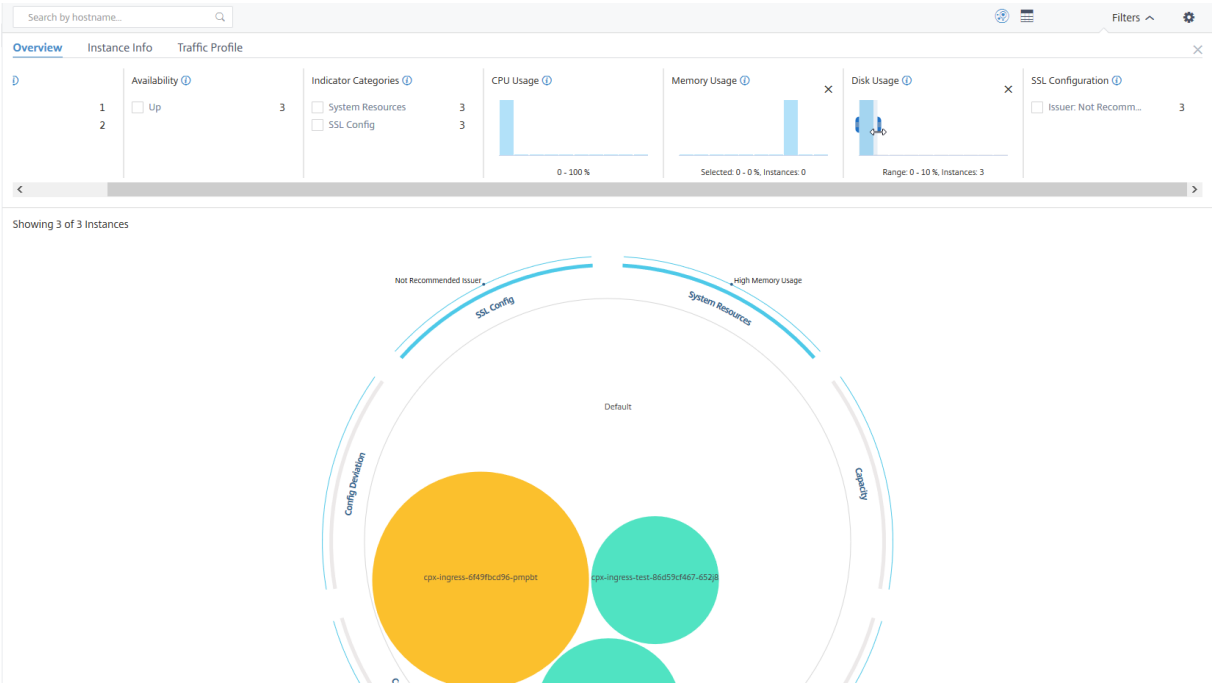
Example 2: View instances that are consuming between 10% and 20% of the allocated memory:

In the memory usage section, click the bar chart. The legend shows that the selected range is 10–20% and there are 29 instances operating in that range.

You can also select multiple ranges in these histograms.

Example 3: View instances that are consuming high disk space in multiple ranges:

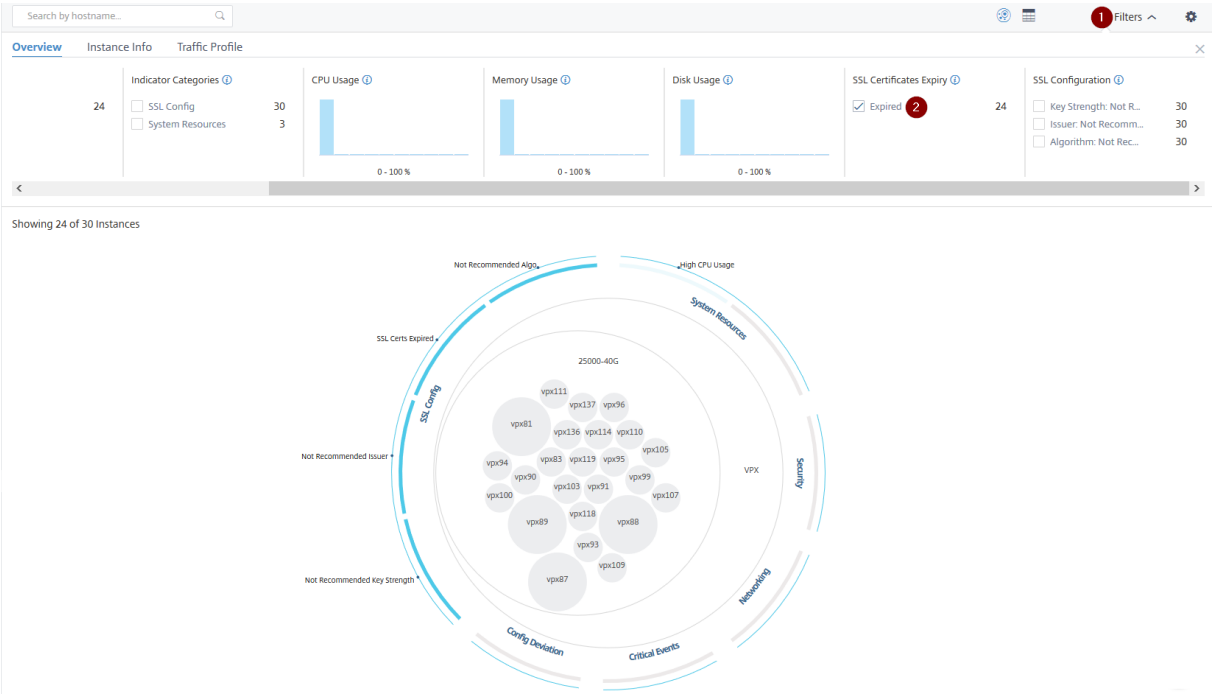
To view instances that have consumed disk space between 0 and 10%, drag the mouse pointer over the two ranges.



> **Note**
>
> Click "X"to remove the selection. You can also click **Reset** to remove multiple selections.

The horizontal bar charts in the **Overview** panel indicate the number of instances that report system errors, critical events, and expiry status of the SSL certificates. Select the check box to view those instances.

Example 4: View instances for expired SSL certificates:



1 - Click the **Filter** list.

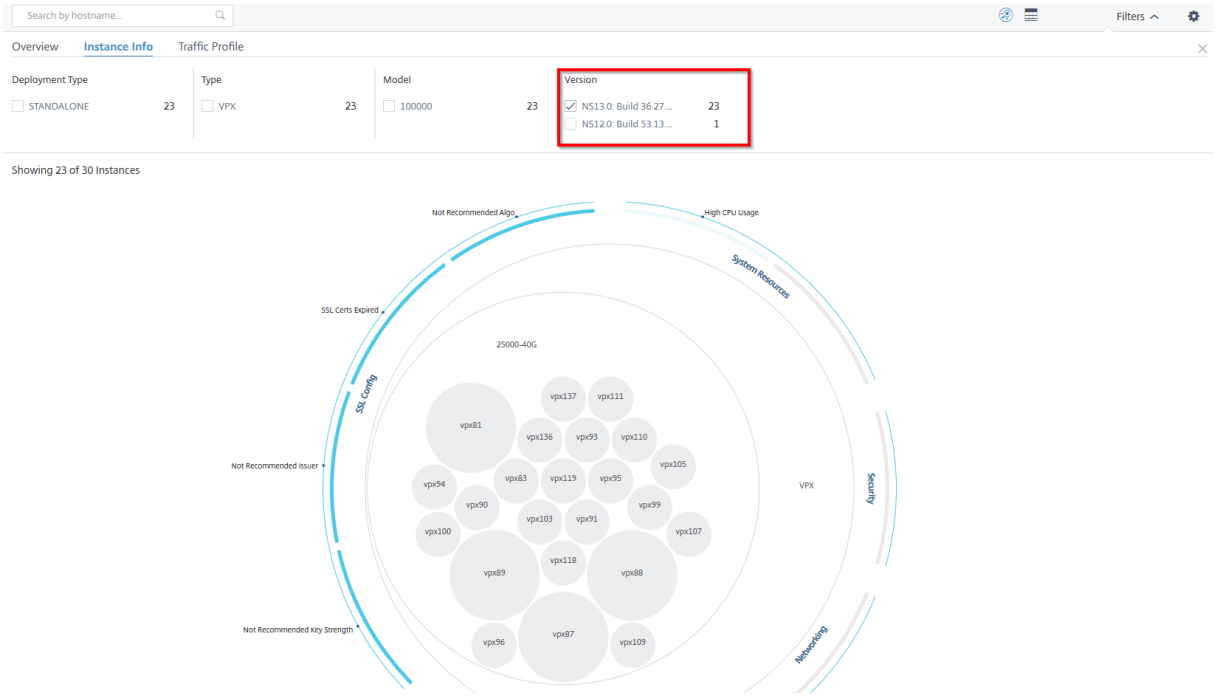
2 - In the **SSL certificates expiry** section, select **Expired** check box to view the instances.

Instance info

The **Instance Info** panel allows you to view instances based on the type of deployment, instance type, model, and software version. You can select multiple check boxes to narrow down your selection.

Example 5: View NetScaler VPX instances with specific build number:

Select the version that you want to view.



Traffic profile

The Histograms in the **Traffic profile** panel represent an aggregated number of instances based on the licensed throughput on the instances, number of requests, connections, and transactions handled by the instances. Select the bar chart to view instances in that range.

Example 6: View instances supporting TCP connections:

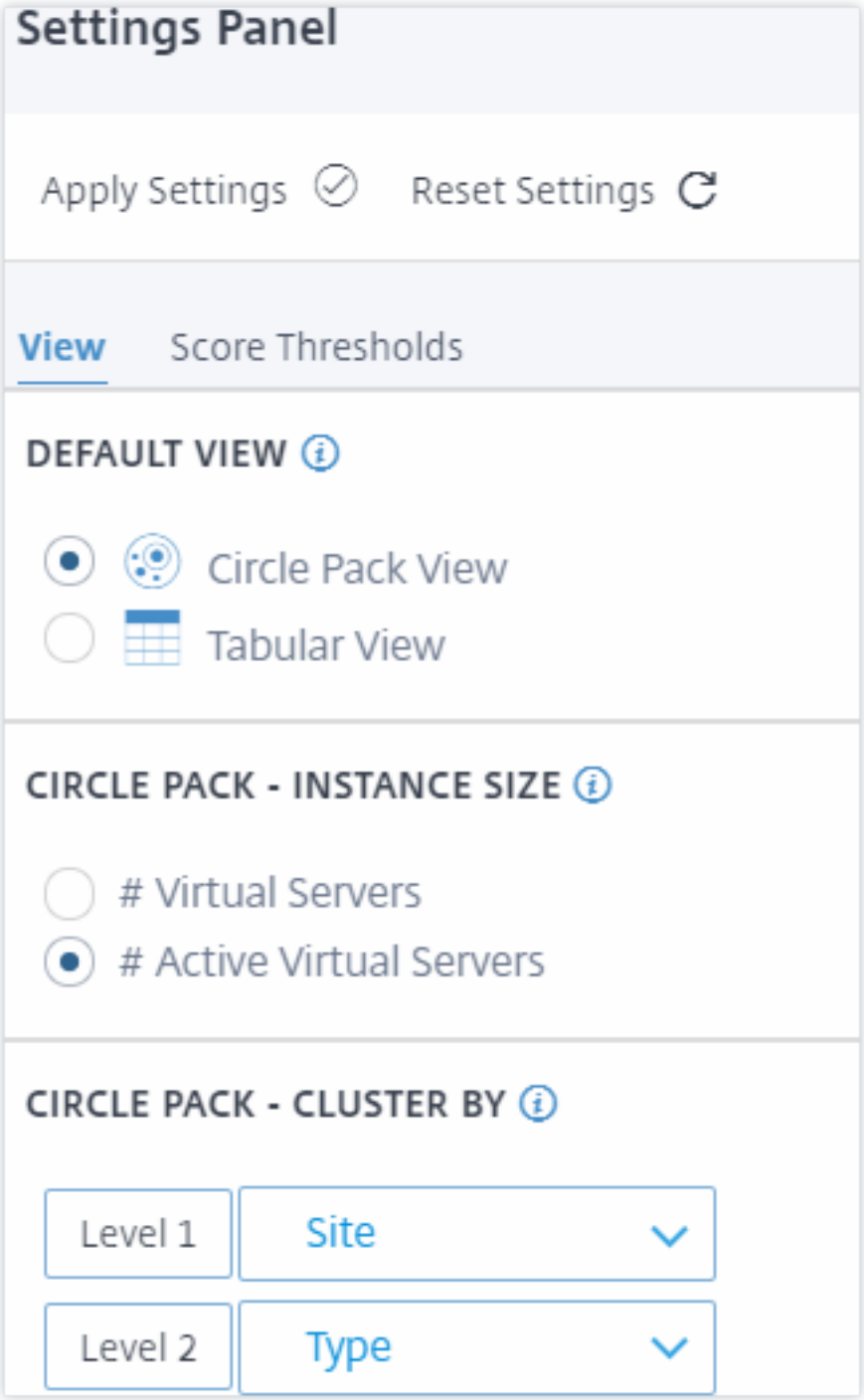
The following image shows the number of instances supporting TCP connections.

How to use the settings panel

The **Settings** panel allows you to set the default view of the Infrastructure Analytics. It also allows you to set the low and high threshold values for high CPU usage, high disk usage, and high memory usage. The settings panel is divided into two tabs - View and Score Thresholds.

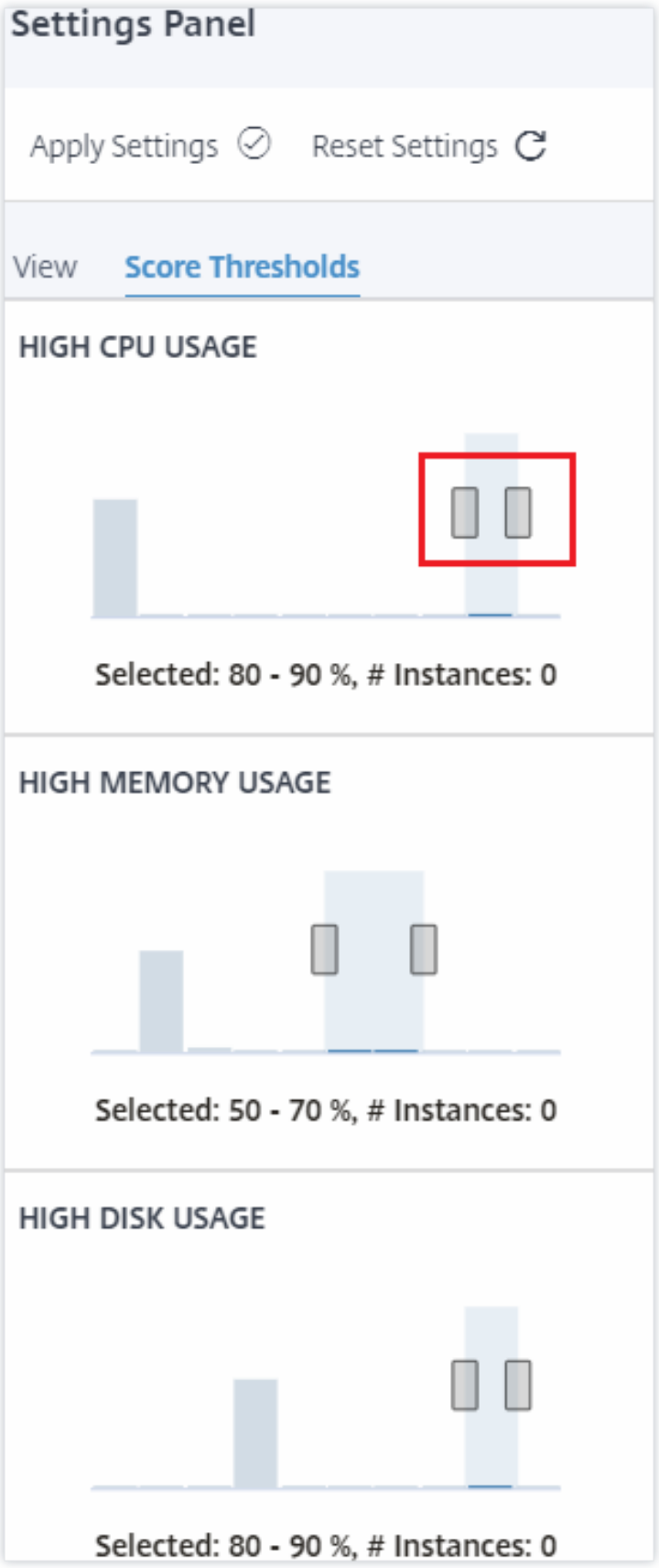
View

- **Default View**. Select **Circle Pack** or Tabular format as the default view on the analytics page. The format you select is what you see whenever you access the page in NetScaler ADM.
- **Circle Pack - Instance Size**. Allow the size of the instance circle to by either the number of virtual servers or the number of active virtual servers.
- **Circle Pack - Cluster By**. Decide the two-level clustering of the instance circles. For more information on instance clustering, see Clustered instance circles.



Score thresholds

You can modify the low and high threshold values for high CPU, memory, and disk usage depending on the traffic requirements in your organization. Drag the handles in each of the selection Histogram to set the values.



> **Note**
>
> Click **Apply Settings** to apply these changes, or click **Reset** to remove all changes.

How to visualize data on the dashboard

Using Infrastructure Analytics, network admins can now identify instances needing the most attention within a few seconds. To understand data visualization in more detail, let us consider the case of Chris, a network admin of ExampleCompany.

Chris maintains many NetScaler instances in the organization. A few of the instances process high traffic, and Chris needs to monitor them closely. Chris notices that a few high-traffic instances are no longer processing the full traffic passing through them. To analyze this reduction, earlier, Chris had to read multiple data reports coming in from various sources. Chris had to spend more time trying to correlate the data manually and ascertain which instances are not in optimal state and need attention.

Chris uses the Infrastructure Analytics feature to see the health of all instances visually.

The following two examples illustrate how Infrastructure Analytics assists Chris in maintenance activity:

Example 1 - To monitor the SSL traffic:

Chris notices on the Circle Pack that one instance has a low instance score and that instance is in "Critical"state. Chris clicks that instance to see what the issue is. The instance summary displays that there is an SSL card failure on that instance and the instance is unable to process SSL traffic (the SSL traffic has reduced). Chris extracts that information and sends a report to the team to look into the issue immediately.

Example 2 - To monitor configuration changes:

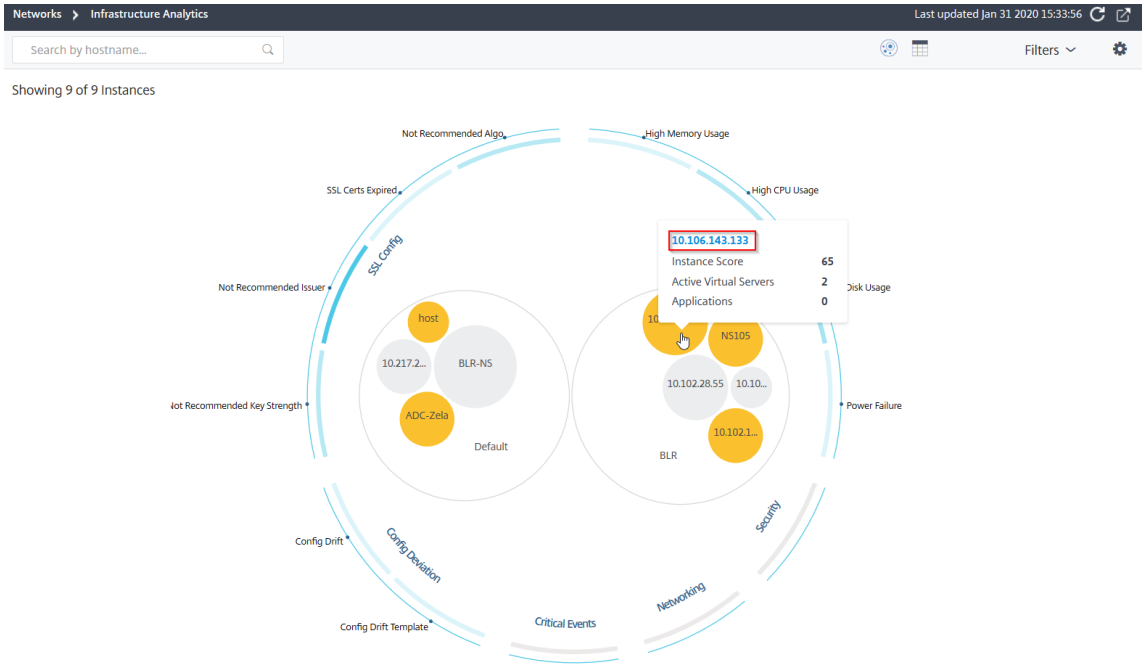
Chris also notices that another instance is in "Review"state and that there has been a config deviation recently. When Chris clicks the config deviation risk indicator, Chris notices that RC4 Cipher, SSL v3, TLS 1.0, and TLS 1.1 related configuration changes have been made which might be due to security concerns. Chris also notices that the SSL transaction traffic profile for this instance has gone down. Chris exports this report and sends it to the admin to inquire further.

View instance details in Infrastructure Analytics

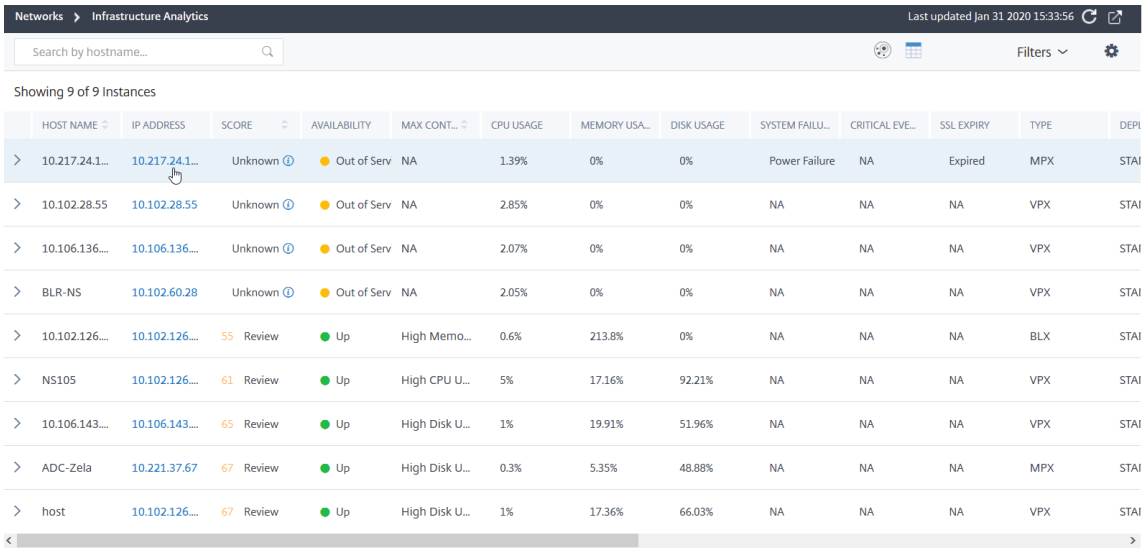
February 6, 2024

1. Navigate to **Infrastructure > Infrastructure Analytics**

2. Click the circle pack view and select the IP address.



You can also click an IP address from the table view.

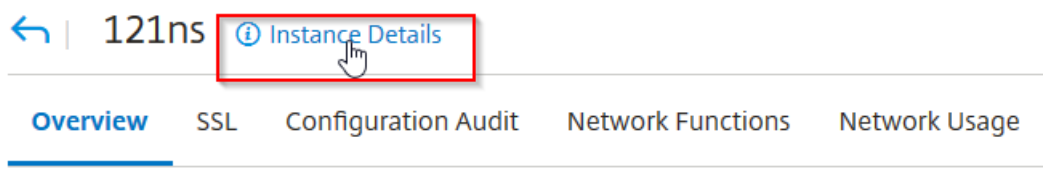


- **Host name** –Denotes the host name assigned to the ADC instance
- **IP address** –Denotes the IP address of the ADC instance
- **Score** –Denotes the ADC instance score and the status such as Critical, Good, and Fair
- **Availability** –Denotes the status of the ADC instance such as **Up**, **Down**, or **Out of service**.
- **Max Contribution** –Denotes the issue category that the ADC instance has the maximum error counts.

- **CPU usage** –Denotes the current CPU % used by the instance
- **Memory usage** –Denotes the current memory % used by the instance
- **Disk usage** –Denotes the current disk % used by the instance
- **System Failure** –Denotes the total number of errors for the instance system
- **Critical Events** –Denotes the event category that the NetScaler instance has the maximum events
- **SSL expiry** –Denotes the status of the SSL certificate installed on the ADC instance
- **Type** –Denotes the ADC instance type such as VPX, SDX, MPX, or CPX
- **Deployment** –Denotes if the ADC instance is deployed as a standalone instance or HA pair
- **Model** –Denotes the ADC instance model number
- **Version** –Denotes the ADC instance version and build number
- **Throughput** –Denotes the current network throughput from the ADC instance
- **HTTPS request/sec** –Denotes the current HTTPS requests/sec received by the ADC instance
- **TCP connection** –Denotes the current TCP connections established
- **SSL transaction** –Denotes the current SSL transactions processed by the ADC instance
- **Site** –Denotes the name of the site that the ADC instance is deployed.

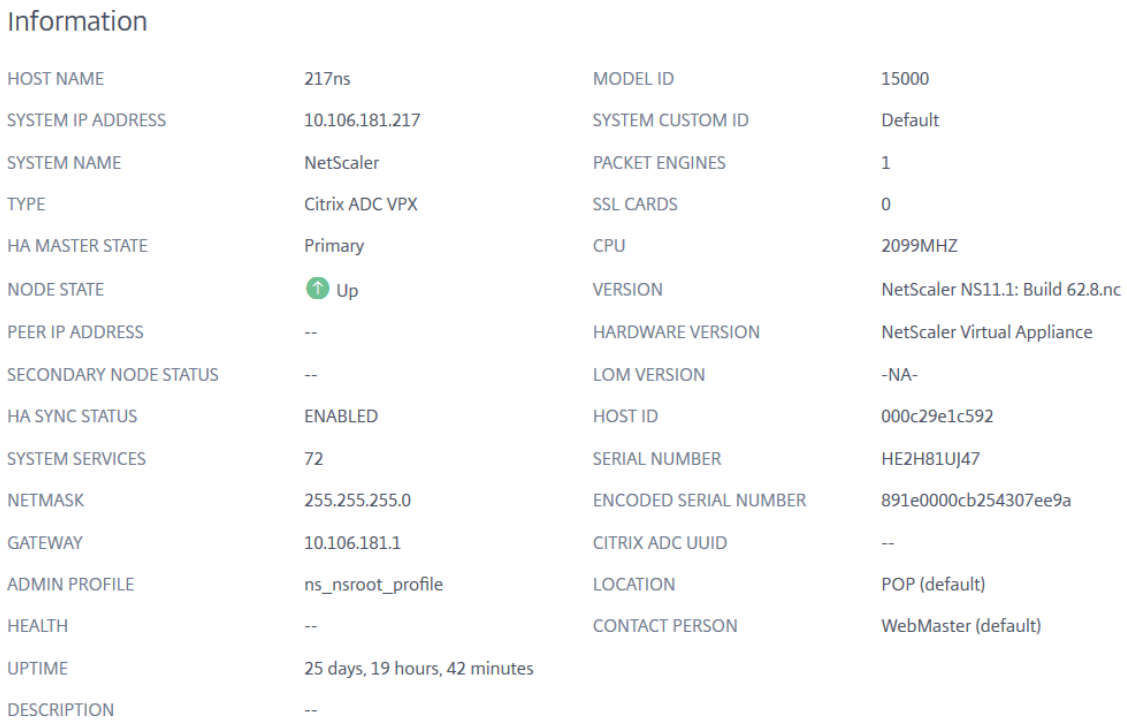
> **Note**
>
> For every 5 minutes, the current values for CPU usage, memory usage, disk usage, throughput, and so on are updated.

Click **Instance Details** to view the details.

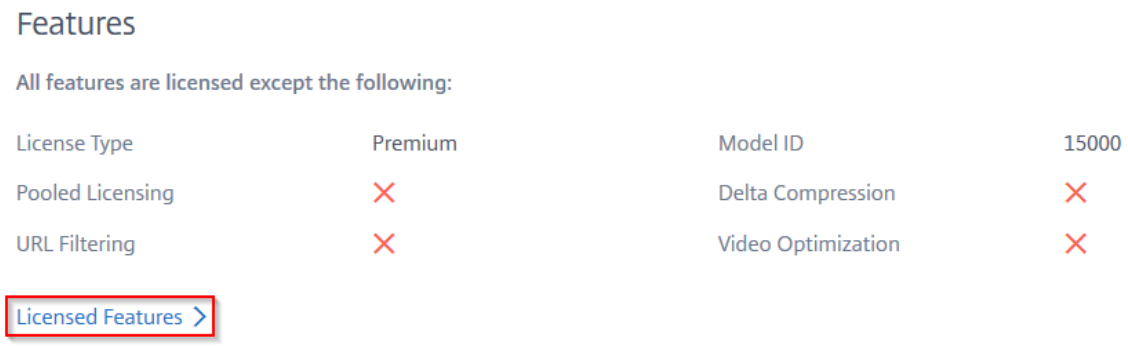


The following details are displayed:

- **Information** - Instance details such as instance type, deployment type, version, model.



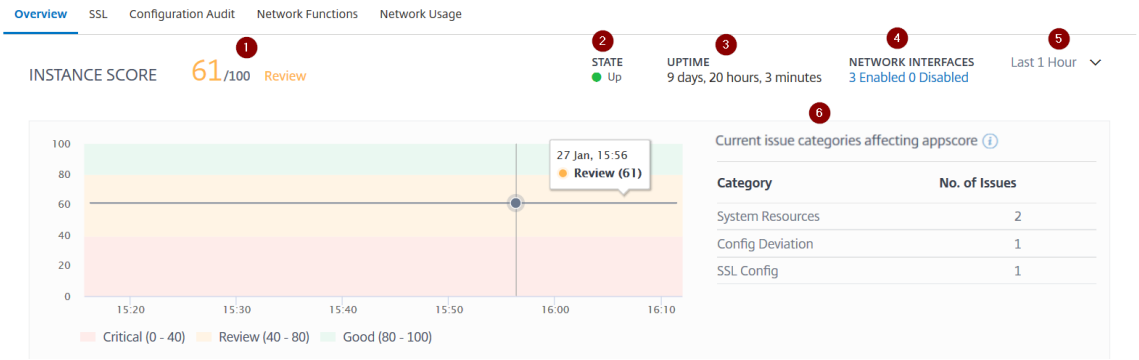
- **Features** –By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



- **Modes** –By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**



1 –Indicates the current NetScaler instance score for the selected time duration. The final score is calculated as **100 minus total penalties**. The graph displays the score ranges for the selected time duration.

2 –Indicates the status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 –Indicates the duration that the NetScaler instance is up and running.

4 –Indicates the total network interfaces enabled and disabled for the instance. Click to view the details such as network interface name and the status (enabled or disabled).

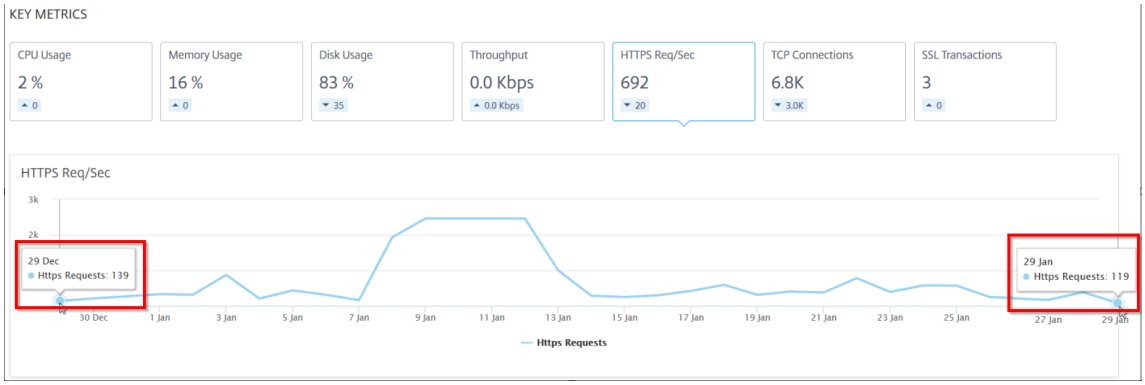
5 –Select the time duration from the list to view the instance details.

6 –Displays the total issues and issue category of the ADC instance.

- **Key Metrics**

Click each tab to view the details. In each metric, you can view the average value and the difference value for the selected time.

The following image is an example for HTTPS Req/Sec and the selected time duration is 1 hour. The value **692** is the average HTTPS Req/Sec for the 1-month duration and the value **20** is the difference value. In the graph, the first value is **139** and the last value is **119**. The difference value is **139 –119 = 20**.



You can view the following instance metrics in a graph format for the selected time duration:

- **CPU Usage** –The average CPU % from the instance for the selected duration (displays for both packet CPU and for management CPU).
- **Memory Usage** –The average memory usage % from the instance for the selected duration.
- **Disk Usage** –The average disk space % from the instance for the selected duration.
- **Throughput** –The average network throughput processed by the instance for the selected duration.
- **HTTPS request/sec** –The average HTTPs requests received by the instance for the selected duration.
- **TCP connections** –The average TCP connections established by the client and server for the selected duration.
- **SSL transactions** –The average SSL transactions processed by the instance for the selected duration.

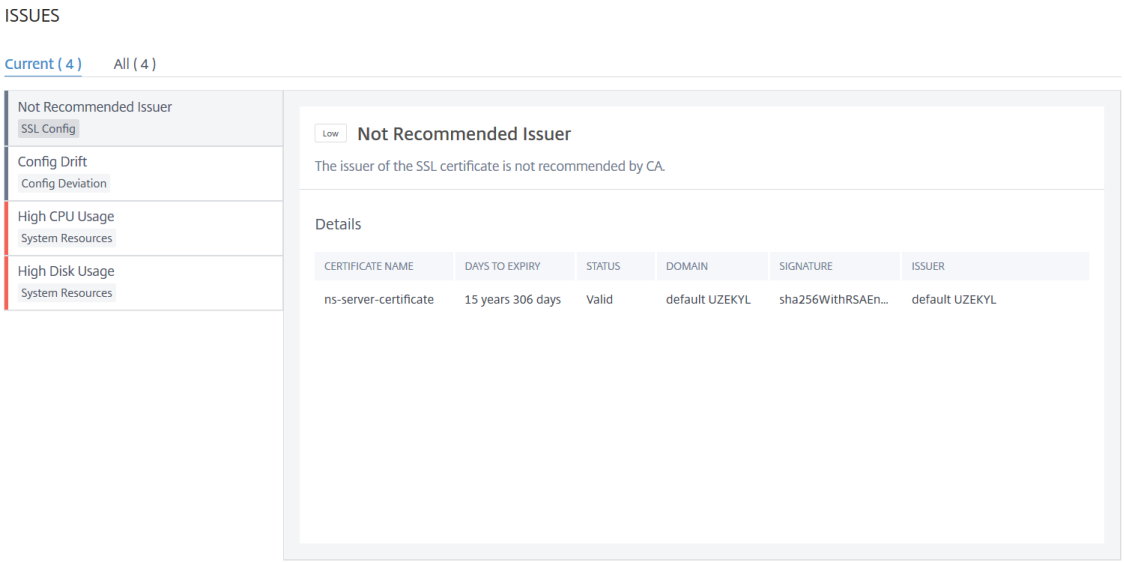
- **Issues**

You can view the following issues that occur in NetScaler instance:

Issue Category	Description	Issues
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage.	– High CPU Usage – High Memory Usage – High Disk Usage – SSL Card Failures – Power Failure – Disk Error – Flash Error – NIC Discards
SSL Config	Displays all issues related to the SSL configuration on the NetScaler instance.	– SSL Certs Expired – Not Recommended Issuer – Not Recommended Algorithm – Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in NetScaler instance.	– Config Drift – Running vs Template
Critical events	Displays all critical events related to NetScaler instances configured in HA pair and in Cluster.	– Cluster Prop Failure – Cluster Sync Failure – Cluster versions Mismatch – HA Bad Secondary State – HA No Heat Beats – HA Sync Failure

Issue Category	Description	Issues
Networking	Displays the operational issues that occur in the instances.	– HA Version Mismatch For more information, see Enhanced Infrastructure Analytics with new indicators.

Click each tab to analyze and troubleshoot the issue. For example, consider that an instance has the following errors for the selected time duration:



- The **Current** tab displays the issues that are currently affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

View the capacity issues in an ADC instance

February 6, 2024

When an ADC instance has consumed most its available capacity, packet-drop may occur while processing the client traffic. This issue causes low performance in an ADC instance. By understanding such ADC capacity issues, you can proactively allocate additional licenses to steady the ADC performance.

In the **Circle Pack View**, you can view the ADC instance capacity issues if exists.

To view ADC capacity issues,

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Select the circle pack view.

> **Note**
>
> In **Infrastructure Analytics**, the circle-pack and tabular views display the events and issues that occurred in the last one hour.

The following illustration suggests the capacity issues exist in the selected instance:

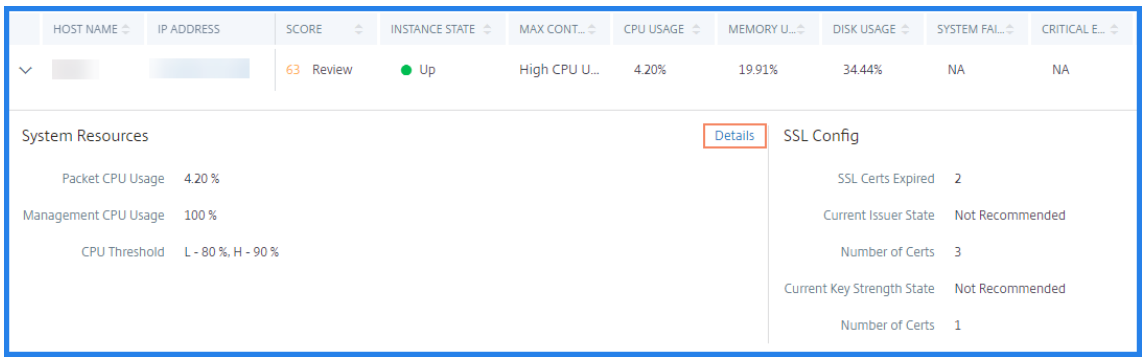
The issues are categorized on the following capacity parameters:

- **Throughput Limit Reached** –The number of packets dropped in the instance after the throughput limit is reached.
- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** –The number of packets dropped in the instance after the PPS limit is reached.
- **SSL Throughput Rate Limit** –The number of times the SSL throughput limit reached.
- **SSL TPS Rate Limit** –The number of times the SSL TPS limit reached.

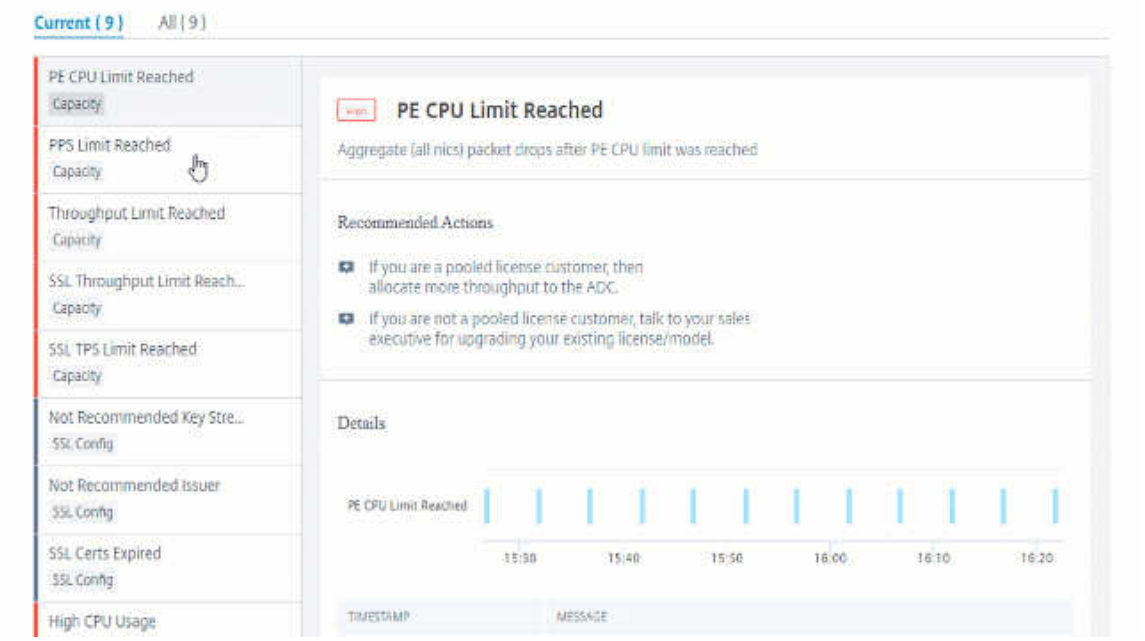
View recommended actions to solve capacity issues

The ADM recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

1. In **Infrastructure > Infrastructure Analytics**, select the tabular view.
2. Select the instance that has capacity issues and click **Details**.



3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.



The ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists.

The ADM calculates the instance score on the defined capacity threshold.

- **Low threshold** –1 packet drop or rate-limit counter increment
- **High threshold** –10000 packets drop or rate-limit counter increment

Therefore, when an ADC instance breaches the capacity threshold, the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the `ADCCapacityBreach` category. To view these events, navigate to **Accounts > System Events**.

Enhanced Infrastructure Analytics with new indicators

March 11, 2024

Using the NetScaler ADM Infrastructure Analytics, you can:

- View a new set of operational issues that occur in NetScaler instances.
- View error messages and check recommendations to troubleshoot the issues.

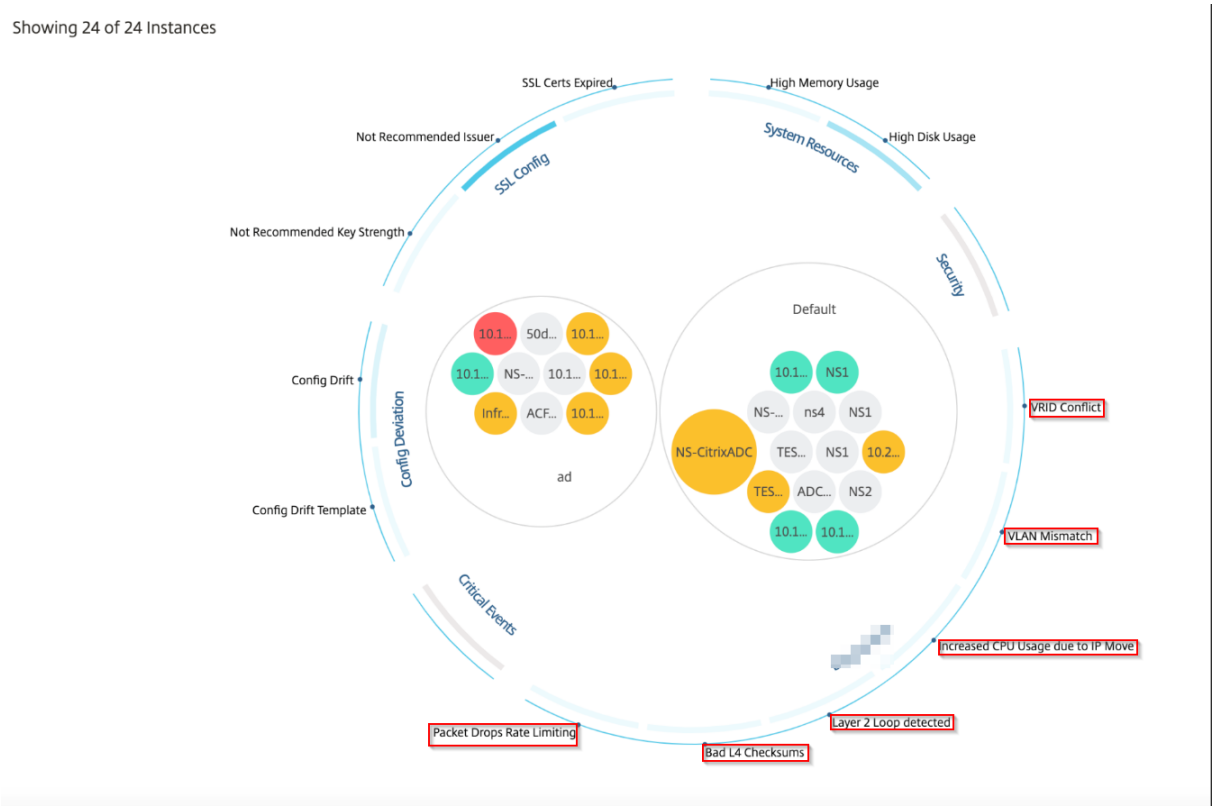
As an administrator, you can quickly identify the root cause analysis of issues.

> **Note**
>
> Rule indicators are not supported for:
>
> - NetScaler instances configured in a cluster mode.
> - NetScaler instances configured with admin partitions.

In NetScaler ADM, navigate to **Infrastructure > Infrastructure Analytics** to view indicators for:

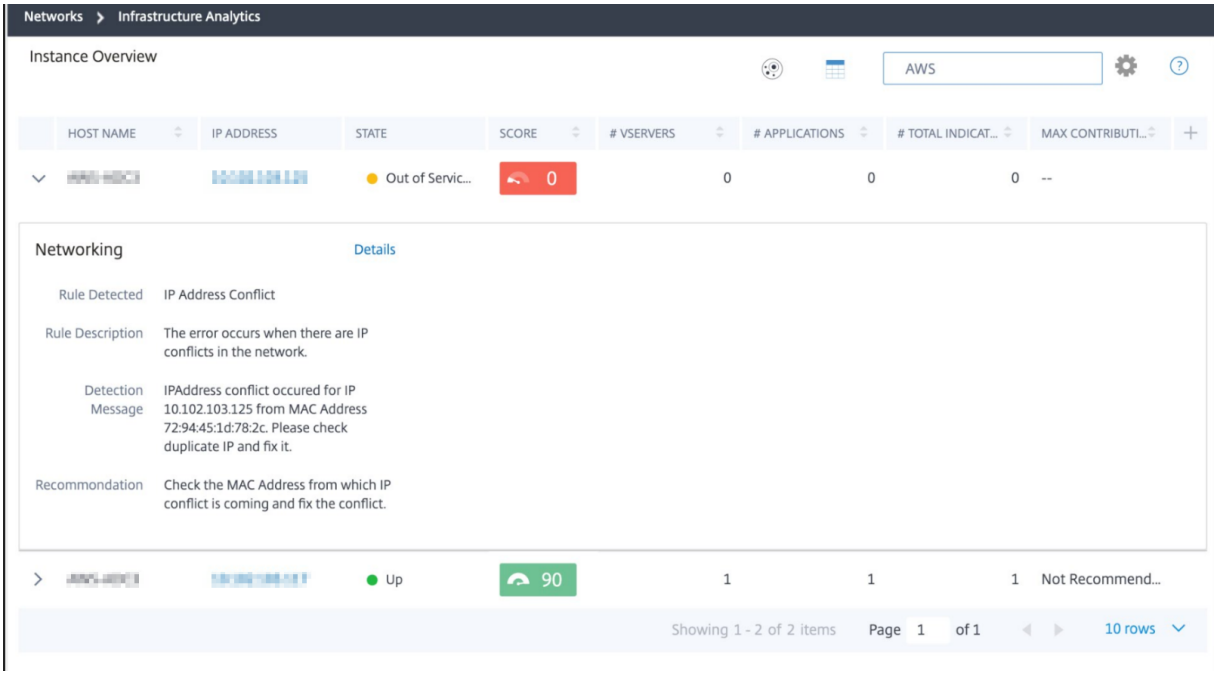
Indicator name in Infrastructure Analytics	Description
Port allocation failure	Detects when NetScaler uses SNIP to communicate with a new server connection and total ports available on that SNIP are exhausted. The recommended action is to add another SNIP in the same subnet.
No default route configuration	Detects when the traffic gets dropped because of non-availability of routes.
IP conflict	Detects if a same IP address is configured or applied on two or more instances in a network.
VRID conflict	Detects when intermittent access problems occur for the specified VRID.
VLAN mismatch	Detects if any errors occur during VLAN configuration bound to IP subnets.

Indicator name in Infrastructure Analytics	Description
TCP small window attack	Detects when there is a possible small window attack in progress. This alert is just for informational, because ADC already mitigates this attack.
Rate control threshold	Detects when packets are dropped based on the configured rate control threshold.
Persistence Limit	Detects when maximum hits are imposed on the NetScaler memory.
GSLB site name mismatch	Detects when GSLB configuration synchronization failures occur because of site name mismatch.
Malformed IP header	Detects when sanity checks on IPv4 packets are failed.
Bad L4 checksums	Detects when checksum validation for TCP packets is failed.
Increased CPU usage due to IP move	Detects if a large number of macs need to be updated.
Excessive packet steering	Detects high levels of software packet steering due to the usage of asymmetric rss key type.
Layer 2 loop	Detects the presence of layer 2 loops in the network.
Tagged VLAN mismatch	Detects when tagged VLAN packets are received on an untagged interface.



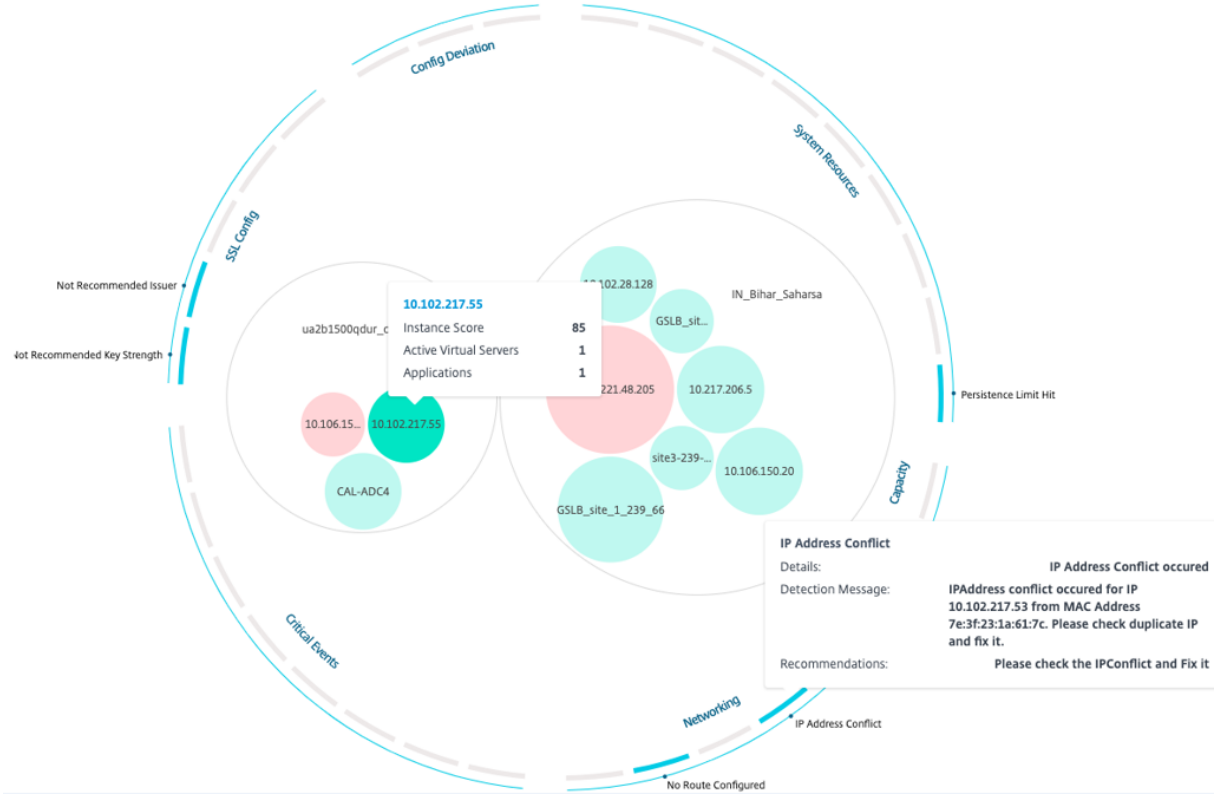
Tabular view

You can also view anomalies using the tabular view option in **Infrastructure Analytics**. Navigate to **Infrastructure > Infrastructure Analytics** and then click to display all managed instances. Click › to expand for details.



View details of an anomaly

For example, if you want to view details for **IP address conflict** in the network, click the anomaly that is displayed for IP address conflict to view the details.



- **Details** - Indicates what anomaly is detected
- **Detection Message** - Indicates the MAC address for which the IP address has the conflict
- **Recommendations** - Indicates the action item to resolve this IP address conflict

Instance management

March 11, 2024

Instances are Citrix Application Delivery Controller (ADC) appliances that you can manage, monitor, and troubleshoot using NetScaler Application Delivery Management (ADM). You must add instances to NetScaler ADM to monitor them. Instances can be added when you set up NetScaler ADM or later. After you add instances to NetScaler ADM, they are continuously polled to collect information that can later be used to resolve issues or as reporting data.

Instances can be grouped as a static group or as a private IP-block. A static group of instances can be useful when you want to run specific tasks such as configuration jobs, and so on. A private IP-block groups your instances based on their geographical locations.

Add an instance

You can add instances either while setting up the NetScaler ADM server for the first time or later. To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

To learn how to add an instance to NetScaler ADM, see Add Instances to NetScaler ADM.

When you add an instance to the NetScaler ADM server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance. To learn more, see How NetScaler ADM discovers instances.

After you've added an instance, you can delete it by navigating to **Infrastructure > Instances** and click **All Instances**. On the Instances page, select the instance you want to delete and click **Remove**.

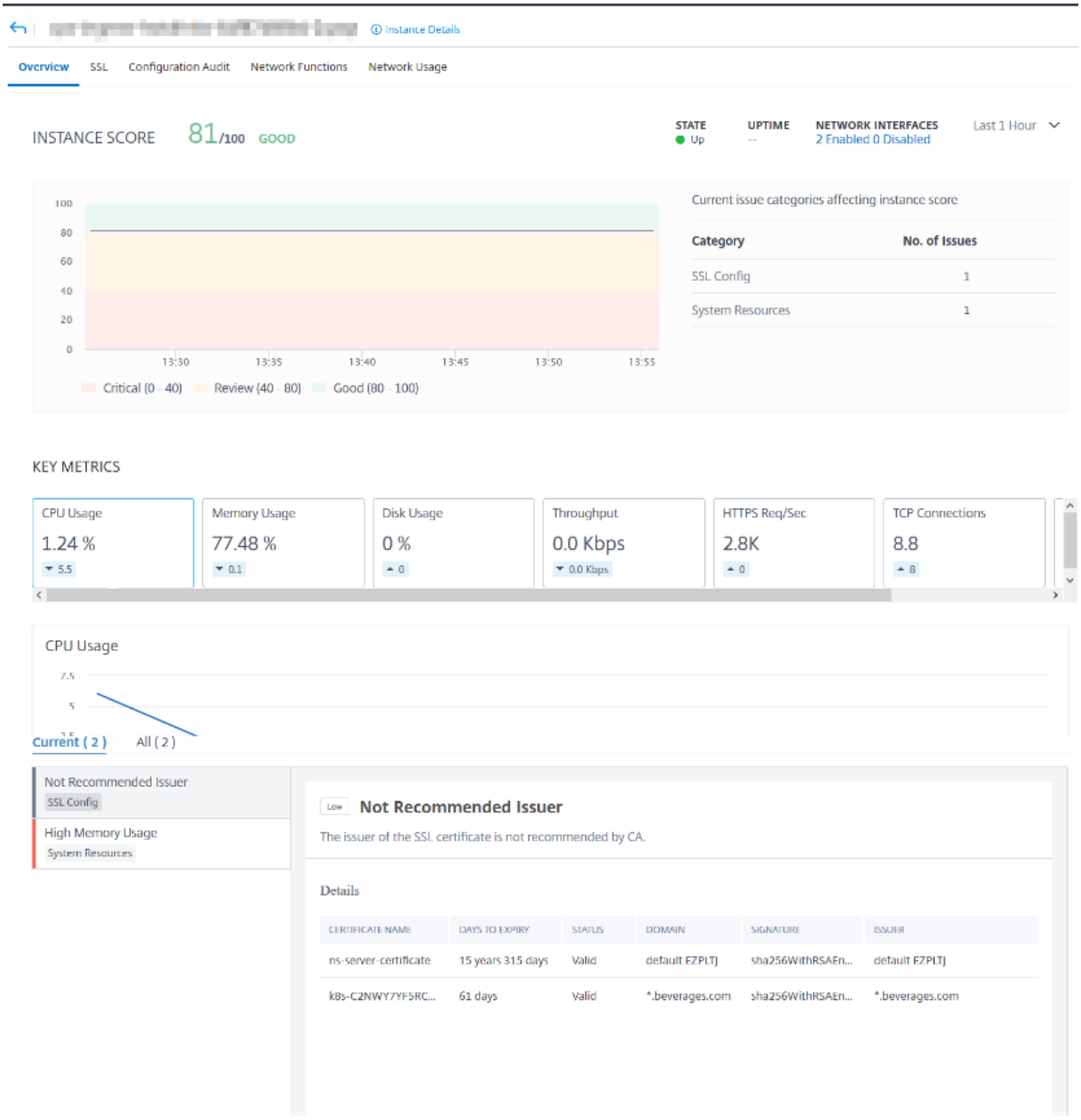
How to use the instance dashboard

The per-instance dashboard in NetScaler ADM displays data in a tabular and graphical format for the selected instance. Data collected from your instance during the polling process is displayed on the dashboard.

By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.

To view a specific instance's dashboard, navigate to **Infrastructure > Instances**. From the summary, choose the instance type and then, select the instance you want to view and click **Dashboard**.

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:



- **Overview**. The overview tab displays the CPU and memory usage of the chosen instance. You

can also view events generated by the instance and the throughput data. Instance-specific information such as the IP address, its hardware and LOM versions, the profile details, serial number, contact person, and so on is also displayed here. By scrolling down further, the licensed features that are available on your chosen instance along with the modes configured on it.

For more information, see Instance details.

- **SSL dashboard**. You can use the SSL tab on the per-instance dashboard to view or monitor the details of your chosen instance's SSL certificates, SSL virtual servers, and SSL protocols. You can click the "numbers"in the graphs to display further details.
- **Configuration Audit**. You can use the configuration audit tab to view all the configuration changes that have occurred on your chosen instance. The **NetScaler config saved status** and **NetScaler config drift** charts on the dashboard display high-level details about configuration changes in saved against unsaved configurations.
- **Network Functions**. Using the network functions dashboard, you can monitor the state of the entities configured on your selected NetScaler instance. You can view graphs for your virtual servers that display data such as client connections, throughput, and server connections.
- **Network usage**. You can view network performance data for your selected instance on the network usage tab. You can display reports for an hour, a day, a week, or for a month. The timeline slider function can be used to customize the duration of the network reports being generated. By default, only eight reports are displayed, but you can click the "plus"icon at the bottom right-corner of the screen to add additional performance report.

Monitor globally distributed sites

March 11, 2024

As a network administrator, you might have to monitor and manage network instances deployed across geographical locations. However, it is not easy to gauge the requirements of the network when managing network instances in geographically distributed data centers.

Geomaps in NetScaler Application Delivery Management (ADM) provides you with a graphical representation of your sites and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

The following section explains how you can monitor data centers in NetScaler ADM.

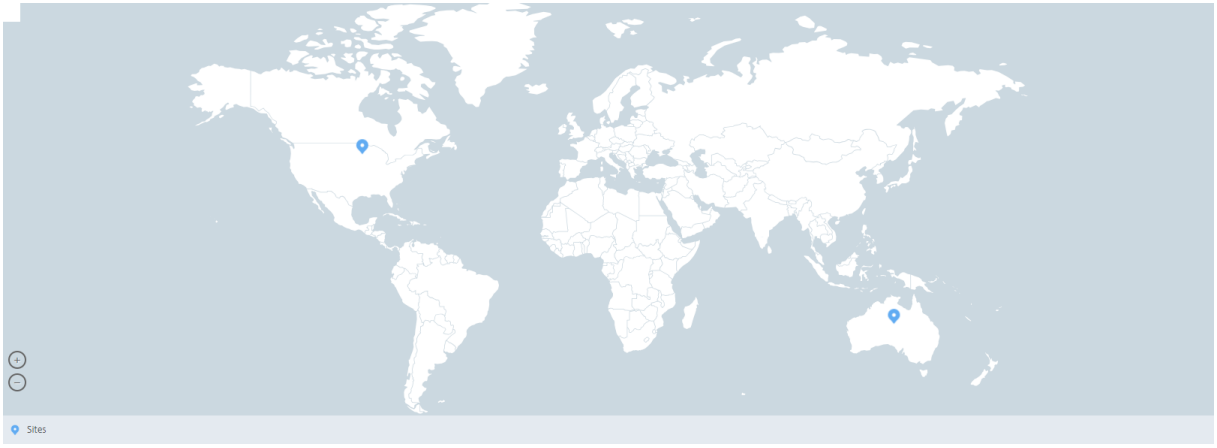
NetScaler ADM site is a logical grouping of Citrix Application Delivery Controller (ADC) instances in a specific geographical location. For example, while one site is assigned to Amazon Web Services

(AWS) and another site might be assigned to Azure™. Still another site is hosted on the premises of the tenant. NetScaler ADM manages and monitors all NetScaler instances connected to all sites. You can use NetScaler ADM to monitor and collect syslog, AppFlow, SNMP, and any such data originating from the managed instances.

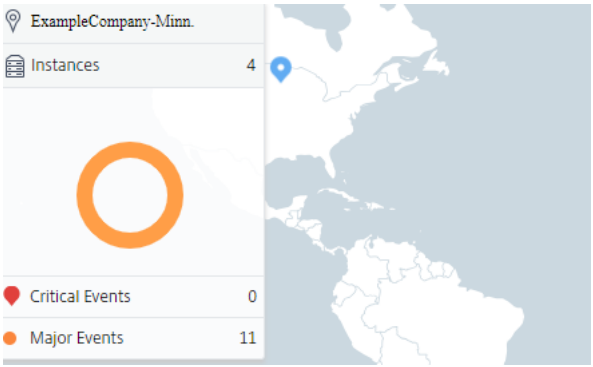
Geomaps in NetScaler ADM provides you with a graphical representation of your sites. Geomaps also breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor all network issues. You can navigate to **Infrastructure > Instances** page for a visual representation of the sites created on the world map.

Use case

A leading mobile carrier company, ExampleCompany, was relying on private service providers for hosting their resources and applications. The company already had two sites - one at Minneapolis in the United States and another in Alice Springs in Australia. In this image, you can see that two markers represent the two existing sites.



The markers also display a number, which shows the number of applications in each site. You can click these markers for more information about each site.

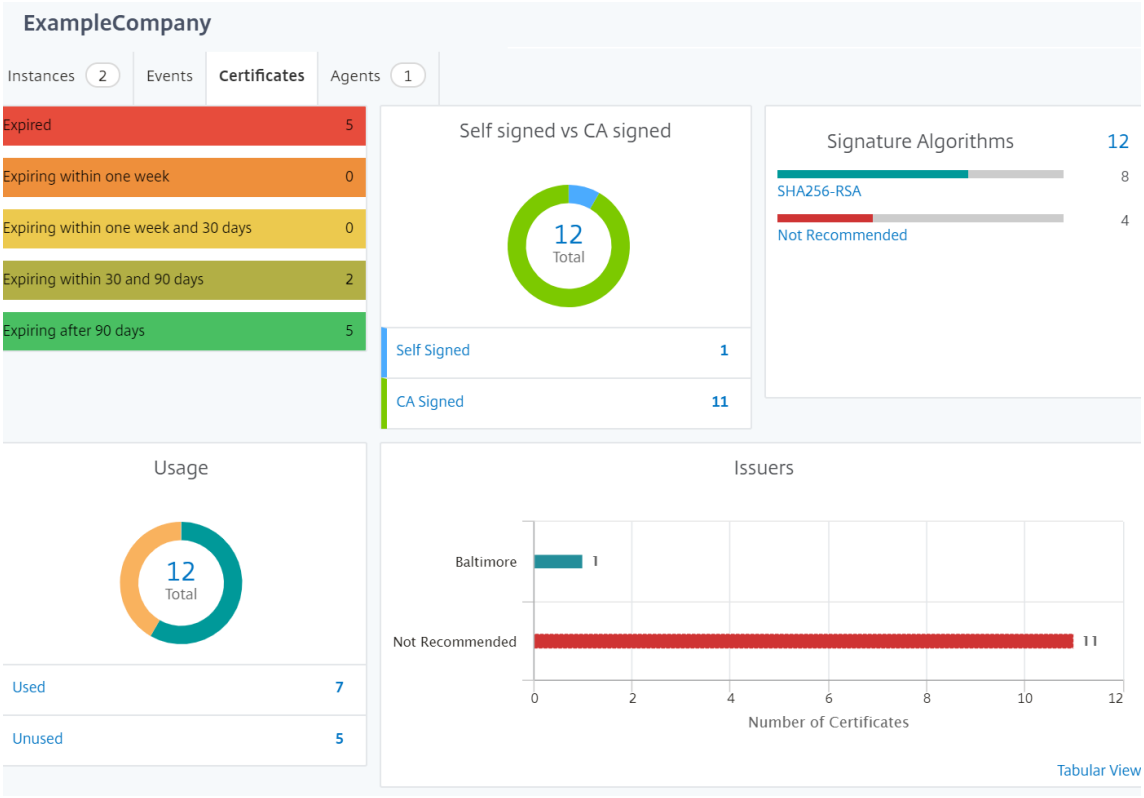


Click the tabs to view more information:

- **Instances** tab: View the following in this tab:

  - IP address of each network instance
  - Type of the instance
  - Number of critical events on them
  - Significant events and all events raised on a NetScaler instance.

- **Events** tab: View a list of critical and significant events raised on the instances.
- **Certificates** tab: View the following in this tab:
  - List of certificates of all the instances
  - Expiration status
  - Vital information and the top 10 instances by many certificates in use.
- **Agents** tab: View a list of agents to which the instances are bound.



Configuring Geomaps

ExampleCompany decided to create a third site in Bangalore, India. The company wanted to test the cloud by offloading some of their less-critical, internal IT applications to the Bangalore office. The company decided to use the AWS cloud computing services.

As an administrator, you must first create a site, and next add the NetScaler instances in NetScaler ADM. You must also add the instance to the site, add an agent, and bind the agent to the site. NetScaler ADM then recognizes the site that the NetScaler instance and the agent belong.

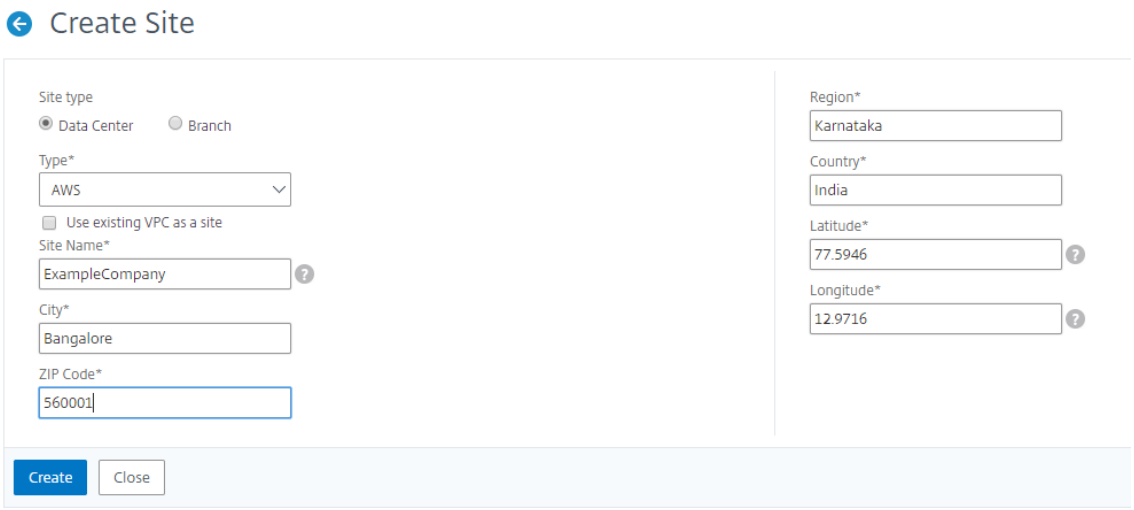
For more information on adding NetScaler instances, see Adding Instances.

To create sites:

Create sites before you add instances in NetScaler ADM. Providing location information allows you to locate the site precisely.

Navigate to **Infrastucture > Instances > Sites**, and then click **Add**.

1. In the **Create Site** page, specify the following information:
    a) **Site Type**: Select **Data Center**.
    > **Note**
    >
    > The site can function as the primary data center or as a branch. Choose accordingly.
    b) **Type**: Select AWS as the cloud provider from the list.
    > **Note**
    >
    > Check the **Use existing VPC as a site** box accordingly.
    c) **Site Name**: Type the name of the site.
    d) **City**: Type the city.
    e) **Zip Code**: Type the Zip Code.
    f) **Region**: Type the Region.
    g) **Country**: Type the Country
    h) **Latitude**: Type the latitude of the location.
    i) **Longitude**: Type the longitude of the location.
2. Click **Create**.

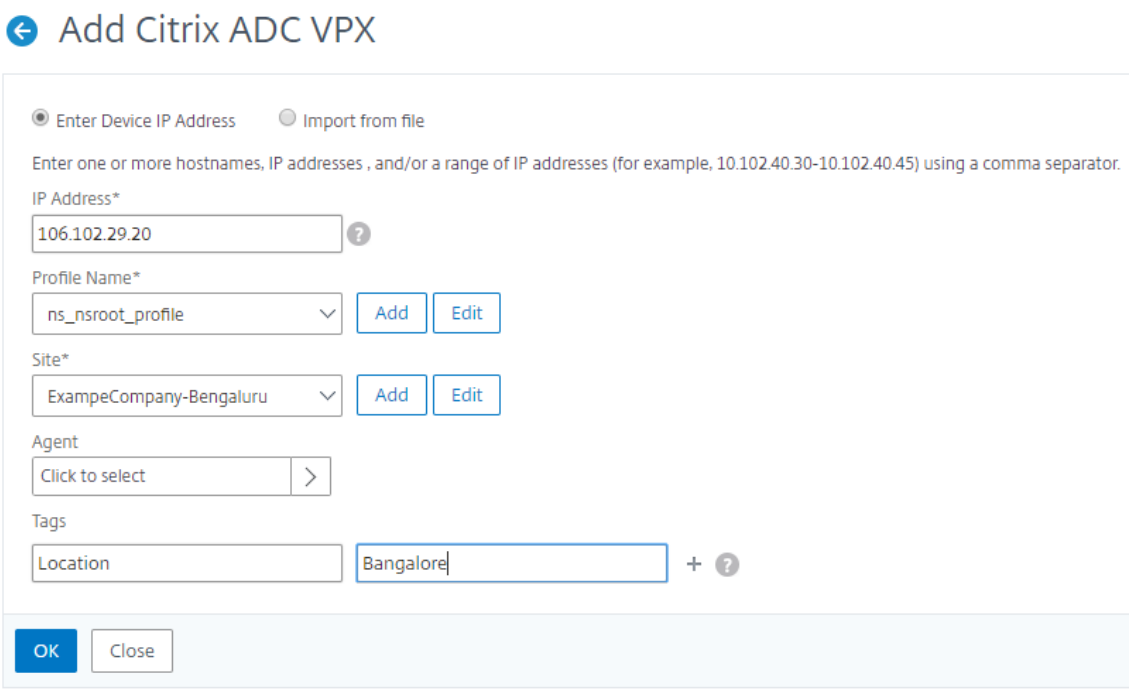


To add instances and select sites:

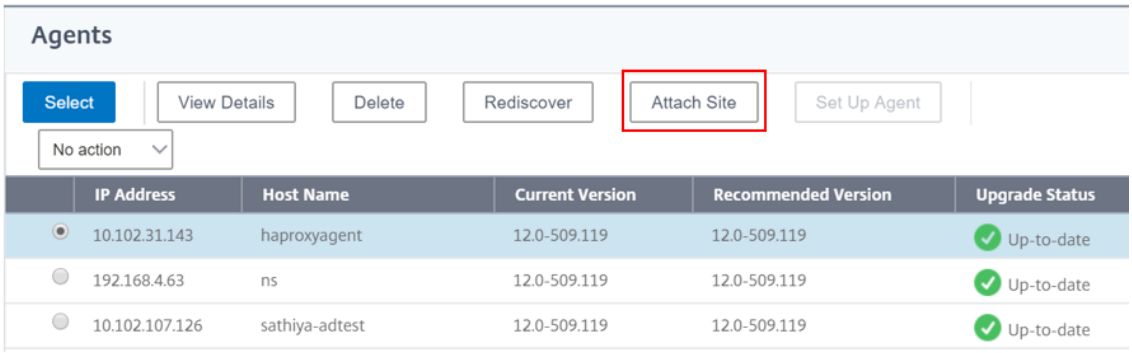
After creating sites, you must add instances in NetScaler ADM. You can select the previously created site, or you can also create a site and associate the instance.

After creating sites, you must add instances in NetScaler ADM. You can select the previously created site, or you can also create a site and associate the instance.

1. In NetScaler ADM, navigate to **Infrastructure > Instances**.
2. Select the type of instance you want to create, and click **Add**.
3. On the **Add NetScaler VPX** page, type the IP address and select the profile from the list.
4. Select the site from the list. You can click the + sign next to **Site** field to create a site or click the edit icon to change the details of the default site.
5. Click the right arrow and select the agent from the list that displays.



6. After choosing the agent, you must associate the agent with the site. This step allows the agent to be bound to the site. Select the agent and click **Attach Site**.

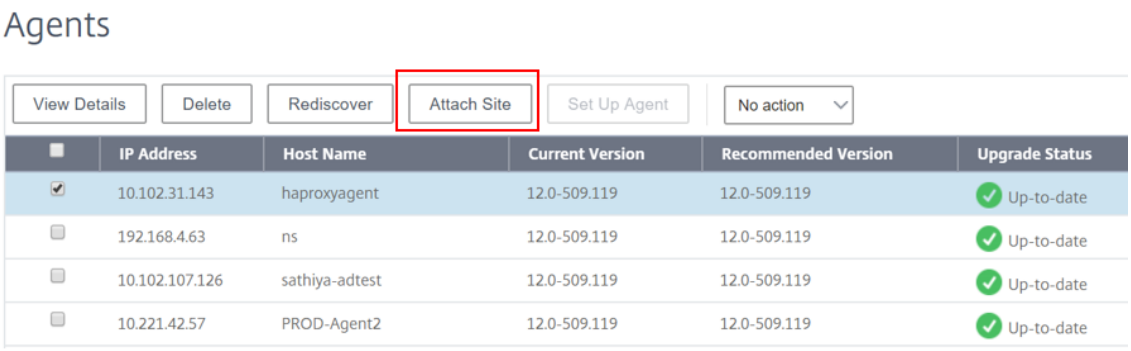


1. Select the site from the list and click **Save**.
1. Click **OK**.

You can also attach an agent to a site by navigating to **Infrastructure > Instances > Agents**.

To associate a NetScaler agent with the site:

1. In NetScaler ADM, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent, and click **Attach Site**.



1. You can associate the site and click **Save**.

NetScaler ADM starts monitoring the NetScaler instances added in Bangalore site along with the instances at the other two sites as well.

How to create tags and assign to instances

March 11, 2024

NetScaler Application Delivery Management (ADM) now allows you to associate your Citrix Application Delivery Controller (ADC) instances with tags. A tag is a keyword or a one-word term that you can assign to an instance. The tags add some additional information about the instance. The tags can be thought of as metadata that helps describe an instance. Tags allow you to classify and search for instances based on these specific keywords. You can also assign multiple tags to a single instance.

The following use cases help you to understand how tagging of instances helps you to better monitor them.

- **Use case 1**: You can create a tag to identify all instances in the United Kingdom. Here, you can create a tag with the key as "Country"and the value as "UK."This tag helps you to search and monitor all those instances in the UK.
- **Use case 2**: You want to search for instances that are in the staging environment. Here, you can create a tag with the key as "Purpose"and the value as "Staging_NS."This tag helps you to segregate all instances that are being used in the staging environment from the instances that have client requests running through them.
- **Use case 3**: Consider a situation where you want to find out the list of NetScaler instances that are in "Swindon"area in the UK and owned by you, David T. You can create tags for all these requirements and assign that to all the instances that satisfy these conditions.

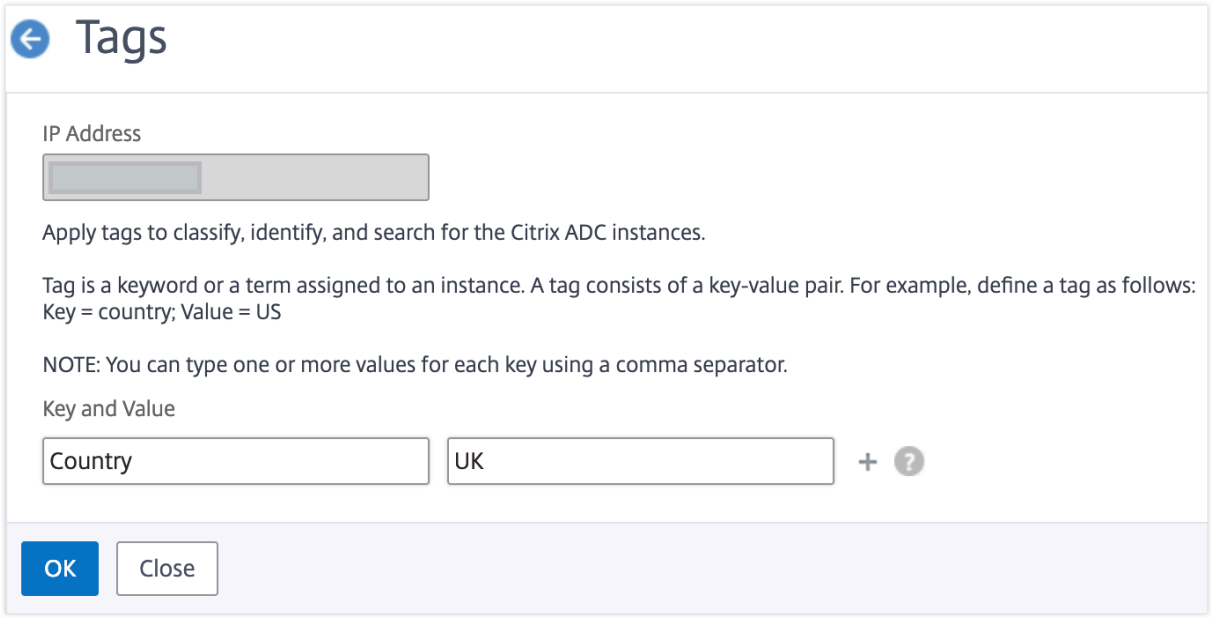
To assign tags to NetScaler VPX instance:

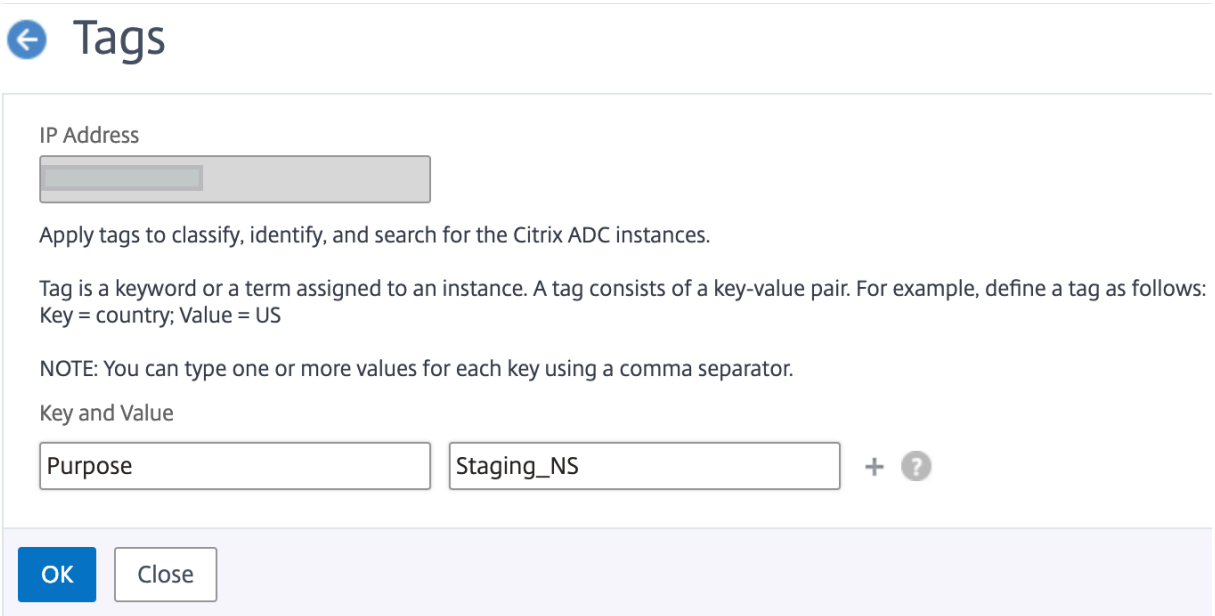
1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler**.

2. Select the **NetScaler VPX** tab.
3. Select the required NetScaler VPX.
4. Click **Tags**.
5. Create tags and click **OK**.

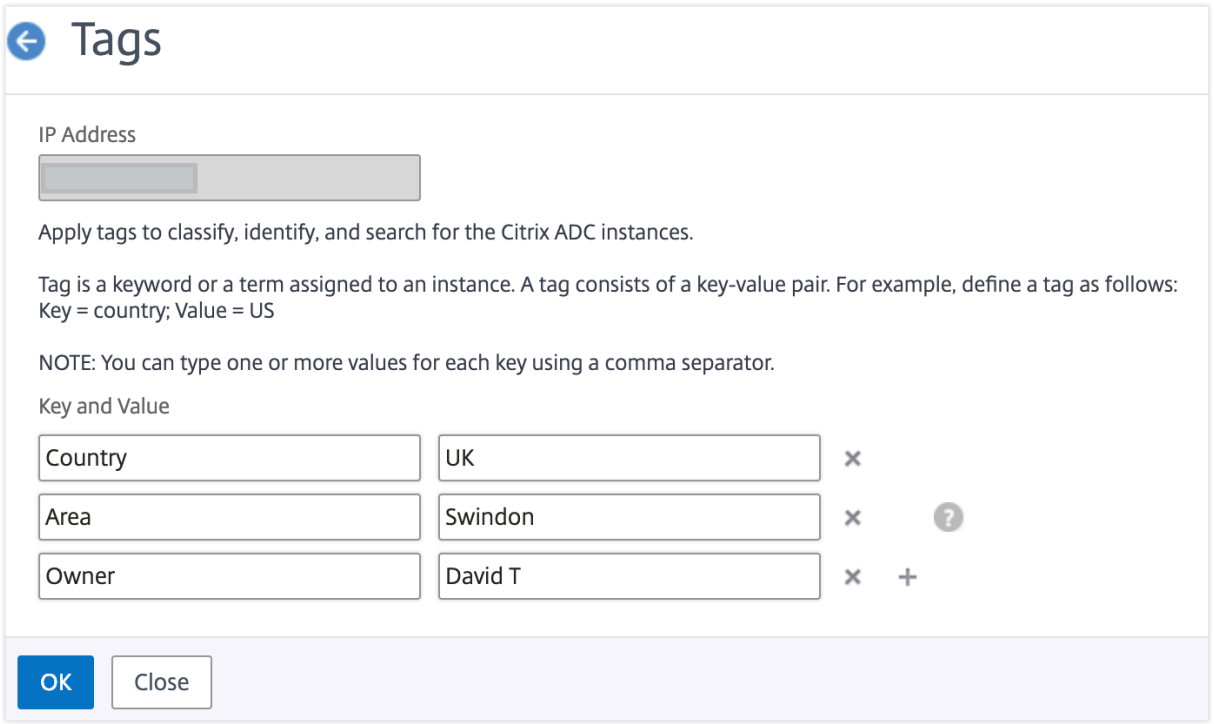
The **Tags** window that appears allows you to create your own "key-value"pairs by assigning values to every keyword that you create.

For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.



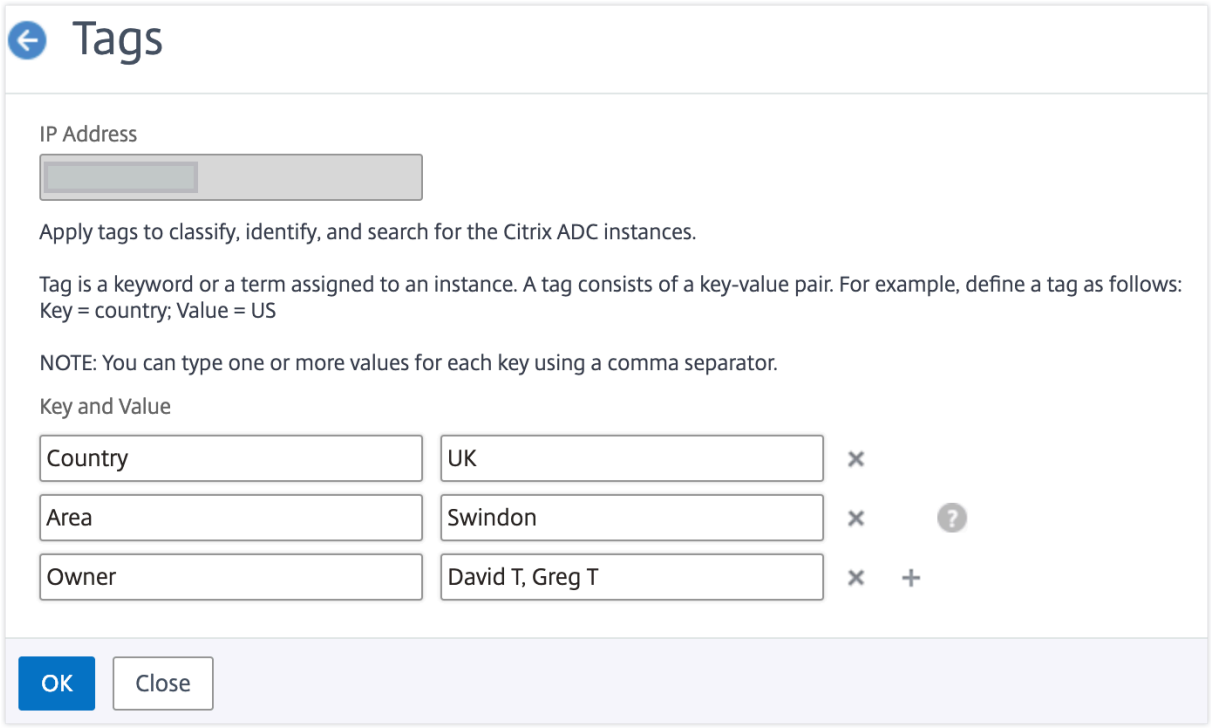


You can also add multiple tags by clicking "+."Adding multiple and meaningful tags allows you to efficiently search for the instances.



You can add multiple values to a keyword by separating them with commas.

For example, you are assigning admin role to another coworker, Greg T. You can add his name separated by a comma. Adding multiple names helps you to search by either of the names or by both names. NetScaler ADM recognizes the comma separated values into two different values.



To know more about how to search for instances based on tags, see How to search instances using values of tags and properties.

> **Note**
>
> You can later add new tags or delete existing tags. There is no restriction on the number of tags that you create.

How to search instances using values of tags and properties

March 11, 2024

There might be a situation where NetScaler Application Delivery Management (ADM) is managing many NetScaler instances. As an admin, you might want the flexibility to search on the instance inventory based on certain parameters. NetScaler ADM now offers improved search capability to search a subset of NetScaler instances based on the parameters that you define in the search field. You can search for the instances based on two criteria - tags and properties.

- **Tags**. Tags are terms or keywords that you can assign to a NetScaler instance to add some additional description about the NetScaler instance. You can now associate your NetScaler instances with tags. These tags can be used to better identify and search on the NetScaler instances.

- **Properties**. Each NetScaler instance added in NetScaler ADM has a few default parameters or properties associated with that instance. For example, each instance has its own host name, IP address, version, host ID, hardware model ID and so on. You can search for instances by specifying values for any of these properties.

For example, consider a situation where you want to find out the list of NetScaler instances that are on version 12.0 and are in the UP state. Here, the version and the state of the instance are defined by the default properties.

Along with the 12.0 version and UP state of the instances, you can also search those instances owned by you. You can create an "Owner"tag and assign a value "David T"to that tag. For more information on how to create and assign tags, see How to create tags and assign to instances.

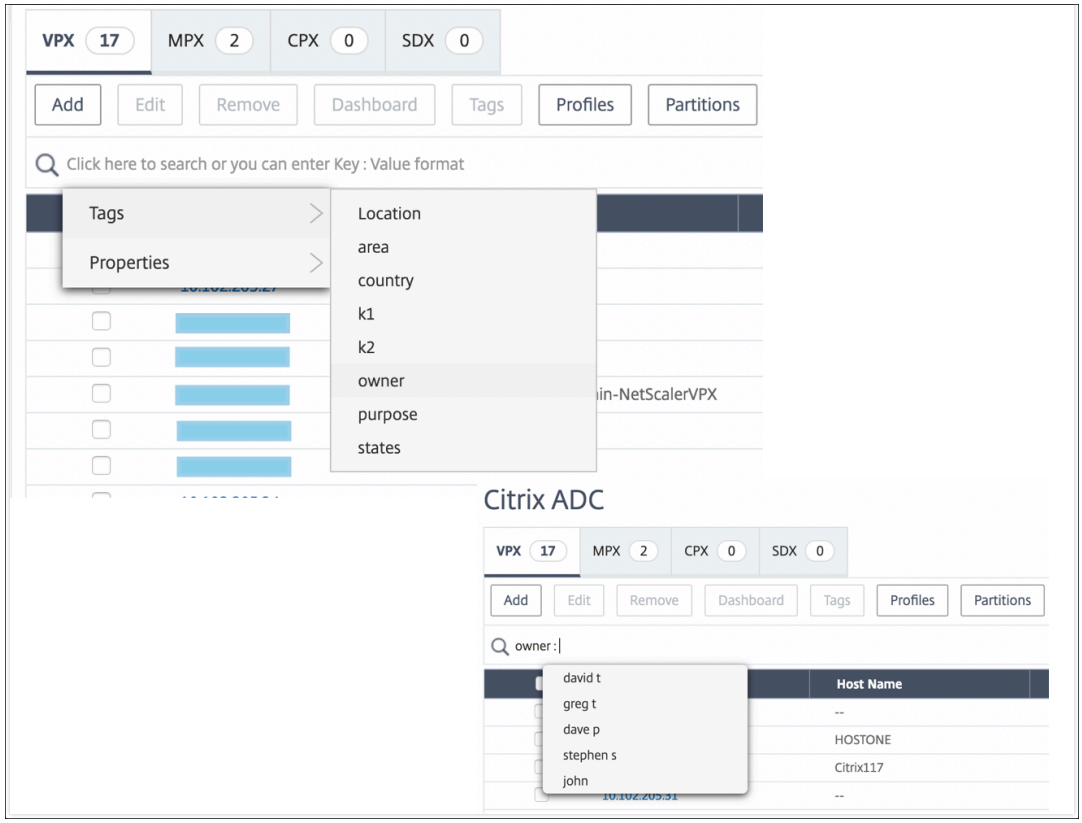
You can use a combination of tags and properties to create your own search criteria.

To search for NetScaler VPX instances

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. Click the search field. You can create a search expression by using Tags or Properties or by combining both.

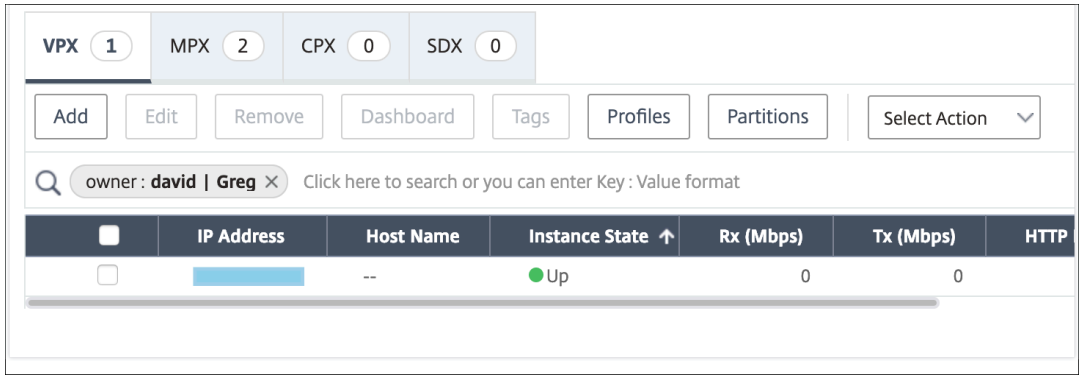
   The following examples show how you can use the search expression efficiently to search for the instance.

   a) Select **Tags** option and select **Owner**. Select "David T."

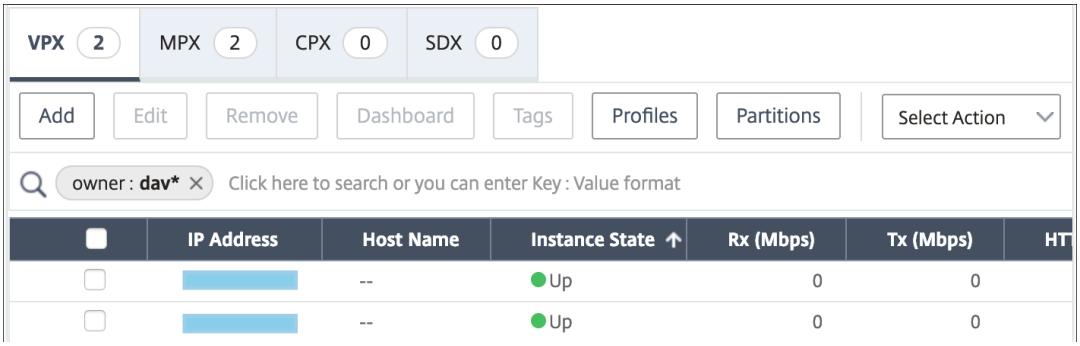


NetScaler ADM supports regular expressions and wildcard characters in the search expressions.

b) You can use regular expressions to further expand the search criteria. For example, you want to search instances owned by either David or Stephen. In such a case, you can type the values by separating the values with a "|"expression.



c) You can also use wildcard characters to replace or represent one or more characters. For example, you can type Dav* to search for all instances owned by David T and Dave P.



> **Note**
>
> For more information on regular expressions and wildcard characters and how to use them, click the "information"icon in the search bar.

Manage admin partitions of NetScaler instances

March 11, 2024

You can configure admin partitions on your Citrix Application Delivery Controller (ADC) instances so that different groups in your organization are assigned different partitions on the same NetScaler instance. A network administrator can be assigned to manage multiple partitions on multiple NetScaler instances.

NetScaler Application Delivery Management (ADM) provides a seamless way of managing all partitions owned by an administrator from a single console. You can manage these partitions without disrupting other partition configurations.

To allow multiple users to manage different admin partitions, you have to create groups and then, assign users and partitions to those groups. Each user can view and manage only the partitions in the group to which the user belongs. Each admin partition is considered as an instance in NetScaler ADM. When you discover a NetScaler instance, the admin partitions configured on that NetScaler instance get added to the system automatically.

Consider that you have two NetScaler VPX instances with two partitions configured on each instance. For example, NetScaler instance 10.102.216.49 has Partition_1, Partition_2, and Partition_3, and NetScaler instance 10.102.29.120 has p1 and p2 as shown in the following image.

To view the partitions, navigate to **Infrastructure > Instances > NetScaler > VPX**, and then click **Partitions**.

You can assign user-p1 the following partitions: 10.102.29.120-p1 and 10.102.216.49-Partition_1. And, you can assign user-p2 to manage partitions 10.102.29.80-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3.

Then , you have to create the two users, user-p1 and user-p2, and you have to assign the users to the groups that you created for them.

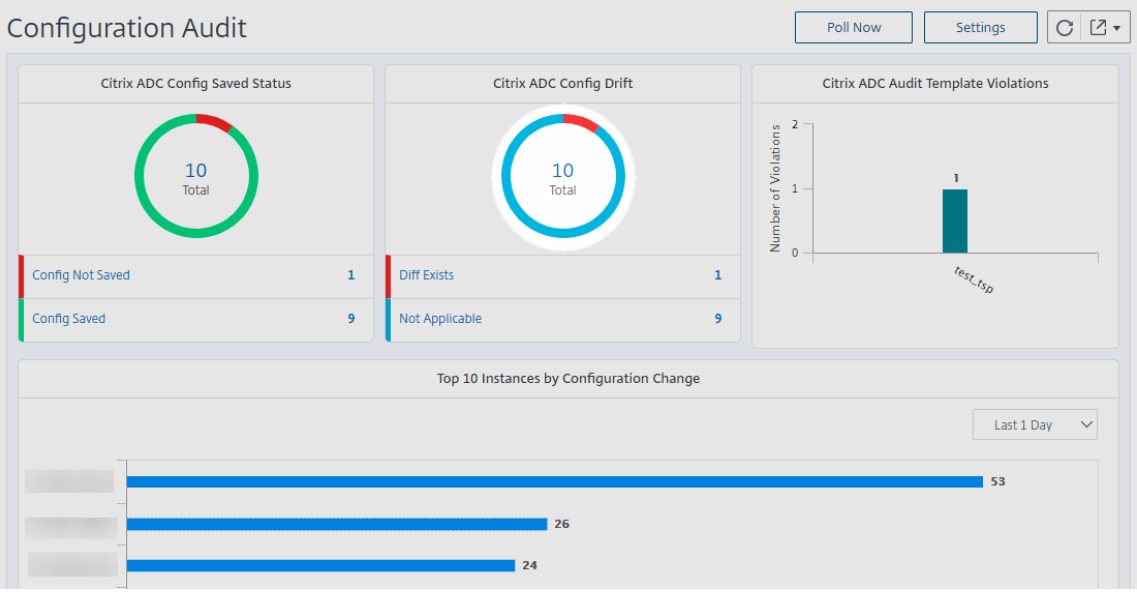
First, you have to create two groups with appropriate permissions (example: admin permissions) and include the required admin partition instances in each group. For example, create system group partition1-admin and add NetScaler admin partitions 10.102.29.120-p1 and 10.102.216.49-Partition_1 to this group. Also create system group partition2-admin and add NetScaler admin partitions 10.102.29.120-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3 and to this group.

After you have created the admin partition, you can also use the revision history difference feature and the audit template for admin partition feature for auditing purposes

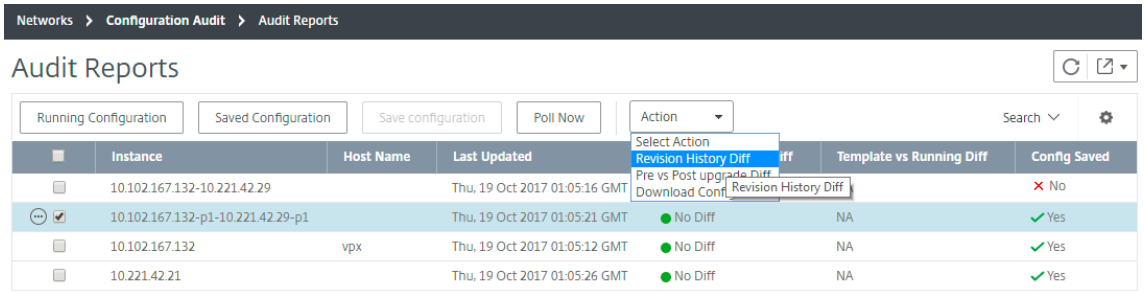
Revision history difference for admin partition allows you to view the difference between the five latest configuration files for a partitioned NetScaler instance. You can compare the configurations files against each other (example Configuration Revision - 1 with Configuration Revision -2) or against the current running/saved configuration with Configuration Revision. Along with the differences in configuration, the correction configurations are also shown. You can export all the corrective commands to your local folder and correct the configurations.

To view the revision history difference:

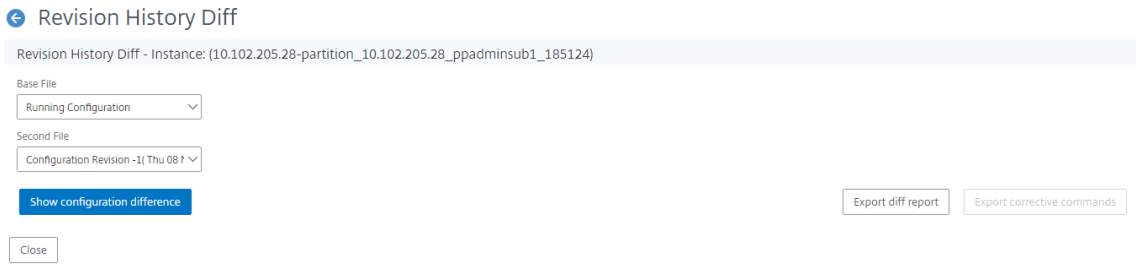
1. Navigate to **Infrastructure > Configuration Audit.** Click inside the donut chart that represents the instance config status. In the **Audit Reports** page that opens, click the partitioned NetScaler instance.



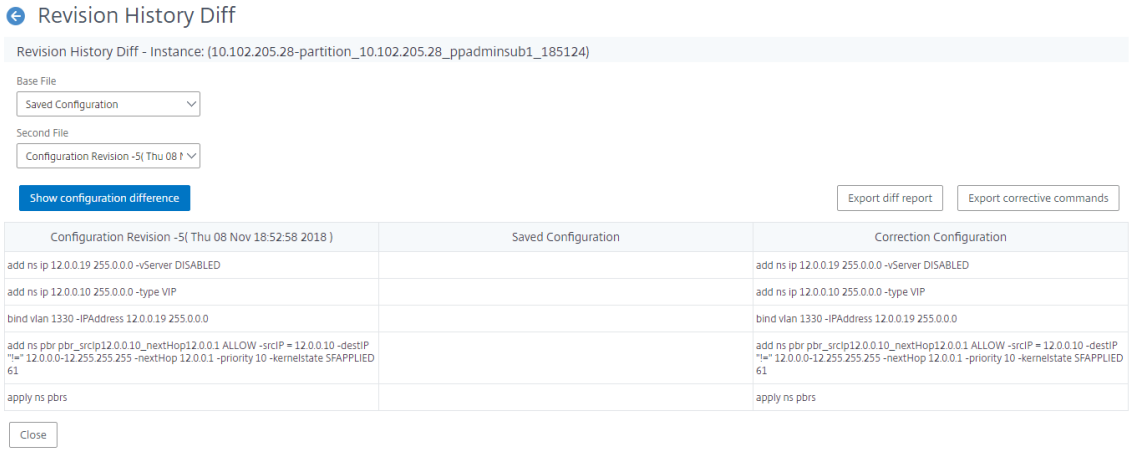
2. From the **Action** menu, click **Revision History Diff.**



3. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision -1 and then, click **Show configuration difference**.



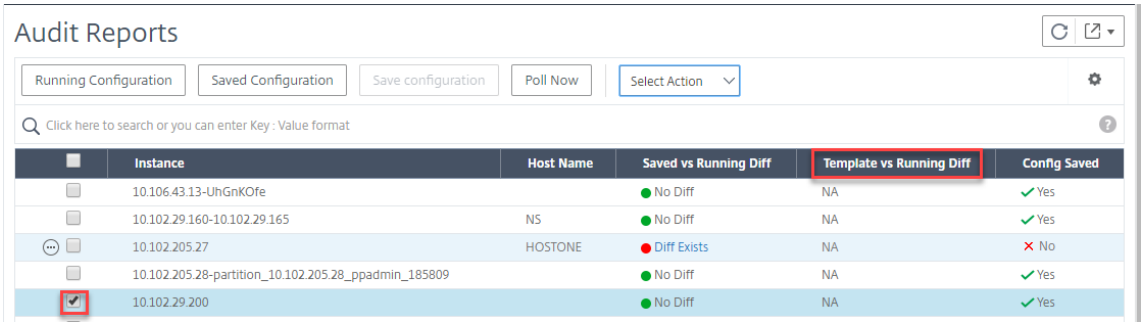
4. You can then view the difference between the five latest configuration files for the selected partitioned NetScaler instance as shown below. You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be run on the base file in order to get the configuration to the desired state (configuration file that is being used for comparison).



Audit templates for partition allow you to create a custom configuration template and associate it with a partition instance. Any variation in the running configuration of the instance with the audit template is shown in the **Template vs Running diff** column of the **Audit Reports** page. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

To view the template vs running difference:

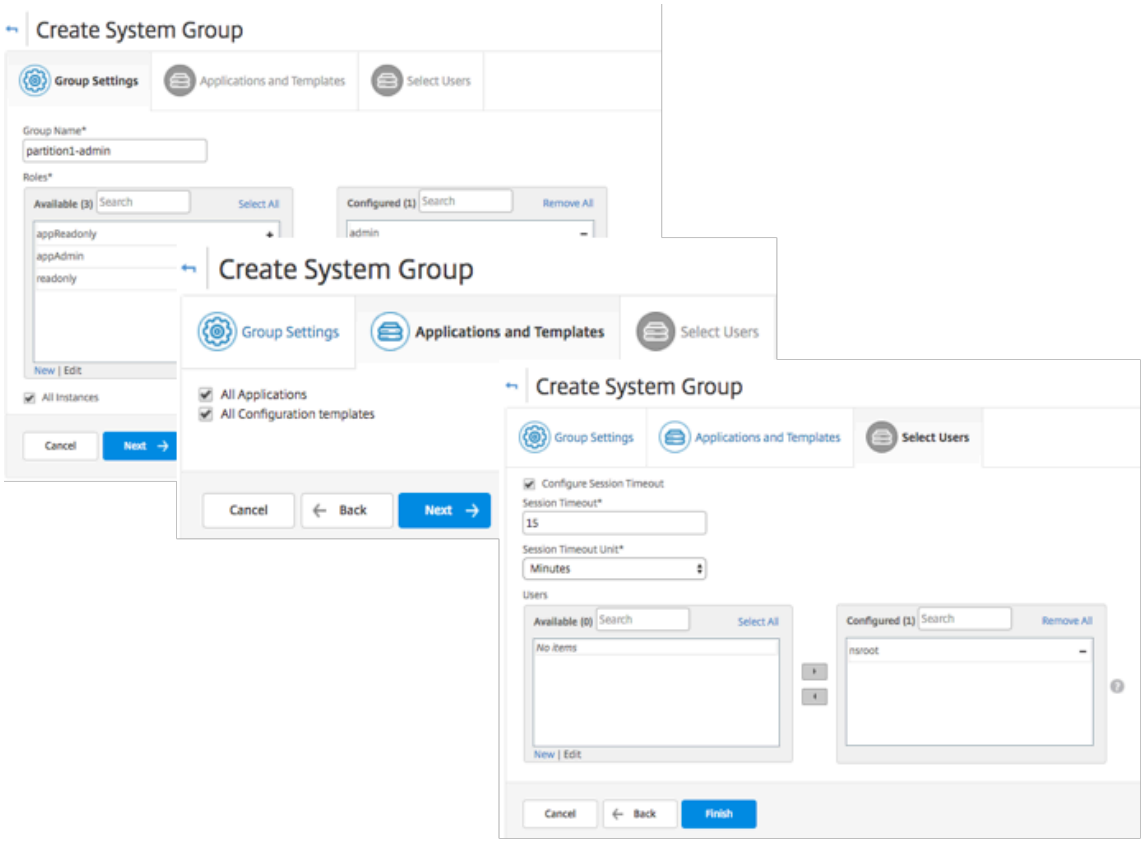
1. From the **Audit Reports** page, click the partitioned NetScaler instance.



2. If there is any difference between the audit template and the running difference, the difference is shown as a hyperlink. Click the hyperlink to view the differences if there is any. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

To create groups:

1. Navigate to **Settings > User Administration > Groups**, and then click **Add**.
2. In the **Create System User** page, specify the following:
   - **Group Settings** tab: Enter the group name and role permissions. To allow access to specific instances, clear the **All Instances** check box, and then choose your instances on the **Select Instances** page.
   - **Applications and Templates** tab: You can choose to use this group across all applications and configuration templates.
   - **Select Users** tab: Select users that you'd like to add to this group. You can click the **New** link in the **Available** table to create new users. Optionally, configure the session timeout, where you can configure the time period for how long a user can remain active.
3. Click **Finish**.



To create users:

1. Navigate to **Settings > User Administration > Users**, and then click **Add**.
2. On the **Create System User** page, specify the user name and password. Optionally, you can enable external authentication and configure the session timeout.
3. Assign the user to a group by adding the group name from the **Available** list to the **Configured** list.
4. Click **Create**.

Now log out and log on with user-p1 credentials. You can view and manage only the admin partitions assigned to you to manage and monitor.

Create a NetScaler high-availability pair

March 11, 2024

A NetScaler high-availability (HA) pair can provide an uninterrupted operation during downtime or

network failures. You can create a HA pair of ADC instances using NetScaler ADM. For more information, see NetScaler high-availability.

Perform the following steps to create a HA pair of ADC instances in NetScaler ADM:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select an ADC instance from the list with which you want to create a HA pair.

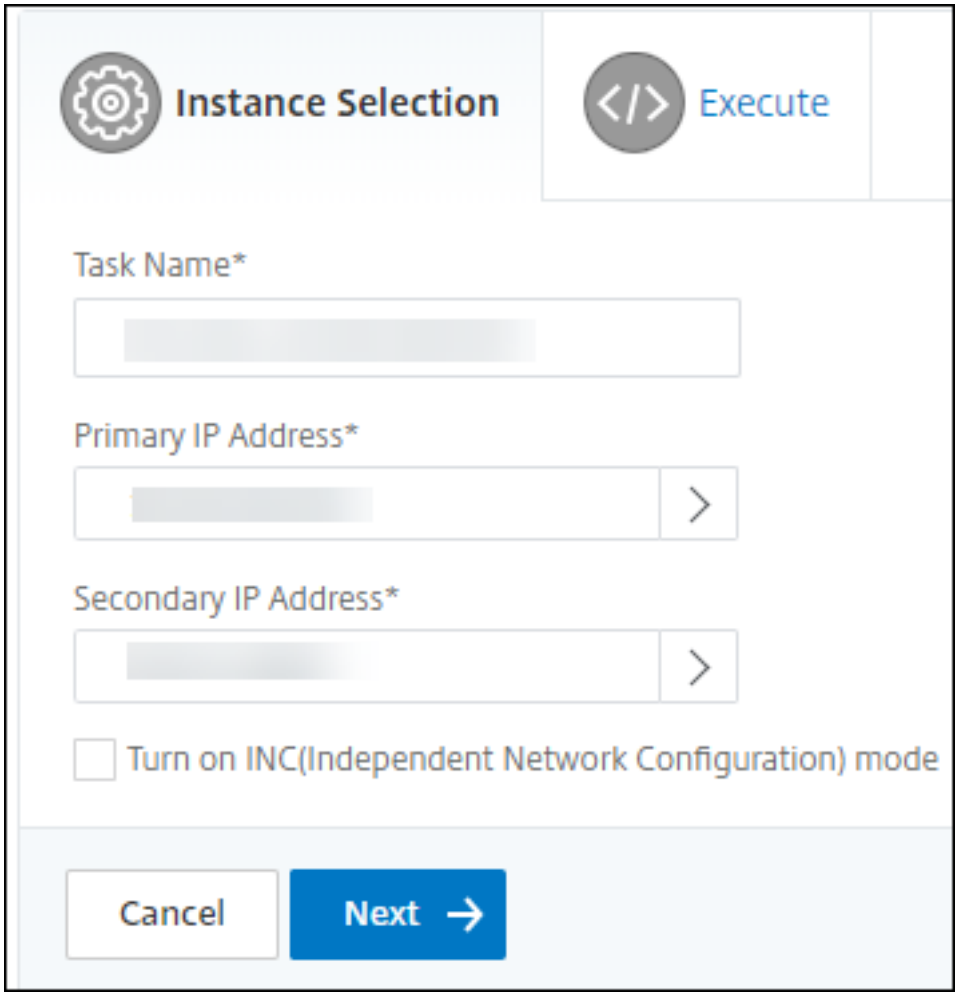
   The selected instance becomes a primary instance in the HA pair.
3. Click Select **Action > Create HA Pair**.
4. In **Instance Selection**, perform the following steps:

   a) In **Secondary IP Address**, click to select a secondary instance.

   b) Select an ADC instance that you want to configure as secondary in the HA pair.

   c) Optional, select **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.

   d) Click **Next**.



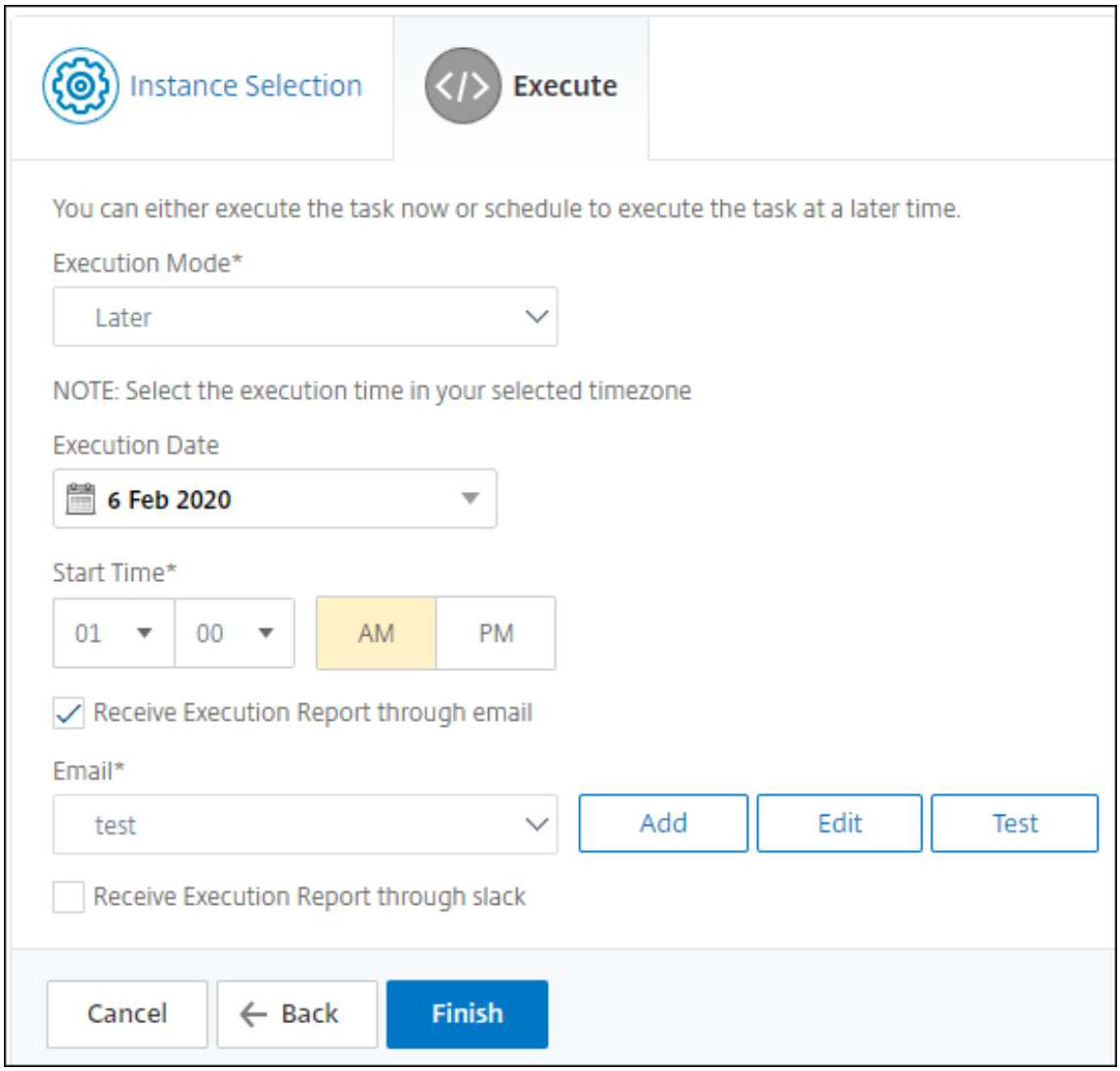
5. In **Execute**, you can decide to create a HA pair now or later.

   a) In **Execution Mode**, select one of the following execution modes:

      - **Now** - Select this option to create a HA pair now.
      - **Later** - Select this option to create a HA pair on specific date and time.

   b) If you have selected **Later** in the **Execution Mode** list, select **Execution Date** and **Start Time** when you want to run this task.

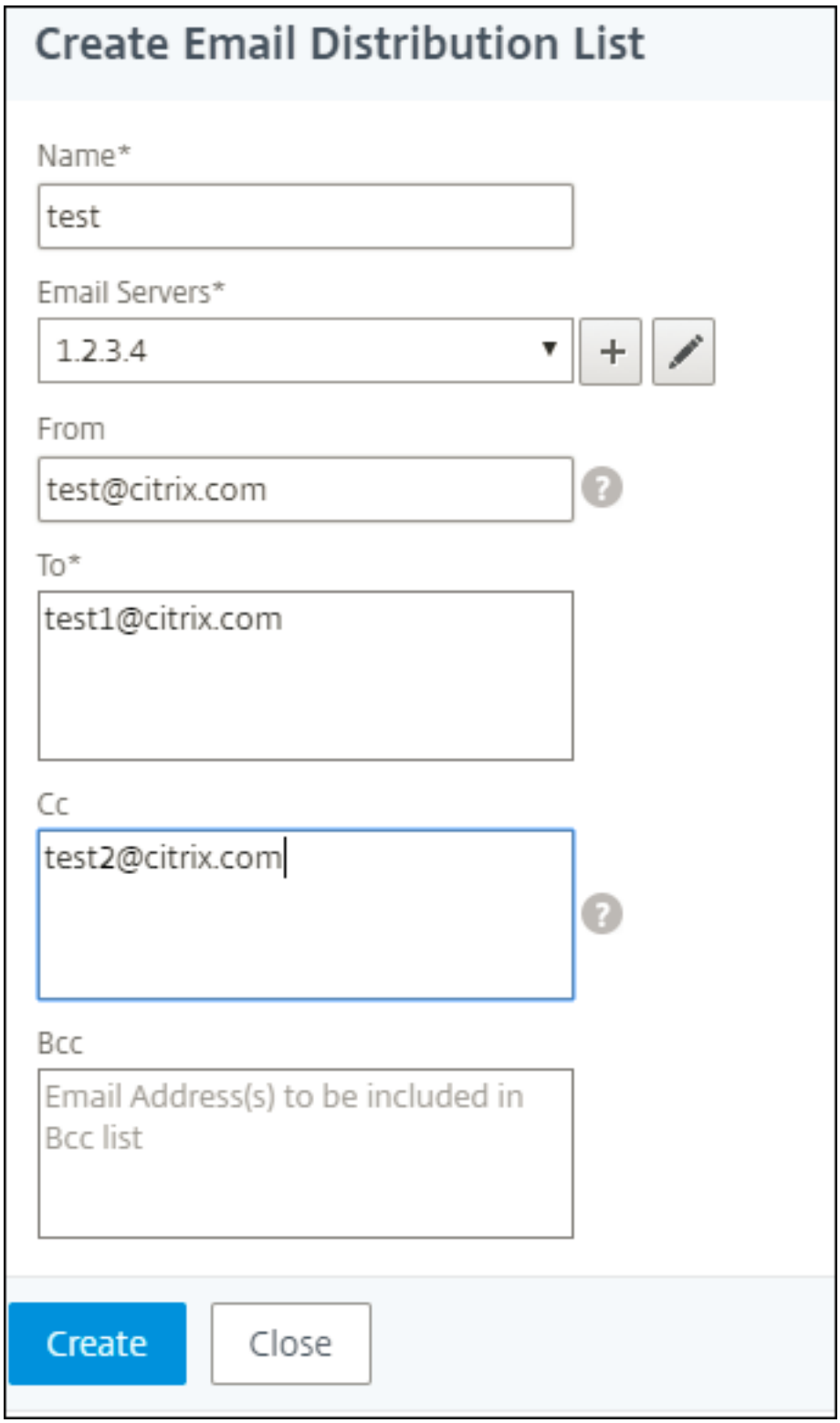
      > **Note**
      >
      > The execution time is displayed in the timezone set in NetScaler ADM.



You can receive an execution report of this task through the following:

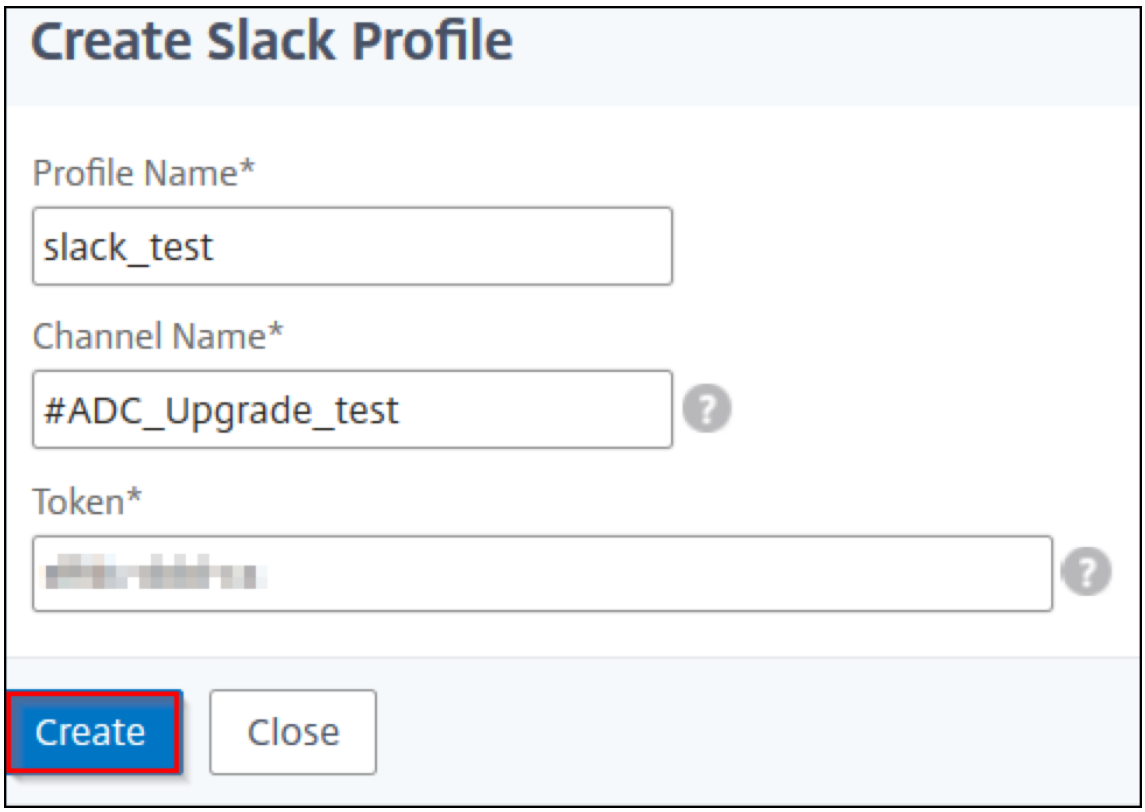
- **Email** - Select the email distribution from the list.

To add a distribution list, click **Add**. Specify the required parameters to add the distribution list and click **Create**.



- **Slack** - Select the Slack profile from the list.

To add a Slack profile, click **Add**. Specify **Profile Name**, **Channel Name**, and **Token** and click **Create**.



Back up and restore NetScaler instances

March 11, 2024

You can back up the current state of a NetScaler instance and later use the backed-up files to restore it to the same state. Always back up an instance before you upgrade it or for precautionary reasons. A backup of a stable system enables you to restore it back to a stable point if it becomes unstable.

There are multiple ways to perform backups and restores on a NetScaler instance. You can manually backup and restore NetScaler configurations using the GUI and CLI. You can also use NetScaler ADM to perform automatic backups and manual restores.

NetScaler ADM backs up the current state of your managed NetScaler instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

NetScaler ADM creates a complete backup and restores the following NetScaler instance types:

- NetScaler SDX

- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

For more information, see Backup and restore an ADC instance.

> **Note**
>
> - Ensure that the NetScaler ADM profile has the admin access to backup and restore ADC instances.
> - From NetScaler ADM, you cannot perform the backup and restore operation on a NetScaler cluster.
> - You cannot use the backup file taken from one instance to restore a different instance.

The backed-up files are stored as a compressed TAR file in the following directory:

```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

To avoid issues due to non-availability of disk space, you can save a maximum of 50 backup files per ADC instance in this directory.

To back up and restore NetScaler instances, you must first configure the backup settings on NetScaler ADM. After configuring the settings, you can select a single NetScaler instance or multiple instances and create a backup of the configuration files in these instances. If necessary, you can also restore the NetScaler instances by using these backed-up files.

Configure instance backup settings

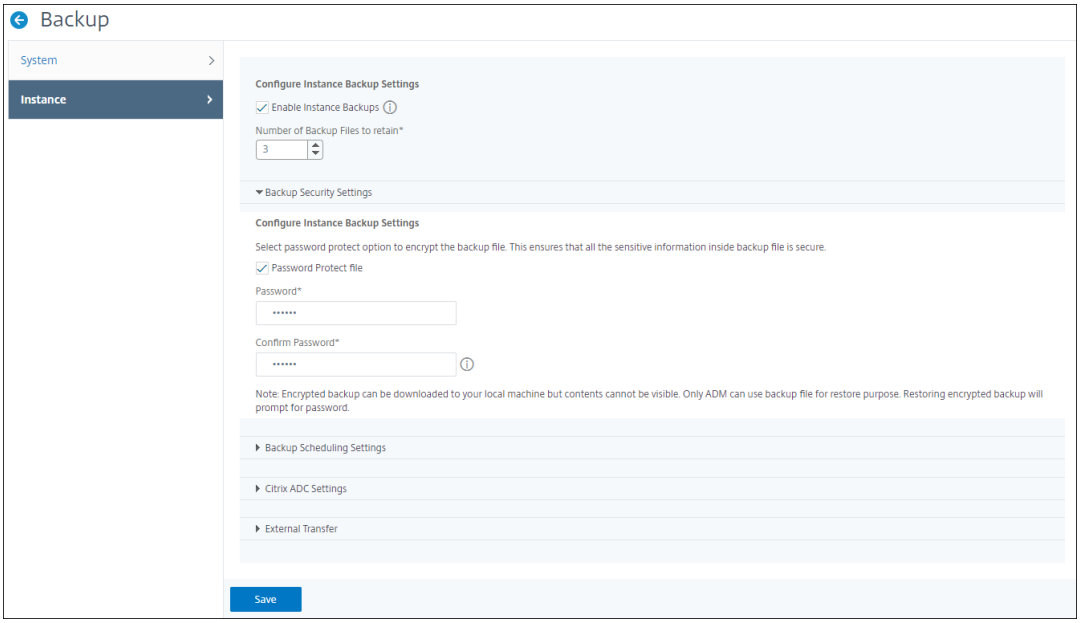
The **Instance Backup Settings** page allows you to configure settings on NetScaler ADM to back up a selected NetScaler instance or multiple instances:

1. In NetScaler ADM, navigate to **Settings** > **Administration**.
2. In **Backup**, select **Configure System and Instance backup**.
3. Select **Instance** and specify the following:
    - **Enable Instance Backups**: By default, NetScaler ADM is enabled for taking backups of NetScaler instances. Clear this option if you do not want to create backup files for the instances.
    - **Password Protect File**: (optional) Select the password protect option to encrypt the backup file. Encrypting the backup file ensures that all the sensitive information inside the backup file is secure.

> **Note**
>
> You can download the encrypted backup file to your local machine, but you cannot open the file either with the NetScaler ADM GUI or with any text editor. You are prompted to provide the password when restoring the encrypted backup file. You can, however, open an unencrypted backup file on your system.

- **Number of Backup Files to retain**: Specify the number of backup files to retain in NetScaler ADM. You can retain up to 50 backup files per ADC instance. The default is three backup files.

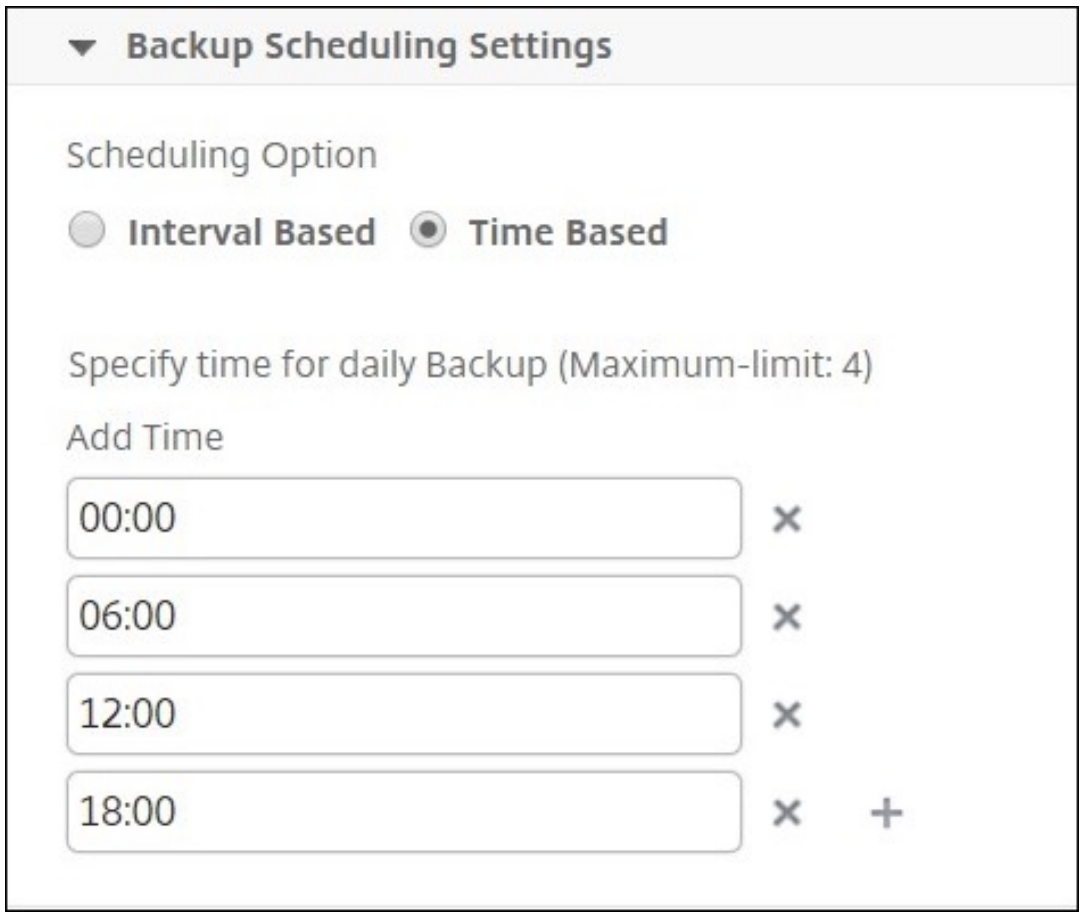
> **Note**
>
> Each backup file accounts for some storage requirement. Citrix recommends that you store an optimal number of NetScaler backup files on NetScaler ADM as per your requirement.



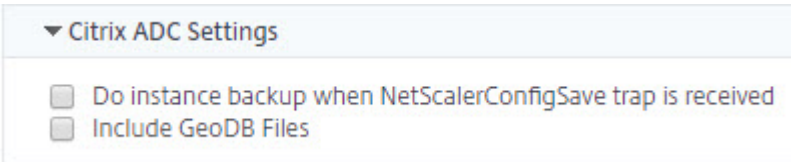
- **Backup scheduling settings**: (optional) There are two options available for creating backup files, though you can use only one option at a time:

  a) The default backup scheduling option is "interval-based."A backup file is created in NetScaler ADM after the specified interval elapses. The default backup interval is 12 hours.

  b) You can also change the type of scheduled backups to "time-based."In this option, specify the time in `hours:minutes` format to back up instances at the specified time. NetScaler ADM allows a maximum of four daily backups to happen on the instances.



- **NetScaler settings**: (optional) By default, NetScaler ADM does not create a backup file when it receives the "NetScalerConfigSave"trap. But, you can enable the option to create a backup file whenever a NetScaler instance sends a "NetScalerConfigSave"trap to NetScaler ADM. A NetScaler instance sends "NetScalerConfigSave"every time the configuration on the instance is saved.
- **Geodatabase files**: (optional) By default, NetScaler ADM does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.

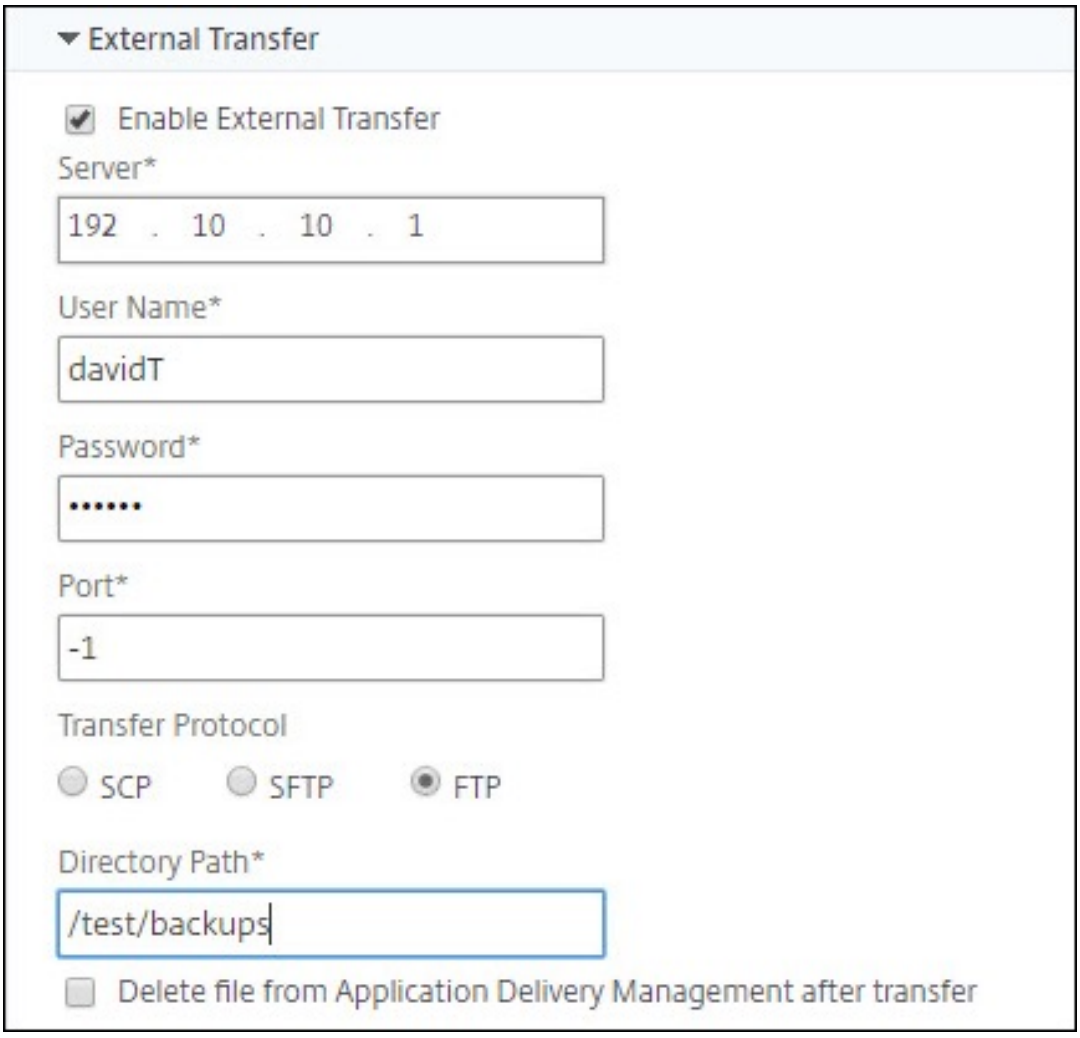


- **External Transfer:**(optional) NetScaler ADM allows you to transfer the NetScaler instance backup files to an external location:
  a) Specify the IP address of the location.
  b) Specify the user name and the password of the external server to which you want to transfer the backup files.

c) Specify the transfer protocol and the port number.

d) You can specify the directory path where the file must be stored.

e) Optional, you can also delete the backup file from NetScaler ADM after transferring it to the external server.



Note

NetScaler ADM sends an SNMP trap or a Syslog notification to itself when there is a backup failure for any of the selected NetScaler instances.

Create a backup for a selected NetScaler instance by using NetScaler ADM

Perform this task if you want to back up a selected NetScaler instance or multiple instances:

1. In NetScaler ADM, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instances (for example, NetScaler VPX) to display on the screen.

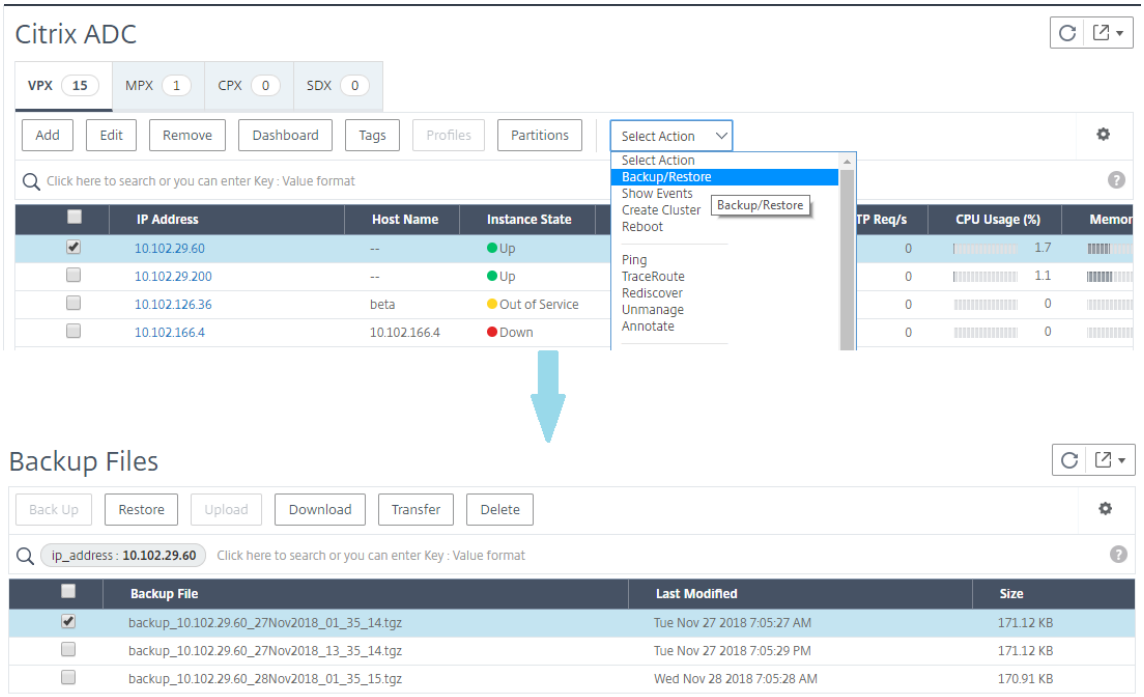
2. Select the instance that you want to back up.
    - For MPX, VPX, and BLX instance, select **Backup/Restore** from the **Select Action** list.
    - For an SDX instance, click **Backup/Restore**.
3. On the **Backup Files** page, click **Back Up**.
4. You can specify whether to encrypt your backup file for more security. You can either enter your password or use the global password that you previously specified on the Instance Backup Settings page.
5. Click **Continue**.

Restore a NetScaler instance by using NetScaler ADM

> Note:
>
> If you have NetScaler instances in a HA pair, you need to note the following:
>
> - Restore the same instance from which the backup file was created. For example, let us consider a scenario that a backup was taken from the primary instance of the HA pair. During the restore process, ensure that you are restoring the same instance, even if it is no longer the primary instance.
> - When you initiate the restore process on the primary ADC instance, you cannot access the primary instance and the secondary instance gets changed to **STAYSECONDARY**. Once the restore process is completed on the primary instance, the secondary ADC instance changes from **STAYSECONDARY** to **ENABLED** mode and becomes part of the HA pair again. You can expect a possible downtime on the primary instance until the restore process gets completed.

Perform this task to restore a NetScaler instance by using the backup file that you created earlier:

1. Navigate to **Infrastructure > Instances**, select the instance that you want to restore, and then click **View Backup**.
2. On the **Backup Files** page, select the backup file containing the settings that you want to restore, and then click **Restore**.



Restore a NetScaler SDX appliance using NetScaler ADM

In NetScaler ADM, the backup of the NetScaler SDX appliance includes the following:

- NetScaler instances hosted on the appliance
- SVM SSL certificates and keys
- Instance prune settings (in XML format)
- Instance backup settings (in XML format)
- SSL certificate poll settings (in XML format)
- SVM db file
- NetScaler config files of devices present on SDX
- NetScaler build images
- NetScaler XVA images, these images are stored in the following location: `/var/mps/sdx_images/`
- SDX Single Bundle Image (SVM+XS)
- Third Party instance images (if provisioned)

Restore your NetScaler SDX appliance to the configuration available in the backup file. During appliance restore, the entire current configuration is deleted.

If you are restoring the NetScaler SDX appliance by using a backup of a different NetScaler SDX appliance, ensure that you add the licenses and configure the new appliance's Management Service network settings to match the settings in the backup file before you start the restore process. That is, the new appliance must be licensed and meet the minimum license requirements of the backup file.

For example, if the backup had five VPX instances with a total of 5 GB, then the new appliance must also be able to support these requirements. Or if the backup appliance had a platinum license, the new appliance must have the same or higher license. Network settings, such as IP address, netmask, gateway, XenServer IP address, and DNS server must be properly configured on the new appliance.

Before you restore the SDX appliance, ensure that the backed-up SDX appliance platform variant is the same as the appliance. You cannot restore from a different platform variant.

> **Note**
>
> Before you restore an SDX RMA appliance, ensure that the backed-up version is either the same or higher than the RMA version.

To restore the SDX appliance from the backed-up file:

1. In the NetScaler ADM GUI, navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Backup/Restore**.
3. Select the backup file of the same instance that you want to restore.
4. Click **Repackage Backup**.

   When the SDX appliance is backed up, the XVA files and images are stored separately to save the network bandwidth and the disk space. Therefore, you must repackage the backed-up file before you restore the SDX appliance.

   When you repackage the backup file, it includes all the backed-up files together to restore the SDX appliance. The repackaged backup file ensures the successful restoration of the SDX appliance.
5. Select the backup file that is repackaged and click **Restore**.

Force a failover to the secondary NetScaler instance

March 11, 2024

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix Application Delivery Controller (ADC) instance. You can force failover from either the primary instance or the secondary instance. When you force a failover on the primary instance, the primary becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the instance.

A forced failover fails in any of the following circumstances:

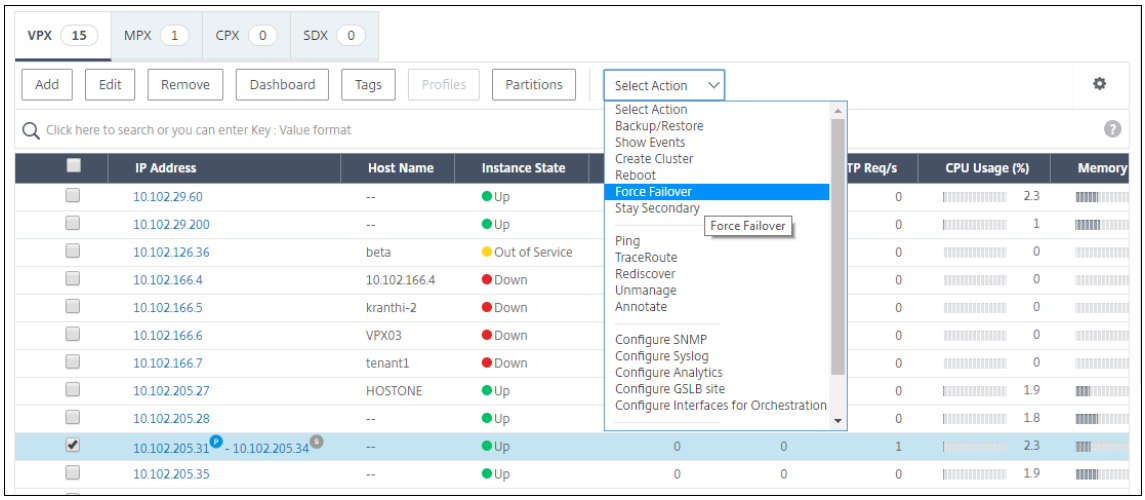
- You force failover on a standalone system.
- The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.
- The secondary instance is configured to remain secondary.

The NetScaler instance displays a warning message if it detects a potential issue when you run the force failover command. The message includes the information that triggered the warning, and requests confirmation before proceeding.

You can force a failover on a primary instance or on a secondary instance.

To force a failover to the secondary NetScaler instance using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Instances > NetScaler > VPX** tab, and then select an instance .
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Force Failover.**
4. Click **Yes** to confirm the force failover action.



Force a secondary NetScaler instance to stay secondary

March 11, 2024

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

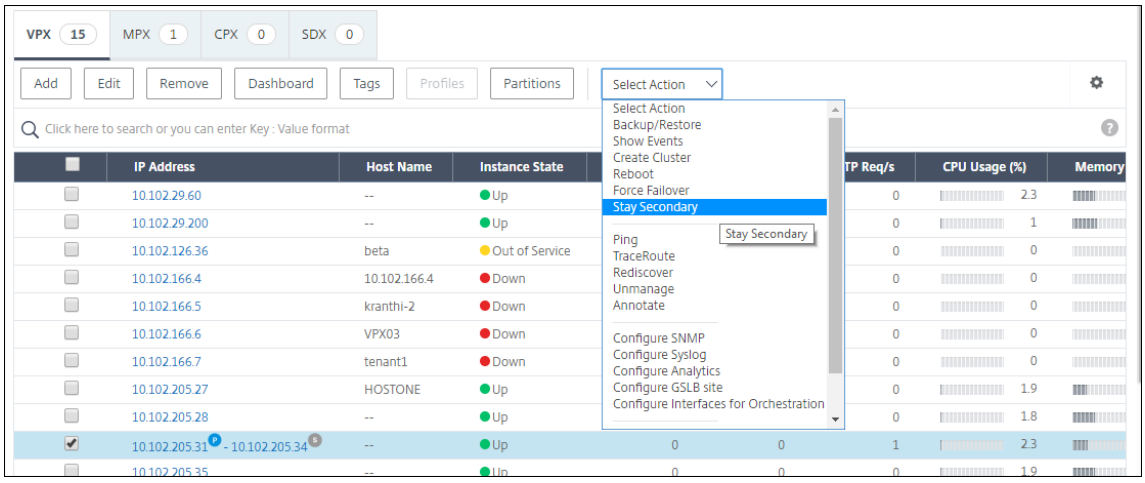
For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want the secondary node to take over. You want it to remain the secondary node even if it detects a failure in the primary node.

When you force the secondary node to stay secondary, it remains secondary even if the primary node goes down. Also, when you force the status of a node in an HA pair to stay secondary, it does not participate in HA state machine transitions. The status of the node is displayed as STAYSECONDARY.

> **Note**
>
> When you force a system to remain secondary, the forcing process is not propagated or synchronized. It affects only the node on which you run the command.

To configure a secondary NetScaler instance to stay secondary by using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Instances > NetScaler > VPX** tab, and then select an instance.
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the "Stay Secondary"action.



Create instance groups

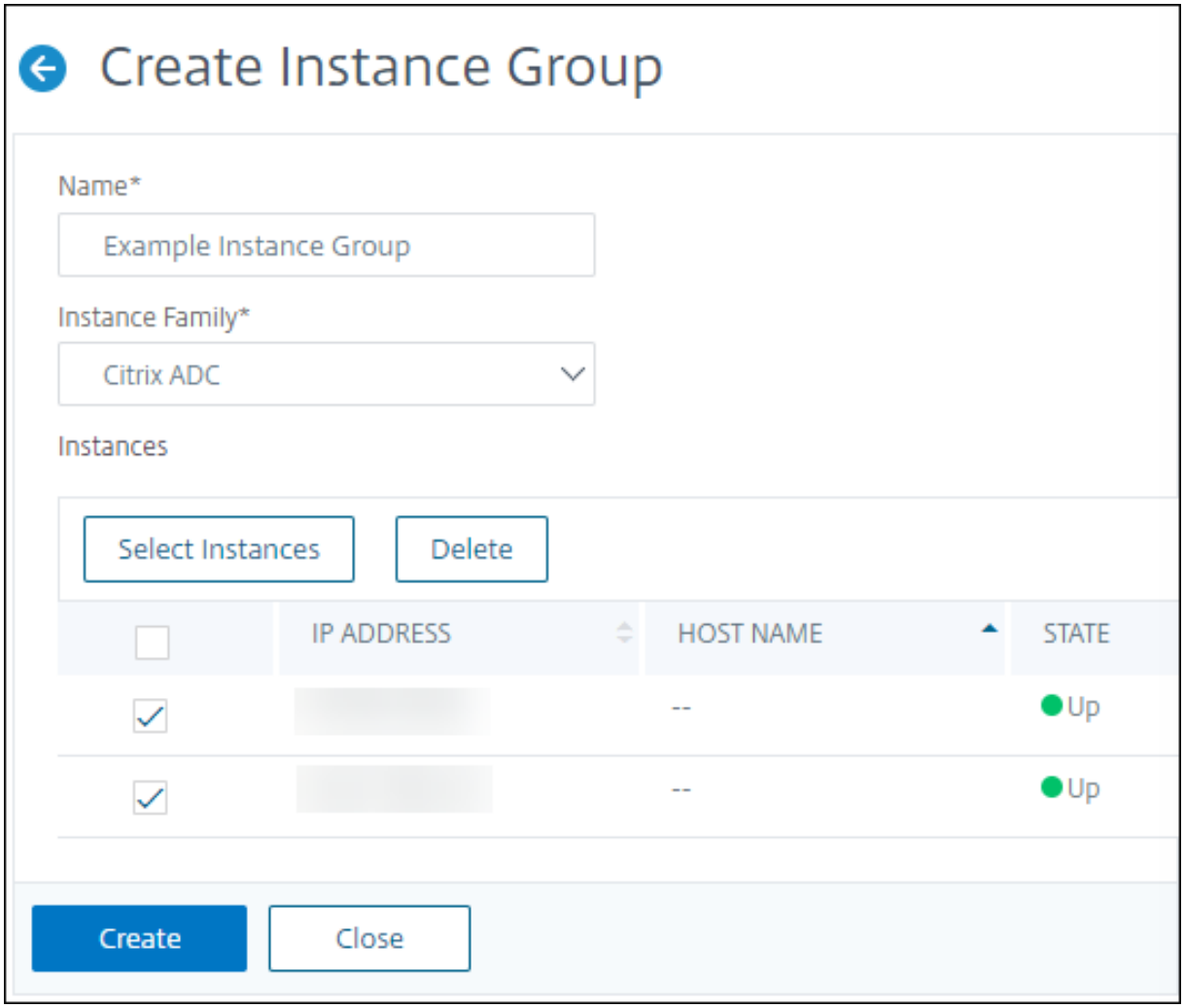
March 11, 2024

To create an instance group, you must first add all your NetScaler instances to NetScaler ADM. After you have added the instances successfully, create instance groups based on their instance family. Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

To create an instance group using NetScaler ADM

1. In NetScaler ADM, navigate to **Infrastructure > Instance Groups**, and then click **Add**.
2. Specify a name to your instance group and select **NetScaler** from the **Instance Family** list.
3. Click **Select Instances**. On the **Select Instances** page, select the instances that you want to group and click **Select**.

   The table lists the selected instances and their details. If you want to remove any instance from the group, select the instance from the table and click **Delete**.
4. Click **Create**.



Provision NetScaler VPX instances on SDX using ADM

March 11, 2024

You can provision one or more NetScaler VPX instances on the SDX appliance by using NetScaler ADM. The number of instances that you can deploy depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the ADM restricts you from provisioning more NetScaler instances.

Before you begin, ensure to add an SDX instance in ADM where you want to provision VPX instances.

To provision a VPX instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **SDX** tab, select an SDX instance where you want to provision a VPX instance.
3. In **Select Action**, select **Provision VPX**.

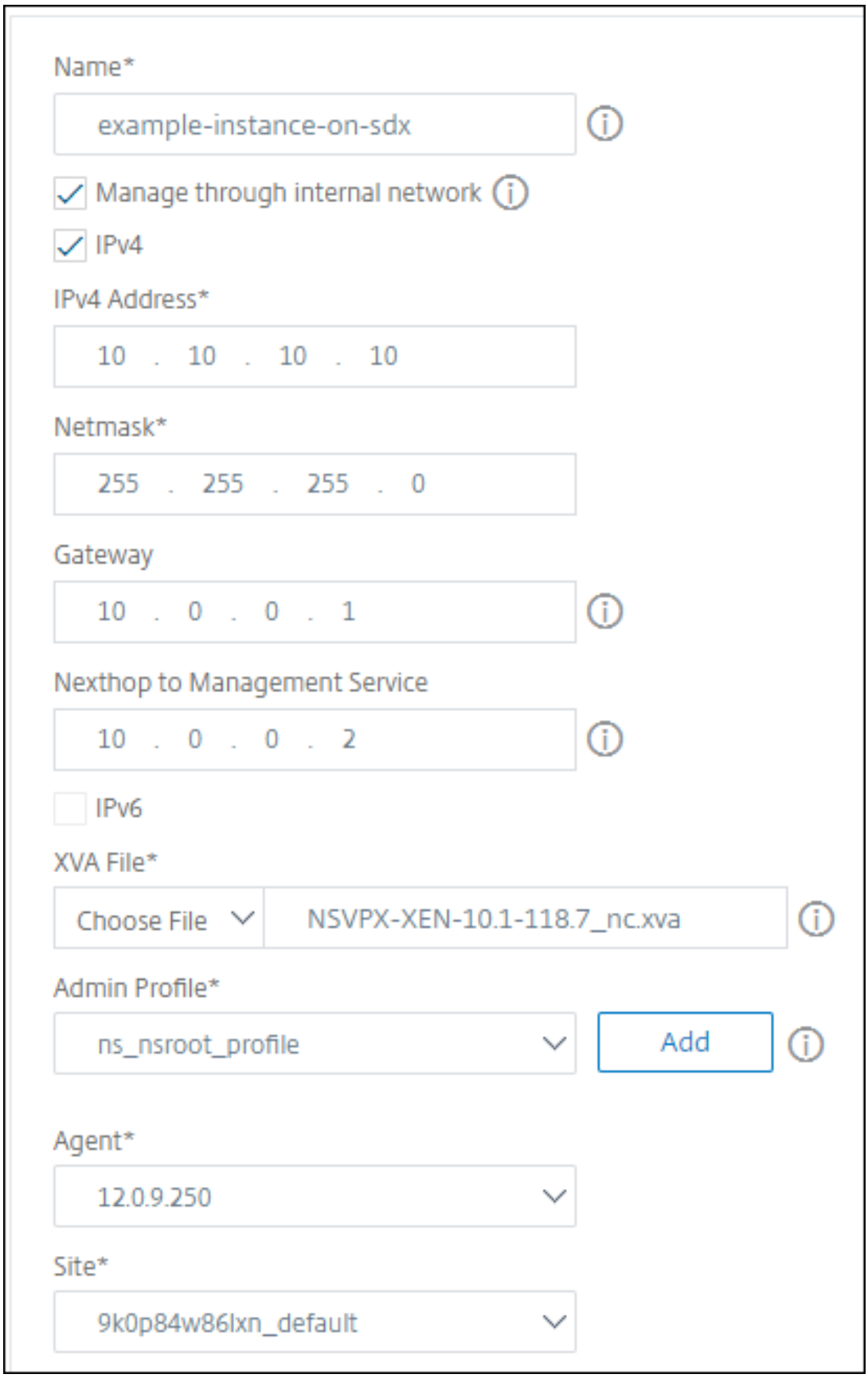
Step 1 - Add a VPX instance

The ADM uses the following information to configure VPX instances in an SDX appliance:

- **Name** - Specify a name to an ADC instance.
- Establish a communication network between SDX and VPX. To do so, select the required options from the list:
  - **Manage through internal network** - This option establishes an internal network for a communication between the ADM and a VPX instance.
  - **IP address** - You can select an **IPv4** or **IPv6** address or both to manage the NetScaler VPX instance. A VPX instance can have only one management IP (also called NetScaler IP). You cannot remove the NetScaler IP address.

    For the selected option, assign a netmask, default gateway, and next hop to the ADM server for the IP address.
- **XVA File** - Select the XVA file from which you want to provision a VPX instance. Use one of the following options to select the XVA file.
  - **Local** - Select the XVA file from your local machine.
  - **Appliance** - Select the XVA file from an ADM file browser.
- **Admin Profile** - This profile provides access to provision VPX instances. With this profile, ADM retrieves the configuration data from an instance. If you have to add a profile, click **Add**.

- **Agent** - Select the agent with which you want to associate the instances
- **Site** - Select the site where you want the instance to be added.



Step 2 - Allocate licenses

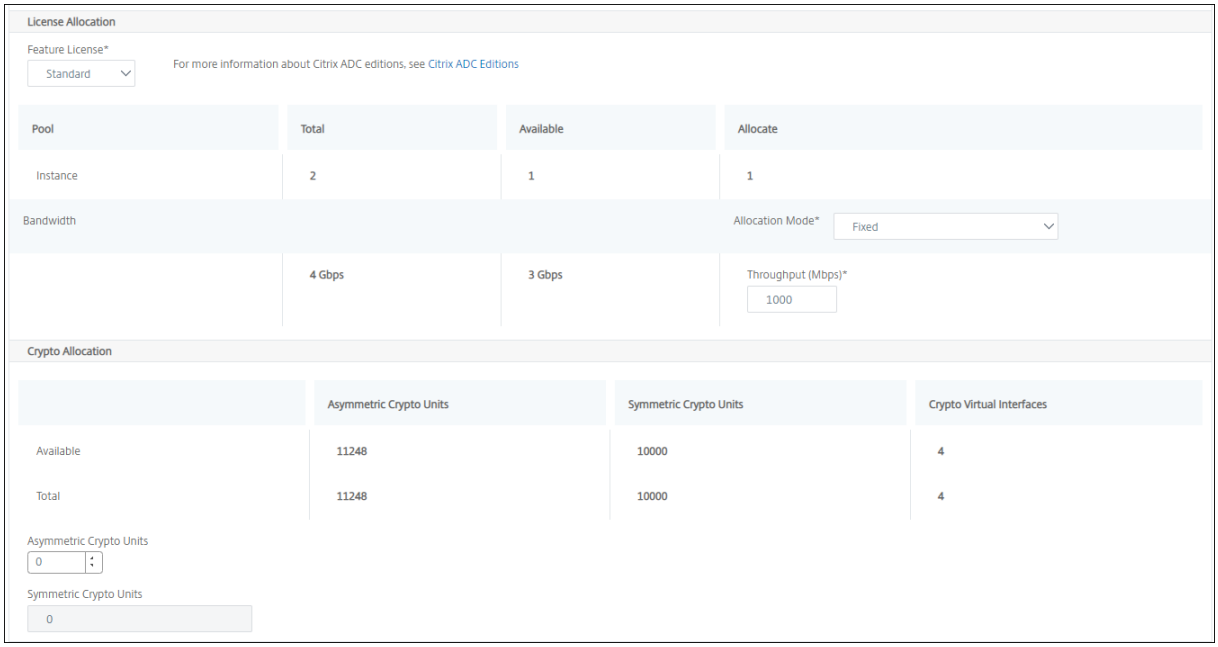
In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **Allocation mode** - You can choose **Fixed** or **Burstable** modes for the bandwidth pool.

  If you choose **Burstable** mode, you can use extra bandwidth when the fixed bandwidth is reached.

- **Throughput** - Assign the total throughput (in Mbps) to an instance.

> **Note**
>
> Buy a separate license (SDX 2-Instance Add-On Pack for Secure Web Gateway) for Citrix Secure Web Gateway (SWG) instances on SDX appliances. This instance pack is different from the SDX platform license or SDX instance pack.
>
> For more information, see Deploying a Citrix Secure Web Gateway Instance on an SDX Appliance.



From the SDX 12.0 57.19 version, the interface to manage crypto capacity has changed. For more information, see Manage crypto capacity.

Step 3 - Allocate resources

In the **Resource Allocation** section, allocate resources to a VPX instance to maintain traffic.

- **Total Memory (MB)** - Assign total memory to an instance. The minimum value is 2048 MB.

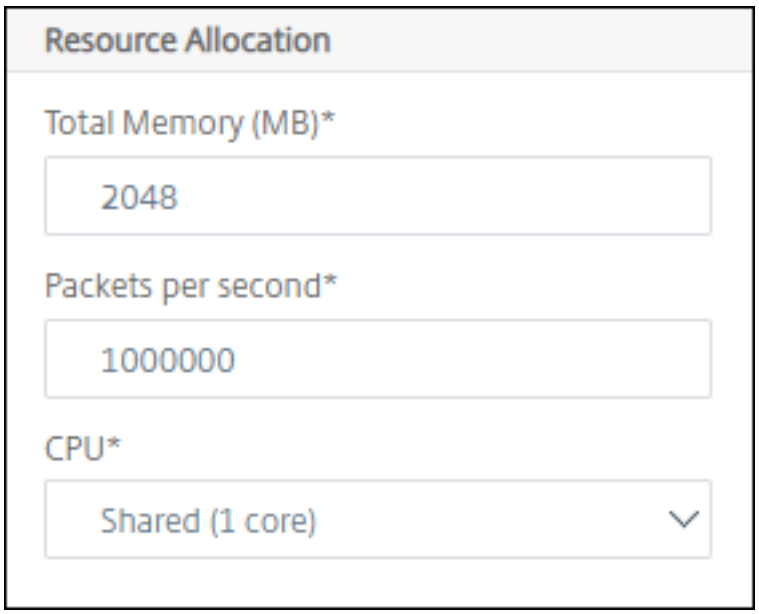
- **Packets per second** - Specify the number of packets to transmit per second.
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  When you select a shared core to an instance, the other instances can use the shared core at the time of resource shortage.

  Restart instances on which CPU cores are reassigned to avoid any performance degradation.

  If you are using the SDX 25000xx platform, you can assign a maximum of 16 cores to an instance. Also, if you are using the SDX 2500xxx platform, you can assign a maximum of 11 cores to an instance.

  > **Note**
  >
  > For an instance, the maximum throughput that you configure is 180 Gbps.



The following table lists the supported VPX, Single bungle image version, and the number of cores you can assign to an instance:

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 8015, SDX 8400, and SDX 8600	4	3	3
SDX 8900	8	7	7

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542	12	10	5
SDX 17500, SDX 19500, and SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550, and SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 and SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100, and SDX 22120	16	14	7
SDX 24100 and SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G and SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS and SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S, and SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (if version is 11.1-51.x or higher); 9 (if version is 11.1-50.x or lower; all versions of 11.0 and 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

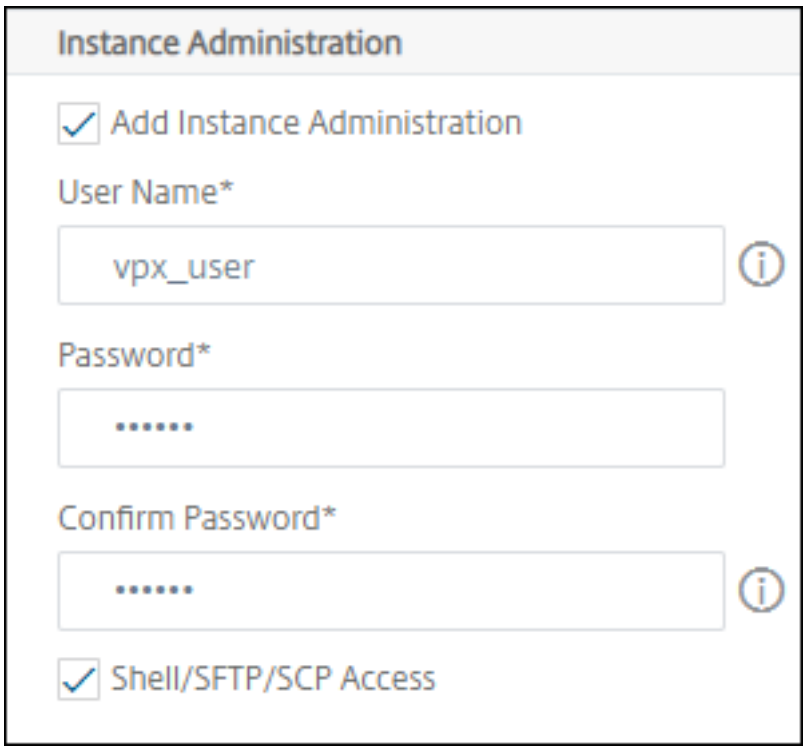
> **Note**
>
> On the SDX 26xxx platform, a maximum of 26 CPU cores can be assigned to a VPX instance. If crypto units are assigned to the instance, the maximum number of cores depends on the number of crypto units and data interfaces.
>
> For example, if you assign 24000 crypto units to an instance, you can assign 24 CPU cores and maximum two data interfaces to the instance. The SDX appliance considers data interfaces and crypto units as PCI devices. For 26000 crypto units, VPX instance provisioning fails because of no space to add data interfaces.

Step 4 - Add instance administration

You can create an admin user for the VPX instance. To do so, select **Add Instance Administration** in the **Instance Administration** section.

Specify the following details:

- **User name**: The user name for the NetScaler instance administrator. This user has superuser access but does not have access to networking commands to configure VLANs and interfaces.
- **Password**: Specify the password for the user name.
- **Shell/Sftp/Scp Access**: The access allowed to the NetScaler instance administrator. This option is selected by default.



Step 5 - Specify network settings

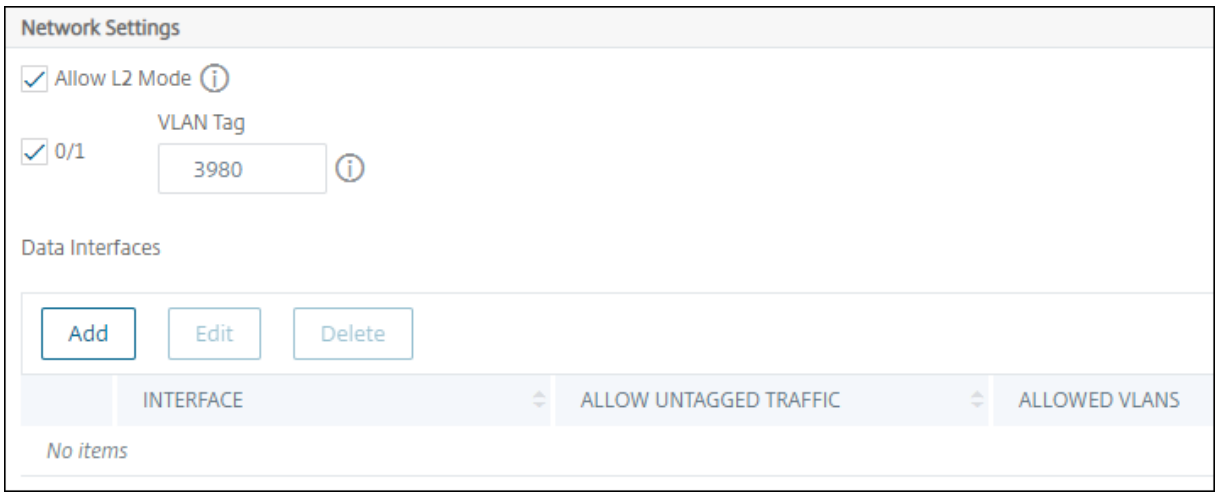
Select the required network settings to an instance:

- **Allow L2 Mode under network settings** - You can allow L2 mode on the NetScaler instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode. For more information, see Allowing L2 Mode on a NetScaler instance.

  > **Note**
  >
  > If you disable L2 mode for an instance, you must log on to the instance and disable L2 mode from that instance. Otherwise, it might cause all the other NetScaler modes to be disabled after you restart the instance.

- **0/1** - In **VLAN tag**, specify a VLAN ID for the management interface.
- **0/2** - In **VLAN tag**, specify a VLAN ID for the management interface.

By default interface **0/1** and **0/2** are selected.

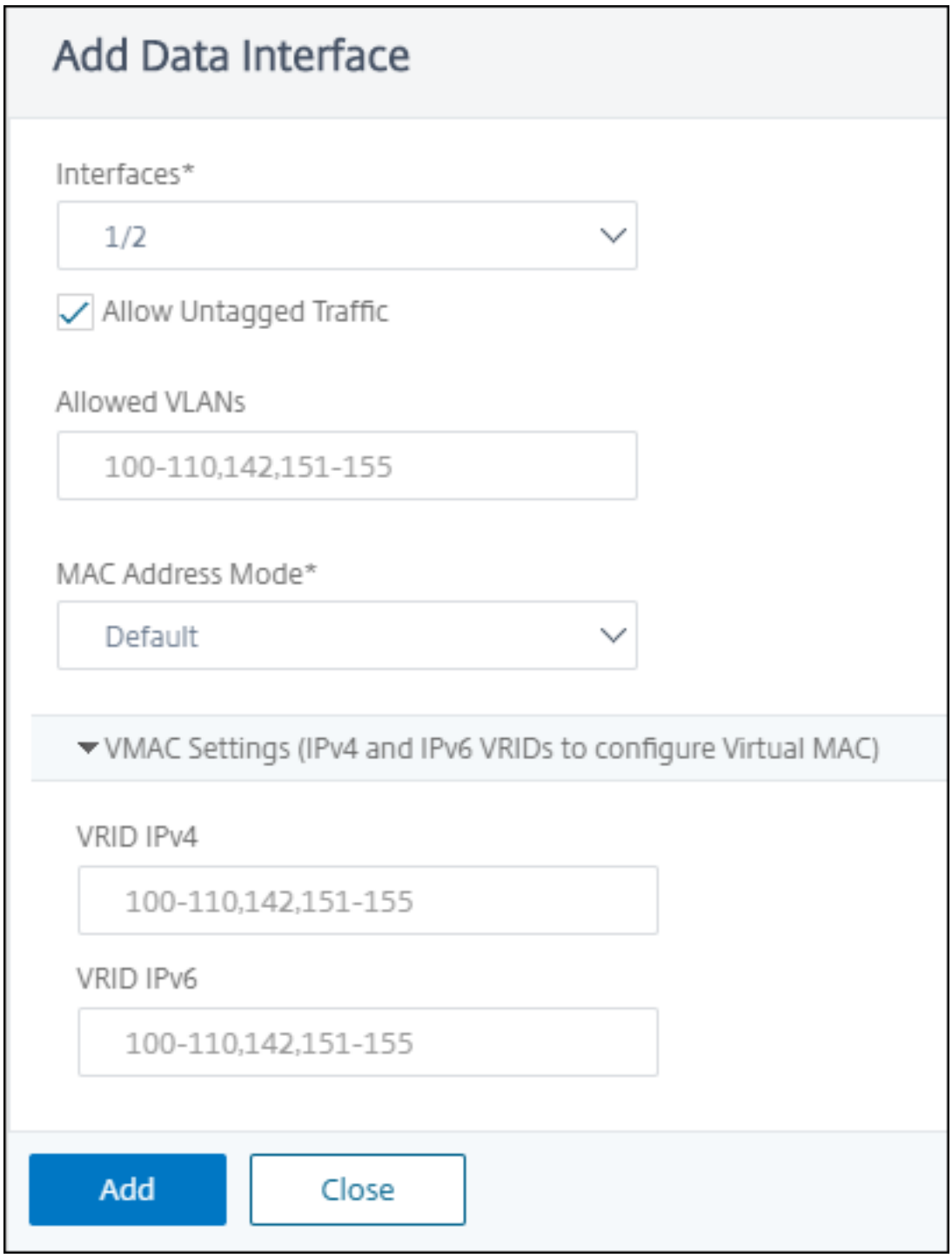


In **Data Interfaces**, click **Add** to add data interfaces and specify the following:

- **Interfaces** - Select the interface from the list.

  > **Note**
  >
  > The interface IDs of interfaces that you add to an instance do not necessarily correspond to the physical interface numbering on the SDX appliance.
  >
  > For example, the first interface that you associate with instance-1 is SDX interface 1/4, it appears as interface 1/1 when you view the interface settings in that instance. This interface indicates it is the first interface that you associated with instance-1.

- **Allowed VLANs** - Specify a list of VLAN IDs that can be associated with a NetScaler instance.
- **MAC Address Mode** - Assign a MAC address to an instance. Select from one of the following options:
  - **Default** - Citrix Workspace assigns a MAC address.
  - **Custom** - Choose this mode to specify a MAC address that overrides the generated MAC address.
  - **Generated** - Generate a MAC address by using the base MAC address set earlier. For information about setting a base MAC address, see Assigning a MAC Address to an Interface.
- **VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)**
  - **VRID IPV4** - The IPv4 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.
  - VRID IPV6 - The IPv6 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.



Click **Add**.

Step 6 - Specify Management VLAN settings

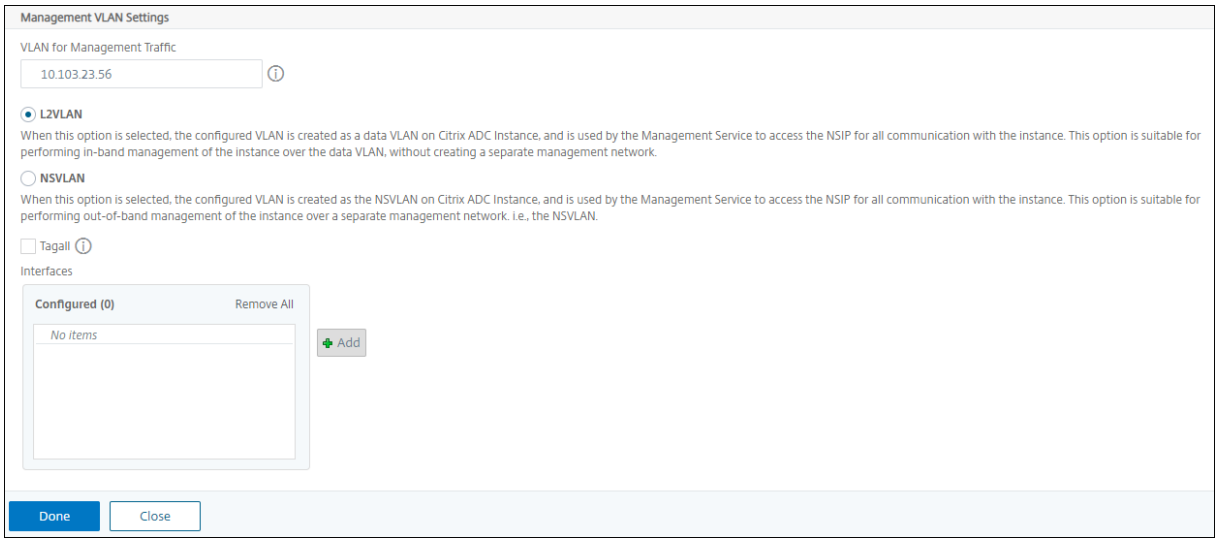
The Management Service and the management address (NSIP) of the VPX instance are in the same subnetwork, and communication is over a management interface.

If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

If your deployment requires the NSIP is accessible only through the selected interface while provisioning the VPX instance, select **NSVLAN**. And, the NSIP becomes inaccessible through other interfaces.

- HA heartbeats are sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from the VPX XVA build `9.3-53.4` and later.

> **Important**
>
> - You cannot change this setting after you provision the VPX instance.
> - The `clear config full` command on the VPX instance deletes the VLAN configuration if **NSVLAN** is not selected.

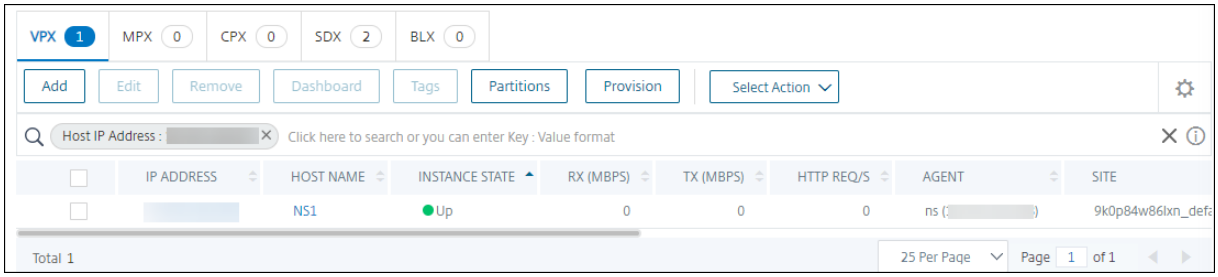


Click **Done** to provision a VPX instance.

View the provisioned VPX instance

To view the newly provisioned instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, search an instance by the **Host IP address** property and specify SDX instance IP to it.



Rediscover multiple NetScaler VPX instances

March 11, 2024

You can rediscover multiple NetScaler VPX instances in your NetScaler Application Delivery Management (ADM) setup. Also, you can rediscover multiple NetScaler VPX instances when you want to view the latest states and configurations of those instances. The NetScaler ADM server rediscovers all the NetScaler VPX instances and checks whether the Citrix Application Delivery Controller (ADC) instances are reachable.

To rediscover multiple NetScaler VPX instances:

1. In a web browser, type the IP address of the NetScaler ADM server (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials. The default administrator credentials are `nsroot` and `nsroot`.
3. Navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab and select the instances you want to rediscover.
4. In the **Select Action** menu, click **Rediscover**.
5. When the confirmation message for running the Rediscover utility appears, Click **Yes**.

   The screen reports the progress of rediscovery of each of the NetScaler VPX instances.

Unmanage an instance

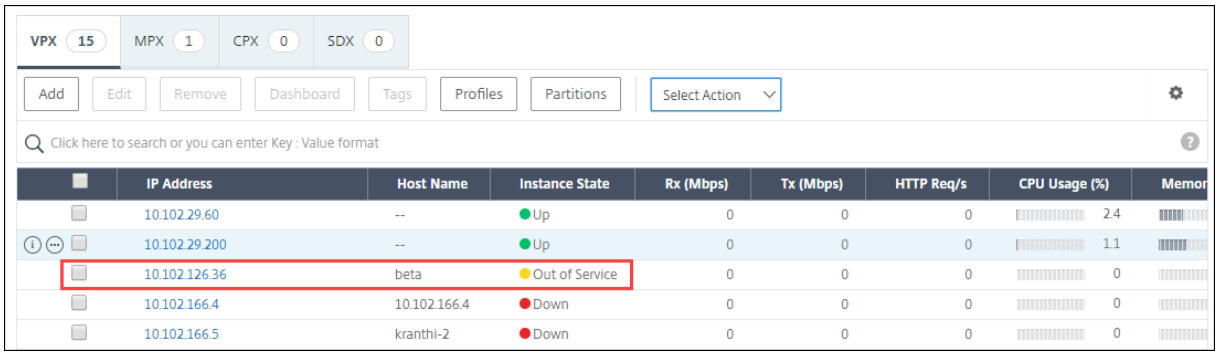
March 11, 2024

If you want to stop the exchange of information between NetScaler Application Delivery Management (ADM) and the instances in your network, you can unmanage the instances.

To unmanage an instance:

Navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab. In the list of instances, either right-click an instance and then select **Unmanage**, or select the instance and from the **Select Action** list, select **Unmanage**.

The status of the selected instance changes to **Out of Service** as shown in the following figure.



The instance is no longer managed by NetScaler ADM, and it no longer exchanges data with NetScaler ADM.

Trace the route to an instance

March 11, 2024

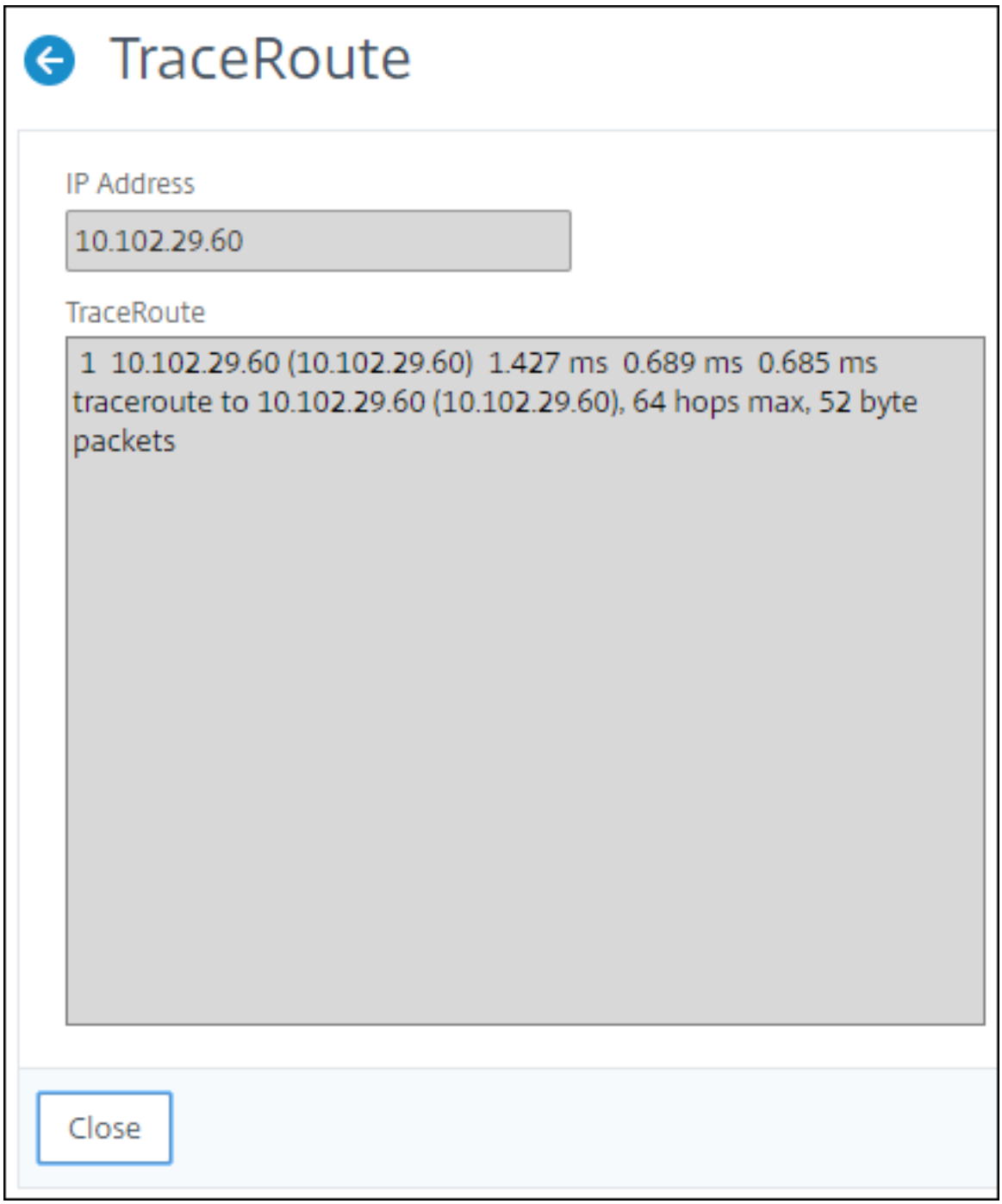
By tracing the route of a packet from the NetScaler Application Delivery Management (ADM) to an instance, you can find information such as the number of hops necessary to reach the instance. Traceroute traces the path of the packet from source to destination. It displays the list of network hops along with the host name and IP address of each entity in the route.

Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, traceroute shows where the problem exists.

To trace the route of an instance:

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. In the list of instances, either right-click an instance and then select **TraceRoute** or select the instance and from the **Select Action** menu, click **TraceRoute**.

The **TraceRoute** message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.



Replicate configurations from one NetScaler instance to another

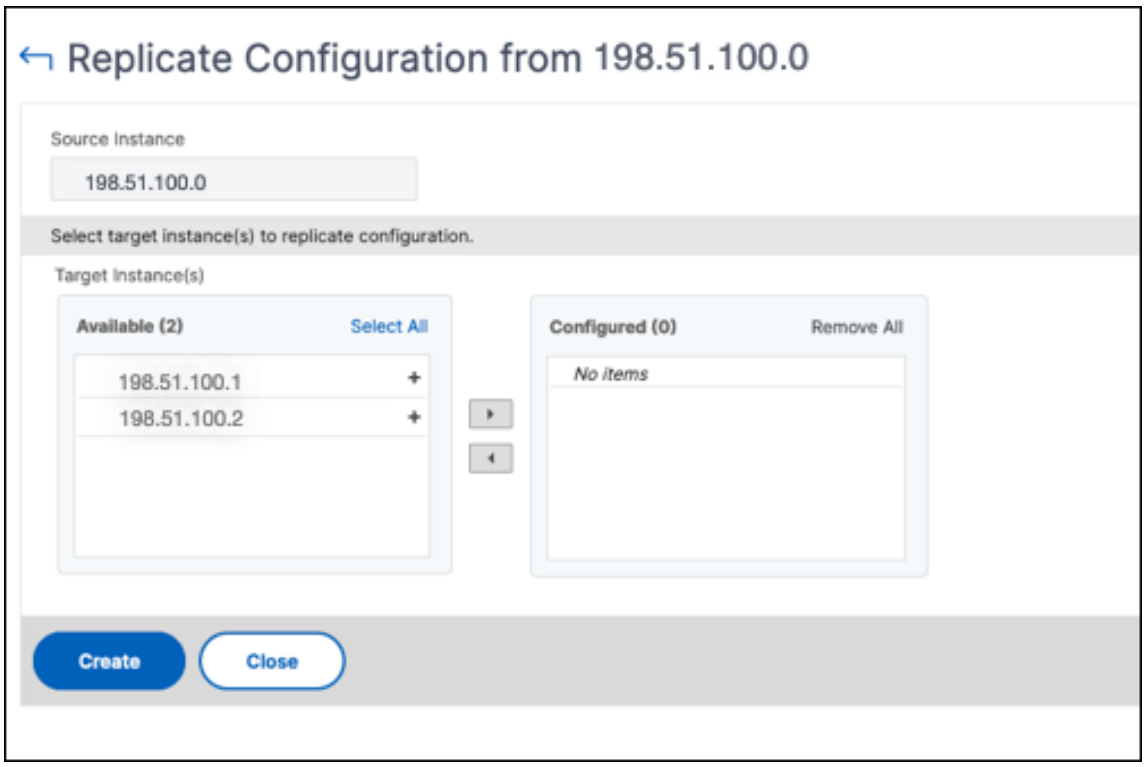
March 11, 2024

You can use the Replicate Configuration feature of NetScaler ADM to copy configurations from a

NetScaler instance and replicate it on a single instance or many instances.

To replicate configurations from one instance to other NetScaler instances

1. Navigate to **Infrastructure > Instances > NetScaler**. Select the source instance whose configurations you want to replicate on other instances and from the **Select Action** list, click **Replicate Configuration**.
2. In **Replicate Configuration**, select the target instance on which you want to apply the configurations from the source instance. You can replicate the configurations from a single source instance to a single instance or many target instances.



3. Click **Create**.

The replicated configurations are added to the list of NetScaler instances. To view the status of the replicated instances, click the refresh icon.

> **Note:**
>
> During replication, all the network IPs from the source instance are replicated to the target instance. If the target instance is in a different network from the source instance, the IPs in the target instance might not be reachable. When IPs are not reachable, the status of the entities in the target instance is shown as Down.

> To view the status of the entities configured on your managed NetScaler instance, navigate to **Infrastructure > Network Functions**.

SSL certificate management

March 11, 2024

Any organization or individual website that requires handling confidential or sensitive information must have an SSL certificate. SSL certificate on a web server helps guarantee the authenticity of the web server to the connecting client. It not only authenticates a website's identity but also helps in generating the session key, which is used later for encryption of the entire session.

A Secure Socket Layer (SSL) certificate, which is a part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the Citrix Application Delivery Controller (ADC) appliance, is used to complete asymmetric key (or public key) encryption and decryption.

NetScaler Application Delivery Management (ADM) provides you a unified console to automate the installation, updating, deletion, linking, and download of SSL certificates. It helps in retaining the reputation of the website and customer trust. NetScaler ADM now streamlines every aspect of certificate management for you. Through a unified console, you can configure automated policies to ensure the recommended issuer, key strength, protocol, and algorithms as per organization IT policies. By doing so, you can keep close watch on certificates that are unused or about to expire.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as Verisign
- By generating a new SSL certificate and key on the NetScaler appliance

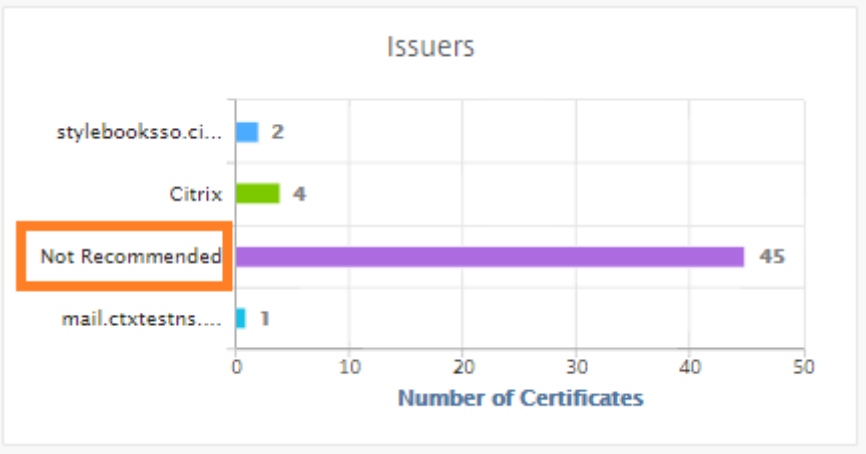
Enterprise SSL policy settings

Every enterprise has its own SSL policy and defines the requirements that all SSL Certificates must adhere to. Security has always been among the top priorities across all enterprise users and hence SSL settings play an important role.

For example, an ABC Company mandates that all certificates must have minimum key strengths of 2,048 bits and above. The certificates must be authorized by trusted CA or issuers. Administrators must check all such SSL parameters to ensure that the certificates abide by the company policy. It is a tedious job to verify each certificate manually. To overcome this scenario, the NetScaler ADM helps

you to configure enterprise SSL policy settings, and shows any non-compliance certificate with the "Not Recommended"tag.

You can view the summary of the non-compliance (Not Recommended) certificates on the SSL Dashboard.

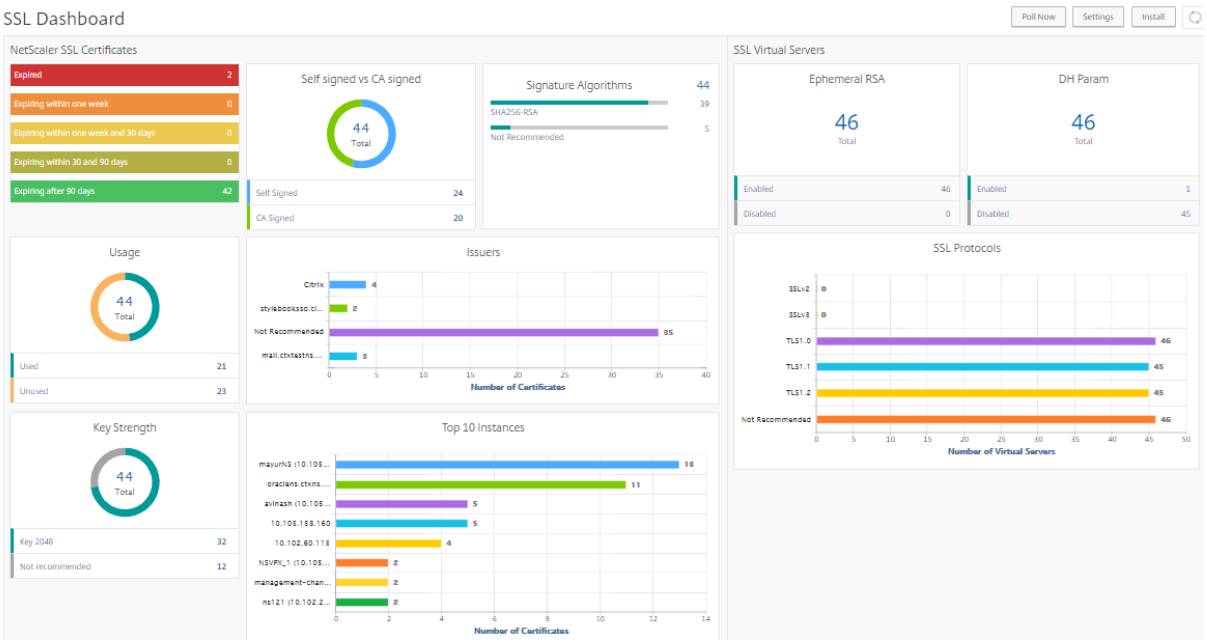


> **Note**
>
> The "Not Recommended"certificates are categorized based on different parameters, and you can view them in relevant components.

How the NetScaler ADM certificate works

SSL Dashboard provides you a visual presentation of all the SSL certificates that are installed on different NetScaler instances. SSL dashboard includes the following information for each certificate installed on NetScaler instances. It is categorized based on the following:

- **Self-signed vs CA signed.** The self-signed vs CA signed section helps you to segregate the certificates into Self-signed certificates and, CA signed certificates.
- **Signature Algorithms.** This section segregates the SSL certificates based on signature algorithms being used for encryption.
- **Usage.** This section segregates your SSL certificates based on used and unused certificates. Unused certificates demand special attention as they might have been missed to be bound to the virtual servers.
- **Issuers.** This section segregates the SSL certificates based on the issuer of the certificates.
- **Key Strength.** This section segregates the SSL certificates based on the key strength of a private key.
- **Top 10 Instances.** This section provides the details of the top 10 NetScaler instances based on the number of SSL certificates installed.



SSL certificate management use cases

The following use cases describe how you can use the SSL certificate to manage and monitor the certificates across multiple NetScaler instances.

Install SSL certificates

Imagine, you have a fleet of NetScaler instances across, on which you have to deploy the required SSL certificates. NetScaler ADM provides you a unified console to deploy the SSL certificates across multiple NetScaler instances in one attempt.

For example, you might want to install some SSL certificates on one or more NetScaler instances. With this approach, you can minimize the manual intervention of installing the SSL certificate on each NetScaler instance. You can do a bulk installation of SSL certificates across one or more NetScaler instances.

To obtain a summary of the SSL certificates, log on to **NetScaler ADM**, and then navigate to **Infrastructure > SSL Dashboard**.

Notification settings for certificate expiry

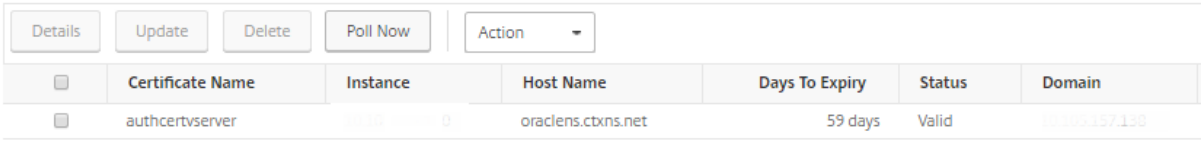
In this use case, you might have many certificates across multiple NetScaler instances, and it becomes an overhead to track the expiry of each certificate. It is a tedious job for you to track each certificate manually and update it before it expires. To avoid such scenarios, you can configure NetScaler ADM to

send the notifications or alerts to the configured email, pager, Slack, or ServiceNow profiles. This way you can stay abreast of the certificates expiry dates and renew the certificates well before the expiry dates.

For example, you might forget to track the certificate that is nearing expiry. And the certificate expires causing service outage, which might affect numerous applications to the users. With ADM certificate expiry notification settings, you can avoid such unforeseen scenarios.

You can view the summary and track the certificates that are nearing expiry on the **SSL Dashboard**.

To view the report of certificates expiring in any duration, you can click the tile to get the details of all such certificates expiring in that window.



Renewal of certificates

You can now renew the certificates from NetScaler ADM. You can either renew the existing certificates or create the certificates based on the following:

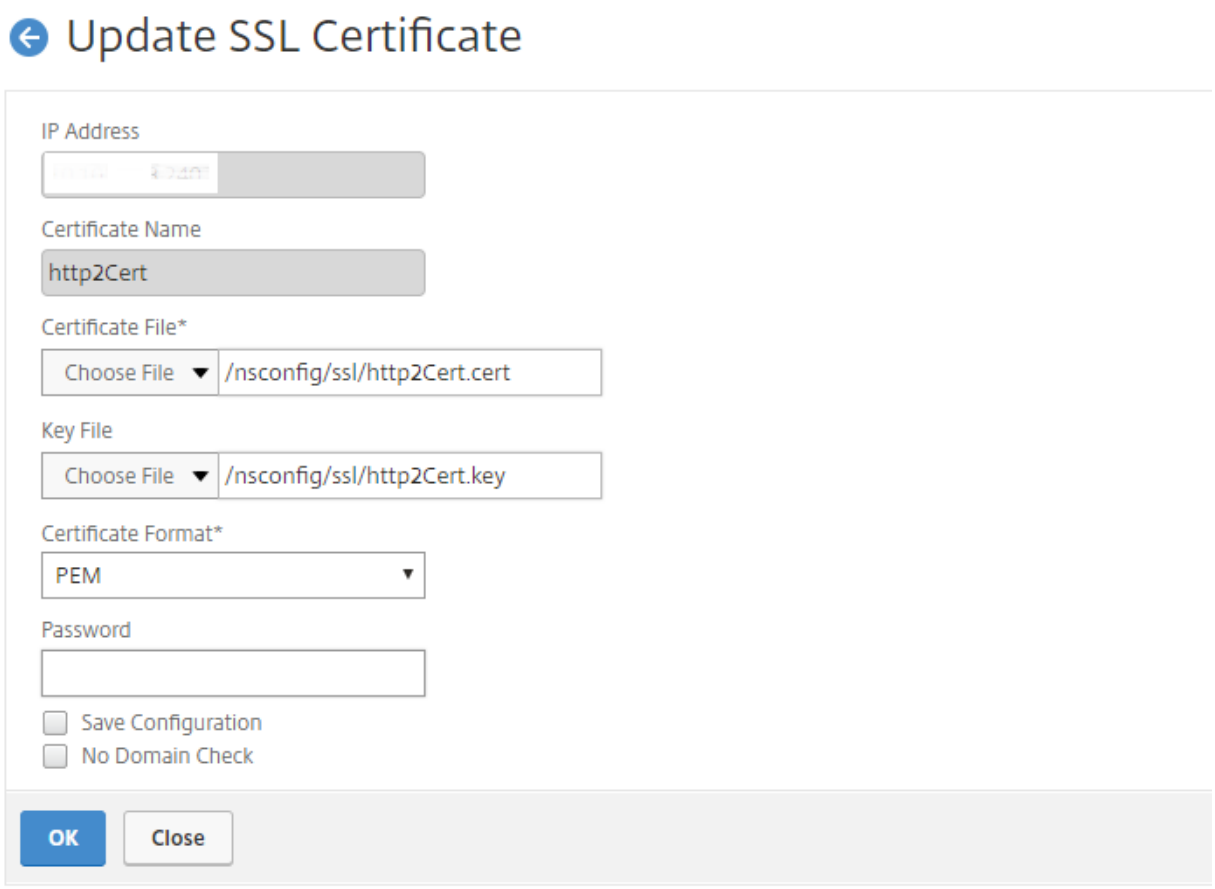
Update the existing certificate In this use case, you have to update an existing certificate once you receive a renewed certificate from the certificate authority (CA). You can now update the existing certificates from NetScaler ADM without logging into NetScaler instances.

For example, there might be some changes or modifications to the existing certificates. The CA issues renewed certificates. Instead of going to the NetScaler appliance, you can now update the SSL certificate from NetScaler ADM.

To update any certificate, log on to NetScaler ADM, then navigate to **Infrastructure > SSL Dashboard**.

Select the certificate you want to update, and click **Update**.

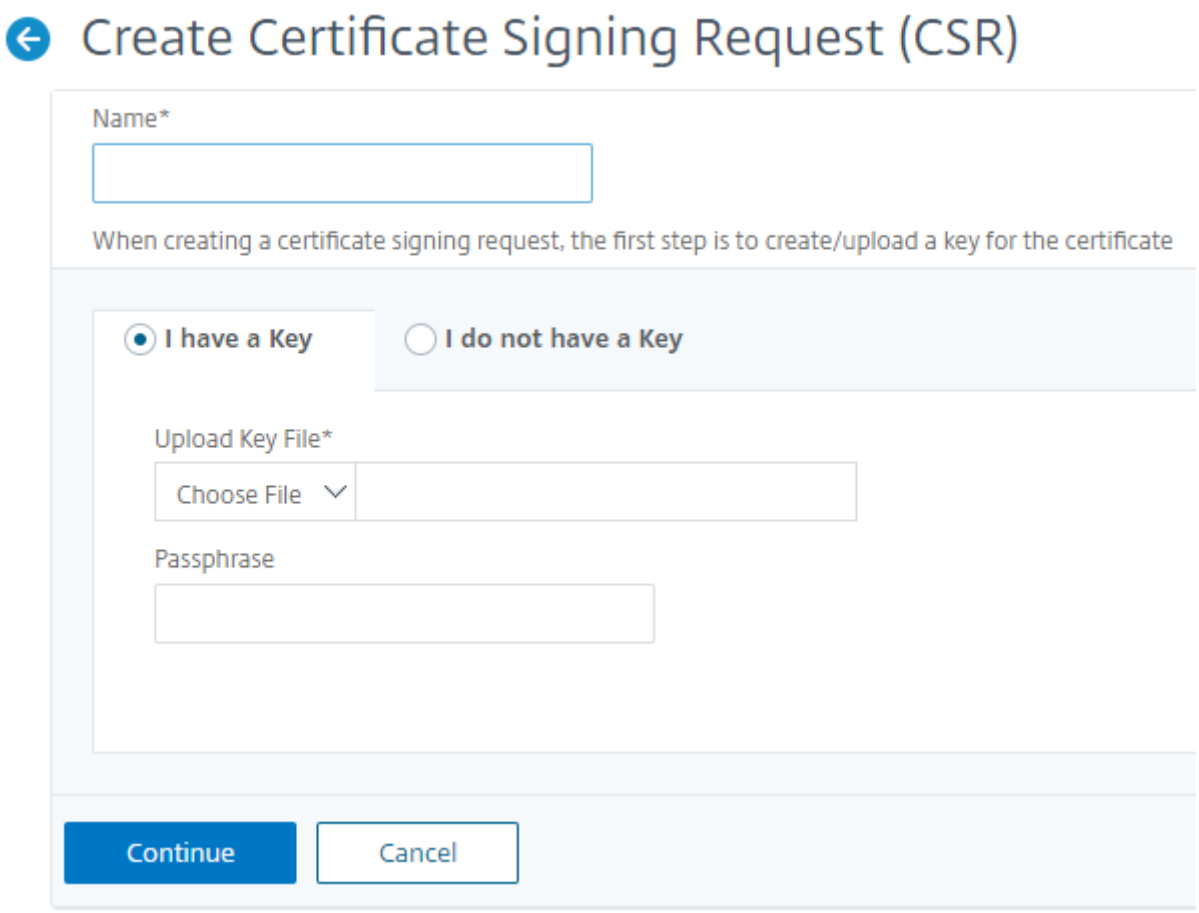
You have an option to update the relevant fields of the selected certificate from NetScaler ADM.



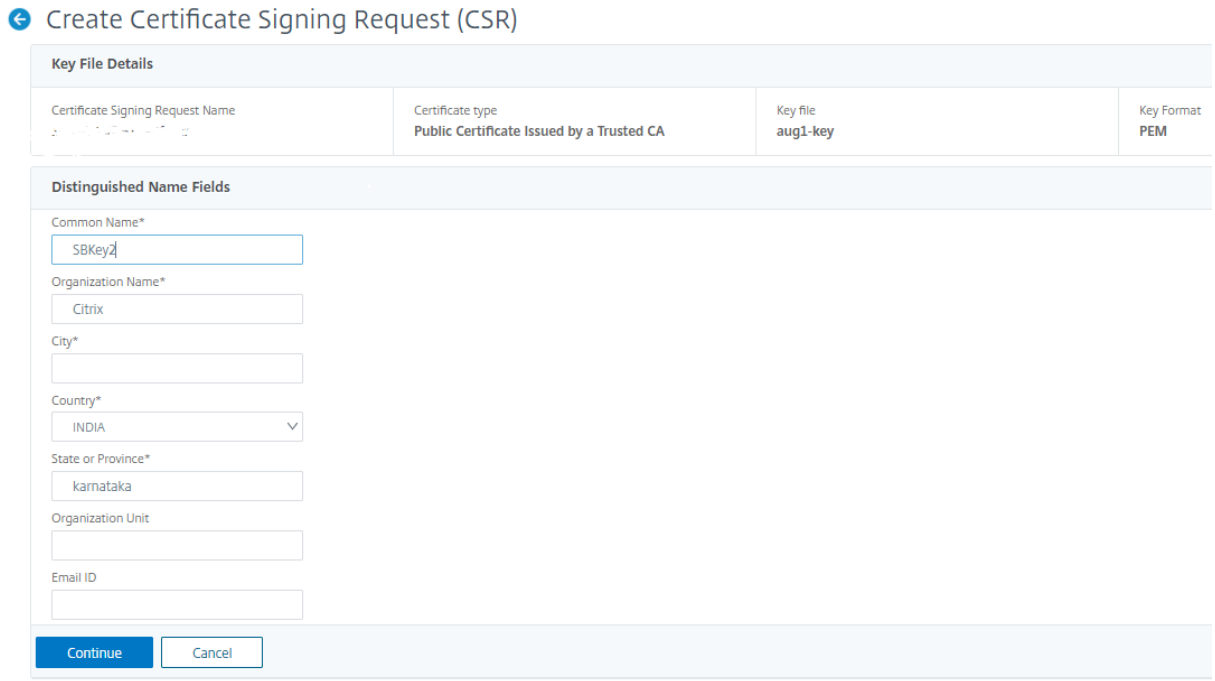
Create certificate signing request Imagine a use case where one of the SSL certificates does not comply with the organization policies. You want to get a new certificate from the certification authority. You can now generate a certificate signing request (CSR) from NetScaler ADM. A CSR and a public key can be sent to a CA to obtain the SSL certificate.

To determine and create CSR, select the desired certificate and click **Create CSR**.

You need to have a public or private key value pair. To upload a key, click **Choose File** and select from the list. To create a key, select **I do not have a Key option** and specify the relevant parameters.

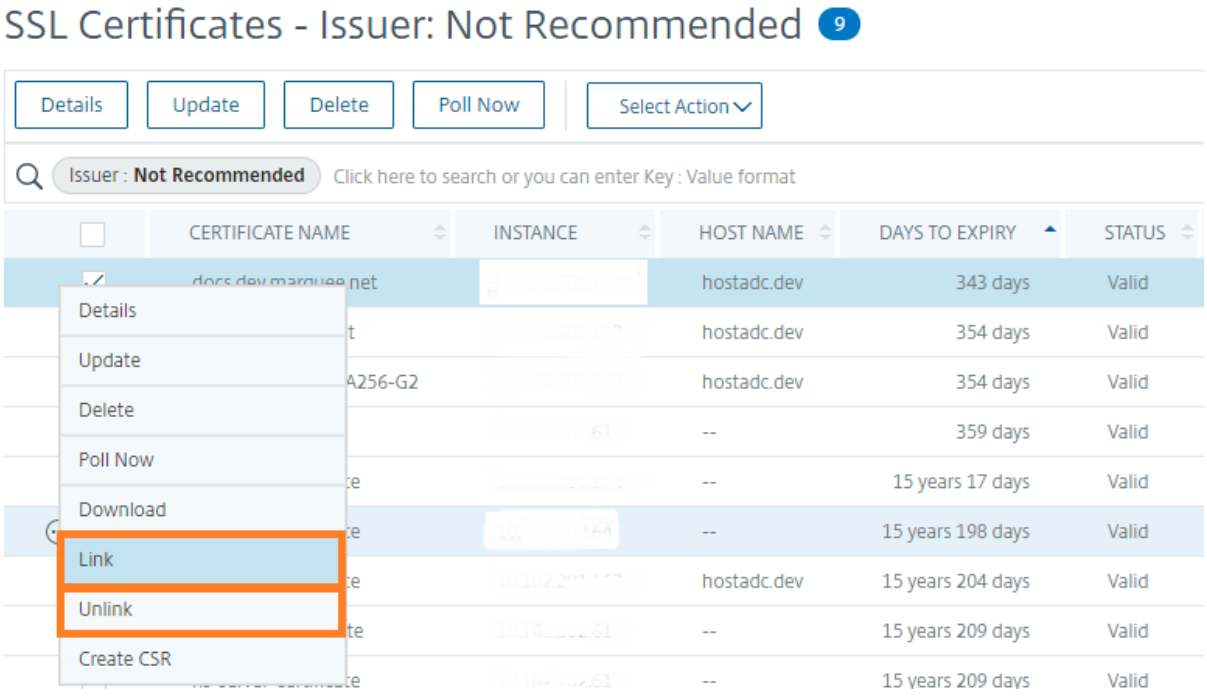


To give more details of the selected key like Common Name, Org Name, City, Country, State, Org Unit, and Email ID to create the CSR.



Link and unlink SSL certificates

You can bind multiple SSL certificates to each other to create a certificate bundle. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate.

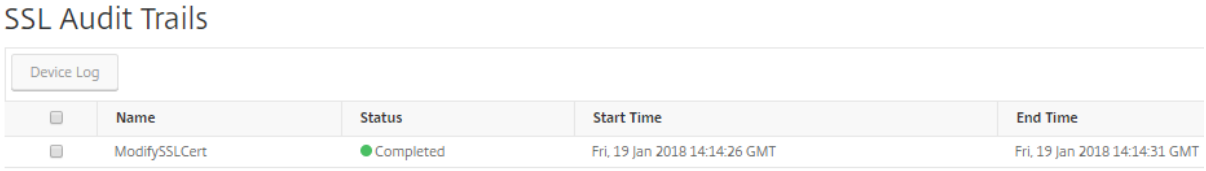


Audit logs

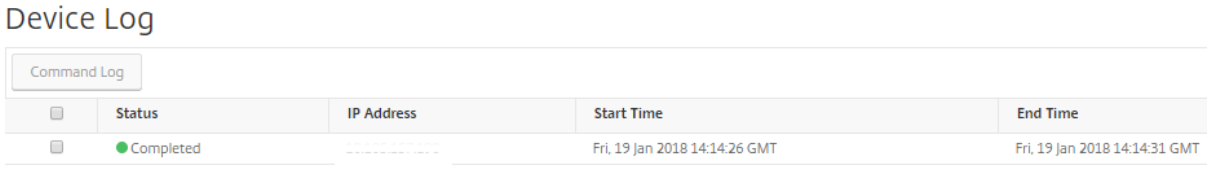
Audit Logs is a collection of text log files generated by the NetScaler ADM. It shows a history of SSL certificates that are added, modified, and changed by using NetScaler ADM to the specific NetScaler appliance. The Audit Logs also shows the IP Address of the NetScaler appliance, Status, Start Time, and End Time of the particular operation.

In this example, you might want to verify the change that has taken place over a period to the particular certificate. And you have an option to view the history of changes to the certificate over the Device Log and Command Log.

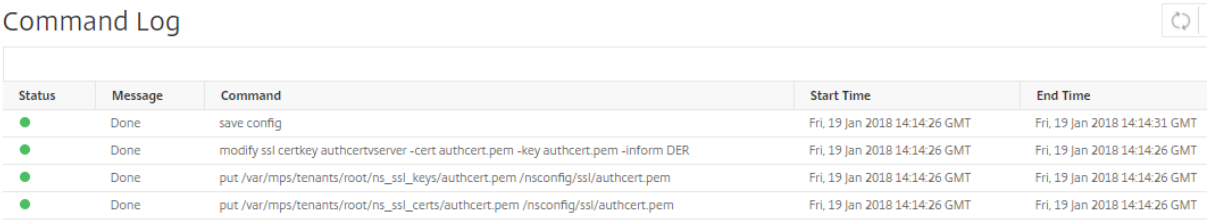
To determine the information of SSL certificates, on the **SSL Dashboard**, click **Audit Log**. The application summary includes the SSL certificates status with Start Time and End Time.



To determine the information of the NetScaler appliance of a particular SSL certificate, choose the relevant certificate check box of your choice. Click **Device Log**.



To view the information of command type, and message, click **Command Log**.



Use the SSL Dashboard

March 11, 2024

You can use the SSL certificate dashboard in NetScaler Application Delivery Management (ADM) to view graphs that help you track certificate issuers, key strengths, and signature algorithms. The SSL certificate dashboard also displays graphs that indicate the following:

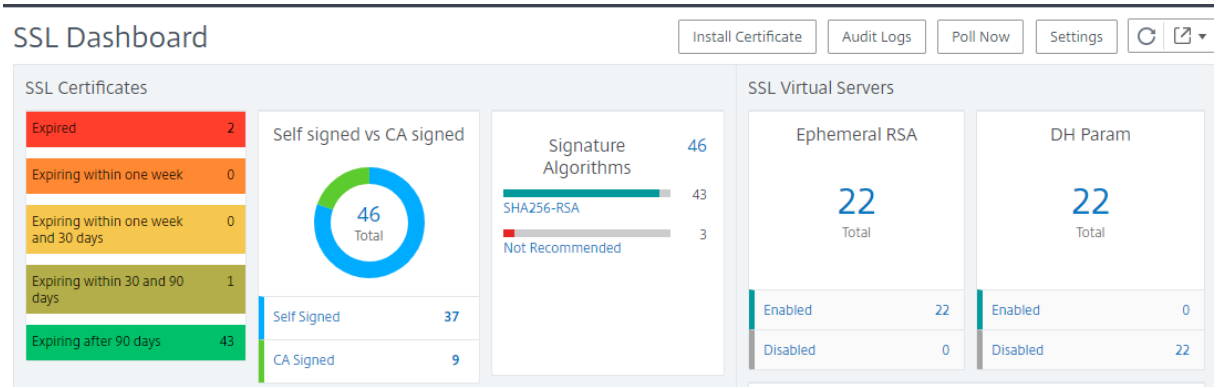
- Number of days after which certificates expire
- Number of used and unused certificates
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

To monitor SSL certificates

You might use the SSL dashboard on NetScaler ADM to monitor your certificates if your company has SSL Policy where you have defined certain SSL certificate requirements such as all certificates must have minimum key strengths of 2048 bits and a trusted CA authority must authorize it.

In another example, you might have uploaded a new certificate but forgotten to bind it to a virtual server. The SSL dashboard highlights the SSL certificates being used or not used. In the **Usage** section, you can see the number of certificates that have been installed, and the number of certificates being used. You can further click the graph, to see the certificates name, the instance on which it's being used, its validity, its signature algorithm, and so on.

To monitor SSL certificates in NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.



NetScaler ADM allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to NetScaler ADM. To do so,

1. Navigate to **Infrasturcture > SSL Dashboard**.
2. Click **Poll Now**.

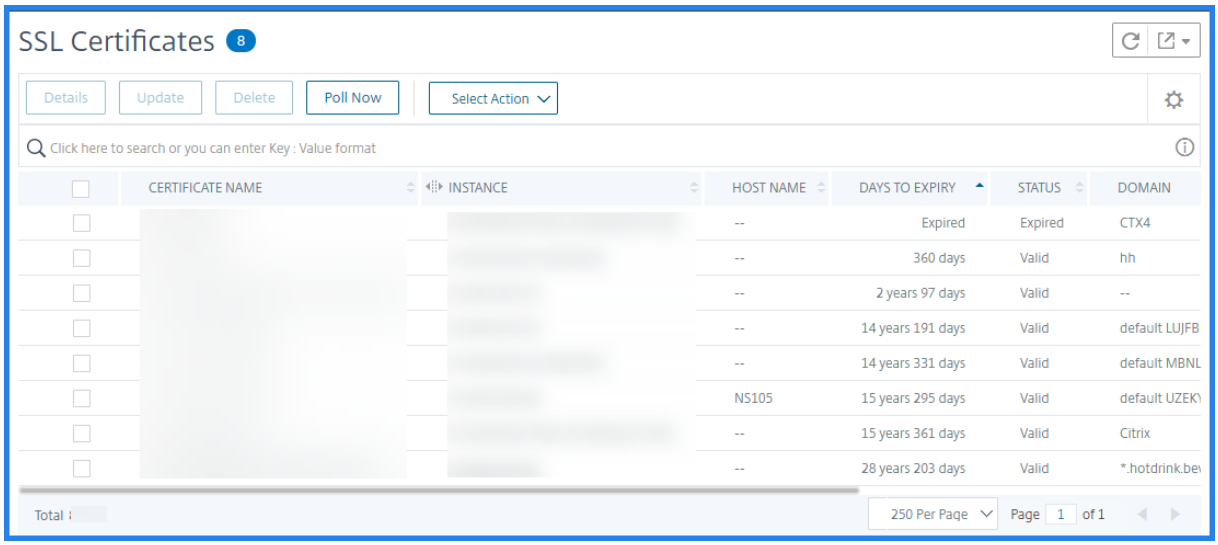
   On the **Poll Now** page, you can either poll all managed ADC instances or select specific instances.

3. Click **Start Polling**.

In **SSL Dashboard**, you can monitor the ADC SSL certificates, SSL virtual servers, and SSL protocols.

You can click the metrics on the dashboard to view details related to SSL certificates, SSL Virtual Servers, or SSL protocols.

For example, when you click the number under **Self signed vs CA signed** on the dashboard, the ADM GUI displays all the SSL certificates on the NetScaler instances.



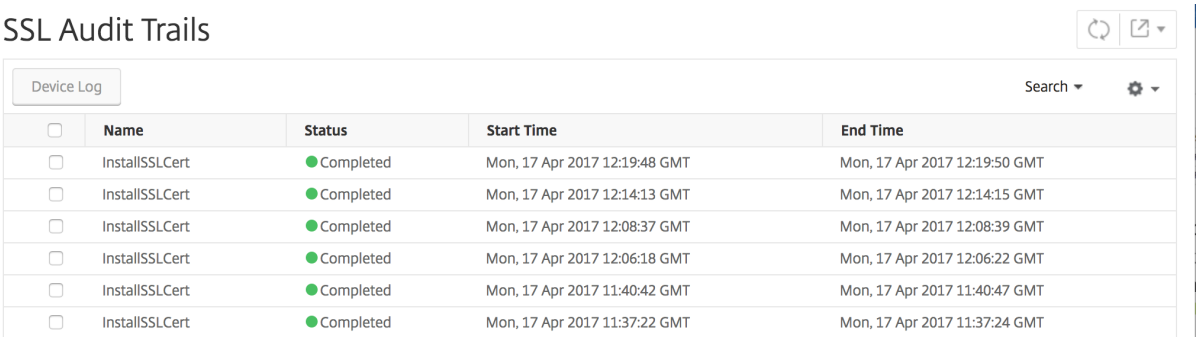
The NetScaler ADM SSL Dashboard also shows the distribution of SSL protocols that are running on your virtual servers. As an administrator, you can specify the protocols that you want to monitor through the SSL policy, for more information, see Configuring SSL Policies. The protocols supported are SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. The SSL protocols used on virtual servers appear in a bar chart format. Clicking a specific protocol displays a list of virtual servers using that protocol.

A donut chart appears after Diffie-Hellman (DH) or Ephemeral RSA keys are enabled or disabled on the SSL dashboard. These keys enable secure communication with export clients even if the server certificate does not support export clients, as in the case of a 1024-bit certificate. Clicking the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.

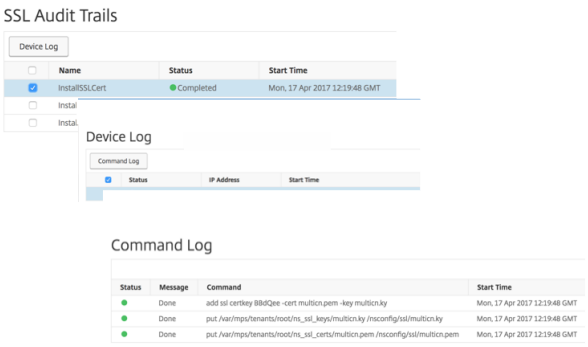
To view audit trails for SSL certificates

You can now view log details of SSL certificates on NetScaler ADM. The log details display operations performed using SSL certificates on NetScaler ADM such as: installing SSL certificates, linking and unlinking SSL certificates, updating SSL certificates, and deleting SSL certificates. Audit trail information is useful while monitoring SSL certificate changes done on an application with multiple owners.

To view an audit log for a particular operation performed on NetScaler ADM using SSL certificates, navigate to **Infrastructure > SSL Dashboard** > and click **Audit Logs**.



For a particular operation performed using SSL certificate you can view its status, start time, and end time. Furthermore, you can view the instance on which the operation was performed and the commands run on that instance.

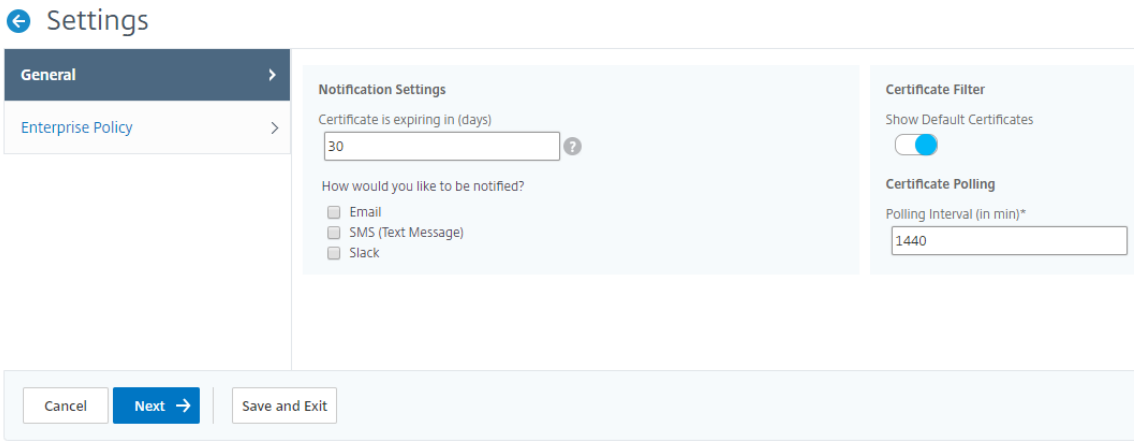


To exclude default NetScaler certificates on the SSL Dashboard

NetScaler ADM allows you to show or hide default NetScaler certificates showing up on the SSL Dashboard charts based on your preferences. By default, all certificates are displayed on the SSL dashboard including default certificates.

To show or hide default certificates on the SSL dashboard:

1. Navigate to **Infrastructure > SSL Dashboard** in the NetScaler ADM GUI.
2. On **SSL Dashboard** page, click **Settings**.
3. On the **Settings** page, select **General**.
4. Type the number of days when the certificate expires to receive notification about certificate expiry.
5. Select the method of notification and create the respective profiles.
6. In the **Certificate Filter** section, clear the **Show Default Certificates** check box and click **Save and Exit**.



View, upload, and download SSL files

To view SSL files on NetScaler ADM, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler ADM**.

In this page, you can view, upload, and download the following files on NetScaler ADM:

- SSL certificates
- SSL keys
- SSL CSRs

To view and download SSL files on a NetScaler instance, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler**.

You can access the SSL files only after the NetScaler instances have been backed up, either manually or through a scheduled backup process.

> **Important:**
>
> To enable the SSL files download from ADC instances, enable the **Instance SSL certificates** feature. For more information, see Enable or disable ADM features.

Set up notifications for SSL certificate expiry

March 11, 2024

As a security administrator, you can set up notifications to inform you when certificates are about to expire and to include information about which Citrix Application Delivery Controller (ADC) instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

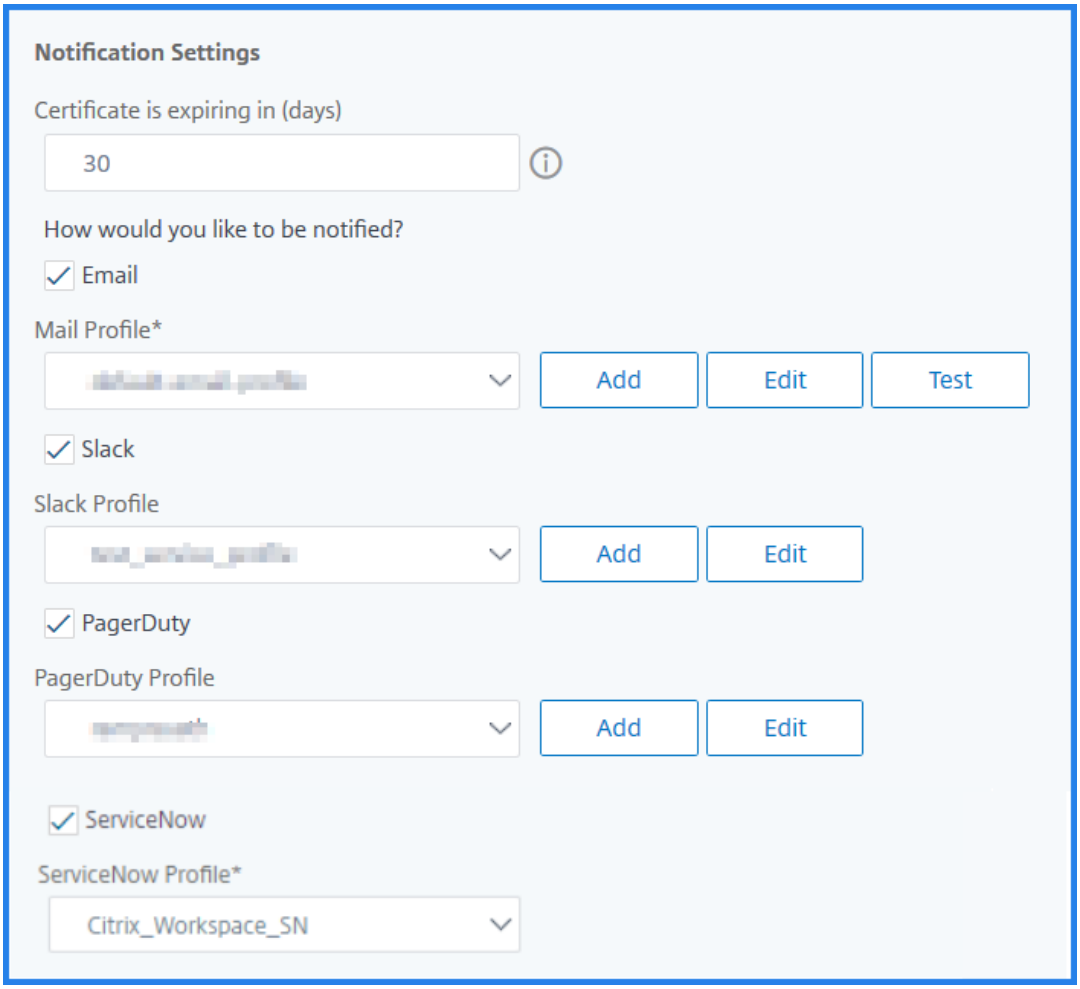
For example, you can set an email notification to be sent an email distribution list 30 days before your certificate is due to expire.

To set up notifications from NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. On the **SSL Dashboard** page, click **Settings**.
3. On the **SSL Settings** page, click the **Edit** icon .
4. In the **Notification Settings** section, specify when you want to send the notification in terms of number of days prior to the expiration date.
5. Choose the type of notification you want to send. Select the notification type and the distribution list from the drop-down menu. The notification types are as follows:

    - **Email** –Specify a mail server and profile details. An email is triggered when your certificates are about to expire.
    - **SMS** –Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your certificates are about to expire.
    - **Slack** - Specify Slack profile details.
    - **PagerDuty alerts** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
    - **ServiceNow** - A notification is sent to the default ServiceNow profile when your certificates are about to expire.

      > **Important**
      >
      > Ensure Citrix Cloud ITSM Adapter is configured for ServiceNow and integrated with NetScaler ADM. For more information, see Integrate NetScaler ADM with ServiceNow instance.



6. Click **Save and Exit**.

NetScaler ADM now sends SSL certificate expiry trap to external trap destination server when your SSL certificates are due for expiry. NetScaler ADM sends a trap when the following two conditions are satisfied:

- You have configured the number of days for the certificate expire in SSL dashboard settings page.
- You have added the trap destination.

You can set trap destinations by navigating to **Settings > SNMP > Trap Destinations**. Type the IP address of the destination SNMP server where the traps are sent. Enter the port number and type "public"(without quotes) as the community string.

Update an installed certificate

March 11, 2024

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from NetScaler Application Delivery Management (ADM) without needing to log on to individual Citrix Application Delivery Controller (ADC) instances.

To update an SSL certificate, key, or both from NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. On the **SSL Certificates** page, select a certificate and click **Update**. Alternatively, click the SSL certificate to view its details, and then click **Update** in the upper-right corner of the **SSL Certificate** page.
4. On the **Update SSL Certificate** page, make the required modifications to the certificate, key, or both and click **OK**.

Install SSL certificates on a NetScaler instance

March 11, 2024

Before installing SSL certificates on Citrix Application Delivery Controller (ADC) instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed with secure signature algorithms.

To install an SSL certificate from another NetScaler Instance:

You can also import a certificate from a chosen NetScaler instance and apply it to other targeted NetScaler instances from the NetScaler Application Delivery Management (ADM) GUI.

1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the SSL dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:

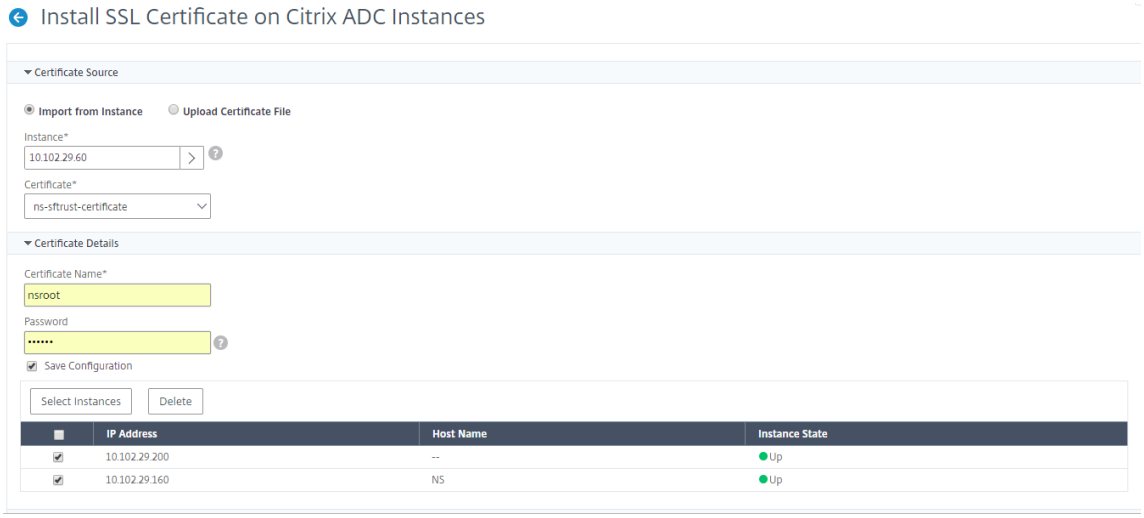
    a) Certificate Source
    Select the option to **Import from Instance**.

    - Choose the **Instance** that you want to import the certificate from.
    - Choose the **Certificate** from the list of all SSL certificate files on the instance.

b) Certificate Details

- **Certificate Name**. Specify a name for the certificate key.
- **Password**. Password to encrypt the private key. You can use this option to upload encrypted private keys.

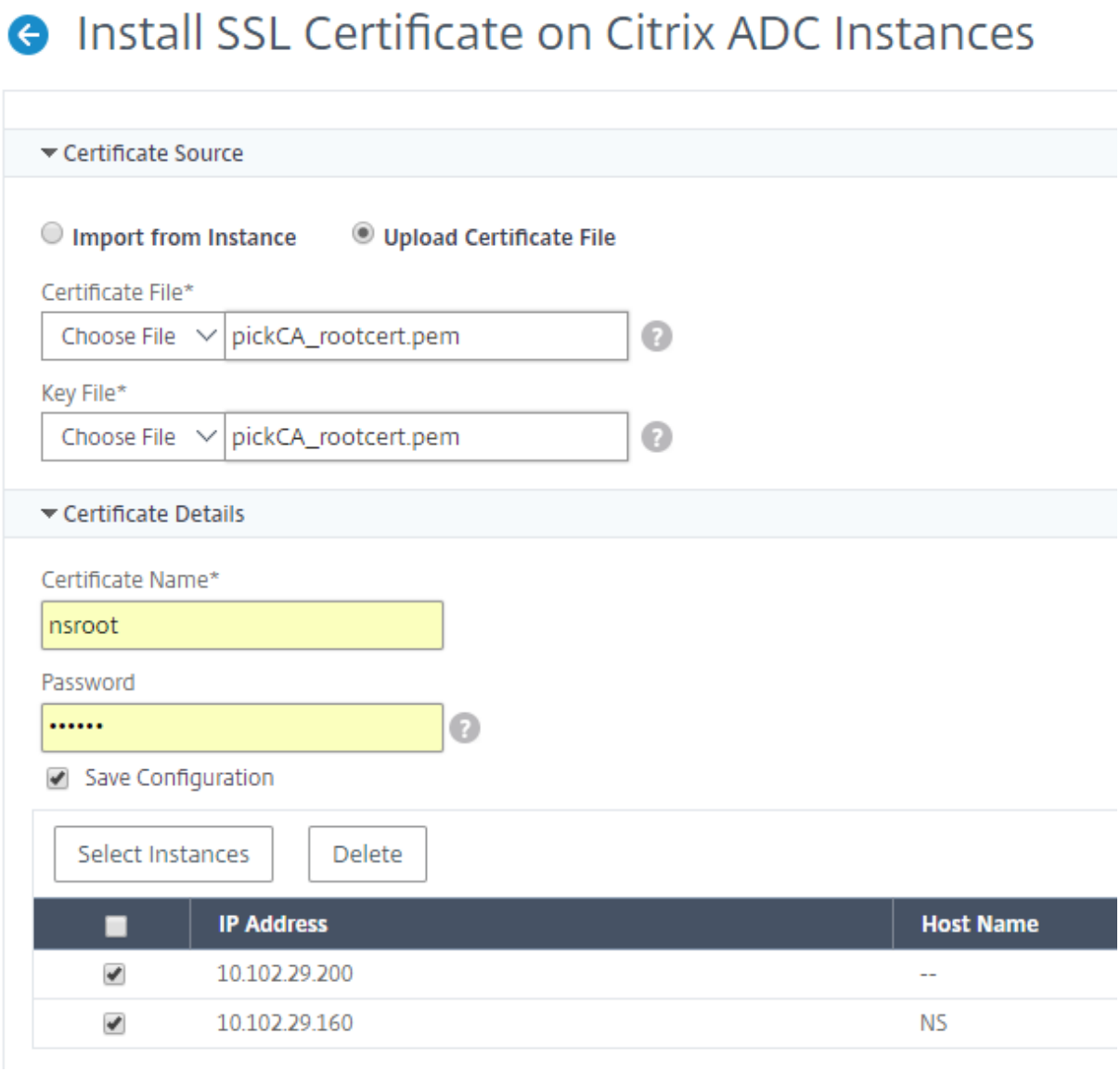
4. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.
5. Click **OK**.



To install an SSL certificate from NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instance** page, select **Upload Certificates File** and specify the following parameters:
   - **Certificate File** - Upload an SSL certificate file by selecting either **Local** (your local machine) or **Appliance** (the certificate file must be present on the NetScaler ADM virtual instance).
   - **Key File** - Upload the key file.
   - **Certificate Name** –Specify a name for the certificate key.
   - **Password** - Password to encrypt the private key. You can use this option to upload encrypted private keys.
   - **Select Instances** - Select the NetScaler ADM instances on which you want to install your certificates.
4. To save the configuration for future use, select the **Save Configuration** check box.

5. Click **OK**.



Create a Certificate Signing Request (CSR)

March 11, 2024

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate will be used. It contains information that will be included in the certificate such as the name of your organization, common name (domain name), locality, and country.

To create a CSR using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select **Create CSR** from the **Select Action** list.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:
   - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the NetScaler ADM virtual instance).
   - **Create a key** - Select the I do not have a Key option, and then specify the following parameters:

Encryption Algorithm	Type of key. For example, RSA.
Key File Name	Name for your file in which the RSA key is stored.
Key Size	Key size in bits.
Public Exponent Value	Choose either **3** or **F4** from the drop-down list provided. This value is part of the cipher algorithm that is required to create your RSA key.
Key Format	Be default PEM is selected. PEM is the recommended key format for your SSL certificate.
PEM Encoding Algorithm	In the drop-down list, select the algorithm (**DES** or **DES3**) that you want to use to encrypt the generated RSA key. If you select this algorithm, you'll need to provide a PEM Passphrase.
PEM Passphrase	If you've chosen the PEM Encoding Algorithm, enter a passphrase.
Confirm PEM Passphrase	Confirm your PEM passphrase.

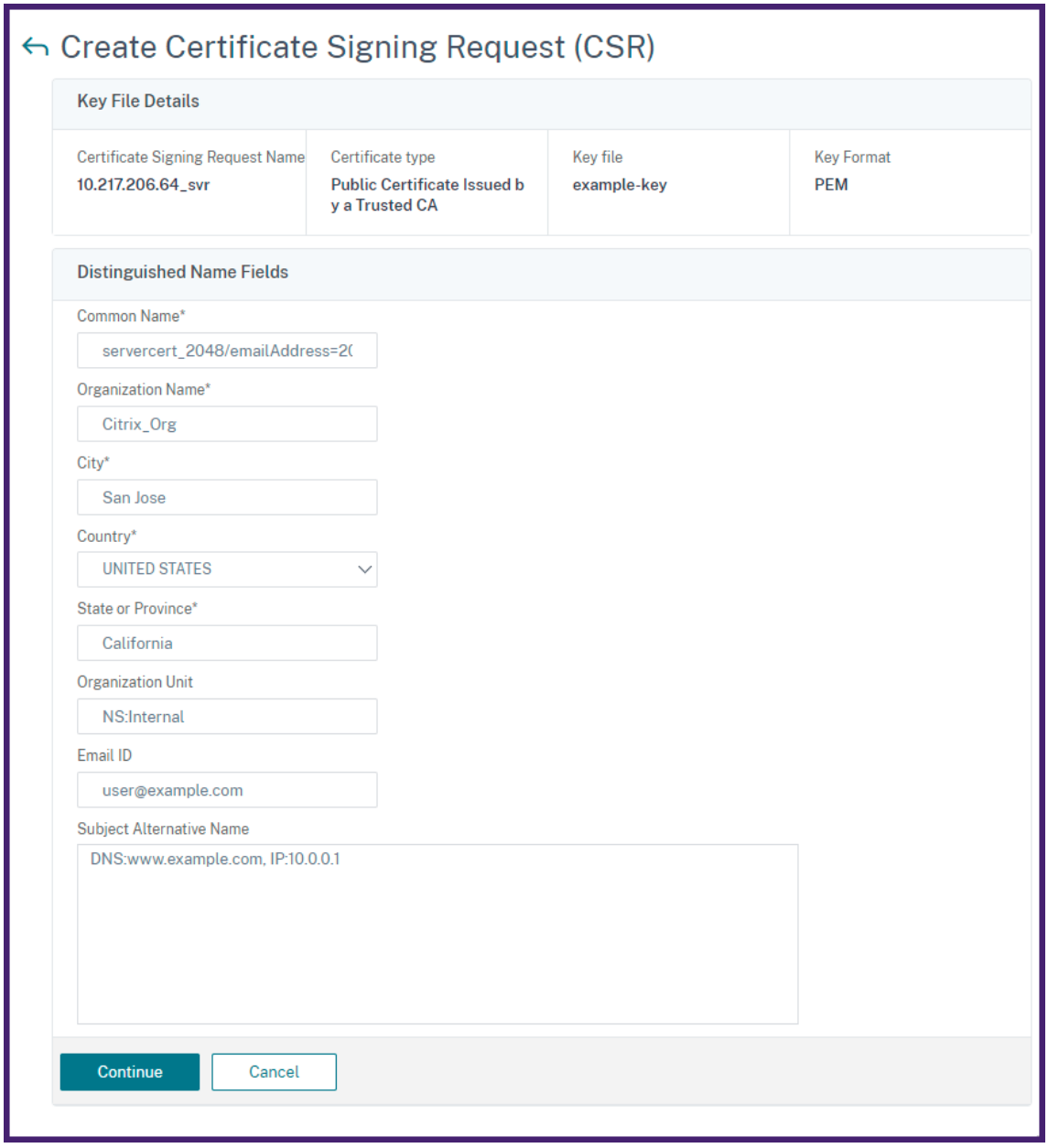
5. Click **Continue**.
6. On the following page, provide more details.

   Most fields have default values extracted from the subject of the selected certificate. The subject contains details such as the common name, organization name, state, and country.

In the **Subject Alternative Name** field, you can specify multiple values, such as domain names and IP addresses with a single certificate. The Subject Alternative names help you secure multiple domains with a single certificate.

Specify the domain names and IP addresses in the following format:

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```



In this example, it secures `10.0.0.1` and `www.example.com`.

Review the fields and click **Continue**.

> **Note**
>
> Most CAs accept certificate submissions by email. The CA returns a valid certificate to the email address from which you submit the CSR.

Link and unlink SSL certificates

March 11, 2024

You create a certificate bundle by linking multiple certificates together. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate. For example, if you want to link certificate A to certificate B, the "issuer" of certificate A must match the "domain" of certificate B.

To link one SSL certificate to another certificate using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select **Link** from the **Action** drop-down list.
4. From the list of matched certificates, select the certificate to which you want to link, and then click **OK**.

> **Note**
>
> If a matching certificate is not found, the following message is displayed: No certificate found to link.

To unlink an SSL certificate using NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select **Unlink** from the **Action** drop-down list.
4. Click **OK**.

> **Note**
>
> If the selected certificate is not linked to another certificate, the following message is displayed:

> Certificate does not have any CA link.

Configure an enterprise policy

March 11, 2024

You can configure an enterprise policy and add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificate keys in NetScaler Application Delivery Management (ADM). If any of the certificates installed on your Citrix Application Delivery Controller (ADC) instance have not been added to the enterprise policy, the SSL certificate dashboard displays the issuer of those certificates as **Not Recommended**.

Also, if the certificate key strength does not match the recommended key strength in the enterprise policy, the SSL certificate dashboard displays the strengths of those keys as **Not Recommended**.

To configure an enterprise policy on NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure** > **SSL Dashboard**, and then click **Settings**.
2. On the SSL Settings page, click the **Edit** icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys.
3. Click **Save** to save your enterprise policy.

> **Note**
>
> The SSL dashboard displays only the **Signature Algorithms** that are selected through the **Settings** option and others are displayed as **Not Recommended**.

Poll SSL certificates from NetScaler instances

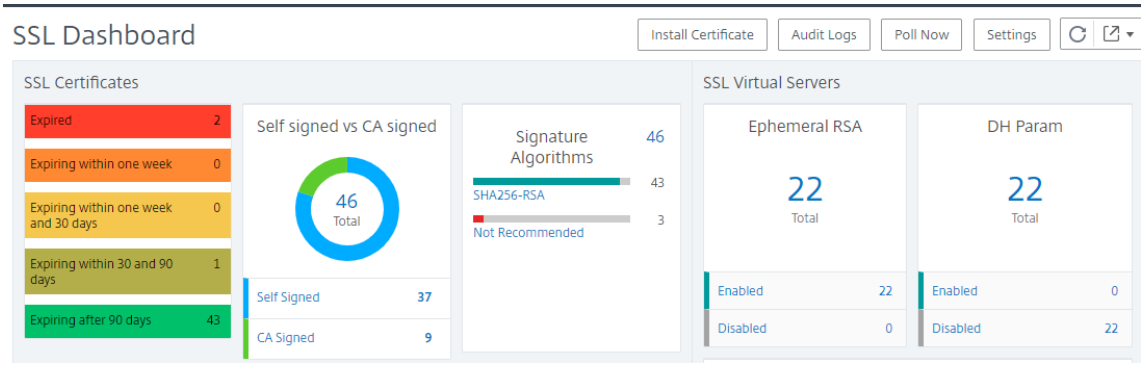
March 11, 2024

NetScaler Application Delivery Management (ADM) automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix Application Delivery Controller (ADC) instances. Polling all the NetScaler instances SSL certificates places a heavy load on the network.

Instead of polling all the NetScaler instances SSL certificates, you can manually poll only the SSL certificates of a selected instance or instances.

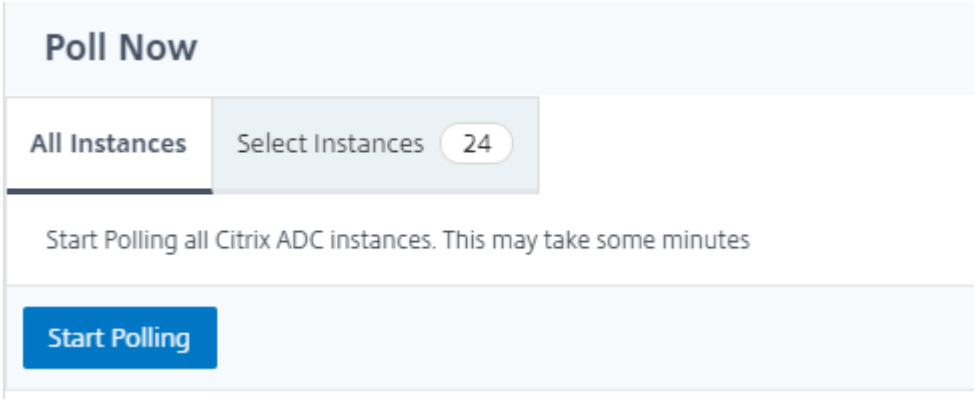
To poll SSL certificates on NetScaler instances:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. On **SSL Dashboard** page, in the top right-hand corner, click **Poll Now**.

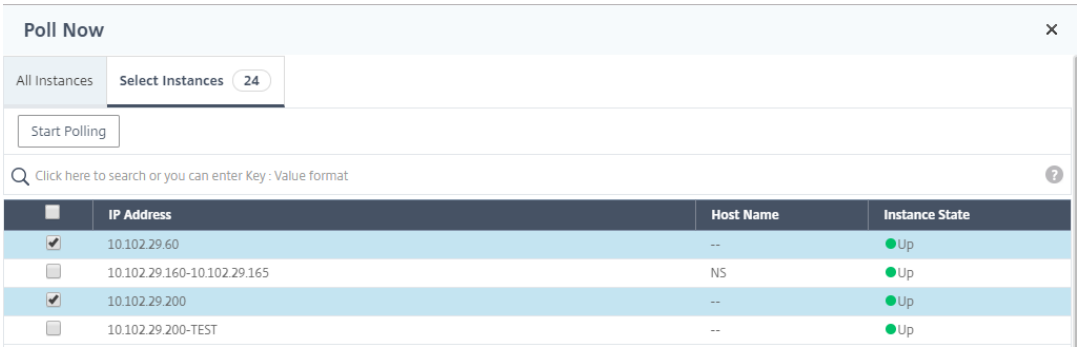


3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or to poll the selected instances.

   a) To poll the SSL certificates of all the NetScaler instances, select the **All Instances** tab and click **Start Polling**.



   b) To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.



Events

March 11, 2024

When the IP address of a Citrix Application Delivery Controller (ADC) instance is added to NetScaler Application Delivery Management (ADM), NetScaler ADM sends a NITRO call and implicitly adds itself as a trap destination for the instance to receive its traps or events.

Events represent occurrences of events or errors on a managed NetScaler instance. For example, when there is a system failure or change in configuration an event is generated and recorded on the NetScaler ADM server. Events received in NetScaler ADM are displayed on the Events Summary page (**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**).

NetScaler ADM also checks the events generated on instances to form alarms of different severity levels. These alarms are then displayed as messages, some of which might require immediate attention. For example, system failure can be categorized as a "Critical"event severity and would need to be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor the events, which can be many, generated across your NetScaler infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, NetScaler instances, category, failure objects, configuration commands, and messages.

You can also ensure multiple notifications are triggered for an event for a specific time interval, until the event is cleared. As an extra measure, you can customize your email with a specific subject line and user message, and upload an attachment.

Use events dashboard

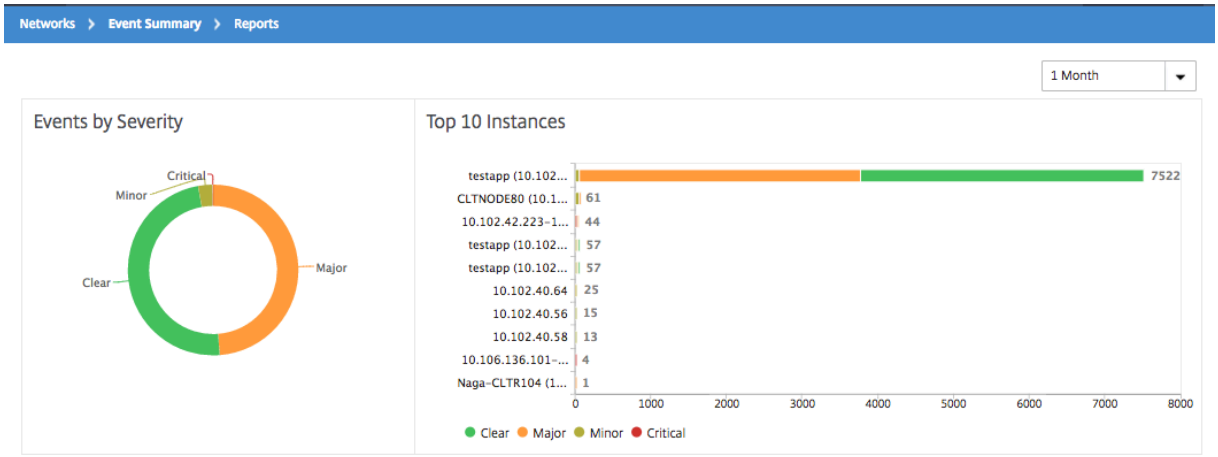
December 31, 2023

As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your Citrix Application Delivery Controller (ADC) instances, along with events and their severity on specific instances. You can use the NetScaler Application Delivery Management (ADM)'s events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

To view the details on the events dashboard:

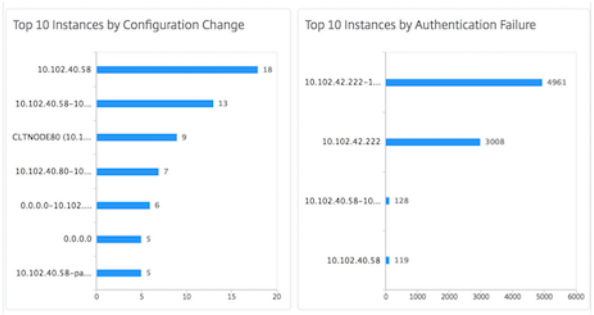
Navigate to **Infrastructure > Events > Reports**.

The Top 10 Devices graph on the dashboard displays a report of the top 10 instances by the number of events generated on them. You can click an instance on the graph to view further details of the event's severity.

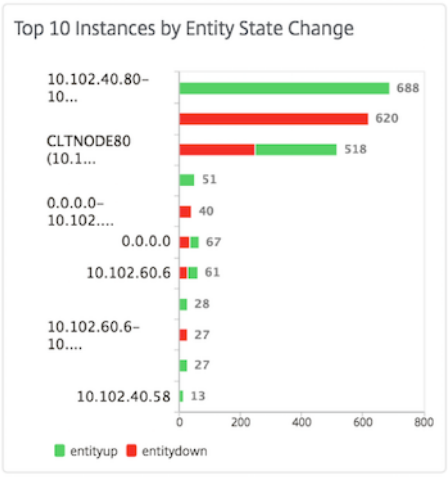


You can view more details by navigating to the NetScaler instance type (**Infrastructure > Events > Reports** > **NetScaler/ NetScaler SDX**) to view the following:

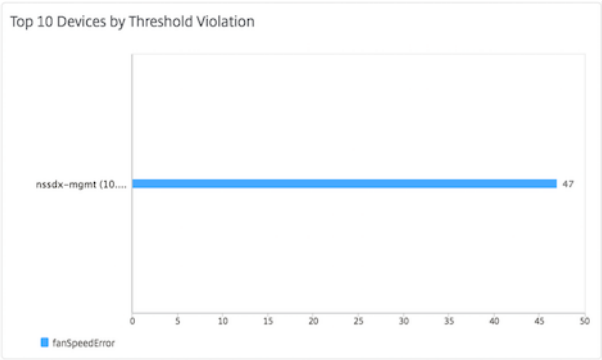
- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure



- Top 10 devices by entity state changes



- Top 10 devices by threshold violation



Set event age for events

March 11, 2024

You can set the event age option to specify the time interval (in seconds). NetScaler ADM monitors the appliances until the set duration and generates an event only if the event age exceeds the set duration.

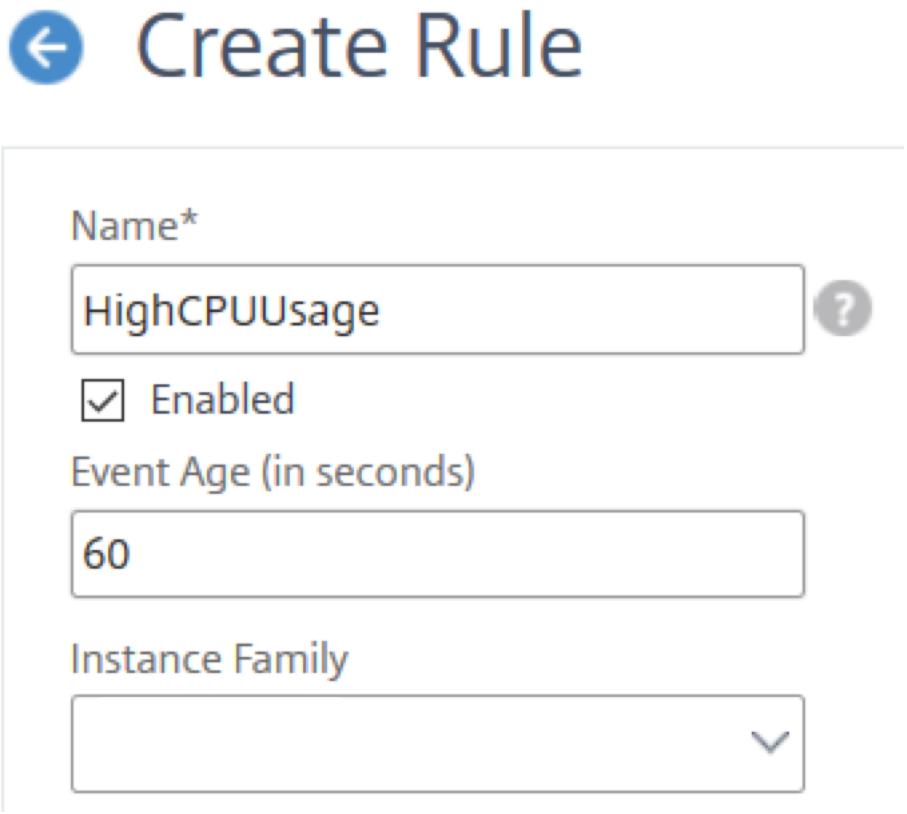
> Note:
>
> The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event is occurred.

For example, consider that you want to manage various ADC appliances and get notified by email when any of your virtual servers goes down for 60 seconds or longer. You can create an event rule with the necessary filters and set the rule's event age to 60 seconds. Then, whenever a virtual server

remains down for 60 or more seconds, you receive an email notification with details such as entity name, status change, and time.

To set event age in NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > Events > Rules**, and click **Add**.
2. On the **Create Rule** page, set the rule parameters.
3. Specify the event age in seconds.



Ensure to set all the co-related traps in the **Category** section and also set the respective severity in the **Severity** section when you set event age. In the preceding example, select the `entityup`, `entitydown`, and `entityofs` traps.

Schedule an event filter

March 11, 2024

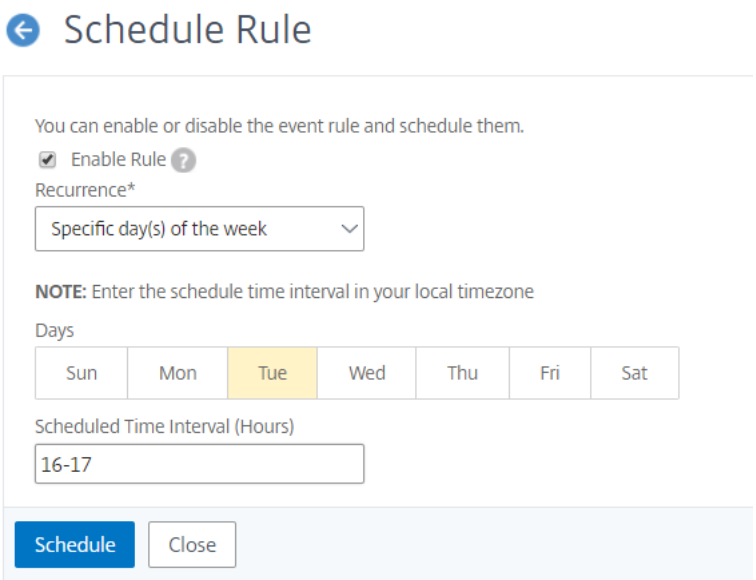
After creating a filter for your rule, if you do not want the NetScaler Application Delivery Management (ADM) server to send a notification every time the event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals such as daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends a large number of email notifications when NetScaler ADM receives these traps. If you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using NetScaler ADM:

1. In the NetScaler ADM, navigate to **Infrastructure > Events > Rules**.
2. Select the rule you want to schedule a filter for, and click **View Schedule**.
3. On the **Scheduled Rule** page, click **Schedule** and specify the following parameters:
    - **Enable Rule** –Select this check box to enable the scheduled event rule.
    - **Recurrence** - Interval at which to schedule the rule. Select either a specific day of the week or a specific date in a month.
    - **Days**: Select the day of the week to run the rule. You can select multiple days.
    - **Dates**: Type in the dates. You can type multiple dates as comma-separated values.
    - **Scheduled Time Interval (Hours)** –Hours, at which to schedule the rule (use the 24-hour format).
4. Click **Schedule**.



Set repeated email notifications for events

March 11, 2024

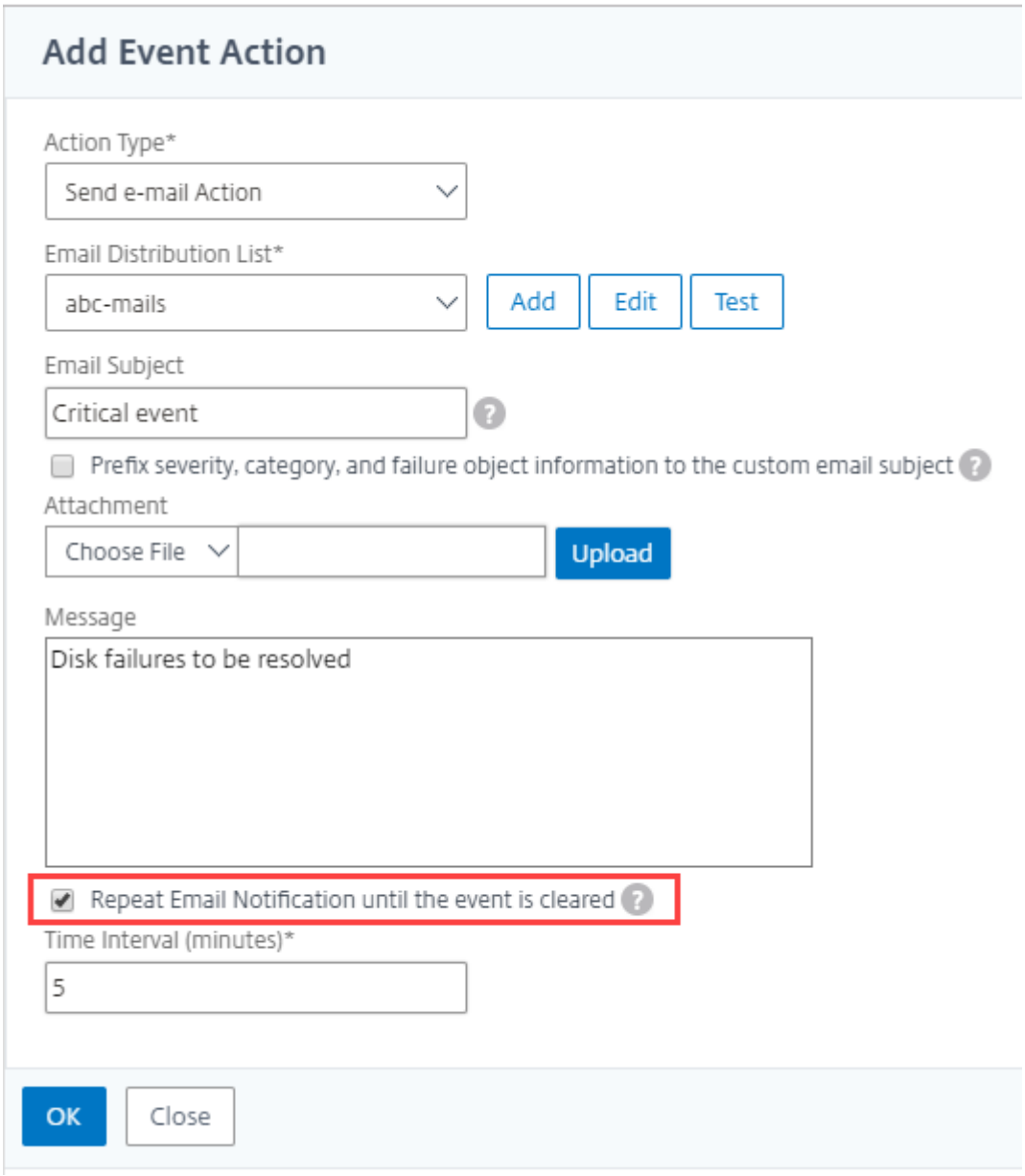
To ensure that all critical events are addressed and no important email notifications are missed, you can opt to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

> **Note**
>
> Events can only be cleared automatically if there is an equivalent "clear"trap set and sent from your Citrix Application Delivery Controller (ADC) instance.
>
> To clear an event manually, you can do the following:
>
> - Navigate to **Infrastructure > Events > Event Summary**, choose a **Category** and select an event in the category and click **Clear**.
> - Or, navigate to **Infrastructure > Events > Event Messages**. Choose an instance type and then, select an event from the grid below and click **Clear**.

To set repeated email notifications from NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters.
3. Under **Event Rule** Actions, click **Add Action**. Then, select **Send e-mail Action** from the **Action Type** drop-down list and select an **Email Distribution List**.
4. You can also add a customized subject line and user message, and upload an attachment to your email when an incoming event matches the configured rule.
5. Select the **Repeat Email Notification until the event is cleared** check box.



Suppress events

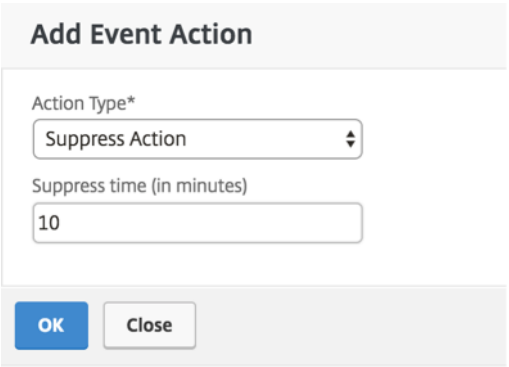
March 11, 2024

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.

> Note:
>
> You can also configure the suppress time as 0 minutes and it means infinite time. If you do not specify any time duration, then NetScaler ADM considers the suppress time as zero and it never expires.

To suppress events by using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Events > Rules**. Click **Add**.
2. Specify all the parameters required to create a rule.
3. Under **Event Rule Actions**, click **Add Action** to assign notification actions for the event.
4. On the **Add Event Action** page, select **Suppress Action** from the **Action Type** drop-down list and specify the time period, in minutes, for which an event must be suppressed.
5. Click **OK**.



Create event rules

March 11, 2024

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of events generated across your infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, Citrix Application Delivery Controller (NetScaler) instances, category, failure objects, configuration commands, and messages.

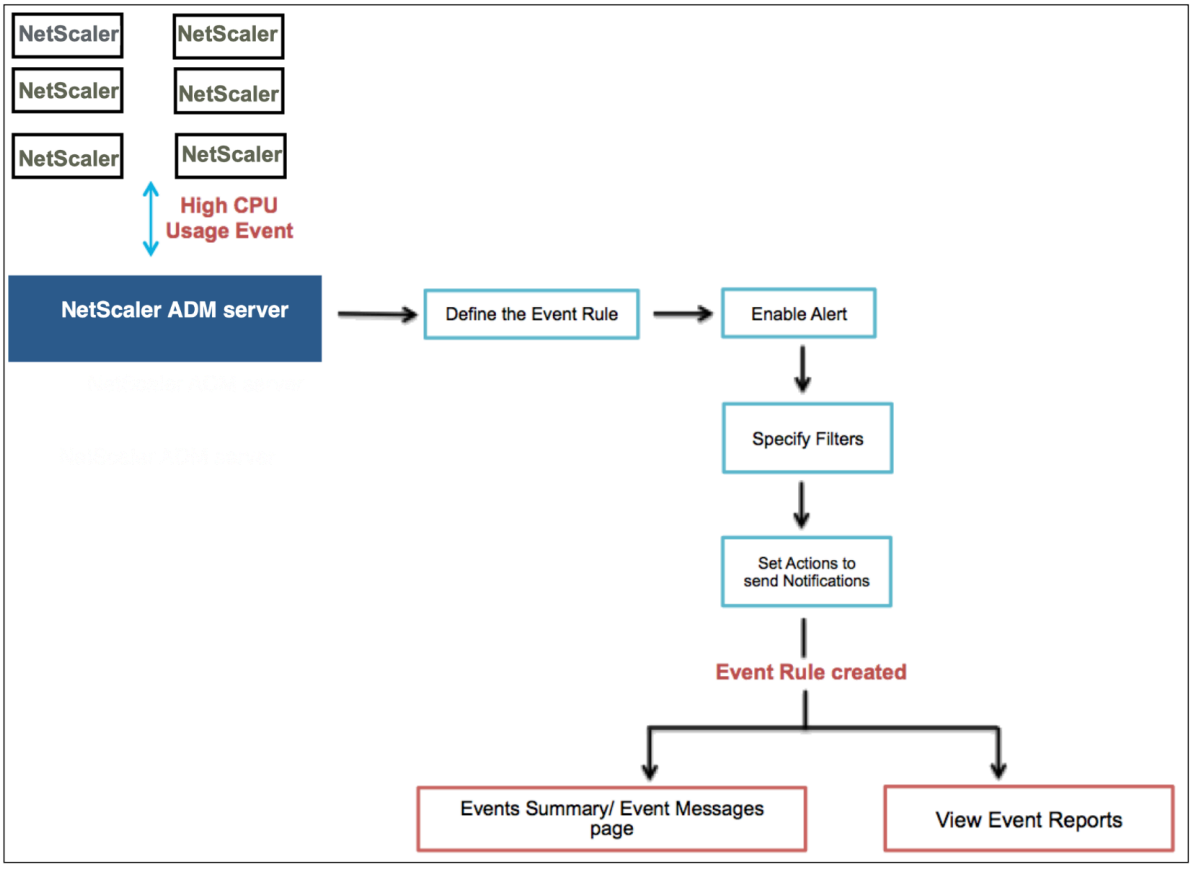
You can assign the following actions to the events:

- **Send e-mail Action**: Send an email for the events that match the filter criteria.

- **Send Trap Action**: Send or forward SNMP traps to an external trap destination
- **Run Command Action**: Run a command when an incoming event meets the configured rule.
- **Execute Job Action**: Run a job is for events that match the filter criteria that you've specified.
- **Suppress Action**: Suppresses drop an event for a specific time period.
- **Send Slack Notifications**: Send notifications on the configured Slack channel for the events that match the filter criteria.
- **Send PagerDuty Notifications**: Send event notifications based on the PagerDuty configurations for the events that match the filter criteria.
- **Send ServiceNow Notifications**: Auto-generate ServiceNow incidents for an event that match the filter criteria.

For more information, see Add event rule actions

You can also have notifications resent at a specified interval until an event is cleared. And you can customize the email with a specific subject line, user message, and attachment.



For example, as an administrator you might want to monitor "high CPU usage"events for specific NetScaler instances if those events can lead to an outage of your NetScaler instances. You can:

- Create a rule to monitor the instances and specify an action that sends you an email notification when an event in the “high CPU usage”category occurs.
- Schedule the rule to run at a specific time, such as between 11 AM to 11 PM, so that you are not notified every time there is an event generated.

Configuring an event rule involves the following tasks:

1. Define the rule
2. Choose the severity of the event that the rule detects
3. Specify the category of the event
4. Specify NetScaler instances to which the rule applies
5. Select failure objects
6. Specify advanced filters
7. Specify actions to be taken when the rule detects an event

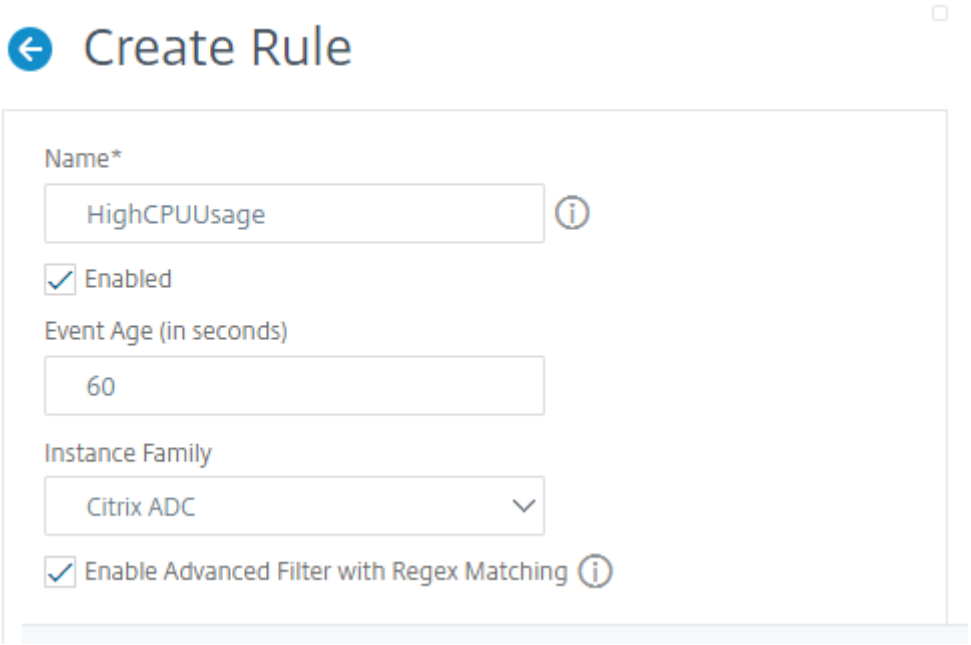
Step 1 - Define an event rule

Navigate to **Infrastructure > Events > Rules**, and click **Add**. If you want to enable your rule, select the **Enable Rule** check box.

You can set the **Event Age** option to specify the time interval (in seconds) after which NetScaler ADM refreshes an event rule.

> Note:
>
> The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event is occurred.

Based on the example above, you may want to be notified by email every time your NetScaler instance has a “high CPU usage”event for 60 seconds or longer. You can set the event age as 60 seconds, so that every time your NetScaler instance has a “high CPU usage”event for 60 seconds or more, you receive an email notification with details of the event.



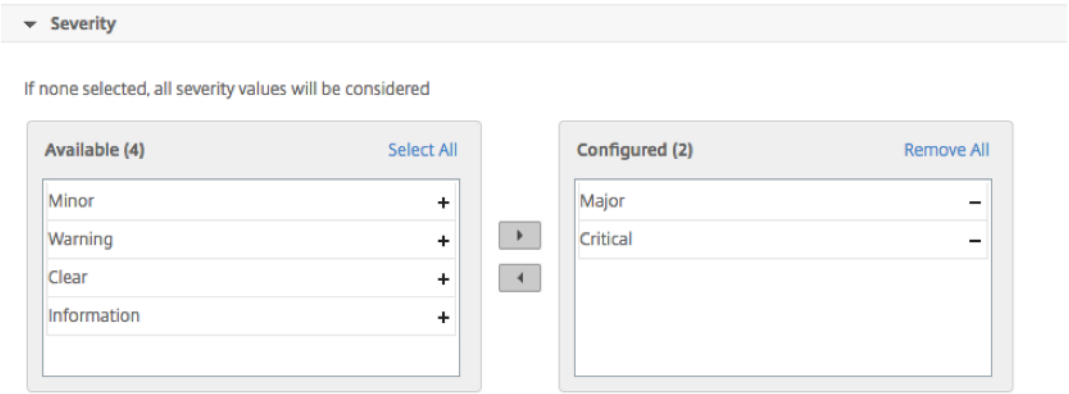
You can also filter event rules by **Instance Family** to track the NetScaler instance from which NetScaler ADM receives an event.

If you want to include a regular expression other than asterisk (*) pattern matching, select **Enable Advanced Filter with Regex Matching**.

Step 2 - Choose the severity of the event

You can create event rules that use the default severity settings. Severity specifies the current severity of the events you which you want to add the event rule.

You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.

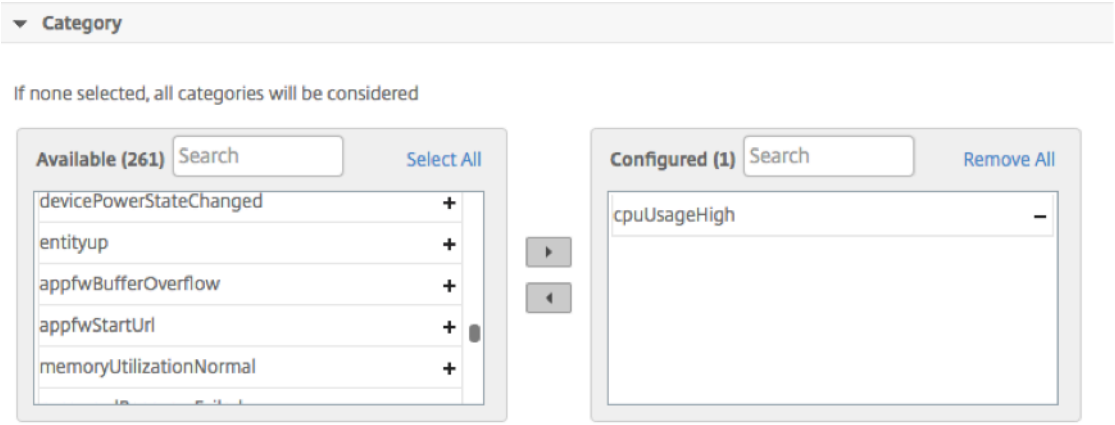


> **Note**
>
> You can configure severity for both generic and Advanced-specific events. To modify event severity for NetScaler instances managed on NetScaler ADM, navigate to **Infrastructure > Events > Event Settings**. Choose the **Category** for which you want to configure event severity and click **Configure Severity**. Assign a new severity level and click **OK**.

Step 3 - Specify the event category

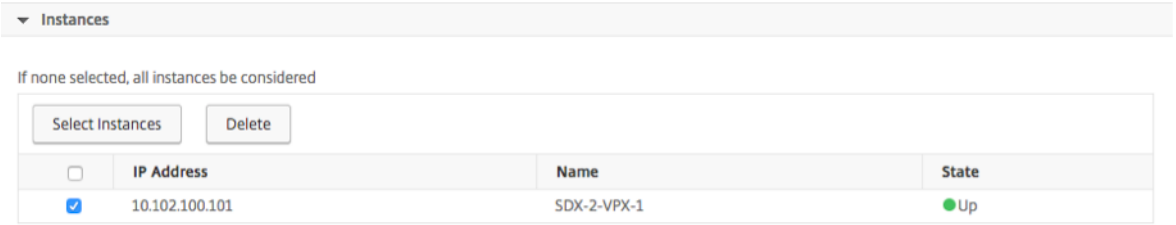
You can specify the category or categories of the events generated by your NetScaler instances. All categories are created on NetScaler instances. These categories are then mapped with NetScaler ADM that can be used to define event rules. Select the category you want to consider and move it from the **Available** table to the **Configured** table.

In the example above, you must choose “cpuUsageHigh”as the event category from the table displayed.



Step 4 - Specify NetScaler instances

Select the IP addresses of the NetScaler instances for which you want to define the event rule. In the **Instances** section, click **Select Instances**. In the **Select Instances** page, choose your instances, and click **Select**.



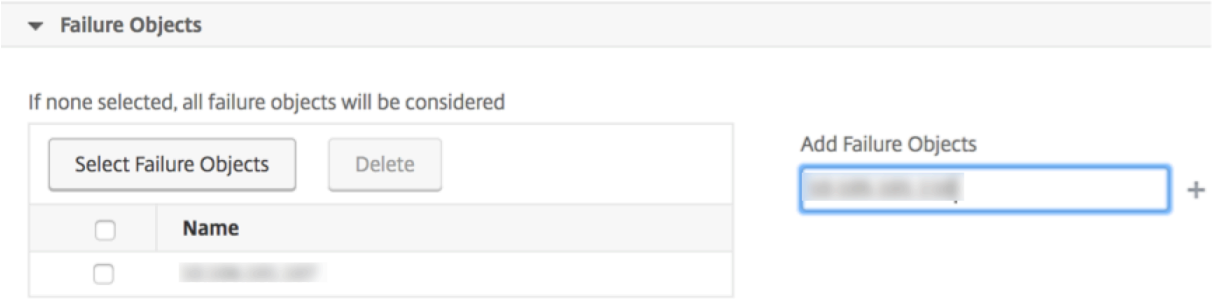
Step 5 - Select failure objects

You can either select a failure object from the list provided or add a failure object for which an event has been generated. You can also specify a regular expression to add failure objects. Depending on the specified regular expression, the failure objects are automatically added to the list. Failure objects are entity instances or counters for which an event has been generated.

> **Important**
>
> To list failure objects using regular expression, select **Enable Advanced Filter with Regex Matching** in Step 1.

The failure object affects the way that an event is processed and ensures it reflects the exact problem as notified. With this filter, you can track issues on the failure objects quickly and identify the cause for an issue. For example, if a user has login issues, then the failure object here is the user name or password, such as `nsroot`.

This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events, and so on.

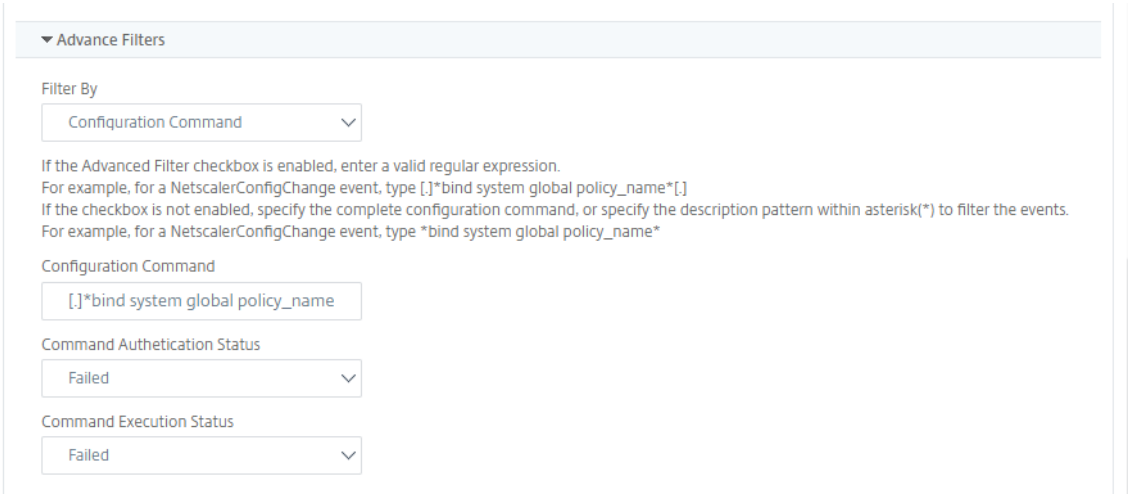


Step 6 - Specify advanced filters

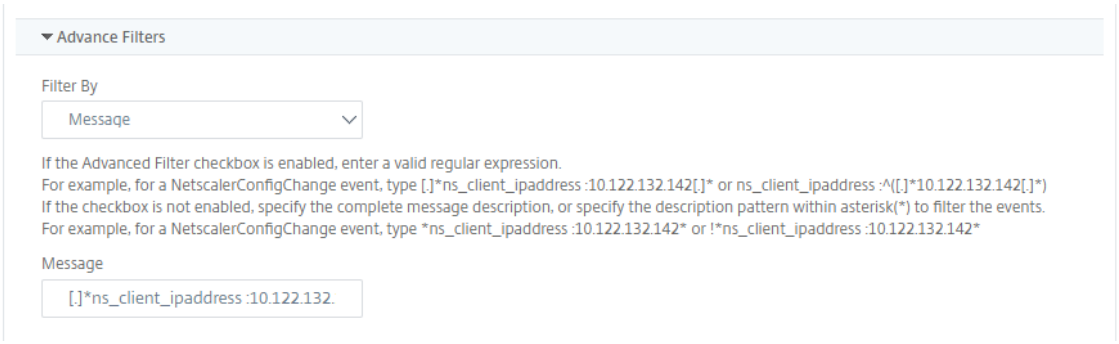
You can further filter an event rule by:

- **Configuration Commands** - You can specify the complete configuration command, or specify a regular expression to filter events.

  You can further filter the event rule by the command's authentication status and/ or its execution status. For example, for a `NetscalerConfigChange event`, type `[.]*bind system global policy_name[.]*`.



- **Messages** - You can specify the complete message description, or specify a regular expression to filter the events.
  For example, for a `NetscalerConfigChange` event, type `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`
  .



Step 7 - Add event rule actions

You can add event rule actions to assign notification actions for an event. These notifications are sent or performed when an event meets the defined filter criteria that you've set above. You can add the following event actions:

- Send email Action
- Send Trap Action
- Run Command Action
- Run Job Action
- Suppress Action
- Send Slack Notifications

- Send PagerDuty Notifications
- Send ServiceNow Notifications

To set email Event Rule Action

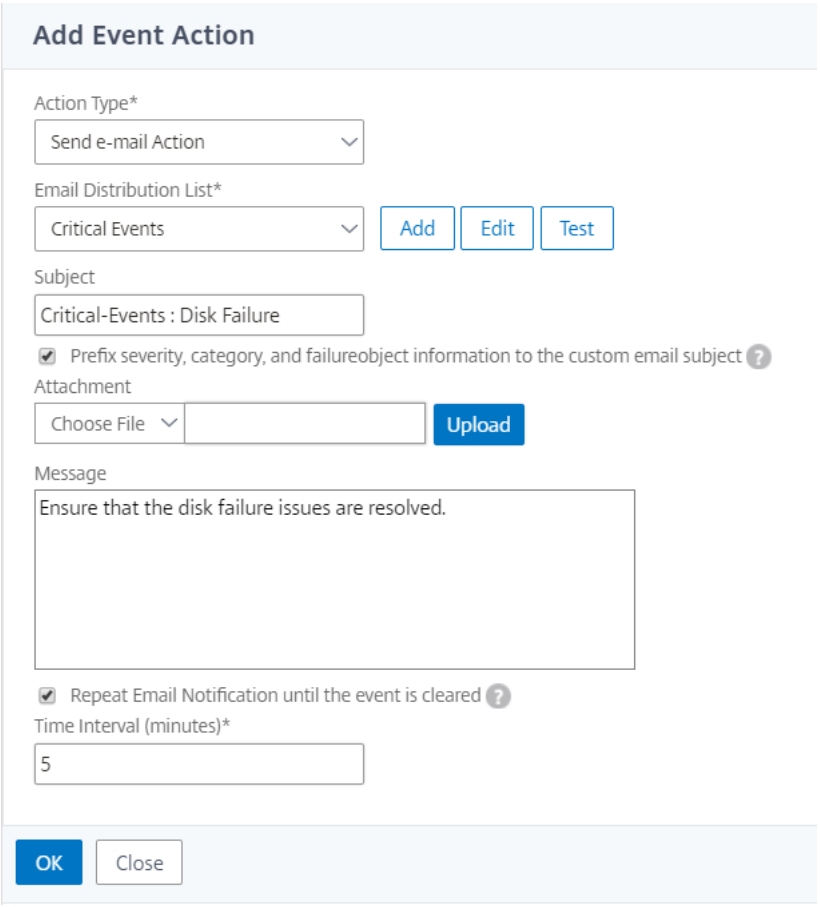
When you choose the Send email Action event action type, an email is triggered when the events meet the defined filter criteria. You must either create an email distribution list by providing mail server or mail profile details or you can select an email distribution list that you've previously created.

Due to a high number of virtual servers being configured in NetScaler ADM, you might receive a high number of emails every day. The emails have a default subject line that provides information about the severity of the event, the category of the event and the failure object. But the subject line does not carry any information about the name of the virtual server where these events originate from. You now have an option to include some additional information like the name of the affected entity, name of the failure object.

You can also add a customized subject line and a user message, and upload an attachment to your email when an incoming event matches the configured rule.

While sending emails for event notifications, you might want to send a test email to test the configured settings. The "Test"button now allows you to send a test email after configuring an email server, associated distributed lists, and other settings. This feature ensures that settings are working fine.

You can also ensure that all critical events are addressed and no important email notifications are missed, by selecting the **Repeat Email Notification until the event is cleared** check box to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.



To set Trap Event Rule Action

When you choose the **Send Trap Action** event action type, SNMP traps are sent or forwarded to an external trap destination. By defining a trap distribution list (or a trap destination and trap profile details), trap messages are sent to specific trap listeners when events meet the defined filter criteria.

To set the Run Command Action

When you choose the **Run Command Action** event action, you can create a command or a script that can be run on NetScaler ADM for events matching a particular filter criterion.

You can also set the following parameters for the **Run Command Action** script:

Parameter	Description
$source	This parameter corresponds to the source IP address of the received event.

$category	This parameter corresponds to the type of traps defined under category of the filter
$entity	This parameter corresponds to the entity instances or counters for which an event has been generated. It can include the counter names for all threshold-related events, entity names for all entity-related events, and certificate names for all certificate-related events.
$severity	This parameter corresponds to the severity of the event.
$failureobj	The failure object affects the way that an event is processed and ensures that the failure object reflects the exact problem as notified. This can be used to track down problems quickly and to identify the reason for failure, instead of simply reporting raw events.

> **Note**
>
> During command execution, these parameters are replaced with actual values.

For example, consider that you want to set a run command action when a load balancing virtual server status is **Down**. As an administrator, you might want to consider providing a quick workaround by adding another virtual server. In NetScaler ADM, you can:

- Write a script (.sh) file.

  The following is a sample script (.sh) file:

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
```



```
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Save the .sh file in any persistent location on NetScaler agent. For example, /var.
- Provide the .sh file location in NetScaler ADM to run when the rule criteria are met.

To set the **Run Command** action for creating a new virtual server:

1. Define the rule
2. Select the severity of the event
3. Select the event category **entitydown**
4. Select the instance that has the virtual server configured
5. Select or create a failure object for the virtual server
6. Under **Event Rule Actions**, click **Add Action** and select **Run Command Action** from the **Action Type** list.
7. Under **Command Execution List**, click **Add**.

   The Create Command Distribution List page is displayed.

   a) In **Profile Name**, specify a name of your choice

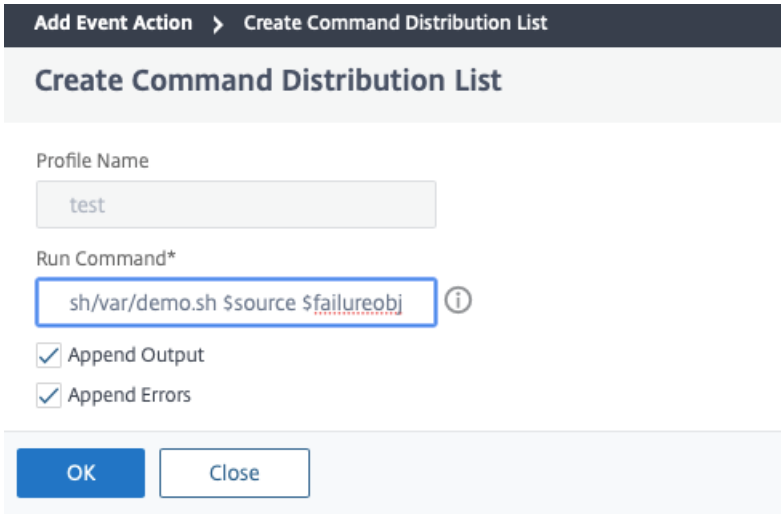
   b) In **Run Command**, specify the NetScaler agent location, where the script must be run. For example: /sh/var/demo.sh $source $failureobj.

   c) Select **Append Output** and **Append Errors**

   > **Note**
   >
   > You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler ADM server log files. If you do not enable these options, NetScaler ADM discards all outputs and errors generated while running the command script.

   d) Click **Create**.

8. In the **Add Event Action** page, click **OK**.

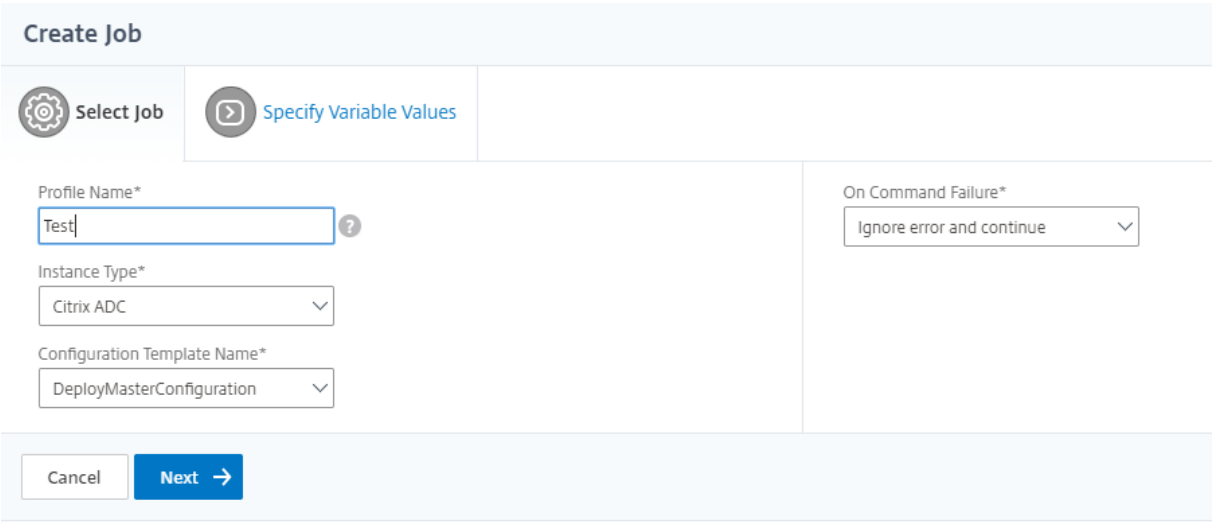


> **Note**
>
> You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler ADM server log files. If you do not enable these options, NetScaler ADM discards all outputs and errors generated while running the command script.

To set the `Execute` Job Action

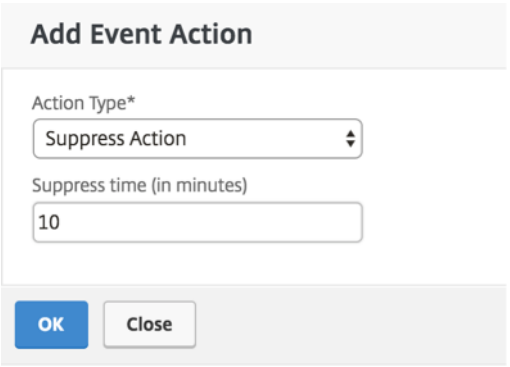
By creating a profile with configuration jobs, a job is run as a built-in job or a custom job for NetScaler and NetScaler SDX instances, for events and alarms that match the filter criteria you've specified.

1. Under **Event Rule Actions**, click **Add Action** and select **Execute Job Action** from the **Action Type** drop-down list.
2. Create a profile with a job that you want to run when the events meet the defined filter criteria.
3. While creating a job, specify a profile name, the instance type, the configuration template, and what action you'd like to perform if the commands on the job fail.
4. Based on the instance type selected and the configuration template chosen, specify your variables values and click **Finish** to create the job.



To set the Suppress Action

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.



To set Slack notifications from NetScaler ADM

Configure the required Slack channel by providing the profile name and the webhook URL in NetScaler ADM GUI. The event notifications are then sent to this channel. You can configure multiple Slack channels to receive these notifications

1. In NetScaler ADM, navigate to **Infrasturcture > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters such as severity and category. Select instances and also failure objects that must be monitored.
3. Under **Event Rule Actions**, click **Add Action**. Then, select **Send Slack Notifications** from the **Action Type** list and select **Slack Profile List.**

4. You can also add a Slack profile list by clicking **Add** next to the **Slack Profile List** field.
5. Type the following parameters to create a profile list:
    a) **Profile Name**. Type a name for the profile list to be configured on NetScaler ADM
    b) **Channel Name**. Type the name of the Slack channel to which the event notifications are to be sent.
    c) **Webhook URL**. Type the Webhook URL of the channel that you have entered earlier. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name and all event notifications are sent to this URL to be posted on the designated Slack channel. An example of a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Click **Create** and click **OK** in the **Add Event Action** window.

> **Note:**
>
> You can also add the Slack profiles by navigating to **System** > **Notifications** > **Slack Profiles**. Click **Add** and create the profile as described in the earlier section.

You can view the status of the Slack profiles that you have created.

Your event rule is now created with appropriate filters and well defined event rule actions.

To set PagerDuty notifications from NetScaler ADM

You can add a PagerDuty profile as an option in NetScaler ADM to monitor the incident notifications based on your PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on registered number.

Before you add a PagerDuty profile in NetScaler ADM, ensure you have completed the required configurations in PagerDuty. For more information, see PagerDuty documentation.

You can select your PagerDuty profile as one of the options to get notifications for the following features:

- **Events** –List of events that are generated for NetScaler instances.
- **Licenses** –List of licenses that are currently active, about to expire, and so on.
- **SSL Certificates** –List of SSL certificates that are added to NetScaler instances.

To add a PagerDuty profile in ADM:

1. Log on to NetScaler ADM using administrator credentials.
2. Navigate to **Settings > Notifications > PagerDuty Profiles**.

3. Click **Add** to create a new profile.
4. In the Create PagerDuty Profile page:
    a) Provide a profile name of your choice.
    b) Enter the **Integration Key**.
        You can get the Integration Key from your PagerDuty portal.
    c) Click **Create**.

    Use case:

    Consider a scenario that you:

    - want to send notifications to your PagerDuty profile.
    - have configured phone call as an option in PagerDuty to receive notifications.
    - want to get phone call alerts for NetScaler events.

    To configure:

    a) Navigate to **Events** > **Rules**
    b) On the **Create Rule** page, configure all other parameters to create a rule.
    c) Under **Create Rule Actions**, click **Add Action**.
        The **Add Event Action** page is displayed.
        i. Under **Action Type**, select **Send PagerDuty Notifications**.
        ii. Select your PagerDuty profile and click **OK**.

    After the configuration is complete, whenever a new event is generated for NetScaler instance, you will receive a phone call. From the phone call, you can decide to:

    - Acknowledge the event
    - Mark it as resolved
    - Escalate to another team member

To auto-generate ServiceNow incidents from NetScaler ADM

You can auto-generate ServiceNow incidents for NetScaler ADM events by selecting the ServiceNow profile on the NetScaler ADM GUI. You must choose the ServiceNow profile in NetScaler ADM to configure an event rule.

Before you configure an event rule to auto-generate ServiceNow incidents, integrate NetScaler ADM with a ServiceNow instance. For more information, see Configure ITSM adapter for ServiceNow.

To configure an event rule, navigate to **Events** > **Rules**.

1. On the **Create Rule** page, configure all other parameters to create a rule.
2. Under **Create Rule Actions**, click **Add Action**.

   The **Add Event Action** page is displayed.

   a) In **Action Type**, select **Send ServiceNow Notifications**.

   b) In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.

   c) Click **OK**.

Modify the reported severity of events that occur on NetScaler instances

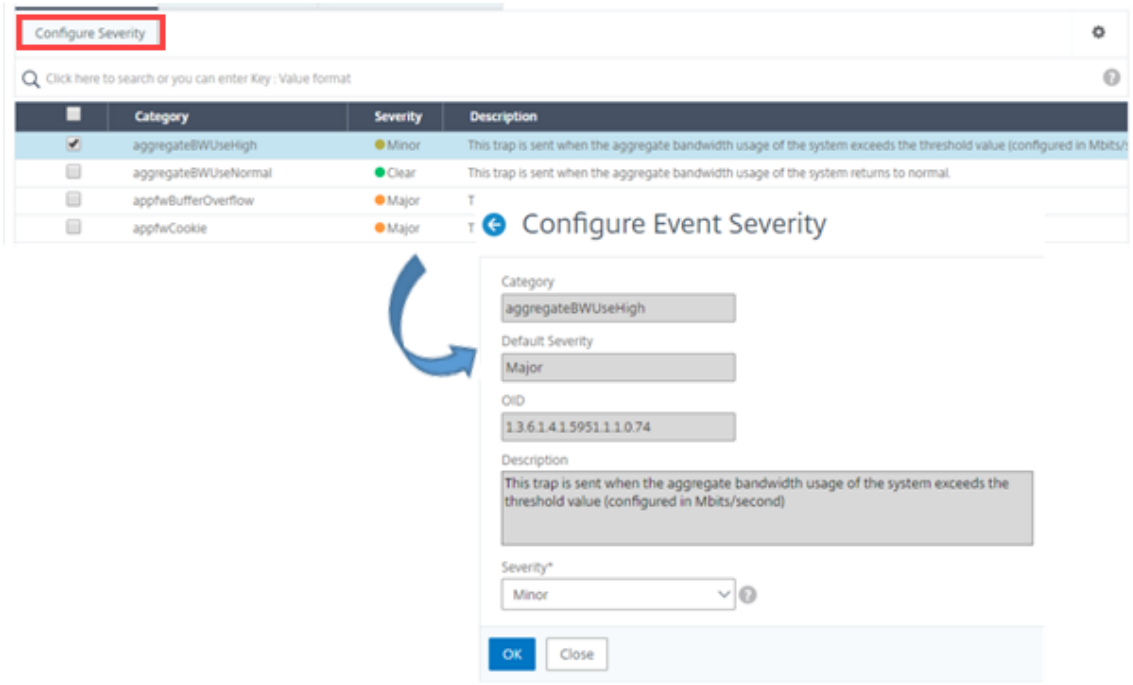
December 31, 2023

You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on a particular instance and view reports on the basis of event severity. You can create event rules that use the default severity settings, and you can change the severity settings. You can configure severity for both generic and enterprise-specific events.

You can define the following levels of severity: Critical, Major, Minor, Warning, and Clear.

To modify event severity:

1. Navigate to **Infrastructure > Events > Event Settings**.
2. Click the tab for the Citrix Application Delivery Controller (ADC) instance type that you want to modify. Then, select the category from the list and click **Configure Severity**.
3. In **Configure Event Severity**, select the severity level from the drop-down list.
4. Click **OK**.

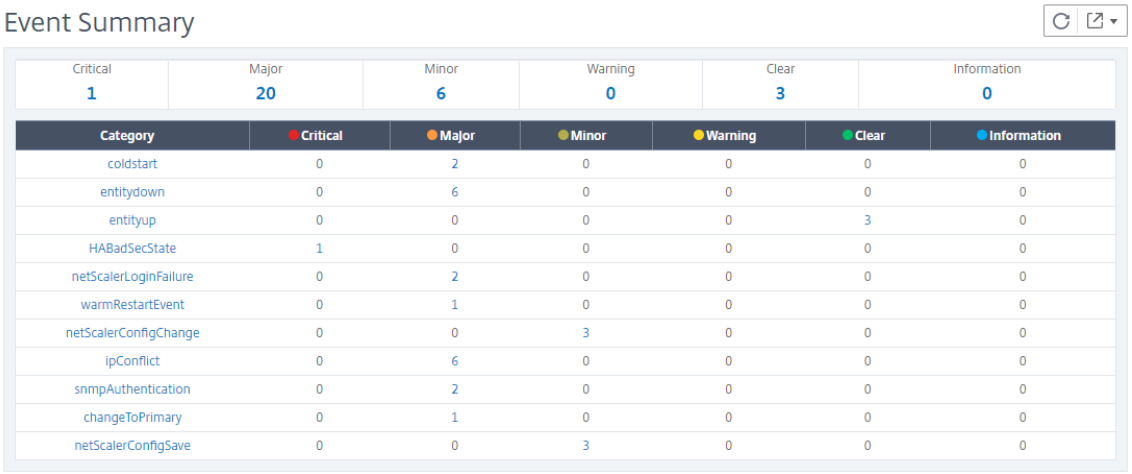


View events summary

March 11, 2024

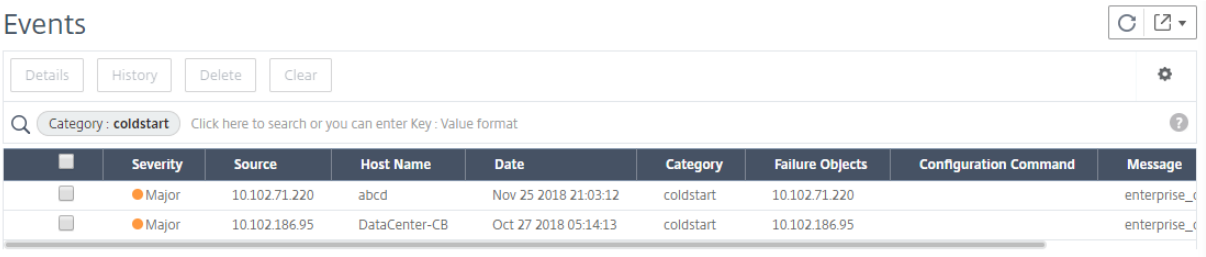
You can now view an Events Summary page to monitor the events and traps received on your NetScaler Application Delivery Management (ADM) server. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by NetScaler ADM**. The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a Citrix Application Delivery Controller (ADC) instance goes down and stops sending information to the NetScaler ADM server. During the event, a notification is sent to an administrator, explaining the reason why the instance is down, the time for which it had been down, and so on. The event is then recorded on the Events Summary page, on which you can view a summary and access the details of the event.



- **Number of traps received for each category**. The number of traps received, categorized by severity. By default, each trap sent from NetScaler instances to NetScaler ADM has an assigned severity, but as the network administrator, you can specify its severity in the NetScaler ADM GUI.

If you click a category type or a trap, you are taken to the **Events** page, on which filters such as the Category and Severity are preselected. This page displays more information about the event, such as the NetScaler instance's IP address and host name, date on which the trap was received, category, failure objects, configuration command run, and the message notification.



Display event severities and SNMP trap details

March 11, 2024

When you create an event and its settings in NetScaler Application Delivery Management (ADM), you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all Citrix Application Delivery Controller (ADC) instances added to your NetScaler ADM server in minute detail on the Infrastructure Dashboard.

On the Infrastructure dashboard, you can now mask irrelevant values so that you can more easily view and monitor information such as event by severities, health, up time, models, and version of NetScaler instances in minute detail.

For example, events with a **Critical** severity level might occur rarely. However, when these critical events do occur on your network, you might want to further investigate, troubleshoot, and monitor where and when the event occurred. If you select all severity levels except Critical, the graph displays only the occurrences of critical events. Also, by clicking the graph, you are taken to the **Severity based events** page, where you can see all the details regarding when a critical event occurred for the duration that you've selected: the instance source, the date, category, and message notification sent when the critical event occurred.

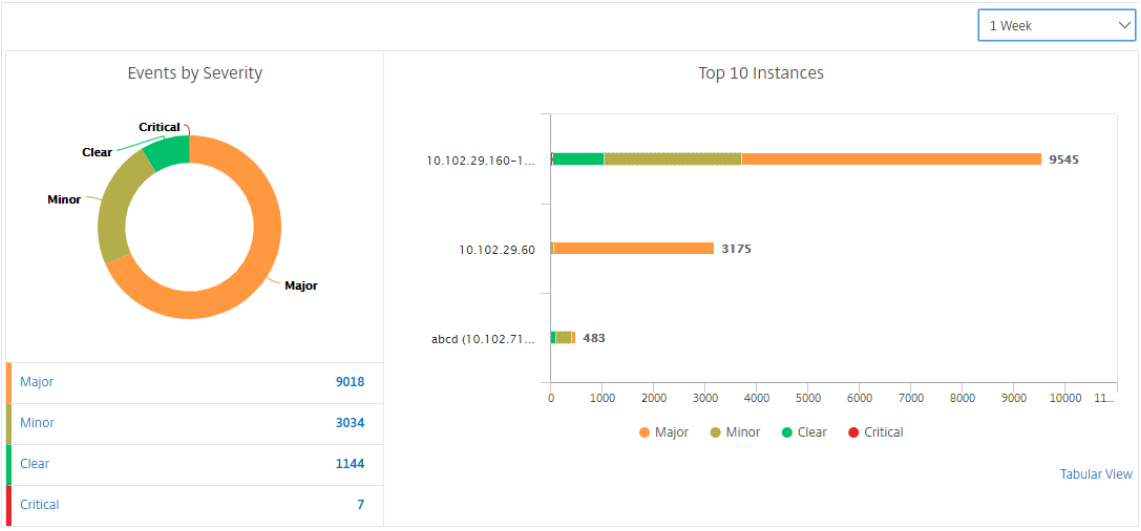
Similarly, you can view the health of a NetScaler VPX instance on the Dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of service. By clicking on the graph, you are taken to that instance's page, where the *out of service* filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and so on. You can also select the instance and see the particular Citrix instance's dashboard for more details.

To select specific events by severity in NetScaler ADM:

1. Log on to NetScaler ADM, using your administrator credentials.
2. Navigate to **Infrastructure > Dashboard**.

   Or,

   Navigate to **Infrastructure > Events > Reports**.
3. From the menu in the upper-right corner of the page, select the duration for which you want to see events by severity.

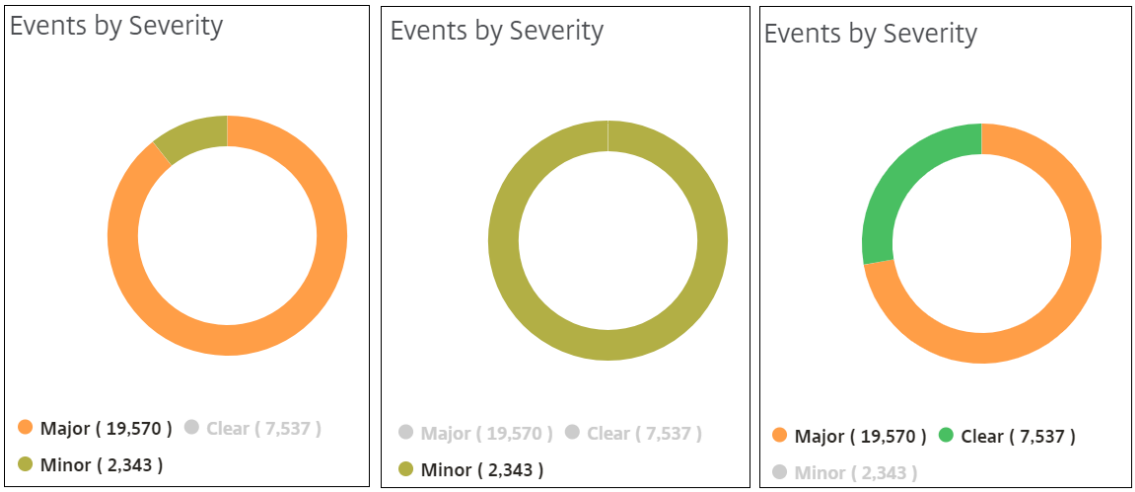


4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.

5. You can click each section on the donut chart to display the corresponding **Severity based events** page, which shows the following details for the selected severity for the selected duration:

    - Instance Source
    - Data of the event
    - Category of events generated by the NetScaler instance
    - Message notification sent

    > **Note**
    >
    > Below the donut chart you can see a list of severities that are represented in the chart. By default, a donut chart displays all events of all severity types, and therefore all severity types in the list are highlighted. You can toggle the severity types to more easily view and monitor your chosen severity.



To view NetScaler SNMP trap details on NetScaler ADM:

You can now view the details of each SNMP trap received from its managed NetScaler instances on the NetScaler ADM server on the **Event Settings** page. Navigate to **Infrastructure > Events > Event Settings**. For a specific trap received from your instance, you can view the following details in tabular format:

- **Category** - Specifies the category of the instance to which the event belongs.
- **Severity** - The severity of the event is indicated by colors and its severity type.
- **Description** - Specifies the messages associated with the event.

For example, an event with the trap category **monRespTimeoutBelowThresh**, the description of the trap is displayed as "This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set."

View and export NetScaler syslog messages

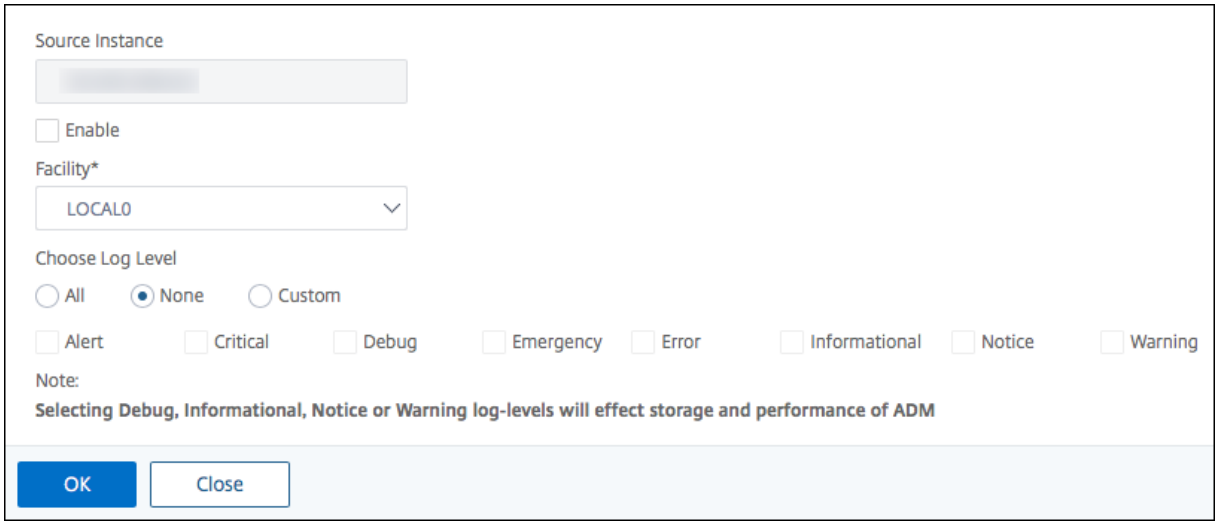
March 11, 2024

From your ADM software, you can monitor the syslog events generated on your Citrix Application Delivery Controller (ADC) instances. For that, you must configure ADM as the syslog server for your NetScaler instances. After you've configured ADM, all syslog messages are redirected from the ADC instances to ADM.

Configure ADM as a syslog server

Follow these steps to configure ADM as the syslog server:

1. From the ADM GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler ADM.
3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.

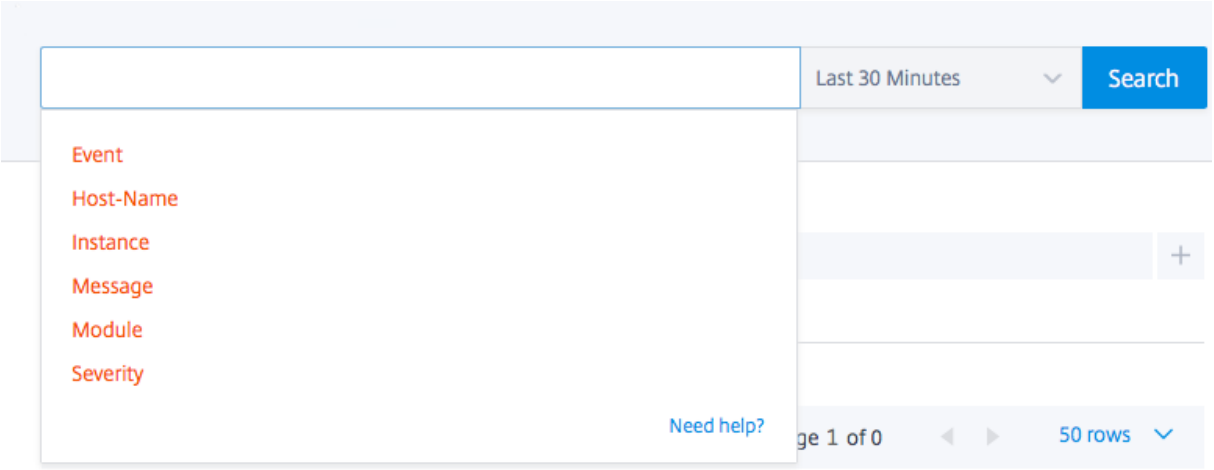


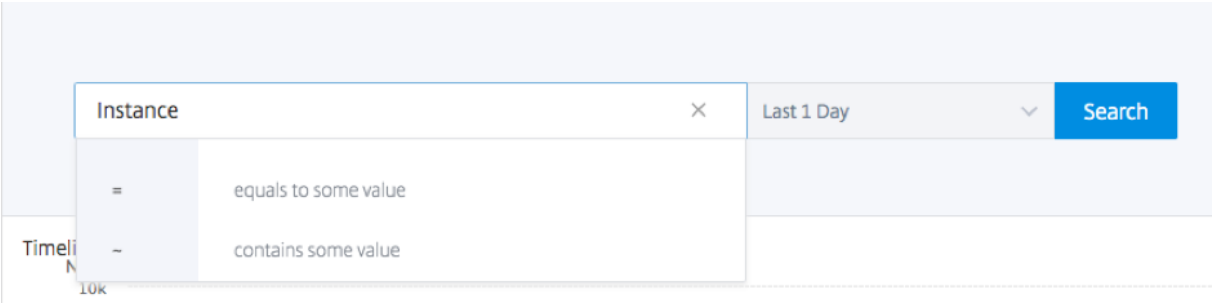
These steps configure all the syslog commands in the NetScaler instance, and NetScaler ADM starts receiving the syslog messages.

View and search syslog messages

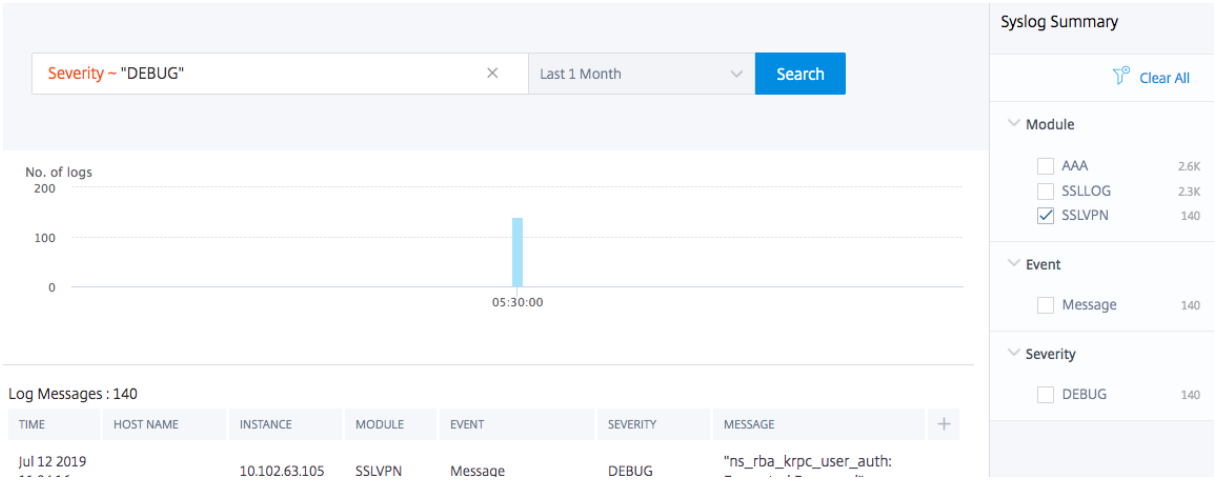
You can view all your syslog messages generated on your managed NetScaler instances. The syslog messages are stored in the database centrally and are available under **Infrastructure > Events > Syslog Messages** for auditing purposes. You can combine this logging information and derive reports for analytics from the collected data.

Further, you can use filters to narrow down the search results of syslog messages and find exactly what you are looking for and in real time. Click **Need Help?** to open the built-in search help.





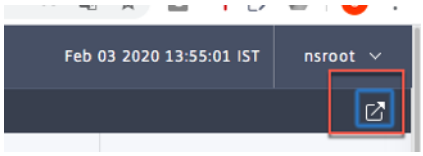
Next, add the search term. For some categories, a prepopulated list of search terms is displayed. By default, the search time is 1 day. You can change the time and date range by clicking the down arrow. You can further narrow down your search by selecting options from the **Syslog Summary** pane.



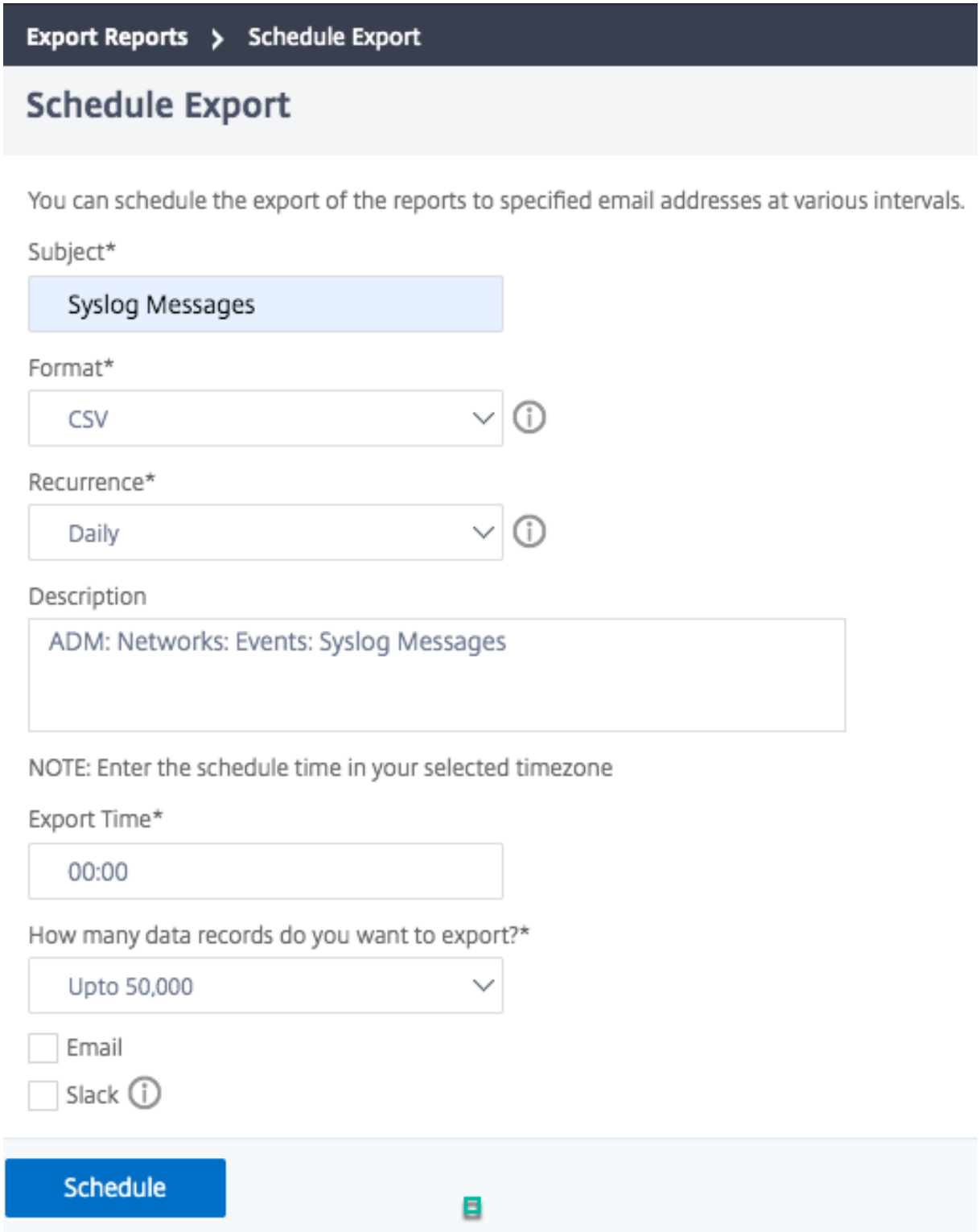
Export and schedule syslog messages

You can view syslog messages without logging into ADM, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your ADC instances in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses or Slack account at various intervals.

To export and schedule the log messages, click the arrow icon on the upper right corner.



- To export the log messages, click **Export Reports > Export Now**, select the required format, and then click **Export**.
- To schedule the export of syslog messages, click **Export Reports > Schedule Report**, and set the required parameters. You can receive the report through email or Slack.



Suppress syslog messages

March 11, 2024

When configured as a syslog server, NetScaler Application Delivery Management (ADM) receives all syslog messages sent to it by the configured Citrix Application Delivery Controller (ADC) instances. There might be a large number of messages that you might not want to see. For example, you might not be interested in seeing all informational level messages. You can now discard some of the syslog messages that you are not interested in. You can suppress some of the syslog messages coming into NetScaler ADM by setting up some filters. NetScaler ADM drops all messages that matches with the criteria. These dropped messages do not appear on the NetScaler ADM GUI and these messages are also not stored in the customer's NetScaler ADM database.

You can suppress some of the logged syslog messages coming into NetScaler ADM by setting up some filters. The two filters that can be used for suppressing syslog messages are severity and facility. You can also suppress messages coming from a particular NetScaler instance or multiple instances. You can also provide a text pattern for NetScaler ADM to search and suppress messages. NetScaler ADM drops all messages that matches with the criteria. These dropped messages do not appear on the NetScaler ADM GUI and these messages are also not stored in the customer database. Therefore, a good amount of space is saved on the storage server.

Some use cases for suppressing syslog messages are as follows:

- If you want to ignore all information level messages, suppress level 6 (informational)
- If you only want to record firewall error conditions, suppress all levels other than level 3 (errors)

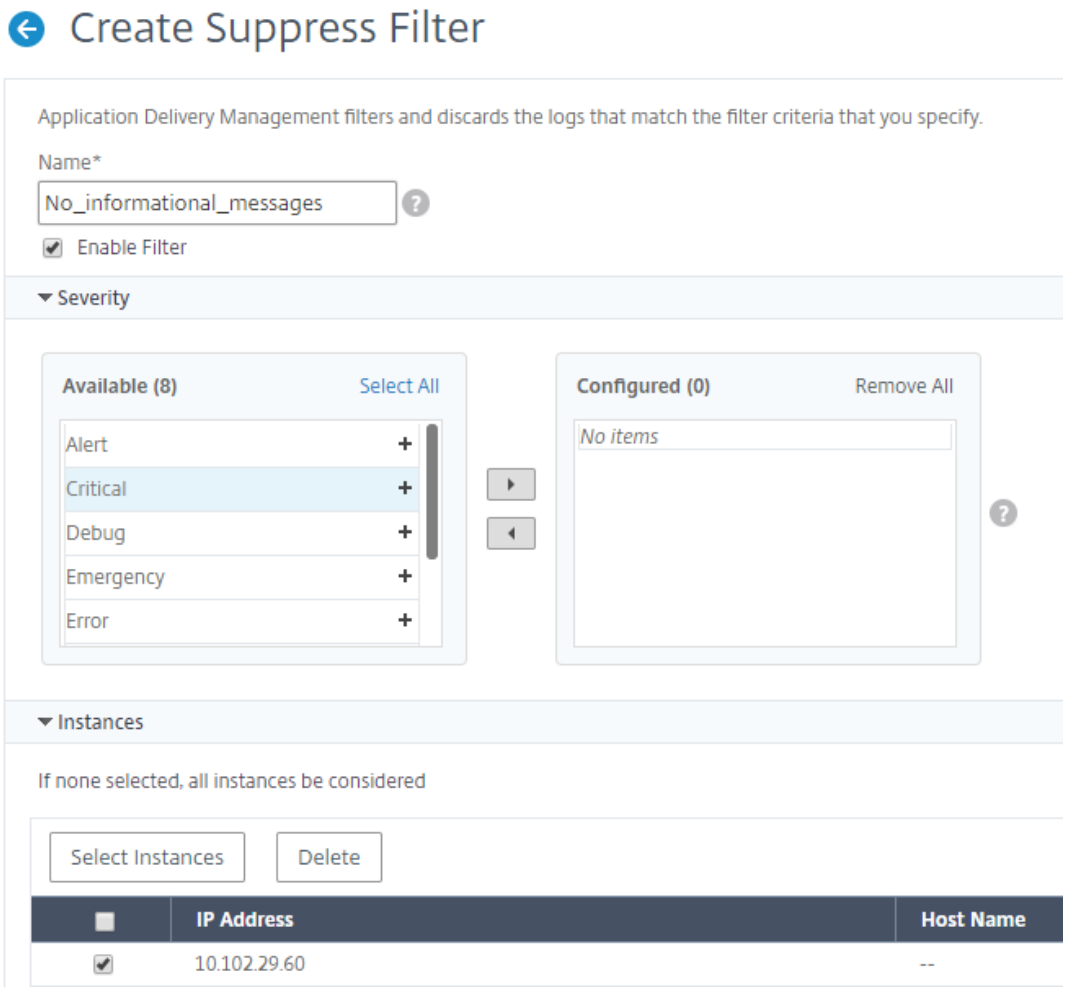
Suppressing syslog messages by creating filters

1. In NetScaler ADM, navigate to **Infrastructure > Events > Syslog Messages** > **Suppress Filter**.
2. On **Create Suppress Filter** page, update the following information:
    a) **Name** - type a name for the filter.

    > **Note**
    >
    > If different users have different access to multiple NetScaler instances, different filters must be created for different instances as users can see only those filters in which they have access to all the instances.

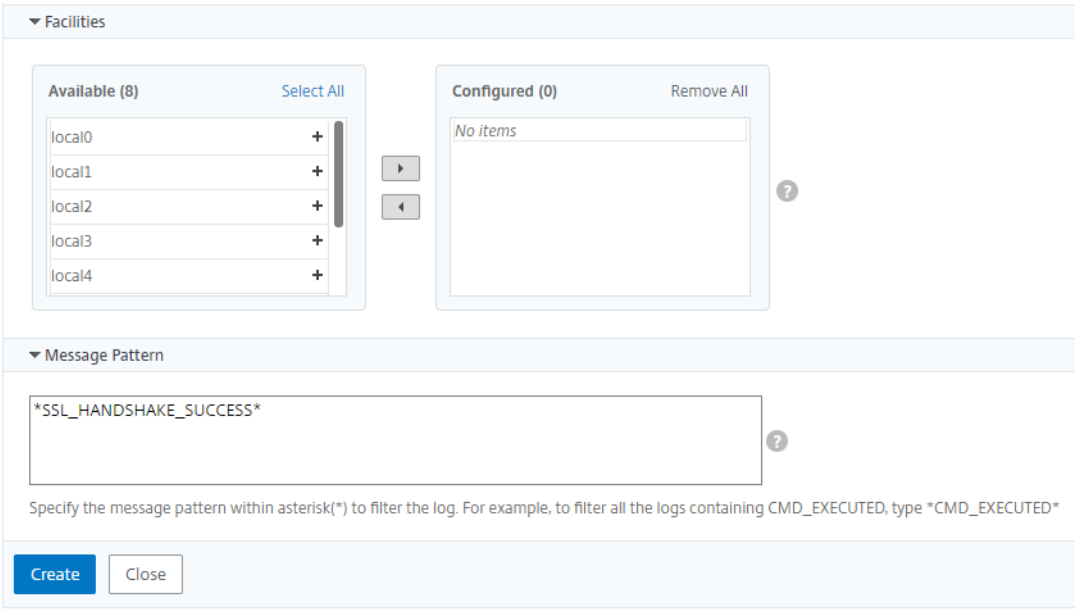
    b) **Severity** - Select and add the log levels for which you must suppress the messages. For example, if you do not want to view any informational messages coming in, you can select Informational to suppress those messages.

c) **Instances** - Select the NetScaler instances on which the syslog messages have been configured.



d) **Facilities** - Select the facility to suppress messages on the basis of the source that generates them.

e) **Message Pattern** - You can also type a text pattern surrounded by asterisk (*) to suppress the messages. The messages are searched for the text pattern string and those messages that contain this pattern are suppressed.



Disabling the filter

To allow the messages to be viewed on NetScaler ADM, you must disable the filter.

1. Navigate to **Infrastructure > Events > Syslog Messages** > **Suppress Filter**, and on **Suppress Filter** page, select the filter and click **Edit**.
2. On **Configure Suppress Filter** page, clear **Enable Filter** check box to disable the filter.

Configure prune settings for instance events

March 11, 2024

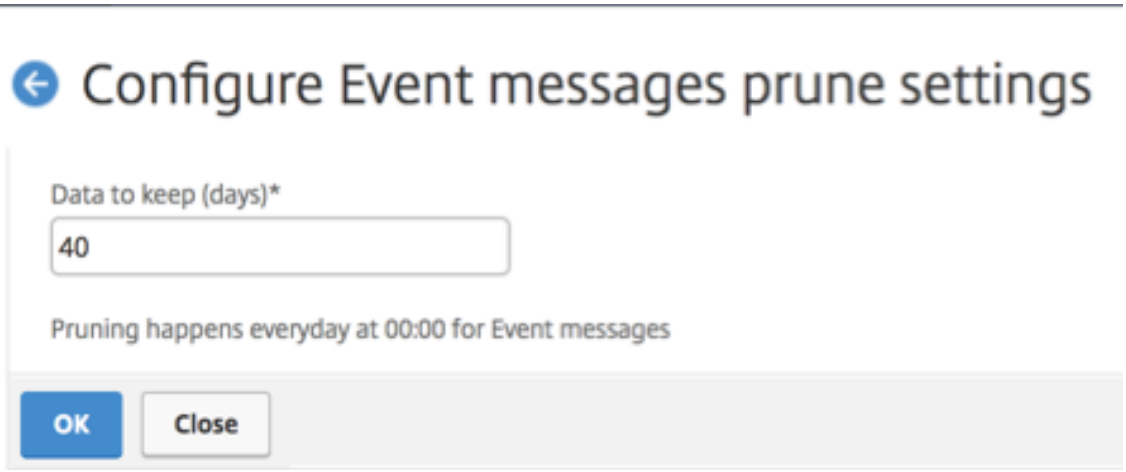
Citrix Application Delivery Controller (ADC) instances managed by your NetScaler Application Delivery Management (ADM) server send event messages data continuously to be stored on NetScaler ADM. You can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

> **Note**
>
> The value you can specify cannot exceed 40 days or be less than 1 day.

To configure prune settings for instance events:

1. Navigate to **System** > **System Administration**.

2. Under **Prune Settings**, click **Instance Events Prune Settings**.
3. Enter the time interval, in days, for which you want to retain data on the NetScaler ADM server and click **OK**.



Network functions

December 31, 2023

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix Application Delivery Controller (ADC) instances. You can view statistics such as transaction details, connection details, and throughput of a load balancing virtual server. You can also enable or disable the entities when you plan a maintenance.

The Network Functions dashboard provides you with the following graphs:

- Top 5 virtual servers with highest client connections
- Top 5 virtual servers with highest server connections
- Top 5 virtual servers with maximum throughput (MB/sec)
- Bottom 5 virtual servers with lowest throughput (MB/sec)
- Top 5 instances with most virtual servers
- State of the virtual servers
- Health of the load balancing virtual servers
- Protocols

Generate reports for load balancing entities

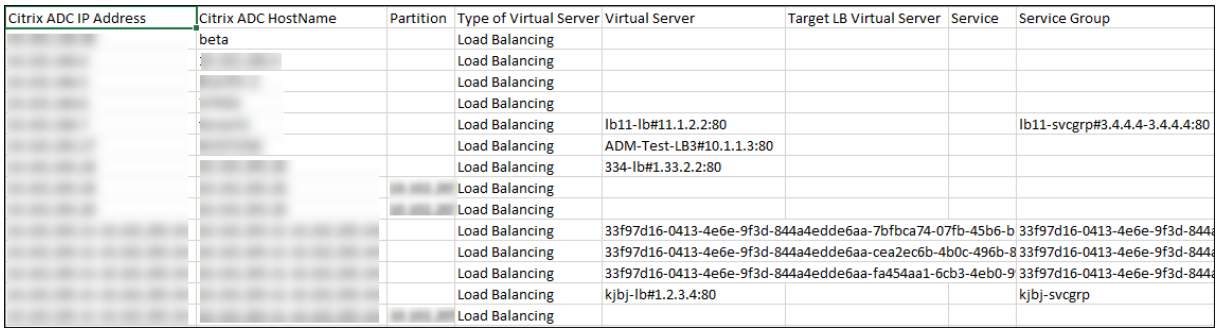
March 11, 2024

NetScaler Application Delivery Management (ADM) allows you to view the reports of Citrix Application Delivery Controller (ADC) instance entities at all levels. There are two types of reports that you can download in NetScaler ADM > Network Functions - consolidated reports and individual reports.

Consolidated reports: You can download and view a consolidated or a summarized report for all entities that are managed on NetScaler instances.

This report allows you to have a high-level view of the mapping between the NetScaler instances, partitions, and the corresponding load balancing entities (virtual servers, service groups, and services) that are present in the network.

The following image shows an example of a summarized report.



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

The consolidated report is in a CSV format. The entries in each column are described as follows:

- **NetScaler IP Address**: IP address of the NetScaler instance is displayed in the report
- **NetScaler HostName**: Host name is displayed in the report.
- **Partition**: IP address of the administrative partition is displayed
- **Virtual Server**: <name_of_the_virtual_server>#virtual_IP_address:port_number
- **Services**: <name_of_the_service>#service-IP_address:port_number
- **Service Groups**: <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_addr
  ……..,server_membern_IP_address:port

> **Note**
>
> - If there is no host name available, the corresponding IP address is displayed.
> - Blank columns indicate that the respective entities are not configured for that NetScaler instance.

Individual reports: You can also download and view independent reports of all instances and entities. For example, you can download a report for only load balancing virtual servers or load balancing services or load balancing service groups.

NetScaler ADM allows you to download the report instantly. You can also schedule the report to be generated at a fixed time once a day, once a week, or once a month.

Generate a combined load balancing report

1. In NetScaler ADM, navigate to **Infrasturcture > Network Funtions > Load Balancing.**
2. On **Load Balancing** page, click  .
3. On the **Export** page that opens, you have two options to view the report:
    a) Select **Export Now** tab and click **OK**.

    The consolidated report downloads to your system.

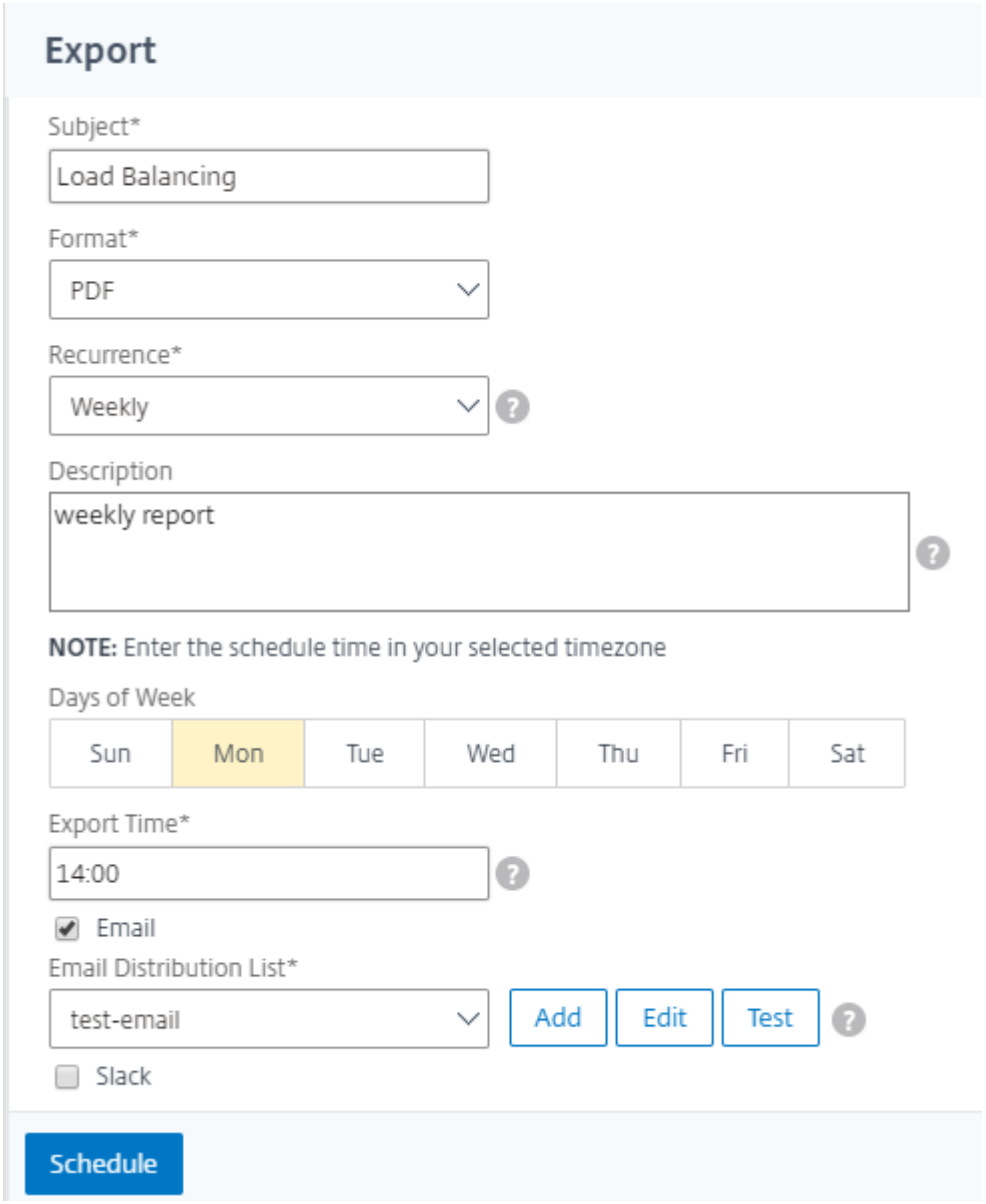
    b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

        i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

        ii. **Recurrence time** - Enter the time as Hour:Minute in 24-hour format.

        iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** to create an email profile.

> **Note**
>
> If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.



Note

If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

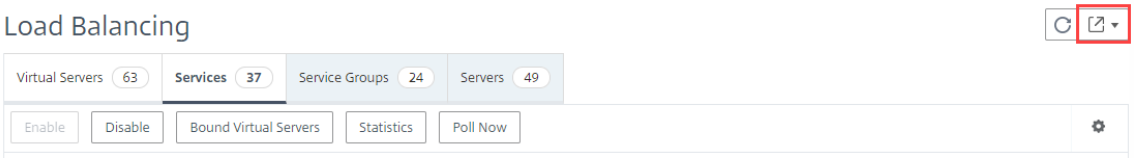
Generate an individual load balancing entity report

You can generate and export an individual report for a particular type of entity associated with the instances. For example, consider a scenario where you want to see a list of all load balancing services in the network.

1. In NetScaler ADM, navigate to **Infrasturcture > Network Funtions > Load Balancing > Ser-**

vices.

2. On **Services** page, click the **Export** button at the top right-hand corner.



   a) Select **Export Now** tab if you want to generate and view the report at this instant.

   b) Select **Schedule Export** to schedule generating and exporting of the report at regular intervals.

> **Note**
>
> You can only download the reports or export the reports as mail attachments. You cannot view the reports on the NetScaler ADM GUI.

Export or schedule export of network functions reports

March 11, 2024

You can generate a comprehensive report for selected network functions such as Load Balancing, Content Switching, Cache Redirection, Global Server Load Balancing (GSLB), Authentication, and NetScaler Gateway in NetScaler Application Delivery Management (ADM). This report allows you to have a high-level view of the mapping between the NetScaler instances, partitions, and the corresponding bound entities (virtual servers, service groups, and services) that are present in the network. You can export these reports in .csv file format.

The report displays the following virtual server data:

- NetScaler IP address
- Host name
- Partition data
- Virtual Server name
- Type of virtual server
- Virtual server
- Target LB virtual server

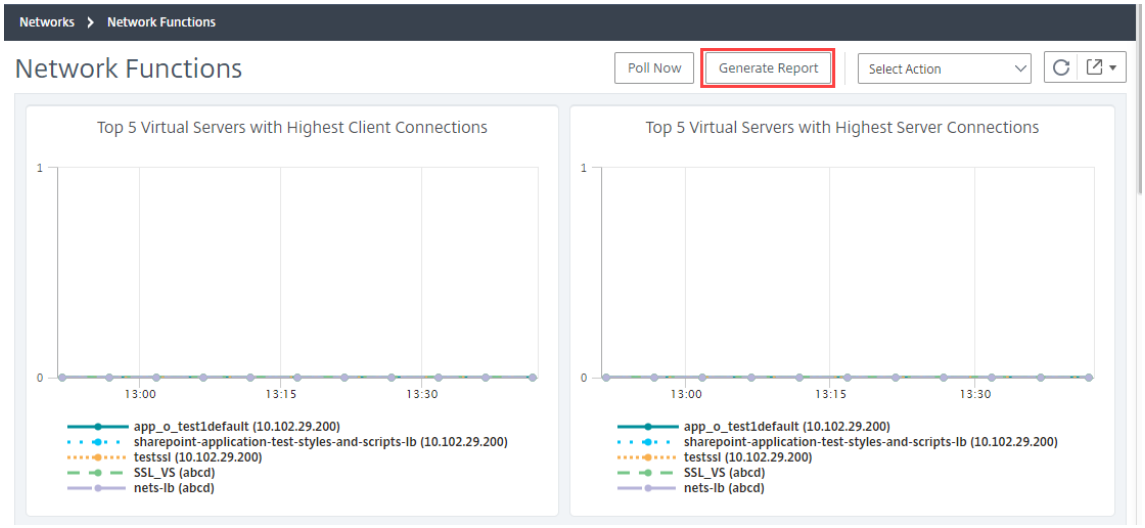
> **Note**
>
> For Content Switching and Cache Redirection virtual servers, the Target LB virtual server column lists all the LB servers, that is, both default servers and policy-based servers.
>
> - Service name
> - Service group name

You can schedule to export these reports to specified email addresses at different intervals.

> **Note**
>
> - For GSLB virtual servers, the network functions report displays only GSLB virtual servers and associated services.
> - For Content Switching and Cache Redirection virtual servers, the report displays only the bindings to the associated LB servers.
> - SSL virtual servers are not listed in this report because a separate list of SSL virtual servers is not maintained on NetScaler ADM.
> - When a new report is generated, the older reports are automatically purged from your account.
> - You cannot generate a network functions report for HAProxy.

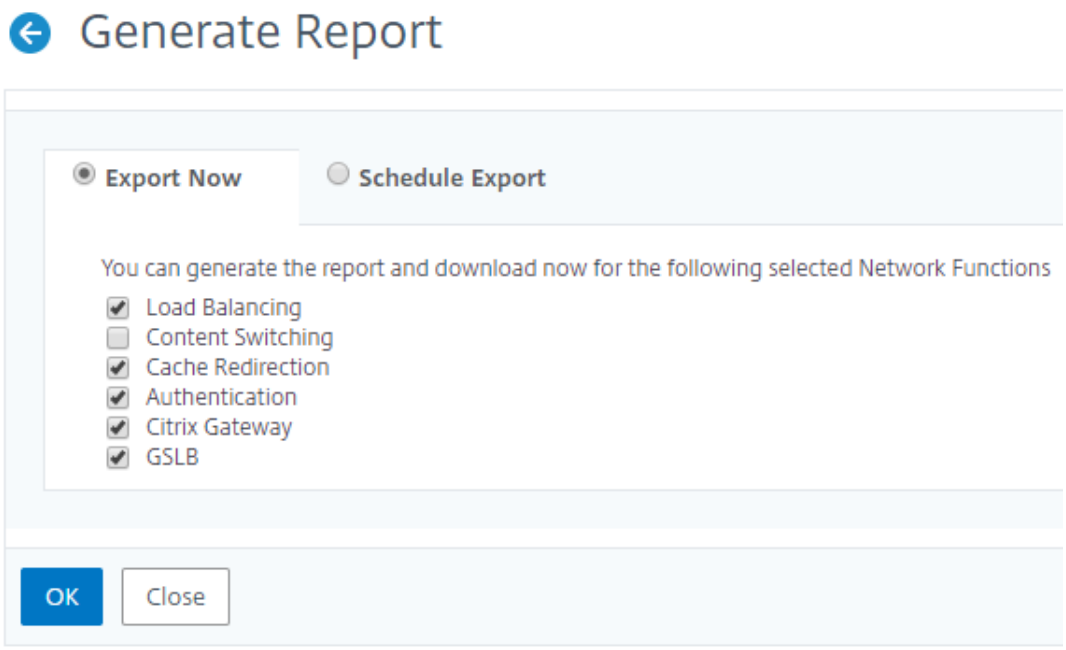
To export and schedule network functions reports:

1. Navigate to **Infrastructure > Network Functions**.
2. On the **Network Functions** page, in the right pane, click **Generate Report** at the top right corner of the page.



3. On the **Generate Report** page, you have the following 2 options:

a) Select **Export Now** tab and click **OK**. The report downloads to your system.



The following image shows an example of a network functions report.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.10	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

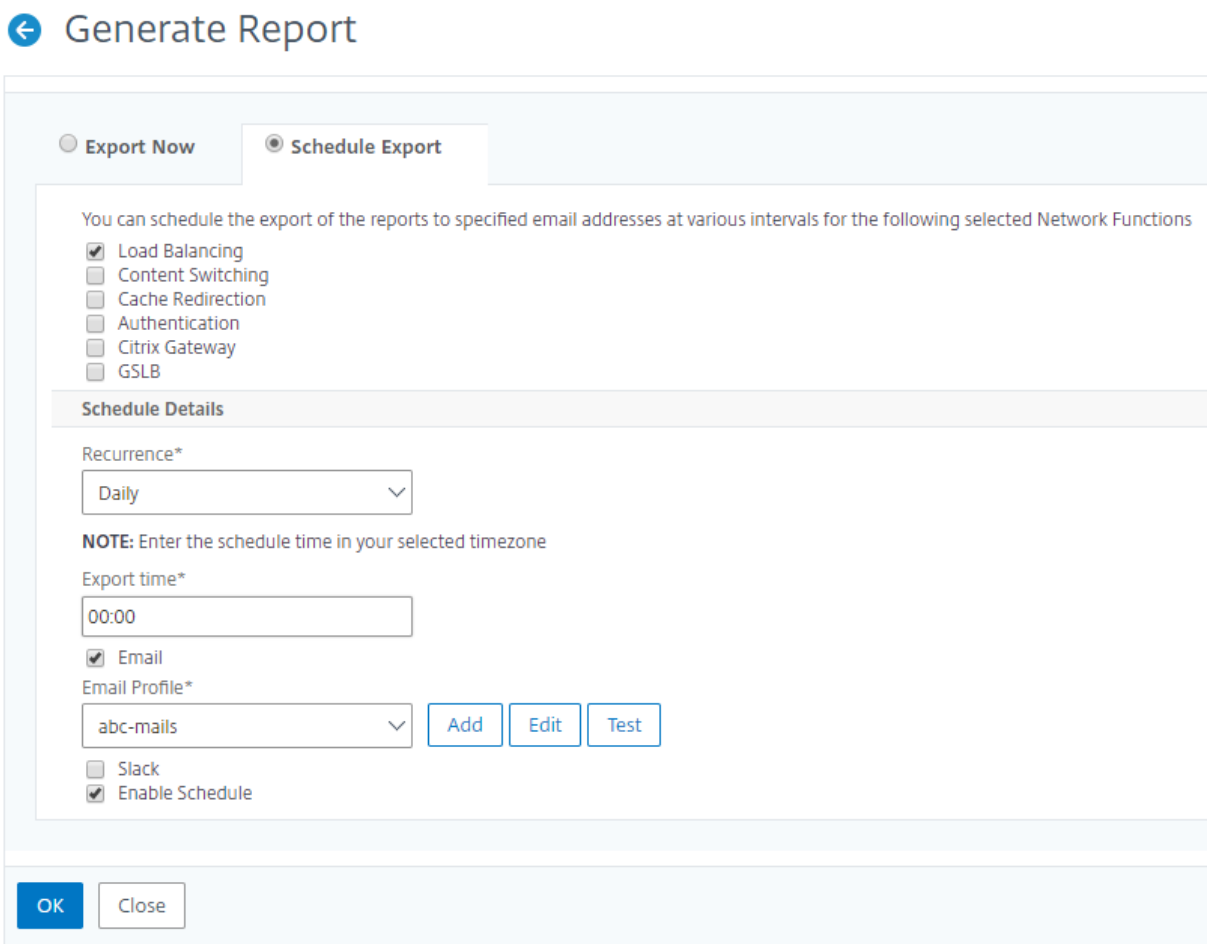
b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

   i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

   ii. **Recurrence time**- Enter the time as Hour: Minute in 24-hour format.

   iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** to create an email profile.

Click **Enable Schedule** to schedule your report and then, click **OK**. By clicking the **Enable Schedule** check box, you can generate the selected reports.



Network reporting

March 11, 2024

You can optimize resource usage by monitoring your network reporting on NetScaler Application Delivery Management (NetScaler ADM). You may have a distributed deployment with many applications deployed at multiple locations. To ensure optimal performance of your applications, you have also deployed multiple Citrix Application Delivery Controller (NetScaler) instances to load balance, content switch, or compress the traffic. Network performance can impact the application performance. To continue to maintain the performance of your applications, you must regularly monitor your network performance and make sure all resources are used optimally.

NetScaler ADM now allows you to generate reports not only for instances at a global level but also for entities such as the virtual servers and network interfaces. The instance family comprises NetScaler instances. The virtual servers for which you can generate reports are as follows:

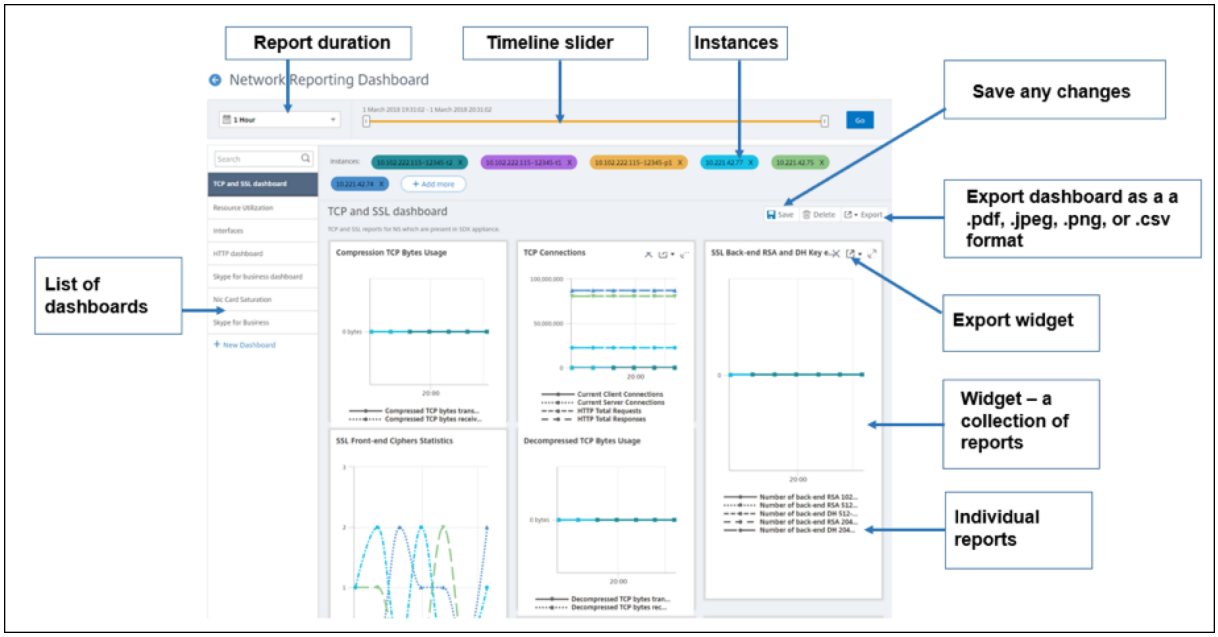
- Load balancing servers, services, and service groups

- Content switching servers
- Cache redirection servers
- Global service load balancing (GSLB)
- Authentication
- NetScaler Gateway

The network reporting dashboard in NetScaler ADM is a highly customizable. You can now create multiple dashboards for various instances, virtual servers, and other entities.

Network reporting dashboard

The following image calls out the various features in the dashboard:



- The left side panel lists all the custom dashboards that are created in NetScaler ADM. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each dashboard with multiple widgets to display various reports. A widget represents a report on the dashboard, that is a collection of more related reports. For example, a compression TCP Bytes Usage report contains reports for compressed TCP bytes transferred and received per second.
- You can display reports for one hour, one day, one week, or for one month. In addition, you can now use the timeline slider option to customize the duration of reports being generated on the NetScaler ADM.
- You can remove a report by clicking "X". You can also export the report as a .pdf, .jpeg, .png, or .csv format to your system. You can also schedule a time and recurrence of when the report

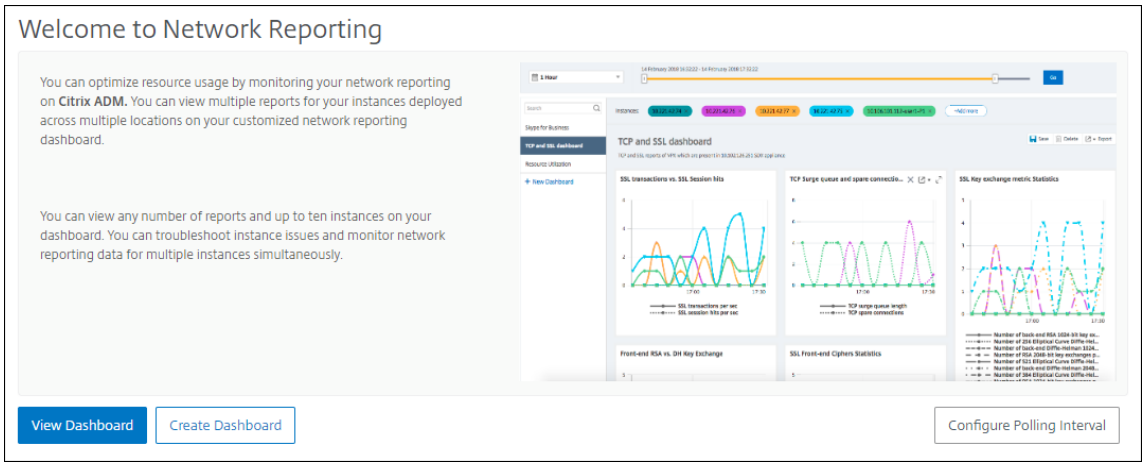
must be generated. You can also configure an email distribution list to which the reports must be sent.

- The Instances section at the top of the dashboard lists the IP addresses of all the instances for which the report is generated.
- You can either remove instances by clicking “X”or add more instances to the reports. But, currently NetScaler ADM allows you to view reports for 10 instances.
- You can also export the entire dashboard as a .pdf, .jpeg, .png, or .csv format to your system. Any changes made to the dashboard must be saved. Click Save to save the changes.

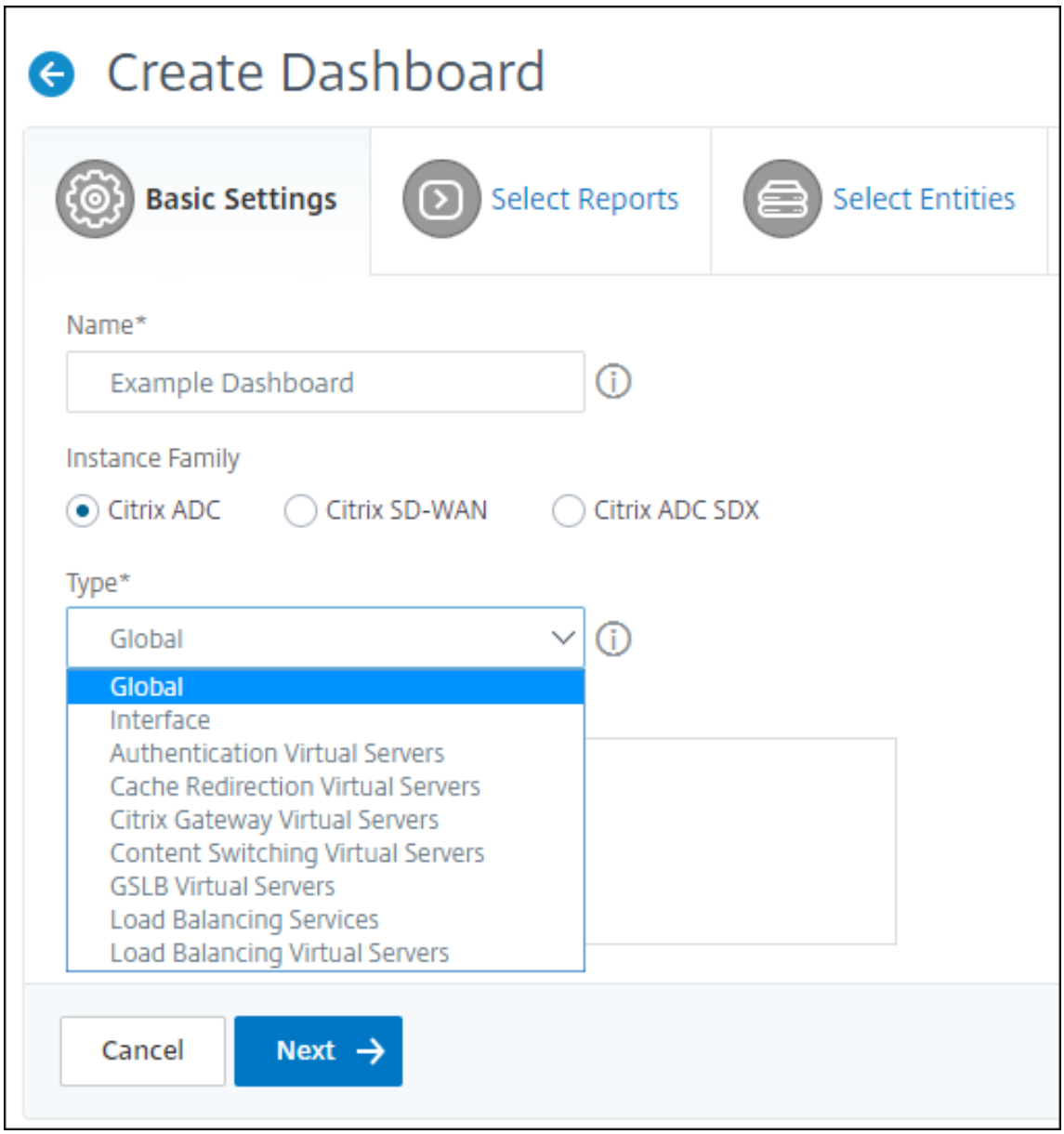
The following section explains in detail the tasks to create a dashboard, generate reports, and to export reports.

To view or to create a dashboard:

1. In NetScaler ADM, navigate to **Infrastructure > Network Reporting**.



2. To view the existing dashboards, click **View Dashboard**. The Network Reporting **Dashboard** page opens where you can view all your dashboards and report widgets.
3. To create a dashboard, click **New Dashboard**. The Create Dashboard page opens.



4. In the Basic Settings tab, enter the following details:

   a) **Name**. Type the name of the dashboard.

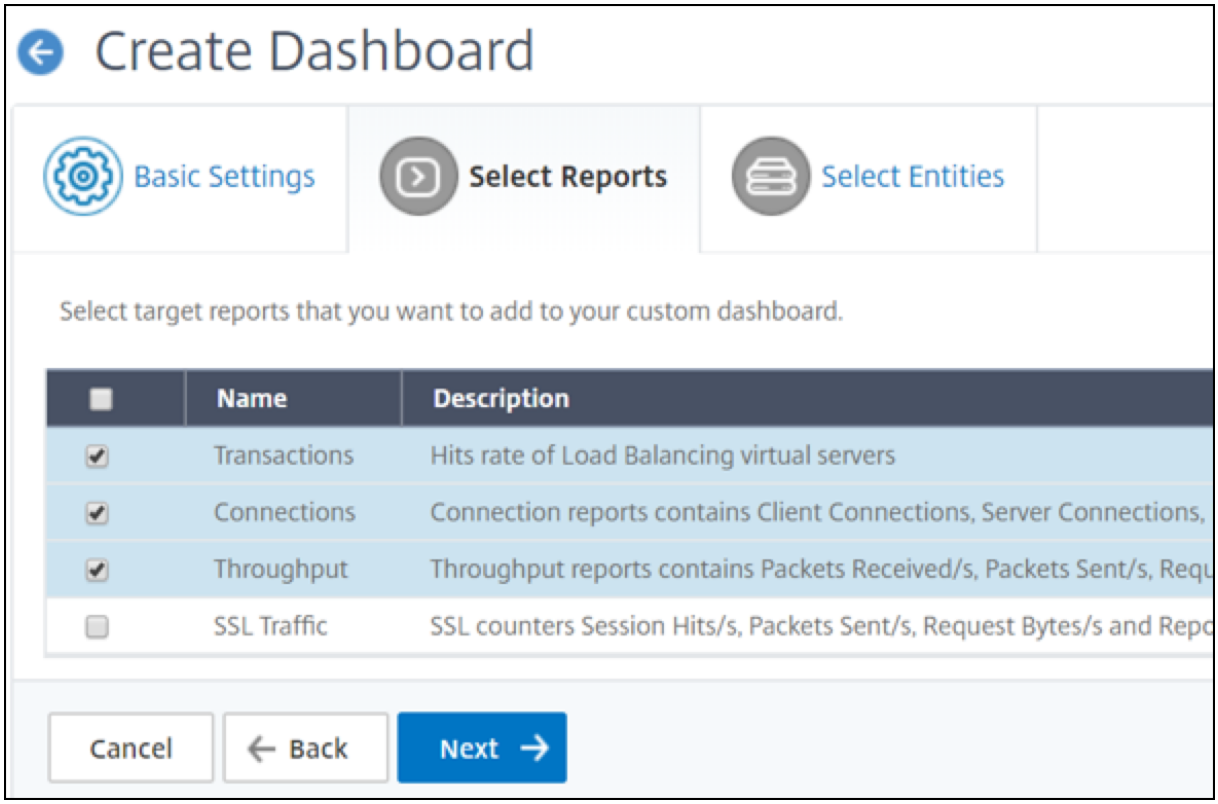
   b) **Instance Family**. Select the type of instance - NetScaler or NetScaler SDX.

   c) **Type**. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.

   d) **Description**. Type a meaningful description for the dashboard.

5. Click **Next**. All the supported reports for the instance and the specific entity appear.

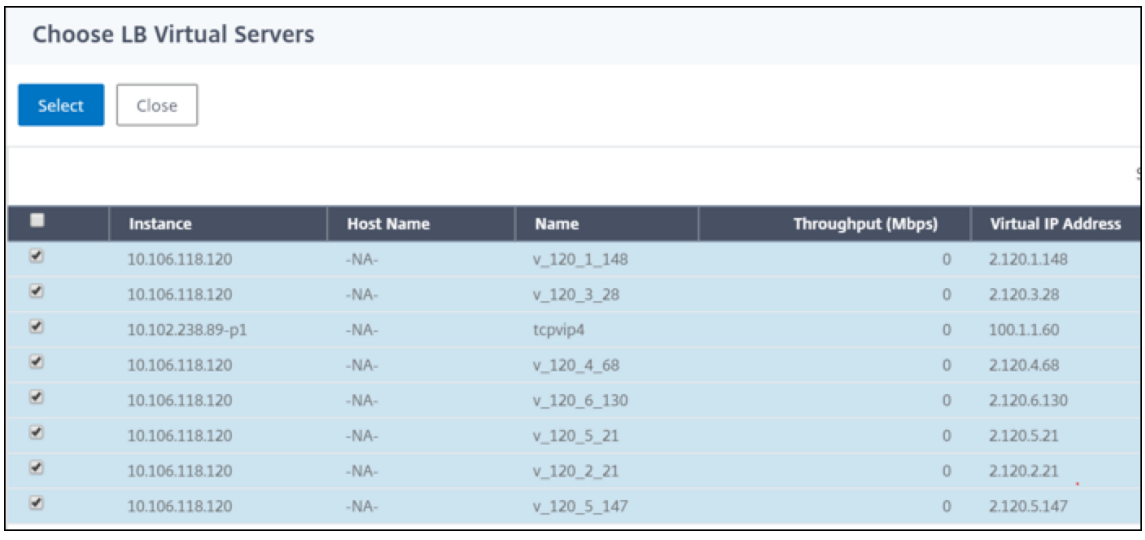
6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.



1. In the **Select Entities** tab, click **Add**.

   A window appears with the entities list depending on the selected entity type in the **Basic Settings** tab. In this example, **Choose LB Virtual Servers** window appears.

2. Select the entities that you want to monitor.



3. Click **Create**.

The dashboard is created and displays all the reports that you have selected.

> **Note**
>
> Currently, any changes that you make to legends or filters cannot be saved.

Exporting network reports

While you can export widget reports in .pdf, .png, .jpeg, or .csv formats, you can export the entire dashboards in only .pdf, .jpeg, or .png formats.

> **Note**
>
> You cannot export reports in NetScaler ADM if you have read-only permissions. You need an edit permission to be able to create a file in NetScaler ADM and to be able to export the file.

To export dashboard reports:

1. Navigate to **Infrastructure > Network Reporting**
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example, click **Dashboard 1**.
4. Click the export button at the top right corner of the page.
5. Under the **Export Now** tab, select the required format, and then click **Export**.

   On the **Export** page, you can do one of the following:
6. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
7. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or slack message.

   You can schedule an export of the **Network Reporting** dashboard page on a recurrent basis. For example, you can set an option to generate a dashboard report every week for the previous one hour at a particular time. The report is generated every week then and shows the status of the dashboard. The report overrides the time and date stamp, if set by the user.

> **Note**
>
> - if you select Weekly recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
> - If you select Monthly recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

While scheduling network reports, you can customize the heading of the report by entering a text string in the **Subject** field. The report created at the scheduled time has this string as its name.

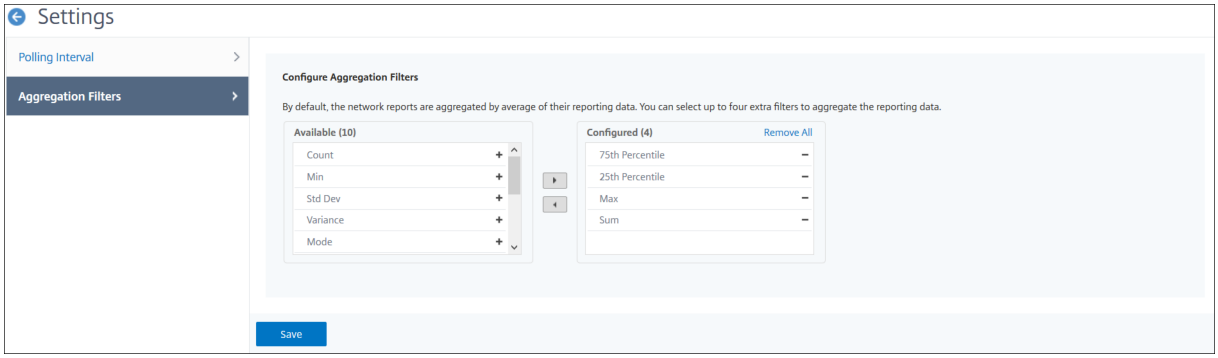
For example, for network reports originating from a particular virtual server, you can type in the subject as “authentication-reports-10.106.118.120,”where 10.106.118.120 is the IP address of the monitored virtual server.

> **Note**
>
> Currently, this option is available only when you schedule the export of reports. You cannot add a heading to the report when you export them instantly.

View network reporting data by applying aggregations

You can apply aggregations to the network performance data and view application performance on the dashboard. You can also export the results based on your requirement. Using these aggregations applied to the data, you can analyze and ensure if all resources are used optimally. Navigate to **Network > Network Reporting** and select the time duration 1 day or later to get the **View By** option.

In the existing average data, you can apply aggregations by selecting the option from the **View By** list. When you apply aggregation, the data is updated for each metric in the dashboard. Click **Settings** and select **Aggregation Filters**.



The following are the aggregations that you can add:

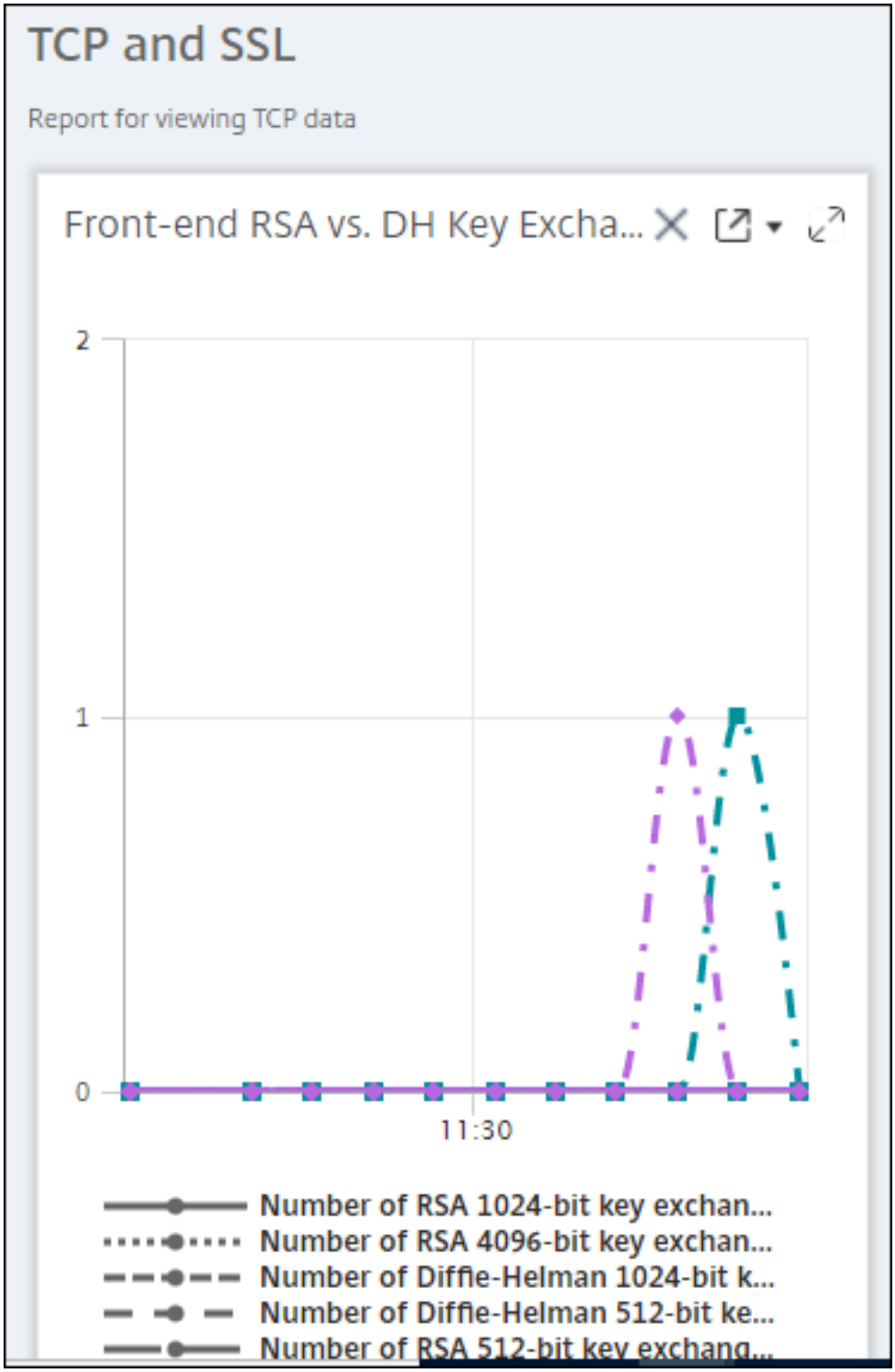
- Count
- Max
- Min
- Sum
- Std Dev
- Variance
- Mode
- Median
- 25th Percentile

- 75th Percentile
- 95th Percentile
- 99th Percentile
- First
- Last

You can add up to 4 aggregation options to the dashboard. After you add the aggregation options, NetScaler ADM takes approximately 1 hour to generate reports for the selected aggregation options.

To export widget reports:

1. Navigate to **Infrastructure > Network Reporting**.
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example also click **Skype for Business**.
4. Select a widget. For example, select **Load Balancing Virtual Server Transactions**.
5. Click the export button at the top right corner of the page
6. Under the **Export Now** tab, select the required format, and then click **Export**.



How to manage Thresholds for Network Reports on NetScaler ADM

To monitor the state of a NetScaler instance, you can set thresholds on counters and receive notifications when a threshold is exceeded. On NetScaler ADM, you can configure thresholds and view, edit, and delete them.

For example, you can receive an email notification when the Connections counter for a content switching virtual server reaches a specified value. You can define a threshold for a specific instance type. You can also choose the reports you want to generate for specific counter metrics from your chosen instance.

When the value of a counter exceeds or falls below (as specified by the rule) the threshold value, an event of the specified severity is generated to signify a performance-related issue. When the counter value returns to a value that you consider normal, the event is cleared. These events can be viewed by navigating to **Infrastructure > Events > Reports**. On the Reports page, you can click the **Events by Severity** donut to view events by their severity.

You can also associate an action with a threshold such as sending an email or SMS message when the threshold is breached.

To create a threshold:

1. In NetScaler ADM, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Threshold** page, specify the following details:
    - **Name**. Name of the threshold.
    - **Instance Type**. Choose NetScaler.
    - **Report Name**. Name of the performance report that provides information about this threshold.
3. You can also set rules to specify when an event is to be generated or cleared. You can specify the following details under the **Configure Rule** section:
    - **Metric**. Select the metric for which you want to set a threshold.
    - **Comparator**. Select a comparator to check whether the monitored value is greater than or equal to or less than or equal to the threshold value.
    - **Threshold Value**. Type the value for which the event severity is calculated. For example, you might want to generate an event with critical event severity if the monitored value for Current Client Connections reaches 80 percent. In this case, type 80 as the threshold value. You can view "critical severity"events by navigating to **Infrastructure > Events > Reports**. On the Reports page, you can click the **Events by Severity** donut to view events by their severity.

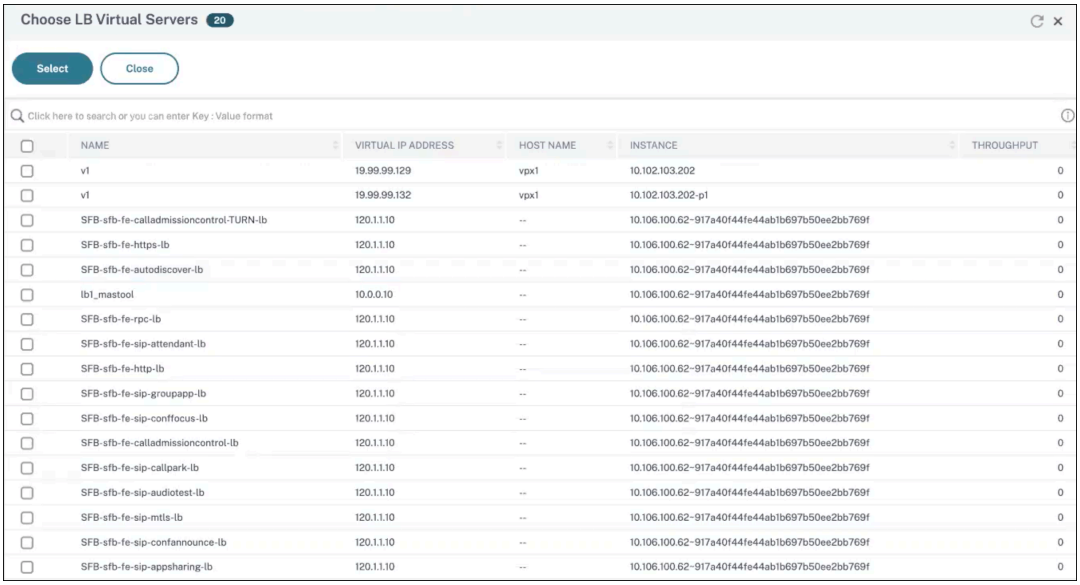
- **Clear Value**. Type the value that indicates when to clear the value. For example, you might want to clear the Current Client Connections threshold when the monitored value reaches 50 percent. In this case, type 50 as the clear value.
- **Event Severity**. Select the security level that you want to set for the threshold value.

4. You can choose instances and entities to be set with the threshold value. In the **Instances** section, choose one of the following options:

   - **All Instances**. The threshold is set for all the instances.
   - **Specific Instances**. The threshold is set for specific instances. Use the right arrow to move instances from the **Available** list to the **Configured** list. The threshold is set for the instances in the **Configured** list.
   - **Specific Entities**. The threshold is set for specific entities.

     Click **Add** to select the entities.

     A window appears with the entities list depending on the selected report type in the **Report Name** field. In this example, the **Choose LB Virtual Servers** window appears.



     Select the entities for which you want to set a threshold. Click **Select**. The selected entities appear in the **Instances** section.

     > **Note**
     >
     > The **Specific Entities** option appear only if you select vserver based reports in **Report Name**. For example, if you select **LB Service Statistics**

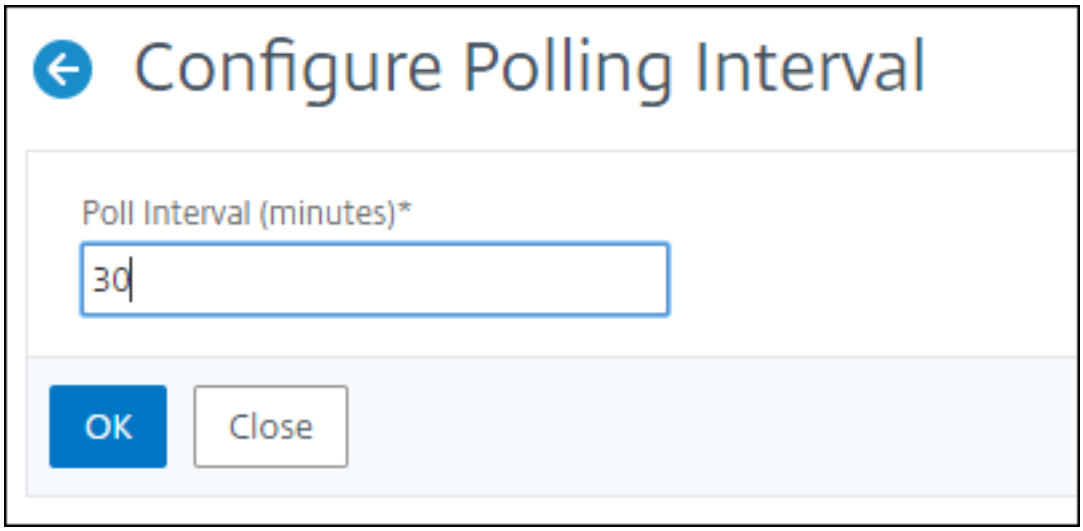
5. You can also add an **Event Message**. Type a message that you want to appear when the threshold is reached. NetScaler ADM appends the monitored value and the threshold value to this message.

6. Select **Enable** to enable the threshold to generate alarms.
7. Optionally, you can configure **Actions** such as email or Slack notifications or both email and Slack notifications.
8. Click **Create**.

Set Performance Polling Interval for Network Reports

By default, every 5 minutes, NITRO calls collect performance data for network reporting. ADM retrieves instance statistics such as counter information and aggregates them based on per minute, per hour, per day, or per week. You can view this aggregated data in predefined reports.

To set the performance polling interval, navigate to **Infrasturcture > Network Reporting** and click **Configure Polling Interval**. Your polling interval cannot be less than 5 minutes or more than 60 minutes.



Configuring Network Reporting Prune Settings

You can configure the purge interval of network reporting data in NetScaler ADM. This setting limits the amount of network reporting data being stored in the NetScaler ADM server's database. By default, pruning happens every 24 hours (at 01.00 hours) for the network reporting historical data.

> **Note**
>
> The value that you can specify cannot exceed 30 days or be less than 1 day.

Configuration jobs

March 11, 2024

NetScaler Application Delivery Management (NetScaler ADM) configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple Citrix Application Delivery Controller (ADC) instances in the network.

NetScaler ADM allows you to create configuration jobs that help you to perform all these activities with ease on several devices as a single task. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on NetScaler ADM. A configuration job contains a set of configuration commands that you can run on one or multiple managed devices.

Configuration Jobs can either use SSH commands to do configuration commands or use SCP to do file copy from either locally or to another appliance, for example, we can schedule a HA-failover or HA-upgrade.

You can create a configuration job by using one of the following four options in NetScaler ADM. Use one of these to create a reusable source of commands and instructions to the system to run a configuration job.

1. Configuration Template
2. Instance
3. File
4. Record and Play

Configuration Template

You can create configuration templates while creating a job and saving a set of configuration commands as a template. When you save these templates on the Create Jobs page, they are automatically displayed on the Create Template page.

> **Note**
> The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

You can use one of the following templates:

Configuration Editor: You can use the configuration editor to type in CLI commands, save the configuration as a template, and use it to configure jobs.

Inbuilt Template: You can choose from a list of configuration templates. These templates provide the syntaxes of the CLI commands and allow you to specify values for the variables. The inbuilt templates are listed, with their descriptions in the table below. You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can also, choose to run the job immediately or schedule the job to be run at a later stage.

Instance

You can perform a single-bundle upgrade of your NetScaler SDX instances running NetScaler release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in NetScaler ADM. You can also upgrade a NetScaler instance by extracting the running configuration or a saved configuration and running the commands on another NetScaler instance of the same type. This allows you to replicate the configuration of one instance on the other.

File

You can upload a configuration file from your local machine and create jobs.

Advantages of using a file

- You can use any text file to create a reusable source of configuration commands.
- Any kind of formatting is not required.
- The file can be saved on your local machine.

You can either create and save a new file or import an existing file, and run the commands.

Record and Play

Using Create job you can either enter your own CLI commands, or you can use the record and play button to get commands from a NetScaler session. When you run the job, changes in the ns.conf on the selected instance are recorded and copied to NetScaler ADM.

Related Articles

- How to Use SCP (put) Command in Configuration Jobs
- How to Use Variables in Configuration Jobs
- How to Create Configuration Jobs from Corrective Commands

- How to Use Configuration Templates to Create Audit Templates
- How to Use Record-and-Play to Create Configuration Jobs
- How to Use the Master Configuration Template on NetScaler ADM

Create a configuration job

March 11, 2024

A job is a set of configuration commands that you can create and run on one or more multiple managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler Application Delivery Management (ADM) GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of NetScaler ADM to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on NetScaler ADM:

1. Navigate to the **Infrastructure > Configuration Jobs**.
2. Click **Create Job**.
3. On the **Create Job** page, under the **Select Configuration** tab, specify the Job Name and select the **Instance Type** from the list.
4. In the **Configuration Source** list, select the configuration job template that you want to create. Add the commands for the selected template.
    - You can either enter the commands or import the existing commands from the saved configuration templates.
    - You can also add multiple templates of different types in the Configuration editor while creating a job in the Configuration Jobs.
    - From the **Configuration Source** list, select the different templates and then drag the templates into the configuration editor. The template types can be **Configuration Template**, **In built Template**, **Master Configuration**, **Record and Play**, **Instance** and **File**.

    > **Note**
    >
    > If you add the `Deploy Master Configuration Job` template for the first time, add a template of different type, then the whole job template becomes a `Master Configuration` type.

You can also rearrange and reorder the commands in the configuration editor. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing the command line number in the text box. You can also rearrange and reorder the command line while editing the configuration job.

You can define variables that enable you to assign different values for these parameters or run a job across multiple instances. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view. Click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

You can customize rollback commands for every command on the configuration editor. To specify your customized commands, Enable the custom rollback option.

> **Important**
>
> For custom rollback to take effect, complete the **Create Job** wizard. And in the **Execute** tab, select the **Rollback Successful Commands** option from the **On Command Failure** list.

5. In the **Select Instances** tab, select the instances on which you want to run the configuration audit.

   a) In a NetScaler high-availability pair, you can run a configuration job local to a primary or a secondary node. Select on which node you want to run the job.

      - **Execute on primary nodes** - Select this option to run the job only on primary nodes.
      - **Execute on secondary nodes** - Select this option to run the job only on secondary nodes.

      You can also choose both primary and secondary node to run the same configuration job. If you do not select either primary or secondary node, automatically the configuration job runs on the primary node.

6. In the **Specify Variable Values** tab, you have two options:

   a) Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler ADM server.

   b) Enter common values for the variables that you have defined for all instances

   c) Click **Next**.

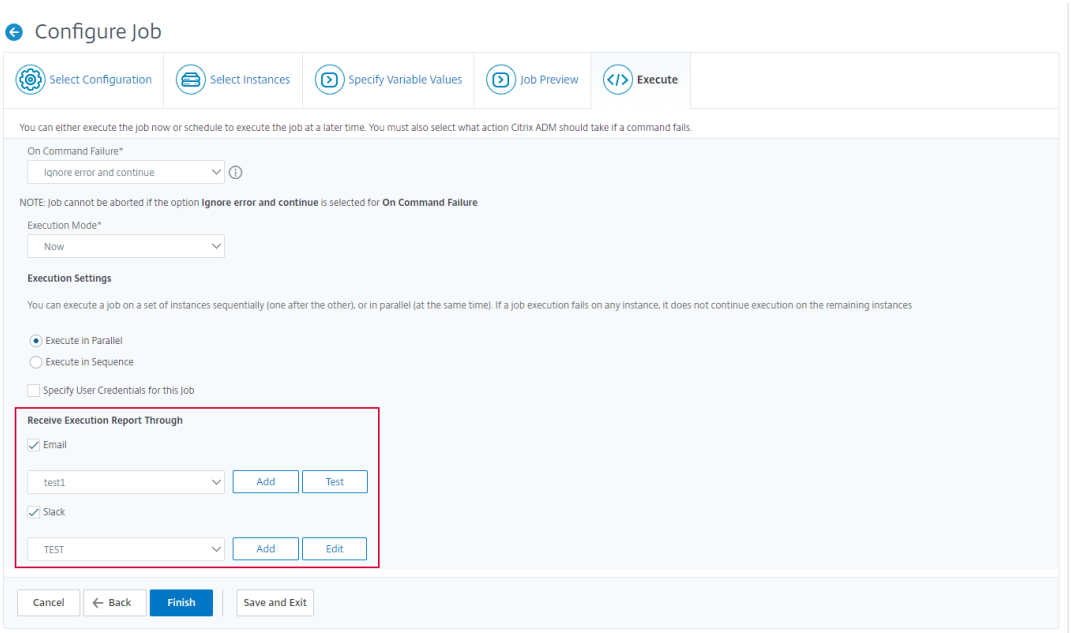
To send an email and Slack notification for a job:

An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

1. Navigate to **Infrastructure > Configuration Jobs**.
2. Select the job that you want to enable email and Slack notification and click **Edit**.
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

     If you want to add an email distribution list, click **Add** and specify the email server details.
   - Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

     If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.



4. Click **Finish**.

To send an email and Slack notification for a job:

An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

1. Navigate to **Infrastructure > Configuration Jobs**.
2. Select the job that you want to enable email and Slack notification and click **Edit**.
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

If you want to add an email distribution list, click **Add** and specify the email server details.

- Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

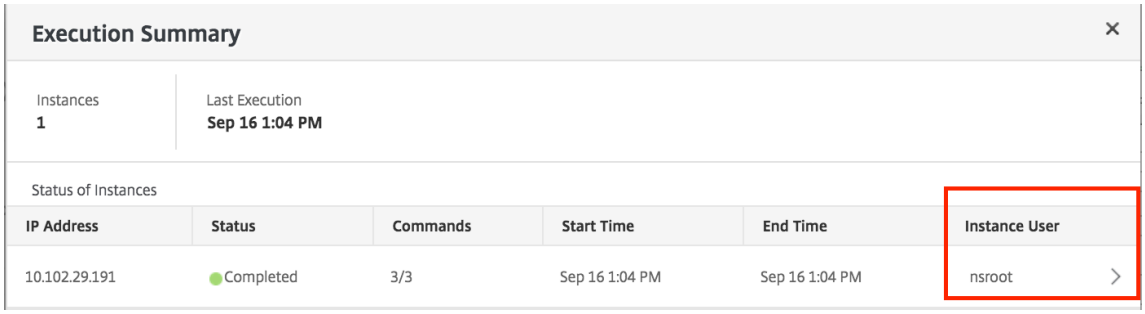
  If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.

4. Click **Finish**.

To view execution summary details:

1. Navigate to **Infrastructure > Configuration Jobs**.
2. Select the job that you want to view the execution summary and click **Details**.
3. Click **Execution Summary** to see:

   - The status of the instance on that run the job
   - The commands run on the job
   - The start and end time of the job, and
   - The instance user's name



Configuration audit

December 31, 2023

This document includes:

- Creating Audit Templates
- Viewing Audit Reports
- Audit Configuration Changes Across Instances
- Get Configuration Advice on Network Configuration
- How to Poll Configuration Audit of NetScaler Instances

Upgrade jobs

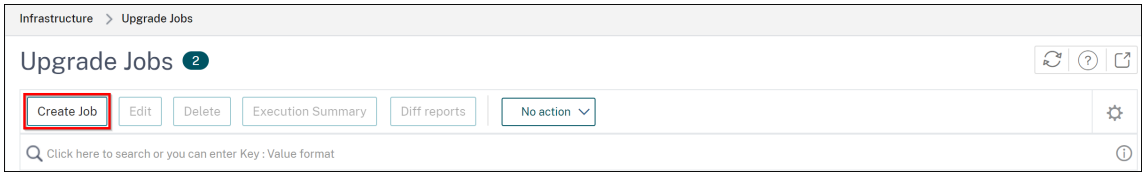
March 11, 2024

You can create the following maintenance tasks using NetScaler ADM. You can then schedule the maintenance tasks at a specific date and time.

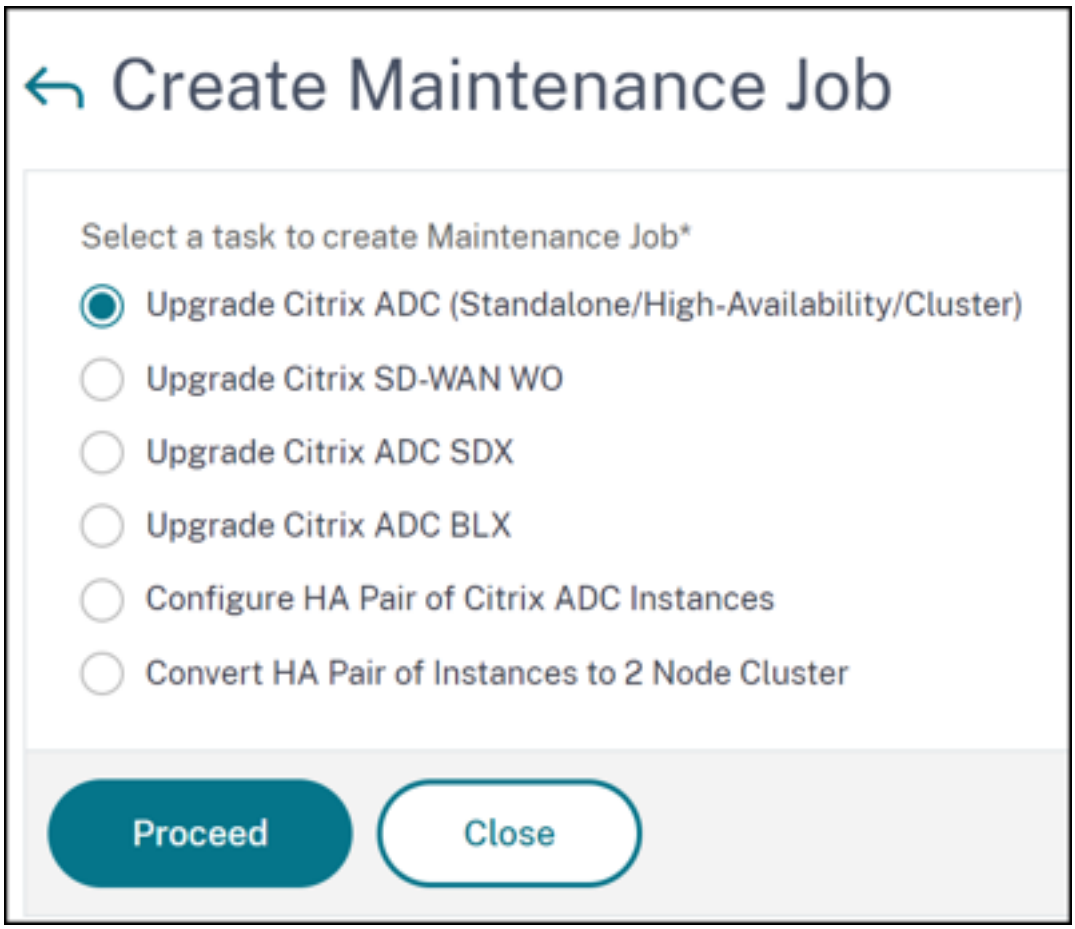
- Upgrade NetScaler instances
- Upgrade NetScaler SDX instances
- Upgrade NetScaler BLX instances
- Upgrade NetScaler instances in the Autoscale Group
- Configure HA pair of NetScaler instances
- Convert HA pair of instances to Cluster

Schedule upgrading of NetScaler instances

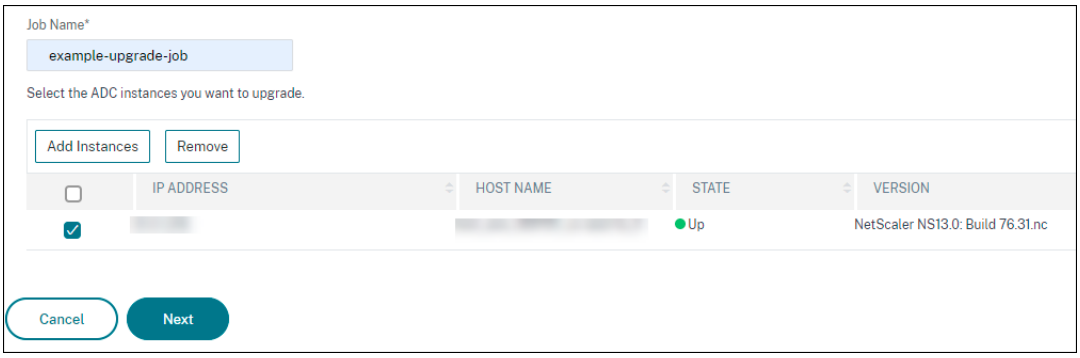
1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.



2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/Cluster)** and click **Proceed**.



3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add ADC instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.



5. Click **Next** to select the image. Select one of the following options from the **Software Image** list:

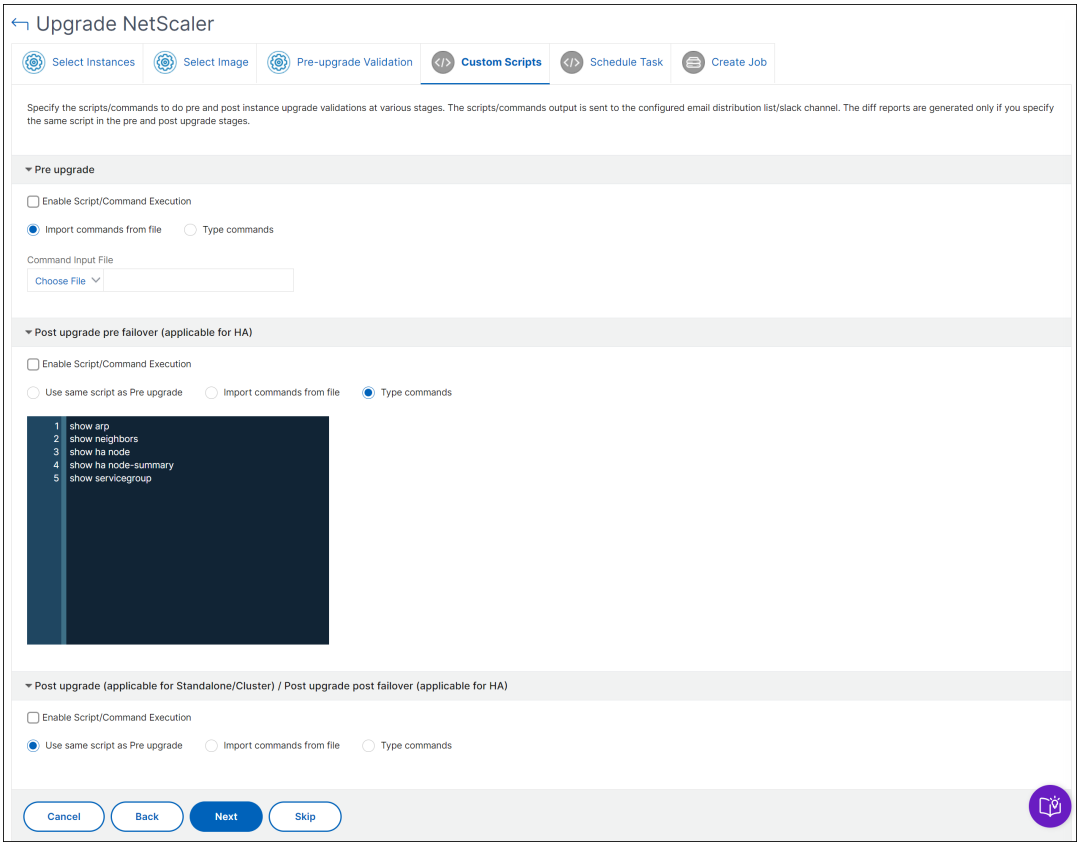
- **Local** - Select the instance upgrade file from your local machine.
- **Appliance** - Select the instance upgrade file from NetScaler ADM file browser. The NetScaler ADM GUI displays the instance files that are present at `/var/mps/mps_images`.
  - **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.
  - **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.

6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **Important**
   >
   > If you specify cluster IP address, NetScaler ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:
   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.



You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. Click **Next**. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an ADC HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

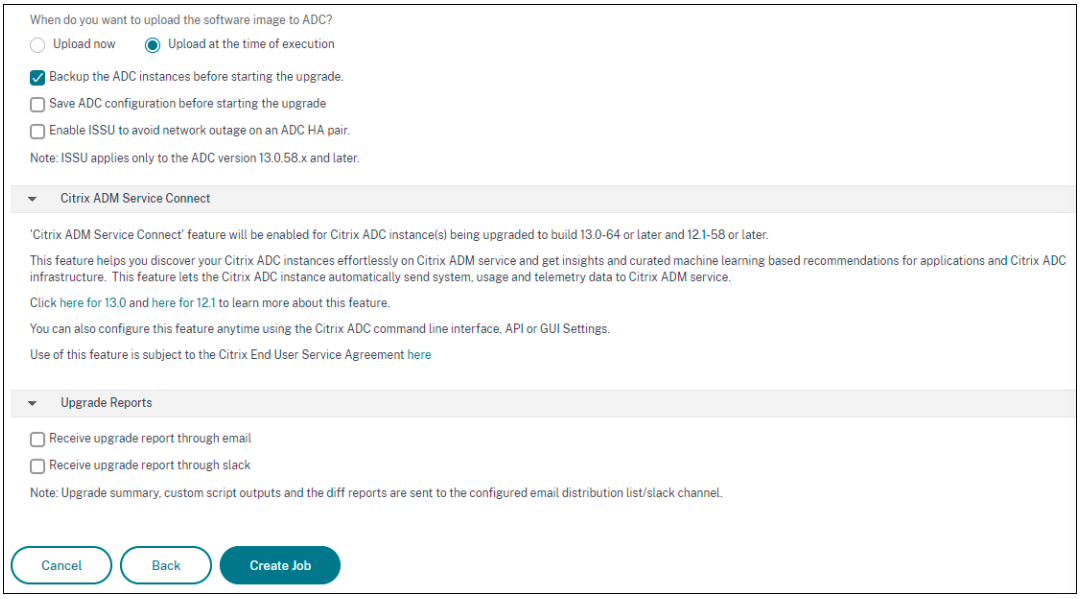
     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. Click **Next**. In **Create Job**, specify the following details:

    a) Specify when you want to upload the image to an instance:

    - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
    - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
    - **Backup the ADC instances before starting the upgrade.** - Creates a backup of the selected ADC instances.
    - **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
    - **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

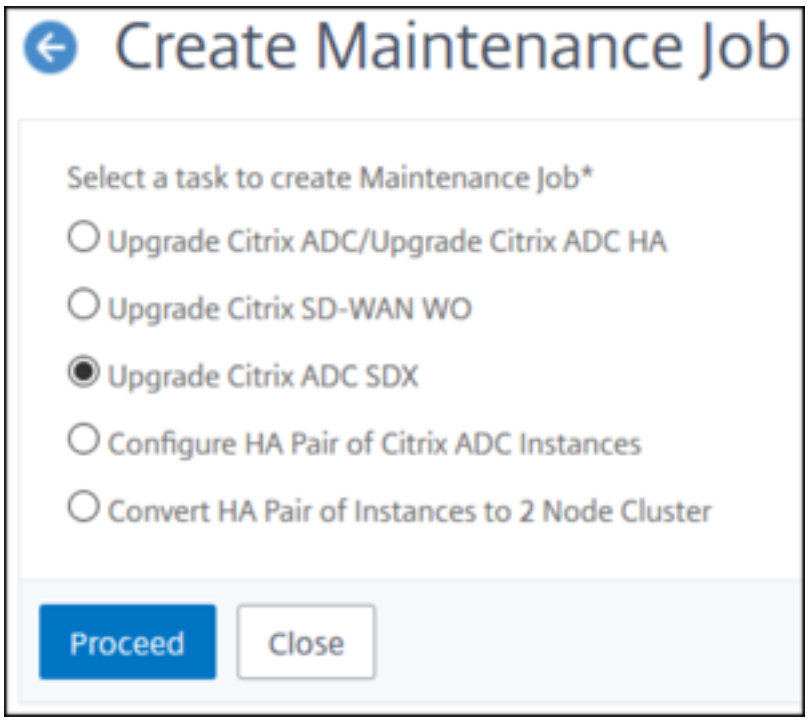
- **NetScaler ADM Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler ADM Service Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using NetScaler ADM service connect.
- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.



10. Click **Create Job**.

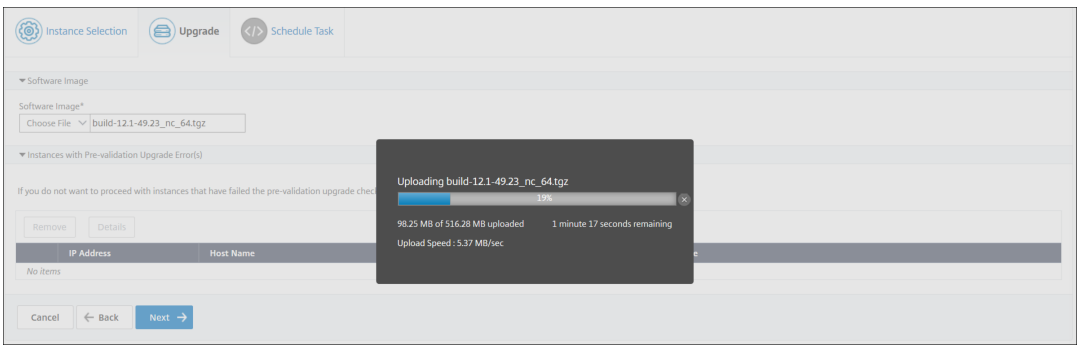
Schedule upgrading of NetScaler SDX instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade NetScaler SDX** and click **Proceed**.



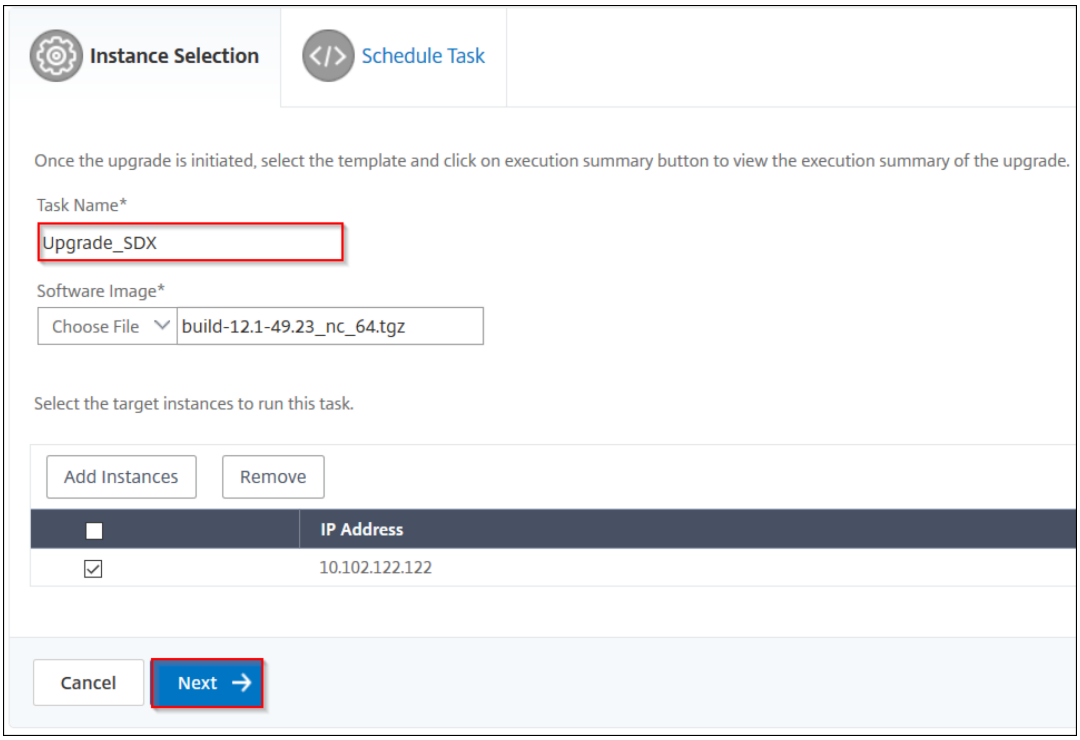
3. On the **Upgrade NetScaler SDX** page, in the **Instance Selection** tab:
   a) Add a **Task Name**.
   b) From the **Software Image** list, select either **Local** (your local machine) or **Appliance** (the build file must be present on NetScaler ADM virtual appliance).

      The upload process begins.

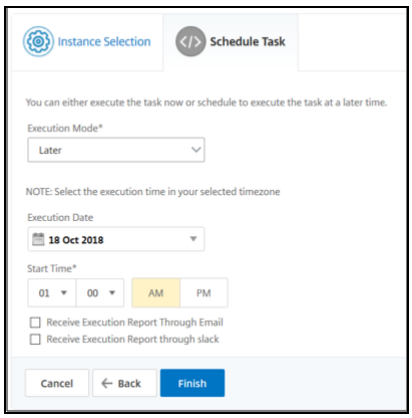


   c) Add the NetScaler SDX instances on which you want to run the upgrade process.

d) Click **Next**.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler SDX instance now, and click **Finish**.
5. To upgrade a NetScaler SDX instance later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the NetScaler instance, and click **Finish**

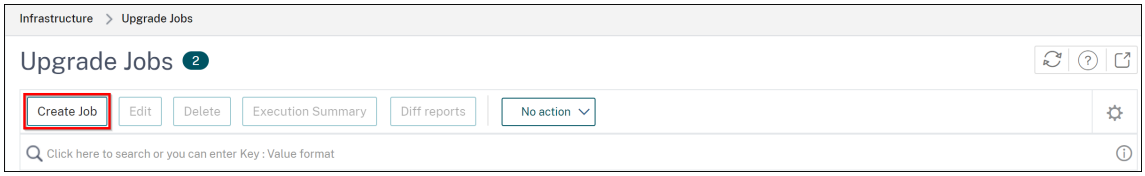


6. You can also enable email and slack notifications to receive the execution report of the upgrading NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

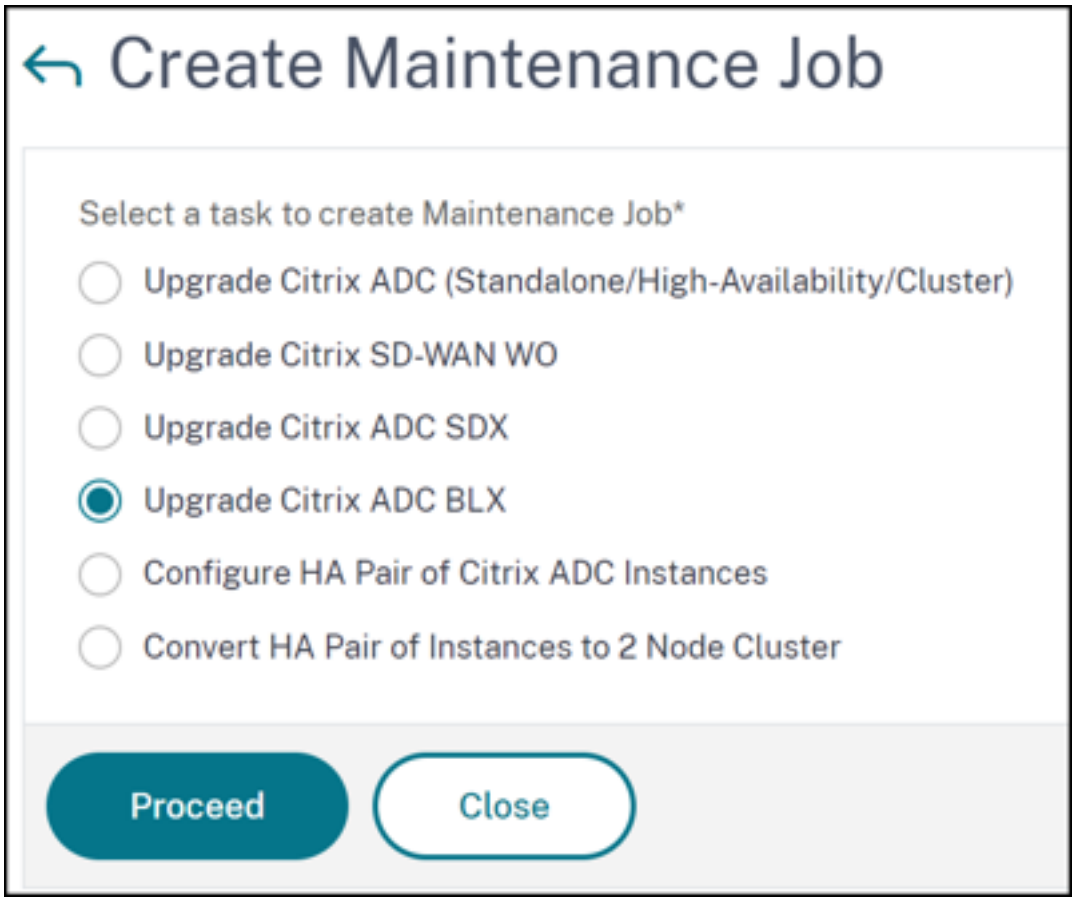
   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Schedule upgrading of NetScaler BLX instances

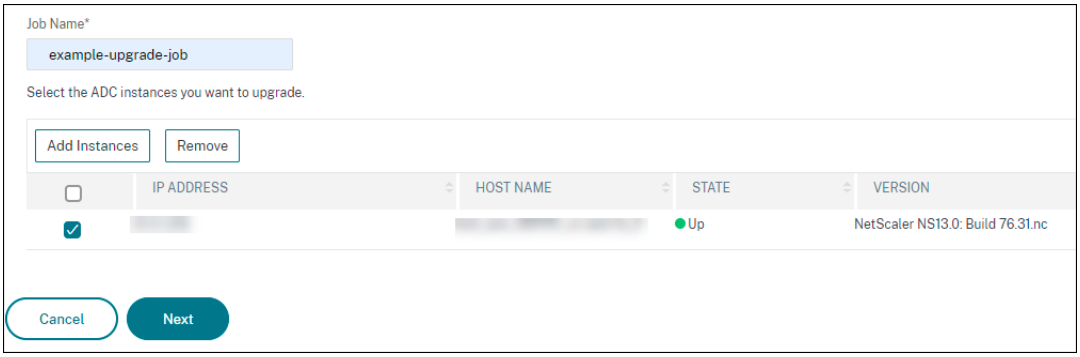
1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.



2. In **Create Maintenance Jobs**, select **Upgrade NetScaler BLX** and click **Proceed**.

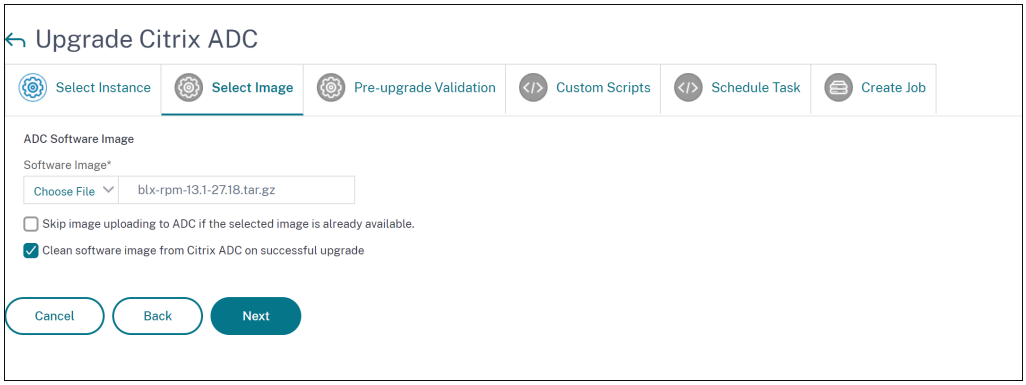


3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add the BLX instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.



5. Click **Next** to select the image. elect one of the following options from the **Software Image** list:

   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from NetScaler ADM file browser. The NetScaler ADM GUI displays the instance files that are present at `/var/mps/mps_images`.
     - **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.
     - **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.



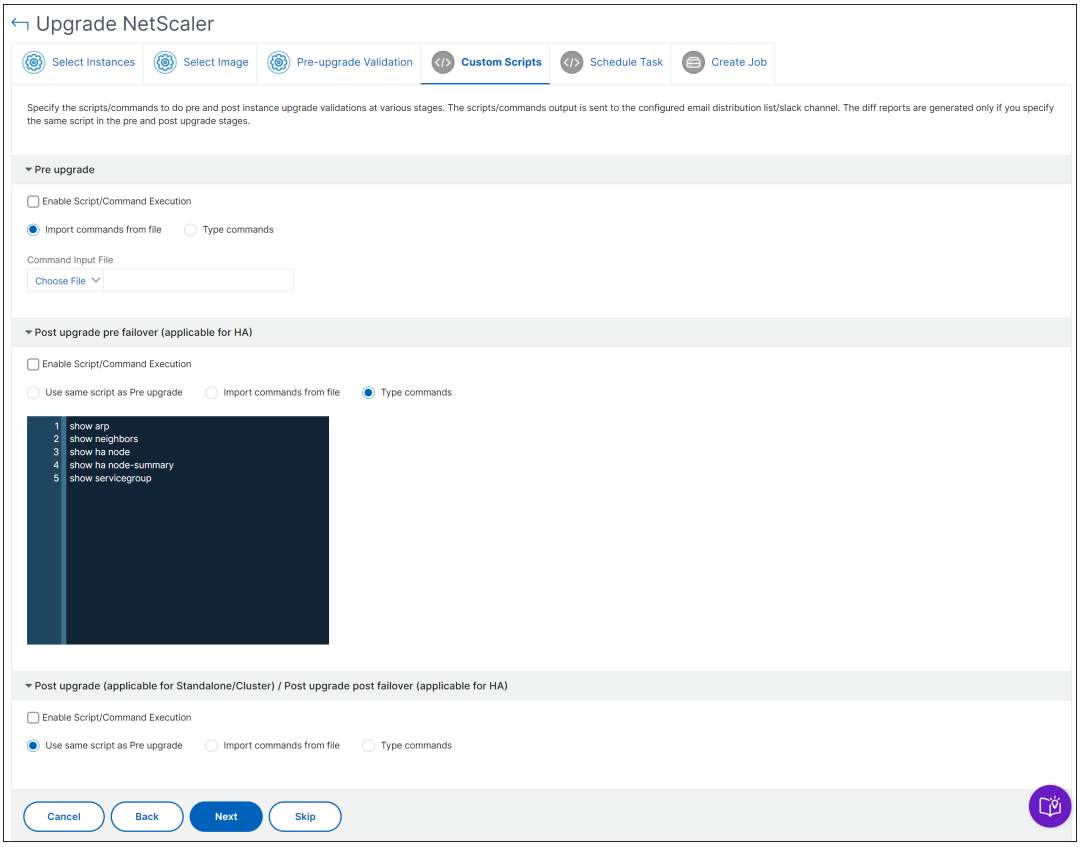
6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **Important**
   >
   > If you specify cluster IP address, NetScaler ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

- **Import commands from file** - Select the command input file from your local computer.
- **Type commands** - Enter commands directly on the GUI.



You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. Click **Next**. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

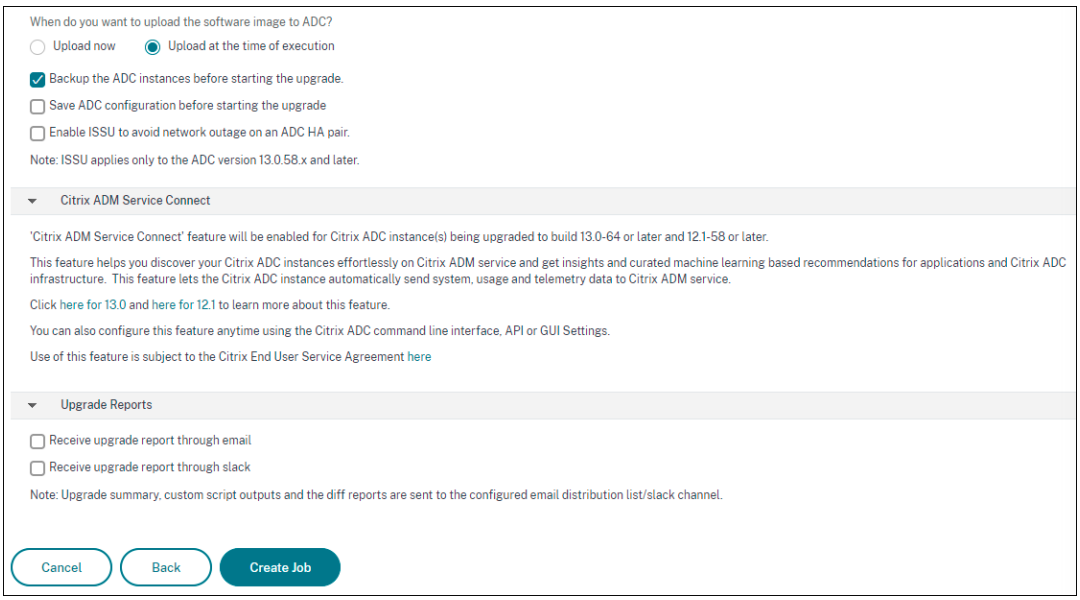
Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. Click **Next**. In **Create Job**, specify the following details:

   a) Specify when you want to upload the image to an instance:

      - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
      - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
      - **Backup the ADC instances before starting the upgrade** - Creates a backup of the selected ADC instances.
      - **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
      - **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

   - **NetScaler ADM Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler ADM Service Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using NetScaler ADM service connect.
   - **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
   - **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.



10. Click **Create Job**.

Schedule upgrading Autoscale group

Perform the following steps to upgrade all the instances in the cloud services that are part of the Autoscale group:

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade Autoscale Group** and click **Proceed**.
3. In the **Upgrade Settings** tab:
   a) Select the **Autoscale Group** that you want to upgrade.
   b) In **Image**, select the NetScaler version. This image is the existing version of NetScaler instances in the Autoscale group.
   c) In **NetScaler Image**, browse the NetScaler version file to which you want to upgrade.

      If you check **Graceful Upgrade**, the upgrade task waits until the specified drain connection period to expire.
   d) Click **Next**.
4. In the **Schedule Task** tab:
   a) Select one of the following from the Execution Mode list:
      - **Now:**To start the NetScaler instances upgrade immediately.
      - **Later:** To start the NetScaler instances upgrade at later time.

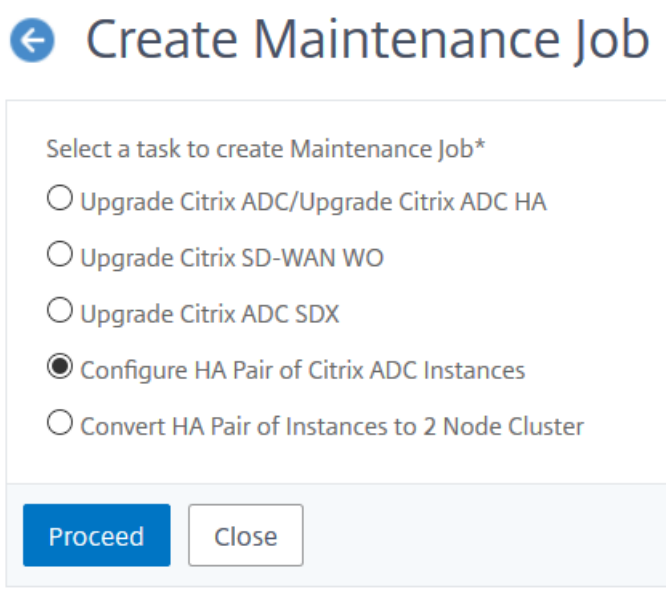
b) If you select the **Later** option, select the Execution Date and Start Time when you want to start the upgrade task.

You can also enable email and slack notifications to receive the execution report of the upgrading Autoscale group. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

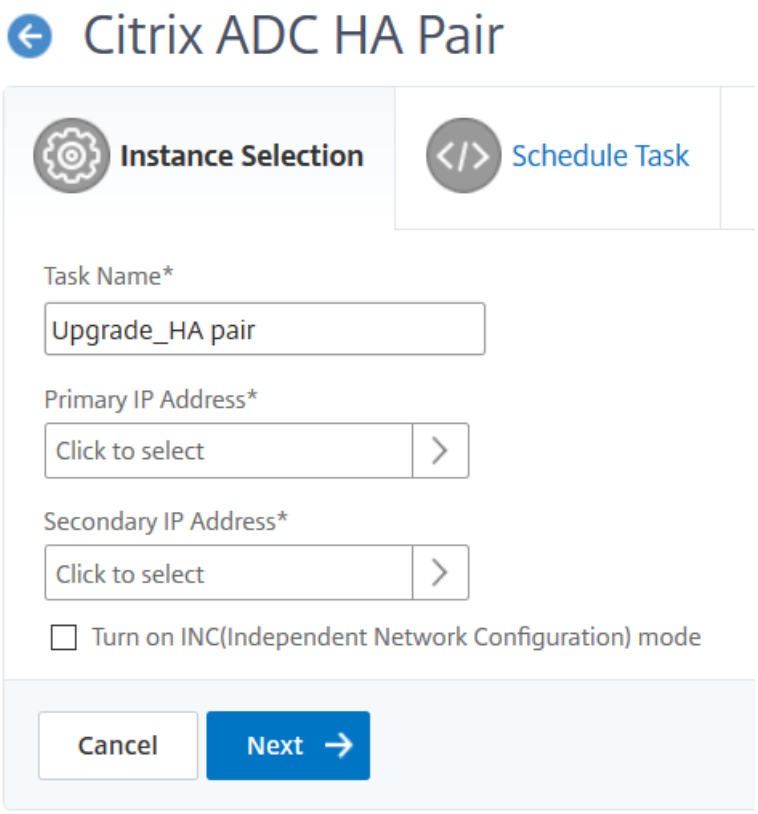
5. Click **Finish**.

Schedule configuring HA pair of NetScaler instances

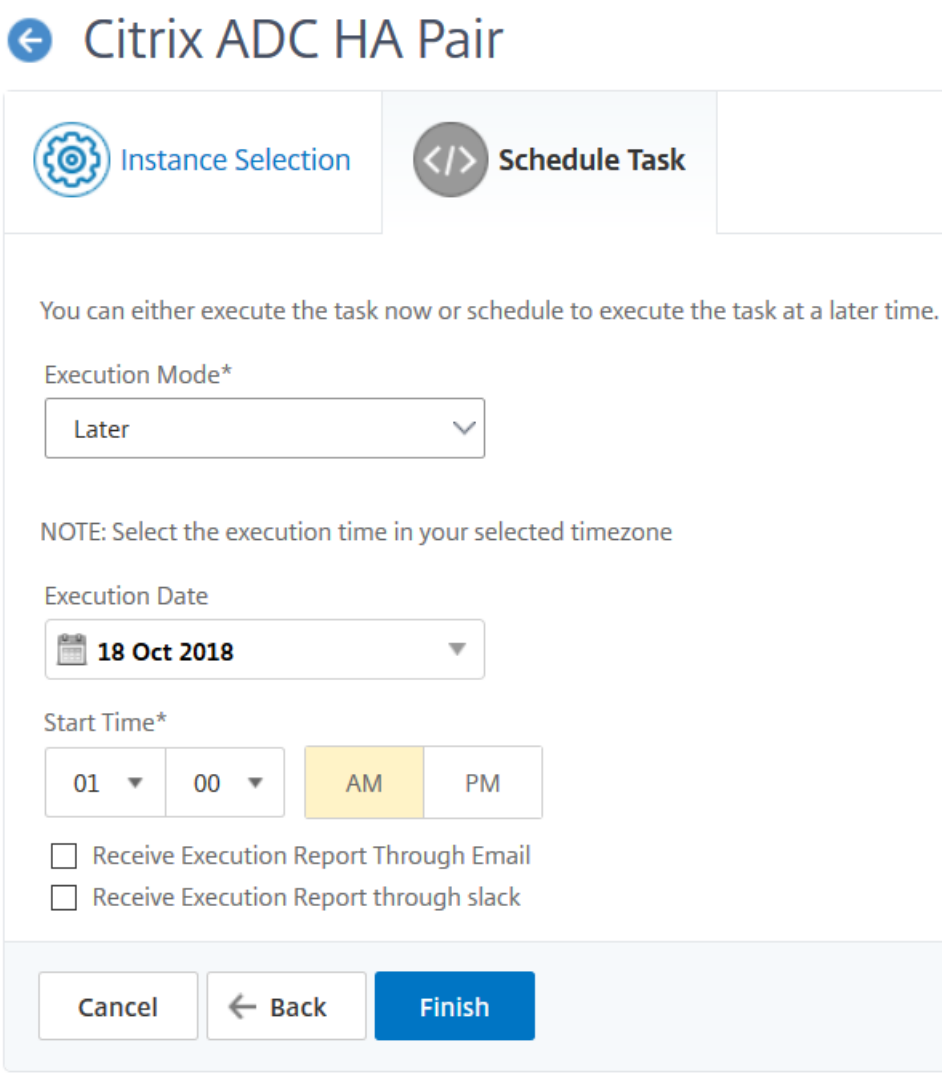
1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Configure HA Pair of NetScaler Instances** and click **Proceed**.



3. On the **NetScaler HA Pair** page, in the **Instance Selection** tab:
   a) Add a **Task Name**.
   b) Enter the Primary IP Address.
   c) Enter the Secondary IP Address.
   d) Click **Next**.
   e) Click to enable **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.
5. To upgrade a NetScaler HA pair later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the NetScaler instance, and click **Finish**.

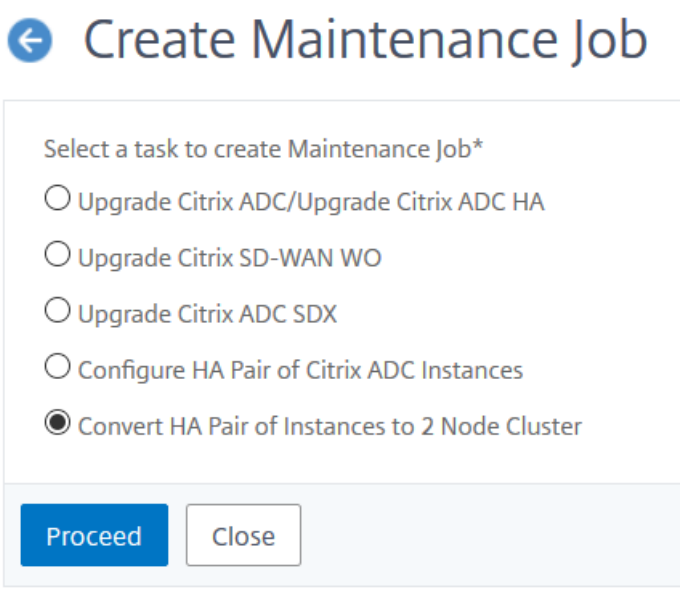


6. You can also enable email and slack notifications to receive the execution report of creating the ADC HA pair. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

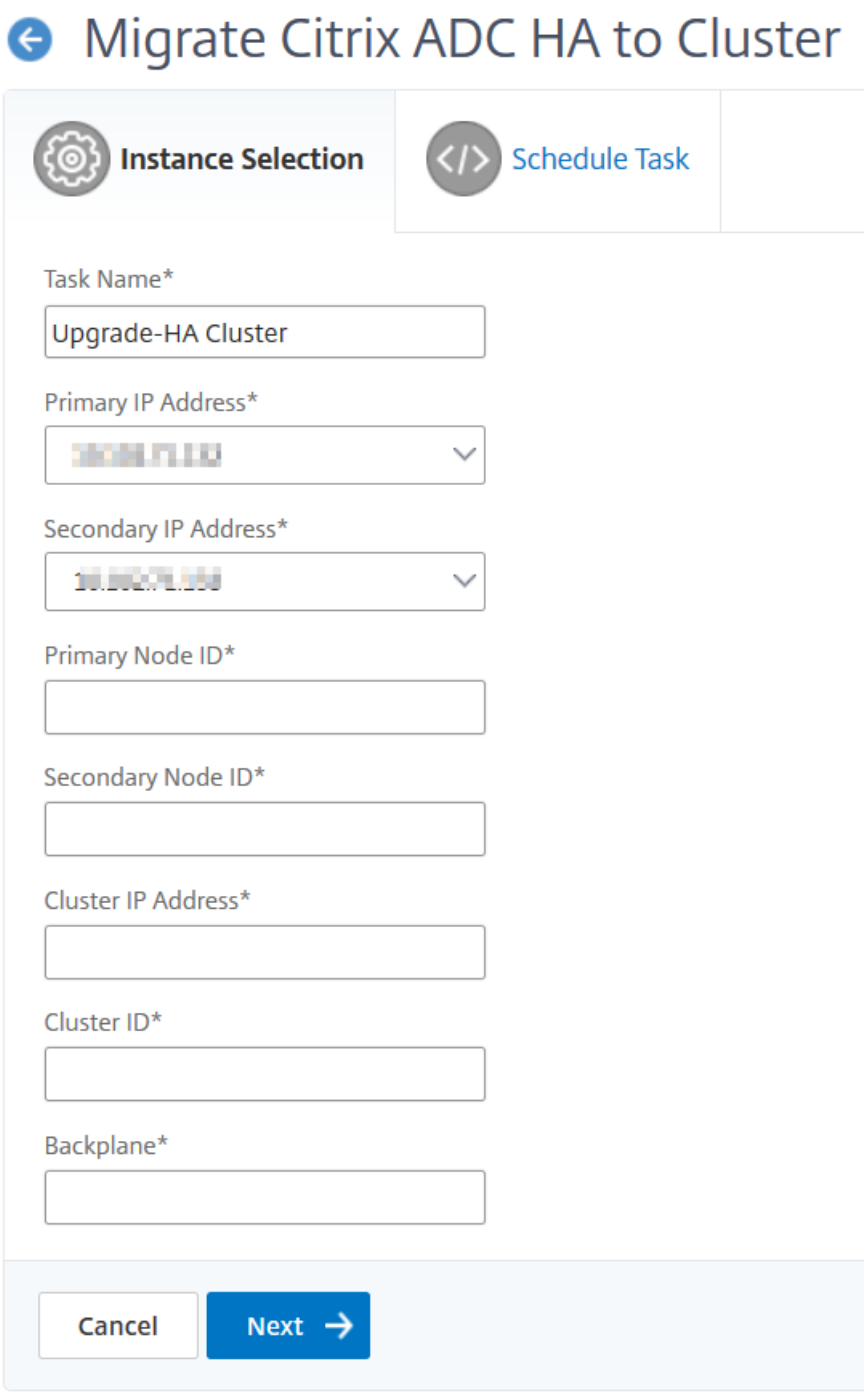
   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Schedule converting HA pair of instances to cluster

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.



3. On the **Migrate NetScaler HA to Cluster** page, in the **Instance Selection** tab, add a **Task Name**. Specify the Primary IP address, Secondary IP address, Primary Node ID, Secondary Node ID, Cluster IP Address, Cluster ID, and Backplane, and then click **Next**.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.
5. To upgrade later, select **Later** from the **Execution Mode** list. You can then choose the **Execution Date** and the **Start Time** for upgrading the NetScaler HA pair instance, and click **Finish**.
6. You can also enable email and slack notifications to receive the execution report of upgrading a NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and

Receive Execution Report through slack check box to enable the notifications.

For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Upgrade Advisory (Preview)

March 11, 2024

As a network administrator, you might manage many ADC instances running on different ADC builds in NetScaler ADM. Monitoring the lifecycle of each ADC instance can be a cumbersome task. You must visit NetScaler product Matrix, identify the ADC instances that are reaching or have reached the End of Life (EOL) or End of Maintenance (EOM). Then, plan their upgrade.

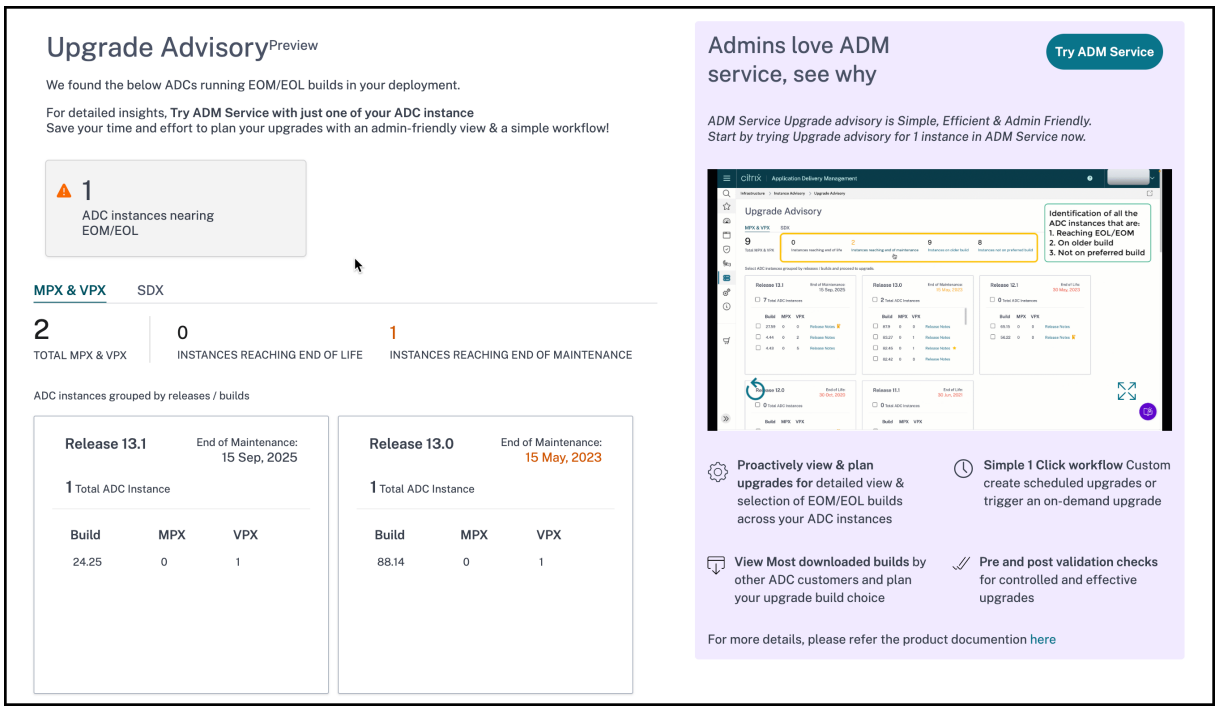
NetScaler ADM on-premises Upgrade Advisory performs a version scan on the ADCs and provides a view of the EOM/EOL builds across your ADC instances.

> **IMPORTANT**
>
> For detailed insights, and the workflow to upgrade the ADC instances, **try NetScaler ADM Service**.

View upgrade advisory

Navigate to **Infrastructure > Instance Advisory > Upgrade Advisory** and view the following information:

- Total count of ADC instances.
- Instances reaching the end of life.
- Instances reaching the end of maintenance.



The **Upgrade Advisory** page groups the ADC instances by their releases.

NetScaler ADM on-premises upgrade advisory also allows you to select one of the ADC instances, and onboard the ADC instance to ADM Service. Click **Try ADM Service** and onboard the ADC instance to ADM Service. ADM Service Upgrade Advisory provides you the workflow to upgrade by selected ADC instance.

For more information on the ADM Service Upgrade Advisory, view the gif animation on the **Upgrade advisory** page.

Security Advisory (Preview)

June 18, 2024

> **Note:**
>
> Starting from 13.1-53.22 build, Security Advisory is automatically enabled. For more information, see Security Advisory

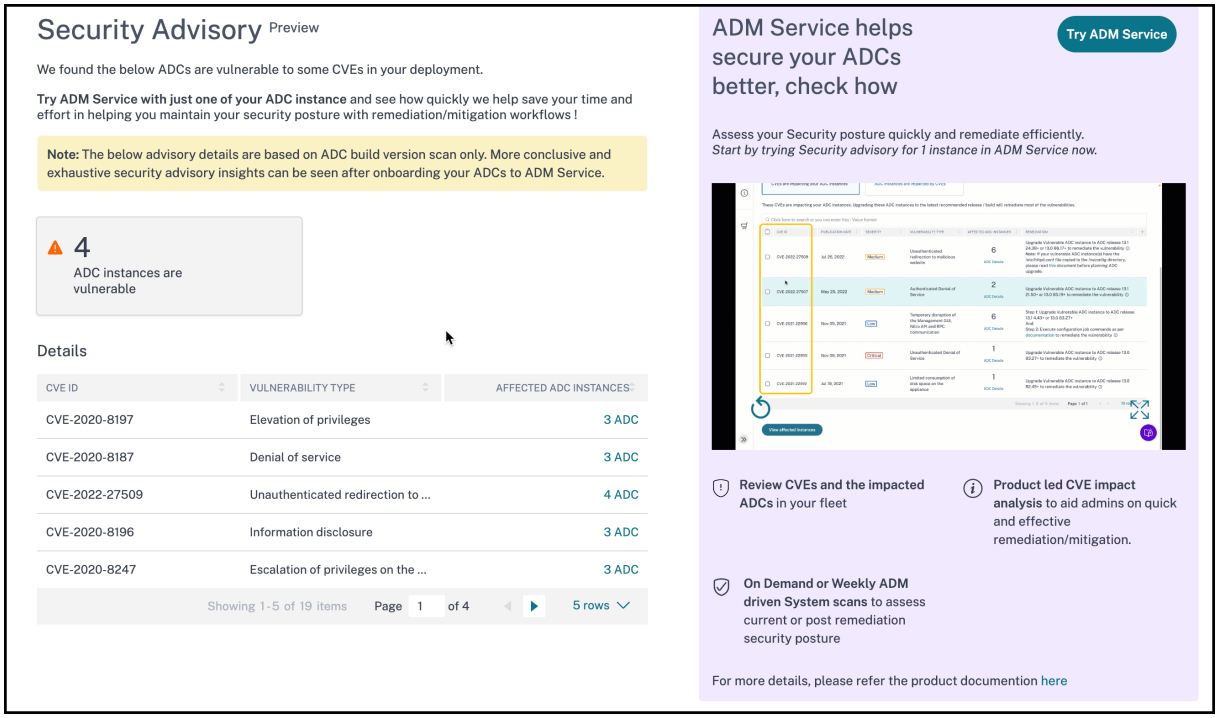
A safe, secure, and resilient infrastructure is the lifeline of any organization. Organizations must track new Common Vulnerabilities and Exposures (CVEs), and assess the impact of CVEs on their infrastructure. They must also understand and plan the mitigation and remediation to resolve the vulnerabilities.

NetScaler ADM on-premises Security Advisory only highlights the NetScaler CVEs and the ADC instances that are at risk.

> **IMPORTANT**
>
> For a detailed analysis on the CVE impact, conclusive information on custom scans/system scans, remediation and mitigation workflows, **try NetScaler ADM Service**.

View security advisory

To access **Security Advisory**, navigate to **Infrastructure > Instance Advisory > Security Advisory**. You can see the vulnerability status of all the ADC instances that you manage through NetScaler ADM.



NetScaler ADM on-premises Security Advisory performs only ADC Version scan to check for CVEs and following information is displayed.

- **CVE ID**: The ID of the CVE impacting the instances.
- **Vulnerability type**: The type of vulnerability for this CVE.
- **Affected ADC instances**: The instance count that the CVE ID is impacting.

NetScaler ADM on-premises Security Advisory also allows you to select one of the ADC instances, and onboard the ADC instance to ADM Service. Click **Try ADM Service** and onboard the ADC instance to ADM Service. ADM Service Security Advisory allows you to check the vulnerability type of a particular CVE and get information on mitigation and remediation to resolve the vulnerability.

For more information on the ADM Service Security Advisory, view the gif animation on the **Security Advisory** page.

Orchestration

March 11, 2024

In Software Defined Networking (SDN), a software application controller manages a network and its activities instead of hardware that supports the network. That is, SDN allows the network administrators to virtualize a physical network connectivity into a logical network connectivity and manage network services using a software based centralized management tool. SDN allows network engineers and administrators to respond to rapidly changing business requirements.

While the better known advantages of SDN are traffic programmability, greater agility, the ability to create policy driven network supervision, and implementing network automation, some of the specific advantages of SDN are listed below:

- Centralized network provisioning
- Increased network security at granular level
- Reduced operating costs
- Increased levels of cloud abstraction
- Guaranteed content delivery
- Reduced network downtime

NetScaler Application Delivery Management (ADM) supports SDN in enterprises network by integrating with SDN controllers of different vendors. NetScaler ADM supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

NetScaler ADM integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter administrators to programmatically deploy NetScaler services faster.

VMware NSX Manager exposes logical firewalls, switches, routers, ports, and other networking elements to allow virtual networking among diverse hypervisors, cloud management systems, and associated network hardware. It also supports external networking, and security services.

The Cloud Orchestration feature of NetScaler ADM enables the integration of NetScaler products with VMware NSX, and provides the following capabilities:

- Ability to allocate a pre-provisioned VPX on-demand to a certain Edge gateway as part of service insertion.
- Ability to configure advanced features of NetScaler such as SSL and CS along with basic load balancing through application templates on the instances that are running inside NSX environment.
- Ability to de-allocate a VPX from a certain Edge gateway as part of service deletion and reallocate the same VPX for another Edge gateway.
- Ability to rapidly deploy NetScaler functions from the vCenter console as part of the deployment workflow of all the infrastructure required for an application.

Benefits:

- Automated, on-demand allocation of new ADC services as part of an application deployment workflow
- Simplified configuration of application specific, advanced ADC functionality through application templates
- Multitenant separation-of-duties and a self-service consumption model while providing cloud administrators a single point of control
- Easier integration with NetScaler ADM API's, which help to support unanticipated future uses.

For more information on how to configure VMware NSX Manager on NetScaler ADM, see Integrating NetScaler Appliances with VMware NSX Manager.

Cisco ACI Hybrid Mode

Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to NetScaler ADM, which acts as a Device Manager in the APIC.

The NetScaler Hybrid Mode solution is supported by a hybrid mode device package and NetScaler ADM. You need to upload the hybrid mode device package in the APIC. For more information, see NetScaler Automation Using NetScaler ADM in Cisco ACI's Hybrid Mode.

OpenStack: Integrating NetScaler instances

March 11, 2024

The Cloud Orchestration feature of NetScaler Application Delivery Management (ADM) enables integration of NetScaler products with OpenStack platform. By using this feature with OpenStack platform, the OpenStack users are able to avail the load balancing feature (LBaaS) of the NetScaler. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in NetScaler instance.

The following sections provide a brief description of the features in NetScaler ADM and OpenStack integration workflow.

NetScaler Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plug-in includes a NetScaler driver that enables OpenStack to communicate with the NetScaler ADM. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the NetScaler ADM, which creates the load balancer configuration on the desired NetScaler instances. OpenStack also uses the driver to call NetScaler ADM at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the NetScalers. NetScaler driver software for OpenStack platform is bundled along with the NetScaler ADM. To download and install the drivers, you have to first install NetScaler ADM and launch the application.

Registering NetScaler ADM and OpenStack with each other

You have to first register OpenStack information on the NetScaler ADM. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack NetScaler driver user credentials. You can later specify the same login credentials in the NetScaler_driver section of the Neutron configuration file (neutron.conf) so that NetScaler driver in OpenStack can connect to NetScaler ADM during LB configurations.

After OpenStack and NetScaler ADM are registered with each other, both can talk to each other. Also, OpenStack users can use their existing credentials in OpenStack to log on to the NetScaler ADM user interface to check how their LB configurations are performing in NetScalers.

Tenants in OpenStack

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

Placement policies

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Alternatively, the NetScaler ADM also provides an option to assign a NetScaler instance based on OpenStack tenants.

Service packages

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
- Multiple tenants can be associated with the same service package.
- In a service package that is set for auto-provisioning, virtual NetScaler instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

Features Supported on LBaaS V1 and LBaaS V2

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
  - Load Balancing
- LBaaS V2
  - Load Balancing
  - SSL Offload with certificates managed by **Barbican**, the Key Manager in OpenStack
  - Certificate Bundles (includes intermediary Certification Authorities)
  - SNI support

This document provides information about:

- Use Case Scenario
- NetScaler ADM Integration with OpenStack Workflow

- Prerequisites
- Pre-configuration Tasks in NetScaler ADM and OpenStack
- Configuration Steps for LBaaS V1 using Horizon
- Configuration Steps for LBaaS V2 using Command Line
- Manual Provisioning of NetScaler VPX Instance on OpenStack
- Integrating NetScaler ADM with OpenStack Heat Services
- Monitoring OpenStack Applications in NetScaler ADM

Use Case Scenario

The following use-case scenario explains the workflow of integrating NetScaler ADM with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider's cloud infrastructure. Tom's organization, Example-SportsOnline.com, requires two servers S1 and S1, and Tom also requires a dedicated NetScaler device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and NetScaler ADM, and prepare them to compatible with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.

Steve has to register OpenStack details with NetScaler ADM, and configure the NetScaler LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, NetScaler ADM displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the NetScaler LBaaS features and configure Tom to get a dedicated NetScaler allotted for his load balancer configurations in NetScaler ADM.

For this, Steve can either provision a NetScaler VPX instance on the computing layer (Nova) of OpenStack using NetScaler ADM user interface or enable MAS to auto-provision a NetScaler VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, NetScaler ADM manages the VPX instance. For achieving this, Steve creates a service package in NetScaler ADM, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the 'dedicated'isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many NetScaler VPX instances to the service package, and associates Example-SportsOnline,

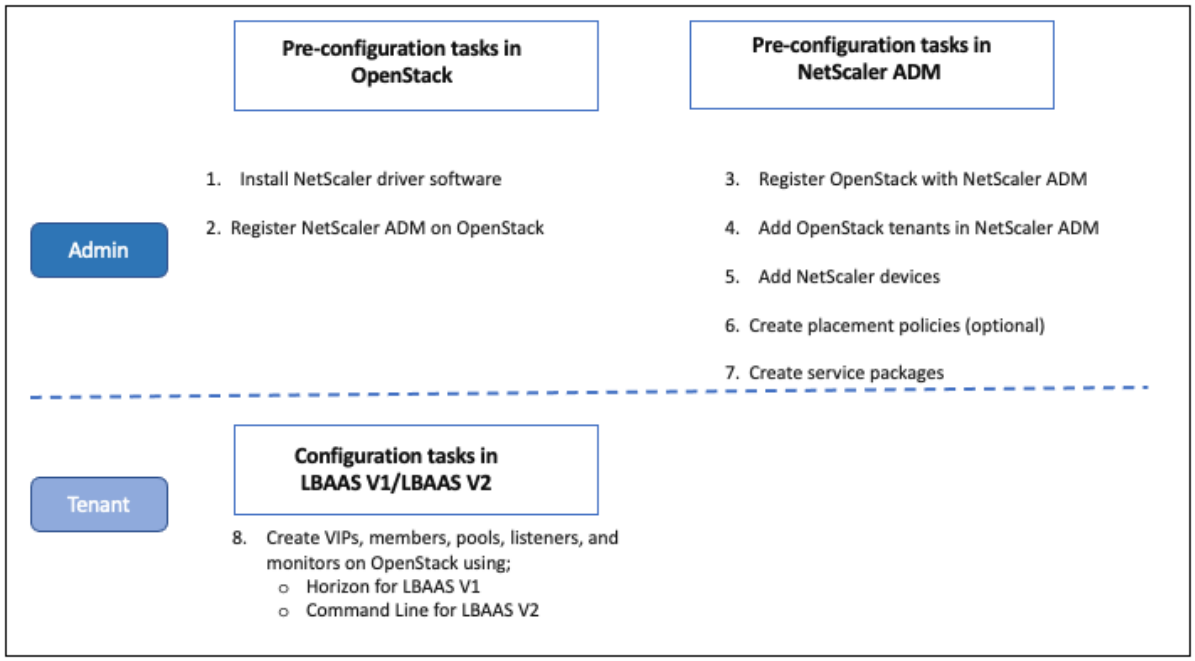
along with other tenants, who require a dedicated NetScaler with the service package. As a result, when Tom performs his first load balancer configuration, NetScaler ADM allots one of the NetScaler VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that NetScaler.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and virtual servers on the NetScaler instance. Tom can also create health monitors to monitor the servers, and send application traffic to only those servers which are UP at any point of time and reachable from NetScaler.

The load balancing configuration created in OpenStack is now implemented on the NetScaler instance. Once fully configured, the NetScaler VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

NetScaler ADM Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.



NSX Manager: manual provisioning of NetScaler instances

March 11, 2024

NetScaler Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

This article provides you with a list of tasks that you have to perform on both VMware NSX Manager and on NetScaler ADM.

> **Note**
>
> Ensure that VMware NSX for vSphere 6.2 and above is installed and configured, and the edge gateways, DLR, and virtual machines that have to be load balanced are already created.

Prerequisites

- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
- Install NetScaler ADM on any of the supported hypervisors.

  For tasks to install NetScaler ADM build 13.1, on any of the supported hypervisors, see Deploying NetScaler ADM.

VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you require on your VMware ESXi server to install a NetScaler ADM virtual appliance.

Component	Requirement
RAM	8 GB
Virtual CPU	8

Storage space	500 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

> **Note**
>
> The memory and hard disk requirements specified above are for deploying NetScaler ADM on VMware ESXi server, considering that there are no other virtual machines running on the host. The hardware requirements for VMware ESXi server depends on the number of virtual machines running on it.

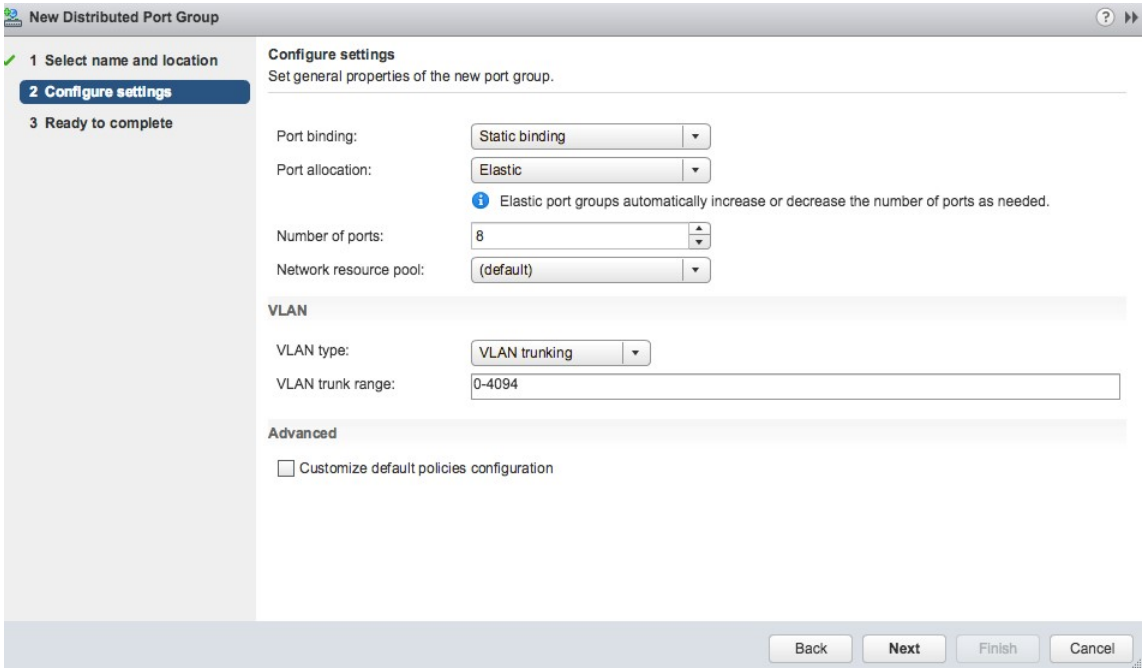
Configuring VMware NSX

- Create a pool of NetScaler VPX instances of different capacities, which are added to the different service packages.

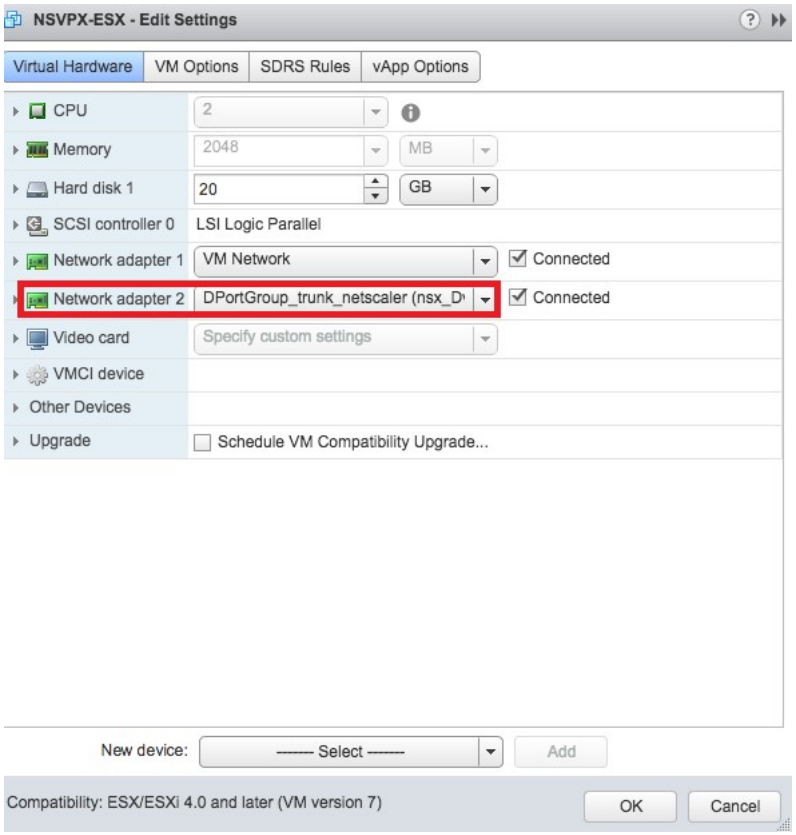
For example:

- Create five NetScaler VPX instances of VPX1000 (1 Gbps). These instances are added to the Gold service package.
- Create five NetScaler VPX instances of VPX10 (10 Mbps). These instances are added to the Bronze service package.

1. In vSphere client, navigate to **Networking**, and create a port group of type VLAN trunking with range, for example, 101-105 (you can even provide the full range, but create port group of type VLAN for only the required VLANs).

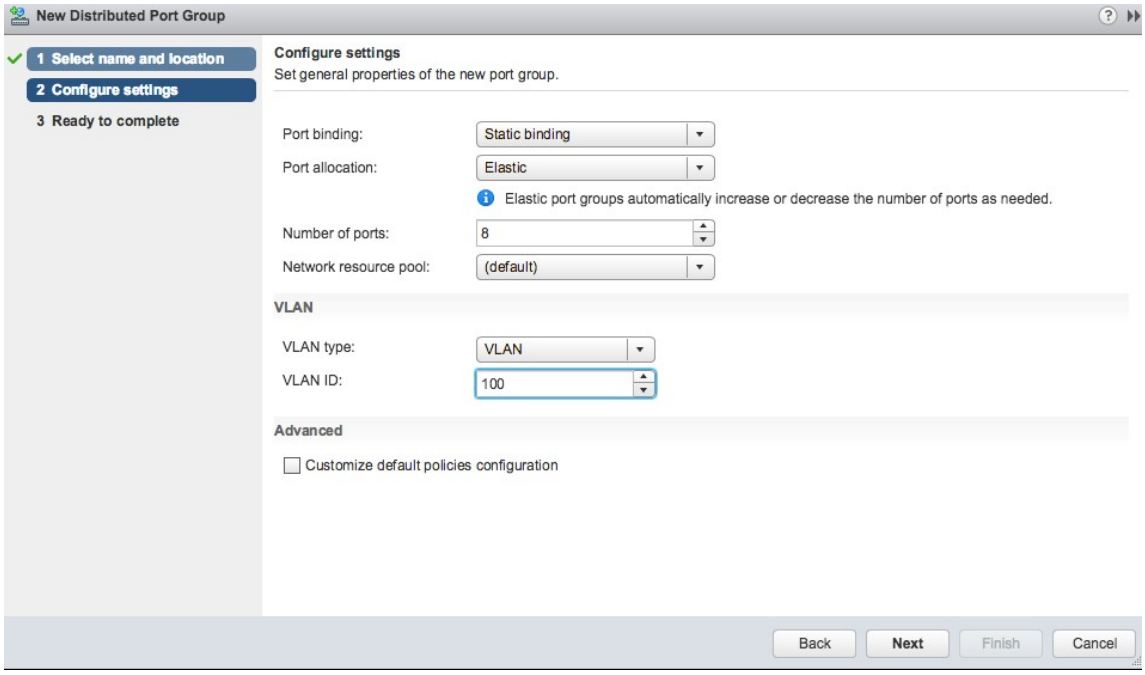


2. Create a new interface for each NetScaler VPX instance, and attach it to the VLAN range trunk port group that was created above.



3. In vSphere client, navigate to **Networking**, and create a port group of type VLAN.

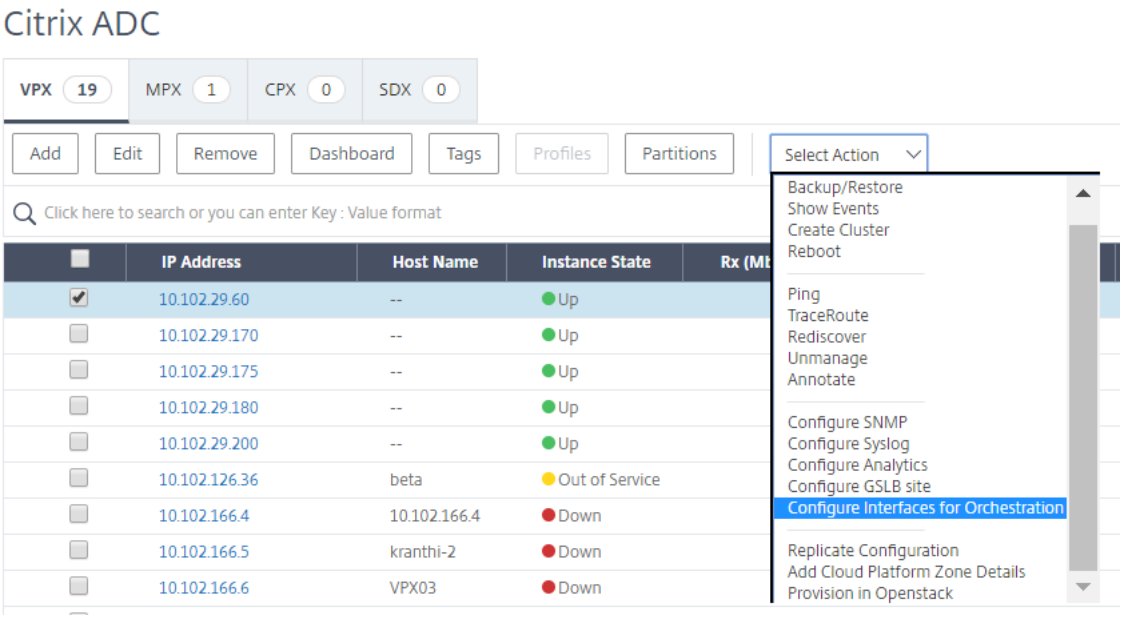
For example, If the initial trunked port group was created with range 101-105, create five VLAN port groups one per VLAN, that is a port group with VLAN 101, another with VLAN102, and so on, until VLAN 105.



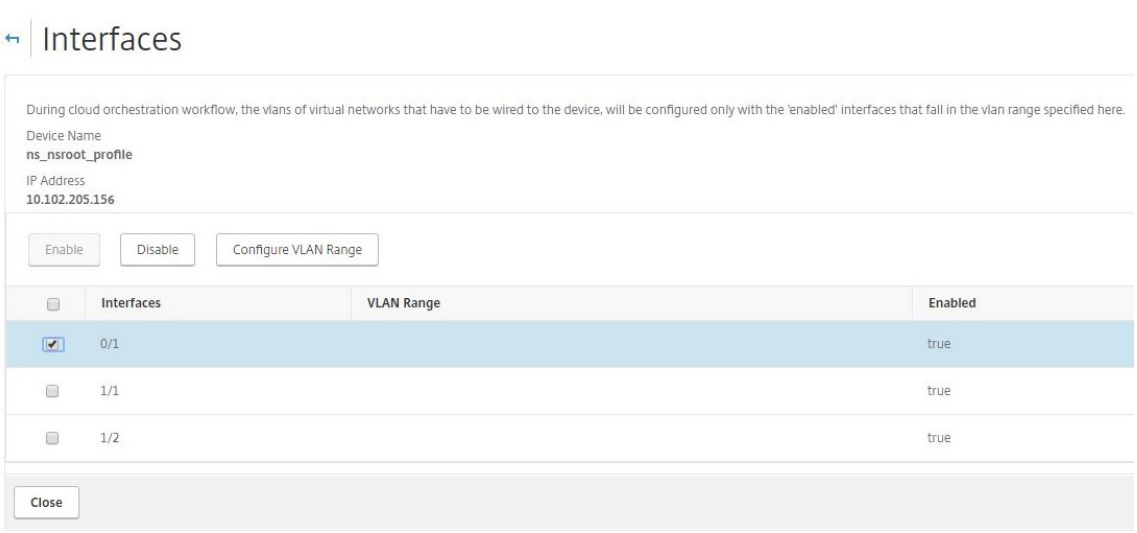
Adding NetScaler VPX Instance in NetScaler ADM

Add NetScaler VPX instances in NetScaler ADM and specify the VLAN range of the trunked group for each device.

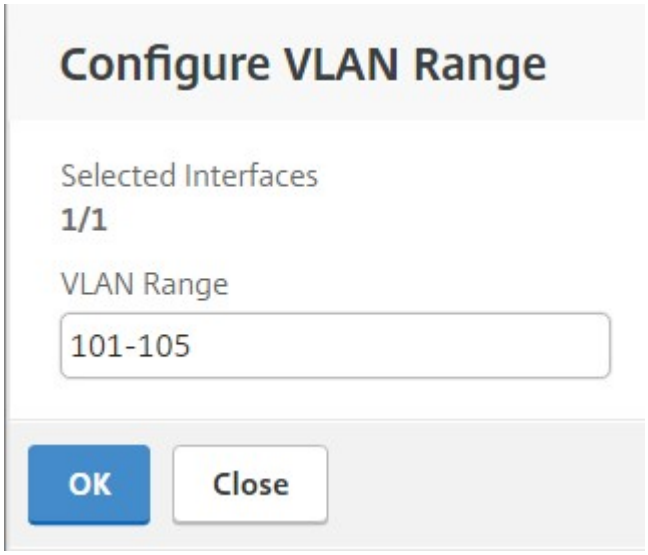
1. In NetScaler ADM, navigate to **Infrastructure** > **Instances** > **NetScaler VPX**, and click **Add**.
2. On the **Add NetScaler VPX** page, specify either the host names of the instances, the IP address of each instance, or a range of IP addresses, and then select an instance profile from the P**rofile Name** list. You can also create a new instance profile by clicking the + icon.
3. Click **OK**.
4. Select the newly added NetScaler VPX instance from the list on the **NetScaler VPX** page, and click the down arrow button in **Action** field. Select **Configure Interfaces for Orchestration**.



5. On the **Interfaces** page, select the management interface, and click **Disable** to disable VLAN from binding to the management interface.



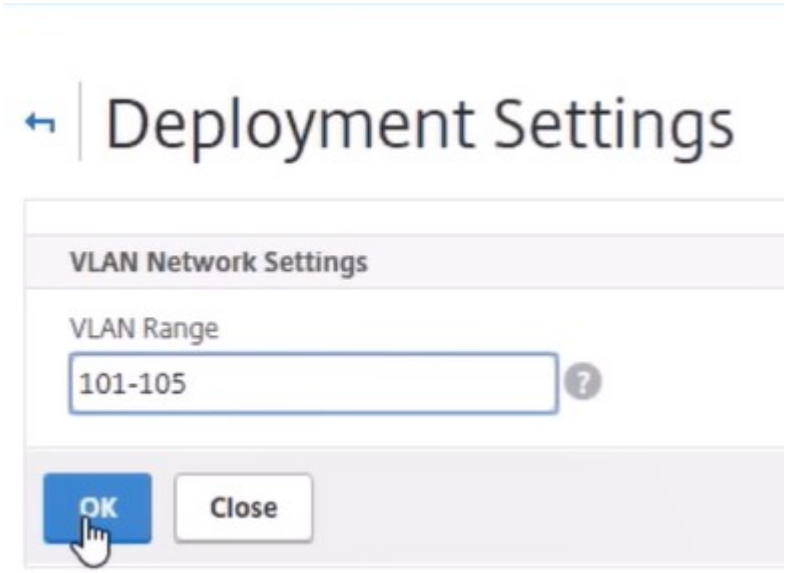
6. On the **Interfaces** page, select the required interface, and click **Configure VLAN Range**.
7. Enter the VLAN range configured in NSX Manager, click **OK**, and then click **Close**.



Registering VMware NSX Manager with NetScaler ADM

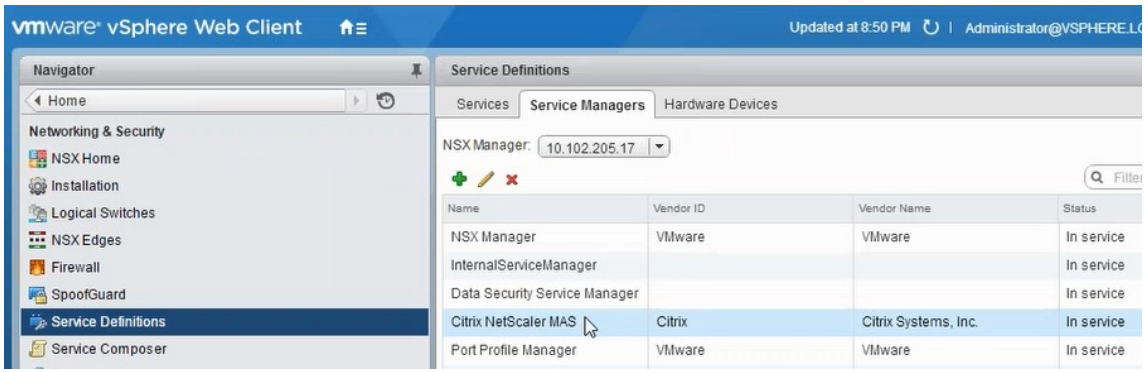
Register VMware NSX manager with NetScaler ADM to create a communication channel between them.

1. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** from the drop-down list, and click **Configure NSX Manager Settings**.
2. On **Configure NSX Manager Settings** page, set the following parameters:
    a) NSX Manager IP Address - IP address of NSX Manager.
    b) NSX Manager user name - Administrative user name of NSX Manager.
    c) Password - Password of the administrative user of NSX Manager.
3. In **NetScaler ADM account used by NSX Manager** section, set the NetScaler Driver user name and Password for the NSX Manager. NetScaler ADM authenticates load balancer configuration requests from the NSX Manager by using these logon credentials.
4. Click **OK**.
5. Navigate to **Orchestration** > **System** > **Deployment Settings**. Provide the VLAN range which was configured in trunked port group.



6. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** > **Service Managers**.

   You can view Citrix NetScaler ADM as one of the service managers. This indicates that the registration is successful and a communication channel is established between the NSX manager and NetScaler ADM.

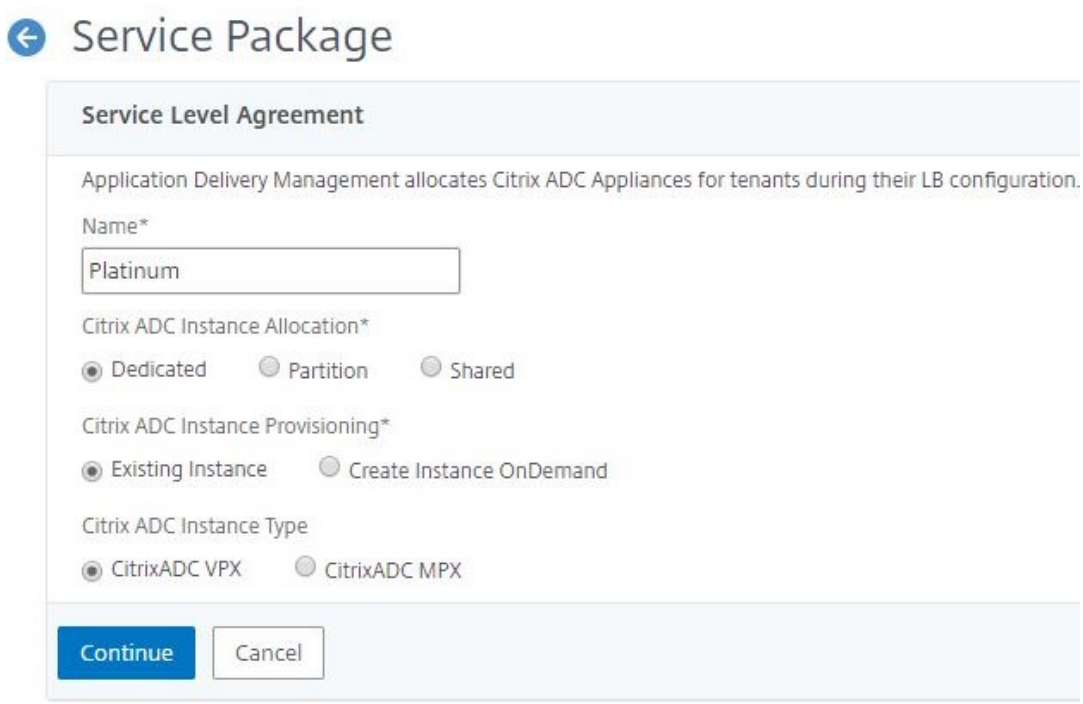


Creating a Service Package in NetScaler ADM

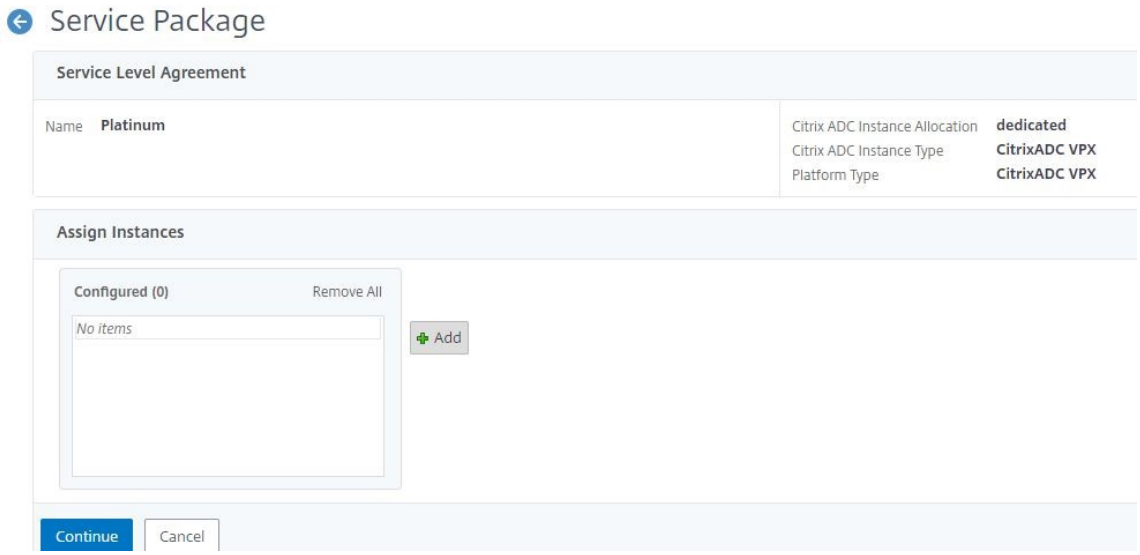
1. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a) Name –type the name of a service package
   b) Isolation Policy –by default, the isolation policy is set to Dedicated
   c) Device Type –by default, the device type is set to NetScaler VPX

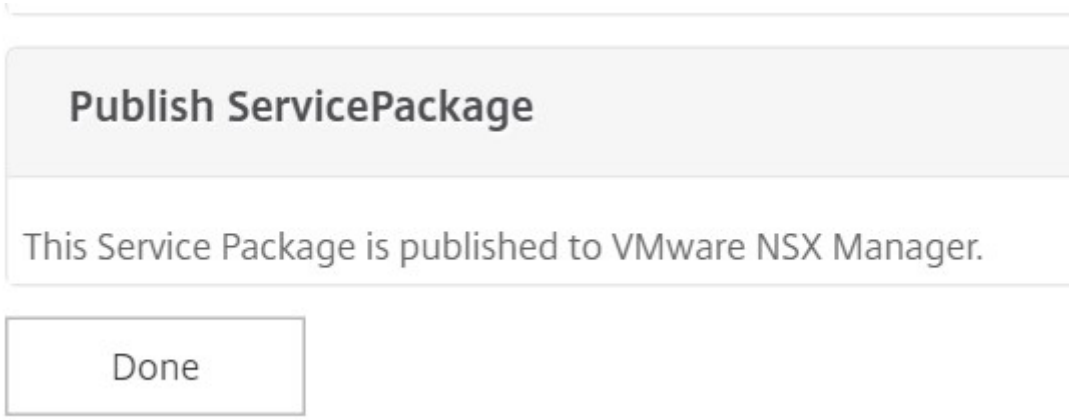
> **Note**
>
> These values are set by default in this version, and you cannot modify them.

d) Click **Continue**.



3. In **Assign Devices** section, select the pre-provisioned VPX for this package, and click **Continue**.
4. In **Publish Service Package** section, click **Continue** to publish the service package to VMware NSX, and then click **Done**.





This procedure configures a service package in the NSX Manager. A service can have multiple devices added to it and multiple edges can use the same service package to offload the NetScaler VPX instance to NetScaler ADM.

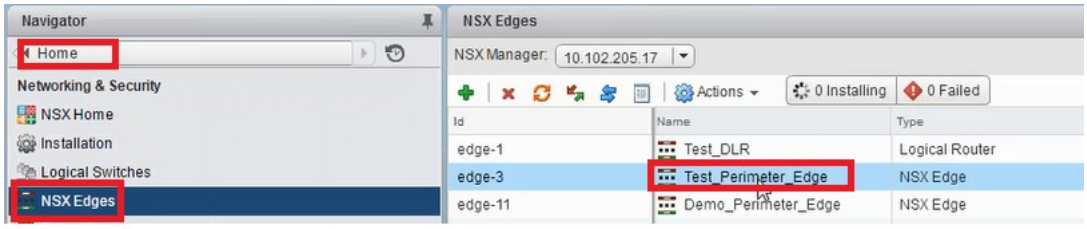
5. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** > **Services**.

   You can see that the NetScaler ADM service package is registered.

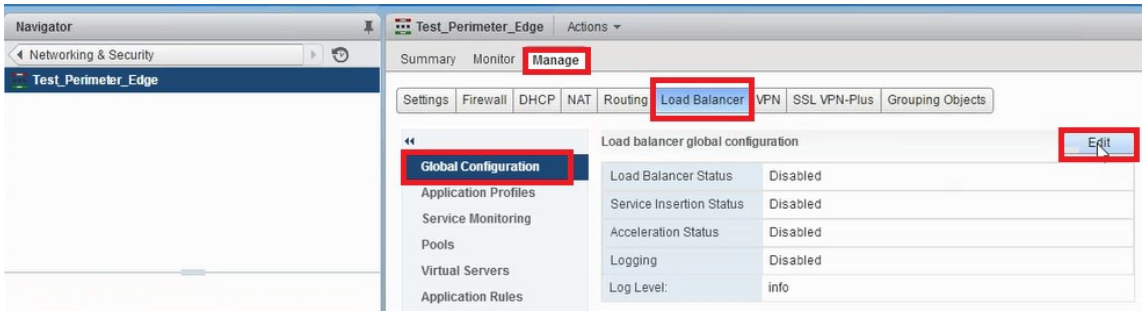
Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the previously created NSX Edge gateway (offload the load balancing function from NSX LB to NetScaler).

1. In NSX Manager, navigate to **Home** > **NSX Edges**, and select the edge gateway that you have configured.

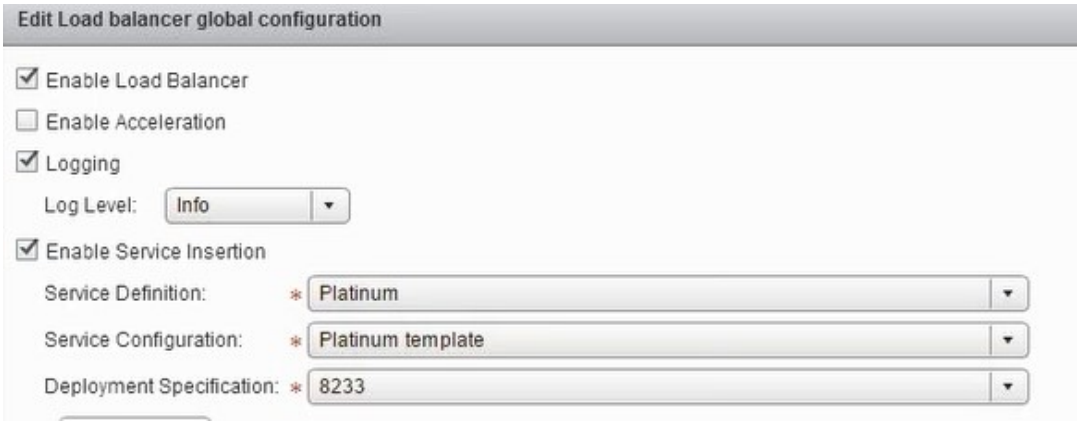


2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.

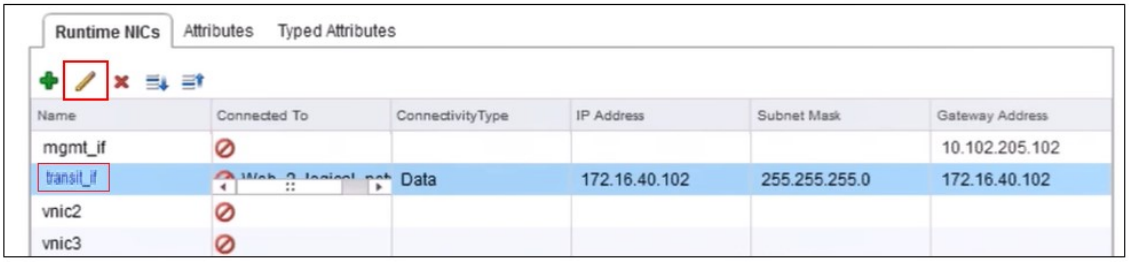


3. Select **Enable Load Balancer**, **Logging**, **Enable Service Insertion** to enable them.

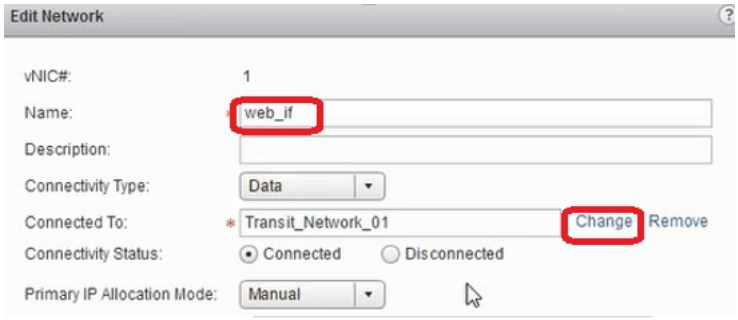
   a) In **Service Definition,** select the service package that was created in NetScaler ADM and published to NSX Manager.



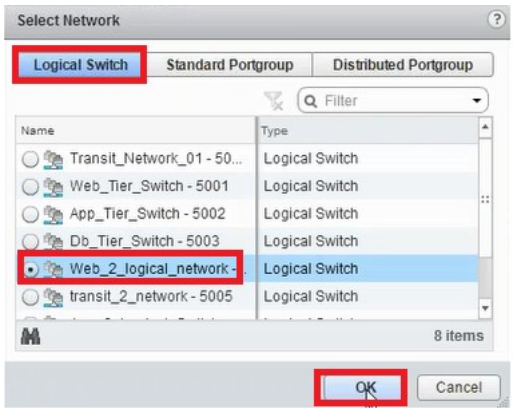
4. Select the existing runtime NICs and click the Edit icon to edit runtime NICs that have to be connected when NetScaler VPX is allocated.



5. Edit the name of the NIC, specify Connectivity Type as **Data**, and click **Change**.

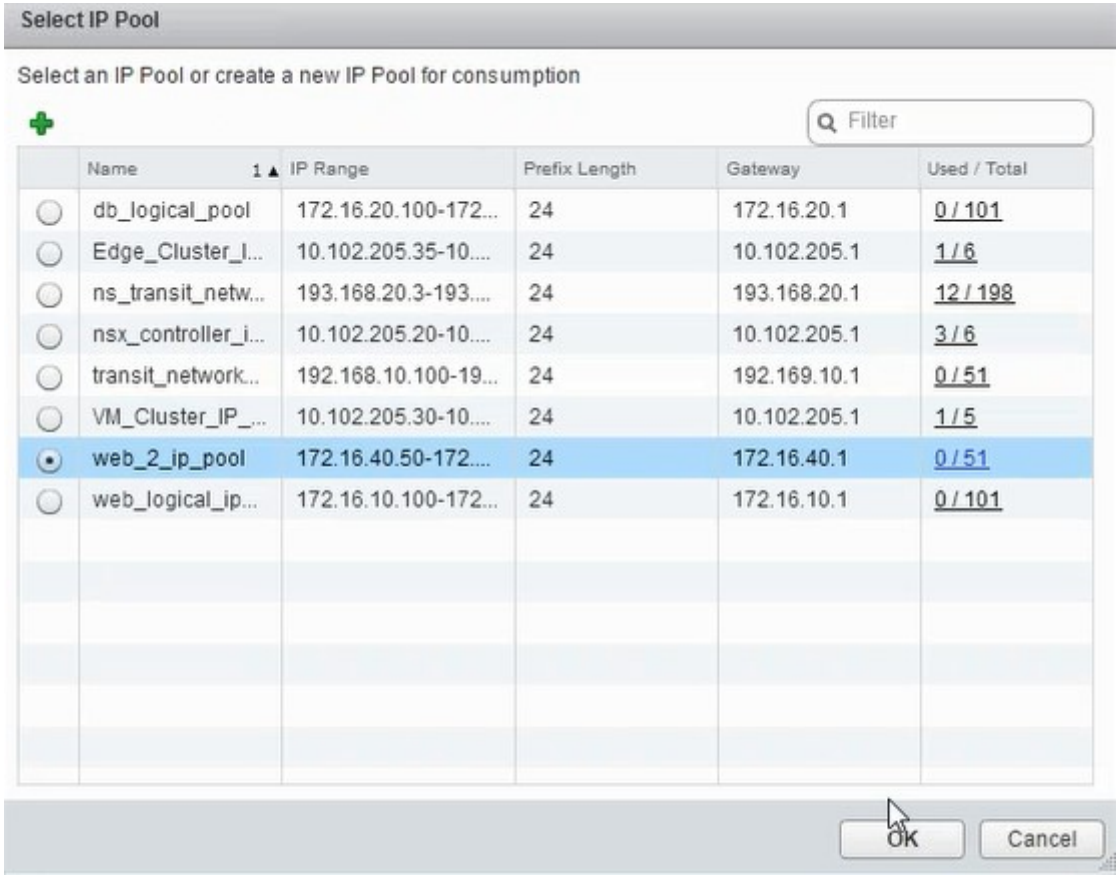


6. Select the appropriate web logical switch.



7. In **Primary IP Allocation Mode**, select IP Pool from the drop-down list, and click the down-arrow button on IP Pool field.

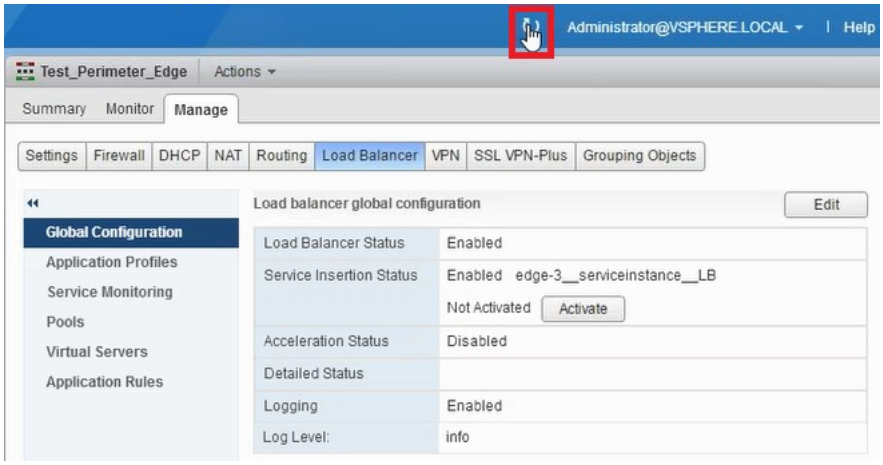
8. In the **Select IP Pool** window, select the appropriate IP pool, and click **OK**.

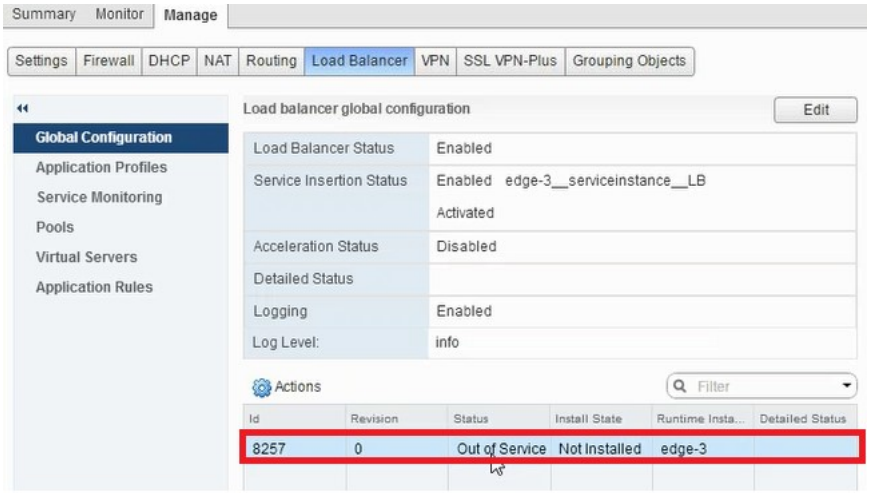


The IP address is acquired and is set as the source net IP address in the NetScaler VPX appliance. A L2 gateway is created in the NSX Manager to map the VXLAN to VLAN.

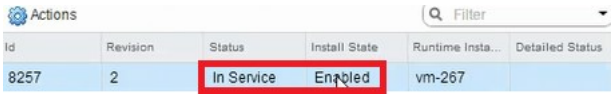
> **Note**
>
> All data interfaces are connected as run-time NICs, and they are part of interfaces for DLR.

9. Refresh the view to see the creation of the run time.





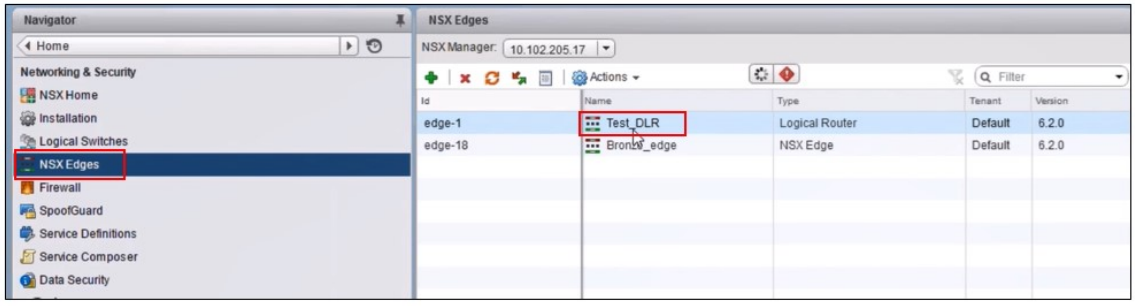
10. After the VM has started, the value of Status changes to **In Service** and that of Install State changes to **Enabled**.



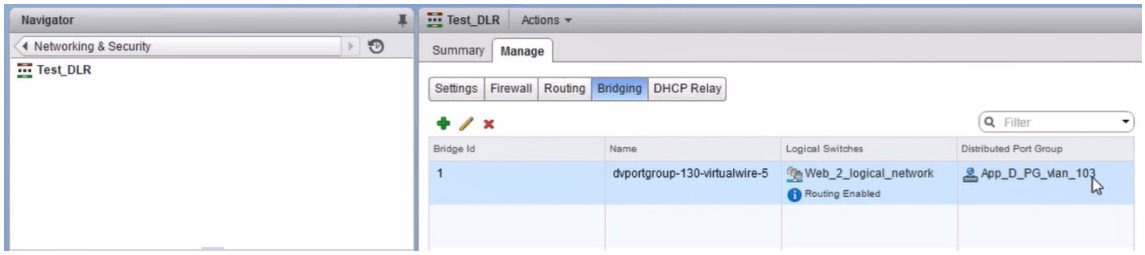
> **Note**
>
> In NetScaler ADM, navigate to **Orchestration** > **Requests** to see progress details of completion of LB service insertion.

Viewing L2 Gateway on NSX Manager

1. Log on to the NSX Manager on vSphere Web Client, navigate to **NSX Edges**, and select the DLR created.



2. In the DLR page, navigate to **Manage** > **Bridging**. You can see the L2 gateway displayed in the list.

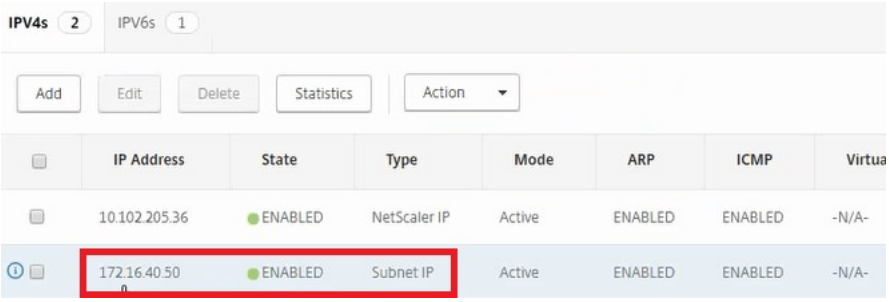


> **Note**
>
> An L2 gateway gets created for each data interface.

Viewing Allotted NetScaler

1. Log on to the NetScaler VPX instance using the IP address displayed in NetScaler ADM. Then, navigate to **Configuration** > **System** > **Networking**. In the right pane, you can see that the two IP address are added. Click the IP address hyperlink to see the details.

   The subnet IP address is same as the IP address of the web interface added in the NSX.



2. Navigate to **Configuration** > **System** > **Licenses** to view the licenses that are applied to this instance.

Configuring NetScaler VPX Instance Using StyleBook

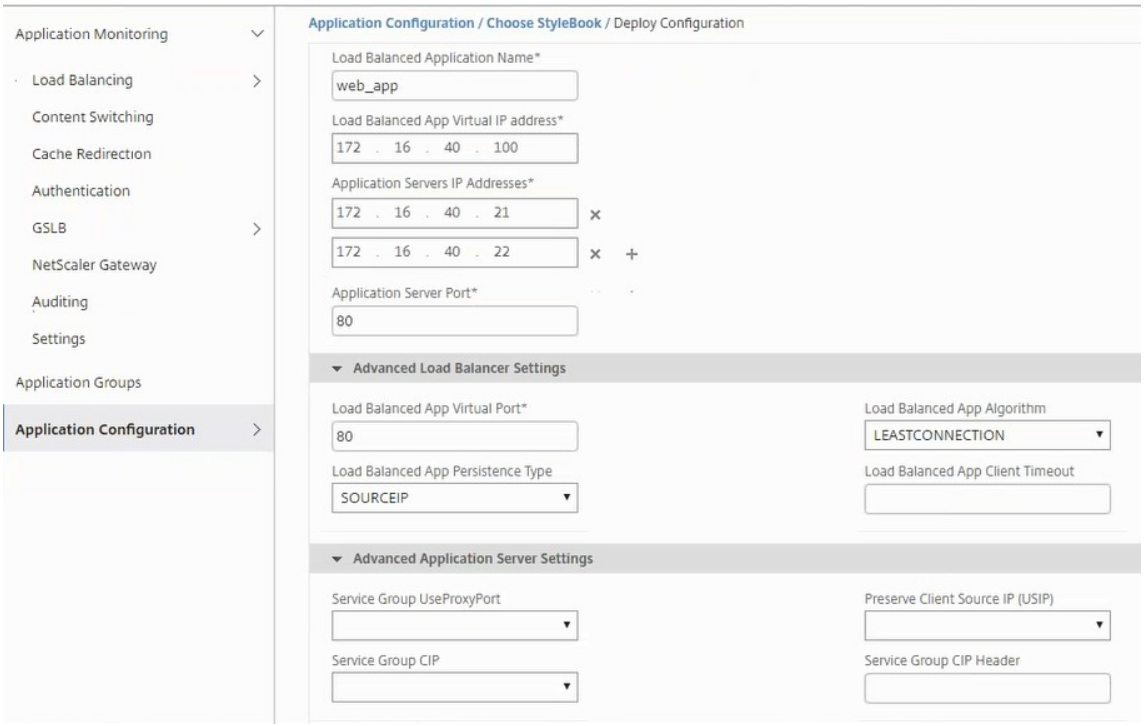
1. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **Configure NSX Manager** > **Edge Gateways**.

   Make a note of the NetScaler instance IP that is allotted to the respective Edge Gateway on which Load Balancing configuration through StyleBooks has to be applied.

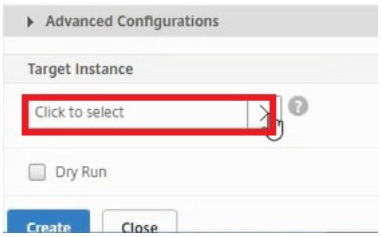
2. Create a new StyleBook. Navigate to **Applications** > **Configuration**, import the StyleBook, and select the StyleBook from the list.

   To create a new StyleBook, see Create Your Own StyleBook.

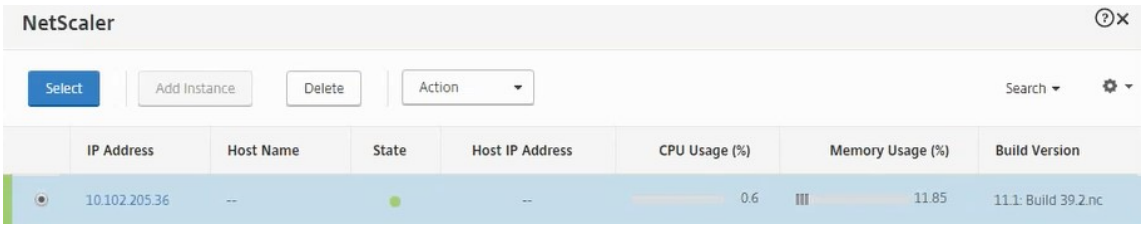
3. Specify values for all the required parameters.



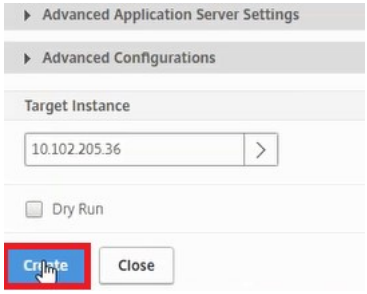
4. Specify the NetScaler VPX instance on which you want to run these configuration settings.



5. Select the IP instance noted earlier, and click **Select**.

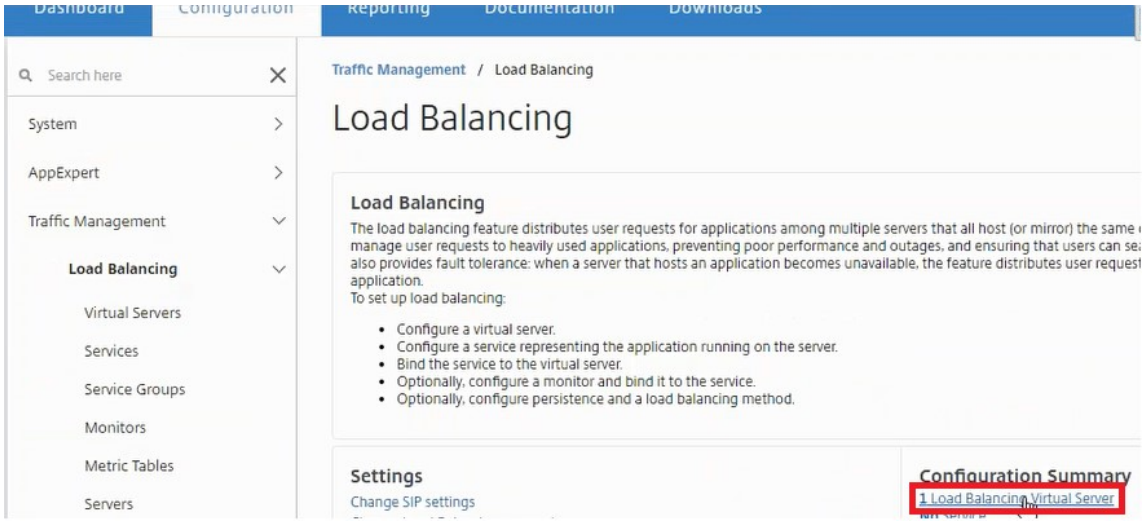


6. Click **Create** to apply the configuration on the selected device.

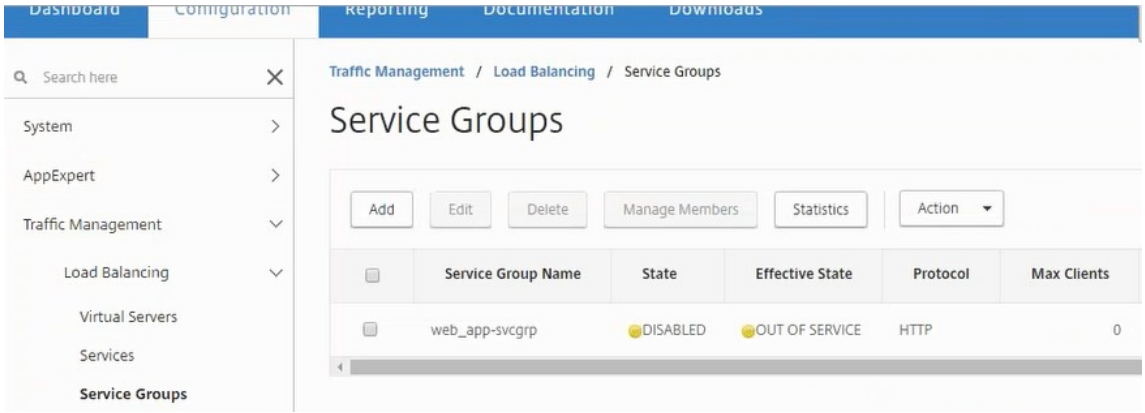


Viewing Load Balancer Configuration

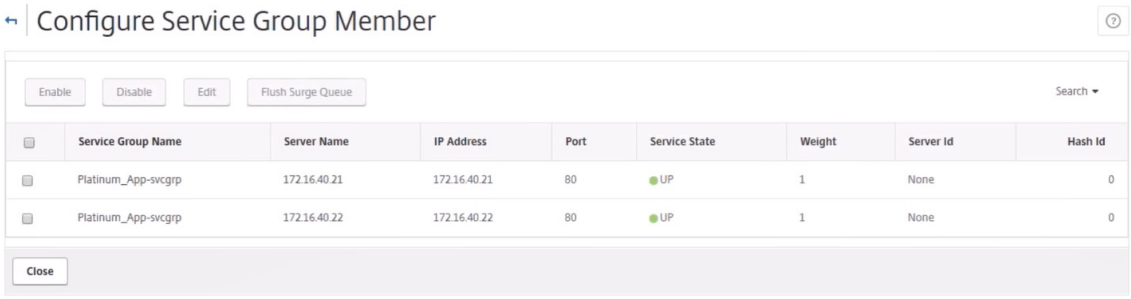
1. Log on to the NetScaler VPX instance, navigate to **Configuration** > **Traffic Management** > **Load Balancing** to view the load balancing virtual server that is created.



   You can also view the service groups that are created.



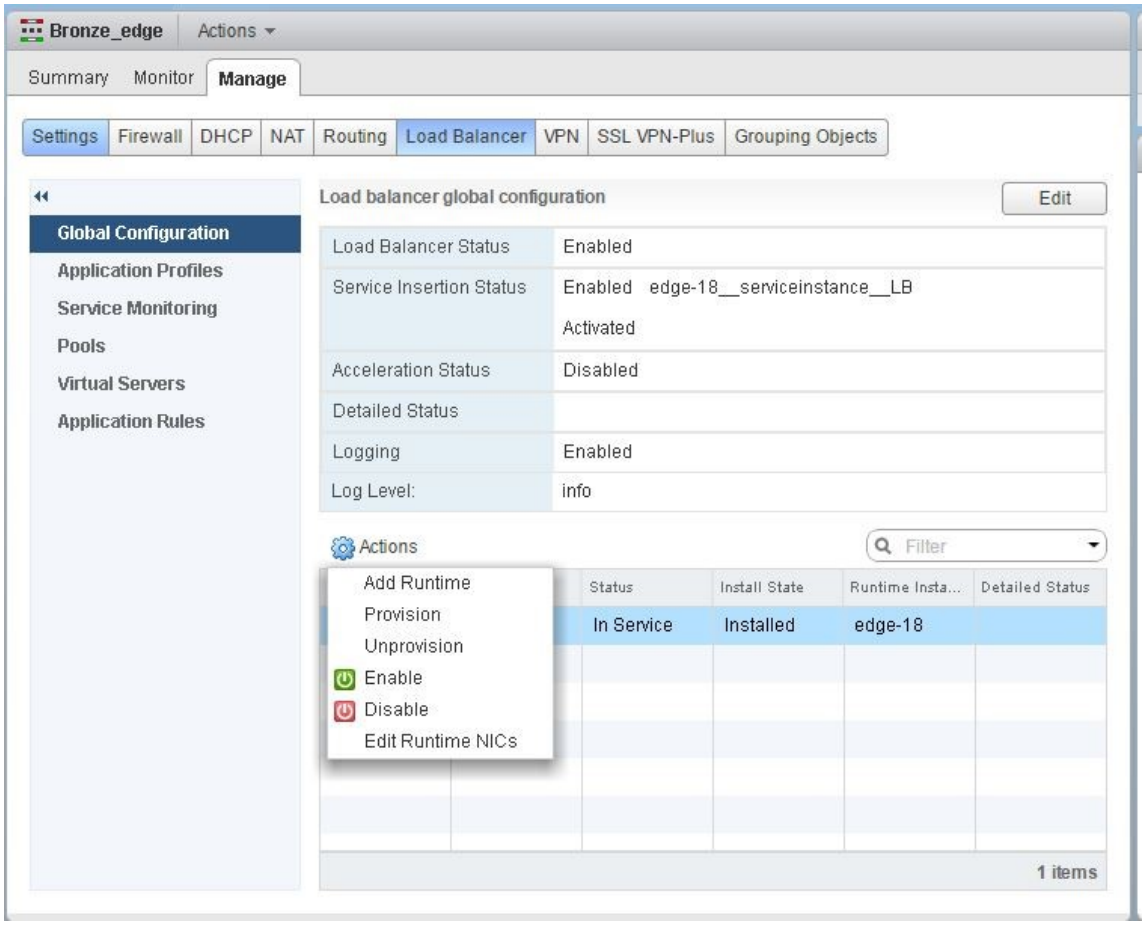
2. Select the service group, and click **Manage Members**. The **Configure Service Group Member** page displays the members associated with the service group.



Deleting Load Balancer Service

1. In NetScaler ADM, navigate to **Applications** > **Configuration**, and click **X** icon to delete the application configuration.
2. Log on to the NSX Manager on vSphere Web Client and navigate to the edge gateway to which the NetScaler VPX instance is connected.
3. Navigate to the **Manage** > **Load Balancer** > **Global Configuration**, right-click on the runtime entry, and click **Unprovision**.

> **Note**
>
> Edge Gateways in NetScaler ADM corresponds to runtime entries in NSX manager.



The NetScaler VPX instance is rendered out of service.

4. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **Configure NSX Manager** > **Edge Gateways**. Verify that the respective mapping of Edge Gateway to the deleted instance is not present.

NSX Manager: auto provisioning of NetScaler instances

March 11, 2024

Overview

NetScaler Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

During load-balancing service insertion and deletion on VMware NSX Manager, NetScaler ADM dynamically provisions and destroys the NetScaler instances. This dynamic provisioning requires the NetScaler VPX license assignments to be automated in NetScaler ADM. When the NetScaler licenses are uploaded to the NetScaler ADM, NetScaler ADM performs the role of license server.

Prerequisites

> **Note**
>
> This integration is supported only for **VMware NSX for vSphere 6.1 or earlier**.

- NetScaler ADM, version 13.0 setup in high availability and installed on ESX.
- NetScaler VPX, version 13.0
- NetScaler VPX licenses for NetScaler VPX instances, version 13.0
- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.

High-Availability Deployment of NetScaler ADM and NetScaler Instances

To provision the NetScaler ADM HA setup, install the NetScaler ADM image file that you have downloaded from the NetScaler site. For more information on how to provision NetScaler ADM HA setup, see Deploying NetScaler ADM in High Availability.

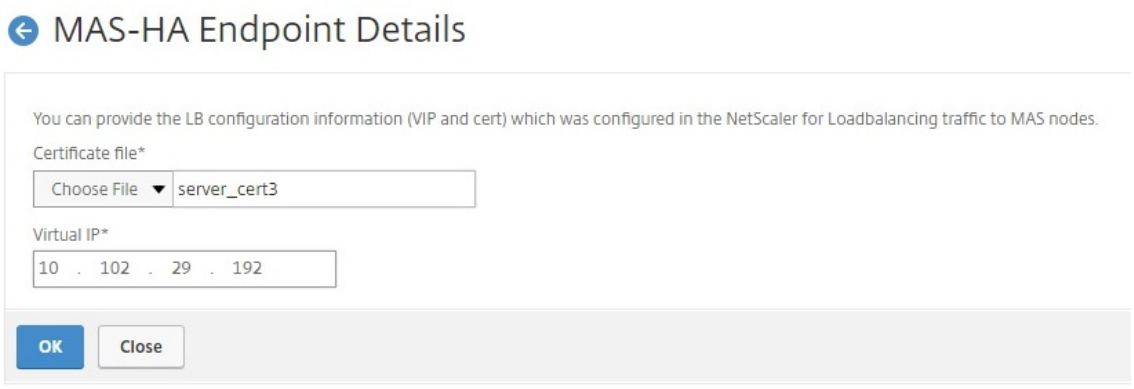
Setting up NetScaler ADM HA Endpoint Details

To integrate VMware NSX manager with NetScaler ADM that is deployed in a HA mode, you must first enter the virtual IP address of the load balancing NetScaler instance. You must also upload the certificate file that is present on the NetScaler load balancing virtual server to the NetScaler ADM file system.

To provide load balancing configuration information in NetScaler ADM:

1. In NetScaler ADM HA node, navigate to **System** > **Deployment**.
2. Click **HA Settings** in the top-right corner, and in **MAS-HA Settings** page, click **MAS-HA Endpoint Details**.

3. On **MAS-HA Endpoint Details** page, upload the same certificate that is already present on the load balancing NetScaler instance.
4. Enter the virtual IP address of the load balancing NetScaler instance and click **OK**.



Registering VMware NSX Manager with NetScaler ADM

When you set up two NetScaler ADM servers in high availability, the two server nodes are in active-passive mode. Log on to the primary NetScaler ADM server node to register VMware NSX manager with NetScaler ADM in HA, to create a communication channel between them.

To register VMware NSX manager with NetScaler ADM in HA:

1. In the primary NetScaler ADM server node, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Click **Configure NSX Manager Settings**.
3. On **Configure NSX Manager Settings** page, set the following parameters:
    a) NSX Manager IP Address - IP address of NSX Manager.
    b) NSX Manager user name - Administrative user name of NSX Manager.
    c) Password - Password of the administrative user of NSX Manager.
4. In NetScaler ADM account used by NSX Manager section, set the NetScaler Driver Password for the NSX Manager.
5. Click **OK**.

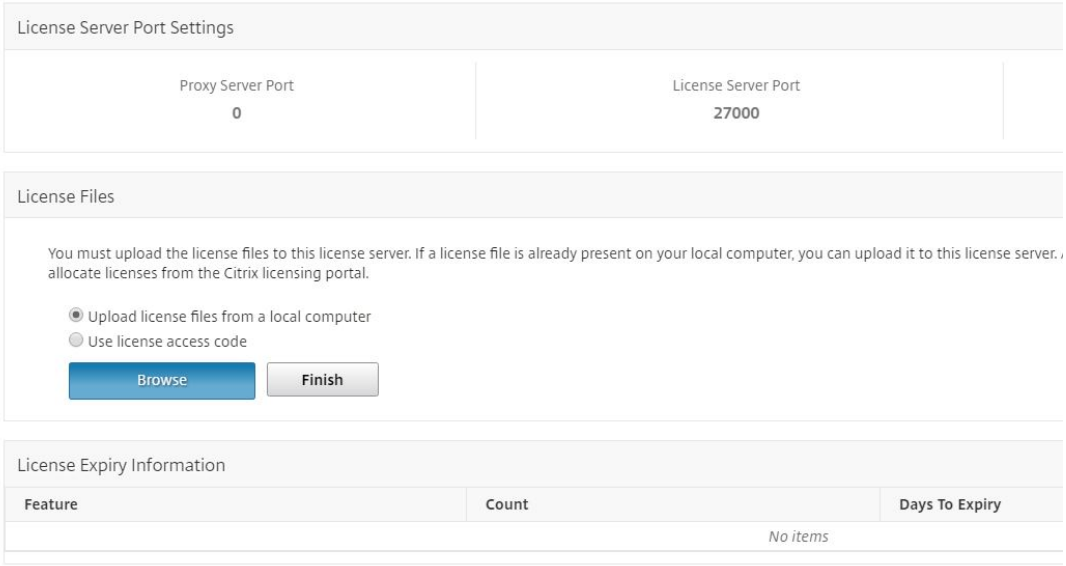
Uploading Licenses in NetScaler ADM

Upload the NetScaler VPX licenses to NetScaler ADM, so that NetScaler ADM can automatically allocate licenses to the instances during orchestration with NSX.

To install license files on NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing**.
2. In **License Files** section, select one of the following options:
   a) **Upload license files from a local computer** - If a license file is already present on your local computer, you can upload it to the NetScaler ADM. To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   b) **Use License Access Code** - Citrix emails the License Access Code for the licenses that you purchase. To add license files, enter the license access code in the text box and then click **Get Licenses**.

> **Note**
>
> At any time, you can add more licenses to the NetScaler ADM from the License Settings.



Uploading NetScaler VPX Images in NetScaler ADM

Add the NetScaler images to NetScaler ADM, so that the NetScaler ADM uses these images as defined in the service package.

To upload NetScaler VPX Images in NetScaler ADM:

1. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **ESX NSVPX Images**.
2. Click **Upload**, and select the NetScaler VPX zip package from the local storage folder.

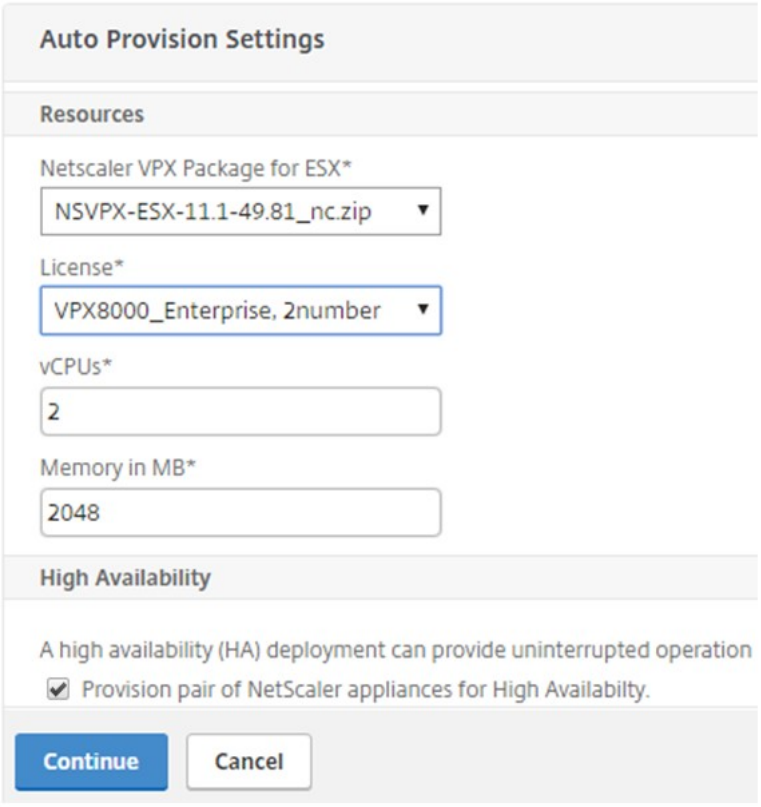
Creating Service Packages in NetScaler ADM

Create service packages in NetScaler ADM to define the set of SLAs, which states how the NetScaler resources are allocated.

To create service packages in NetScaler ADM:

1. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a) Name - name of a service package
   b) Isolation Policy - select **Dedicated**
   c) NetScaler Instance Provisioning - select **Create Instance OnDemand**
   d) Auto Provision Platform - select **CitrixNetScaler SDX**
   e) Click **Continue**
3. In the **Auto Provision Settings** section, select the recently uploaded NetScaler VPX zip package for deploying it on NSX platform, select the corresponding license, and click **Continue**.

   > **Note**
   >
   > In **High Availability** section, check the box to provision NetScaler instances for HA.



> **Note**
>
> The name of license displayed in the list box shown in the figure above, VPX8000_Advanced, 2 number is an example and is explained as below:
>
> - VPX - the license is to deploy NetScaler VPX instances
> - 8000 - consumable bandwidth is 8GB
> - Advanced - NetScaler provides three types of licenses - Standard, Advanced, and Premium
> - 2 number - two NetScaler VPX instances can be deployed by using this license
>
> The name of license displayed in the **License** list box depends on the license that you have purchased from Citrix.

4. Click **Continue**.
5. The service package is published to NSX Manager. In NSX Manager, navigate to **Service Definitions** > **Service Managers**. You can view NetScaler ADM as one of the service managers. This indicates that the registration is successful and bi-directional communication is established between the NSX manager and NetScaler ADM.

> **Note**
>
> For NetScaler ADM in high availability deployment, the licenses are uploaded only in the NetScaler ADM license server node. The NetScaler ADM nodes are in an active-passive mode.

Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the existing NSX Edge Gateway, that is, offload the load balancing function from NSX load balancer to NetScaler.

To insert load balancing service on NSX Edge Gateway:

1. In NSX Manager, navigate to **Home** > **Networking and Security** > **NSX Edges**, and double-click to select the edge gateway that you have configured.
2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.
3. Select **Enable Load Balancer** and **Enable Service Insertion** to enable them.
4. In **Service Definition**, select the service package that was published to NSX Manager.
5. Configure one virtual NIC for management interface, and one or more virtual NICs for data interfaces. Select the networks for management and data accordingly.

   > **Note**
   >
   > Select IP Pool option in Primary IP Allocation mode. NetScaler ADM does not support manual or DHCP allocation of IP addresses.

6. Click the refresh icon to see the creation of the run time.

   > **Note**
   >
   > Because you are deploying two NetScaler VPX instances in HA deployment, two run times are created in the NSX manager.
   >
   > You might have to refresh the screen to view the run times displayed on the screen.

7. Select the run time, click **Actions**, and select **Install** from the pop-up menu. For HA, repeat this for the other run time also.
8. When both the virtual machines start, the value of Status changes to “In Service”and that of Install State changes to “Enabled.”

   > **Note**
   >
   > You might have to refresh the screen to view the change in status.

9. In NetScaler ADM, navigate to **Orchestration** > **Requests** to see progress details of completion of service insertion. You can see that a request to create and update the run time has come in to NetScaler ADM. When the run time has been updated, select the request and click the **Tasks** button to view that NetScaler ADM has been added in NSX Manager.

   For HA, there will be two requests to create and update two run times in NetScaler ADM. When both run times have been updated, select both requests and click the **Tasks** button to view that two NetScaler ADM HA nodes have been added in NSX Manager.

10. In NetScaler ADM, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge Gateways**. In the right-hand side panel, you can view that the NetScaler VPX has been added to the NSX Edge Gateway.

    For HA, you can see that two NetScaler VPX instances in HA mode have been added to the NSX Edge Gateway.

11. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**. Select the NetScaler VPX license and the edition that you have installed.

    The NetScaler VPX instances that are in HA mode consume two licenses and the status is displayed on your screen as below.

    When the service insertion is complete, you can use StyleBooks to configure the NetScaler instances in one of the following two methods:

    - Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI

- Configuring Load Balancing Services on NetScaler VPX in NetScaler ADM GUI

Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI

Perform the following task to enable configuration of load balancing services on the NSX Edge gateway device using built-in StyleBooks.

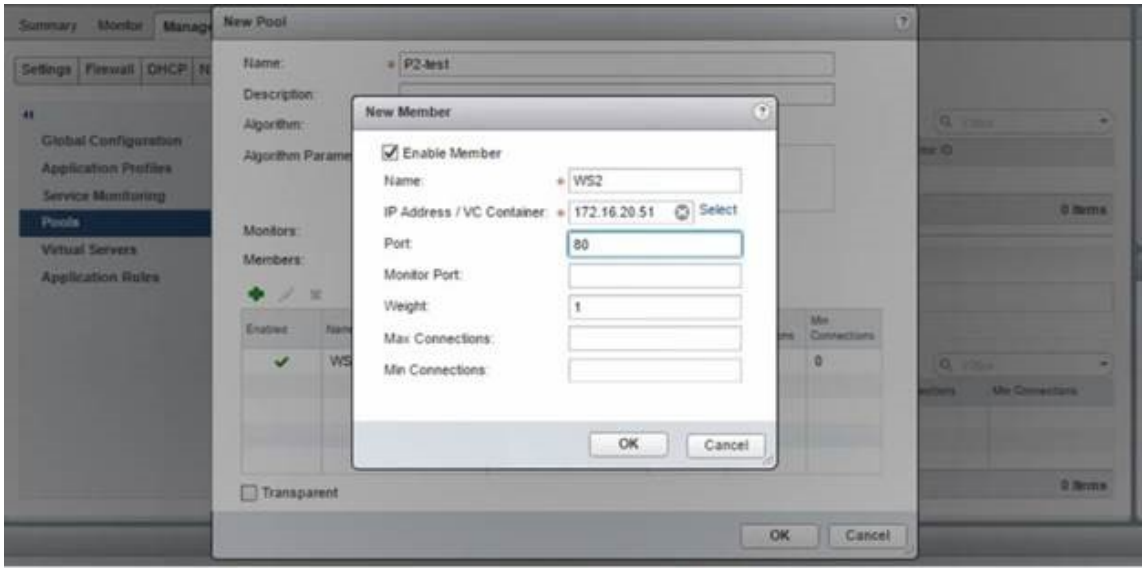
In NSX Manager, navigate to **Home** > **Networking and Security** > **NSX Edges**, and double-click to select the edge gateway that you have configured.

Creating pools and pool members

Create a pool of servers and members of different capacities.

1. Click **Manage**, and on the **Load Balancer** tab, select **Pools**, and click "**+**"icon to add a new pool, and set the following parameters:
    a) Name - Name of the new pool
    b) Algorithm - Select an algorithm from the drop-down list base on which the pool will be selected.
    c) Monitors - Make sure the service monitor is set to default_http_monitor
    d) Members - Click "+"to add members to the pool and enter the required parameters in the New Member window.
        i. Name - Name of the member
        ii. IP Address/ VC Container - Click Select to select the object from the available list or enter the IP address of the object.
2. Click **OK**.

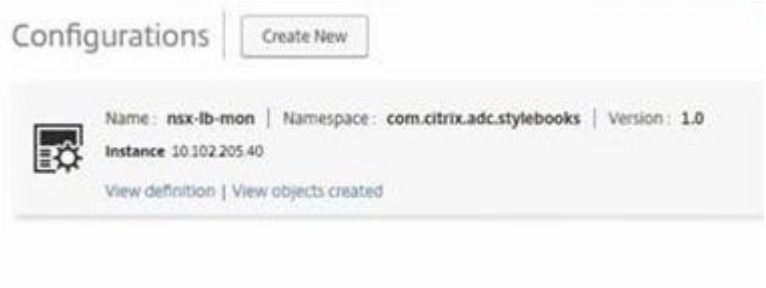
    Add as many members as required.



Creating virtual servers

Create a set of virtual servers and assign a pool to each virtual server.

1. Click **Manage**, and on the Load Balancer tab, select **Virtual Servers**, and click "**+**"icon to add a virtual server, and set the following parameters:
    a) Application profile - By default, the service profile that you created in NetScaler ADM is displayed.
    b) Name - Name of the virtual server.
    c) IP Address - Click Select to select an existing pool of IP addresses or create a new pool of IP addresses.
    d) Default pool - Select the default pool from the drop-down list.
2. Click **OK**.
3. In NetScaler ADM, navigate to **Orchestration** > **Requests** to see progress details of completion of service creation on one or more selected NetScaler instances.
4. In NetScaler ADM, navigate to **Applications** > **Configuration**, and check that the `nsx-lb-mon` config pack has been created.



Configuring Load Balancing Services on NetScaler VPX in NetScaler ADM GUI

Deploy load balancer configurations on the NetScaler instance using NetScaler ADM StyleBooks. For HA, the configuration is deployed on both NetScaler instances that are in HA.

To create configuration packs through StyleBooks:

1. In NetScaler ADM, navigate to **Applications** > **Configuration** > **Create New**, and select the **HTTP/SSL LoadBalancing (with Monitors) StyleBook** from the list. The StyleBook opens as a user interface page on which you enter the values for all the parameters defined in this StyleBook.
2. Specify values for all the required parameters.
3. Select the target NetScaler VPX instance that is provisioned in the NSX environment, and click **Create** to apply the configuration on the selected device. For HA deployment, select the instances that are in HA mode.

Verifying Creation of Virtual Servers and Service Groups in NetScaler VPX Instances

You can view that the service groups and virtual servers are created by login on to the NetScaler VPX instance.

To view the service groups and virtual servers:

1. Log on to the NetScaler VPX instance. For HA deployment, you must log on to both NetScaler instances that are in HA.
2. Navigate to **Configuration** > **System** > **Networking**. In the right pane, you can view the IP addresses that are added. Click the IP address hyperlink to see the details. You can see that the subnet IP address is same as the IP address of the web interface that was added in NSX.
3. Next, navigate to **Traffic Management** > **Load Balancing** > **Virtual Servers** and view the virtual server details.
4. Next, navigate to **Service Groups** and view the service group details.

5. Finally, navigate to **Configuration** > **System** > **Licenses** to view the licenses that are applied to this instance.

Deleting Load Balancing Services

When the load balancing services are no longer required on the NetScaler VPX instances deployed on the NSX manager, you can delete the service insertions that were performed earlier.

To delete configuration and service insertion:

1. In NetScaler ADM, Navigate to **Applications** > **Configuration**, select the application configuration created, and then delete the configuration by clicking the "X"icon.
2. In NSX Manager, navigate to the edge gateway to which the NetScaler VPX instance is connected. Navigate to **Manage** > **Load Balancer** > G**lobal Configuration**, right-click on the runtime entry, and then click **Unprovision**. The virtual machine is rendered out of service.
3. In NetScaler ADM, navigate to **Orchestration** > **Cloud Orchestration** > **Edge Gateways**. Ensure there is no respective mapping of Edge gateway to deleted instance.

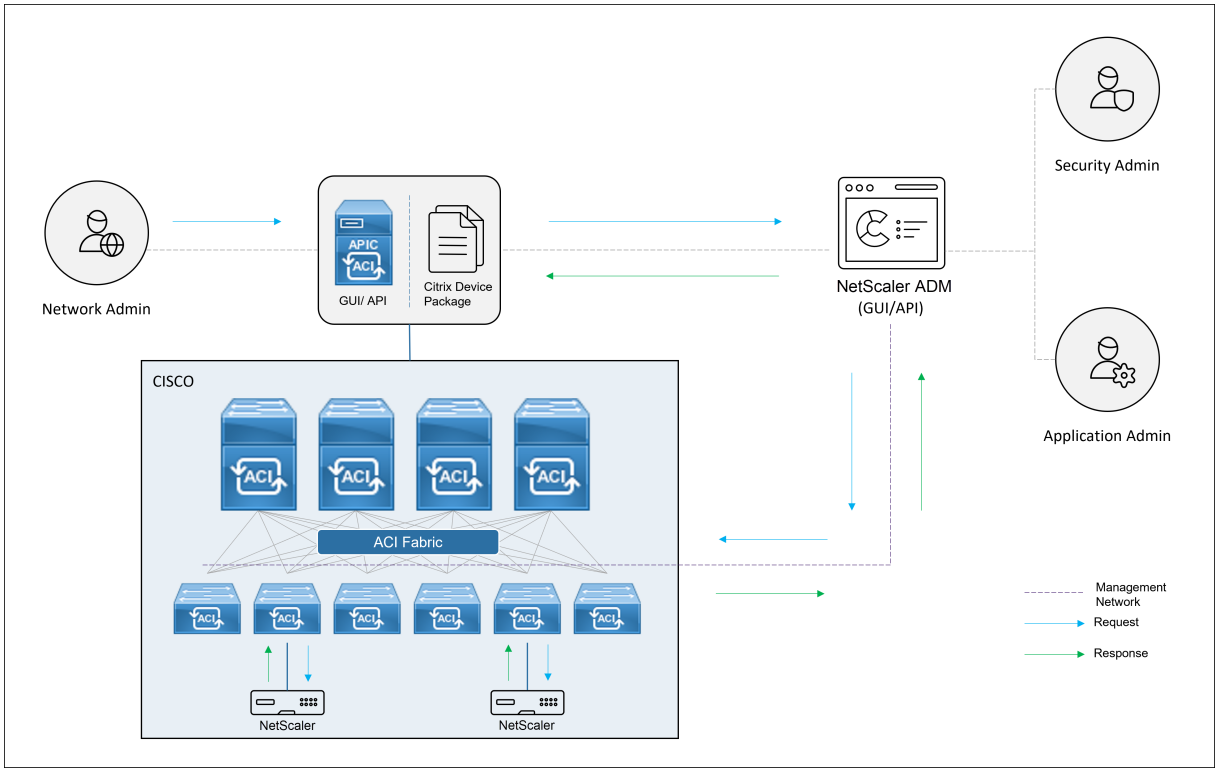
NetScaler automation using NetScaler ADM in Cisco ACI hybrid mode

March 11, 2024

Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to NetScaler Application Delivery Management (ADM), which acts as a Device Manager in the APIC.

The NetScaler Hybrid Mode solution is supported by a hybrid mode device package and NetScaler ADM. You need to upload the hybrid mode device package in the APIC. This package provides all network L2-L3 configurable entities from NetScaler. Application parity is mapped by StyleBook from NetScaler ADM to the APIC. In other words, StyleBook acts as reference between L2-L3 and L4-L7 configurations for a given application. You must provide a StyleBook name while configuring the network entities from the APIC for NetScaler.

The following illustration provides an overview of NetScaler in a hybrid mode solution:

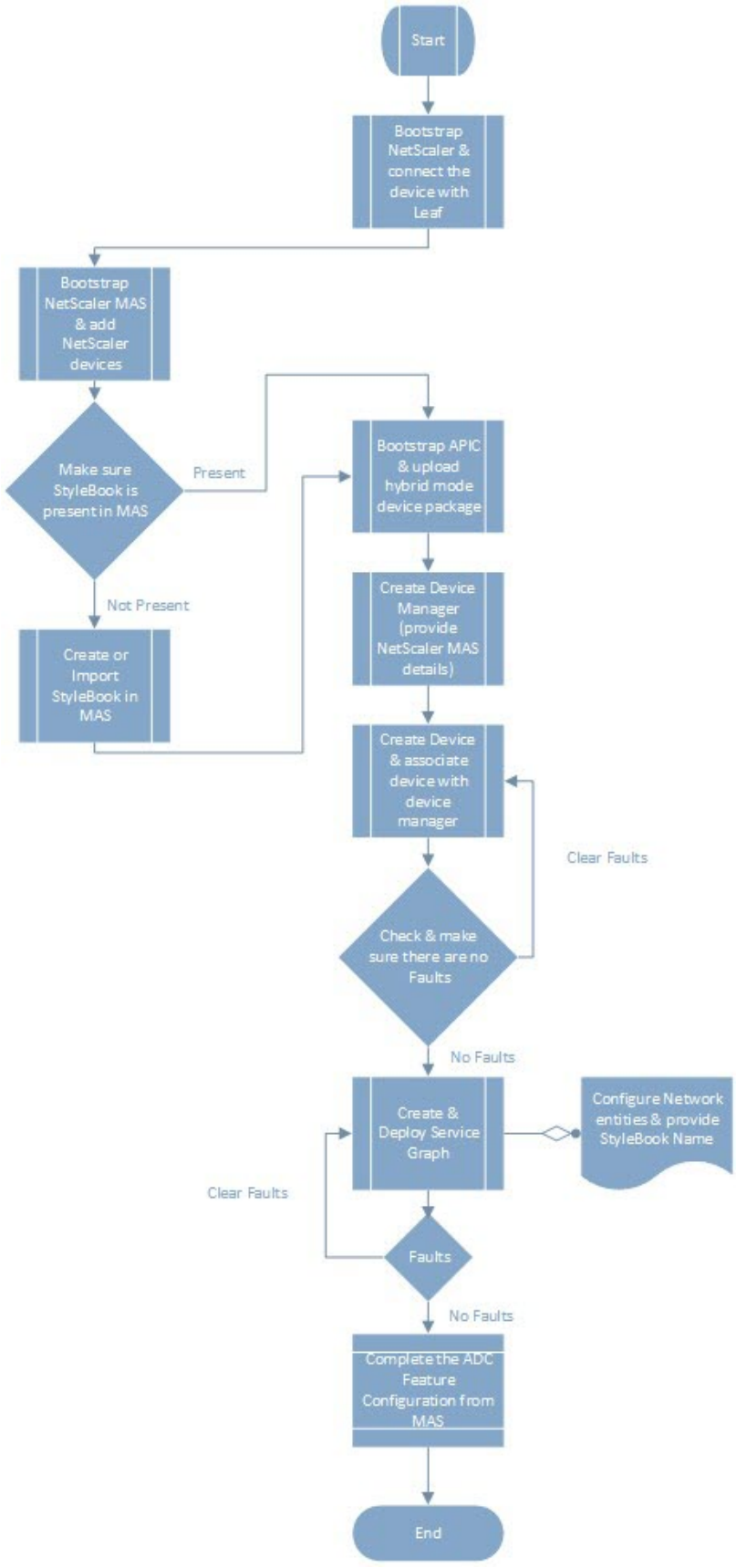


In Hybrid Mode, the NetScaler configuration is performed in the following two phases:

1. Network stitching is done from the Cisco APIC
2. Configuration is done from the NetScaler ADM

For any given application, a network administrator has to provide network specific details, such as IP addresses, port, VLAN (automated) and so on, as part of the service graph creation and deployment in the Cisco APIC. These configuration details are then pushed to NetScaler ADM through the device package, and NetScaler ADM internally processes them and configures the NetScaler. An application administrator creates the application's ADC related configuration by using StyleBook in NetScaler ADM, and these configurations are then pushed from NetScaler ADM to the NetScaler. The Cisco APIC and NetScaler ADM communicate with the ADC through the management network.

The following diagram shows a NetScaler workflow in the hybrid solution:



NetScaler device package in Cisco ACI's cloud orchestrator mode

March 11, 2024

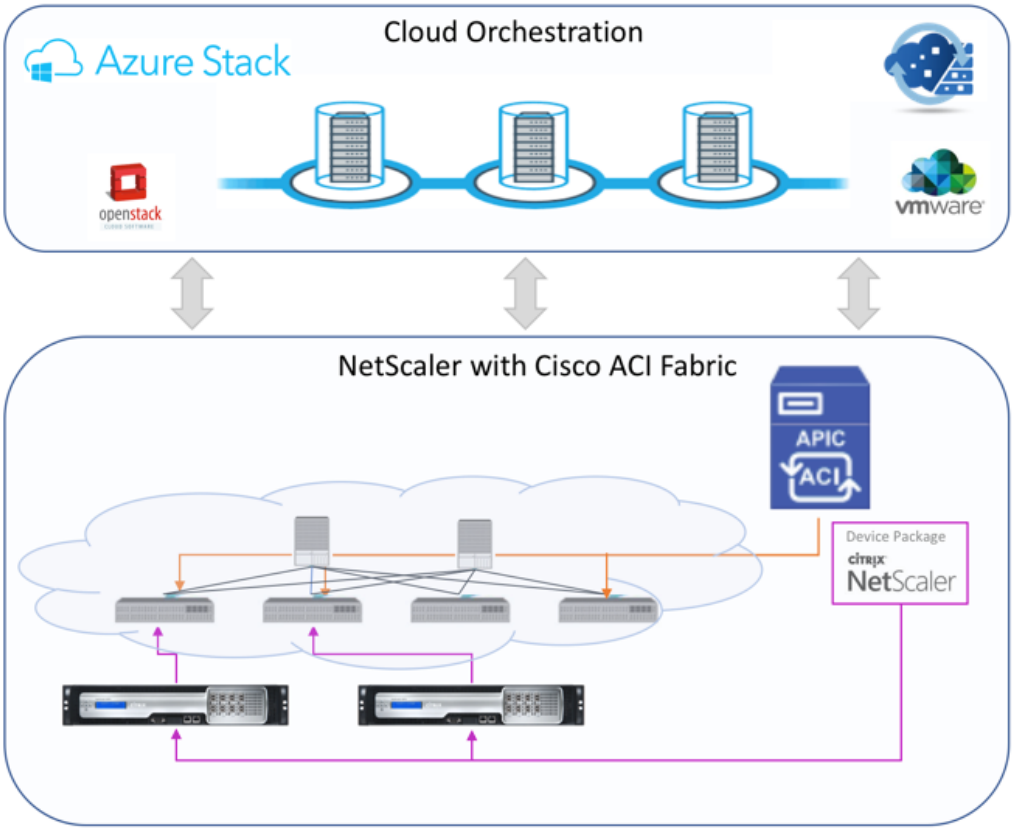
With Application Policy Infrastructure Controller (APIC) version 3.1 Citrix NetScaler, and Cisco ACI expand the joint integration portfolio to provide a new solution addressing customer's needs. The new integration mode, ACI Cloud Orchestrator Mode, simplifies L4-L7 integrations by abstracting configuration complexity through standardized parameters. The solution works seamlessly to automate L4-L7 services, achieving the goals of agile application deployments, operational flexibility, and simplicity.

The Cisco ACI cloud orchestrator mode by using NetScaler solution provides the following benefits:

- Automation of L4-L7 services reduces the human error.
- The pre-built integration of Cisco ACI solution helps you in reducing the deployment time, and increases the performance of applications, such as web applications, virtual machines, and SQL.
- Fully integrated visibility into the health of applications such as web applications, virtual machines, and SQL across physical and virtual network components.

The ACI cloud orchestrator mode now gives you more choices to utilize the new simplified APIC GUI directly or by selecting any cloud orchestrator, such as Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize, or any other based on your preference. This new change is achieved by exposing a set of ADC attributes as ADC schema. These attributes are mapped in the device packages function profiles. You can provide values for these attributes while provisioning the ADC service by the cloud orchestrator (Cisco Cloud Center or Wireless Application Protocol (WAP)).

The following illustration provides an overview of NetScaler in a cloud orchestration solution:

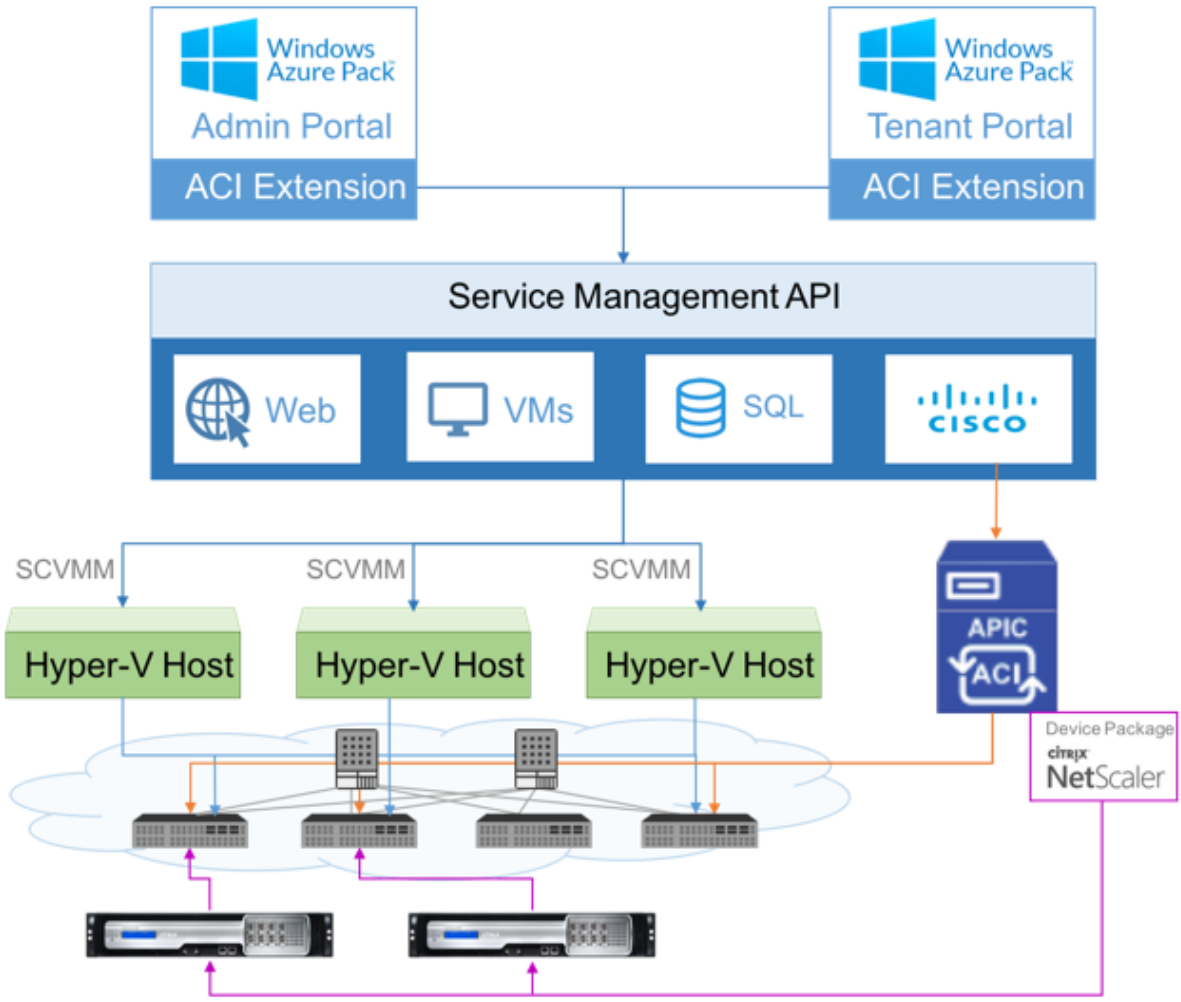


The cloud orchestrator mode solution using Microsoft Azure Pack involves many integration points, such as Azure Pack to Cisco APIC, Cisco APIC to System Central virtual machine Manager (SCVMM), and Cisco APIC to NetScaler. As a tenant in the private cloud, you can enable NAT, provision network services, and can add a load balancer.

Azure Pack supports tenant and administrator portals, and each of them has their own set of operations that can be performed.

- As an administrator, you can perform administrative tasks such as ACI registration, VIP range, NetScaler device association with virtual machine cloud, and tenant user account creation.
- As a tenant, you can perform tasks such as log on to the Azure Pack tenant Portal and configure the network, bridge domains, and Virtual Routing and Forwarding (VRFs), and can use the NetScaler load balancing and RNAT features.

The following illustration provides an overview of Azure Pack in a cloud mode solution:



Important

- Cloud administrator can facilitate with L4-L7 schema supported by APIC and any additional changes can be done by APIC administrator directly in the APIC. This allows you to configure and deploy NetScaler at par with the supported feature set.
- Tenants can deploy multiple VIP addresses with different ports for the same network. You must ensure that the IP and port combination is unique.
- The NetScaler device package supports only single-context deployment. Each tenant gets a dedicated NetScaler instance.
- Wireless Application Protocol (WAP) supports NetScaler MPX appliances and NetScaler VPX appliances (includes NetScaler VPX instances deployed on the NetScaler SDX platform).

The cloud orchestrator mode device package supports both fully managed mode and service manager mode. The fully managed mode package supports a wide variety of function profiles, such as simple

load balancing, content switching, SSL offload, and other profiles. These function profiles cover a complete feature set and deployment mode of the NetScaler. Similarly, service manager mode device package supports one-arm and two-arm configuration and deployment of NetScaler using APIC. The NetScaler Application Delivery Management (ADM) acts as service manager for APIC and you can use NetScaler ADM to configure NetScaler L4-L7 parameters.

> **Note**
>
> In service manager mode (hybrid mode), you cannot reuse or reassign the same server IP address, which is already present in the NetScaler appliance.

Cloud orchestrator mode function profile has a set of parameters mapped to APICs ADC schema and the orchestrator uses these parameters. The cloud orchestrator provides the values for ADC parameters (VIP, while provisioning the NetScaler through APIC). The orchestrator communicates with APIC's APIs and passes the ADC specific details as part of the payload for a specific function profile. Internally, APIC extracts the values and passes them to the device package which configures the NetScaler internally.

For more information on the complete list of ADC schema's, which are supported by Cisco APICs, see Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x and earlier).

The fully managed mode device package supports the following function profiles:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM

16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

The service manage mode device package supports the following cloud mode function profiles:

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler supports the above-mentioned function profiles. The APIC supports a subset of these parameters in the ADC schema. If there are any unsupported attributes by Cisco ACI present in the function profile, you have to clone the cloud orchestrator mode function profile and provide the values for all unsupported attributes by APIC and must save the attributes. Later, the orchestrator can use the newly cloned function profile.

Citrix Cloud Mode Device Package supports NetScaler 12.0 and service manager mode uses NetScaler ADM 12.0 as well. Device package has changed the model version from 1.0 to 2.0 and can be used as a new install. Cloud orchestrator Mode Device package cannot be upgraded from previous device package versions since the model version is changed.

Cloud orchestrator Mode device packages can be used in regular deployment as well. The package does not mandate user to provision NetScaler through any cloud orchestrator. The device package is compatible with just APIC and APIC with cloud orchestrator.

Manage the Kubernetes Ingress configuration in NetScaler ADM

March 11, 2024

Kubernetes (K8s) is an open source container orchestration platform that automates the deployment, scaling, and management of cloud-native applications.

Kubernetes provides the Ingress feature which allows client traffic outside the cluster to access microservices of an application running inside the Kubernetes cluster. ADC instances can act as the Ingress to applications running inside a Kubernetes cluster. ADC instances can load balance and content route North-South traffic from the clients to any microservices inside the Kubernetes cluster.

> **Note**
>
> - NetScaler ADM supports the Ingress feature on the clusters with Kubernetes version 1.14–1.21.
> - NetScaler ADM supports NetScaler VPX and MPX appliances as Ingress devices.
> - In the Kubernetes environment, the NetScaler instance load balances only the "NodePort" service type.

You can configure multiple ADC instances to act as Ingress devices on the same cluster or different clusters or namespaces. After you configure the instances, you can assign each instance to different applications based on the Ingress policy.

You can create and deploy an Ingress configuration using Kubernetes `kubectl` or APIs. You can also configure and deploy an Ingress from NetScaler ADM.

You can specify the following aspects of Kubernetes integration in ADM:

- **Cluster** –You can register or unregister Kubernetes clusters for which ADM can deploy Ingress configurations. When you register a cluster in NetScaler ADM, specify the Kubernetes API server information. Then, select an ADM agent that can reach the Kubernetes cluster and deploy Ingress configurations.
- **Policies** –Ingress policies are used to select the ADC instance based on cluster or namespace to deploy an Ingress configuration. Specify the cluster, site, and instance information when you add a policy.
- **Ingress Configuration** –This configuration is the Kubernetes Ingress configuration, which includes the content switching rules and the corresponding URL paths of the microservices and their ports. You can also specify the SSL/TLS certificates (to offload SSL processing on the ADC instance) using Kubernetes secret resources.

The NetScaler ADM automatically maps the Ingress configurations to ADC instances using Ingress policies.

For each successful Ingress configuration, NetScaler ADM generates a StyleBook ConfigPack. The ConfigPack represents the ADC configuration applied to the ADC instance that corresponds to the Ingress configuration. To view the ConfigPack, navigate to **Applications > StyleBooks > Configurations**.

Before you begin

To use NetScaler instances as Ingress devices on Kubernetes clusters, ensure you have:

- Kubernetes cluster in place.
- Kubernetes cluster registered in NetScaler ADM.

Configure the NetScaler ADM with a secret token to manage a Kubernetes cluster

For NetScaler ADM to be able to receive events from Kubernetes, you need to create a service account in Kubernetes for NetScaler ADM. And, configure the service account with the necessary RBAC permissions in the Cluster.

1. Create a service account for NetScaler ADM. For example, the service account name can be `citrixadm-sa`. To create a service account, see Use Multiple Service Accounts.
2. Use the `cluster-admin` role to bind the NetScaler ADM service account. This binding grants a `ClusterRole` across the cluster to a service account. The following is an example command to bind a `cluster-admin` role to the service account.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
      =cluster-admin --serviceaccount=default:citrixadm-sa
   <!--NeedCopy-->
   ```

   After binding the NetScaler ADM service account to the `cluster-admin` role, the service account has the cluster-wide access. For more information, see `kubectl create clusterrolebinding`.
3. Obtain the token from the created service account.

   For example, run the following command to view the token for the `citrixadm-sa` service account:

   ```
   kubectl describe sa citrixadm-sa
   <!--NeedCopy-->
   ```
4. Run the following command to obtain the secret string of the token:

   ```
   kubectl describe secret <token-name>
   <!--NeedCopy-->
   ```


Add the Kubernetes cluster in NetScaler ADM

After you configure a NetScaler agent and configure static routes, you must register the Kubernetes cluster in NetScaler ADM.

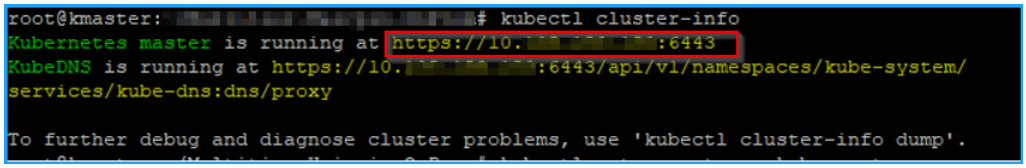
To register the Kubernetes cluster:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**.
   The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

   a) **Name** - Specify a name of your choice.

   b) **API Server URL** - You can get the API Server URL details from the Kubernetes main node.

      i. On the Kubernetes main node, run the command `kubectl cluster-info`.

      ii. Enter the URL that displays for **"Kubernetes master is running at."**

   c) **Authentication Token** - Specify the authentication token string obtained while you configure NetScaler ADM to manage a Kubernetes cluster. The authentication token is required to validate access for communication between the Kubernetes cluster and NetScaler ADM. To generate an authentication token:

      i. On the Kubernetes main node, run the following commands:

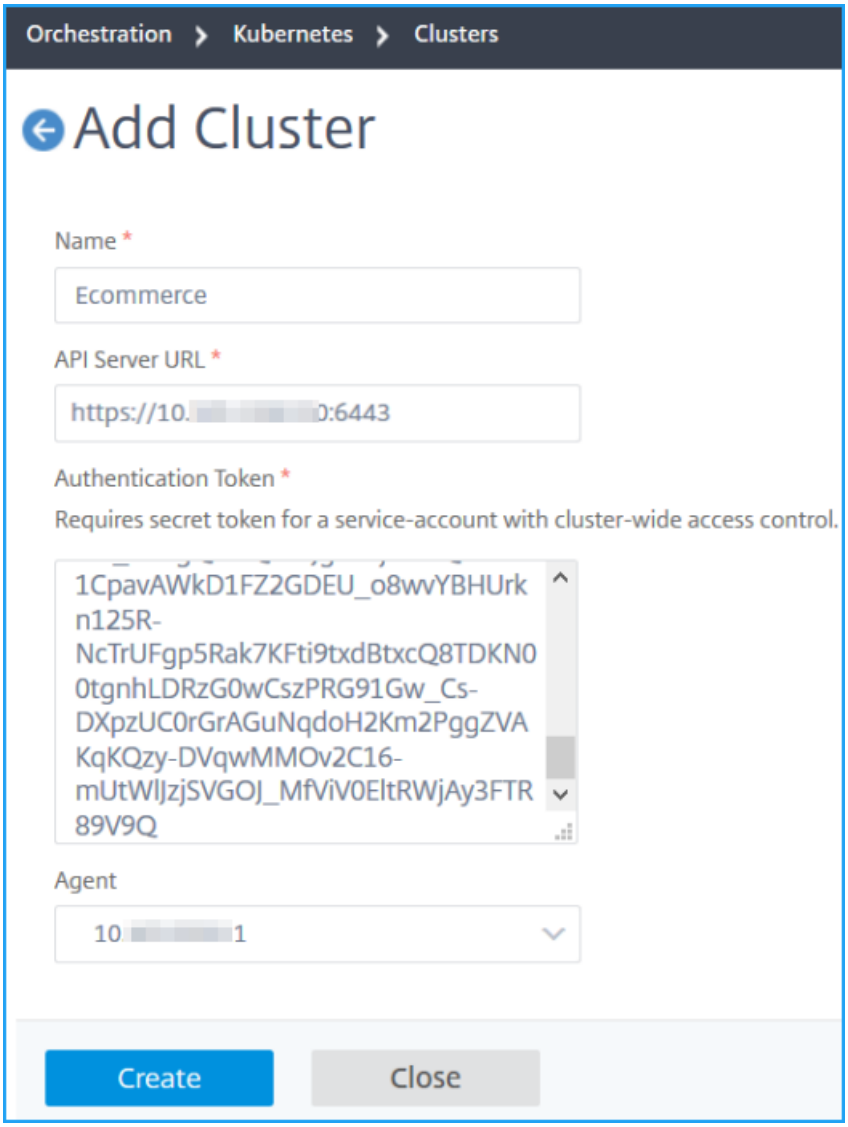
      ```
      kubectl describe secret <token-name>
      <!--NeedCopy-->
      ```

      ii. Copy the token that is generated and paste it as the Authentication Token

      For more information, see Kubernetes documentation.

   d) Select the agent from the list.

   e) Click **Create**.



Define an Ingress policy

The Ingress policy decides which NetScaler is used to deploy an Ingress configuration, based on the Ingress Cluster or Namespace.

1. Navigate to **Orchestration > Kubernetes > Policy**.
2. Click **Add** to create a policy.
    a) Specify the policy name.
    b) Define **Conditions** to deploy the Ingress configuration on a Kubernetes cluster. These conditions are typically based on Ingress Cluster and Namespace.
    c) In the Infrastructure panel,

- **Site** - Select a site from the list.
- **Instance** - Select the ADC instance from the list.

The **Site** and **Instance** lists populate the options based on the cluster selection in the **Conditions** panel.

These lists display the sites or instances that are associated with the NetScaler agent configured with the Kubernetes cluster.

d) In **Choose Network**, select the network from which ADM auto-assigns the virtual IP addresses to an Ingress configuration.

This list displays the networks created in **Infrastructure > IPAM**.

e) Click **Create**.

Deploy the Ingress configuration

You can deploy the Ingress configuration from Kubernetes using `kubectl`, Kubernetes API, or other tools. You can also deploy the Ingress configuration directly from NetScaler ADM.

1. Navigate to **Orchestration > Kubernetes > Ingresses**.
2. Click **Add**.
3. In the **Create Ingress** field, specify the following details:

   a) Specify the name of the Ingress.

   b) In **Cluster**, select the Kubernetes cluster on which you want to deploy an Ingress.

   c) Select the **Cluster Namespace** from the list. This field lists the namespaces that are present in the specified Kubernetes cluster.

   d) Optional, select **Auto Assign Frontend IP address**.

   e) Select **Ingress Protocol** from the list. If you select **HTTPS**, specify **TLS secret**.

   This secret embeds the Kubernetes secret resource that embeds the HTTPS certificate and private key.

   An HTTPS Ingress requires a TLS based secret configured on the Kubernetes cluster. Specify the `tls.crt` and `tls.key` fields to include the server certificate and the certificate key respectively.

   f) For content routing, specify the following details:

   - **URL paths** - Specify the path that is associated with the Kubernetes service and port.
   - **Kubernetes service** - Specify the desired service.

- **Port** - Specify the service port.
- **LB method** - Select the preferred load-balancing method to the selected Kubernetes service.

  The selected method updates the Ingress Specification with an appropriate annotation. For example, if you select **ROUNDROBIN** method, the Citrix annotation appears as follows:

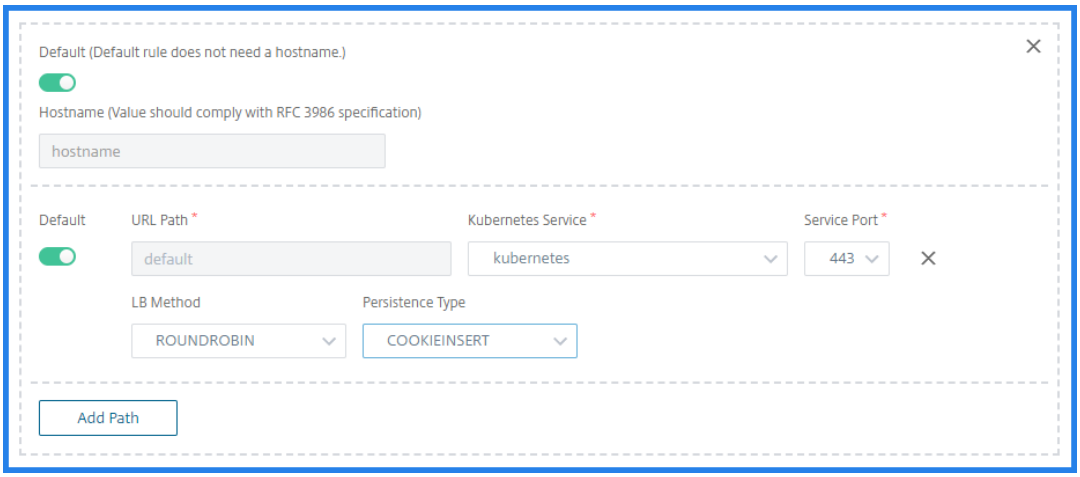
```
"lbmethod":"ROUNDROBIN"
<!--NeedCopy-->
```

- **Persistence Type** - Select the preferred load-balancing persistence type to the selected Kubernetes service.

  The selected persistence type updates the Ingress Specification with an appropriate annotation. For example, if you select **COOKIEINSERT**, the Citrix annotation appears as follows:

```
"persistenceType":"COOKIEINSERT"
<!--NeedCopy-->
```

Click **Add** to add more URL paths and ports to the Ingress configuration.



After deployment, the Ingress configuration redirects the client traffic to a specific service based on the following:

- The requested URL path and port.
- The defined LB method and persistence type.

> **Note**
>
> Kubernetes Services used in an Ingress Configuration are expected to be of type NodePort.

g) Optional, specify an **Ingress Description**.

h) click **Deploy**.

If you want to review the configuration before you deploy, click **Generate Ingress Spec**. The specified Ingress configuration appears in the YAML format. After reviewing the configuration, click **Deploy**.

> **Note**
> Apply licenses to the virtual servers that are created using Ingress configurations. To apply license, perform the following steps:
>
> 1. Go to **Settings > Licensing & Analytics Configuration**.
> 2. Under **Virtual Server License Summary**, enable **Auto-select virtual servers**.

Video Insight

March 11, 2024

The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by NetScaler appliances to improve customer experience and operational efficiency, providing benefits such as:

- Manage the network during congestion in peak hours.
- Improve video play consistency and reduce video stalling.
- Enable new video service offerings (for example, Binge-on video services).
- Enable customers to select the best sustainable video quality.
- Provide a consistent user experience for the subscriber.

While optimizing the video traffic, the NetScaler appliance uses a special mechanism to dynamically pace the video bit-rate and a random sampling technique to estimate the savings from the optimization technique. For more information about the NetScaler Video Optimization feature, see Video Optimization. When you integrate NetScaler appliance with NetScaler Application Delivery Management (ADM), it collects key information from the video data flowing through the NetScaler appliance. You can use this information to compare the optimized and unoptimized performance of the ABR video traffic, determine the savings due to optimization and so on.

> **Note**
>
> The statistics of the unoptimized sessions provided in NetScaler ADM corresponds to the sessions

> that you had selected of random sampling in NetScaler appliance. For more information about Random Sampling, see Video Optimization.

Video Insight in NetScaler ADM provides metrics for the following types of video traffic:

- Progressive Download (PD) videos over HTTP
- ABR videos over HTTP
- ABR videos over HTTPS
- YouTube ABR videos over QUIC

Configuring Video Insight

> **Note**
>
> Video Insight is supported on NetScaler instances with NetScaler Premium license. The NetScaler Premium license is supported for NetScaler Telco platforms (VPX T1000 and VPX-T).

To configure Video insight on a NetScaler instance, first enable the AppFlow feature, configure an AppFlow collector, action, and policy, and bind the policy globally. When you configure the collector, you must specify the IP address of the NetScaler ADM server on which you want to monitor the reports.

To configure video insight on a NetScaler instance, run the following commands to configure an AppFlow profile and policy and bind the AppFlow policy globally.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode `ulfd`

enable feature AppFlow

Sample

```
1 add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
     Transport logstream
2 set appflow param -videoInsight ENABLED
```



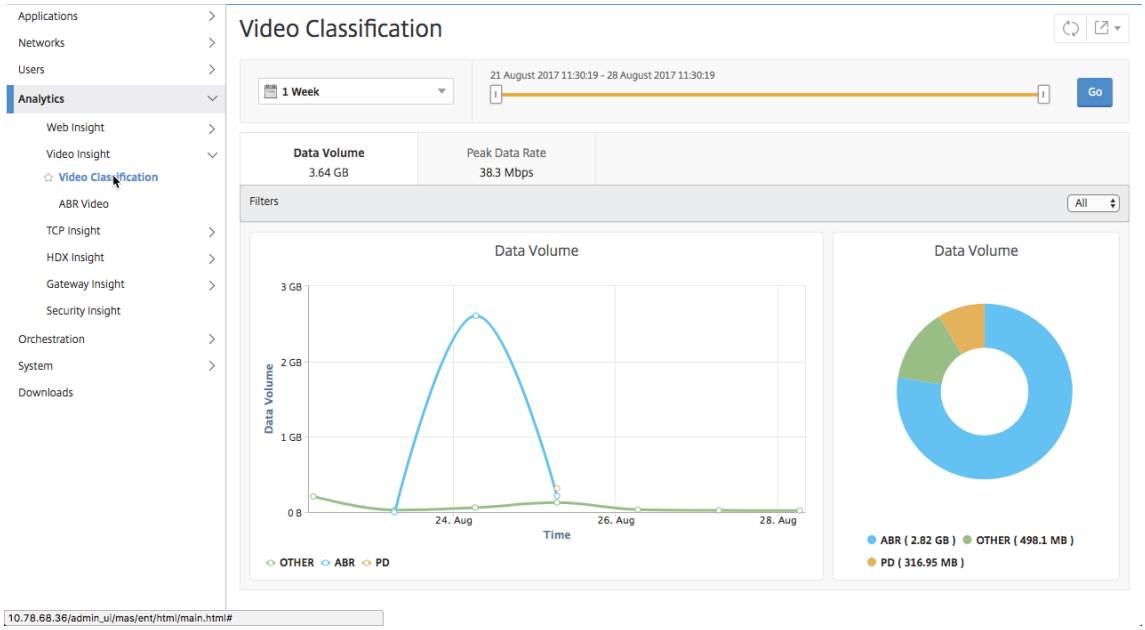
```
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Viewing the Video Insight metrics in NetScaler ADM

After enabling Video Insight in NetScaler ADM, you can view video optimization metrics such as, video classification, data volume, peak data rate, and ABR video plays. These metrics help you analyze your network and optimize the videos for improved subscriber experience, operational efficiency, and other performance criteria.

To view the Video Insight metrics in NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM virtual appliance (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Analytics > Video Insight**.



> **Note**
>
> The values provided by the legend **OTHER** in the charts represent the non-ABR and non-PD data in the video traffic depending on the filter you have selected:
>
> - **All** –Sum of non-ABR (HTTP, HTTPS, and QUIC) and non-PD (HTTP) data in the video traffic.

- **HTTP** –Sum of non-ABR and non-PD data in the video traffic.
- **HTTPS** –Sum of non-ABR video data in the video traffic.
- **QUIC** –Sum of non-ABR video data in the video traffic.

View network efficiency

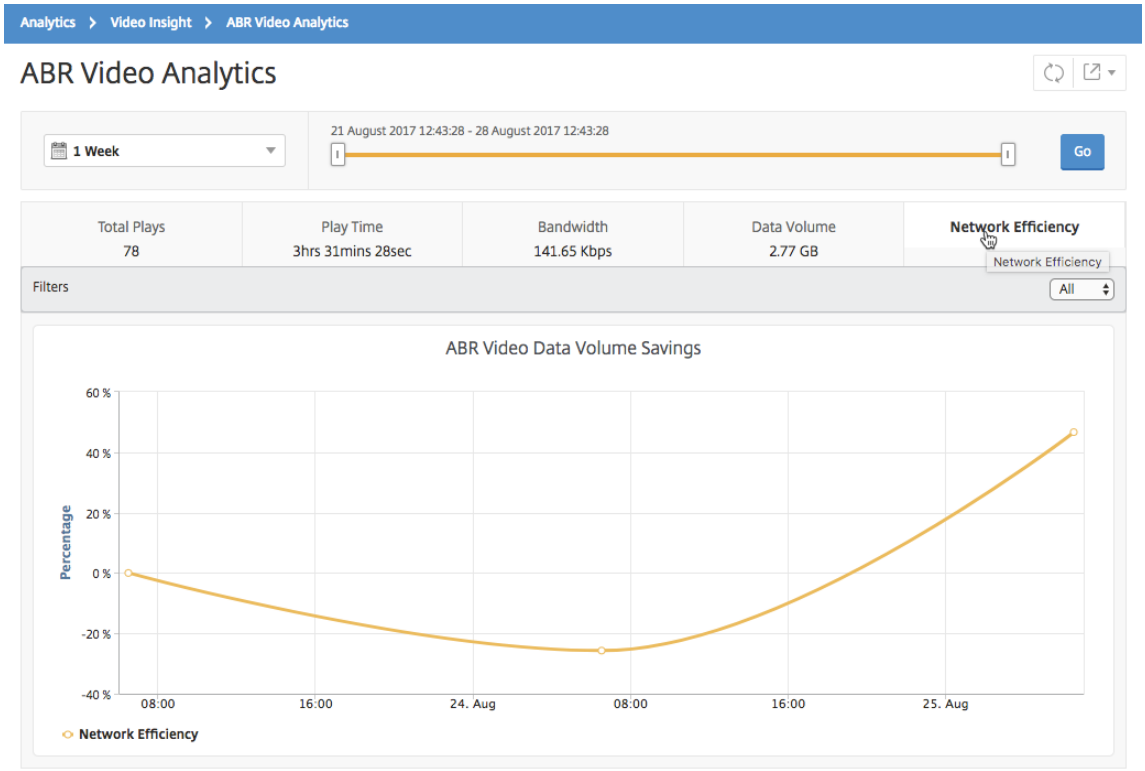
December 31, 2023

For a given time frame, NetScaler Application Delivery Management (ADM) provides a graph that shows the ratio of optimized to unoptimized video sessions in the time frame. It also displays the percentage of bandwidth saved by optimization. The percentage of bandwidth saved is calculated with the following formula:

Percentage of bandwidth saved = **Average optimized ABR video Data Volume / Average of unoptimized ABR Video Data Volume**.

To see the percentage of bandwidth saved by optimization:

1. Navigate to **Analytics > Video Insight**, and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select the **Network Efficiency** tab.



Compare the data volume used by optimized and unoptimized ABR videos

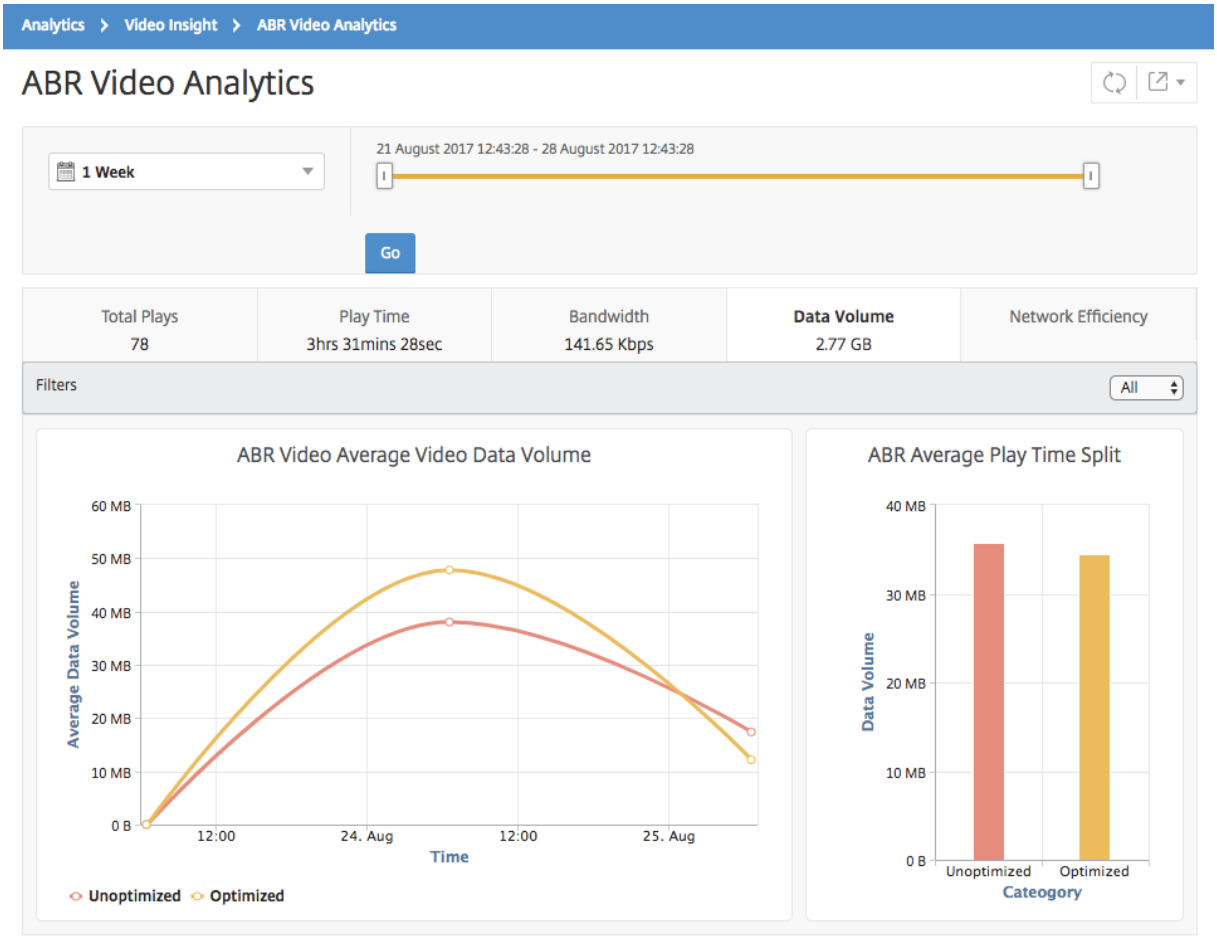
December 31, 2023

For a given time frame, NetScaler Application Delivery Management (ADM) shows the data volume used by optimized and unoptimized ABR videos, so that you can compare the two volumes.

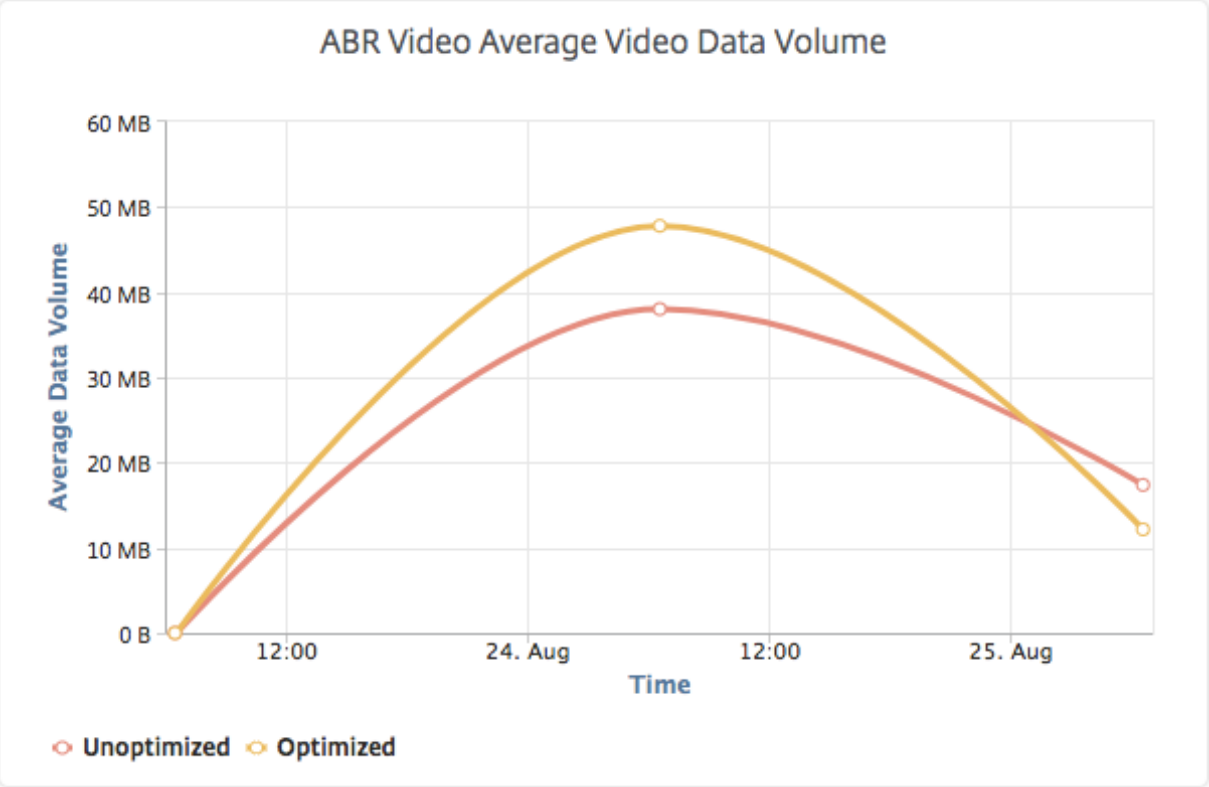
To see the data volume used by ABR videos:

1. Navigate to **Analytics > Video Insight**, and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select the **Data Volume** tab.

You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



The **Data Volume** tab provides a line graph and pie chart describing the average data volume used by ABR videos, and the data volume consumed by optimized and unoptimized ABR videos from your network for the selected time frame. You can hover your mouse pointer on the line graph to view the average data volume used during a particular time frame:



View the type of videos streamed and data volume consumed from your network

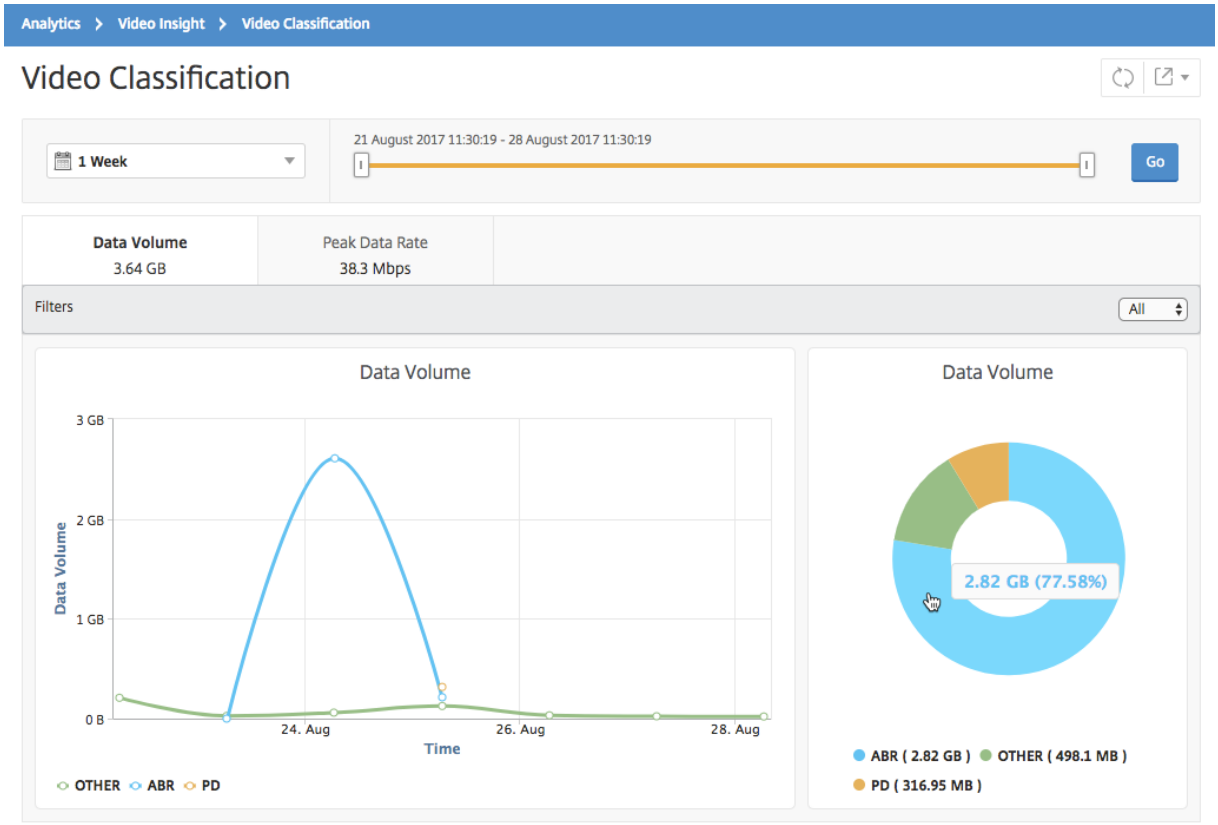
December 31, 2023

The NetScaler appliance detects the encrypted or unencrypted video traffic in your network and the type of video streaming (PD or ABR). NetScaler Application Delivery Management (ADM) displays these metrics and the data volume consumed by the video traffic for a defined time frame.

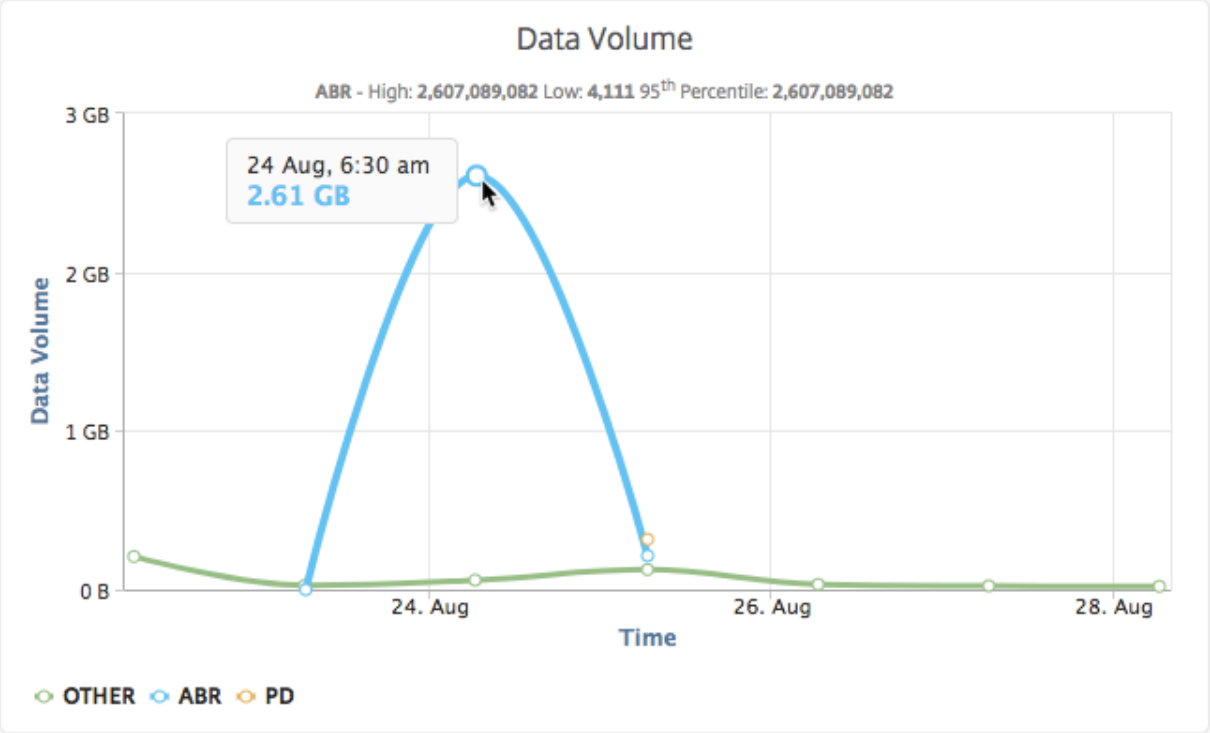
To see the types of videos and the consumed data volume:

1. Navigate to **Analytics > Video Insight** and click **Video Classification**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go**.

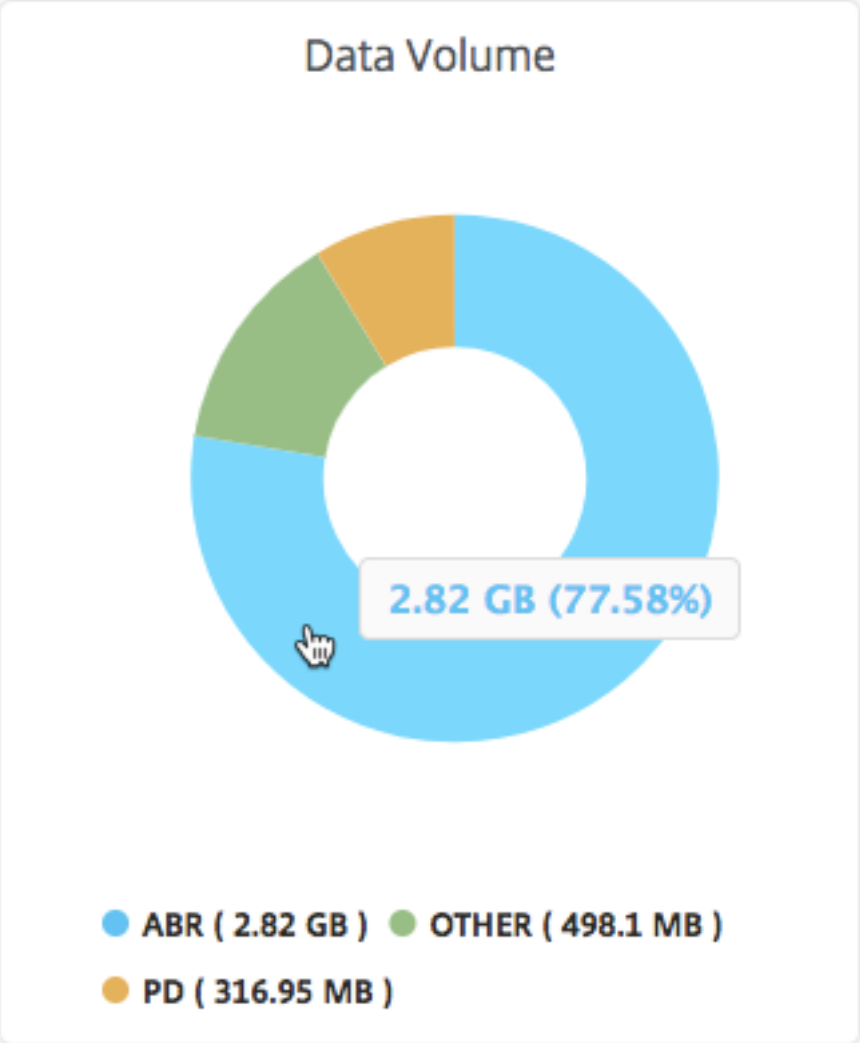
You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.



The **Data Volume** tab provides a line graph and pie chart showing the types of video traffic streaming from your network and the data volume consumed by your network. You can hover your mouse pointer on the line graph to view the data consumed during a particular time frame:



Also, you can hover your mouse pointer on the pie chart to view the percentage of data volume consumed by a particular type of video traffic.



Compare optimized and unoptimized play time of ABR videos

December 31, 2023

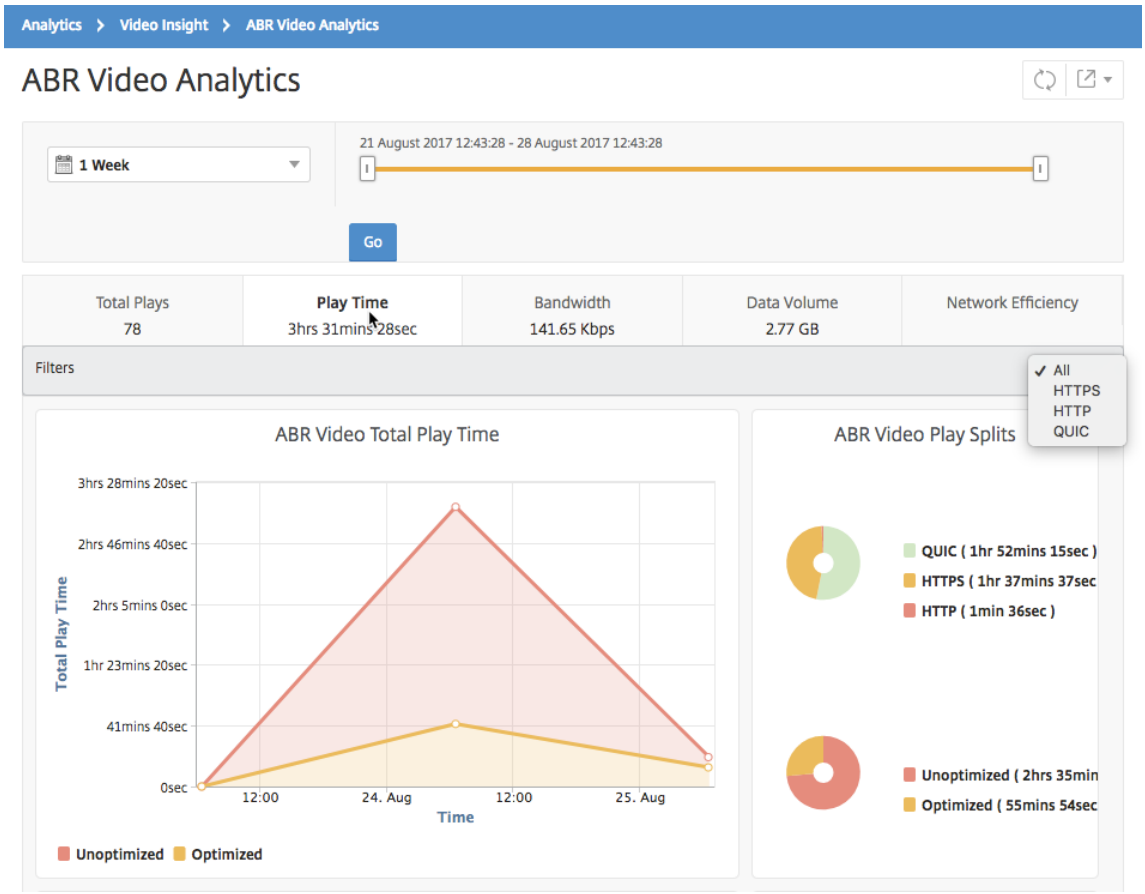
For a given time frame, NetScaler Application Delivery Management (ADM) provides the play time of ABR videos and also enables you to compare the play time of optimized and unoptimized ABR videos in your network.

To view the play time:

1. Navigate to **Analytics > Video Insight** and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.

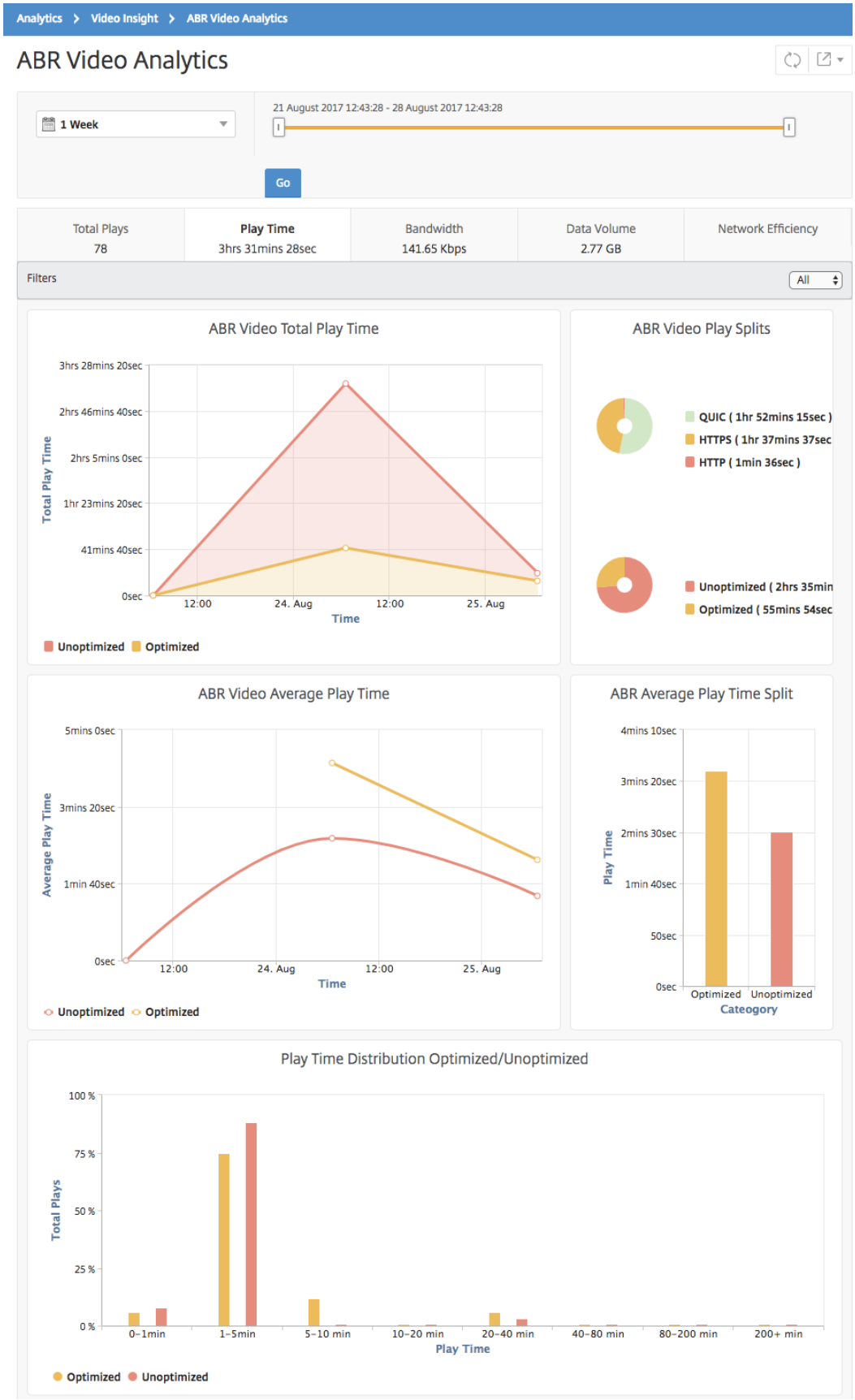
3. Click **Go** and select **Play Time** tab.

   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



For the selected time frame, the **Play Time** tab provides a line graph and pie chart describing the:

- Total play time of ABR videos from your network
- Total play time of optimized and unoptimized plays of ABR videos from your network for the selected time frame
- Total play time of encrypted and unencrypted ABR videos
- Average play time of ABR videos
- Average play time of optimized and unoptimized plays of ABR videos
- Average play time of encrypted and unencrypted ABR videos
- Play time distribution between optimized and unoptimized ABR videos



Compare bandwidth consumption of optimized and unoptimized ABR videos

December 31, 2023

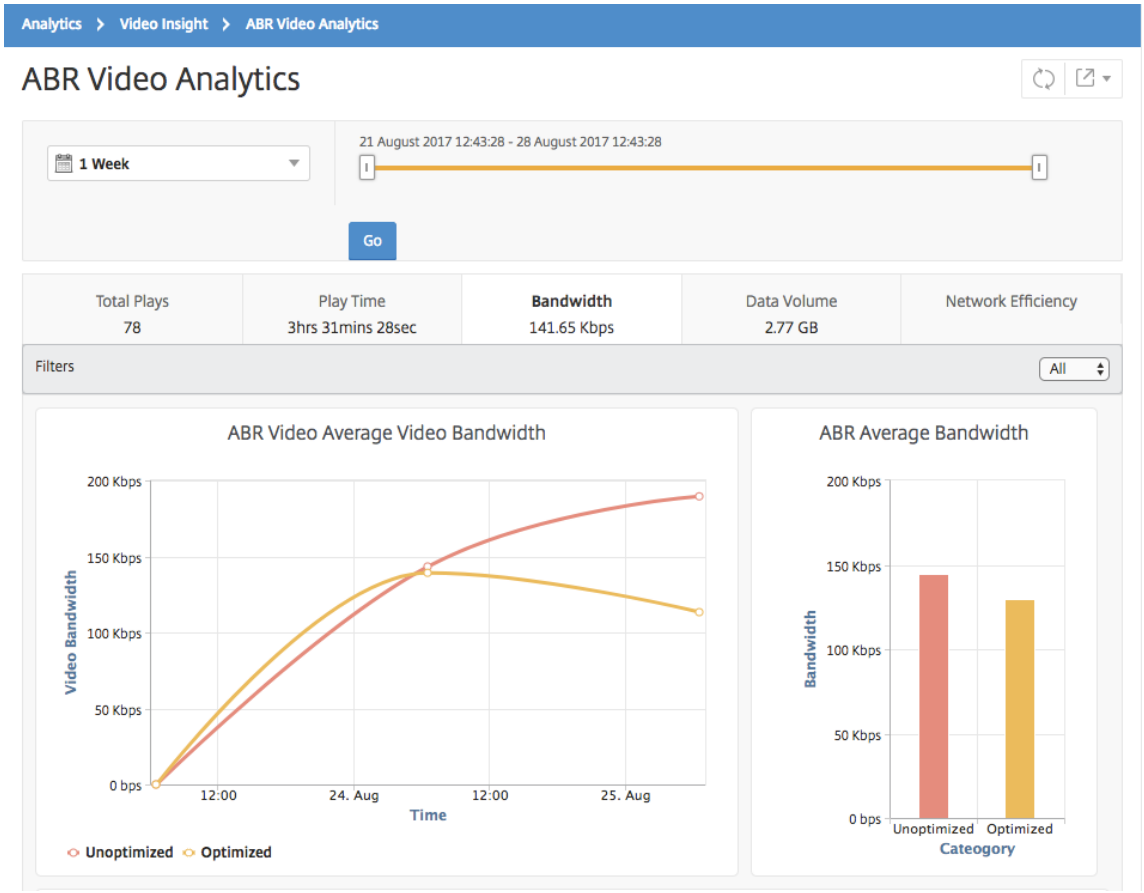
For a given time frame, NetScaler Application Delivery Management (ADM) provides the bandwidth consumed by optimized and unoptimized of ABR videos and also enables you to compare the bandwidth consumed by optimized and unoptimized ABR videos in your network based on:

- Play Time
- Data Volume

To view the bandwidth consumption:

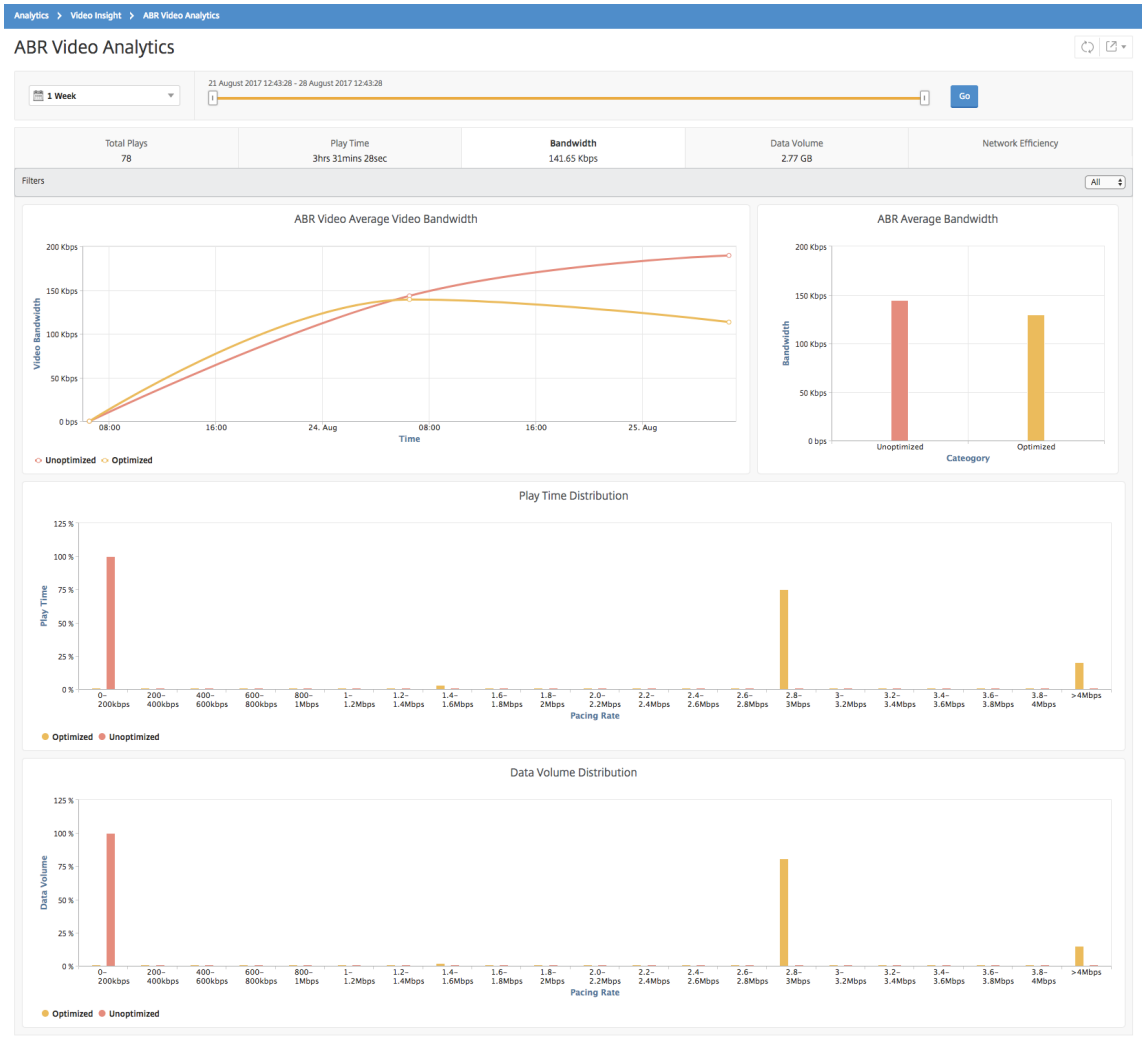
1. Navigate to **Analytics > Video Insight** and click **ABR Video Analytics**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Bandwidth** tab.

   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



For the selected time frame, the **Bandwidth** tab provides a line graph and pie chart describing the:

- Average bandwidth consumed by optimized and unoptimized ABR videos.
- Bandwidth consumed based on the play time distribution between optimized and unoptimized ABR videos.
- Bandwidth consumed based on the data volume distributed between optimized and unoptimized ABR videos.



Compare optimized and unoptimized number of plays of ABR videos

December 31, 2023

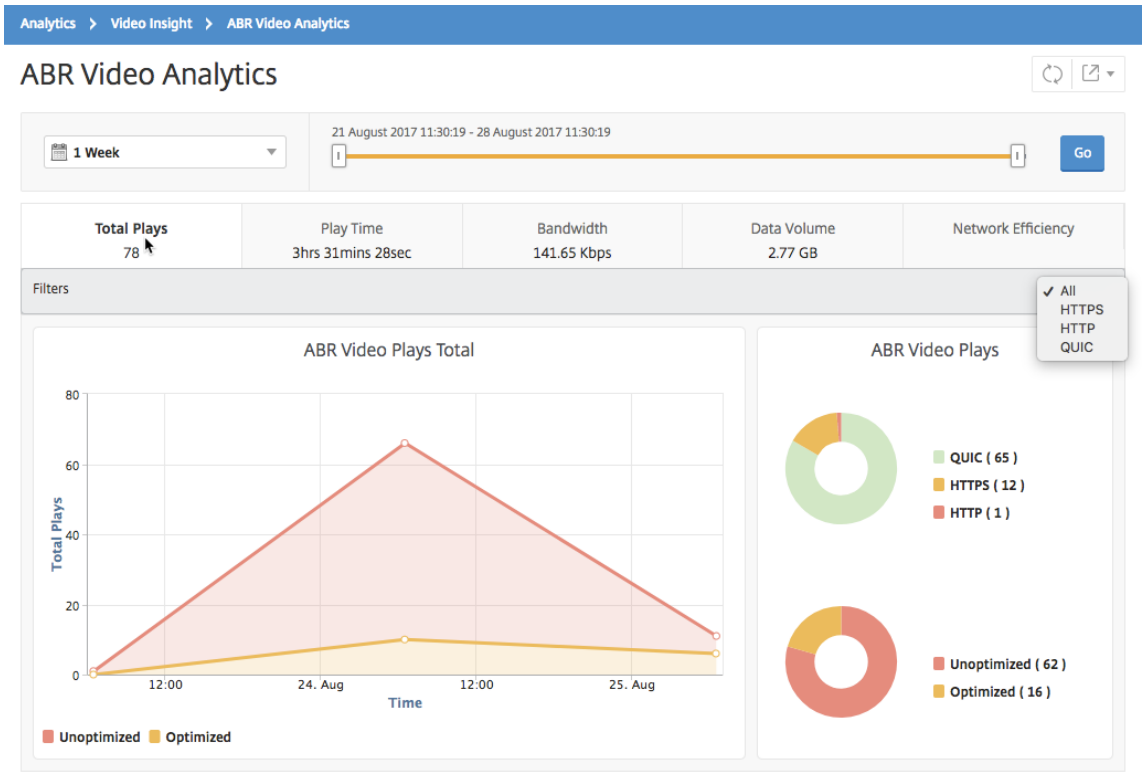
For a given time frame, NetScaler Application Delivery Management (ADM) shows the number of plays of ABR videos and enables you to compare the number of optimized and unoptimized plays in your network.

To see the number of plays:

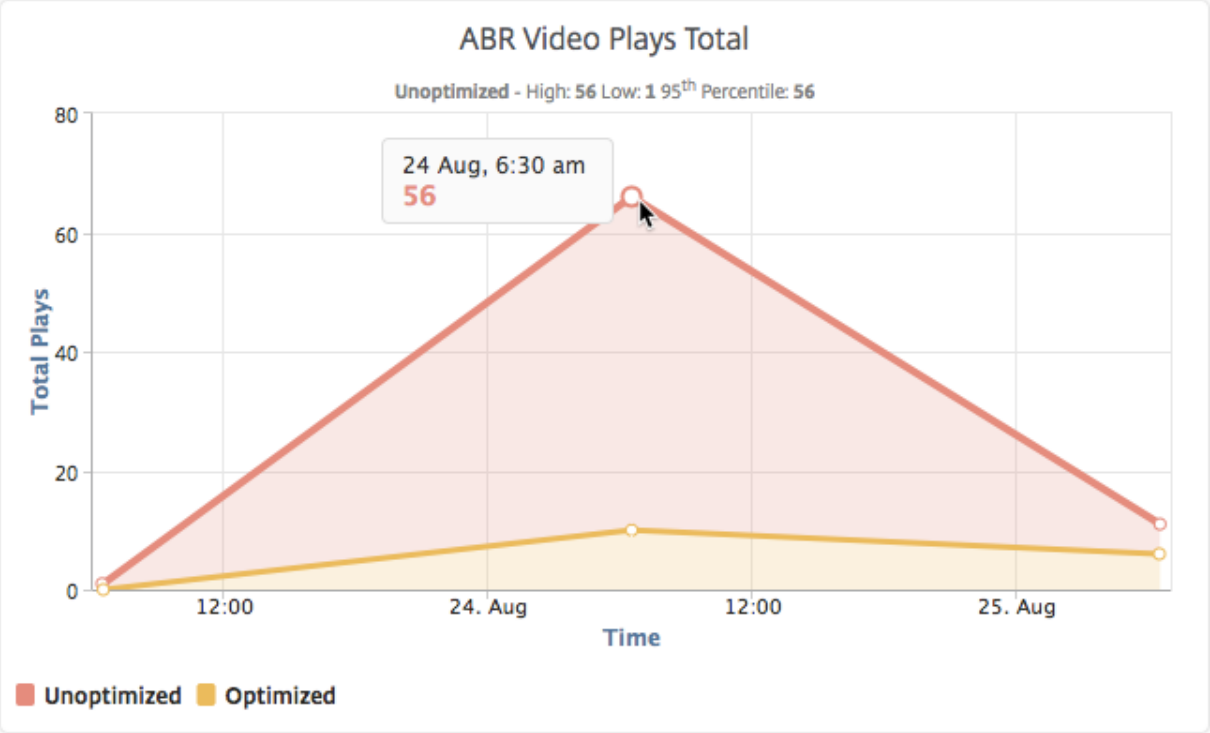
1. Navigate to **Analytics > Video Insight**, and click **ABR Video Analytics**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.

3. Click **Go** and select **# of Plays** tab.

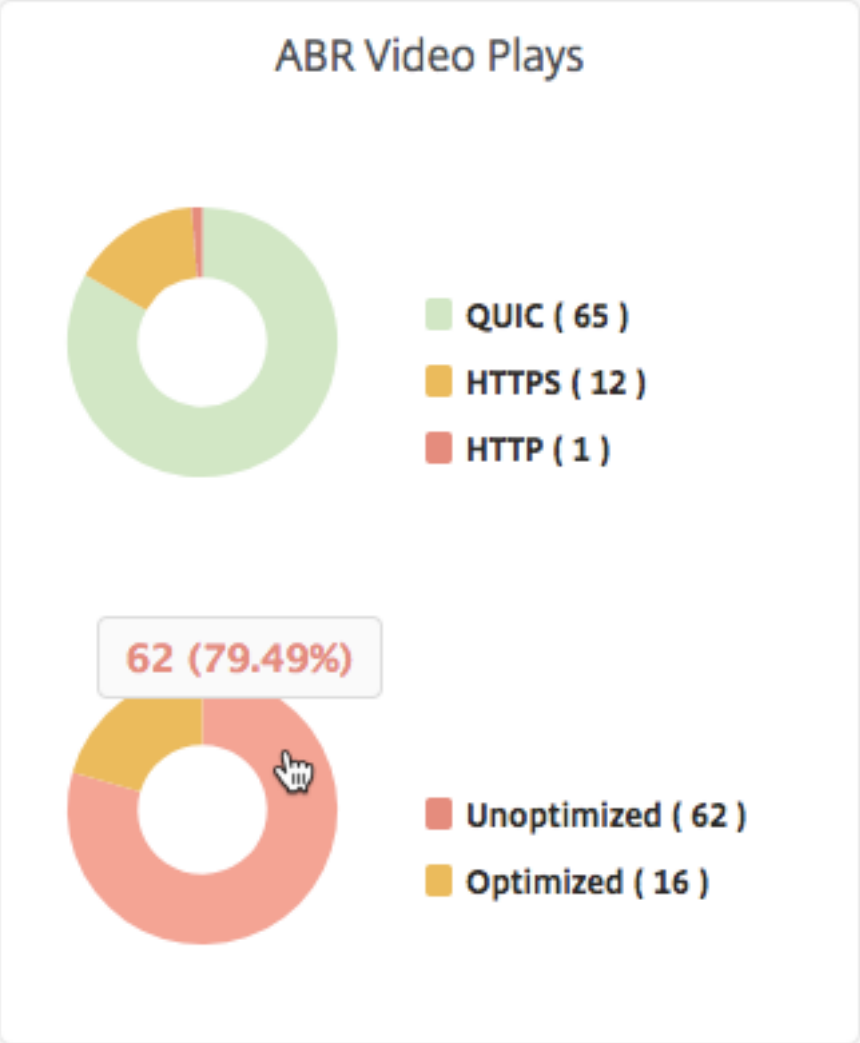
   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



The **# of Plays** tab provides a line graph and pie chart describing the number of plays of ABR videos from your network, and the number of optimized and unoptimized plays of ABR videos from your network for the selected time frame. You can hover your mouse pointer on the line graph to view the number of plays during a particular time frame:



Also, you can hover your mouse pointer on the pie chart to the show the percentage of optimized and unoptimized plays and the percentage of encrypted and unencrypted ABR videos for the selected time frame.



View peak data rate for a specific time frame

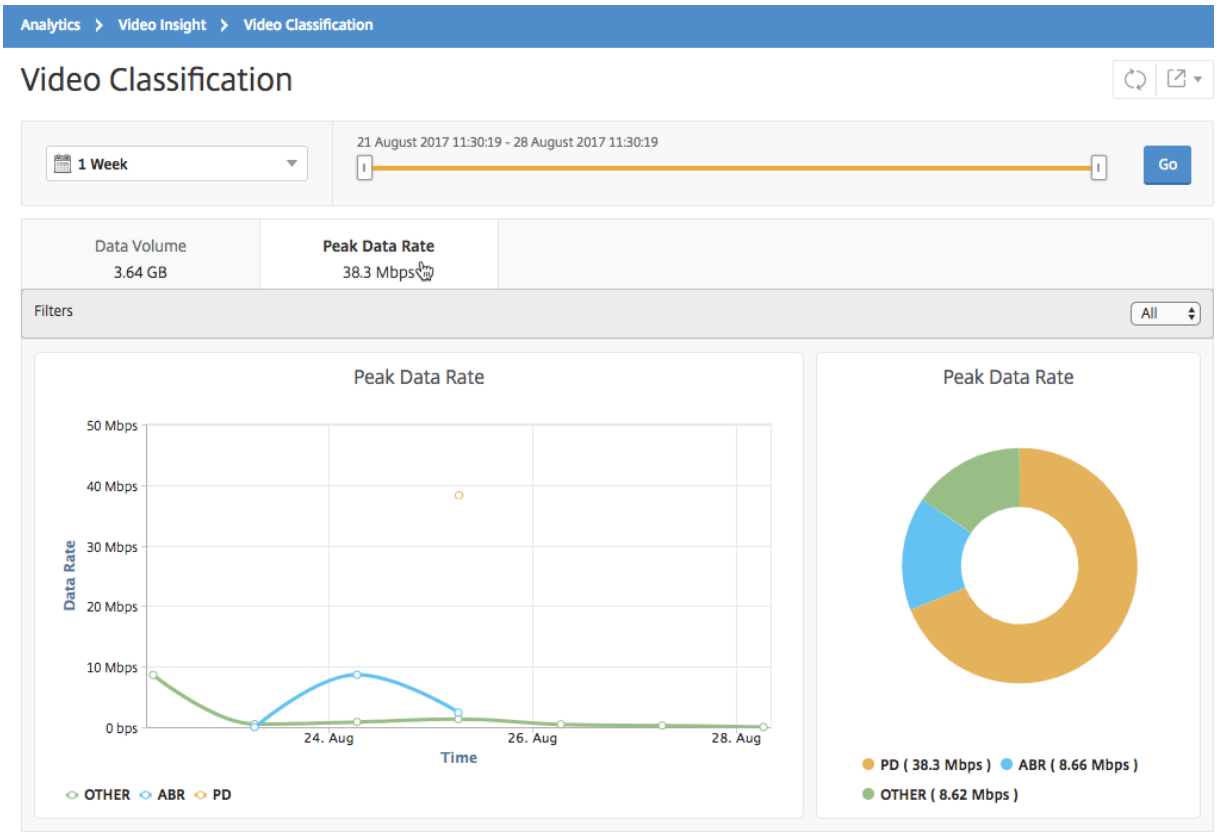
December 31, 2023

NetScaler Application Delivery Management (ADM) shows you the peak throughput or data rate of the video traffic in your network.

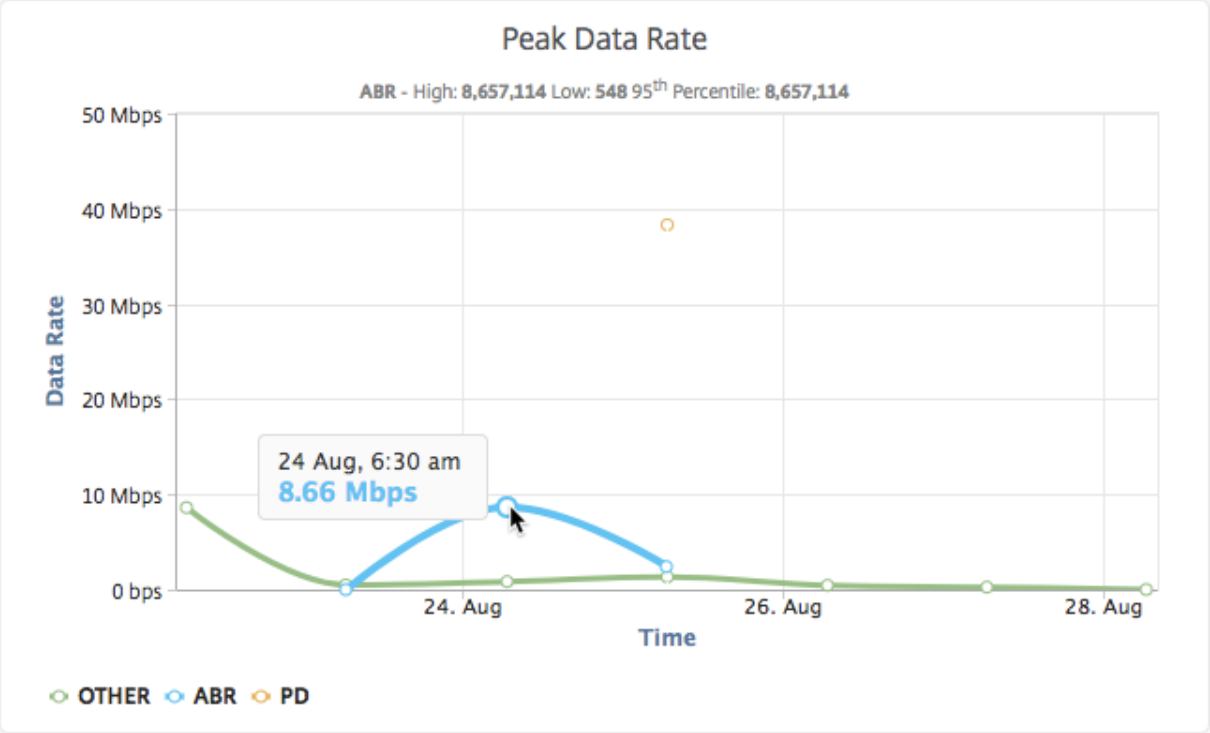
To see the peak data rate of the video traffic:

1. Navigate to **Analytics > Video Insight**, and click **Video Classification**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Peak Data Rate** tab.

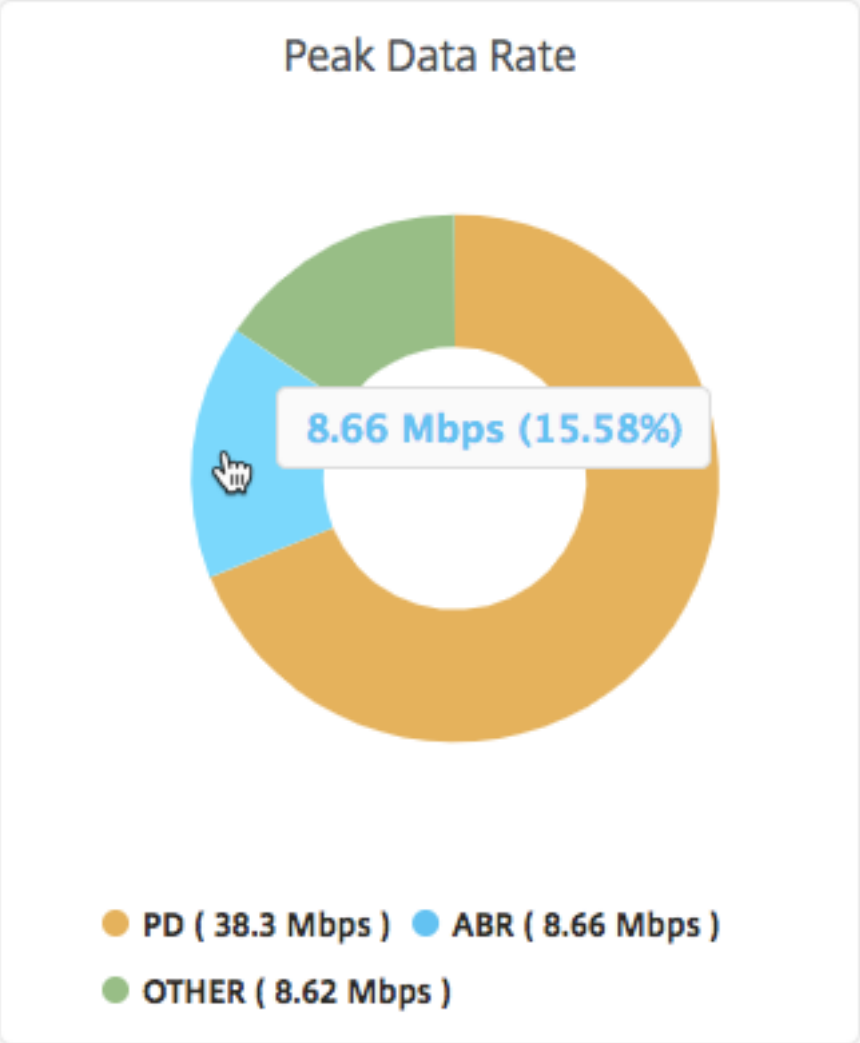
You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.



The **Peak Data Rate** tab provides a line graph and pie chart describing the peak data rate of the type of video traffic streaming from your network and the peak data rate of the video traffic on your network during the selected time frame. You can hover your mouse pointer on the line graph to show the peak data rate during a particular time frame.



Also, you can hover your mouse pointer on the pie chart to the show the percentage of the peak data rate consumed by the type of video traffic streamed during the selected time frame.



Configure IP address management (IPAM)

December 31, 2023

ADM IPAM provides you an ability to auto-assign and release IP addresses in ADM managed configurations. You can assign IP addresses from networks or IP ranges defined using the following IP providers:

- ADM built-in IPAM provider.
- Infoblox IPAM solution. For more information, see Infoblox DDI.

Currently, you can use ADM IPAM in:

- **StyleBooks**: Auto-Allocate IPs to virtual servers when you create configurations.

- **Kubernetes Ingress**: Auto-assign a virtual IP address to an Ingress configuration in a Kubernetes cluster.

You can also track the allocated and available IP addresses in each network or IP range managed by ADM.

Add an external IP address provider

ADM has a built-in IPAM provider to manage IPs and IP ranges. If you want to add an external IP provider solution in ADM, perform the following steps:

1. Navigate to **Infrastructure > IPAM**.
2. In **Providers**, click **Add**.
3. Specify the following details to add an IP provider:
    - **Name** - Specify the IP provider name to use in ADM.
    - **Vendor** - Select an IP address vendor from the list.
    - **URL** - Specify the URL of the IPAM solution that assigns IP addresses in ADM environment.
    - **User Name** - Specify the user name to log in to IPAM solution.
    - **Password** - Specify the password to log in to IPAM solution.
4. Click **Add**.

Add a network

Add a network to use IPAM with ADM managed configurations.

1. Navigate to **Infrastructure > IPAM**.
2. In **Networks**, click **Add**.
3. Specify the following details:
    - **Network Name** - Specify the network name to identify the network in ADM.
    - **Provider** - Select the provider from the list.

      This list displays the providers added in ADM.
    - **Network Type** - Select **IP range** or **CIDR** from the list based on your requirement.
    - **Network Value** - Specify the network value.

> **Note**
>
> ADM IPAM supports only IPv4 addresses.

For **IP range**, specify the network value in the following format:

```
<first-IP-address>-<last-IP-address>
<!--NeedCopy-->
```

Example:

```
10.0.0.20-10.0.0.100
<!--NeedCopy-->
```

For **CIDR**, specify the network value in the following format:

```
<IP-address>/<subnet-mask>
<!--NeedCopy-->
```

Example:

```
10.70.124.0/24
<!--NeedCopy-->
```

4. Click **Create**.

View allocated IP addresses

To view more details about allocated IP addresses from the IPAM network, do the following steps:

1. Navigate to **Infrastructure > IPAM**.
2. In the **Networks** tab, click **View All Allocated IPs**.

   This pane displays IP address, provider name, provider vendor, and description. It also displays the resource details that reserved this IP address:

   - **Module**: Displays the ADM module that reserves the IP address. For example, if the IP address is reserved by StyleBooks, this column displays StyleBooks as the module.
   - **Resource Type**: Displays the resource type in that module. For the StyleBooks module, only the configurations resource type uses the IPAM network.
   - **Resource ID**: Displays the resource ID with a link. Click this link to access the resource that uses the IP address. For the configuration resource type, the resource ID is displayed as the configuration pack ID.

> **Note**
>
> If you want to release the IP address, select the IP address that you want to release and click **Release Allocated IPs**.

Use ADM audit logs for managing and monitoring your infrastructure

March 11, 2024

You can use the NetScaler ADM service to track all events on ADM and syslog events generated on ADM-managed ADC instances. These messages can help you manage and monitor your infrastructure. But log messages are a great source of information only if you review them, and ADM simplifies the way of reviewing log messages.

You can use filters to search ADM syslog and audit log messages. The filters help to narrow down your results and find exactly what you are looking for and in real time. The built-in Search Help guides you to filter the logs. Another way to view log messages is to export them in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses at various intervals.

You can review the following types of log messages from the ADM GUI:

- ADC instance related audit logs
- ADM related audit logs
- Application audit logs

ADC instance related audit logs

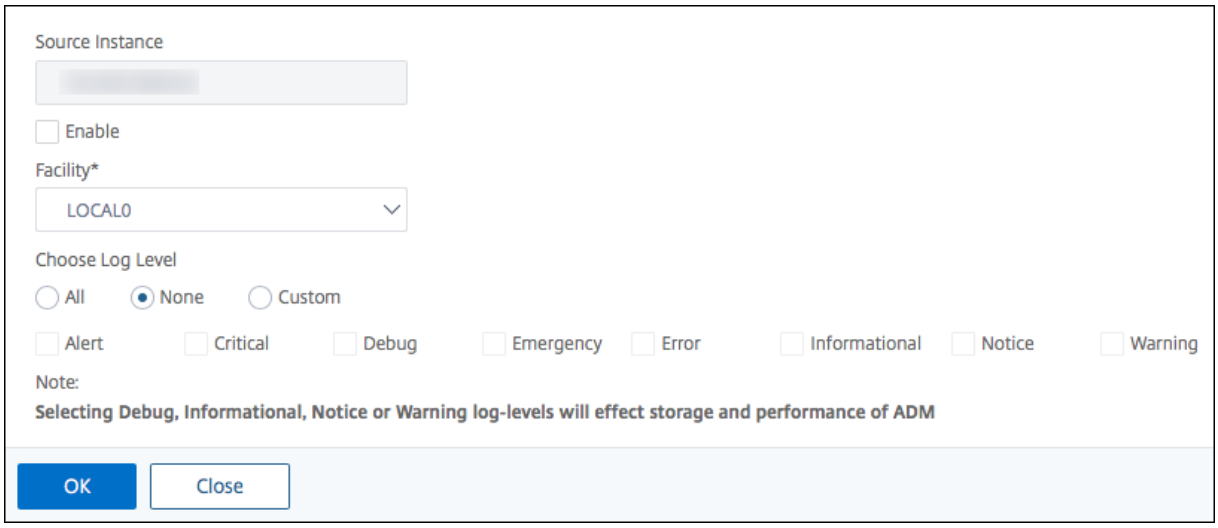
Before you can view ADC instance-related syslog messages from ADM, configure the NetScaler ADM service as the syslog server for your NetScaler instance. After the configuration is complete, all syslog messages are redirected from the instance to ADM.

Configure the ADM service as a syslog server

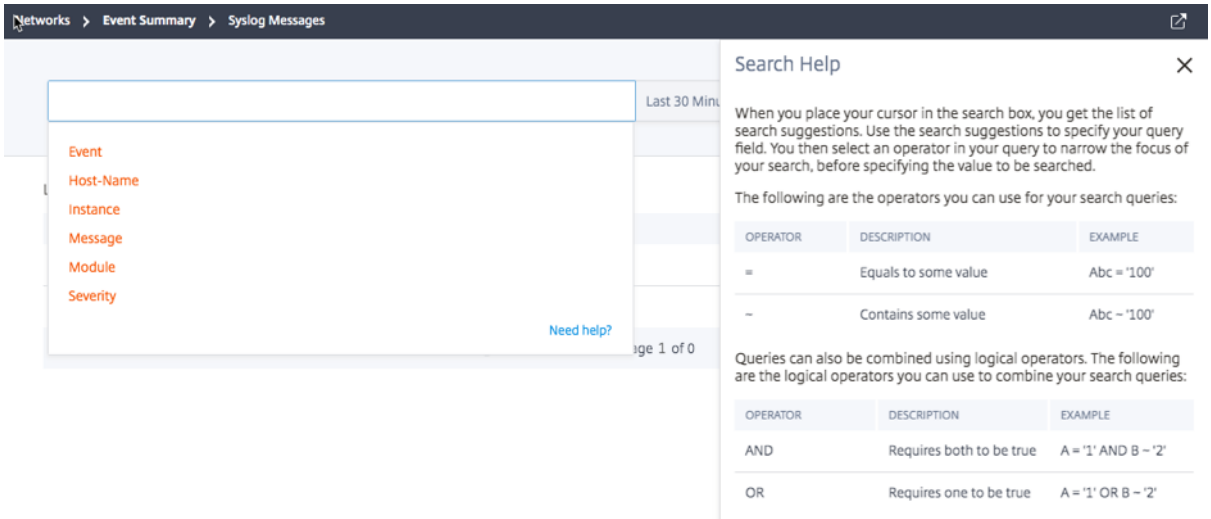
Follow these steps to configure ADM as the syslog server:

1. From the ADM GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler ADM.
3. In the **Select Action** list, select **Configure Syslog**.

4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.



These steps configure all the syslog commands in the NetScaler instance, and NetScaler ADM starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**. Click **Need Help?** to open the built-in search help. For more information, see View and export syslog messages.



To export the log messages, click the arrow icon on the upper right corner.

Next, click **Export Now** or **Schedule Export**. For more information, see View and export syslog messages.

ADM related audit logs

Based on preconfigured rules, ADM generates audit log messages for all events on, helping you monitor the health of your infrastructure. To view all audit log messages present in the ADM, navigate to **Settings > ADM Audit Log Messages**.

To export the log messages, click the arrow icon on the upper right corner.

Application related audit logs

You can view the audit log messages for all ADM applications or for a specific application.

- To view all audit log messages for all applications present in the ADM, navigate to **Infrastructure > Network Functions > Auditing**.
- To view audit log messages for any specific application in the ADM, navigate to **Applications > Dashboard**, click a virtual server and select **Audit Log**.

NetScaler pooled capacity

March 11, 2024

The NetScaler pooled capacity allows you to share bandwidth or instance licenses across different ADC form factors. For virtual CPU subscription-based instances, you can share virtual CPU license across instances. Use this pooled capacity for the instances that are in the data center or public clouds. When an instance no longer requires the resources, it checks the allocated capacity back into the common pool. Reuse the released capacity to other ADC instances that need resources.

You can use pooled licensing to maximize the bandwidth utilization by ensuring the necessary bandwidth allocation to an instance and not more than its need. Increase or decrease the bandwidth allocated to an instance at run time without affecting the traffic. With the pooled capacity licenses, you can automate the instance provisioning.

How NetScaler pooled capacity licensing works

NetScaler pooled capacity has the following components:

- NetScaler instances, which can be categorized into:
  - Zero-capacity hardware
  - Standalone VPX instances or CPX instances or BLX instances

- Bandwidth pool
- Instance pool
- NetScaler ADM configured as a license server

Zero-capacity hardware

When managed through NetScaler pooled capacity, MPX and SDX instances are referred to as "zero-capacity hardware"because these instances cannot function until they check resources out of the bandwidth and instance pools. Thus, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware requires a platform license to be able to check out bandwidth and an instance license from the common pool.

> **Note**
>
> - Instance license subscription is not required for MPX instances. See table 1 in this page, for supported pooled capacity for MPX and SDX instances. See table 5 for license requirement for different MPX and SDX form factors.
> - The zero capacity license installation works the same way as other NetScaler local licenses. For more information about how to obtain and install a zero capacity license, see Licensing guide for NetScaler.

Manage and install platform licenses

You must install a platform license manually, by using the hardware serial number or the license access code. After a platform license is installed, it is locked to the hardware and cannot be shared across NetScaler hardware instances on demand. However, you can manually move the platform license to another NetScaler hardware instance.

NetScaler MPX instances running the ADC software release 11.1 build 54.14 or later and NetScaler SDX instances running 11.1 build 58.13 or later support ADC pooled capacity. For more information, see **Table 1. Supported pooled capacity for MPX and SDX instances**.

Standalone NetScaler VPX instances

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 and later on the following hypervisors supports pooled-capacity:

- VMware ESX 6.0

- Citrix Hypervisor
- Linux KVM

NetScaler VPX instances running NetScaler software release 12.0 Build 51.24 and later on the following hypervisors and cloud platforms supports pooled-capacity:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX instances running NetScaler software release 13.0 and 13.1 (all versions) on the following hypervisors and cloud platforms support pooled-capacity:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Note**
>
> To enable communication between NetScaler ADM and Microsoft Azure or AWS, an IPSEC tunnel has to be configured. For more information, see Add NetScaler VPX Instances Deployed in Cloud to NetScaler ADM.
> Unlike zero-capacity hardware, VPX does not require platform license. To process traffic, it must check out bandwidth and an instance license from the pool.

Standalone NetScaler CPX instances

NetScaler CPX instances deployed on a Docker host support pooled-capacity. Unlike zero-capacity hardware, CPX does not require a platform license. A single CPX instance consuming up to 1 Gbps throughput checks-out only 1 instance and no bandwidth from the license pool. For example, consider that you have 20 CPX instances with 20 Gbps bandwidth pool. If one of the CPX instances consumes 500 Mbps throughput, the bandwidth pool remains 20 Gbps for the remaining 19 CPX instances.

If the same CPX instance starts to consume 1500 Mbps throughput, the bandwidth pool has 19.5 Gbps for the remaining 19 CPX instances.

For pool licensing, you can add more bandwidth only in multiples of 10 Mbps.

Standalone NetScaler BLX instances

NetScaler BLX instances support pooled-capacity licenses. A NetScaler BLX instance does not require a platform license. To process traffic, a NetScaler BLX instance must check out bandwidth and an instance license from the pool.

Bandwidth Pool

The bandwidth pool is the total bandwidth that can be shared by NetScaler instances, both physical and virtual. The bandwidth pool comprises separate pools for each software edition (Standard, Advanced, and Premium). A given NetScaler instance cannot have bandwidth from different pools checked out concurrently. The bandwidth pool from which it can check out bandwidth depends on its software edition for which it is licensed.

Instance pool

The instance pool defines the number of VPX instances or CPX instances or BLX instances that can be managed through NetScaler pooled capacity or the number of VPX instances in an SDX-Z instance.

When checked out from the pool, a license unlocks the MPX-Z, SDX-Z, VPX, CPX, and BLX instance's resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

> **Note**
>
> The Management Service of an SDX-Z does not consume an instance.

NetScaler ADM license server

NetScaler pooled capacity uses the NetScaler ADM configured as a license server to manage pooled capacity licenses: bandwidth pool licenses and instance pool licenses. You can use the NetScaler ADM software to manage pooled capacity licenses without an ADM license.

When checking out licenses from bandwidth and instance pool, NetScaler form factor and hardware model number on a zero-capacity hardware determines

- The minimum bandwidth and the number of instances that a NetScaler instance must check out before being functional.

- The maximum bandwidth and the number of instances that a NetScaler can check out.
- The minimum bandwidth unit for each bandwidth check-out. The minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if the minimum bandwidth unit of a NetScaler is 1 Gbps, 1000 Mbps can be checked out, but not 200 Mbps or 150.5 Gbps. The minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check out more bandwidth with the minimum bandwidth unit.

Tables 1, 2, 3, and 4 summarize the maximum bandwidth/instances, minimum bandwidth/instances, and minimum bandwidth unit for all supported NetScaler instances. Table 5 summarizes the license requirement for different form factors for all supported NetScaler instances:

Table 1. Supported pooled capacity for MPX and SDX instances

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
MPX 5900Z	10	1	N/A	N/A	1 Gbps
MPX 8900Z	30	5	NA	NA	1 Gbps
MPX 9100Z	30	10	NA	NA	1 Gbps
MPX 8900Z FIPS	33	5	NA	NA	1 Gbps
MPX 14000Z series	100	20	NA	NA	1 Gbps
MPX 14000Z 40G series	100	20	N/A	N/A	1 Gbps
MPX 14000Z FIPS series	100	20	N/A	N/A	1 Gbps
MPX 14000Z 40S series	100	20	N/A	N/A	1 Gbps
MPX 15000Z series	120	20	N/A	N/A	1 Gbps
MPX 15000Z FIPS series	120	20	N/A	N/A	1 Gbps

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
MPX 15000Z 50G series	120	20	N/A	N/A	1 Gbps
MPX 16000Z series	200	30	N/A	N/A	1 Gbps
MPX 22000Z series	120	40	N/A	N/A	1 Gbps
MPX 24000Z series	150	100	N/A	N/A	1 Gbps
MPX 25000Z 40G	200	100	N/A	N/A	1 Gbps
MPX 25000ZA	200	100	N/A	N/A	1 Gbps
MPX 26000Z series	200	100	N/A	N/A	1 Gbps
MPX 26000Z 100G series	200	100	N/A	N/A	1 Gbps
MPX 26000Z 50S series	200	100	N/A	N/A	1 Gbps
SDX 8900Z	30	10	2	7	1 Gbps
SDX 9100Z	95	20	4	7	1 Gbps
SDX 14000Z series	100	10	2	25	1 Gbps
SDX 14000Z 40G series	100	10	2	25	1 Gbps
SDX 14000Z 40S series	100	20	10	25	1 Gbps
SDX 14000Z FIPS series	100	10	2	25	1 Gbps

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
SDX 15000Z 50G	120	10	2 (Note: 5 instances for versions lower than 13.0 47.x)	55	1 Gbps
SDX 15000Z	120	10	2 Note: 5 instances for versions lower than 13.0 47.x)	55	1 Gbps
SDX 16000Z series	200	15	10	55	1 Gbps
SDX 22000Z series	120	20	20	80	1 Gbps
SDX 25000Z 40G	200	50	10	115	1 Gbps
SDX 25000ZA	200	50	10	115	1 Gbps
SDX 26000Z 100G	200	50	10	115	1 Gbps
SDX 26000Z	200	50	10	115	1 Gbps
SDX 26000Z 50S	200	50	10	115	1 Gbps
SDX 24000Z series	150	50	10	80	1 Gbps

> Note
>
> The minimum bandwidth and instances are applicable to SDX instances running the following releases and higher: 11.1 64.x, 12.0 63.x, 12.1 54.x, and 13.0 41.x.
>
> The minimum purchase quantity is different from the minimum system requirement.

Table 2. Supported pooled capacity for CPX instances

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Mbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
CPX	10	10	1	1	10 Mbps

Table 3. Supported pooled capacity for VPX instances on Hypervisors and Cloud services

Hypervisor/Cloud Service	Maximum bandwidth (Gbps)	Minimum bandwidth (Mbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

> Note
>
> The minimum purchase quantity is different from the minimum system requirement.

Table 4. Supported pooled capacity for BLX instances

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Mbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
BLX	100	10	1	1	10 Mbps

Table 5. License requirement for different form factors

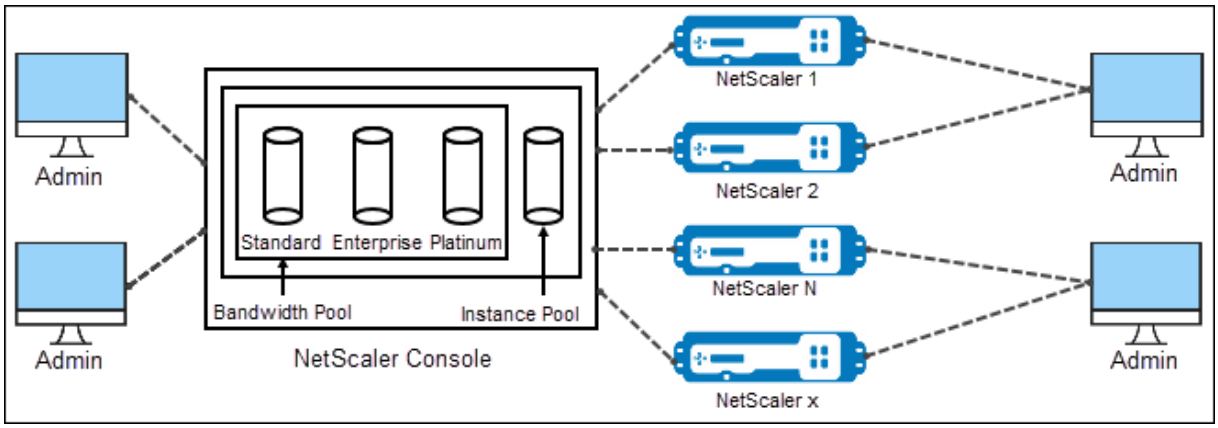
Product line	Zero Capacity Hardware Purchase	Bandwidth and Edition Subscription	Instance Subscription
MPX	License required	License required	-
SDX	License required	License required	License required
VPX	-	License required	License required
CPX	-	-	License required
BLX	-	License required	License required

Configure NetScaler pooled capacity

March 11, 2024

To use ADC pooled capacity, configure NetScaler ADM as a license server to the required ADC instances. ADC instances check in and check out licenses from the ADM. You can perform the following tasks in the ADM GUI:

- Upload the pooled capacity license files (bandwidth and instance pool) to the license server.
- Allocate licenses from the license pool to NetScaler instances on demand.
- Check out the licenses from NetScaler instances (MPX-Z /SDX-Z/VPX/CPX/BLX) based on the minimum and maximum capacity of the instance.
- Configure pooled capacity for NetScaler FIPS instances to check in or check out licenses.



Supported hardware and software versions

For supported hardware and software versions for pooled capacity, see NetScaler pooled capacity.

ADC pooled capacity states

The pooled capacity states indicate the license requirement on an ADC instance. The ADC instances configured with pooled capacity display one of the following states:

- **Optimum**: Instance is running with proper license capacity.
- **Capacity mismatch**: Instance is running with a capacity less than the user configured.
- **Grace**: Instance is running on a grace license.
- **Grace & Mismatch**: Instance is running on grace but with a capacity less than the user configured.
- **Not available**: Instance is not registered with ADM for management, or NITRO communication from ADM to the instances is not working.
- **Not allocated**: License is not allocated in the instance.

Step 1 - Apply licenses in ADM

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Files** section, select **Add License File** and select one of the following options:
   - **Upload license files from a local computer**. If a license file is already present on your local computer, you can upload it to ADM.
   - **Use license access code**. Specify the license access code for the license that you have purchased from Citrix. Then, select **Get Licenses**. Then select **Finish**.

   > **Note**
   >
   > At any time, you can add more licenses to ADM from **License Settings**.

3. Click **Finish**.

   The license files are added to ADM. The **License Expiry Information** tab lists the licenses present in the ADM and the remaining days to expiry.

4. In **License Files**, select a license file that you want to apply and click **Apply licenses**.

   This action enables ADC instances to use the selected license as a pooled capacity.

   For more information on how to apply pooled licenses to NetScaler ADM, see the related video here.

Step 2 - Register NetScaler ADM as a license server

To register ADM as a license server to a NetScaler instance, follow one of the procedures:

- Use GUI
- Use CLI

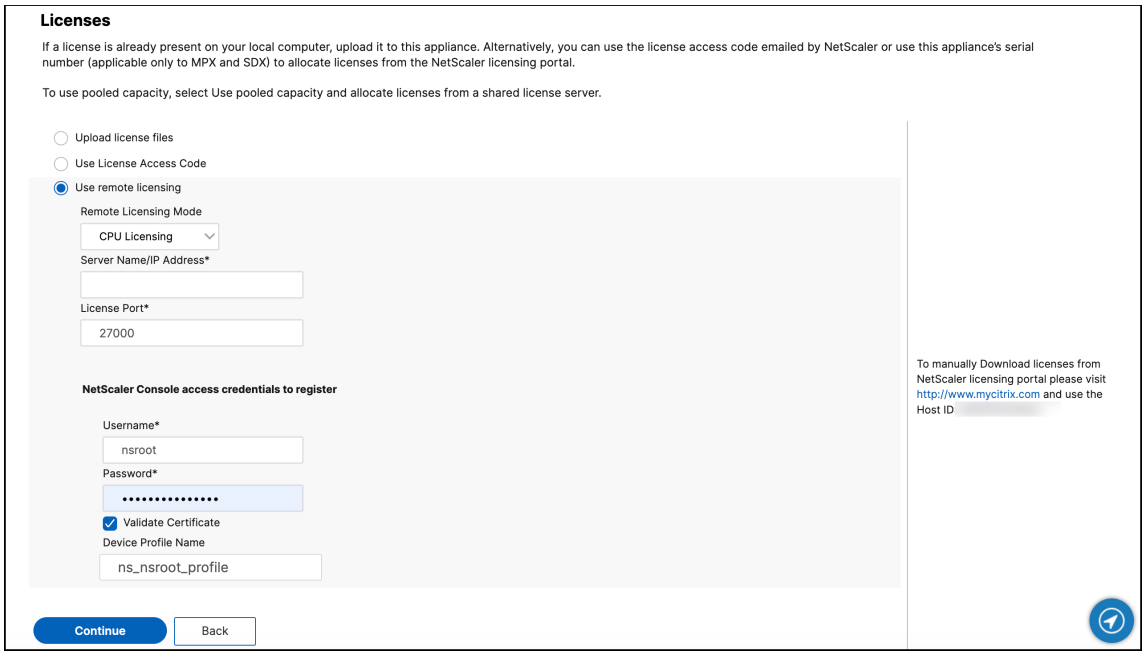
Use GUI to register ADM as a license server

In the ADC GUI, register the ADM server as a license server.

1. Log in to NetScaler GUI.
2. Navigate to **System** > **Licenses** > **Manage Licenses**.
3. Click **Add New License**.
4. Select **Use remote licensing** and select the remote licensing mode from the list.
5. In the **Server Name/IP address** field, specify the ADM server's IP address.

   > For a HA deployment, use a floating IP. For more information on configuration, see Configure High Availability Deployment.
   >
   > For a deployment which uses a standalone ADM or an agent, seeLicensing overview

6. Select **Register with NetScaler ADM**.
7. Enter your ADM credentials to register an instance with NetScaler ADM and click **Continue**.



8. In **Allocate licenses**, select the license edition and specify the required bandwidth.

   For the first time, allocate licenses in NetScaler. You can later change or release the license allocation from the ADM GUI.

   a) Click **Get Licenses**.

   > **Important:**
   >
   > Warm restart the instance if you change the license edition. The configuration changes do not take effect until you restart the instance.

Use CLI to add ADM as a license server

If an ADC instance has no GUI, use the following CLI commands to add the ADM server as a license server:

1. Log in to the ADC console.
2. Add the ADM server IP address:

   ```
   > add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
   <!--NeedCopy-->
   ```

   For more information, see Licensing overview.

3. View the license bandwidth available in the license server.

   ```
   > sh ns licenseserverpool
   <!--NeedCopy-->
   ```

   This command lists the licenses based on the specified license mode while adding the license server.

   Example-1:

   If the specified license mode is `CICO`, the output contains only CICO licenses.

   ```
   > add licenseserver [redacted] -licensemode CICO
    Done
   > sh licenseserverpool
           VPX8000P Total                  : 1
           VPX8000P Available              : 1
   ```

   Example-2:

   If the specified license mode is `Pooled`, the output contains only pooled capacity licenses.


```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                    : 40
        Instance Available                : 38
        Standard Bandwidth Total          : 210.00 Gbps
        Standard Bandwidth Available      : 210.00 Gbps
        Enterprise Bandwidth Total        : 50.00 Gbps
        Enterprise Bandwidth Available    : 50.00 Gbps
        Platinum Bandwidth Total          : 210.00 Gbps
        Platinum Bandwidth Available      : 205.00 Gbps
```

Example-3:

If the specified license mode is vCPU, the output contains only virtual CPU licenses.

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                : 100
        Standard CPU Available            : 100
        Enterprise CPU Total              : 100
        Enterprise CPU Available          : 100
        Platinum CPU Total                : 25
        Platinum CPU Available            : 20
```

To view all the licenses together, run the following command:

```
1  > sh ns licenseserverpool -getallLicenses
2  <!--NeedCopy-->
```

Example output:

```
> sh licenseserverpool -getallLicenses
        Instance Total                    : 40
        Instance Available                : 33
        Standard Bandwidth Total          : 210.00 Gbps
        Standard Bandwidth Available      : 210.00 Gbps
        Enterprise Bandwidth Total        : 50.00 Gbps
        Enterprise Bandwidth Available    : 50.00 Gbps
        Platinum Bandwidth Total          : 210.00 Gbps
        Platinum Bandwidth Available      : 205.00 Gbps
        VPX8000P Total                    : 1
        VPX8000P Available                : 1
        Standard CPU Total                : 100
        Standard CPU Available            : 100
        Enterprise CPU Total              : 100
        Enterprise CPU Available          : 100
        Platinum CPU Total                : 25
        Platinum CPU Available            : 20
```

4. Allocate the license bandwidth from the required license edition:

```
1  > set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
       -amount-license-bandwidth> -edition <specify-license-edition>
2  <!--NeedCopy-->
```


The license edition can be **Standard** or **Enterprise** or **Platinum**.

> **Important**
>
> Warm restart the instance if you change the license edition.
>
> ```
> reboot -w
> ```
>
> The configuration changes does not take effect until you restart the instance.

Step 3 - Allocate pooled licenses to ADC instances

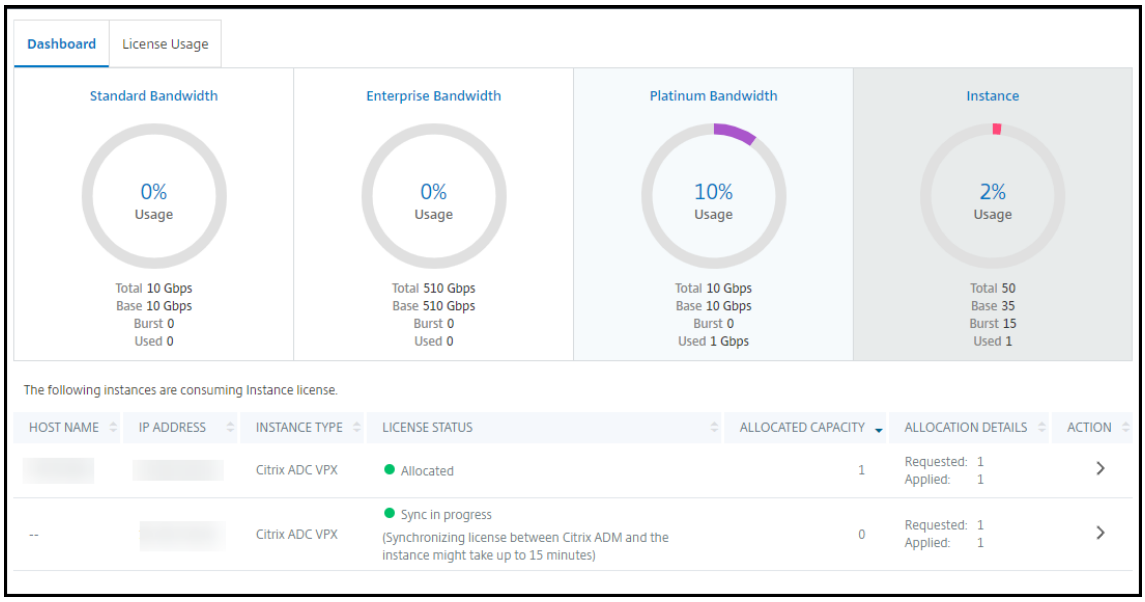
To allocate pooled capacity licenses from the ADM GUI:

1. Log in to NetScaler ADM.
2. Navigate to **Infrastructure > Licenses > Bandwidth Licenses > Pooled Capacity**.

   The FIPS instance capacity appears only if you upload FIPS instance licenses to ADM.
3. Click the license pool that you want to manage.

   > **Note**
   >
   > The **Allocated Capacity** field does not reflect the changed bandwidth immediately. The bandwidth change takes effect after the ADC warm restart.
   >
   > In **Allocation Details**, the **Requested** and **Applied** fields are updated when you change the instance's bandwidth allocation.

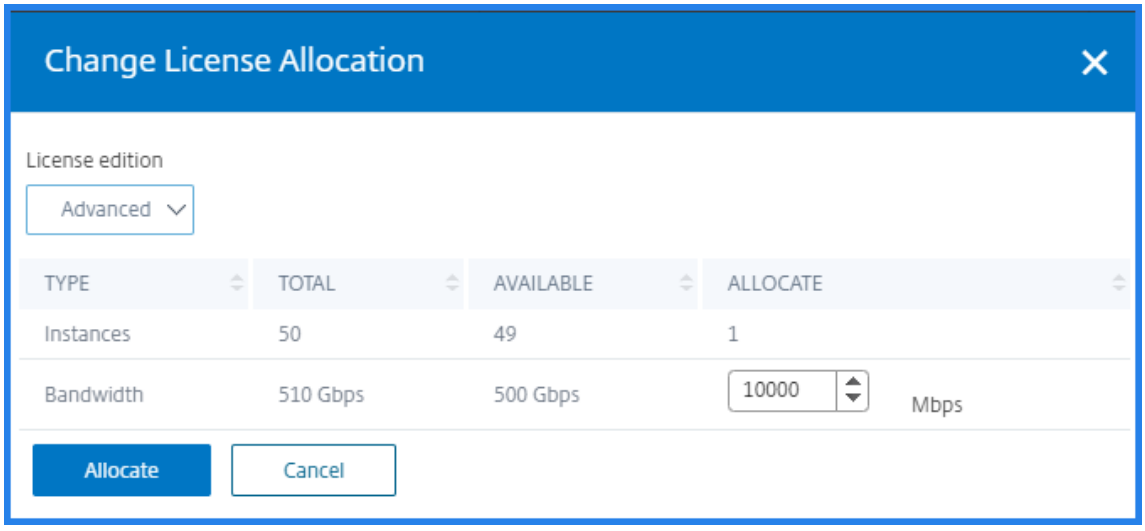
4. Select an ADC instance from the list of available instances by clicking the **>** button.



The **LICENSE STATUS** column displays corresponding license allocation status messages.

> **Note:**
>
> The **Unmanaged Instances** tab displays the instances that are discovered but not managed in NetScaler ADM.
>
> 
>

5. Click **Change allocation** or **Release allocation** to modify the license allocation.
6. A pop-up window with the available licenses in the License Server appears.
7. You can choose the bandwidth or instance allocation to the instance by setting the **Allocate** list options. After making your selections, click **Allocate**.
8. You can also change the allocated license edition from the list options in the **Change License Allocation window**.



> **Note**
>
> Warm restart an instance if you change the license edition.

For more information on how to change the bandwidth allocation, see the related video here.

Configure pooled capacity on ADC instances

You can configure pooled capacity licenses on the following ADC instances:

- NetScaler instances
- NetScaler VPX instances
- NetScaler high-availability pair

NetScaler MPX instances

MPX-Z is the pooled capacity enabled NetScaler MPX appliance. MPX-Z supports bandwidth pooling for Premium, Advanced, or Standard edition licenses.

MPX-Z requires platform licenses before it can connect to the License Server. You can install the MPX-Z platform license by either of the following:

- Uploading the license file from a local computer.
- Using the instance's hardware serial number.
- The License Access Code from the **System** > **Licenses** section of the instance's GUI.

If you remove the MPX-Z platform license, the pooled-capacity feature is disabled. The instance licenses are released to the license server.

You can dynamically modify the bandwidth of an MPX-Z instance without a restart. A restart is required only if you want to change the license edition.

> **Note:**
>
> When you restart the instance, it automatically checks out the pooled licenses required for its configured capacity.

NetScaler VPX instances

A pooled capacity enabled NetScaler VPX instance can check out licenses from a bandwidth pool (Premium/Advanced/Standard editions). You can use the ADC GUI to check out licenses from the License Server.

You can dynamically modify the bandwidth of a VPX instance without a restart. A restart is required only if you want to change the license edition.

> **Note:**
>
> When you restart the instance, the configured pooled capacity licenses are automatically checked out from the ADM server.

NetScaler high-availability pair

Before you begin, ensure that the ADM server is configured as a license server. For more information, see Configure ADM as a license server.

For ADC instances configured in a high availability mode, you have to configure pooled capacity on each node of the high availability pair. For both the primary and secondary nodes, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance in the

HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity to each node.

To allocate pool license to each node in the pair, follow the steps given in Allocate pooled licenses to ADC instances. First allocate license to the first node and then repeat the same steps to allocate license to the second node.

Configure an ADM server only as the pooled license server

March 11, 2024

As an administrator, you can configure an ADM server only as the pooled license server. With this configuration, the ADM server only receives licensing data from ADC instances.

Sometimes, you might have the regulatory mandate that requires restricting ADC instances' data from leaving the regulatory zone. In such situations, you can deploy a local instance of an ADM on-prem server in your regulatory zone to use management, monitoring, and analytics capabilities. When you follow the same approach to use the pooled licenses feature, you have to split pooled licenses across various ADM license servers. This approach does not provide you the flexibility to allocate pooled licenses across your globally deployed ADC instances.

Therefore, configure the ADM server only as the pooled license server. The ADM server receives only licensing data from all ADC instances. So, you can adhere to the regulatory mandate and dynamically allocate pooled capacity licenses across globally deployed ADC instances.

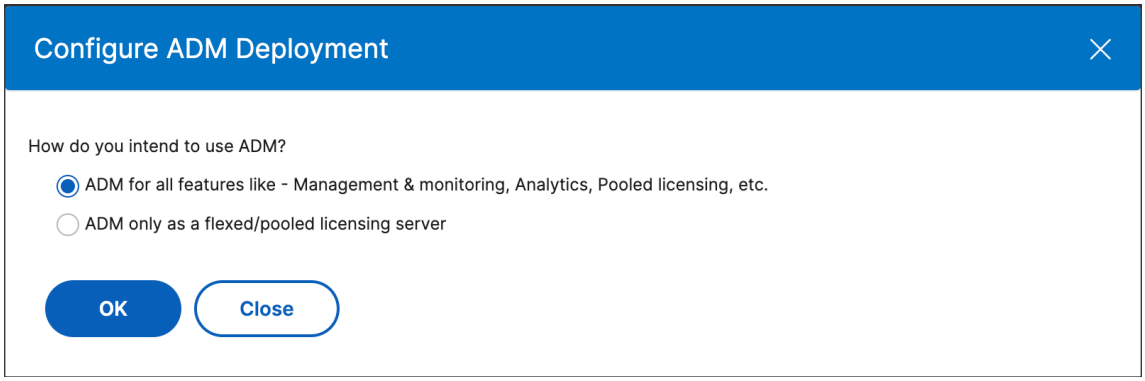
This document explains how to configure an ADM server only as the pooled license server.

How to configure an ADM server only as the pooled license server

Before you begin, ensure no ADC instances are added to an ADM server. Add the ADC instances only after you complete step 4.

Do the following to configure an ADM server only for the pooled license server:

1. Navigate to **Settings > Administration**.
2. In the **System Configurations** section, select **System Deployment**.
3. In **ADM Deployment**, select **ADM only as a pooled licensing server**.



4. Click **OK**.

   This action retains only the pooled licensing feature and disables the following ADM features:

   - ADM backup
   - Event management
   - SSL certificate management
   - Network reporting
   - Network functions
   - Configuration audit

   > **Note**
   >
   > By default, the ADM analytics feature is disabled. Make sure to disable this feature if you have enabled it.

   In the confirmation box, click **Yes**.

   The ADM GUI now displays only the pooled licensing feature. And, the remaining features do not appear.

5. After you configure ADM only for the licensing feature, add ADC instances in the **Infrastructure > Instances** page.

> **Note**
>
> - You can add an ADC instance in one or more ADM servers. When you change the password of such ADC instances, ensure to update the password on all ADM servers where the instance is discovered.
> - A user can still do some operations of the disabled features in the ADM GUI. For example, event polling and ADC backup. As a super administrator, If you want to restrict such operations, disable user accesses for other administrators using an appropriate access policy. For more information, see Configure Access Policies on NetScaler ADM.

Upgrade a perpetual license in NetScaler VPX to NetScaler pooled capacity

March 11, 2024

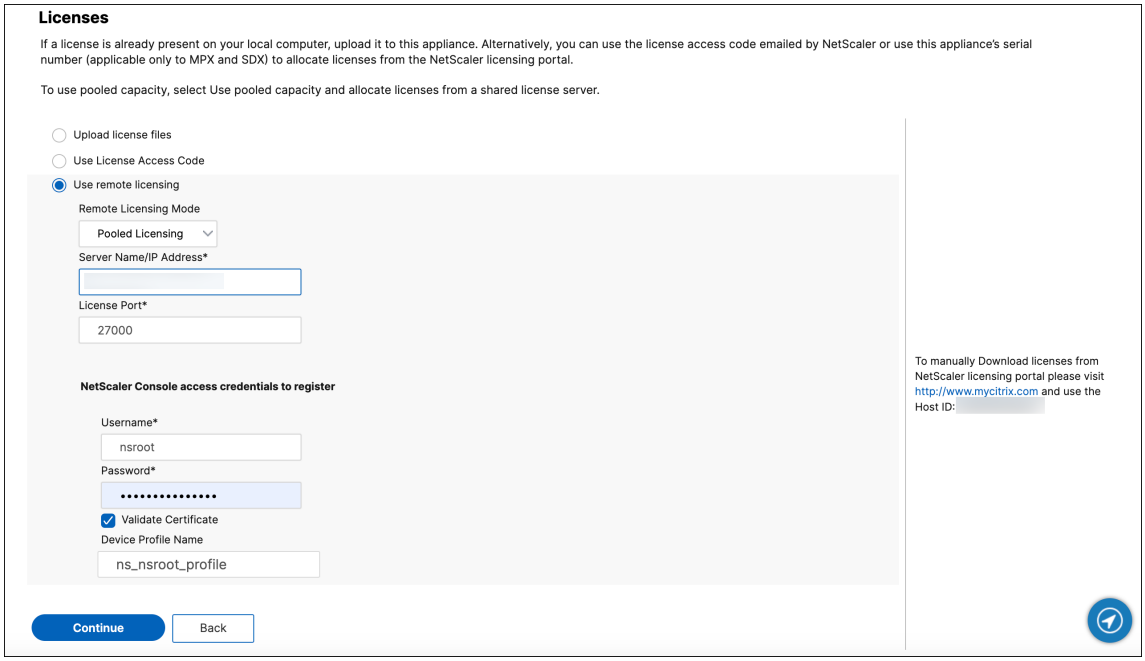
NetScaler VPX instances with perpetual license can be upgraded to ADC pooled capacity license. Upgrading to pooled capacity license enables you to allocate licenses from the license pool to the VPX instances on demand. You can also configure pooled capacity license for ADC instances configured in a high availability mode. To configure pooled capacity license for VPX instances in high availability mode, see Upgrading the Perpetual License in NetScaler VPX High Availability Pair to NetScaler Pooled Capacity.

Prerequisites

Ensure that you upgrade the VPX instance to version 12.0.56.x.

To upgrade to NetScaler pooled capacity:

1. In a Web browser, type the IP address of the VPX instance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the **Configuration tab**, navigate to **System > Licenses** and click **Manage Licenses**.
5. On the **Licenses** page, click **Add New License**.
6. On the **Licenses** page, choose **Use remote licensing** and do the following:



a) In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.

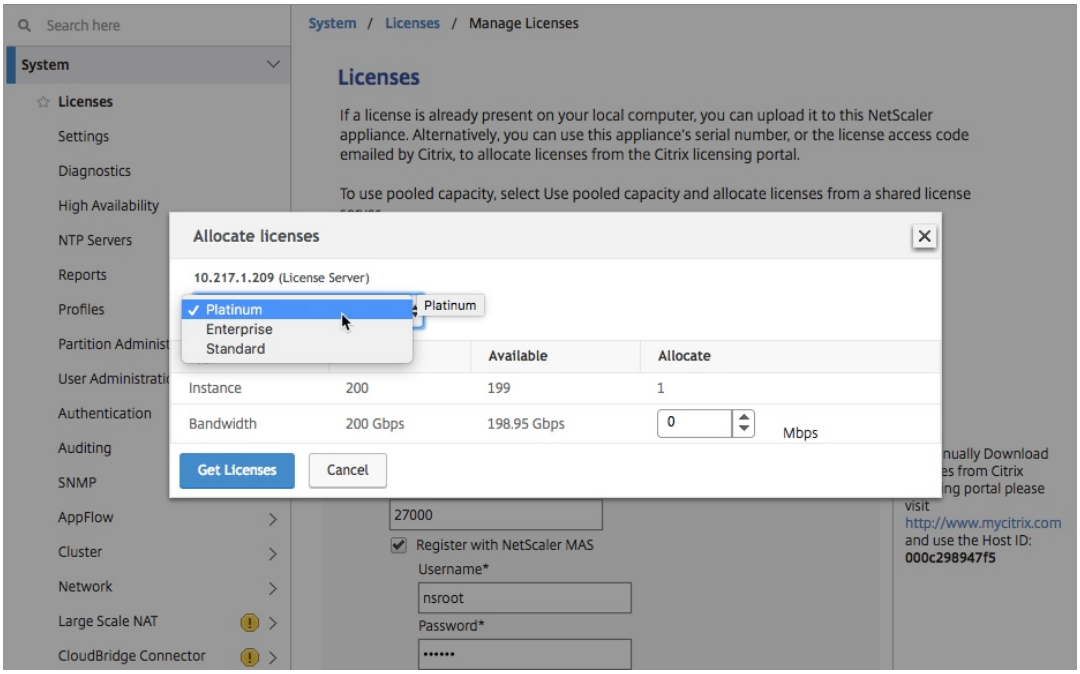
b) In the **Server Name/IP Address** field, Enter the details of the license server.

c) Make sure that the **Register with NetScaler ADM** check box is selected and enter NetScaler ADM credentials, if you want to manage your instance's pool licenses through ADM.

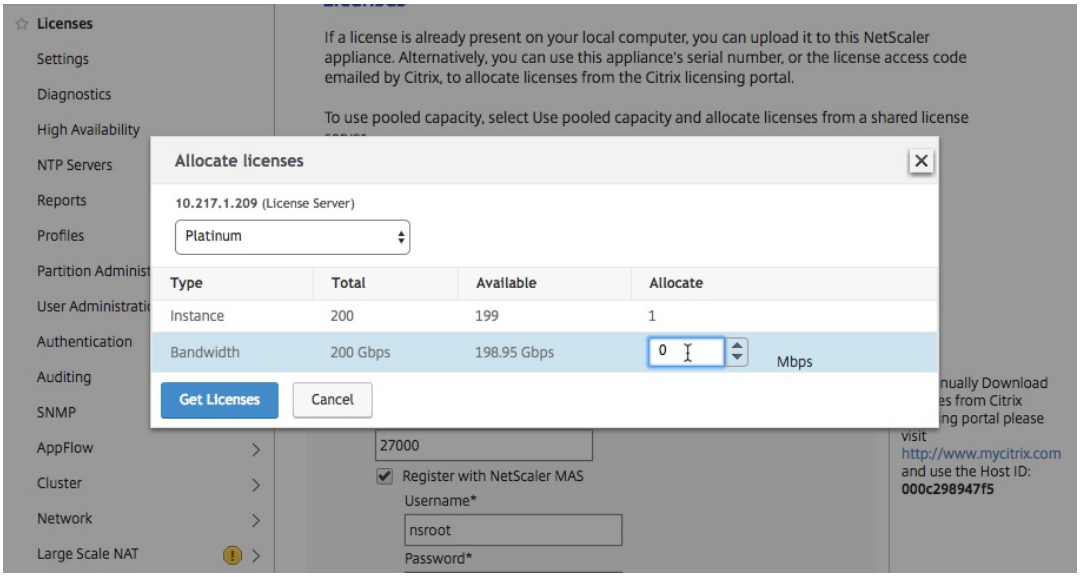
d) Click **Continue**.

7. In **Allocate licenses**, do the following:

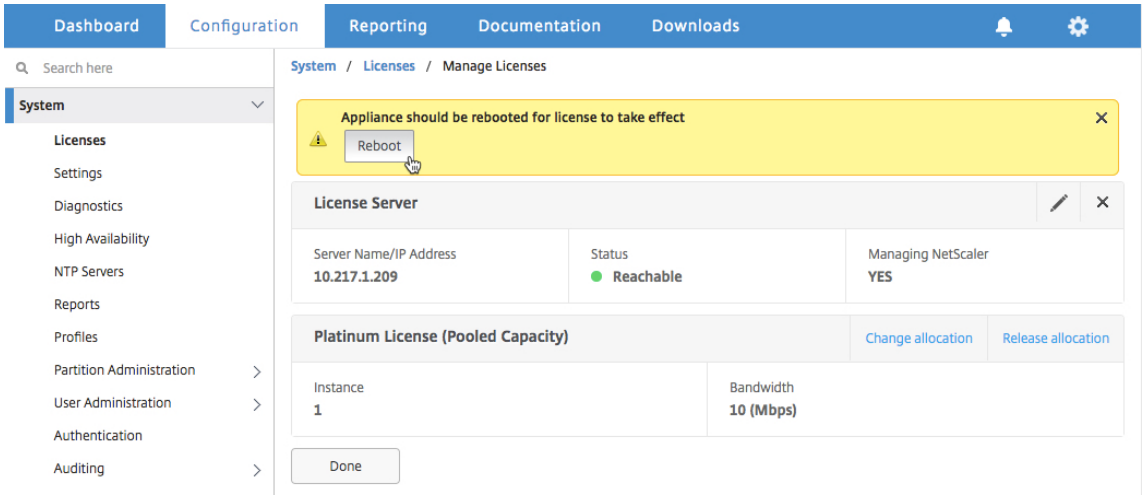
a) Select the license edition from the drop-down list.



b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



8. When prompted, click **Reboot** to reboot the appliance.



9. In the Confirm dialog box, click **Yes**.
10. After the VPX instance restarts, log on to the instance. On the **Welcome** page, click **Continue**.

    The **Licenses** page displays all the features that are licensed on the NetScaler VPX appliance. Click **X**.
11. Navigate to **System > Licenses** and click **Manage Licenses**.

    On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

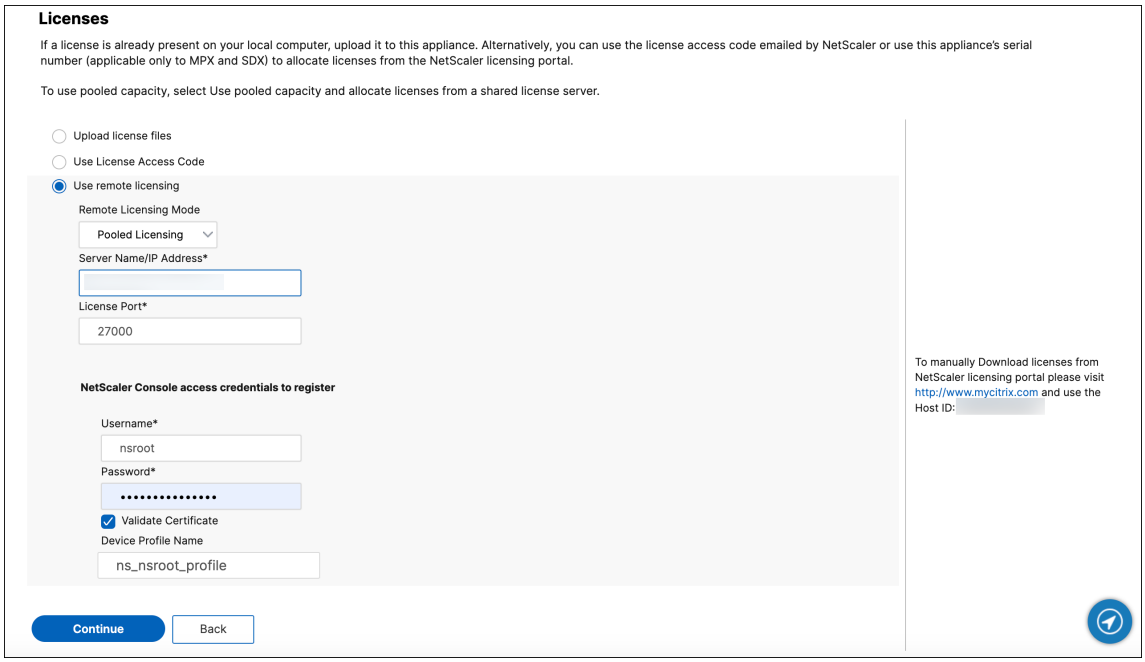
Upgrade the Perpetual License in NetScaler VPX high availability pair to NetScaler pooled capacity

For VPX instances configured in a high availability mode, you have to configure pooled capacity on both the primary and secondary instances in the HA pair. For both the primary and secondary instances, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity each to the primary and secondary instances in the HA pair.

To upgrade an exisiting NetScaler VPX HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary VPX (node 2) instance. In a Web browser, type the IP address of the NetScaler appliance, such as `http://192.168.100.1`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the Configuration tab, navigate to **System** > **Licenses** and click **Manage Licenses**.
5. On the **Licenses** page, click **Add New License**.

6. Choose **Use remote licensing** and do the following:



   a) In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.

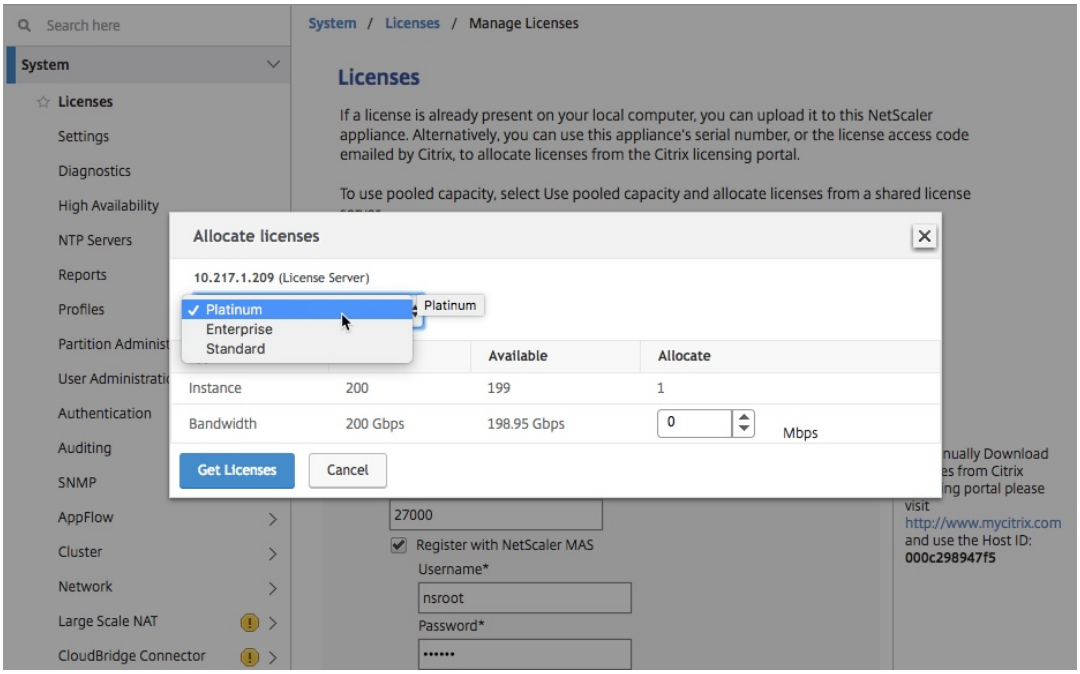
   b) In the **Server Name/IP Address** field, Enter the details of the license server.

   c) Make sure that the **Register with NetScaler ADM** check box is selected and enter the ADM credentials, if you want to manage your instance's pool licenses through NetScaler ADM.

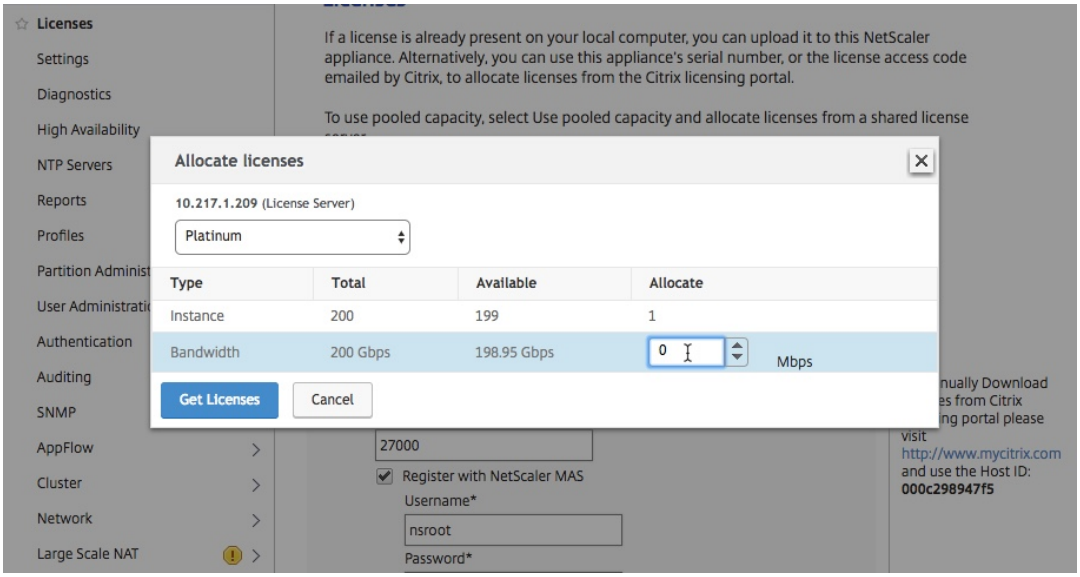
   d) Click **Continue**.

7. In **Allocate licenses**, do the following:

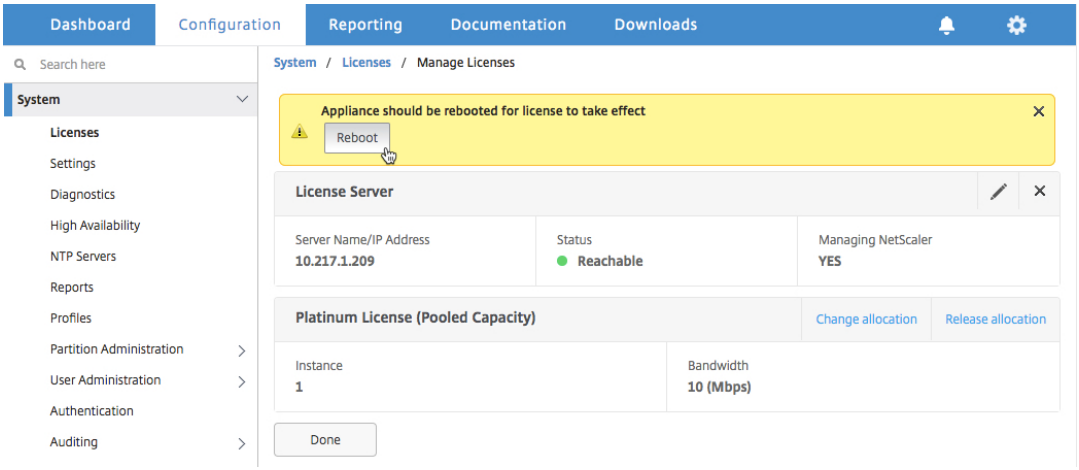
   a) Select the license edition from the drop-down list.



b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c) When prompted, click **Reboot** to warm restart the instance.



8. In the **Confirm** dialog box, click **Yes**.

   The VPX instance reboots.

   When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

9. After the failover, log on to the new secondary VPX instance (node 1) and repeat the same process to add the new secondary to the pool.

   If you want to change the primary and secondary instance in the HA pair to your original HA pair configuration, force a failover. Run the following command on any instance in the HA pair:

   ```
   > force ha failover
   <!--NeedCopy-->
   ```

10. To verify that the VPX instance is upgraded to pooled capacity license, log on to the primary and secondary instances and complete the following steps.

    a) On the **Welcome** page, click **Continue**.

    b) On the Configuration tab, navigate to **System > Licenses** and click **Manage Licenses**. On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

Upgrading a Perpetual License in NetScaler MPX to NetScaler Pooled Capacity

March 11, 2024

NetScaler MPX appliance with perpetual license can be upgraded to NetScaler Pooled Capacity license. Upgrading to NetScaler Pooled Capacity license enables you to allocate licenses from the license pool to NetScaler appliances on demand. You can also configure NetScaler Pooled Capacity license for NetScaler instances configured in high availability mode. To configure NetScaler Pooled Capacity license for NetScaler MPX instances in high availability mode, see Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler pooled capacity.

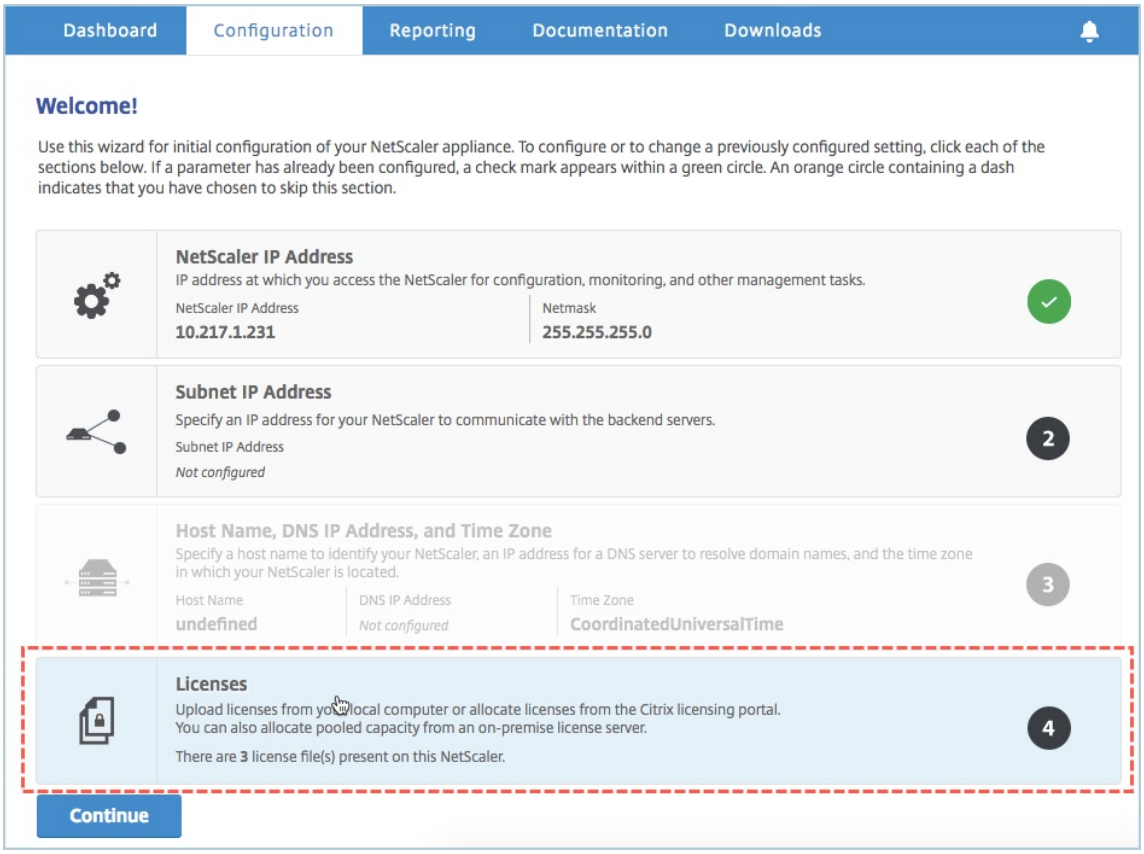
> **Note**
>
> Conversion from a perpetual license to a pooled capacity license is a one-way process for license entitlement. You can't revert the pooled capacity license to perpetual.
>
> **Important**
>
> For upgrading NetScaler MPX appliance to NetScaler Pooled Capacity license, you need to upload the MPX-Z license to the appliance.

To upgrade to NetScaler Pooled Capacity:

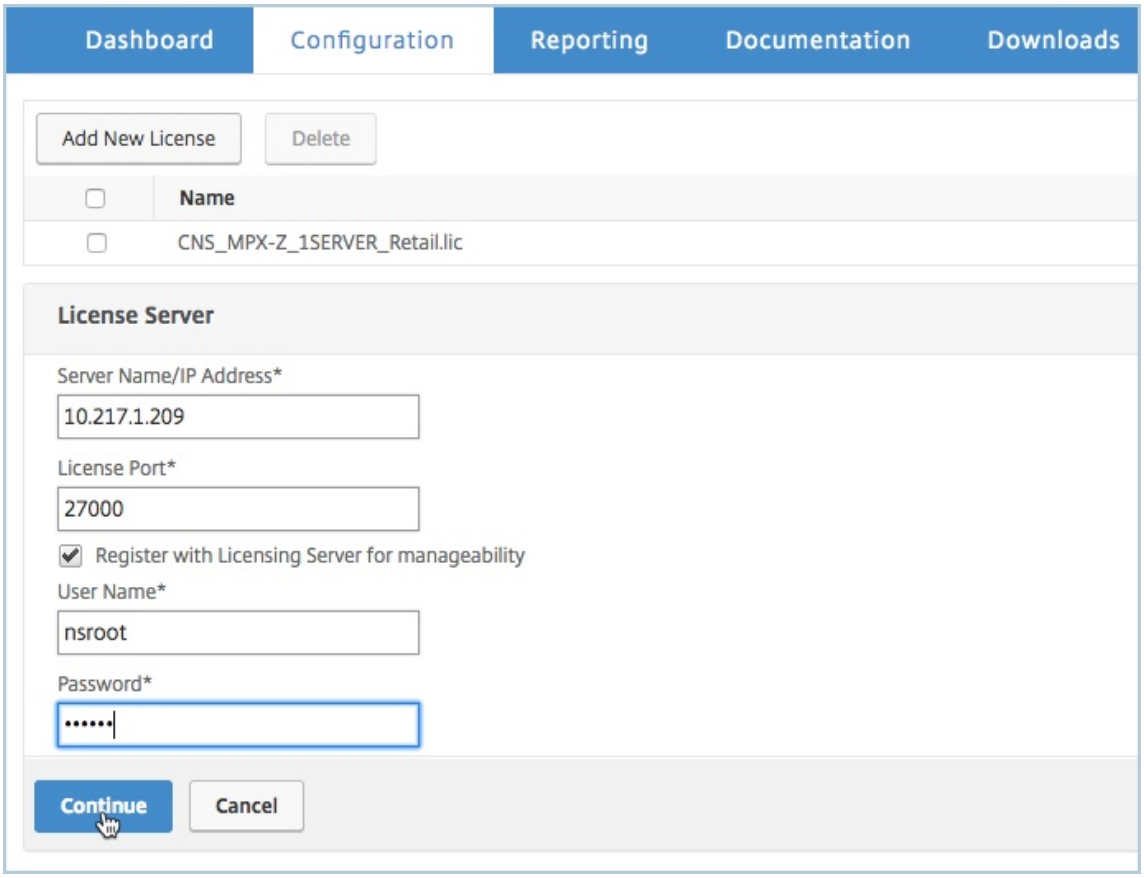
1. In a Web browser, type the IP address of the NetScaler appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the Configuration tab, navigate to **System** > **Licenses**.
5. In the details pane, click **Manage Licenses**, click Add **New License**.
6. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.
7. After the license is uploaded, click **Reboot** to reboot the appliance.

   > **Warning**
   >
   > After applying the MPX-Z license, the features including SSL offloading on the appliance become unlicensed. The appliance stops processing HTTPS requests.
   >
   > If the **Secure Access Only** option is enabled on the appliance before the upgrade, you can't connect to the appliance through NetScaler ADM GUI, by using HTTPS.

8. On the **Confirm** page, click **Yes**.
9. After the appliance reboots, logon to the appliance.
10. On the Welcome page, click the **Licenses** section.



11. In the **License Server** section, do the following:



a) In the **Server Name/IP Address** field, enter the license server details.

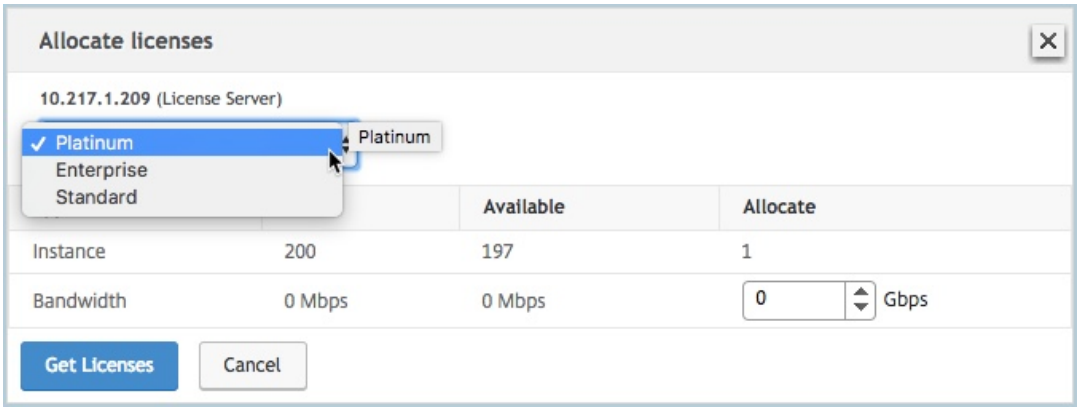
b) In the **License Port** field, enter the license server port. Default value: 27000.

c) If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

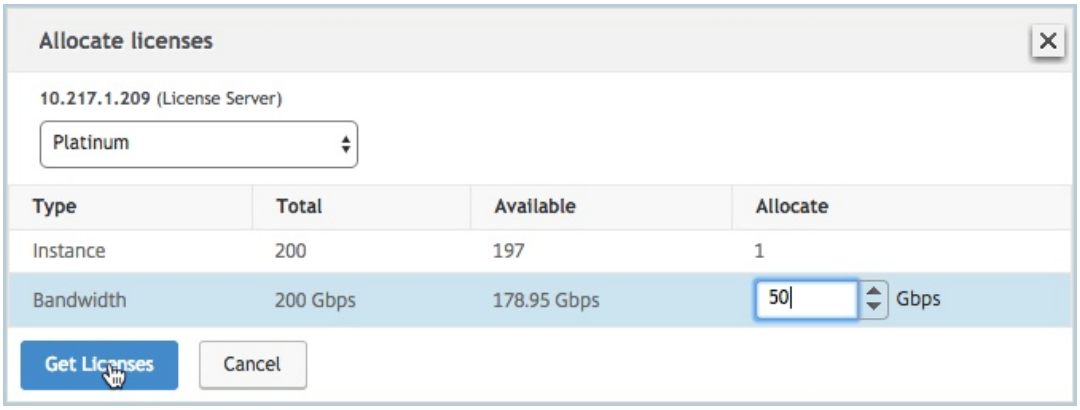
d) Click **Continue**.

12. In **Allocate licenses**, do the following:

a) Select the license edition from the drop-down list.



b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



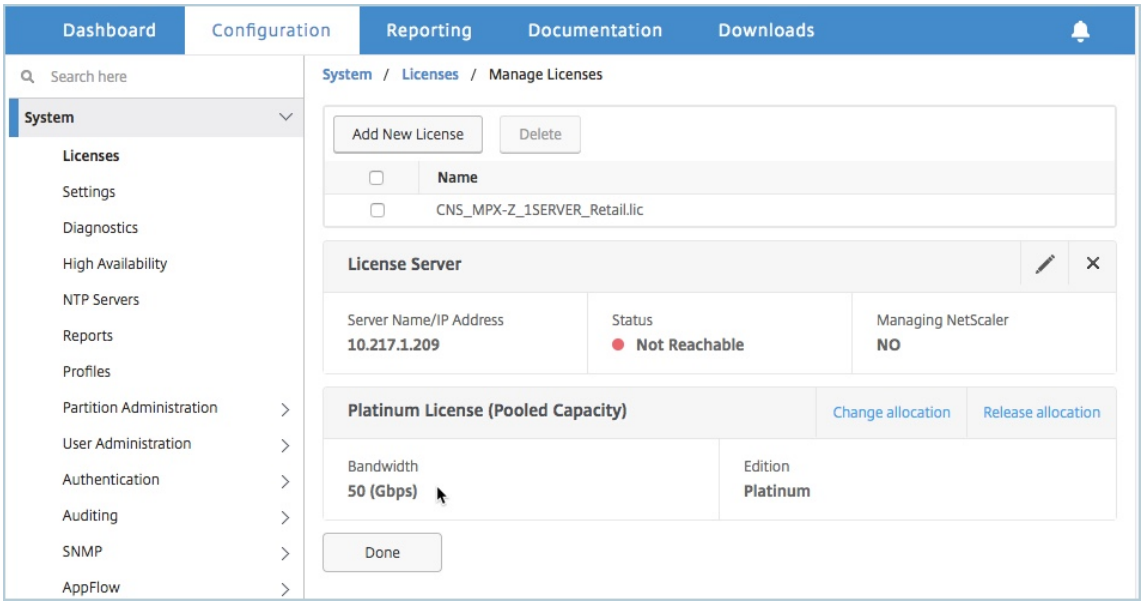
c) When prompted, click **Reboot** to reboot the appliance.

13. Once the NetScaler MPX appliance reboots, logon to the NetScaler MPX appliance. On the **Welcome** page, click **Continue**.

    The **Licenses** page lists all the licensed features.

14. Navigate to **System > Licenses** and click **Manage Licenses**.

    On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated bandwidth.



Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler pooled capacity

For the MPX appliances configured in high availability mode, you have to configure pooled capacity on both the primary and secondary ADC instances in the HA pair. Allocate licenses of the same capacity to both the primary and secondary NetScaler instances in the HA pair. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need to allocate 2 Gbps capacity from the common pool. With 2 Gbps capacity, you can allocate 1 Gbps each to the primary and secondary NetScaler instances in the HA pair.

> **Important**
>
> For upgrading NetScaler MPX appliance to use NetScaler Pooled Capacity license, you need to upload the MPX-Z to the appliance.

Prerequisites

Make sure that you upload the MPX-Z license to both the primary and secondary instances in the HA pair.

To upload the MPX-Z license to the NetScaler MPX instances in the HA pair:

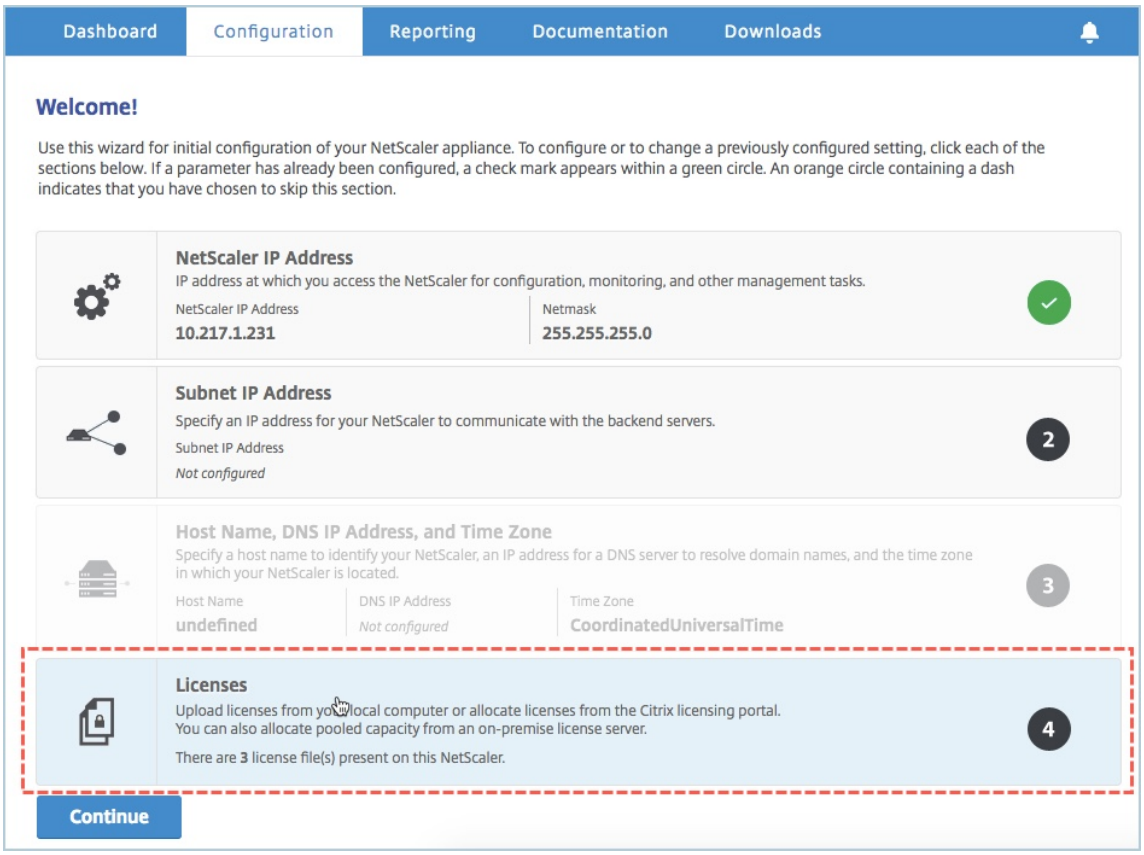
1. In a Web browser, type the IP address of the appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the **Configuration** tab, navigate to **System > Licenses**.
5. In the details pane, click **Manage Licenses**, click **Add New License**.
6. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.

   Once the license is uploaded you are prompted to reboot the appliance.
7. Click **Reboot** to reboot the appliance.
8. On the **Confirm** page, click **Yes**.

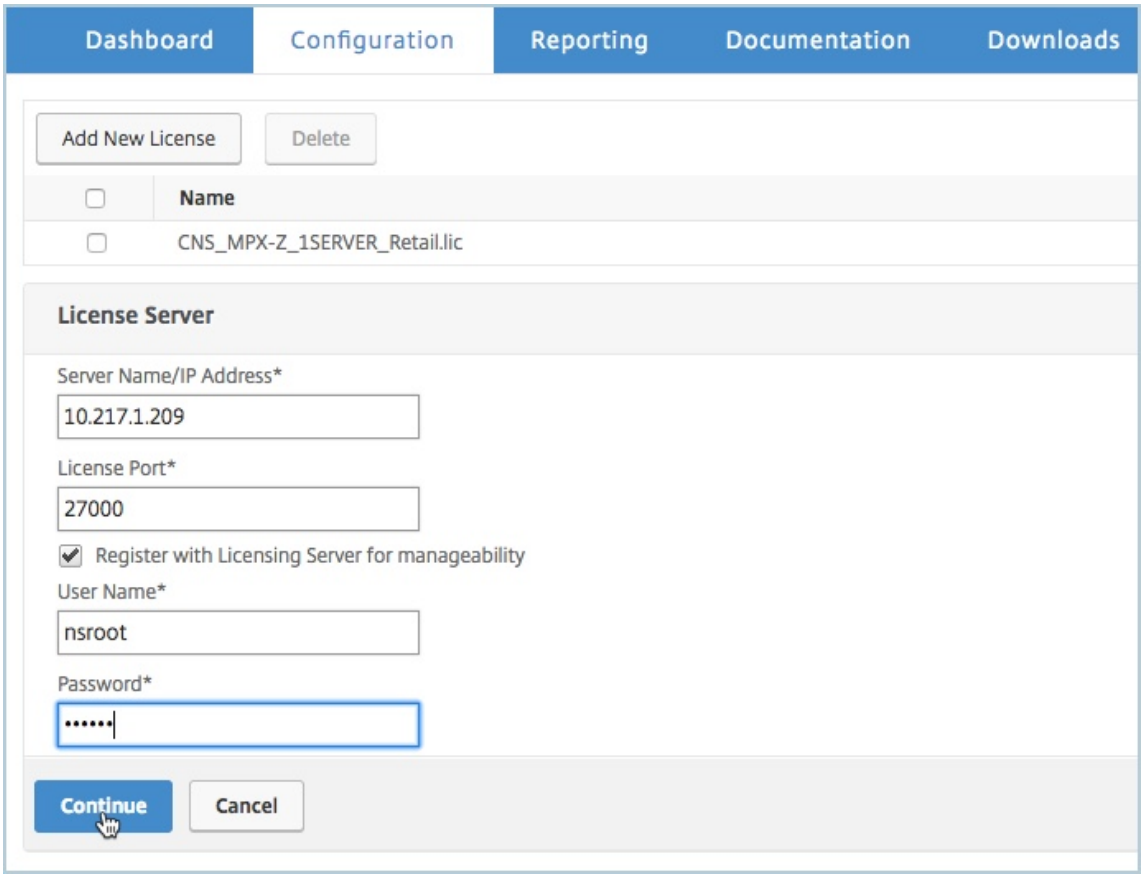
To upgrade an exisiting HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary NetScaler MPX Instance. In a Web browser, type the IP address of the NetScaler appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.

3. On the **Welcome** page, click the **Licenses** section.



4. In the **License Server** section, do the following:



a) In the **Server Name/IP Address** field, enter the license server details.

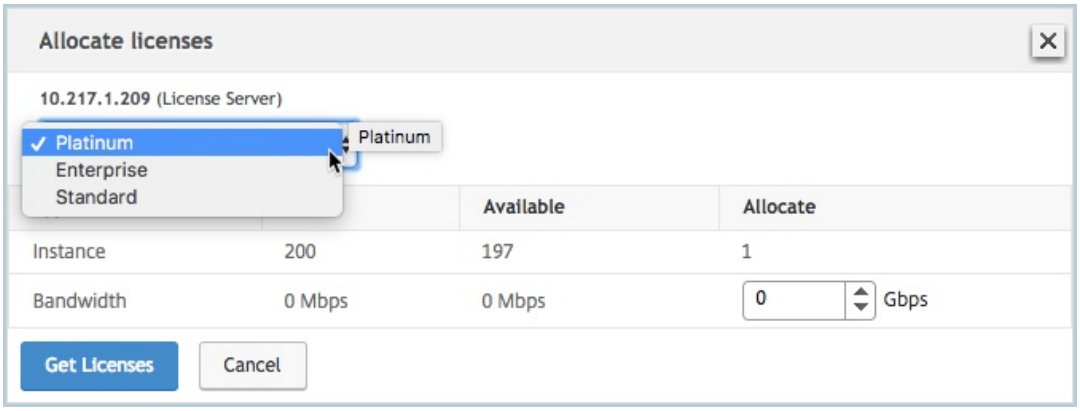
b) In the **License Port** field, enter the license server port. Default value: 27000.

c) If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

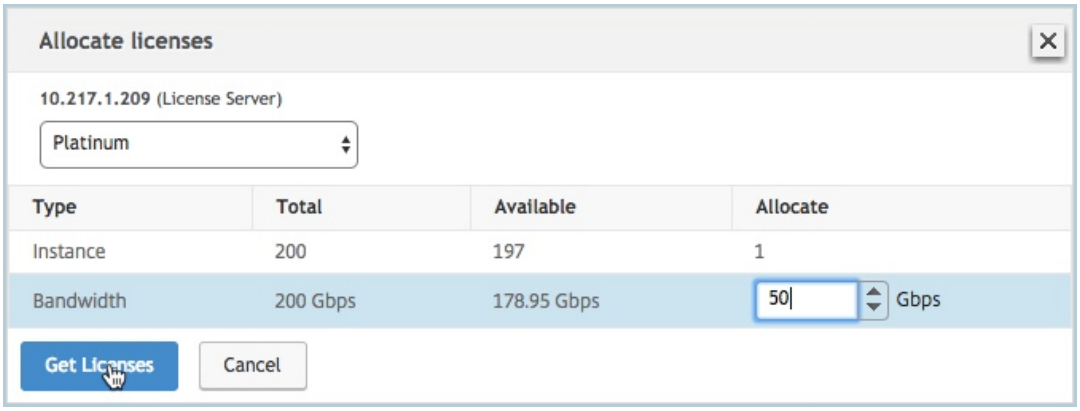
d) Click **Continue**.

5. In **Allocate licenses**, do the following:

a) Select the license edition from the drop-down list.



b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c) When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

6. Log on to the existing primary NetScaler MPX appliance and reboot the appliance. Perform the following:

   a) In a Web browser, type the IP address of the NetScaler appliance, such as http://192.168.100.1.

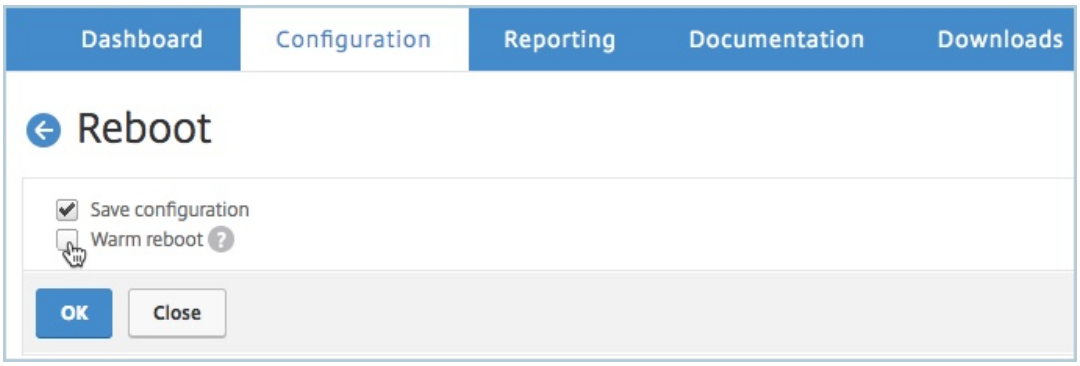
   b) In **User Name** and **Password** fields, type the administrator credentials.

   c) On the **Welcome** page, click **Continue**.

   d) On the **Configuration** tab, click **System**.

   e) On the **System** page, click **Reboot**.

   f) On the **Reboot** page, select **Warm reboot** and click **OK**.



After the primary NetScaler MPX appliance reboots, it becomes the secondary NetScaler MPX appliance in the HA pair. If you want to change the primary and secondary instance in the HA pair to your original HA pair configuration, force a failover. Run the following command on any instance in the HA pair:


```
> force ha failover
<!--NeedCopy-->
```

Upgrade a perpetual license in a NetScaler SDX to NetScaler pooled capacity

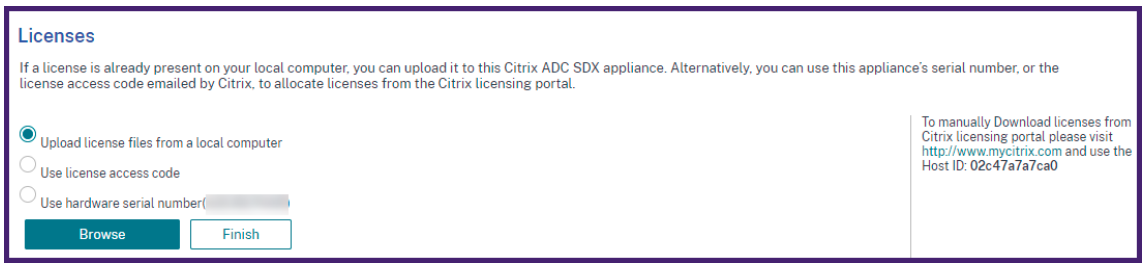
December 31, 2023

A NetScaler SDX appliance with perpetual license can be upgraded to NetScaler Pooled Capacity license. Upgrading to NetScaler Pooled Capacity license enables you to allocate licenses from the license pool to NetScaler appliances on demand. You can also configure the ADC Pooled Capacity license for NetScaler instances configured in high availability mode.

> **Important**
>
> Conversion from a perpetual license to a pooled capacity license is a one-way license entitlement process. You cannot revert the pooled capacity license back to perpetual.
>
> - For upgrading the SDX appliance to NetScaler Pooled Capacity license, you must upload the SDX-Z license to the appliance.
> - Ensure you have the permission to add ADC instances in ADM.
> - To ensure that there is no impact on the current licenses, customer has to allocate the same number of instances and bandwidth that is available as part of the perpetual license.

To upgrade to NetScaler Pooled Capacity:

1. In a Web browser, type the IP address of the SDX appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero-capacity license. On the Configuration tab, navigate to **System** > **Licenses**.
5. On the **Manage Licenses** page, click **Add License File**.
6. In **Licenses** page, select **Upload license files from a local computer** and click **Browse** to select the zero-capacity license from your local machine. Then, click **Finish**.



Once the zero-capacity license is applied successfully, **Pooled Licenses** section appears on the **Licenses** page.

> **Note**
>
> To remove the old license file, you don't have to reboot your SDX appliance so there is no downtime. For more help, contact NetScaler support Team.

7. In the **Pooled licenses** section, do the following:

   a) In the **Licensing Server Name or IP Address** field, enter the license server details.

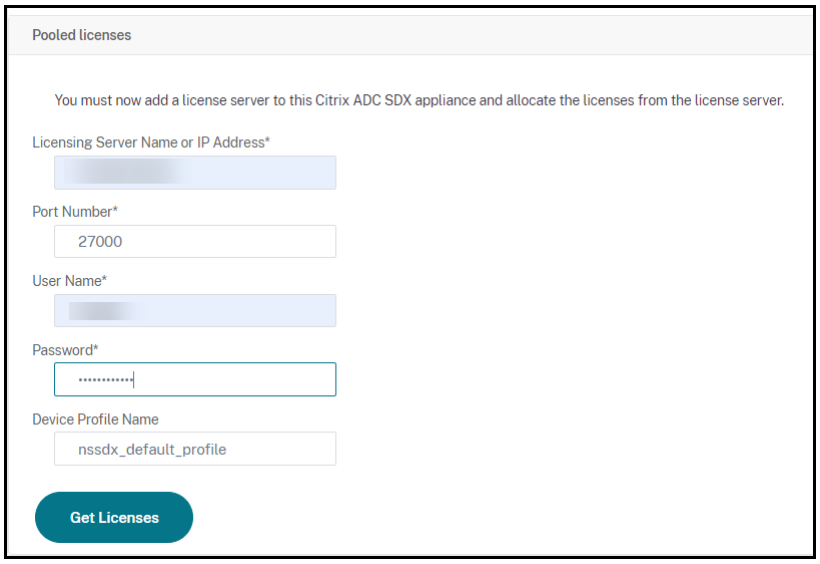
      - If you want to configure ADM server as a license server, specify ADM server's IP address.
      - If you are using an agent to communicate with the ADM server, specify ADM agent's IP address.

   b) In the **Port Number** field, enter the license server port. Default value: 27000.

   c) Specify **User Name** and **Password** of the licensing server.

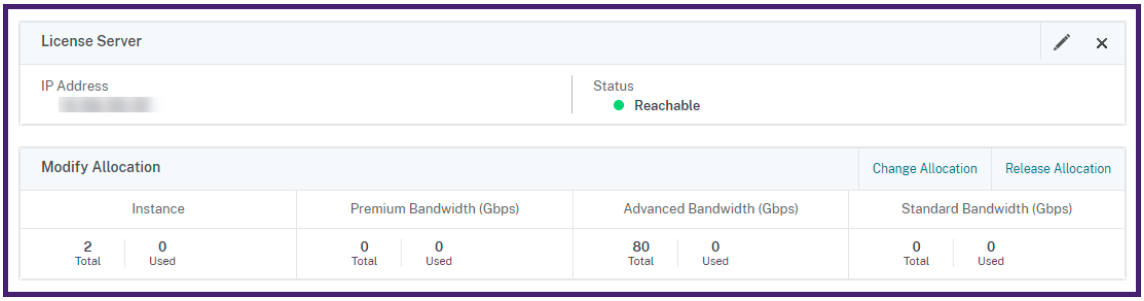
      - For the ADM server, enter the administrator credentials.
      - For the ADM agent, enter the agent credentials.

   d) Click **Get Licenses**.



8. In the **Allocate Licenses** window, specify the required instances and bandwidth and click **Allocate**.

   On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated instances and bandwidth from the pool.



> **Note**
>
> Upgrading a perpetual license to pooled capacity does not require restarting the SDX appliance.

NetScaler pooled capacity on NetScaler instances in cluster mode

March 11, 2024

You can configure NetScaler pooled capacity on the NetScaler instances configured as a cluster. The following are the prerequisites for configuring pooled capacity on NetScaler instances in cluster mode:

- Instances are individually running in a pooled-capacity license mode to form the cluster.
- All the instances must be running with same bandwidth.
- All the instances checked out the pooled capacity from the same NetScaler Application Delivery Management (ADM).
- New instances cannot be added to an existing NetScaler cluster unless their capacity and NetScaler ADM configurations are same as those of the existing instances in the cluster.

Any capacity check-out from the NetScaler cluster assigns same capacity to all the cluster nodes and the checkout Bandwidth = Bandwidth provided * number of nodes.

For example, if you check-out 50 Mbps of bandwidth from the NetScaler cluster, and the cluster includes 12 instances, each instance automatically receives 50 Mbps. And, 600 Mbps is checked out from the pool.

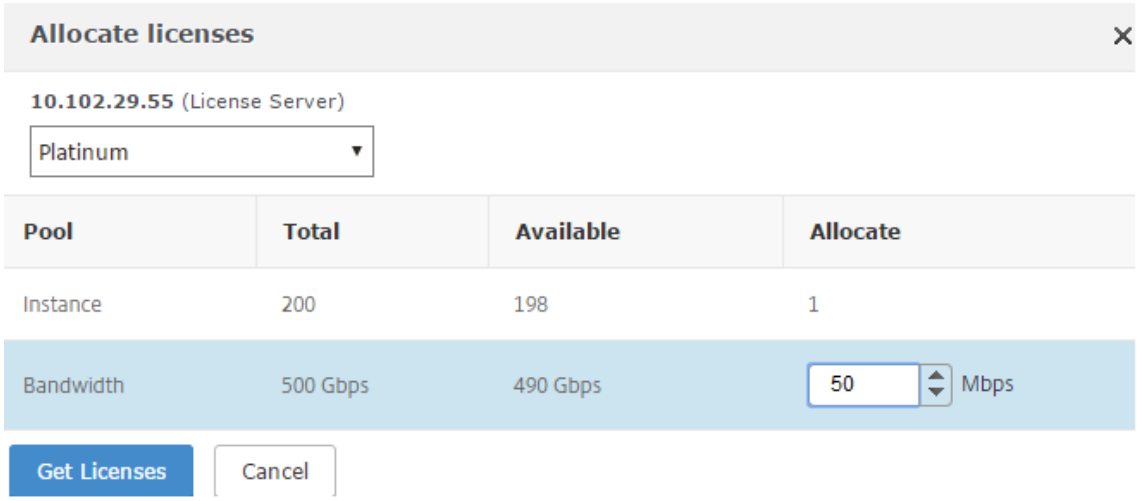
> **Note**
>
> If one or more instances in the cluster become unresponsive, the cluster continues to process the traffic with the remaining instances' capacity.

Allocate ADC Pooled capacity to an ADC cluster

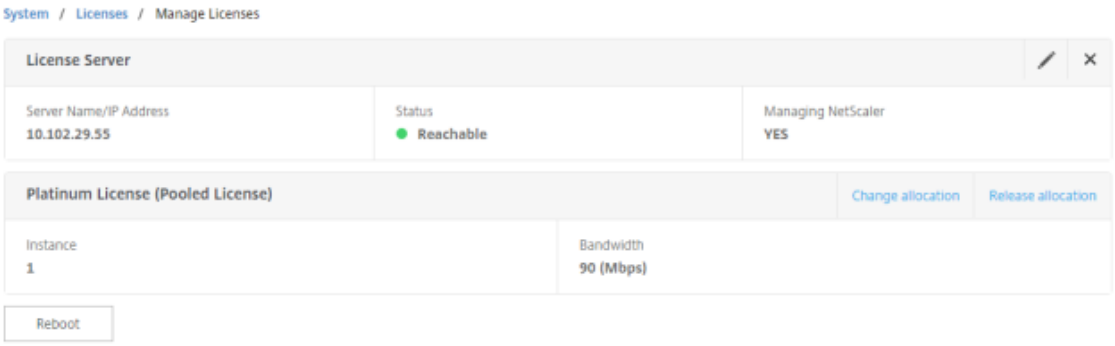
Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

1. In a web browser, type the NetScaler IP address (NSIP). For example, `http://192.168.100.1`.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **Configuration** tab, navigate to **System > Licenses > Manage Licenses**, click **Add New License,** and select **Use Pooled Licensing**.
4. Enter the name or address of the license server in the **Server Name/IP Address** field.
5. If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with NetScaler ADM for manageability** check box and enter the ADM credentials.
6. Select the license edition and the required bandwidth, and click **Get Licenses**.

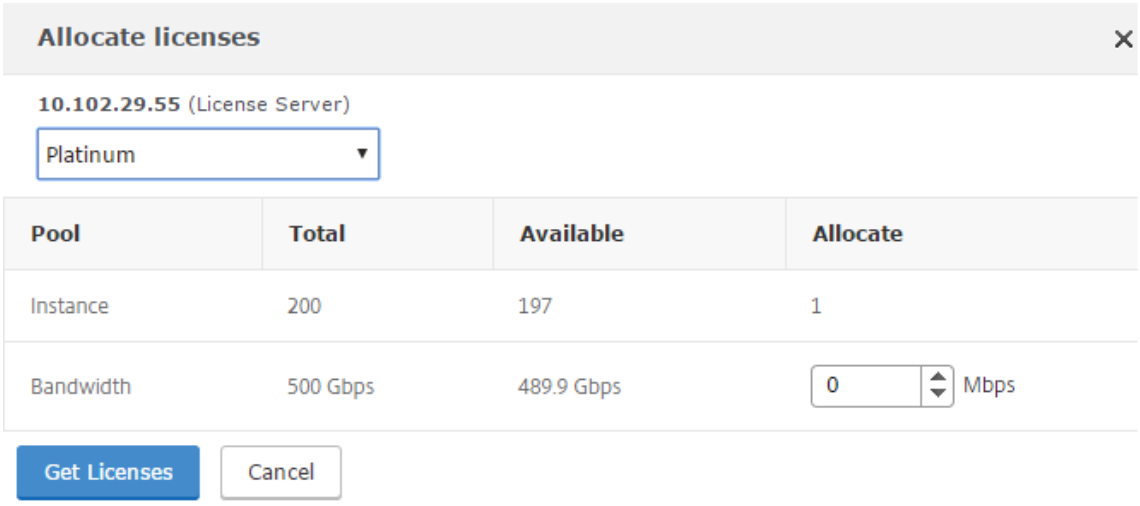


7. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.



8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

> **Note**
>
> Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.



9. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.
10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

> **Note**
>
> A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.

Allocate ADC Pooled capacity to an ADC cluster using CLI

Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

1. In an SSH client, enter the NetScaler IP address (NSIP), and log in by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. To assign a license to the NetScaler VPX appliance, enter the following command:

```
set capacity  –platform V\[S/E/P\]\[Bandwidth\]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```


Health monitoring

December 31, 2023

The license server continuously monitors the health of the NetScaler pooled-capacity enabled instance. The instances communicate through periodical messages to the license server. If few consecutive messages are not received, the license server reports that connectivity has been lost.

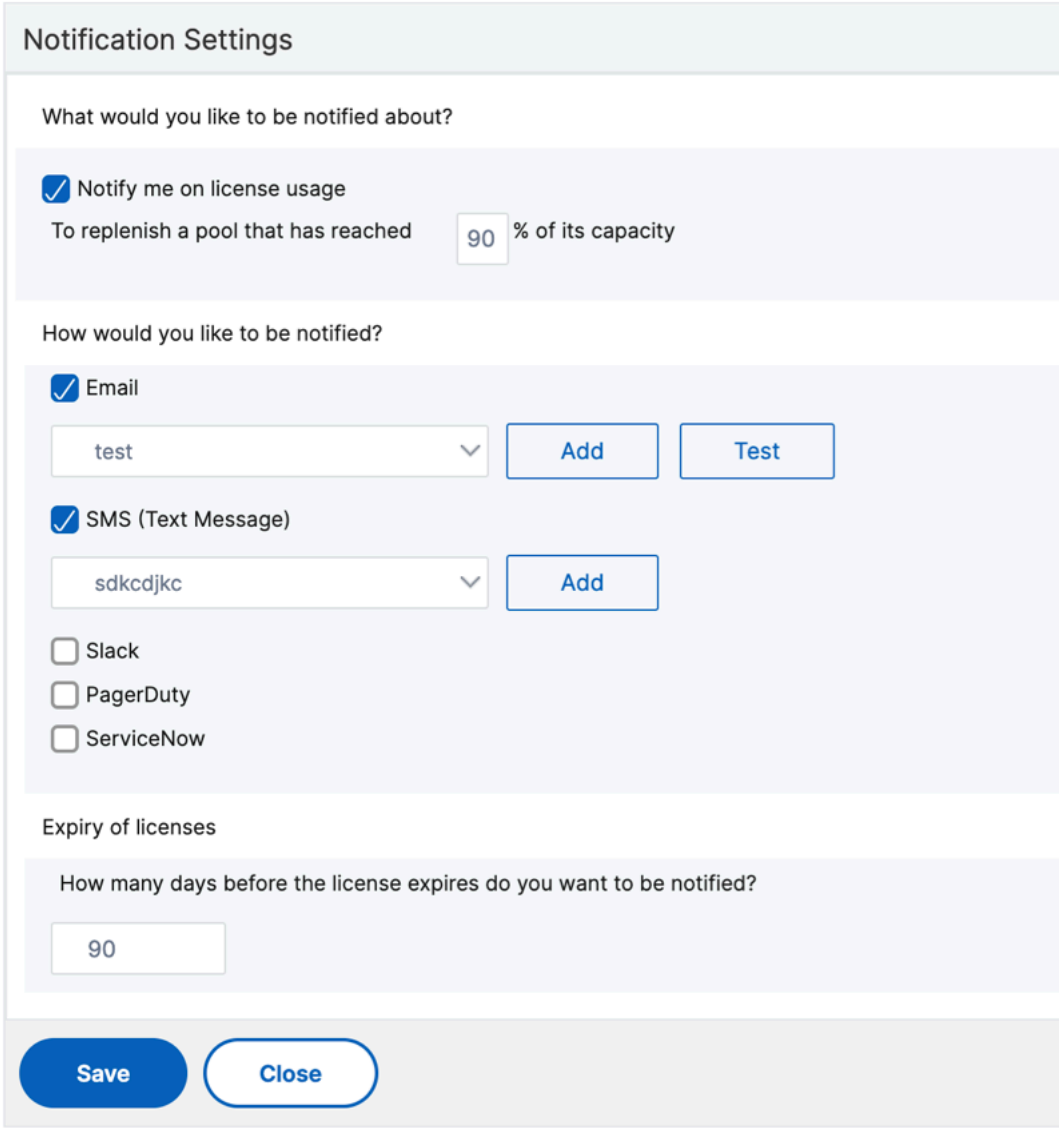
You can create custom notifications to supplement the default alarms.

Grace Period

When a NetScaler pooled-capacity enabled instance is in a healthy state and the license server stops responding, the instance continues to operate with the current capacity for 30 days. If the connectivity to the license server is not restored after 30 days, the instance loses its capacity and stops processing traffic.

Notifications and Alarms

Notifications can be enabled from NetScaler Application Delivery Management (ADM) for any action performed on the instance. Apart from the custom notification settings, some alarms are configured by default. For example: To configure an alarm for replenishing a pool that has depleted a certain percentage of its capacity, navigate to **Infrastructure > Pooled Licensing** and under **Notification Settings**, click the edit icon.



Expected behaviors when issues arise

December 31, 2023

Following are the expected behaviors of the license servers and NetScaler instances when they experience the issues described:

License Server stops responding

> **Warning**
>
> The license Server is not responding. NetScaler continues to operate with the current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the NetScaler loses its current capacity and stops processing traffic.

If the license server stops responding, the NetScaler instance enters the Grace Period until connectivity is restored.

NetScaler pooled-capacity enabled instance stops responding

If the NetScaler pooled-capacity enabled instance stops responding and the license server is in a healthy state, the license server checks in all the NetScaler instance's licenses after 10 minutes. When the instance reboots, it sends a request to check out all the licenses from the licensing server.

Both license server and NetScaler pooled-capacity enabled instance stop responding

If both the license server and the NetScaler pooled-capacity enabled instance restarts and reestablishes the connection, the license server checks-in all its licenses after 10 minutes, and the NetScaler pooled capacity enabled instances automatically check out the licenses after the reboot is completed.

The NetScaler pooled-capacity enabled instance shuts down gracefully

During a graceful shutdown, you can choose to check the licenses in or keep the licenses that were allocated before the graceful shutdown. If you choose to check the licenses in, the NetScaler pooled-capacity enabled instance is unlicensed after it restarts. If you choose to keep the licenses, they are checked in to the licensing server when the instance shuts down. After the instance restarts, it reestablishes the connection with the licensing server and checks out the licenses as specified in the saved configuration.

If the system reboots and the checkout fails due to no capacity available in the pool, the NetScaler checks the inventory of NetScaler Application Delivery Management (ADM) pool licenses and checks out any available capacity. An SNMP alarm is raised to notify this condition to the user if the NetScaler is not running with full capacity as per configuration. If no capacity is available in the bandwidth pool, the pool capacity enabled instance becomes unlicensed.

Network loses connectivity

> **Error message (syslog)**
>
> License Server is not responding.

If the license server and NetScaler pooled-capacity enabled instances are in healthy states but network connectivity is lost, the instances continue to operate with their current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the instances lose their capacity and stop processing traffic, and the license server checks-in all its licenses. After the license server reestablishes connectivity with the NetScaler instances, the instances check the licenses out again.

Configure expiry checks for pooled capacity licenses

March 11, 2024

You can now configure license expiry threshold for NetScaler pooled capacity licenses. By setting thresholds, NetScaler Application Delivery Management (ADM) sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification is also sent when the license has expired on NetScaler ADM.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler ADM.

To configure license expiry checks:

1. Navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
    - **Feature**: Type of license that is going to expire.
    - **Count**: Number of virtual servers or instances that will be affected.
    - **Days to expiry**: Number of days before license expiry.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.
4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
    a) **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
    b) **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.

5. Then, specify when you want to send the notification in terms of number of days before license expiry.
6. Click **Save**.

> **Note**
>
> When you add new licenses to the pool, the NetScaler instances use the new licenses on expiry of their existing licenses.

Check in and check out NetScaler VPX and BLX licenses

March 11, 2024

You can allocate VPX and BLX licenses to NetScaler instances on demand from NetScaler Application Delivery Management (ADM). The ADM software stores and manages the licenses, which have a licensing framework that provides scalable and automated license provisioning. An instance can check out the license from the NetScaler ADM when it is provisioned. When an instance is removed or destroyed, the instance checks back in its license to the NetScaler ADM software.

Prerequisites

Make sure that the following prerequisites are met:

- You are using a NetScaler VPX image running software version 12.0.
  For example: NSVPX-ESX-12.0-xx.xx_nc.zip
- You have installed NetScaler ADM running version 12.0.
  For example: MAS-ESX-12.0-xx.xx.zip

> **Note**
>
> To manage existing VPX licenses by NetScaler ADM, you need to rehost the licenses to NetScaler ADM.

Installing Licenses in NetScaler ADM

> **Note**
>
> Before installing licenses, restart the NetScaler ADM virtual appliance if you have changed the software edition or bandwidth.

To install license files on NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to **Infrastructure > Pooled Licensing**.
4. In the **License Files** section, select one of the following options:

   - **Upload license files from a local computer** - If a license file is already present on your local computer, you can upload it to the NetScaler ADM.
     To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   - **Use license access code** - Citrix emails the license access code for the licenses that you purchase.
     To add license files, enter the license access code in the text box and then click **Get Licenses**.

   > **Note**
   >
   > Make sure you are connected to internet before using license access code for installing the licenses.

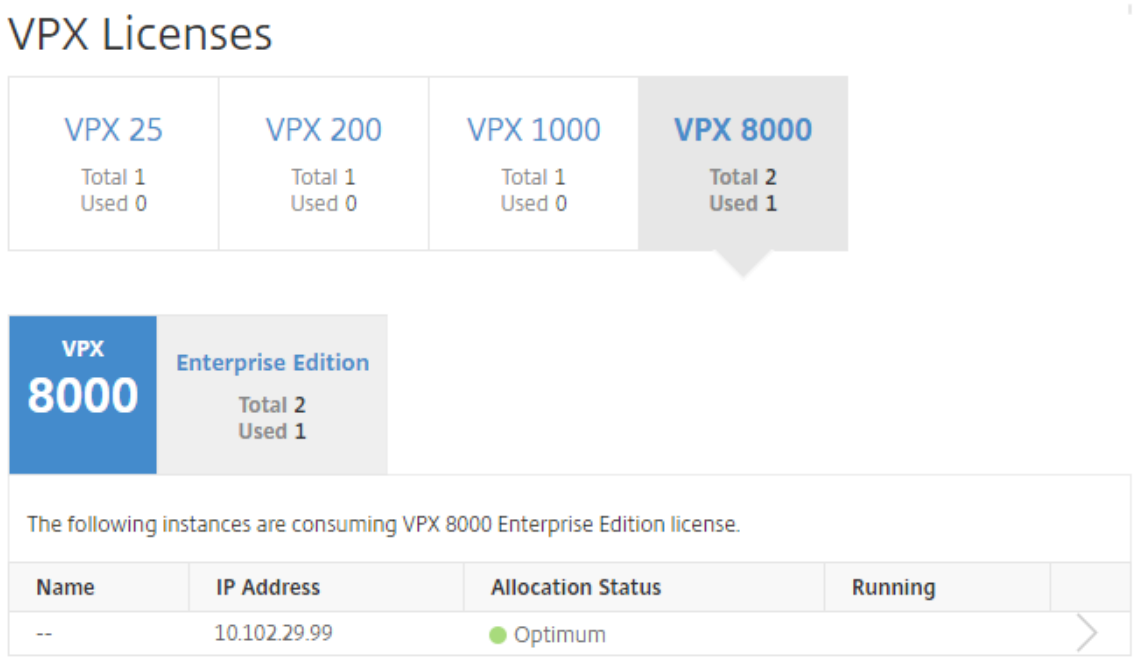
   At any time, you can add more licenses to the NetScaler ADM from the **License Settings** page.

Verification

You can view the available and allocated licenses in the NetScaler ADM GUI.

To display the licenses:

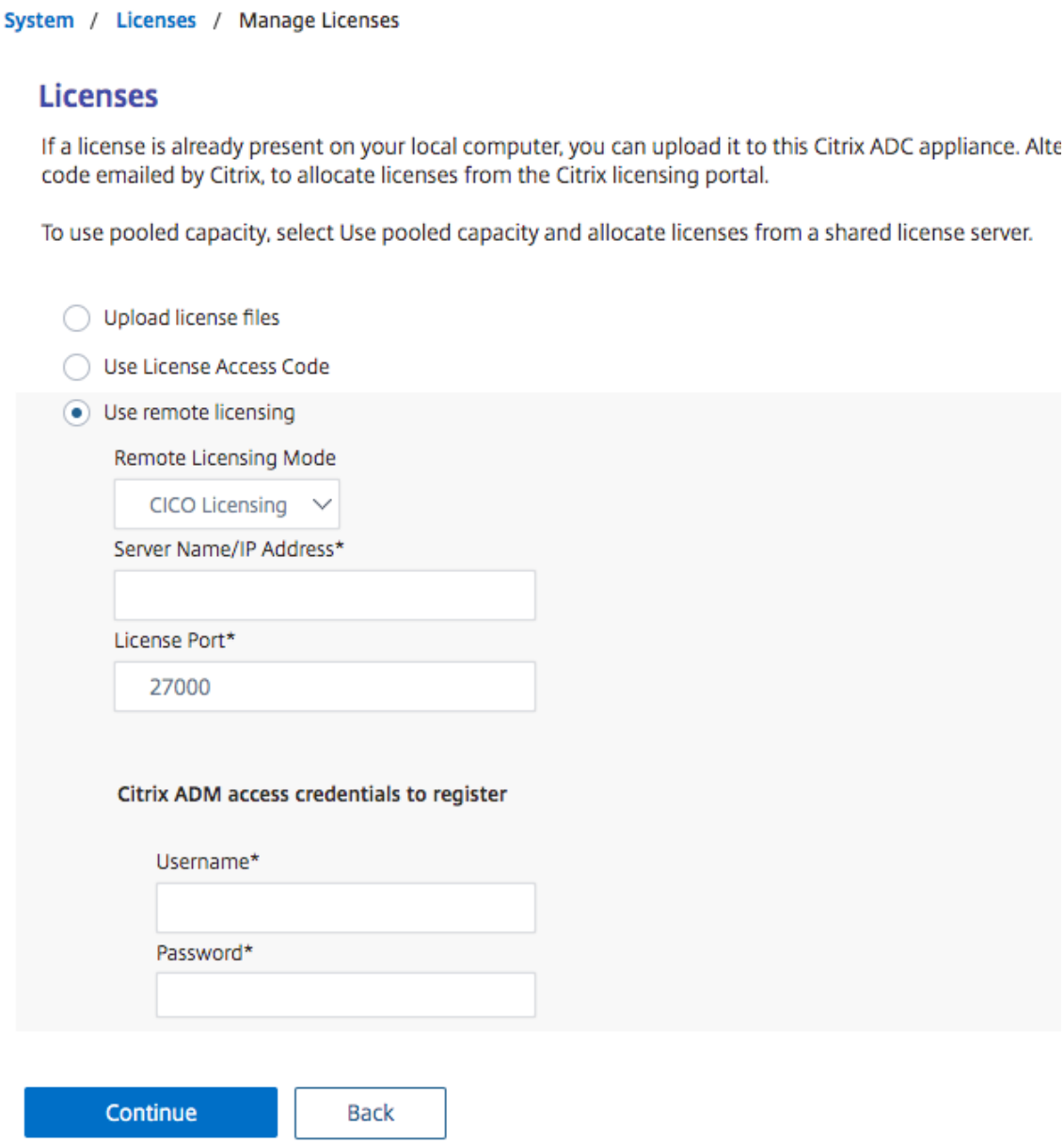
1. In a web browser, type the IP address of NetScaler ADM (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. On the Configuration tab, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**.



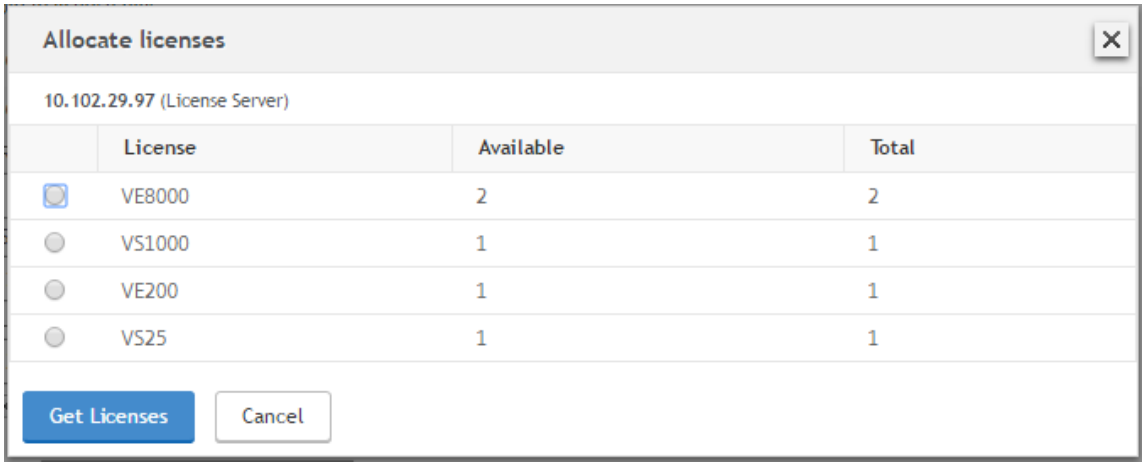
4. You can view the allocated licenses in the table under the available licenses section.

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler GUI

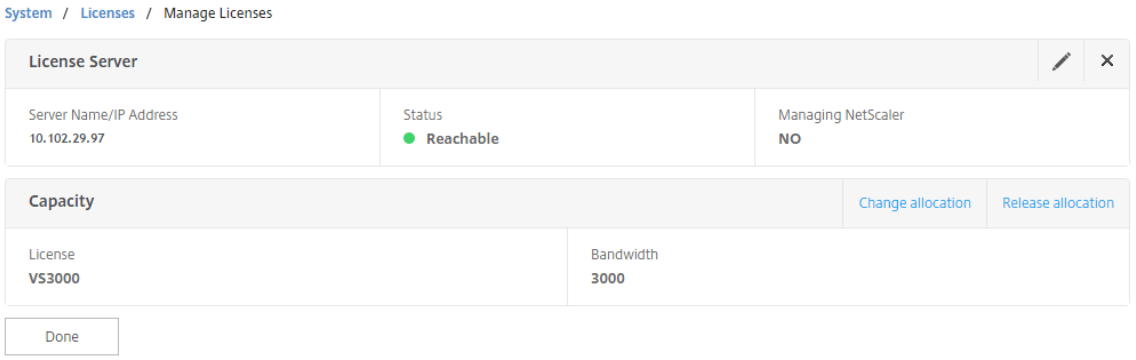
1. In a web browser, type the IP address of the NetScaler instance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the Configuration tab, navigate to **Settings > Licenses > Manage Licenses**, click **Add New License**, and select **Use Remote Licensing > CICO Licensing**.
4. Enter the details of the license server in the **Server Name/IP Address field**.
5. In the **Username** and **Password** fields on the above screen, enter NetScaler ADM credentials and click **Continue**.



6. Select the license edition with the required bandwidth, click **Get Licenses**.



7. Click **Reboot**, your NetScaler instance reboots.
8. You can change or release the license allocation by navigating to **System** > **Licenses** > **Manage Licenses**, and selecting **Change allocation** or **Release allocation.**



9. If you click **Change allocation**, a pop-up window shows the licenses available on the license server. Select the required license, click **Get Licenses**.

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler CLI

1. In an SSH client, enter the IP address of the NetScaler instance, and log on by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. To assign a license to the NetScaler appliance, enter the following command:

```
set capacity  –platform V\[S/E/P\]\[Bandwidth\]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

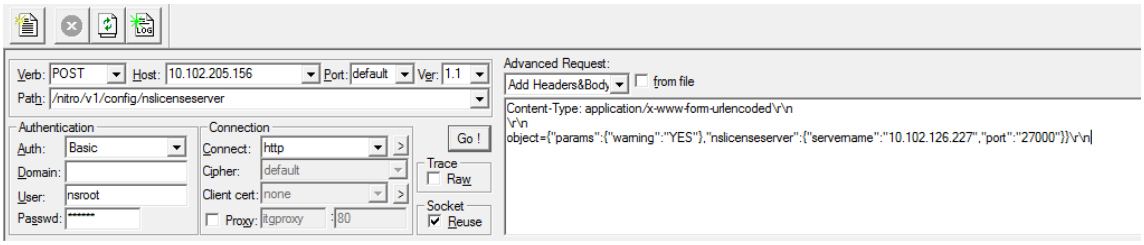
Allocate VPX and BLX Licenses to an ADC instance by using API

In a web browser or an API client, log on to the NetScaler instance by using the administrator credentials.

To add a licensing server:

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nslicensingserver.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n
\\r\\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " \<NetScaler ADM IP\> " , " port " : " 27000 "  }
  }
 \\r\\n
<!--NeedCopy-->
```

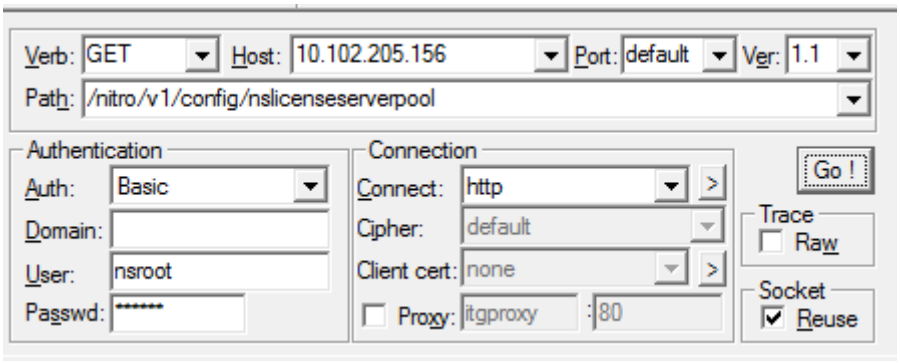


NetScaler ADM responds to the request. The following sample response shows success.

```
RESPONSE: **********\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

To view the available licenses on the licensing server:

1. Set the request type to **Get**.
2. Set the path to /nitro/v1/config/nslicenseserverpool



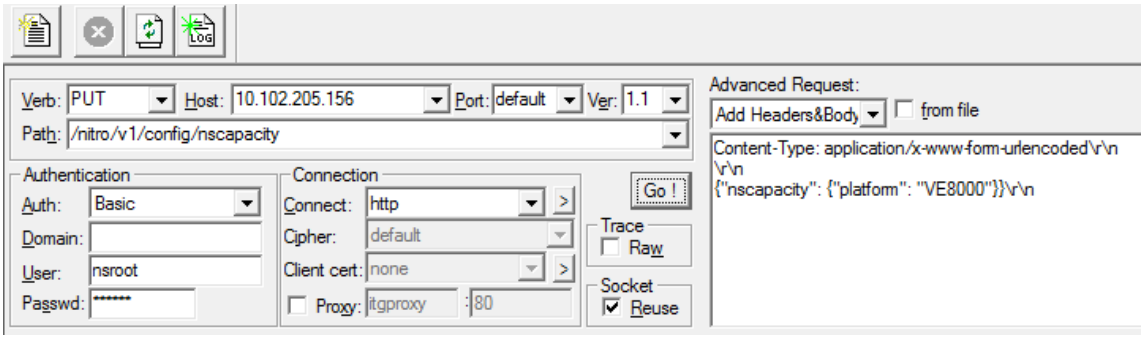
NetScaler ADM responds to the request. The following sample response shows success, and the list of available licenses on the license server.

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

To assign a license to the NetScaler appliance:

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nscapacity.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n
\\r\\n
{
  “ nscapacity:{
  “ platform ” : ” VE8000 ”  }
   }
 \\r\\n
<!--NeedCopy-->
```

NetScaler ADM responds to the request. The following sample response shows success.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Update a licensing server IP address

You can update the licensing server IP address in the VPX and BLX instances, without any impact on the allocated license bandwidth on the instance and data loss.

Update using the CLI: To update the licensing server IP address using the CLI, type the following command on the instance:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and release the resources associated with the previous licensing server.

Update using the GUI: To update the licensing server IP address using the GUI, navigate to **System > Licenses > Manage Licenses**, click **Add New License** For more information, see Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler GUI.

Configure Expiry Checks for NetScaler VPX and BLX Check-In and Check-Out Licenses

You can now configure license expiry threshold for NetScaler VPX and BLX licenses. By setting thresholds, NetScaler ADM sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification are also sent when the license has expired on NetScaler ADM.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler ADM.

To configure license expiry checks:

1. Navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
    - **Feature**: Type of license that is going to expire.
    - **Count**: Number of virtual servers or instances that are affected.
    - **Days to expiry**: Number of days before license expiry.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.
4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
    a) **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
    b) **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.
5. Then, specify when you want to send the notification in terms of number of days before license expiry.
6. Click **Save**.

NetScaler virtual CPU licensing

March 11, 2024

Data center administrators like you are moving to newer technologies that simplify network functions while offering lower costs and greater scalability. Newer data center architecture must include the following features in the least:

- Software-defined networking (SDN)
- Network functions virtualization (NFV)
- Network virtualization (NV)
- Micro-services

Such a movement also needs the software requirements to be dynamic, flexible, and agile to meet the ever-changing business needs. Licenses are also expected to be managed by a central management tool with full visibility into the usage.

Virtual CPU licensing for NetScaler VPX

Earlier, NetScaler VPX licenses were allocated based on the bandwidth consumption by the instances. A NetScaler VPX is restricted to use a specific bandwidth and other performance metrics based on the license edition that it is bound to. To increase the available bandwidth, you must upgrade to a license edition that provides more bandwidth. In certain scenarios, the bandwidth requirement might be less, but the requirement is more for other L7 performance such as SSL TPS, compression throughput, and so on. Upgrading the NetScaler VPX license might not be suitable in such cases. But you might still have to buy a license with large bandwidth to unlock the system resources required for CPU-intense processing. NetScaler ADM now supports allocating licenses to NetScaler instance based on the virtual CPU requirements.

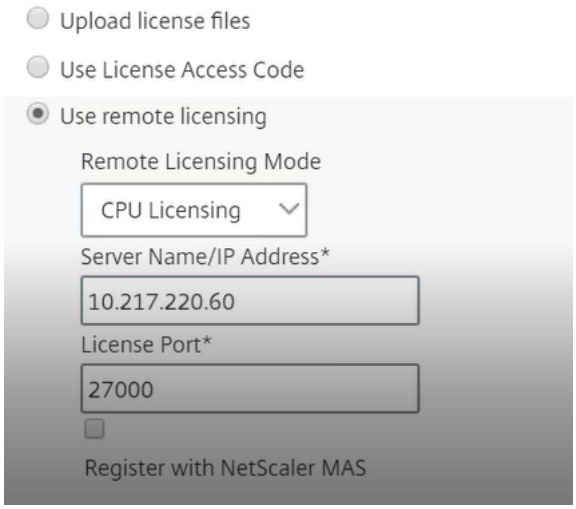
In the virtual CPU-usage-based licensing feature, the license specifies the number of CPUs that a particular NetScaler VPX is entitled to. So, the NetScaler VPX can check out licenses for only the number of virtual CPUs running on it from the license server. NetScaler VPX checks out licenses depending on the number of CPUs running in the system. NetScaler VPX does not consider the idle CPUs while checking out the licenses.

Similar to pooled license capacity and CICO licensing functionalities, the NetScaler ADM license server manages a separate set of virtual CPU licenses. Here also, the three editions managed for virtual CPU licenses are Standard, Advanced, and Premium. These editions unlock the same set of features as those unlocked by the editions for bandwidth licenses.

There might be a change in the number of virtual CPUs or when there is a change in the license edition. In such a case, you must always shut down the instance before you initiate a request for a new set of licenses. Restart the NetScaler VPX after checking out the licenses.

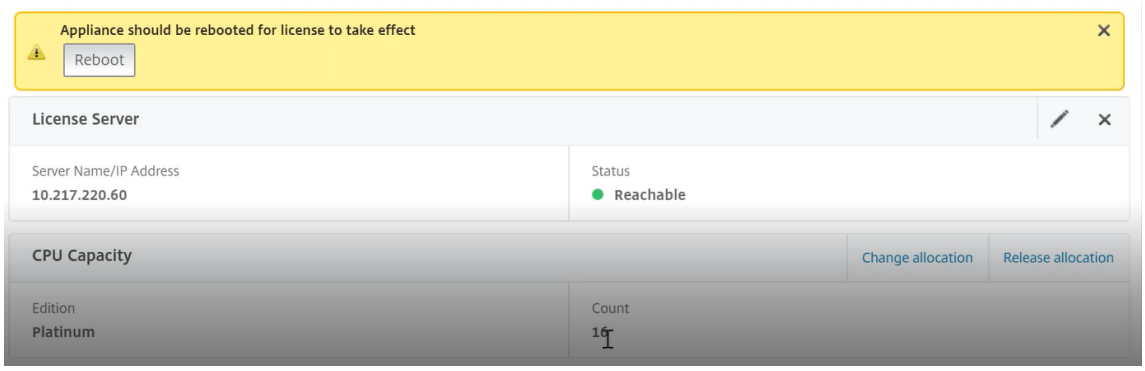
To configure licensing server in NetScaler VPX using GUI:

1. In NetScaler VPX, navigate to **System** > **Licenses** and click **Manage Licenses**.
2. On the **License** page, click **Add New License**.
3. On the **Licenses** page, select the **Use remote licensing** option.
4. Select **CPU licensing** from the **Remote Licensing Mode** list.
5. Type the IP address of the license server and the port number.
6. Click **Continue**.



> **Note**
>
> You must always register NetScaler VPX instance with NetScaler ADM. If not done already, enable **Register with NetScaler ADM** and type NetScaler ADM login credentials.

7. In the **Allocate licenses** window, select the type of license. The window displays the total and the available virtual CPUs and also the CPUs that can be allocated. Click **Get Licenses**.
8. Click **Reboot** on the next page to apply for the licenses.



> **Note**
>
> You can also release the current license and check out from a different edition. For example, you are already running Standard edition license on your instance. You can release that license and then check out from Advanced edition.

Configuring licensing server in NetScaler VPX license using CLI

In the NetScaler VPX console, type the following commands for the following two tasks:

1. To add the licensing server to the NetScaler VPX:


```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. To apply for the licenses:

```
set capacity -vcpu - edition premium
<!--NeedCopy-->
```

When prompted, reboot the instance by typing the following command:

```
reboot -w
<!--NeedCopy-->
```

Update a licensing server IP address

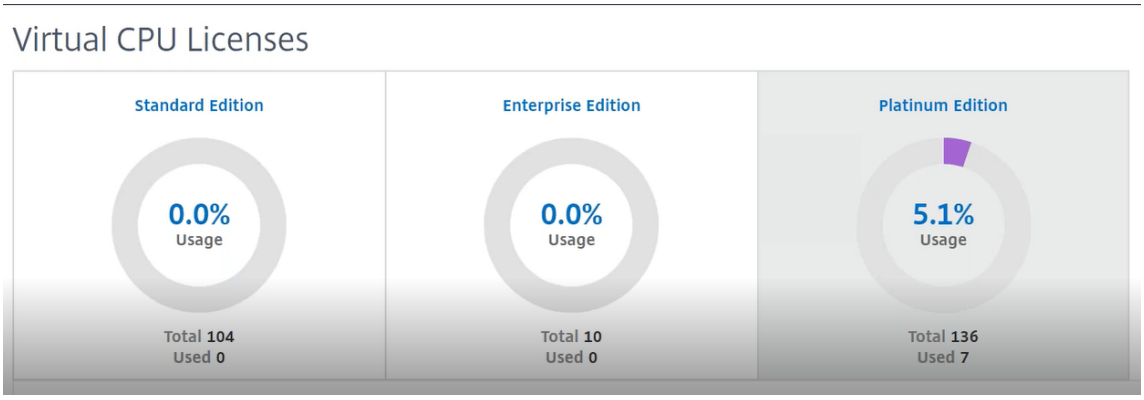
You can update the licensing server IP address in the VPX instance, without any impact on the allocated license bandwidth on the instance and data loss. To update the licensing server IP address, type the following command on the VPX instance:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and release the resources associated with the previous licensing server.

Managing virtual CPU licenses on NetScaler ADM

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing > Pooled VCPU**.
2. The page displays the licenses allocated for each type of license edition.
3. Click the number within each donut to view the NetScaler instances that are using this license.



Virtual CPU licensing for NetScaler CPX

While provisioning the NetScaler CPX instance, you can configure the NetScaler CPX instance to check out licenses from the license server depending on the CPU usage on the instance.

NetScaler CPX relies on the license server, running on NetScaler ADM, to manage the licenses. NetScaler CPX checks out the licenses from the license server when it is starting up. The licenses are checked in back to the license server when the NetScaler CPX shuts down.

You can download the NetScaler CPX image from the Quay container registry using the 'docker pull' command and deploy it on your environment.

There are three license types available for CPX licensing:

1. Virtual CPU subscription licenses supported for CPX and VPX
2. Pooled Capacity licenses
3. CP1000 licenses that support single to multiple vCPUs for CPX only

To configure vCPU subscription licenses while provisioning the NetScaler CPX instance:

Specify the number of vCPU licenses that the NetScaler CPX instance uses.

- This value is entered as an environment variable through Docker, Kubernetes, or Mesos/-Marathon.
- The target variable is "CPX_CORES."The CPX can support from 1 to 16 cores.

To specify 2 cores, you can perform the docker run command as follows:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

While provisioning a NetScaler CPX instance, define the NetScaler Licensing Server as an environmental variable in the **docker run** command as shown below:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

Where,

- *<LS_IP_ADDRESS>* is the IP address of the NetScaler Licensing Server.
- *<LS_PORT>* is the port of the NetScaler Licensing Server. By default, the port is 27000.

> **Note**
>
> By default, the NetScaler CPX instance checks out the license from the vCPU subscription pool. The CPX instance checks out an “n”number of licenses if the instance is running with “n”CPUs.

To configure NetScaler Pooled Capacity or CP1000 licenses while provisioning the NetScaler CPX instance:

If you want to check out licenses for the CPX instance using the pooled licensing (bandwidth-based) or the CPX private pool (CP1000 or private-pool-based), you must provide the environment variables accordingly.

For example,

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```

CP1000. This command triggers the checkout from CP1000 pool (CPX private pool). The NetScaler CPX instance then retrieves “n”number of instances for “n”number of cores specified for CPX_CORES. The most common use case is to specify n = 1 for a checkout of a single instance. Multicore CPX use cases check out “n”vCPUs (where “n”is from 1 to 7).

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e BANDWIDTH=2000 cpx:11.1
2 <!--NeedCopy-->
```

Pooled capacity. This command checks out one license from the instance pool and consumes 1000 Mbps of bandwidth from the Premium bandwidth pool yet enables CPX to run up to 2000 Mbps. In Pooled Licensing, the first 1000 Mbps is not charged.

> **Note**
>
> Specify the corresponding number of vCPUs for the desired target bandwidth when checking out from the bandwidth pool as detailed in the following table:

Number of cores (vCPU)	Maximum bandwidth
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps

5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

Manage system settings

March 11, 2024

The following table describes the list of options available under **Settings** > **Administration**:

Network Configurations

Network Configurations	Options	Description
IP Address, Second NIC, Host Name and Proxy Server	IP address	Displays the NetScaler ADM network configuration IP address details that are used to deploy NetScaler ADM
	Second NIC	Enables you to configure a second NIC to isolate NetScaler ADM management access. For more information, see Configure a dual NIC to access NetScaler ADM
	Host name	Enables you to assign a host name to NetScaler ADM. For more information, see Assign a host name to a NetScaler ADM server
	Proxy Server	Enables you to configure ADM as a proxy server. For more information, see NetScaler ADM as an API proxy server

Network Configurations	Options	Description
Static Routes		Enables you to configure static routes to establish connection between NetScaler ADM and NetScaler VPX instances
NTP Servers		Ensures NetScaler ADM clock has the same date and time settings as the other servers on the network. For more information, see Configure NTP server
ADM Ports Information		Enables you to understand which port must be open for communication between ADM and ADC instances. For more information, see Supported Ports

System Configurations

System Configurations	Options	Description
System, Time zone, Allowed URLs and Message of the day	Basic Settings	Enables you to modify system settings such as enable `nsrecover` login, enable session timeout, and so on
	Time Zone	Enables you to modify the timezone to be used in NetScaler ADM. The default timezone is UTC
	Allowed URL List	Enables you to configure URLs to send uninterrupted requests to ADM. You can configure it with the value “none”if no URL to be added

System Configurations	Options	Description
	Message of the day	Enables you to create a welcome message in NetScaler ADM. You can use this feature to set reminder messages for yourself or the user who logs on to NetScaler ADM. Click **Enable Message**, type the message in the message box, and click **Save**
View ADM Fingerprint		Enables you to copy the unique NetScaler ADM fingerprint ID to get started with service graph
Configure Customer Identity		Enables you to protect the network resources by permitting only authenticated customers or users to access its network. For more information, see Data Governance
CUXIP Settings		If you select this check box, usage statistics are collected for the sole purpose of improving the GUI. The received data is used only by Citrix engineers and is not shared with anyone

System Maintenance

System Maintenance	Description
Upgrade NetScaler ADM	Enables you to upgrade the NetScaler ADM through GUI. For more information, see Upgrade
Reboot NetScaler ADM	Enables you to reboot NetScaler ADM
Shut Down NetScaler ADM	Enables you to shut down NetScaler ADM
Disaster Recovery	Enables you to view disaster recovery node information. For more information, see Configure Disaster Recovery

Data Pruning

Data Pruning	Options	Description
System and Instance Data Pruning	System	Enables you to limit the amount of reporting data being stored in NetScaler ADM server database. For more information, see Configure system prune settings
	Instance Events	Enables you to limit the event messages reporting data stored in NetScaler ADM
	Instance Syslog	Enables you to limit the amount of syslog data stored in the database. For more information, see Configure instance syslog prune settings
	Network Reporting	Enables you to limit the network reporting data stored in NetScaler ADM

Backup

Backup	Options	Description
Configure System and Instance backup	System	Enables you to configure the initial backup settings before doing a system backup. For more information, see System Backup Settings
	Instance	Enables you to configure settings on NetScaler ADM to back up a selected NetScaler instance or multiple instances. For more information, see Configure instance backup settings

Event Notifications

Event Notifications	Options	Description
Configure Event Notification and Digest	Event Notification	You can send notifications to select groups of users for several system-related functions. These system functions are organized into event categories such as SystemReboot, StatusPoll, SystemState, and so on. You can configure NetScaler Application Delivery Management (ADM) to send you notifications either through Email, SMS, or Slack. This ensures that you are notified of any system-level activities such as exceeding of data storage or backup failure.
	Event Digest	Enables you to get a consolidated report of important system and feature events

SSL Settings

SSL Settings	Description
Install SSL Certificate	Enables you to install SSL certificate and SSL Key file
View SSL Certificate	Enables you to view the SSL certificate details
Configure SSL Settings	For more information, see Configure SSL settings
SSL Certificates	Enables you to upload, download, or delete an SSL certificate or SSL Key file
Cipher Groups	For more information, see Configure a Cipher Groups

Configure Features

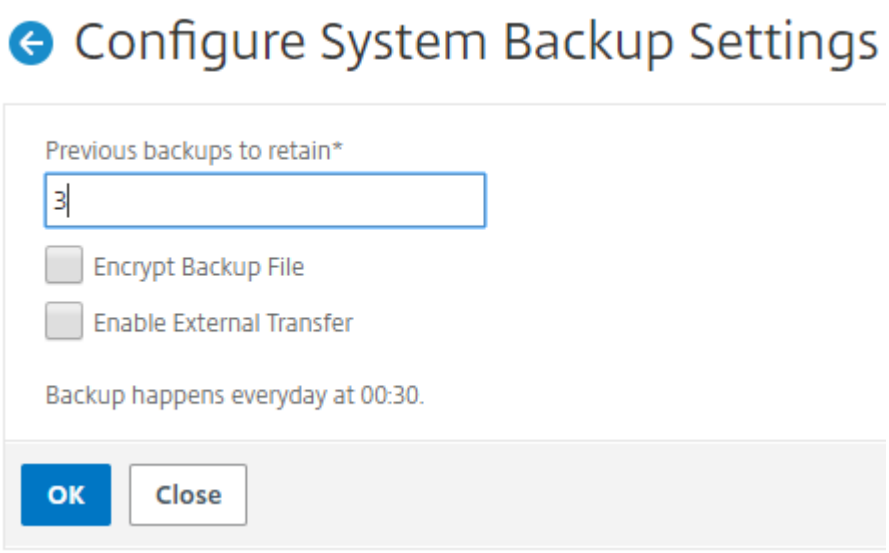
Configure Features	Description
Disable or enable features	You can enable or disable features in NetScaler ADM. For more information, see Enable or disable ADM features

Configure system backup settings

March 11, 2024

Set your initial System Backup Settings before you need to back up and restore the NetScaler Application Delivery Management (ADM) system.

1. Navigate to **Settings > Administration**. Under **Backup**, click **Configure System and Instance backup**.
2. On the **Backup > System** page, specify the following:
   - Previous backups to retain. You can only retain up to 10 backups.
   - Select **Encrypt Backup File** to encrypt the backup files.
   - Select **Enable External Transfer** to transfer a copy of your backup file to another system. When you want to restore the configuration, you have to first upload the file to the NetScaler ADM server and then perform the restore operation. Specify the server, user name and password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see Transfer a NetScaler ADM Backup File to an External System.
3. Click **OK**.



Configure an NTP server

March 11, 2024

You can configure a Network Time Protocol (NTP) server in NetScaler Application Delivery Management (ADM) to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server on NetScaler ADM:

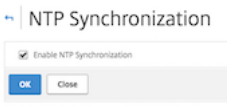
1. Navigate to **Settings > NTP Servers**, and then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
   - **Server Name/IP Address** –Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - **Minimum Poll Interval** –Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2^6, enter 6.
   - **Maximum Poll Interval** –Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2^8, enter 8.
   - **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.
   - **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.

- **Preferred** –Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

To enable NTP synchronization on NetScaler ADM:

1. Navigate to **Settings > NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** check box.
3. Click **OK**.



> Note
>
> You can find the NTP logs messages in the /var/log directory in the file `/var/log/ntpd.log` file.

Upgrade NetScaler Application Delivery Management (ADM)

March 11, 2024

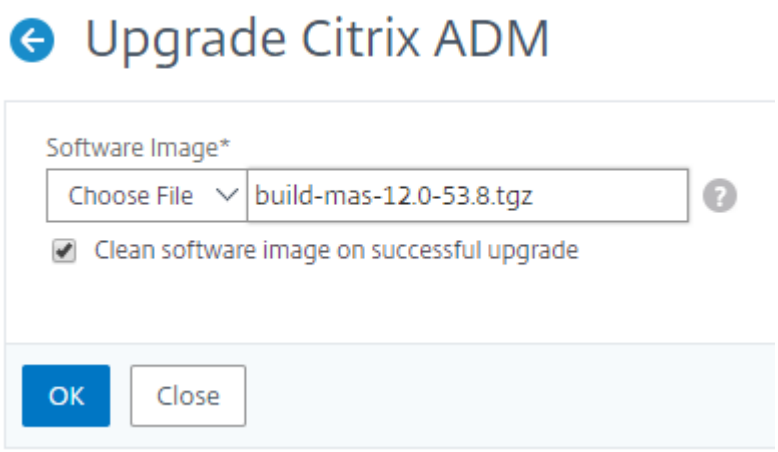
Each NetScaler ADM release offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read the release notes before you upgrade the software. It is important to understand the licensing framework and types of licenses before you start to upgrade.

To upgrade NetScaler ADM:

1. Navigate to **Settings > Administration**. Under **System Maintenance**, click **Upgrade NetScaler ADM**.
2. On the Upgrade NetScaler ADM page, upload a new image file by selecting either **Local** (your local computer) or **Appliance**.

   > **Note**
   >
   > When you select **Appliance**, ensure that the upgrade image is available at `/var/mps/mps_images` in NetScaler ADM.

   By default, the software image is cleaned up after a successful upgrade.
3. Click **OK**.



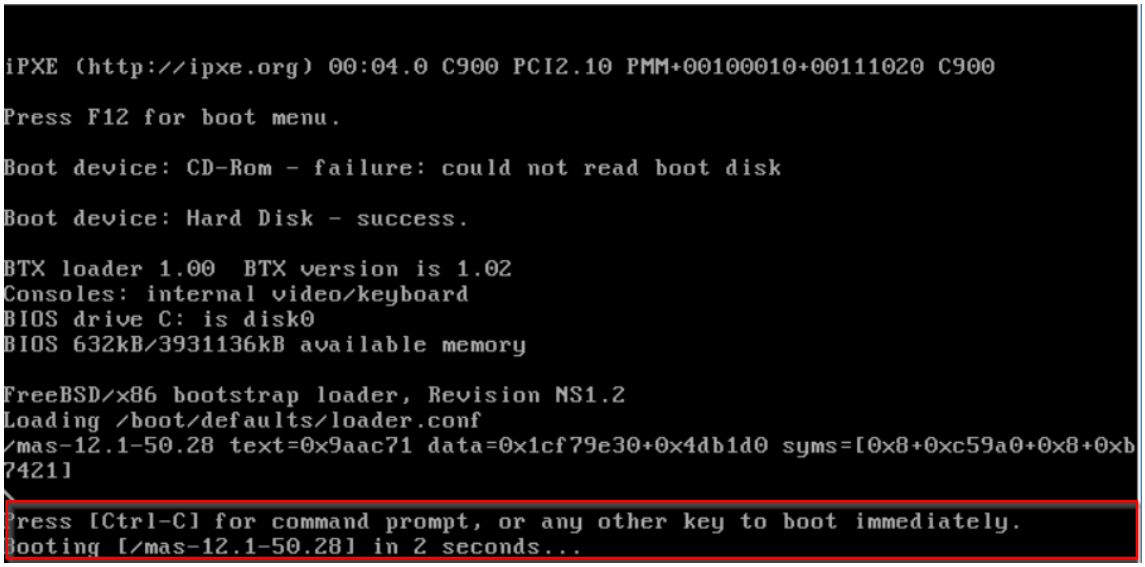
How to reset the password for NetScaler ADM

March 11, 2024

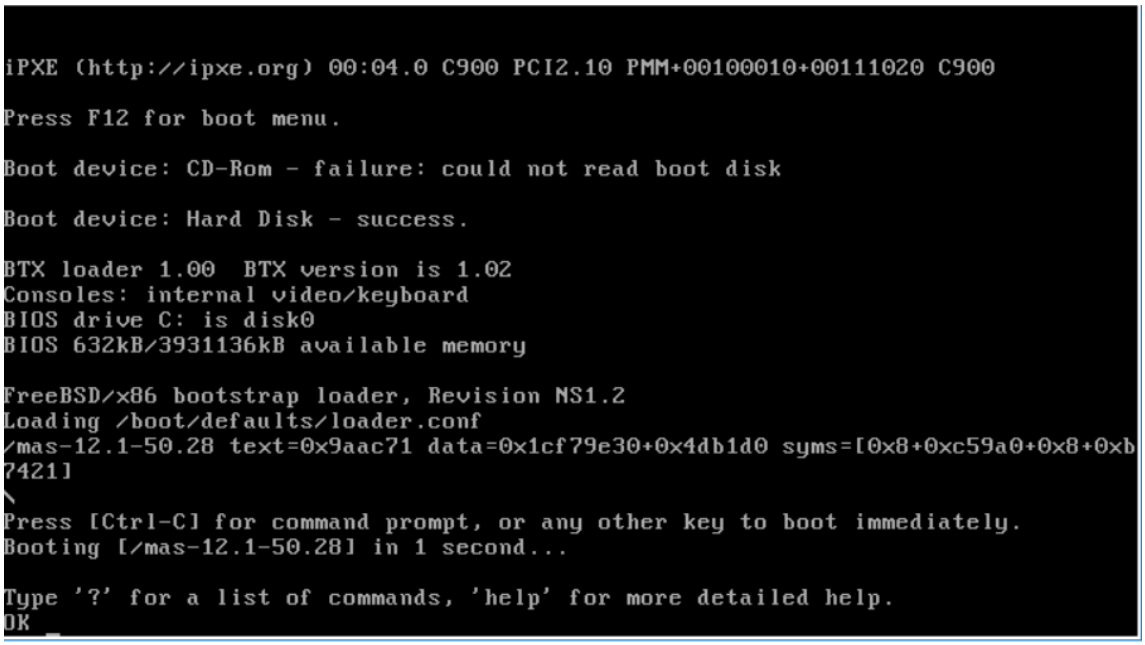
The procedure to reset the password for NetScaler ADM might differ on hypervisors where it is hosted. If you have changed your default password and want to reset to default password, you can reset the password by rebooting the NetScaler ADM node.

Citrix Hypervisor using XenCenter:

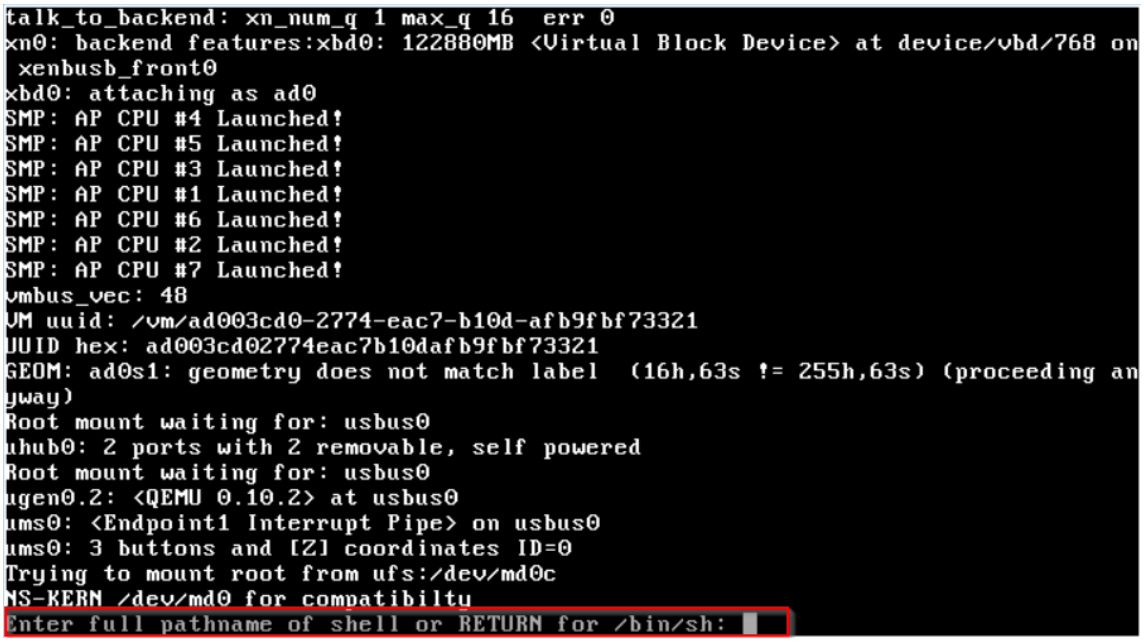
1. Log on to Citrix Hypervisor using XenCenter.
2. Select the NetScaler ADM node, right-click, and select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.



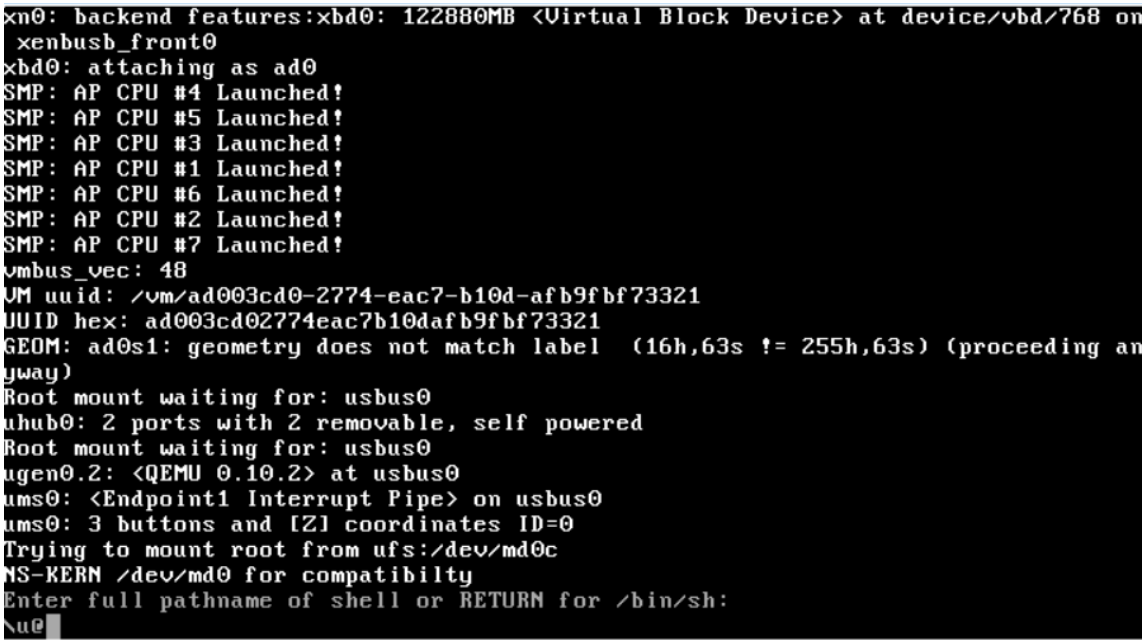
4. Run **boot -s** command at the OK prompt.



NetScaler ADM reboots and displays the following message:

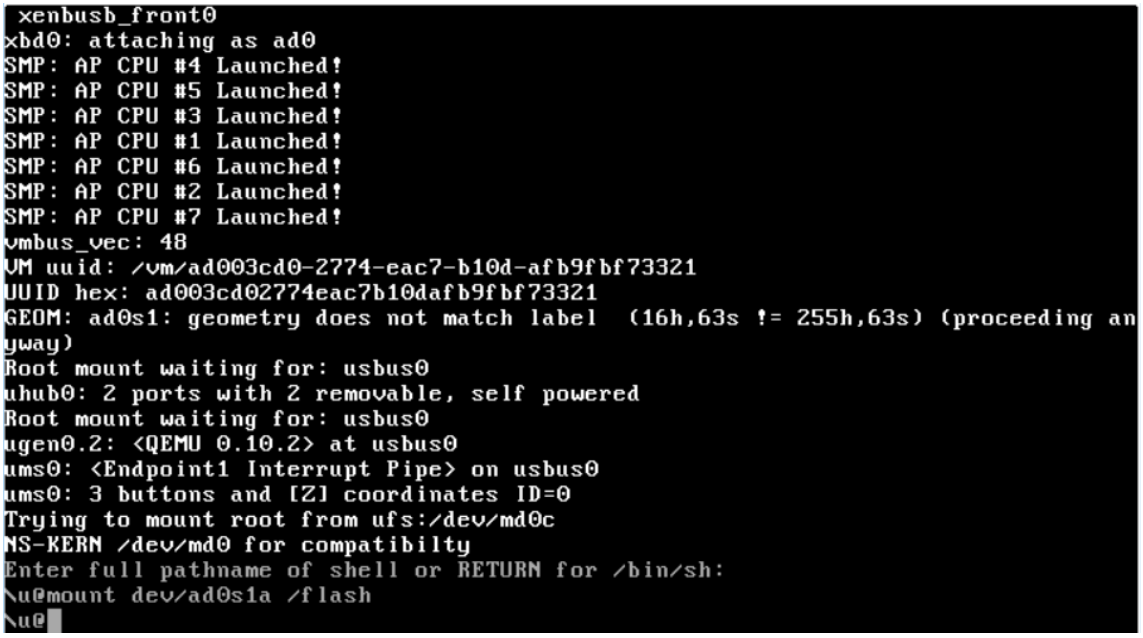


5. Press **Enter** to get the /u@ prompt.



6. Mount the flash partition using the following command:

```
mount /dev/da0s1a /flash
```

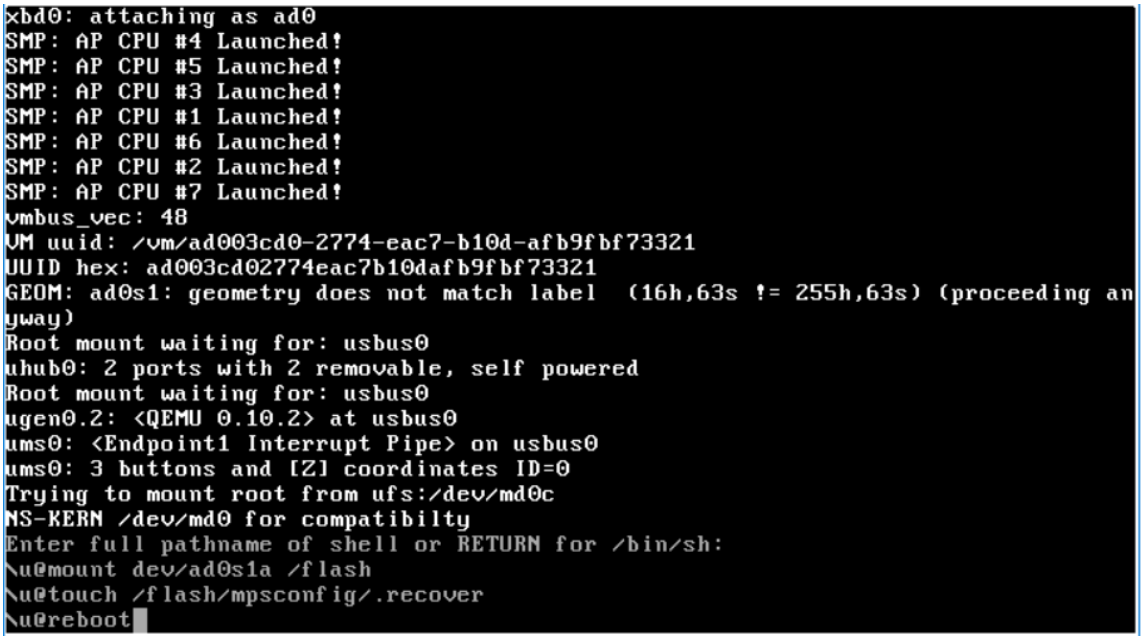



7. Create a file using the following command:

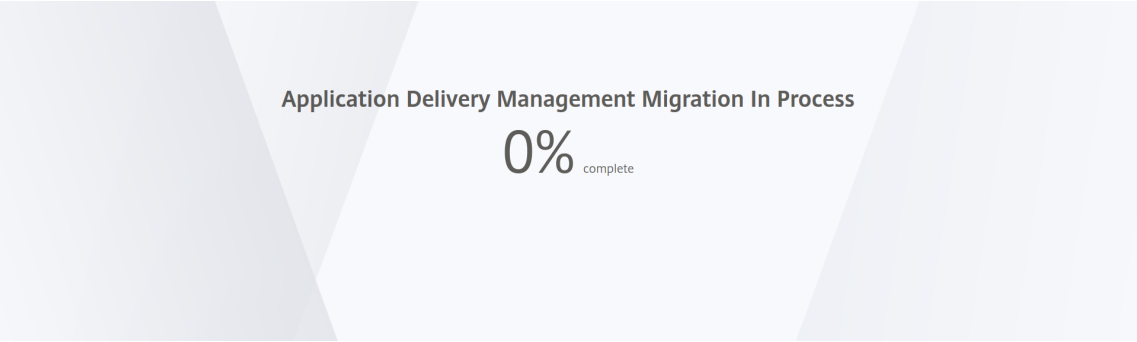
   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler ADM.



9. Access the NetScaler ADM GUI and wait until the reboot is complete.

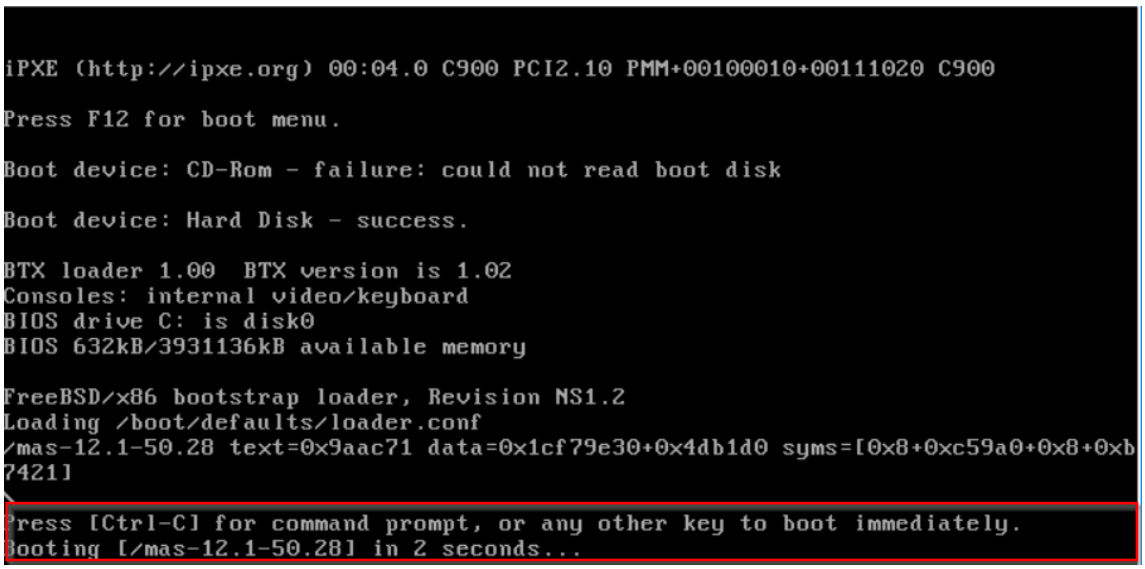


You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hypervisor.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx using vSphere:

1. Log on to ESX using vSphere.
2. Select the NetScaler ADM node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.



4. Run **boot -s** command in the OK prompt.

   The NetScaler ADM reboots.

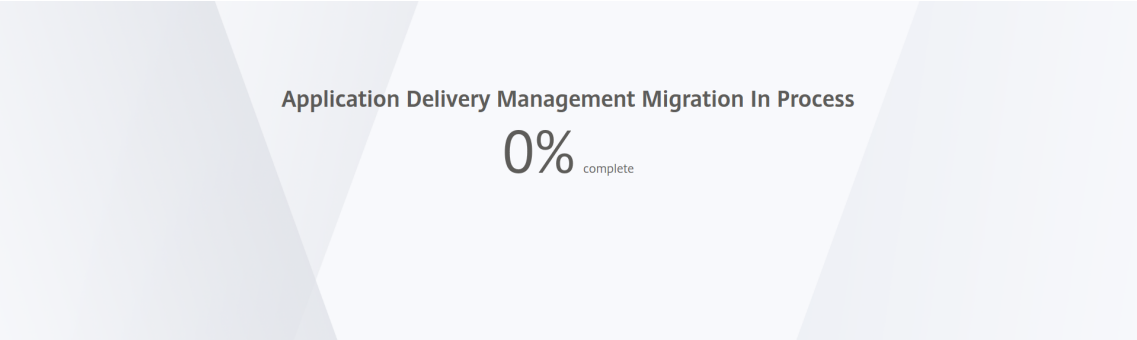
5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

   ```
   mount dev/da0s1a /flash
   ```

7. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.
8. Run the **Reboot** command to reboot NetScaler ADM.
9. Access the NetScaler ADM GUI and wait until the reboot is complete.

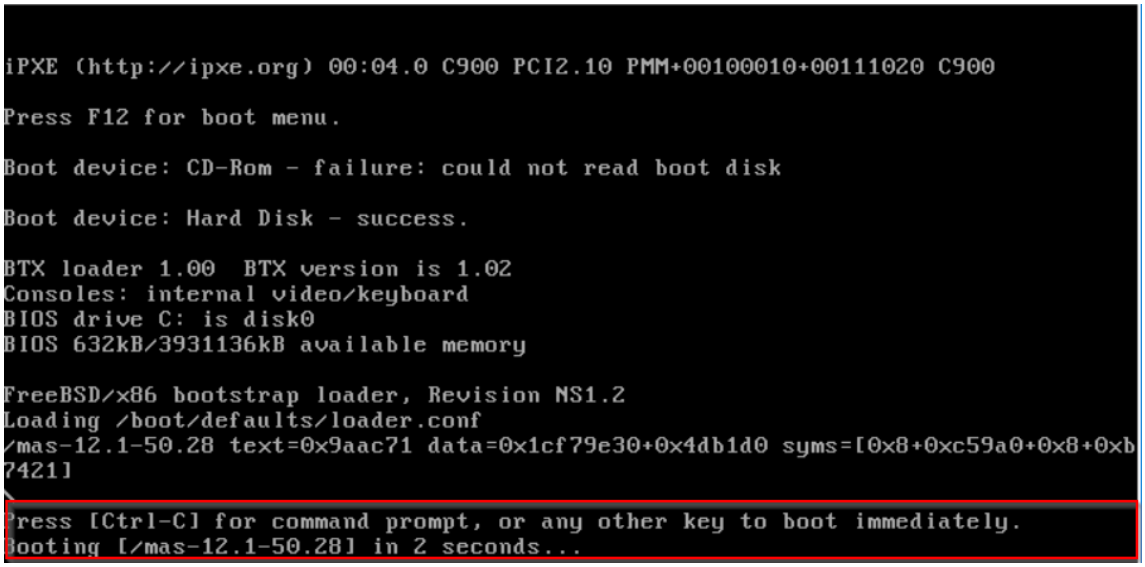


   You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from ESX server.

   > Note
   >
   > After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:
   >
   > - `rm /flash/mpsconfig/master.passwd`
   > - `rm –rf /etc/passwd`

Hyper-v using Hyper-v manager:

1. Log on to hyper-v using hyper-v manager.
2. Select the NetScaler ADM node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.



4. Run the **boot -s** command at the OK prompt.

   The NetScaler ADM reboots.

5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

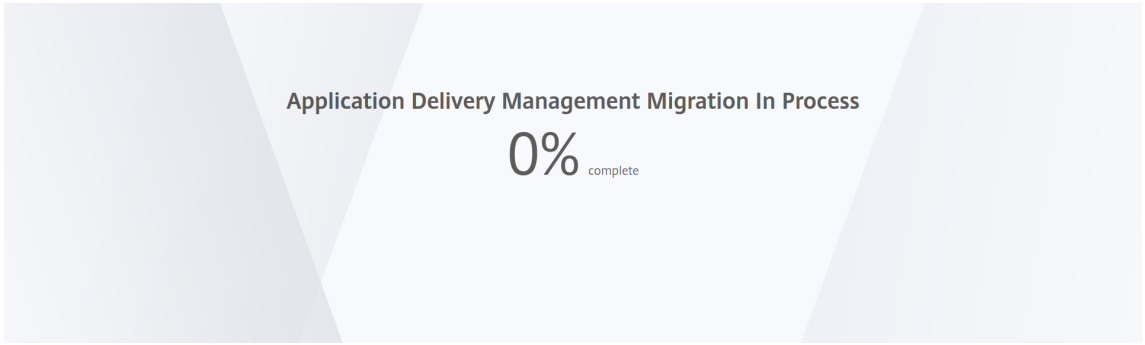
   ```
   mount dev/ad0s1a /flash
   ```

7. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler ADM.
9. Access the NetScaler ADM GUI and wait until the reboot is complete.



   You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hyper-v manager.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Linux KVM server (SSH to KVM Server by using any SSH client):

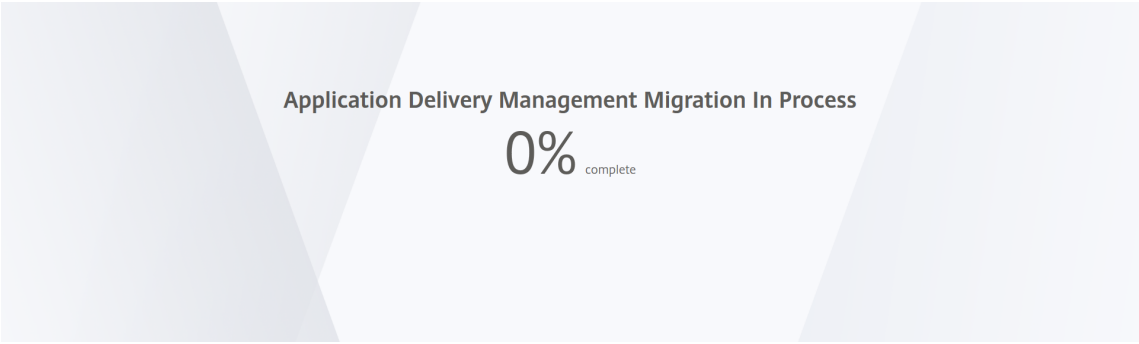
1. Log on to NetScaler ADM using an SSH client to the KVM server.
2. Reboot NetScaler ADM.
3. Press **CTL + C** to interrupt the boot sequence shortly after the **Loading /boot/defaults/loader.conf** message is displayed.
4. At the OK prompt, run the following command:

   ```
   set console='comconsole,vidconsole'
   ```
5. Run the **boot -s** command to reboot NetScaler ADM.
6. After the **Enter full path of shell or RETURN for /bin/sh:** message is displayed, press **Enter** to get the /u@ prompt.
7. Mount the flash partition using the following command:

   ```
   mount dev/vtbd0s1a /flash
   ```
8. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.
9. Run the **Reboot** command to reboot NetScaler ADM.
10. Access the NetScaler ADM GUI and wait until the reboot is complete.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from the SSH console.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Configure a secondary NIC to access NetScaler ADM

March 11, 2024

You can configure a second NIC for isolating management access to NetScaler ADM. Using this second NIC feature, depending upon your requirement, you can choose how you want to isolate the traffic that is received and sent through the NetScaler ADM.

Consider a scenario in which you want to isolate the traffic to:

- Have all communications between NetScaler ADM and its managed NetScaler instances in one network.
- Have management access to NetScaler ADM in another network.

In this scenario, as an administrator, you can:

- Configure one IP address for the traffic between NetScaler ADM and its managed NetScaler instances.
- Configure another IP address for managing the NetScaler ADM software to perform all administrative tasks in the software.

> **Note**
>
> If NetScaler ADM is configured as an HA pair, the management IP address configured on the second NIC is associated with the primary node.

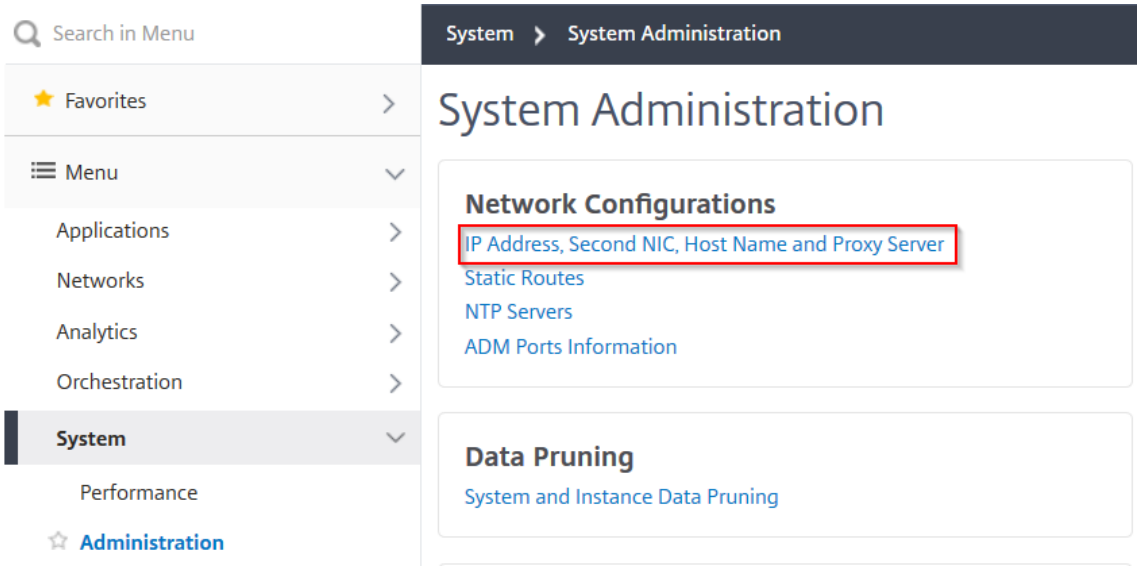
Prerequisites

- Ensure you have deployed and configured **NetScaler ADM 13.0 Build 47.x or later** on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).
- Ensure you have added the second NIC on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).

To assign an IP address to a NIC on a Citrix Hypervisor and create a secondary interface, see Assign an IP Address to a NIC.

Configure a second NIC in NetScaler ADM

1. Log on to ADM GUI.
2. Navigate to **Settings > Administration**.
3. Under **Network Configuration**, click **IP Address, Second NIC, Host Name and Proxy Server**.



   The **Network Configuration** page is displayed.

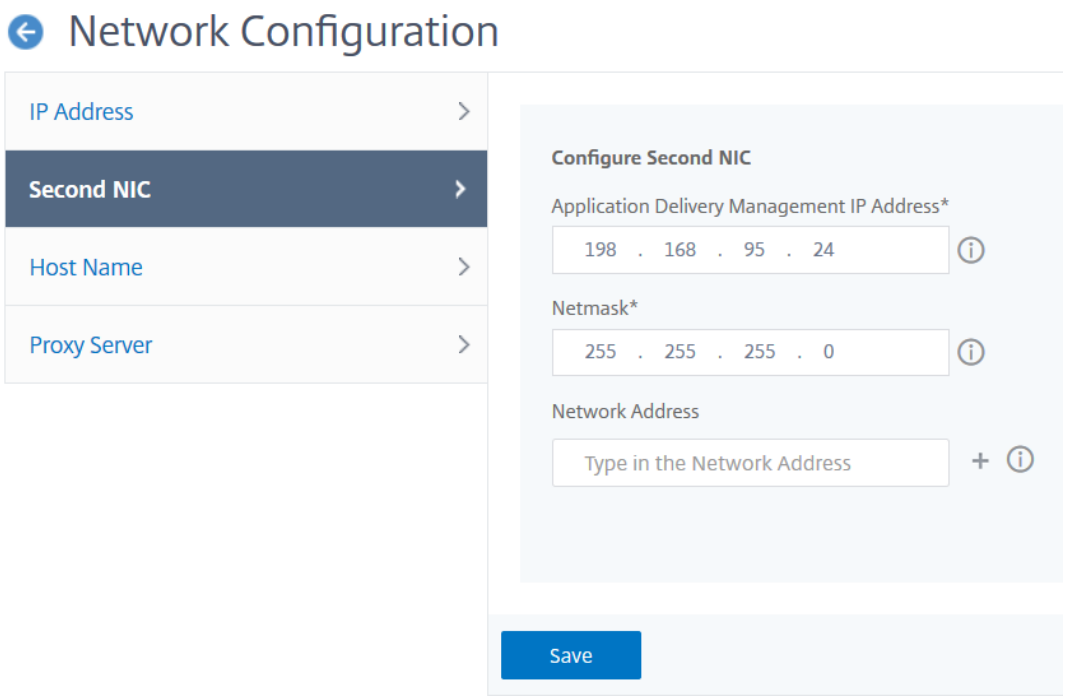
4. Click the Second NIC tab and configure the following parameters:

   a) **Application Delivery Management IP Address** –Enter a valid IP address to access NetScaler ADM. You can use this IP address to access NetScaler ADM, apart from the existing management IP address.

   b) **Netmask** –Enter the netmask address to specify the network host. The default address is 255.255.255.0.

   c) **Network Address** –Enter an IP address to add a route entry for NetScaler ADM. Click **+** to add more IP addresses. This field is optional.

   d) Click **Save**.



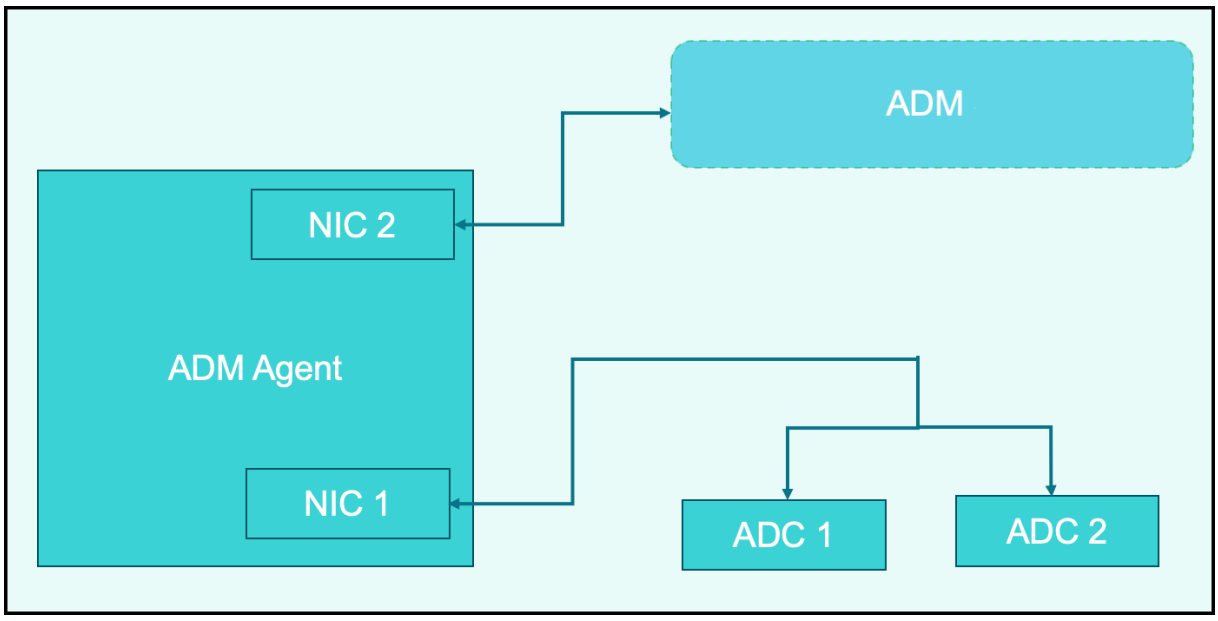
Configure a secondary NIC to access ADM agent

March 11, 2024

You can configure two NICs on an ADM agent. Using the Dual NIC architecture, ADM agent will be able to:

- Establish communication between ADM agent and ADC instances - You can use the first NIC to isolate the traffic that is received and sent through the NetScaler ADM and also to communicate between NetScaler ADM and its managed NetScaler instances in another network.
- Establish communication between ADM agent and NetScaler ADM - You can use the second NIC to manage the NetScaler ADM that is on a network and perform administrative tasks

> **Note**
>
> You cannot interchange the functionality and configuration of both the NICs.



In this scenario, as an administrator, you can:

- Configure IP address for the traffic between NetScaler ADM and its managed NetScaler instances.
- Configure IP address for managing the NetScaler ADM software to perform all administrative tasks in the software.

> **Note**
>
> It is not mandatory to configure Dual NICs for an ADM agent. It is optional and is required only when traffic between ADM agent, NetScaler ADM and ADCs needs to be separated.

Modify the IPV4 NIC network addresses using CLI

1. Open an SSHconnection to the NetScaler agent console by using an SSH client, such as PuTTY.
2. Log in using the **nsrecover/nsroot** credentials and switch to the shell prompt.
3. Run the command **ifconfig**. You can see the details of the two NICs that you have configured -
    - NIC 1 –For communication between ADM Agent to ADC Communication
    - NIC 2 –For communication between ADM Agent to NetScaler ADM


```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Run the command **networkconfig**. A menu appears which allows you to set or modify the IPV4 network addresses.

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> **Note**
>
> Second NIC Network address can take multiple IP values.

5. Select a menu item to modify. Save and quit the settings.

Configure syslog purging interval

March 11, 2024

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the Citrix Application Delivery Controller (ADC) instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the NetScaler instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

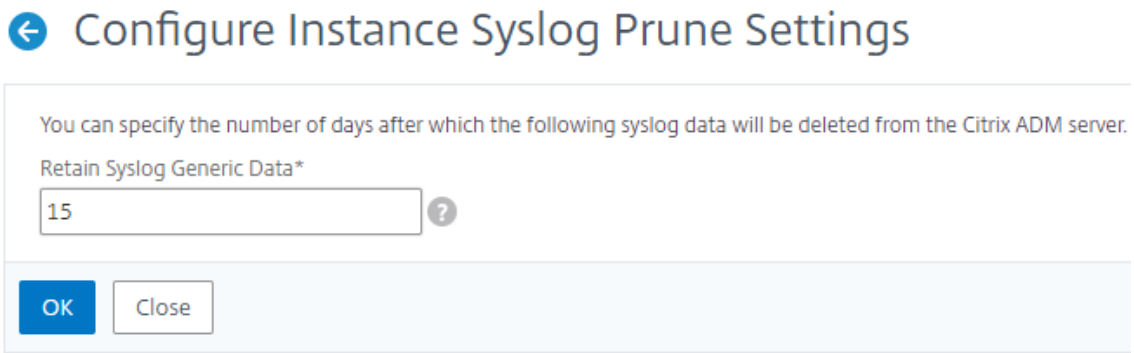
To limit the amount of syslog data stored in the database, you can specify the interval at which you want to prune syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler Application Delivery Management (ADM):

- Generic Syslog Data
- AppFirewall Data
- NetScaler Gateway Data

You can also configure the NetScaler Gateway prune interval by syslog type. This prune interval takes precedence over the rune interval configured to retain NetScaler Gateway data.

To configure syslog prune interval settings for NetScaler ADM:

1. Navigate to **Settings > Administration**. Under **Data Pruning**, click **System and Instance Data Pruning** and then click **Instance Syslog**.
2. In **Configure Instance Syslog Prune Settings** page, specify **Retain Syslog Generic Data(days)**. Type the number of days for which NetScaler ADM retains generic syslog messages.



Configure system prune and event prune settings

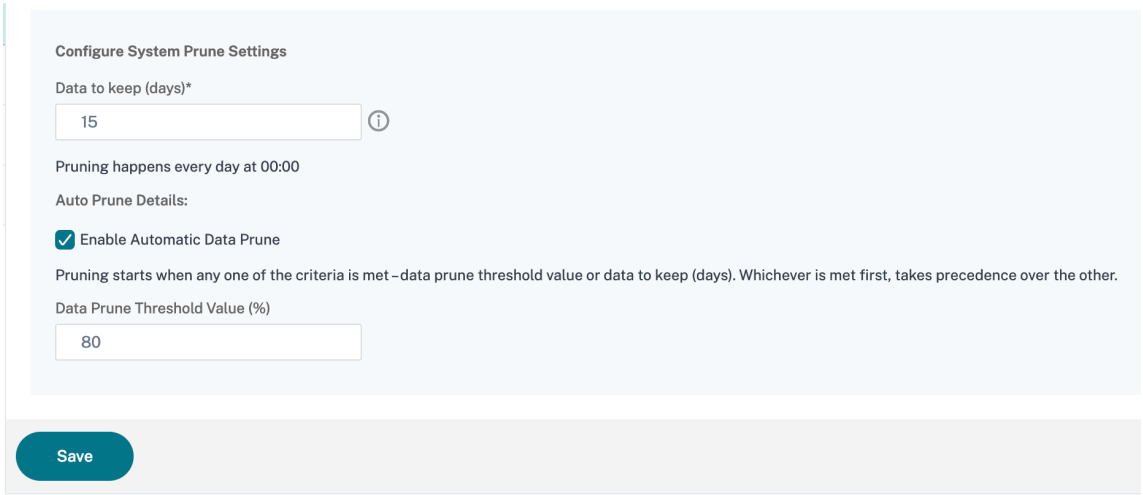
March 11, 2024

To limit the amount of reporting data being stored in your NetScaler Application Delivery Management (ADM) software database, you can prune it. You can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

> **Note**
>
> The value you specify can't be more than 30 days or be less than 15 days.

To configure system prune settings for performance reports:

1. Navigate to **Settings** > **Administration**. Under **Data Pruning**, click **System and Instance Data Pruning**.
2. In the **Configure System Prune Settings** page, specify the following:
   - Number of days to keep the data
   - Percentage of disk space (pruning threshold)
3. Click **OK**.



You can enable automatic pruning by selecting the **Enable Automatic Data Prune** check box. An alarm is triggered and an email is sent when disk usage breaches the configured **Data Prune Threshold Value**.

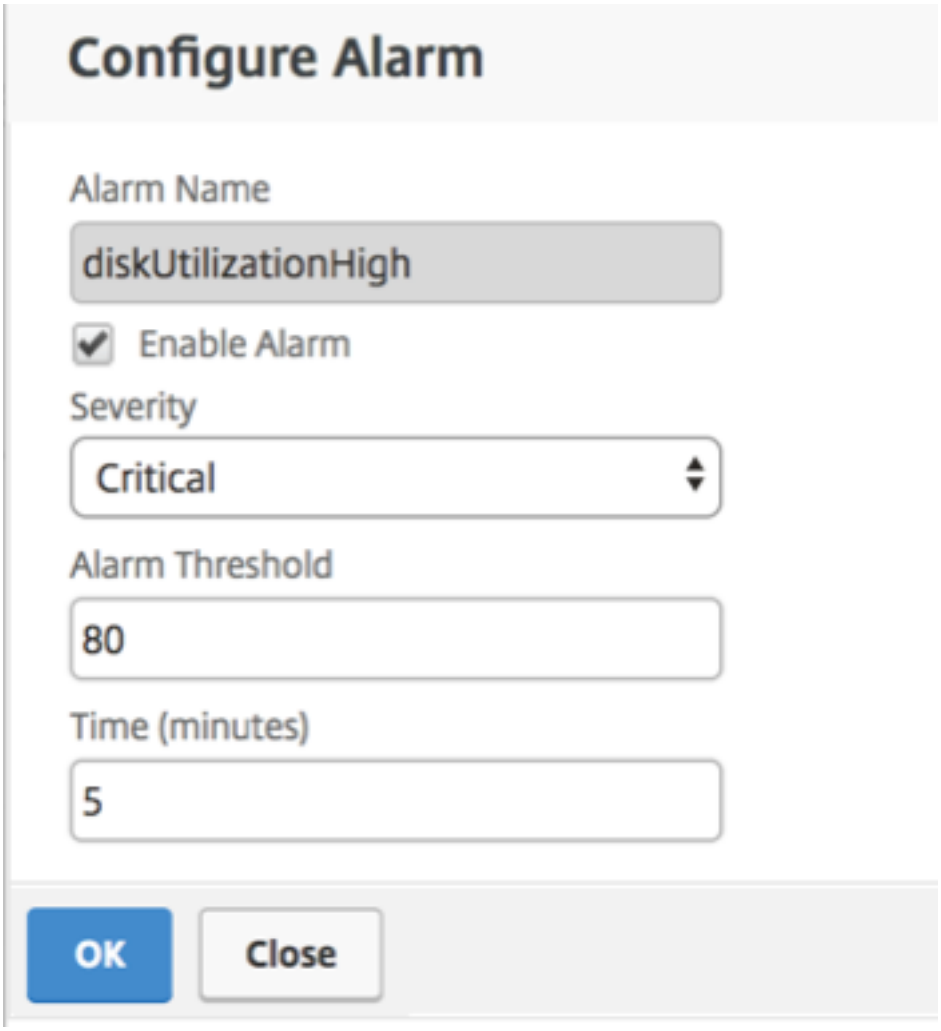
> **Note**
>
> Pruning starts when any one of the criteria is met –data prune threshold value or data to keep

> (days). Whichever is met first, takes precedence over the other.

To configure and enable alarm settings:

1. Navigate to **Settings** > **SNMP**. Click **Alarms** on the upper-right corner.
2. Select the alarm that you want to configure (for example, diskUtilizationHigh) and click **Edit**.
3. In the **Configure Alarm** page, specify the following:

- **Severity**—Select the severity level.
- **Alarm Threshold**—Type the value for which the event severity is calculated.
- **Time**—Type the time (in minutes) after which you want to trigger the alarm.



Configure Events Prune Settings by Using NetScaler ADM

To limit the amount of event messages data being stored in your NetScaler ADM database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit

logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

1. Navigate to **Settings > Administration > Data Pruning** and click **System and Instance Data Pruning**. Click **Instance Events**.
2. Enter the time interval, in days, for which you want to keep the data on the NetScaler ADM server and click **Save**.

Enable shell access for non-default users

March 11, 2024

You can enable shell access for non-default users in NetScaler Application Delivery Management (ADM). You can use this feature to enable and set up communication mode with instances.

> **Note**
>
> By default, shell access is disabled for non-default users.

To enable shell access for non-default users in NetScaler ADM:

1. In NetScaler ADM, navigate to **System** > **System Administration**.
2. In **System Settings**, click **Change System Settings**.
3. On the **Modify System Settings** page, configure the following parameters:
    - **Communication with instances** - Select the communication protocol.
    - **Secure Access** - Enable secure access for NetScaler ADM.
    - **Enable Session Timeout** - Specify the time period for which to retain an inactive session.
    - **Allow Basic Authentication** - Allow Management Service to accept credentials given using Basic Authentication Protocol.
    - **Enable nsrecover Login** - Enable `nsrecover` login on Management Service.
    - **Enable Certificate Download** - Enables you to download certificates from the added NetScaler.
    - **Enable Shell access for non-nsroot User** - Enable shell access for non-default users in NetScaler ADM.
    - **Prompt user credentials for instance login** - Allow users to enter their user credentials while logging on to instances from NetScaler ADM.
4. Click **OK**.

Recover inaccessible NetScaler ADM servers

March 11, 2024

NetScaler Application Delivery Management (ADM) now provides a database maintenance tool to perform cleanup of the system database. You can now launch the NetScaler ADM utility tool to connect to the file system, delete a few components, and make the database accessible. NetScaler ADM recovery script is a tool that helps to recover space in the file system by clearing old or unused database tables and files. The tool assists you to navigate through the database tables and files in successive steps and shows the current space occupied on the filesystem by respective items. Once you have selected the database tables and files to be deleted, the tool deletes those from the filesystem after confirmation.

How to Use NetScaler ADM Database Recovery Script for a NetScaler ADM Standalone Deployment

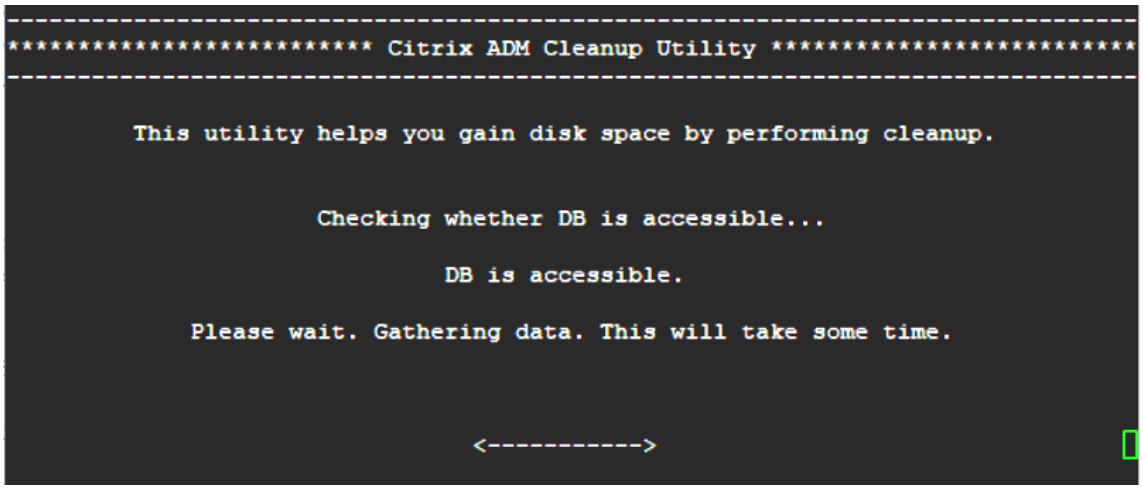
Use the following procedure in a single server NetScaler ADM deployment to connect to the file system, delete a few components, and make the database accessible, and then perform the recovery operations.

1. Using an SSH client or your hypervisor's console, logon to NetScaler ADM and type the following command:

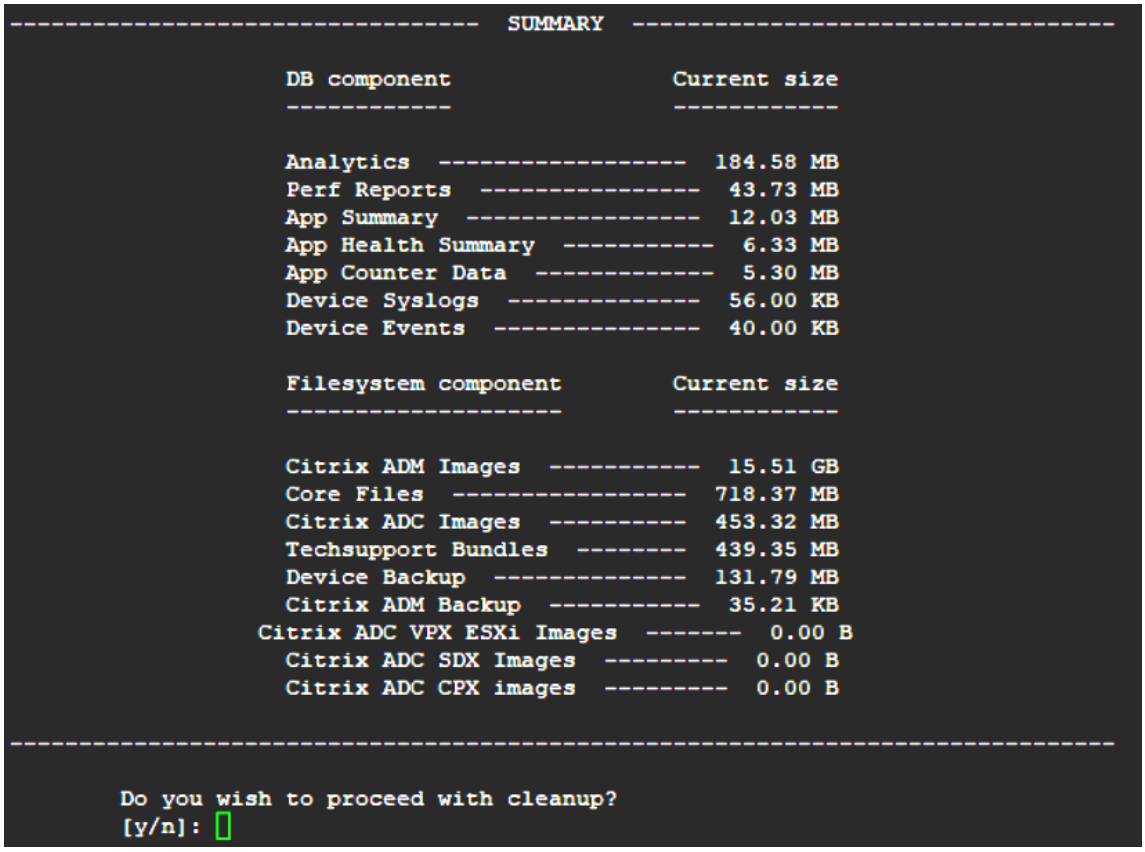
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. When the screen displays a caution message for stopping a few NetScaler ADM processes, type "y"and press the **Enter** key.

   The following screen appears while the system determines which components of the database you can delete without affecting the system's core files.



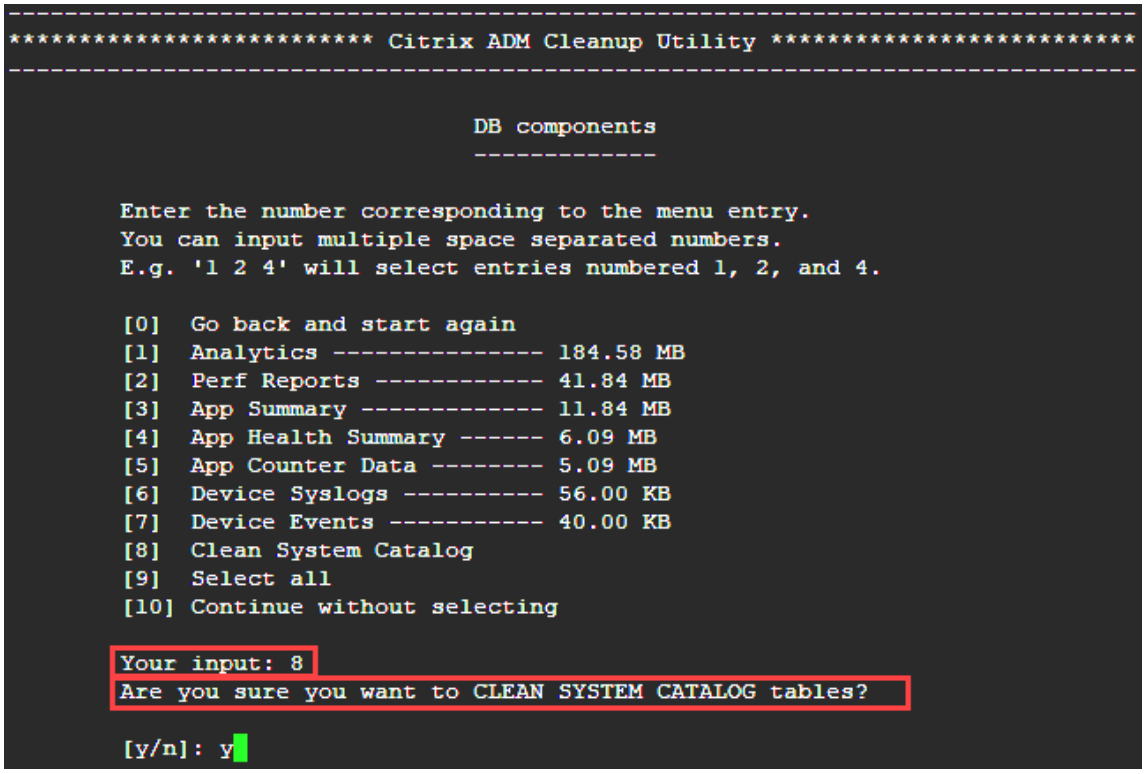
3. The screen displays the list of files in the database. Type “y”and press the Enter key to begin the cleanup process.



4. You can select the specific database component that needs to be cleaned and type the corresponding number. Press the **Enter** key.

   For example, to perform System Catalog cleanup, select option 8 in the **DB component** selection menu and type “y”and press the **Enter** key to continue with the system catalog clean up.

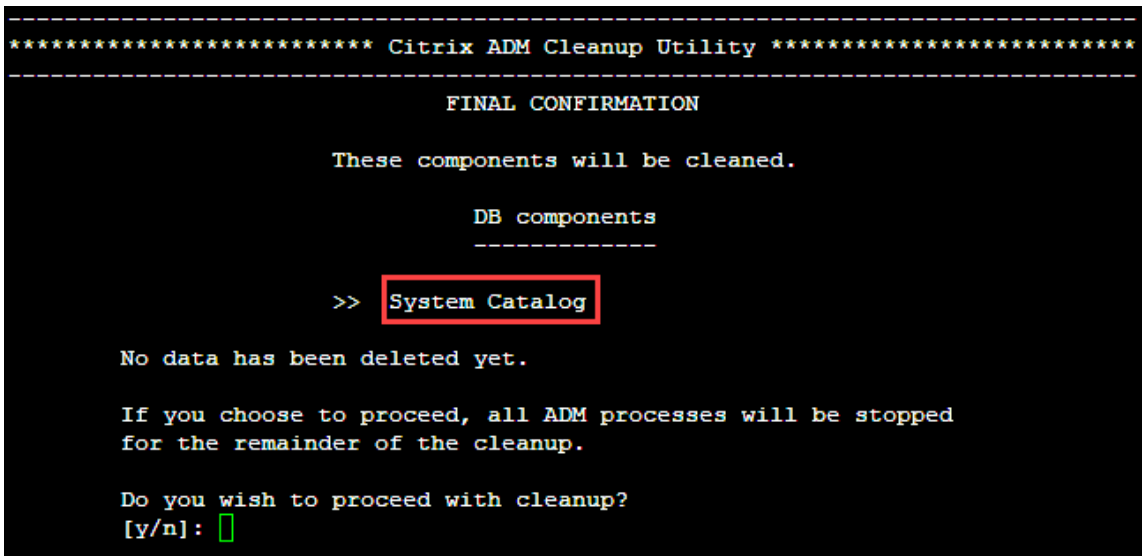
   > **Note**
   >
   > NetScaler ADM includes user tables known as system catalog. The system catalog is a location in the NetScaler ADM database where a relational database management system stores schema metadata, such as information about tables and columns and internal records. The tables in the system catalog are like regular tables that can accumulate inflated and dead rows over time and therefore, need periodic cleanup for optimal performance. It is a good practice to regularly maintain these tables. The activity not only frees up disk space but also improves the overall performance of the database and therefore of the NetScaler ADM.



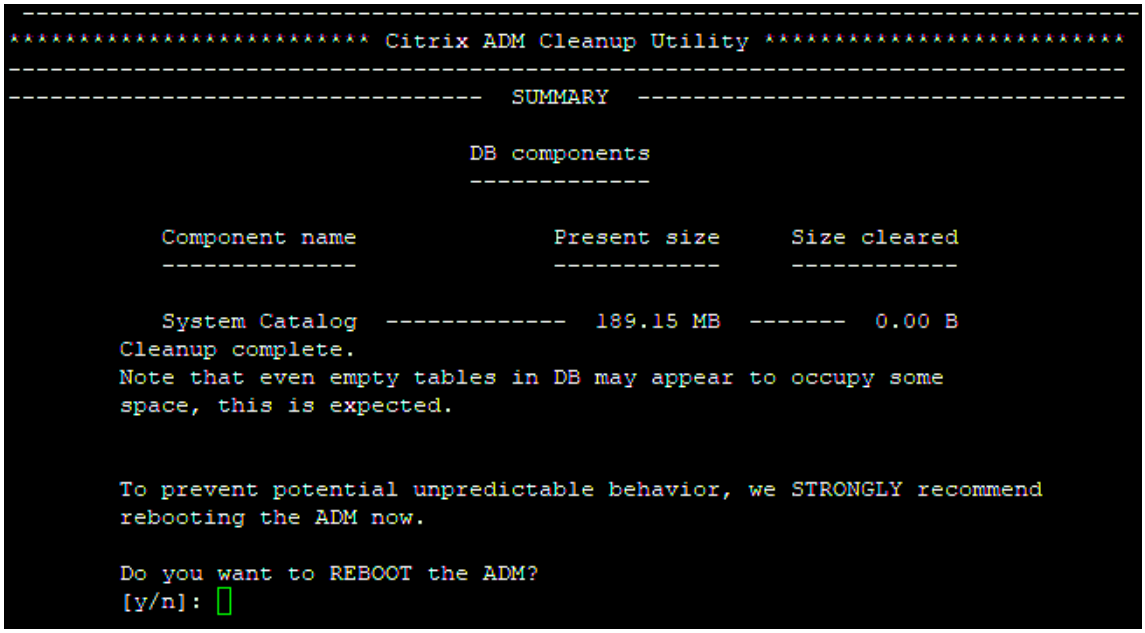
The cleanup utility gives you an option to clean database components and file components. You can select any file component by typing a number between “1”and “9,”or type “11”and press the Enter key to clean the database component.

> **Note**
>
> The number “11”indicates that you have not selected any file component to be cleaned and you are going ahead with cleaning up the earlier database component that you had earlier selected. In this example, it is “system catalog.”

5. Type “y”and press the **Enter** key again in the final confirmation screen.



The System Catalog is cleaned up, which may take time depending on the size of the table in the System Catalog. After the process is complete, a summary screen is shown.



6. Type “y”and press the **Enter** key to restart NetScaler ADM.

   Ensure you restart NetScaler ADM after system clean up. Wait for about 30 minutes for internal database operations to complete after NetScaler ADM has restarted. You should then be able to connect to NetScaler ADM database. If not, run the recovery script again to free up more space. When NetScaler ADM is up and running, it should work as expected.

   > **Note**
   >
   > The current size of the system catalog table is never equal to Zero after clean up. This is because only empty rows are removed from the table and the table might have some valid entries even after they are cleaned up.

How to use NetScaler ADM database recovery script for a NetScaler ADM high availability deployment

The database system for NetScaler ADM servers in a high availability deployment is in continuous synchronization mode. While using the new database recovery tool, you do not need to replicate the procedure on both the NetScaler ADM servers.

1. Using an SSH client or hypervisor’s console, log on to the primary node.
2. Run the following command:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Follow the procedure from step 2 available for NetScaler ADM Standalone Deployment Recovery Script

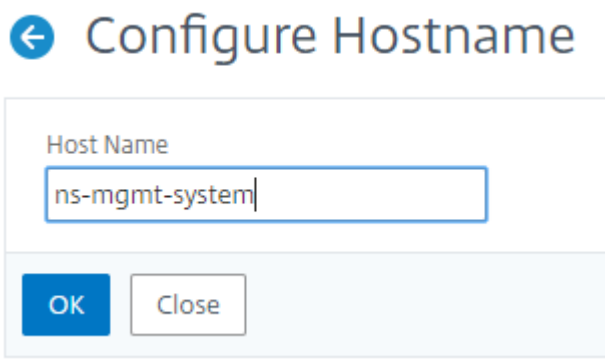
Assign a host name to a NetScaler ADM server

March 11, 2024

To identify a NetScaler Application Delivery Management (ADM) server, you can assign the server a host name. The host name is displayed on the Universal license for NetScaler ADM.

To assign a host name to a NetScaler ADM server:

1. In NetScaler ADM, navigate to **System** > **System Administration**.
2. Under **System Settings**, click **Change Hostname**.
3. On the **Configure Hostname** page, enter a host name and click **OK**.



> **Note**
>
> You can also use the `networkconfig` command in your hypervisor and change the host name.

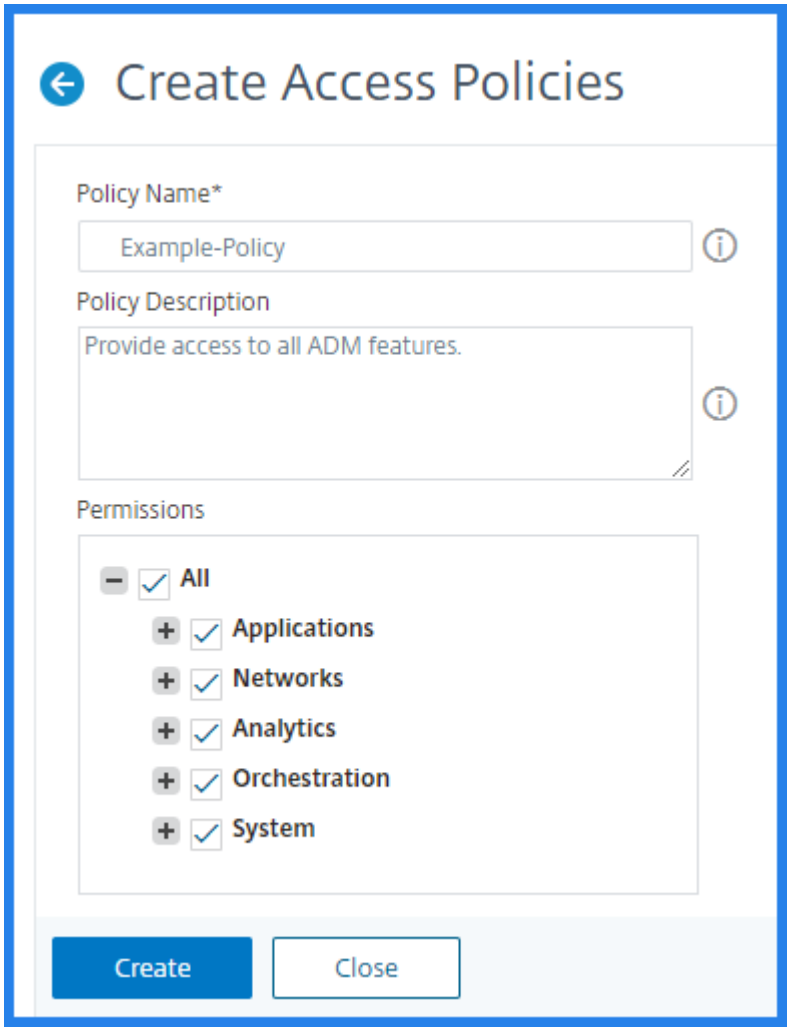
Back up and restore your NetScaler ADM server

March 11, 2024

You can take periodic backups of your NetScaler ADM server. You can back up and restore the configuration files, instance details, system data, and so on.

> **Important**
>
> Citrix recommends you to restore the ADM server using a backup of the same version. For example, if the ADM version is 13.0, use the 13.0 ADM backup to restore the server.
>
> User access to backup and restore the ADM server is limited. The **Settings > Backup Files** page

appears only to the users who have access to all ADM features. A user can access this page only if their access policy has all permissions. Typically, superusers have the access to all ADM features.



For more information, see Configure access policies.

Before you upgrade, back up the ADM server configuration files for precautionary reasons.

The backup includes the following components:

- NetScaler ADM Configuration Files:
  - SNMP
  - Syslog server configuration files
  - NTP files
  - SSL certificates
  - Control Center files

- Backups of NetScaler instances that the NetScaler ADM server manages.
- Configuration audit templates.
- System data stored on the database:
  - List of tenants and users created.
  - External authentication server configuration (LDAP, RADIUS, and others).
  - Configuration jobs and job templates created.
- Infrastructure and application data stored on the database:
  - Data from added and managed NetScaler instances.
  - Instance profile details, version details, instance group details, and so on.
  - A static application (group of virtual servers) created by the administrator.
- SNMP settings.

> **Note**
>
> Analytics data, events, ADM licenses, and syslog messages are excluded from the backup.

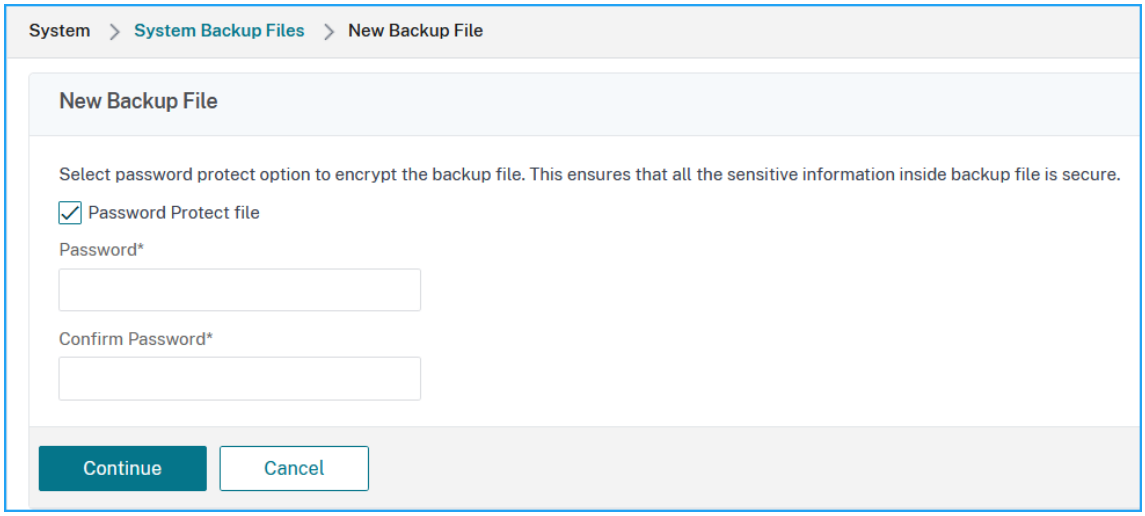
Back up the NetScaler ADM configuration

By default, the NetScaler ADM server backs up the configuration every 24 hours (at 00.30 hours). You can also schedule and select the time for the backup. Further, you can move a copy of the backed-up file to another system.

The backup is stored as a compressed TAR file that can also be encrypted. By default, three backup files are retained in the server. To avoid any low disk space issues, you can store a maximum of 10 backup files on your NetScaler ADM server. However, Citrix recommends that you store some copies of your backup files on the server or transfer the files to another system as a precautionary measure.

To backup a NetScaler ADM configuration:

1. Navigate to **Settings > Backup Files**, and then click **Back Up**.
2. To encrypt the backup file, select the **Password Protect file** check box, and then provide a password to encrypt the file.

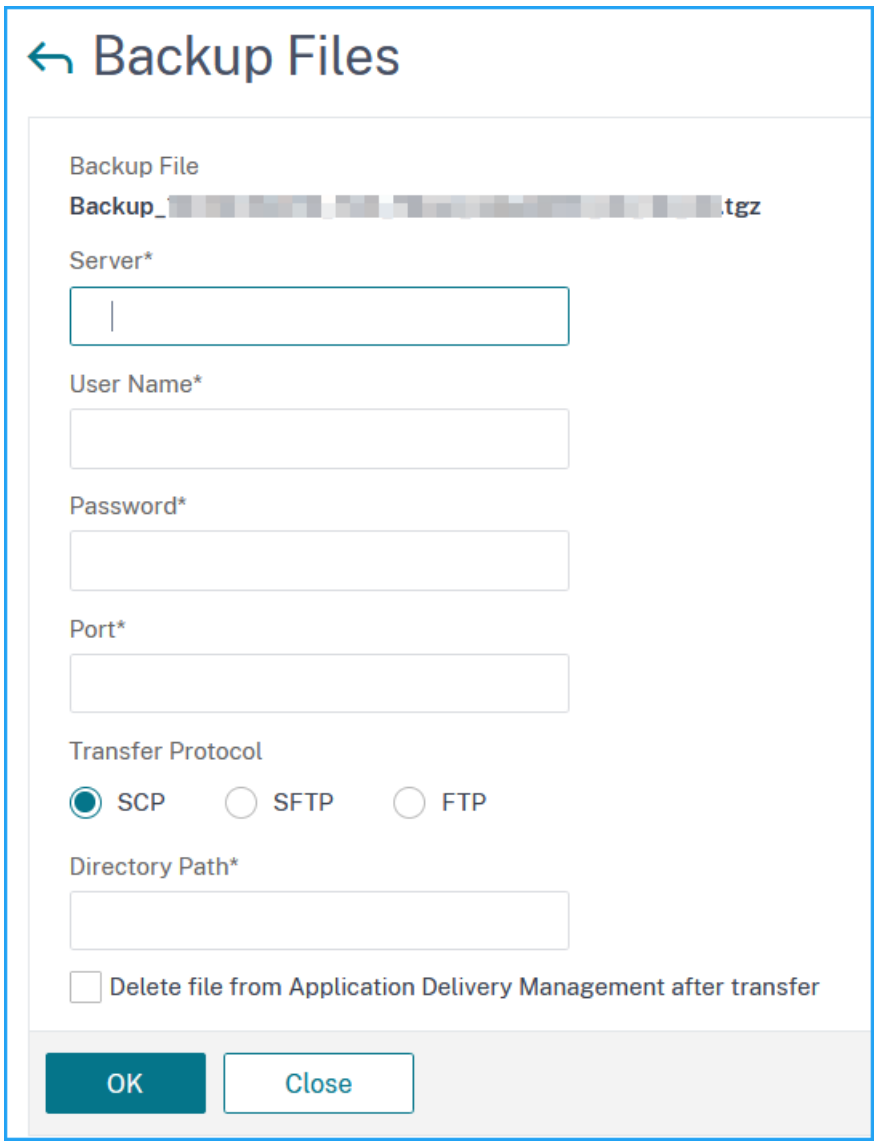


Transfer a NetScaler ADM backup file to an external system

You can transfer a copy of the backup file to another system as a precautionary measure. When you want to restore the configuration, first upload the file to the NetScaler ADM server and then perform the restore operation.

To transfer a NetScaler ADM backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to move to another system, and then click **Transfer**.
3. On the **Backup Files** page, specify the following parameters:
    - **Server** - IP address of the system where you want to transfer the backed-up file.
    - **User Name and Password** - User credentials of the new system where the backed-up files are being copied.
    - **Port** - Port number of the system the files are being transferred to.
    - **Transfer Protocol** - Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the backed-up file.
    - **Directory Path** - The location where the backed-up file is being transferred to on the new system.
4. You can delete the backup file from NetScaler ADM after transfer by selecting the **Delete file from Application Delivery Management after transfer** check box.
5. Click **OK** to make the transfer.



Note

To save a copy of the backup file in your local system, navigate to **Settings > Backup Files**, select the file you want to copy, and then click **Download**.

Restore the NetScaler ADM configuration from a backup file

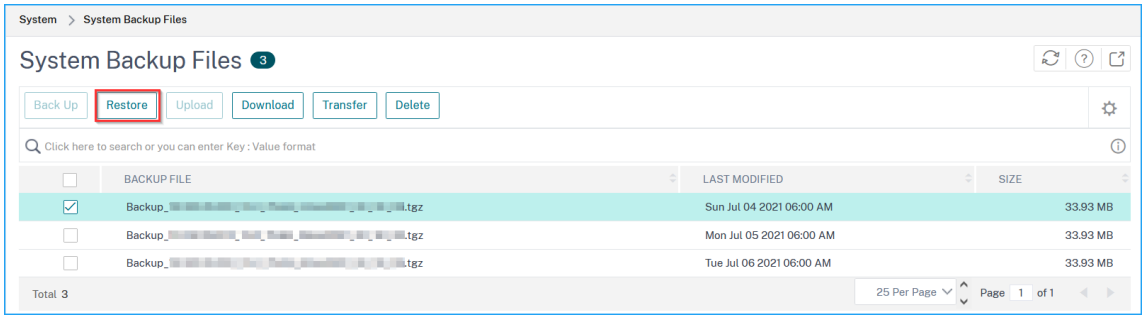
When you restore the NetScaler ADM configuration from a previously backed up file, the restore operation untars the backup file and then restores the configuration. The restore operation deletes the existing configuration and replaces it with the configuration in the backup file.

Note

The restore operation fails if the backup file is renamed or if the backup file contents are modified.

To restore a NetScaler ADM configuration from a backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to restore, and then click **Restore**.



3. On the confirmation dialog box, click **Yes**.

> **Note**
>
> To restore the configuration from a backup file stored in an external system, upload the backup file to the ADM server before performing the restore operation. To upload the file, navigate to **Settings > Backup Files**, and then click **Upload**.

VM snapshots of NetScaler ADM in high availability deployment

March 11, 2024

You can take snapshots of NetScaler ADM servers in the HA deployment before starting your upgrade. Snapshots capture the entire state of the virtual machine at the time that you take them.

Take a snapshot of NetScaler ADM servers

Use the following sequence to take snapshots of the NetScaler ADM servers:

1. NetScaler ADM secondary server
2. NetScaler ADM primary server

To take a snapshot of NetScaler ADM servers:

1. On your hypervisor, select the NetScaler ADM secondary server from the list of virtual machines.
2. Take a VM snapshot.
3. Give the snapshot a meaningful name and enter a description, if needed.

   The snapshot is stored in the default VM directory.

4. Repeat the same steps for the primary server.

> **Note:**
>
> You don't have to power off the VM while taking a snapshot.

Restore a snapshot of NetScaler ADM servers

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot.

Use the following sequence to restore snapshots of the NetScaler ADM servers:

1. NetScaler ADM primary server
2. NetScaler ADM secondary server

To restore the snapshot of NetScaler ADM servers:

1. On your hypervisor, select the NetScaler ADM primary server from the list of virtual machines.
2. Right-click the VM and revert the snapshot.

   The virtual machine is reverted to the most recent snapshot.
3. Repeat the same steps for the NetScaler ADM secondary server.

View auditing information

March 12, 2024

Audit logs have records with certain information for a specific duration such as user details, operations, and actions performed. You can view syslog messages for the following example scenarios:

- If your NetScaler ADM is a HA pair and if there is any latency issue in the database replication between the primary and secondary nodes, you can view details as an event.
- If there are any invalid login attempts (user name or password error) or successful logins, you can view details as an event.

As an administrator, you can use these logs for maintaining security and for recovering lost transactions.

To configure a syslog server on NetScaler ADM:

1. Navigate to **Settings > ADM Audit log messages > Syslog Servers**.

2. In the **Syslog Server** page, click **Add**.
3. On the **Create Syslog Server** page, enter the following values:
    - **Name** - Name for the syslog server.
    - **IP Address** - IP address of the syslog server.
    - **Port** - Syslog server port.
4. Choose the log levels (All, None, or Custom).
5. Click **Create**.

To configure the syslog date and time format on NetScaler ADM:

1. Navigate to **Settings > ADM Audit log messages > Syslog Servers**.
2. In the **Syslog Server** page, select a syslog server, and then, click **Syslog Parameters**.
3. On the **Configure Syslog Parameters** page, specify the date and time format.
4. Click **OK**.

To view syslog messages on NetScaler ADM:

Navigate to **Settings > ADM Audit log messages**.

You can also apply filters from the following filters and view the system log messages:

- Event
- Message
- Module
- Severity
- Source

For more information, see Syslog message references.

Configure SSL settings

March 11, 2024

SSL (Secure Socket layer) and TLS (Transport Layer Security) are commonly used security networking protocols that provide encrypted communication between users and servers. You can configure SSL settings on NetScaler Application Delivery Management (ADM) and specify the type of clients that connect to the system.

To configure SSL settings for NetScaler ADM:

1. Navigate to **System** > **System Administration**. Under **System Settings**, click **Configure SSL Settings**.
2. On the **SSL Settings** page, review the current protocol settings and the cipher suites applied to the system.
3. To modify the protocol settings, navigate to **Edit Settings** > **Protocol Settings** and make the changes that you want.
4. To modify the applied cipher suites, navigate to **Edit Settings** > **Cipher Suites** and make the changes that you want.
5. Click **OK**, and then click **Close**.

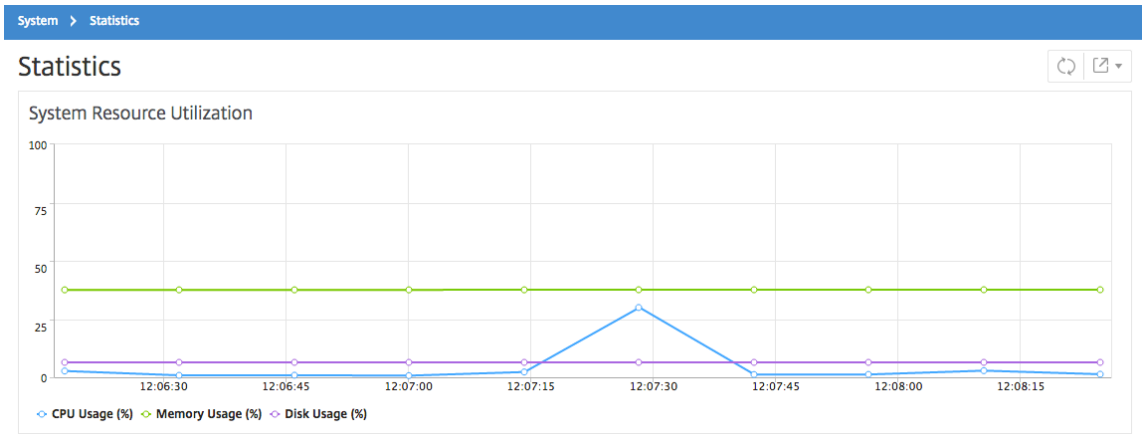
Monitor CPU, memory, and disk usage

January 5, 2024

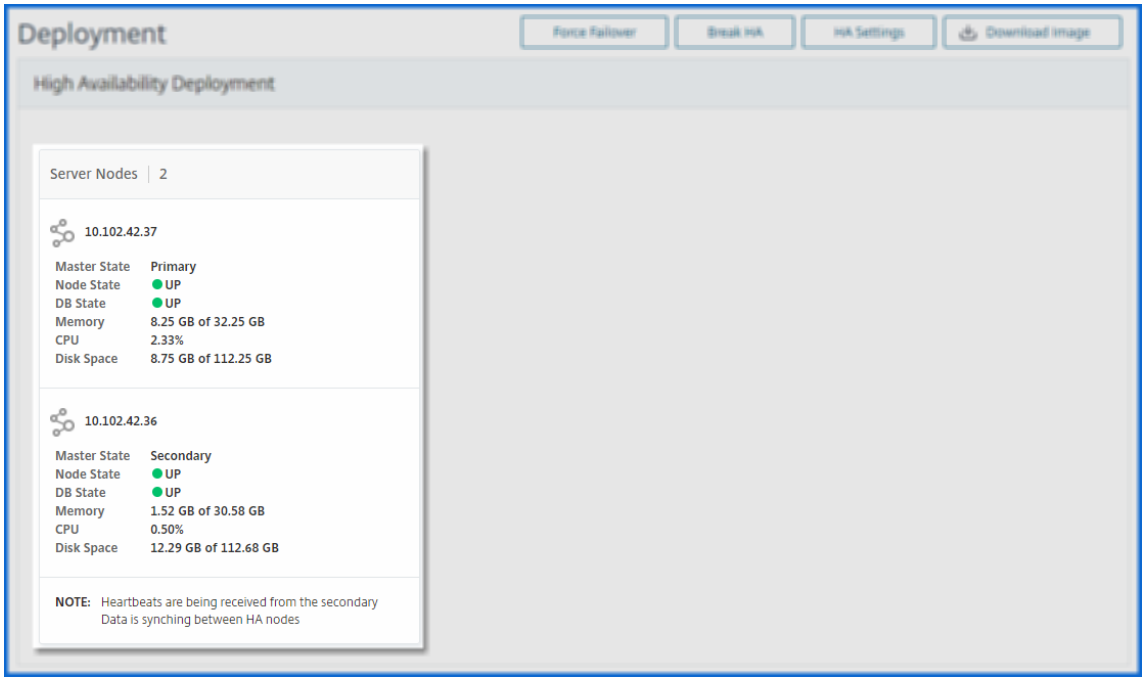
You can use the information maintained in logs and statistics. This information is also displayed in reports that helps you to configure and maintain NetScaler Application Delivery Management (ADM).

To monitor CPU, memory, and disk usage,

- **Standalone deployment.** Navigate to **System** > **Statistics**. You can view real-time CPU, memory, and disk utilization charts.



- **High availability deployment.** Navigate to **Settings > Deployment**. The statistics for memory, CPU, disk space, and managed instances are displayed numerically as shown in the following figure:



Configure notification settings

March 11, 2024

You can select a notification type to receive notifications for the following features:

- **Events** –List of events that are generated for NetScaler instances. For more information, see Add event rule actions.
- **Licenses** –List of licenses that are currently active, about to expire, and so on. For more information, see The NetScaler ADM license expiry.
- **SSL Certificates** –List of SSL certificates that are added to NetScaler instances. For more information, see The SSL certificate expiry

ADM supports the following notification types:

- Email
- SMS
- Slack
- PagerDuty
- ServiceNow

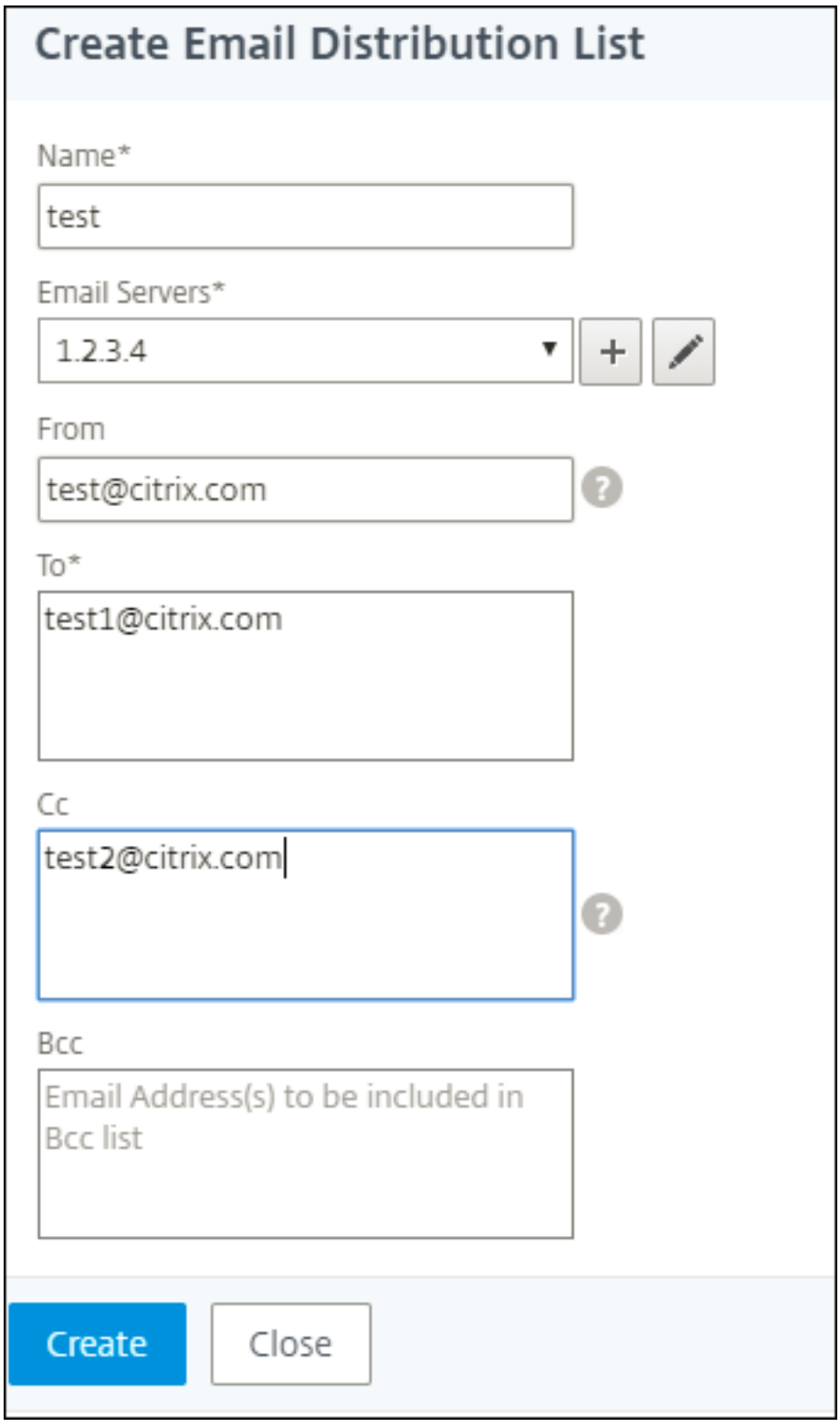
For each notification type, the ADM GUI displays the configured distribution list or profile. The ADM sends notifications to the selected distribution list or profile.

Create an email distribution list

To receive email notifications for ADM functions, you must add an email server and a distribution list.

Perform the following steps to create an email distribution list:

1. Navigate to **Settings > Notifications**.
2. In **Email**, click **Add**.
3. In **Create Email Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **Email Server** - Select the email server that sends email notification. If you want to add an email server, click **Add**.
    - **From** - Specify the email address from which ADM has to send messages.
    - **To** - Specify the email addresses to which ADM has to send messages.
    - **Cc** - Specify the email addresses to which ADM has to send message copies.
    - **Bcc** - Specify the email addresses to which ADM has to send message copies without displaying the addresses.



4. Click **Create**.

Repeat this procedure to create multiple email distribution lists. The **Email** tab displays all the email distribution lists present in ADM.

Create an SMS distribution list

To receive SMS notifications for ADM functions, you must add an SMS server and phone numbers.

Perform the following steps to configure SMS notification settings:

1. Navigate to **Settings > Notifications**.
2. In **SMS**, click **Add**.
3. In **Create SMS Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **SMS Server** - Select the SMS server that sends SMS notification.
    - **To** - Specify the phone number to which ADM has to send messages.
4. Click **Create**.

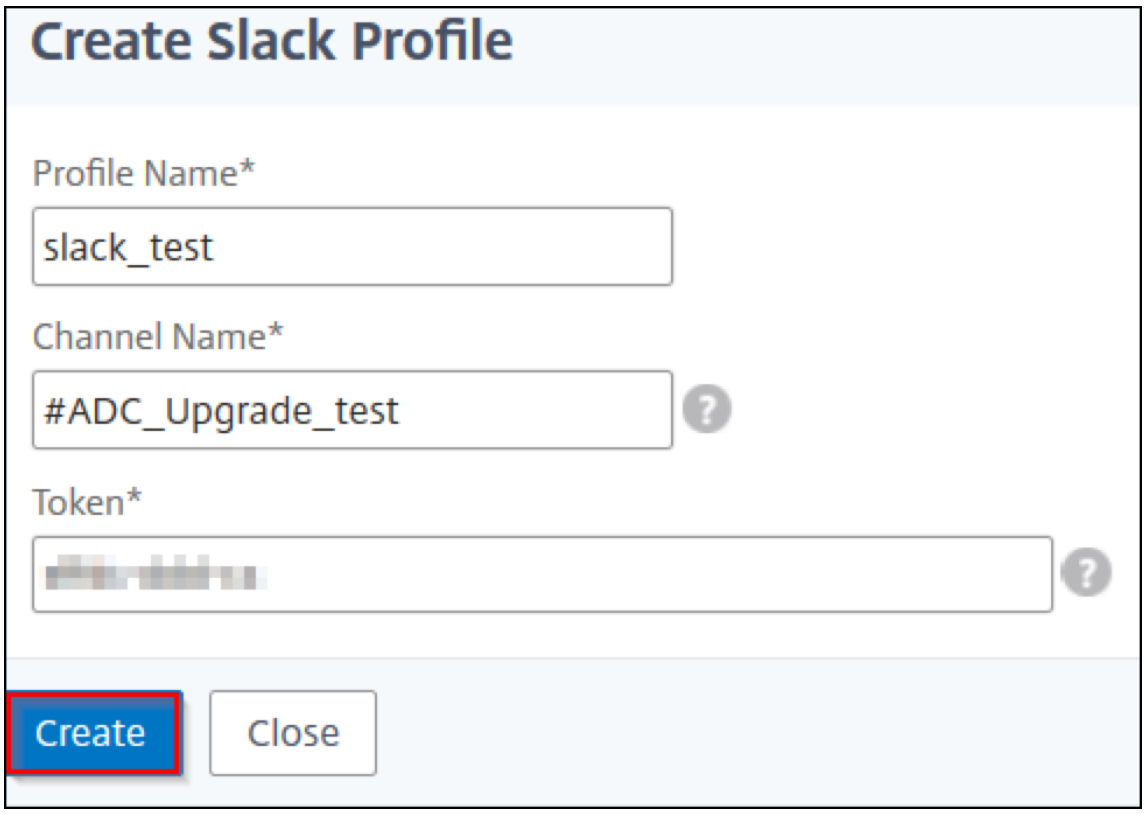
Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in ADM.

Create a Slack profile

To receive Slack notifications for ADM functions, you must create a slack profile.

Perform the following steps to create a Slack profile:

1. Navigate to **Settings > Notifications**.
2. In **Slack**, click **Add**.
3. In **Create Slack Profile**, specify the following details:
    - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
    - **Channel Name** - Specify the Slack channel name to which ADM has to send notifications.
    - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. And, all event notifications are sent to this URL are posted on the designated Slack channel. An example of webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in ADM.

Create a PagerDuty profile

You can add a PagerDuty profile to monitor the incident notifications based on the PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in NetScaler ADM, ensure you have completed the required configurations in PagerDuty. To get started with PagerDuty, see PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. Navigate to **Settings > Notifications**.
2. In **PagerDuty**, click **Add**.
3. In **Create PagerDuty Profile**, specify the following details:
    - **Profile Name** - Specify a profile name of your choice.

- **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal.

4. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

Repeat this procedure to create multiple PagerDuty profiles. The **PagerDuty** tab displays all the PagerDuty profiles present in ADM.

View the ServiceNow profile

When you want to enable ServiceNow notifications for NetScaler events and ADM events, you must integrate NetScaler ADM with the ServiceNow using ITSM connector. For more information, see Integrate NetScaler ADM with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. Navigate to **Settings > Notifications**.
2. In **ServiceNow**, select the **Citrix_Workspace_SN** profile from the list.
3. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   If you want to view ServiceNow tickets in the NetScaler ADM GUI, select **ServiceNow Tickets**.

Generate a tech support file

March 11, 2024

Citrix recommends that you generate an archive of NetScaler Application Delivery Management (ADM) data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

> **Note**
>
> For NetScaler ADM servers in a high availability mode, you can generate a technical support file from either of the servers. Citrix advises you to not use the load balancing virtual server IP address to generate the technical support file.

To configure and send a technical support file from NetScaler ADM:

1. Navigate to **System** > **Diagnostics** > **Technical Support**, and then click **Generate Technical Support File**.

2. On the **Generate Support File** page, select the following options:

- **Collect Debug Logs** –Select this option to collect `afdecoder` logs.
- **Duration** –Enter the duration for which debug logs must be collected. You will only see this option, if you enable the **Collect Debug Logs** option.
- **Collect Data Distribution** –Select this option to collect distinct and diverse logs from the database.

```
1  The archive file is created as a TAR file.
2
3  For example, the archive file that is created might be named as
      follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
      tar.gz
```

1. You can send the technical support files to the support team in two ways:

   a) You can download the file from the ADM GUI to your local storage and then use a web browser to upload to Citrix Insight Services(CIS).

   b) You can also upload the technical support files to the CIS website by running a script on the ADM console.

      i. Using SSH, log on to the ADM console.

      ii. Switch to the Shell prompt and type:

      /mps/collector_upload.pl

The full command is given below with the attributes you need to provide:

```
1 /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
     proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
      <sr>] [-description <description>] [-debug] <file>
2 <!--NeedCopy-->
```

The advantage of running the Perl script is that you don't have to download the technical support file from ADM to your local system and then upload it to CIS. As an option, you can upload the file to CIS directly by using a proxy from the ADM console.

Ensure that you have an account on CIS. You can use your Citrix account credentials to upload files to CIS.

What if you don't have a proxy server? Or what if you are facing some issues with SSL forward proxies? (This can happen if the Perl script does not trust the proxy server's root certificate.)
You can still upload the file directly from the ADM shell to CIS.

> **Note**
>
> You can still download the file and email them to the Citrix technical support team in a situation where ADM fails to upload the file to CIS from the console. Or, you can download the file from ADM to your local storage and then use a web browser to upload to CIS.

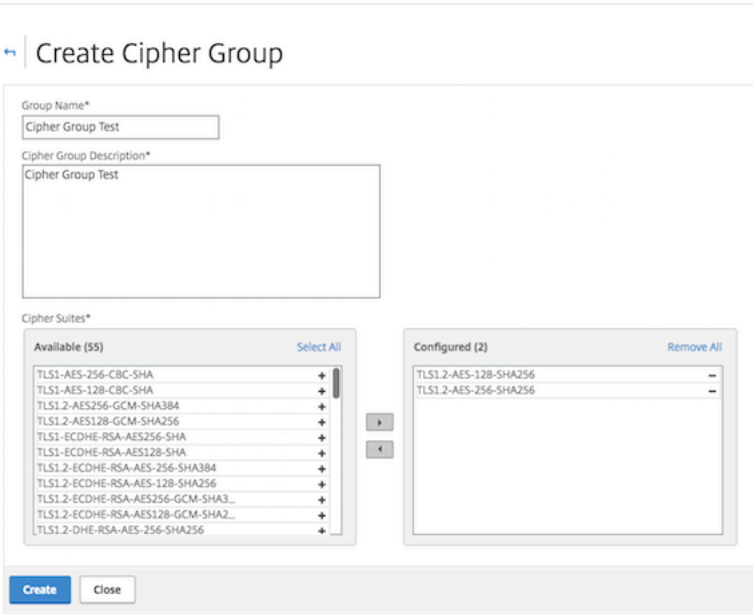
Configure a cipher group

March 11, 2024

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the Citrix Application Delivery Controller (ADC) instance. A cipher suite comprises a protocol, a key exchange (Kx) algorithm, an authentication (Au) algorithm, an encryption (Enc) algorithm, and a message authentication code (Mac) algorithm.

To add a cipher group on NetScaler ADM:

1. Navigate to **Settings > Administration**
2. Under **SSL Settings**, click **Cipher Groups**
3. Click **Add**
4. On the **Create Cipher Group** page, enter the following details:
   - **Group Name** - Name for the cipher group.
   - **Cipher Group Description** –Provide a description for your cipher group.
   - **Cipher Suites** –Click Add to select cipher suites from the Available list, and then move the selected (or all) cipher suites to the Configured list.
5. Click **Create**.



Create SNMP trap destination, manager community, and users

March 11, 2024

Whenever an abnormal condition occurs on the NetScaler ADM, an SNMP trap is generated. The traps are then sent to a remote device called a trap destination server or the *SNMP trap destination*. Here, NetScaler ADM is configured as the trap destination. You can query the SNMP agent for system-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

To create an SNMP trap destination on NetScaler ADM:

1. Navigate to **System** > **SNMP** > **Trap Destinations**.
2. Under **SNMP Traps**, click **Add** to create an SNMP trap, and then specify the following details:
   - **Version.** Select the SNMP version to use.
   - **Destination Server.** Name or IP address of the trap destination.
   - **Port.** Enter the trap destination's port. The port is set to 162 by default.
   - **Community.** Specify the community string to use when sending a trap to the trap listener.
3. Click **Create**.

> **Note**
>
> If you are creating an SNMP v3 trap destination, specify the SNMP user credentials to which you want to bind the trap. To add an SNMP user credential, click **Insert** and then add the user from the list of SNMP users available.

To create an SNMP manager community:

1. Navigate to **System** > **SNMP** > **Managers**.
2. Under **SNMP Manager**, click **Add** to create an SNMP manager community, and then specify the following details:
   - **SNMP Manager.** Enter the name or IP address of the SNMP manager.
   - **Community.** Specify the community string to use when sending traps to the trap listener.
3. Optionally, you can select the **Enable Management Network** check box to specify the **Netmask** which is the subnet mask of the SNMP manager network.
4. Click **Create**.

To create an SNMP user:

1. Navigate to **System** > **SNMP** > **Users**.
2. Under **SNMP User**, click **Add**.
3. Enter the user name and assign a security level to the user from the menu.
4. Based on the security level you've assigned to the user, provide extra authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.

Configure and view system alarms

March 11, 2024

You can enable and configure a set of Alarms to monitor the health of your NetScaler Application Delivery Management (ADM) servers. You must configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, **loginFailure**), a message is recorded in the

system and you can view the message as syslog message. You can further set notifications to receive an email or SMS corresponding to your alarm settings.

You can assign or modify the severity of an alarm. The severity levels that you can assign are Critical, Major, Minor, Warning, and Informational.

Consider a scenario where you want to monitor whenever there is a failed back up attempt. You can enable the backupFailed alarm and assign a severity, such as Major, to it. Whenever NetScaler ADM attempts to back up the system files and when the attempt fails, an alarm is triggered. You can view the message on the NetScaler ADM or get notifications through email or SMS.

To configure the alarm, you must select the backupFailed alarm and specify the severity level as Major. The alarm is enabled by default.

To configure and view a system alarm by using NetScaler ADM:

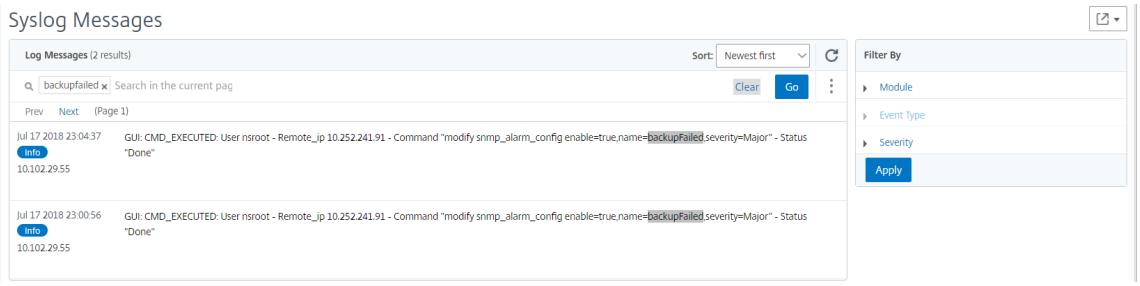
1. Navigate to **Settings > SNMP**. Click **Alarms** on the upper-right corner.

2. Select the alarm you want to configure (for example, backupFailed) and click **Edit** to modify its settings.
3. The alarm is enabled by default. Assign a severity level (example: Major), and then click **OK**.

> **Note**
>
> For a few alarms, you cannot set a threshold.
> When the alarm is triggered, you can view the generated event as a syslog message.

To view the event generated by the backupFailed alarm by using NetScaler ADM:

1. Navigate to **System** > **Auditing**.
2. In the **Auditing** page, under **Audit Messages**, select **Syslog Messages**.
3. In the search field, type in the name of the alarm.
   In this example, you can see that an event was generated for a failed back up attempt.



You can also set notifications to send you either an email or an SMS (Short Message Service) text when an alarm is triggered. For information about how to configure system notifications, see How to Configure System Notification Settings of NetScaler ADM.

Create SNMP managers and users for NetScaler agent

January 5, 2024

You can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

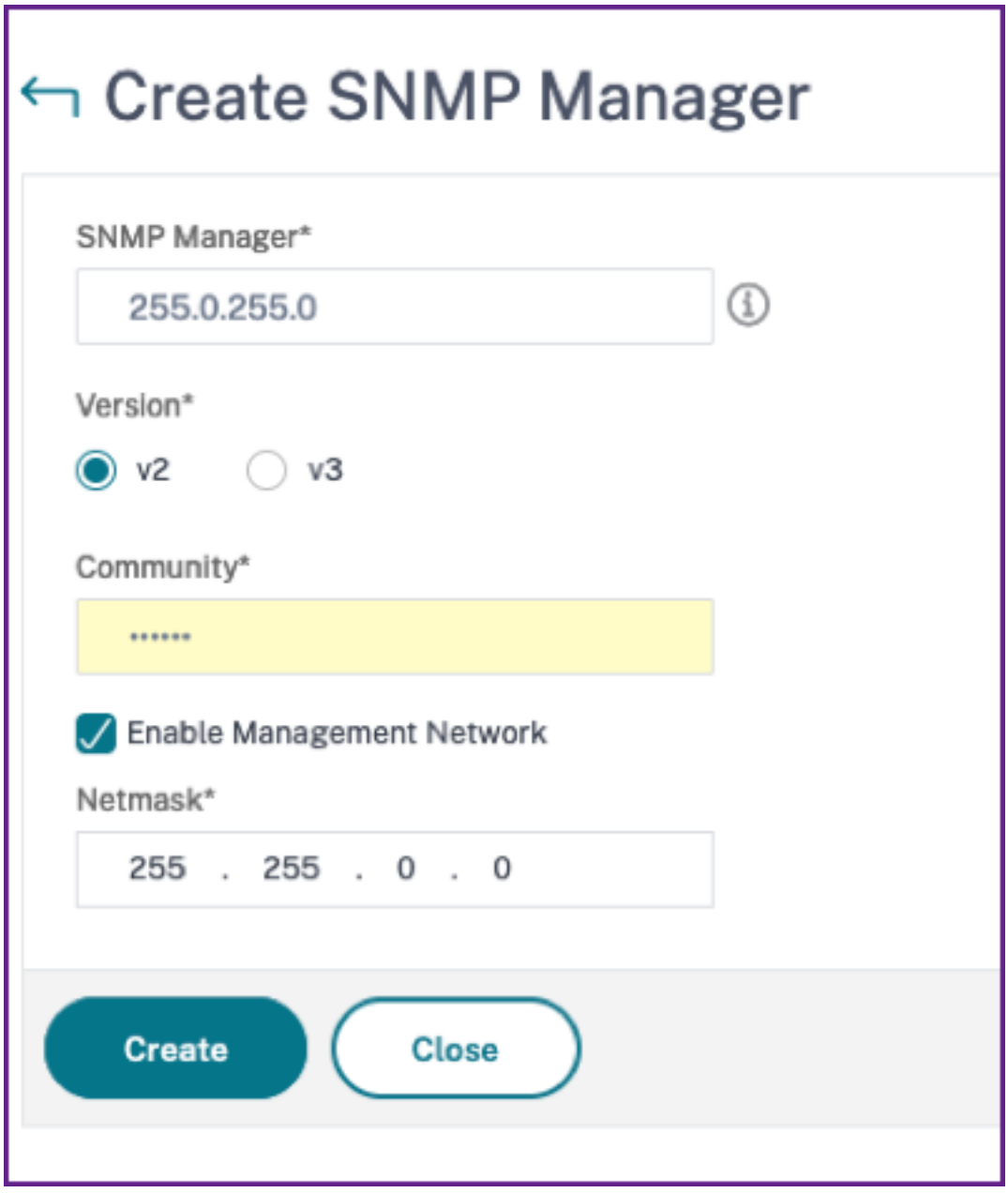
You can add an SNMP manager to query a NetScaler agent. The manager complies with SNMP V2 and V3. If you specify one or more SNMP managers, the NetScaler agent does not accept SNMP queries from any hosts except the specified SNMP managers.

Add an SNMP v2 manager

To add an SNMP v2 manager for the NetScaler agent:

1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
   - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
   - **Version**. Select v2.
   - **Community**. Enter a community name. An SNMP community configuration authenticates SNMP queries from SNMP managers.
   - **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.
   - **Netmask**: Enter the subnet mask associated with an IP address.

4. Click **Create**.



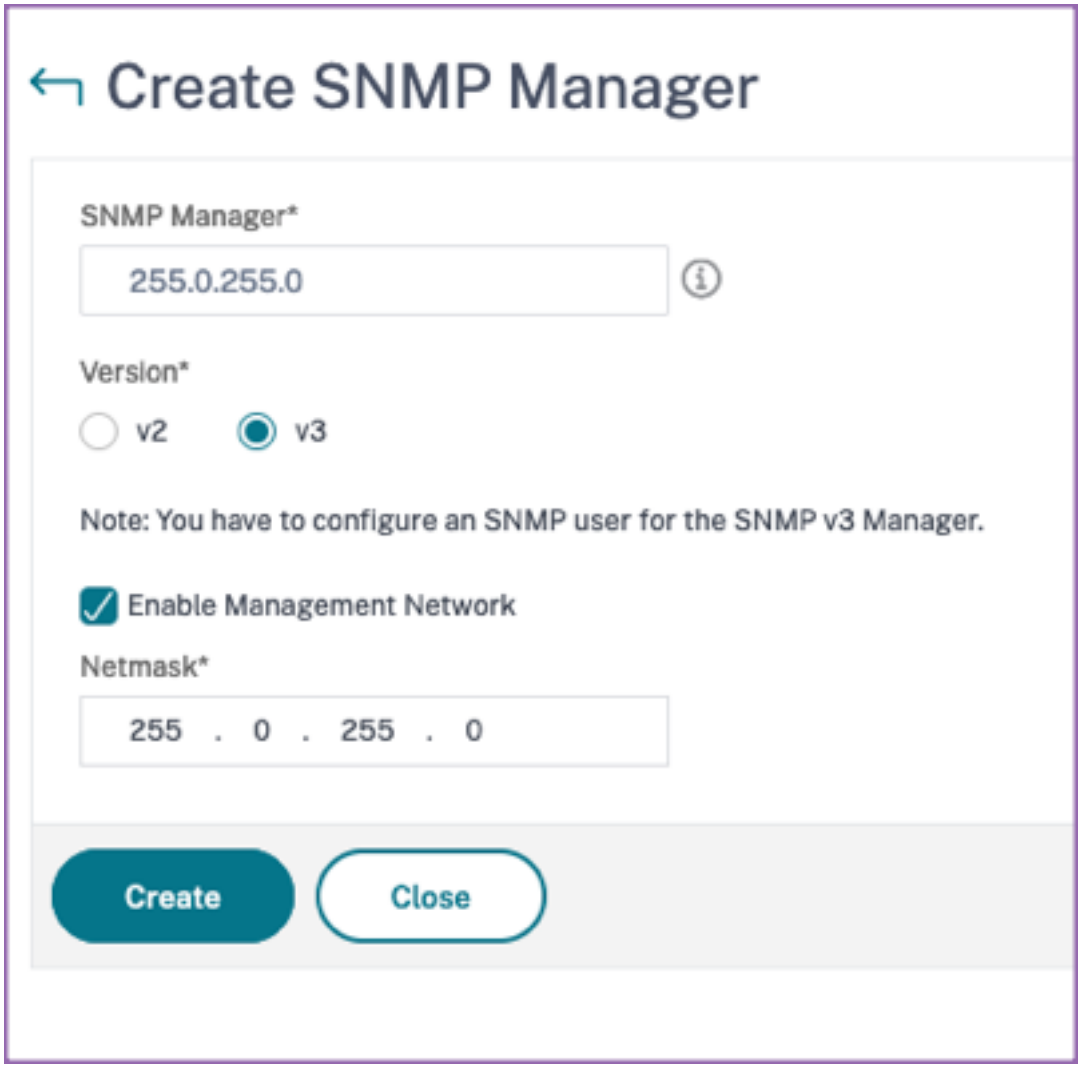
Add an SNMP v3 manager

To add an SNMP v3 Manager for the NetScaler agent:

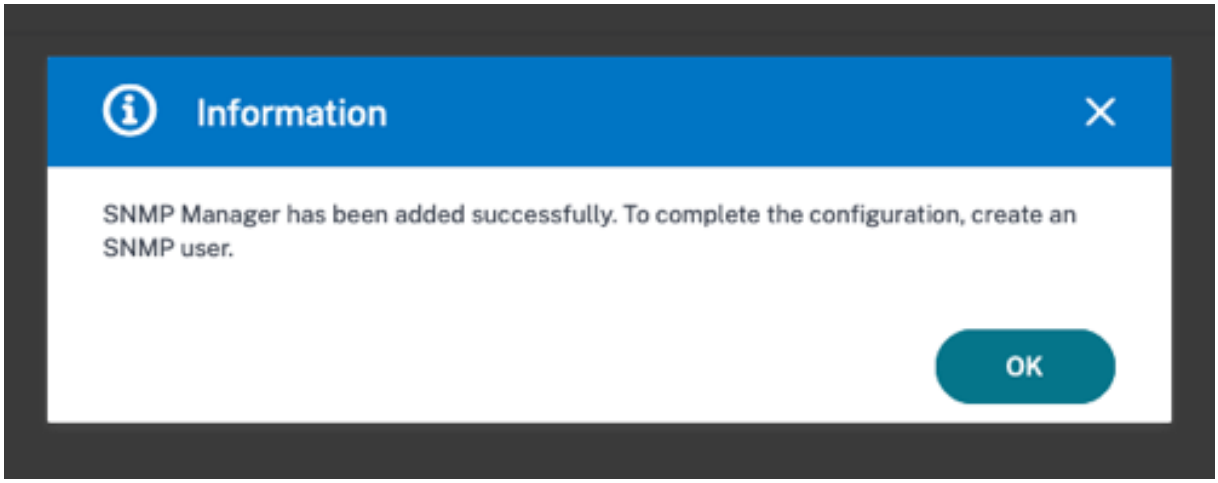
1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:

- **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
- **Version**. Select v3.
- **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.
- **Netmask**: Enter the subnet mask associated with an IP address.

4. Click **Create**.



A dialog box appears confirming that an SNMP manager is created and prompting you to configure an SNMP user.



> **Note**
>
> You must configure an SNMP user for an SNMP v3 manager. To configure the SNMP user, go to **SNMP > SNMP User**.

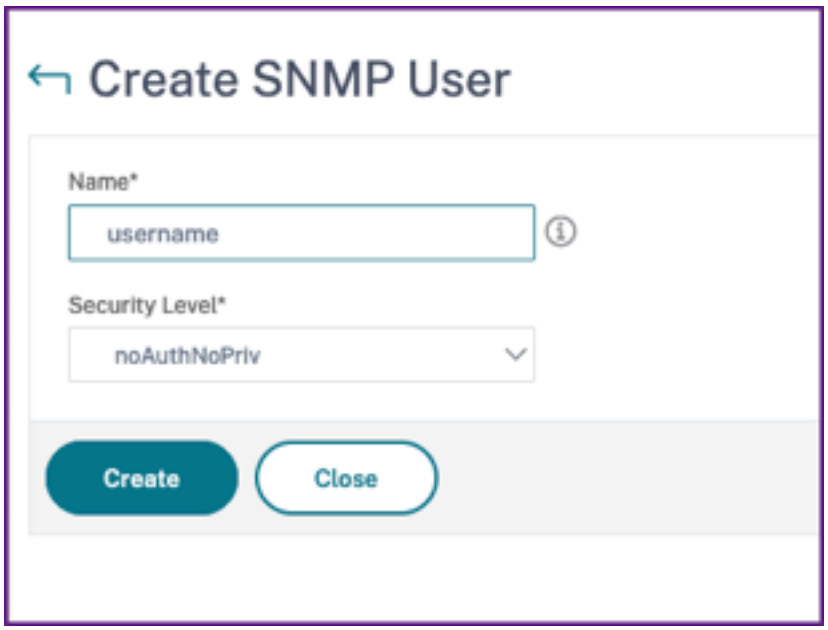
Add an SNMP user

Add an SNMP user to respond to the SNMP v3 queries from an SNMP manager.

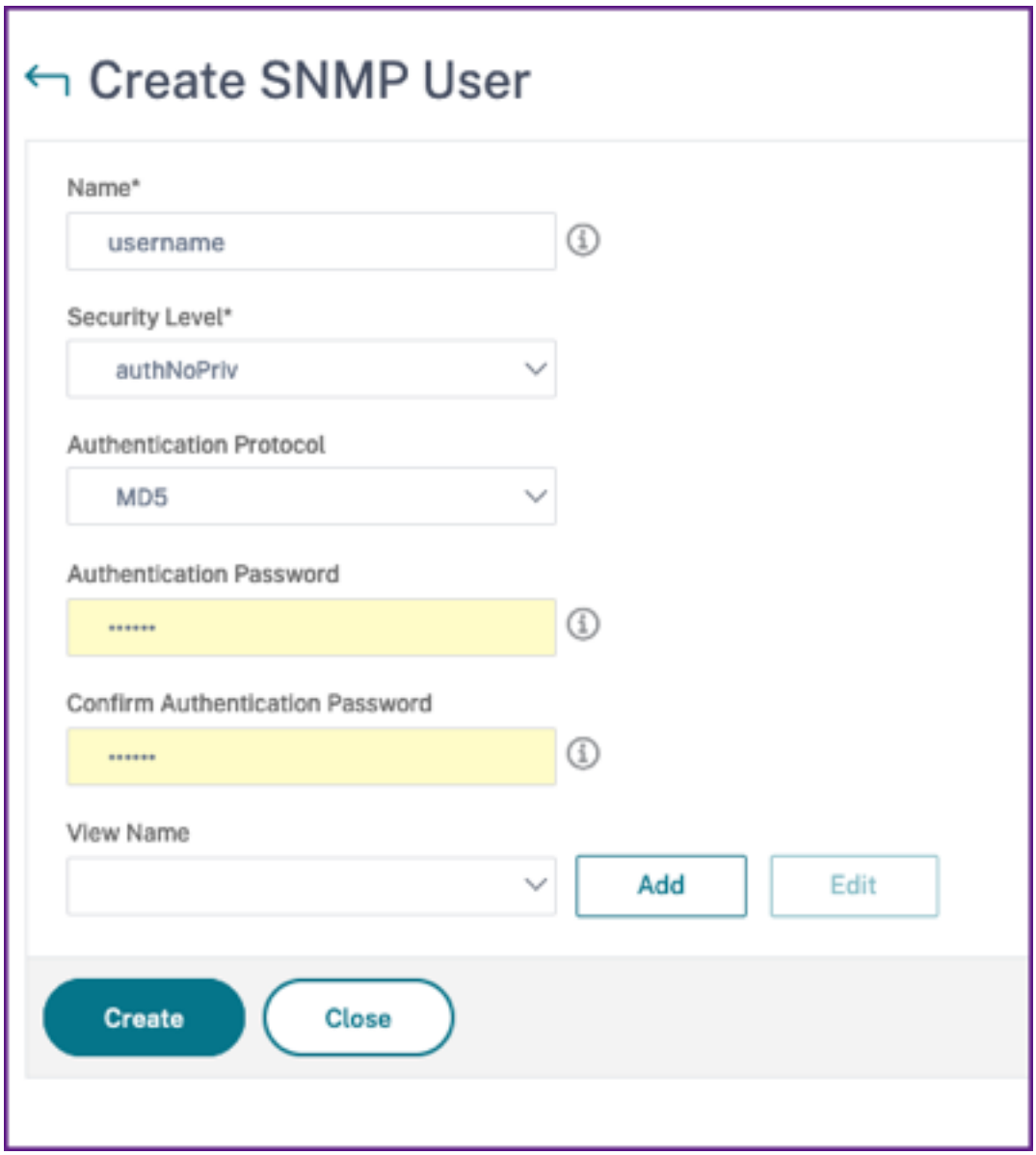
To add an SNMP user for the NetScaler agent:

1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP User** tab, click **Add**.
3. In the **Create SNMP User** page, add the following details:
    - **Name**. Enter the user name.
    - **Security Level**. Security level required for communication between the NetScaler agent and the SNMP manager.

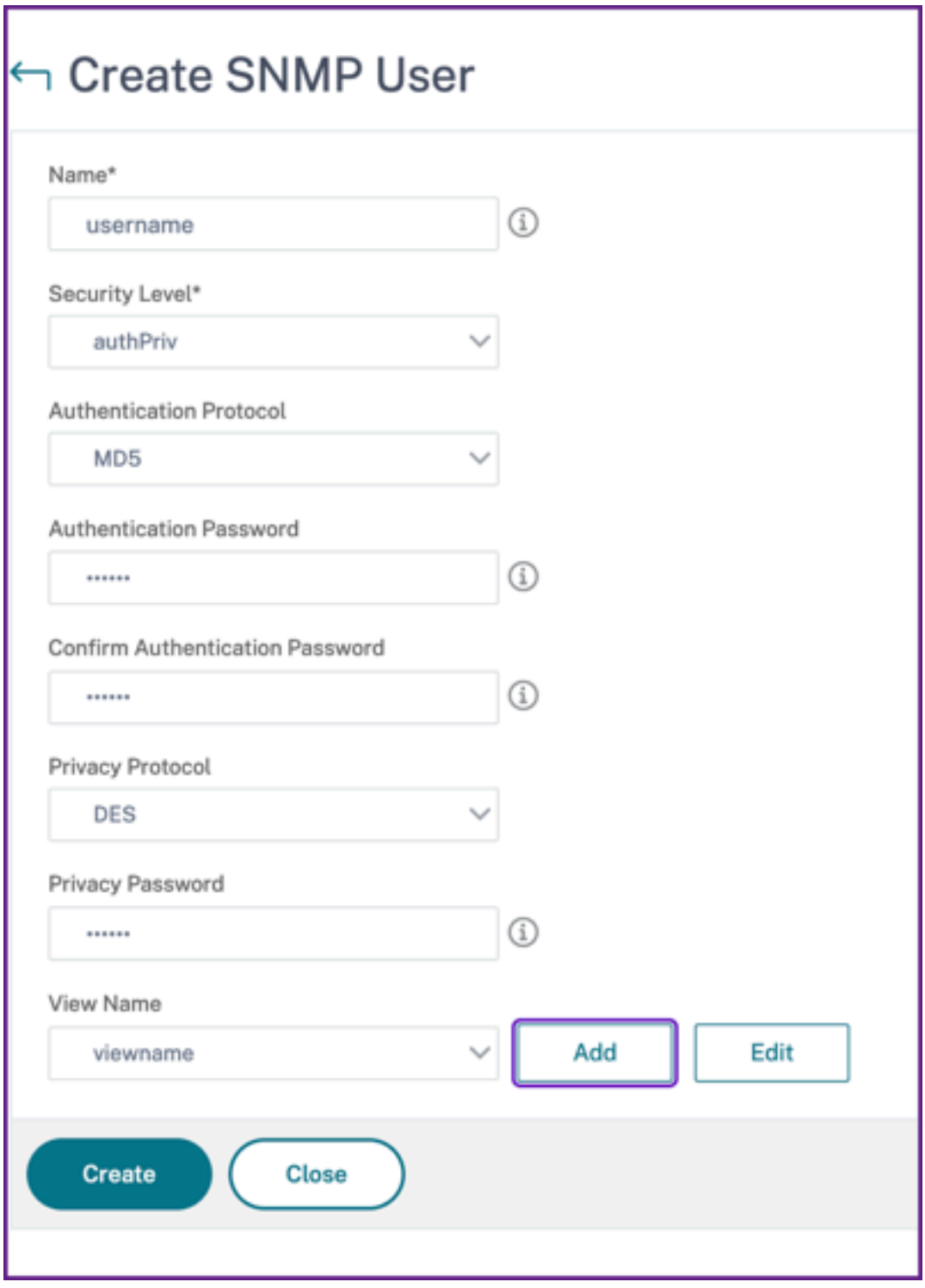
      Select one of the following security levels:
    - **noAuthNoPriv**. Require neither authentication nor encryption.



- **authNoPriv**. Require authentication but no encryption.



- **authPriv**. Require authentication and encryption.



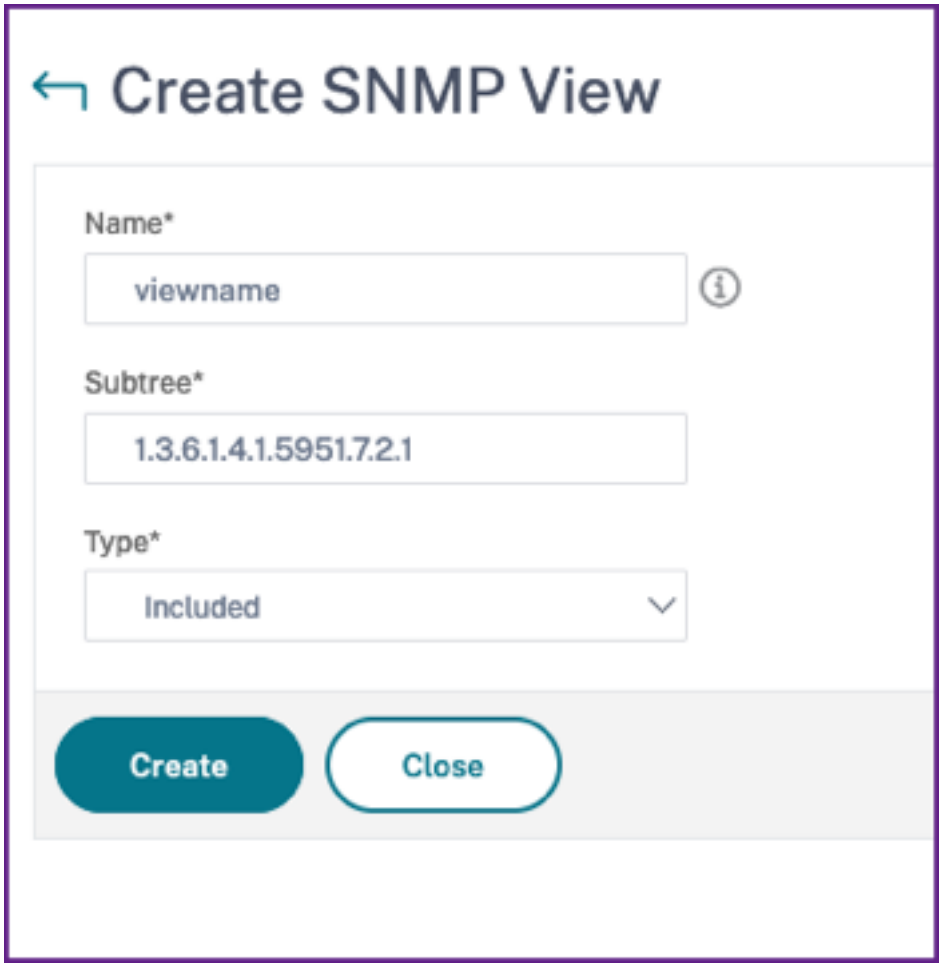
Based on the security level you've assigned to the user, provide extra authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.

Managing SNMP views

SNMP views are used to implement access control for an SNMP user. The SNMP views restrict the user access to specific portions of MIB.

To allow or restrict an SNMP OID for the NetScaler agent:

1. Navigate to **Infrastructure > Agents > Manage SNMP** and in the **SNMP View** tab, click **Add**.
2. In the **Create SNMP View**, enter the following details:
   - **View Name**: A name for the SNMP view. An instance can have many SNMP views with the same name, differentiated by the subtree parameter settings.
   - **Subtree**: A particular branch (subtree) of the MIB tree that you want to associate with this SNMP view. You must specify the subtree as an SNMP OID.
   - **Type**: This field allows you to include or exclude subtrees from a view.
3. Click **Create**.



Configure agent settings

March 11, 2024

You can modify the NetScaler ADM agent's keep-alive interval and password change requirements.

Set agent's keep-alive interval

NetScaler ADM server and agent maintain the same TCP connection for the specified keep-alive interval. An agent uses this connection to send the managed instances data to the NetScaler ADM server.

1. Navigate to **Settings > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.
3. In **Basic Settings > Agent Settings**, specify the keep-alive interval between 30–120 seconds.
4. Click **Save**.

Change agent's password without the current password

You can allow agent passwords to be changed without their current password.

1. Navigate to **Settings > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.
3. In **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change** check box, you can do the following:
   - Select the check box to remove the **Current password** field in the **Change Agent Password** page.
   - Clear the check box to keep the **Current password** field in the **Change Agent Password** page.
4. Click **Save**.

> **Note**
>
> To view the **Change Agent Password** page, navigate to **Infrastructure > Instances > Agents**, select an agent, and click **Select Action > Change Password**.

NetScaler ADM as an API proxy server

March 11, 2024

In addition to being able to receive NITRO REST API requests for its own management and analytics functionality, NetScaler Application Delivery Management (NetScaler ADM) can function as a REST API proxy server for its managed instances. Instead of sending API requests directly to the managed instances, REST API clients can send the API requests to NetScaler ADM. NetScaler ADM can differentiate between the API requests to which it must respond and the API requests that it must forward unchanged to a managed instance.

As an API proxy server, NetScaler ADM provides you with the following benefits:

- **Validation of API requests**. NetScaler ADM validates all API requests against configured security and role-based access control (RBAC) policies. NetScaler ADM is also tenant-aware and ensures that API activity does not cross tenant boundaries.
- **Centralized auditing**. NetScaler ADM maintains an audit log of all API activity related to its managed instances.
- **Session management**. NetScaler ADM frees API clients from the task of having to maintain sessions with managed instances.

How NetScaler ADM Works as an API Proxy Server

When you want NetScaler ADM to forward a request to a managed instance, you configure the API client to include any one of the following HTTP headers in the API request:

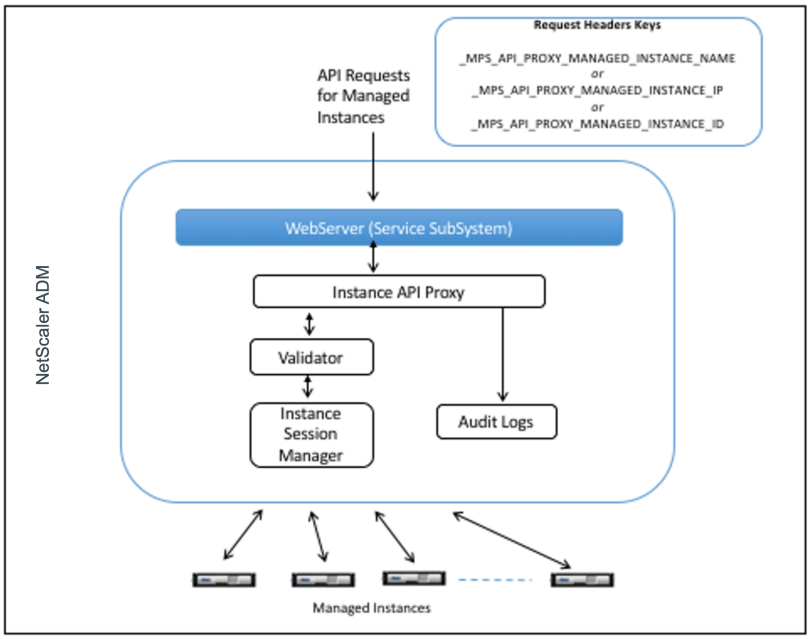
Header values	Description
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Name of the managed instance.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	IP address of the managed instance.
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID of the managed instance.
_MPS_API_PROXY_TIMEOUT	Timeout value for a NITRO API request. Set the timeout value in seconds. When you set a proxy timeout, ADM waits for the specified duration before it times out the request.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	User name to access the managed ADC instance.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Password to access the managed ADC instance.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Session ID to access the managed instance.

Header values	Description

> **Note**
>
> In **Settings > Administration > System Configurations > Basic Settings**, if you select **Prompt Credentials for Instance Login**, ensure to configure user name and password of a managed instance. Alternatively, you can also specify the instance session ID.

The presence of any of these HTTP headers helps NetScaler ADM identify an API request as one that it must forward to a managed instance. The value of the header helps NetScaler ADM identify the managed instance to which it must forward the request.

This flow is depicted in the following figure:



As shown in the above figure, when one of these HTTP headers appears in a request, NetScaler ADM processes the request as follows:

1. Without modifying the request, NetScaler ADM forwards the request to the instance API proxy engine.
2. The instance API proxy engine forwards the API request to a validator and logs the details of the API request in the audit log.
3. The validator ensures that the request does not violate configured security policies, RBAC policies, tenancy boundaries, and so on. It performs extra checks, such as a check to determine whether the managed instance is available.

If the API request is valid and can be forwarded to the managed instance, NetScaler ADM identifies a session that is maintained by the instance Session Manager and then sends the request to the managed instance.

> **Note**
>
> Ensure the **Prompt Credentials for Instance Login** option is disabled. To do so:
>
> 1. Navigate to **Settings > Administration**.
> 2. In **System Configurations**, select **System, Time zone, Allowed URLs and Message of the day**.

How to use NetScaler ADM as an API proxy server

The following examples show REST API requests that an API client sends to a NetScaler ADM server that has an IP address of 192.0.2.5. NetScaler ADM is required to forward the requests, unchanged, to a managed instance with IP address 192.0.2.10. All examples use the _MPS_API_PROXY_MANAGED_INSTANCE_IP header.

Before sending NetScaler ADM the API requests, the API client must:

- Log in to NetScaler ADM
- Obtain a session ID
- Include the session ID in subsequent API requests.

The logon API request is of the following form:

```
POST /nitro/v1/config/login
Content-Type: application/json

{

    "login": {

        "username":"nsroot",
        "password":"nsroot"
      }

 }

<!--NeedCopy-->
```

NetScaler ADM responds to the logon request with a response that includes the session ID. The following sample response body shows a session ID:

```
{


```



```
  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {


      "tenant_name": "Owner",

      "permission": "superuser",

      "session_timeout": "36000",

      "challenge_token": "",

      "username": "",

      "login_type": "",

      "challenge": "",

      "client_ip": "",

      "client_port": "-1",

      "cert_verified": "false",

      "sessionid": "##
    D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",

      "token": "b2f3f935e93db6a"
     }


  ]

 }

<!--NeedCopy-->
```


Example 1: Retrieve load balancing virtual server statistics

The client must send NetScaler ADM an API request of the following form:

```
1     GET /nitro/v1/stat/lbvserver
2     Content-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5  <!--NeedCopy-->
```

Where the value of the Cookie Header is the Session ID returned from the login API call. And the value of the _MPS_API_PROXY_MANAGED_INSTANCE_IP is the IP address of the ADC.

Example 2: Create a load balancing virtual server

The client must send NetScaler ADM an API request of the following form:

```
1     POST /nitro/v1/config/lbvserver/sample_lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9          "lbvserver":{
10
11             "name":"sample_lbvserver",
12             "servicetype":"HTTP",
13             "ipv46":"10.102.1.11",
14             "port":"80"
15          }
16
17      }
18
19 <!--NeedCopy-->
```

Example 3: Modify a load balancing virtual server

The client must send NetScaler ADM an API request of the following form:

```
1     PUT /nitro/v1/config/lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```



```
6
7      {
8
9         "lbvserver":{
10
11              "name":"sample_lbvserver",
12              "appflowlog":"DISABLED"
13           }
14
15       }
16
17 <!--NeedCopy-->
```

Example 4: Delete a load balancing virtual server

The client must send NetScaler ADM an API request of the following form:

```
1      DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2      Accept-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Example 5: Download the CLI running config on the ADC

The client must send NetScaler ADM an API request of the following form:

```
1      GET /nitro/v1/config/nsrunningconfig
2      Accept-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

FAQs

March 11, 2024

This section provides the FAQ on the following NetScaler Application Delivery Management (NetScaler ADM) features. Click a feature name in the following table to view the list of FAQs for that feature.

Analytics	Authentication	Configuration Management
Certificate Management	Deployment	Deployment (Disaster recovery)
Event Management	Instance Management	StyleBooks
System Management		

Analytics

Is it required to enable EUEM virtual channel on NetScaler Gateway instances deployed in single-hop mode?

EUEM virtual channel data is part of HDX Insight data that the NetScaler ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If the EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

The EUEM virtual channel is a default service running on Citrix Virtual Desktop applications (VDA). If it is not running, start the "Citrix End User Experience Monitoring"process in VDA services.

How do I enable NetScaler ADM to monitor web-application and virtual-desktop traffic?

1. Navigate to **Infrastructure** > **Instances** > **NetScaler**, and select the NetScaler instance on which you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. In the **Configure Analytics** page, select all the virtual servers on which you want to enable analytics, and click **Enable AppFlow**. For more details, see How to Enable Analytics on Instances.

> Note
>
> For NetScaler instances of 11.0 release, 65.30 build and later, there is no option on NetScaler ADM to enable Security Insight explicitly. Ensure that you configure the AppFlow parameters on the NetScaler instances, so that NetScaler ADM starts receiving the Security Insight traffic along with the Web Insight traffic. For more information on how to set the AppFlow parameters on NetScaler instances, see To set the AppFlow parameters by using the configuration utility.

After I add the NetScaler instances, does NetScaler ADM automatically start collecting analytical information?

No. Enable analytics on the virtual servers hosted in NetScaler instances that are managed by NetScaler ADM. For more details, see How to Enable Analytics on Instances.

Is it required to access the individual NetScaler appliance for enabling analytics?

No. All configurations are done from the NetScaler ADM user interface, which lists the virtual servers hosted on the specific NetScaler instance. For more details, see How to Enable Analytics on Instances.

What are the types of virtual servers that can be listed on a NetScaler instance to enable analytics?

Currently, the NetScaler ADM user interface lists the following virtual servers for enabling analytics:

- Load balancing virtual server
- Content switching virtual server
- VPN virtual server
- Cache redirection virtual server

How do I attach an extra disk to the NetScaler ADM?

To attach an extra disk to NetScaler ADM:

1. Shut down the NetScaler ADM virtual machine.
2. In the hypervisor, attach an extra disk of the required disk size to the NetScaler ADM virtual machine.

   For example, Let us consider that you want to increase the disk space to 200 GB, in a NetScaler ADM virtual machine of 120 GB. In this scenario, you must attach a disk space of 200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, NetScaler ADM log files. The existing 120 GB disk space is used to store core files, Operating System Log files, and so on.
3. Start the NetScaler ADM virtual machine.

What do you mean by collectors are not configured on NetScaler instances?

A collector receives AppFlow records generated by the NetScaler appliance.

NetScaler ADM receives Security Insight and Web Insight traffic from the NetScaler instances when the AppFlow feature is enabled. When you enable the AppFlow feature on a NetScaler instance, you must specify at least one collector to which the AppFlow records are sent. If the collectors are not configured on the NetScaler instances, NetScaler ADM does not receive the traffic from the instances.

For example, five NetScaler instances are added to NetScaler ADM. If collectors are not specified for two instances, no traffic flows to NetScaler ADM. Self-service diagnostics detects the issue and displays the issue as "Collectors are not configured on 2 instances."

For more information about how to configure the AppFlow Feature, see Configuring the AppFlow Feature.

What does enabling client-side measurements do?

With client side measurements enabled, ADM captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

Authentication

What is load balancing of authentication requests?

The authentication-server load balancing feature enables NetScaler ADM to load balance the authentication requests that are directed to the external authentication servers. Load balancing the authentication servers ensures that the authentication load is split across multiple authentication servers and thus avoid an authentication server from being overloaded. You can create an authentication service to connect with and get user information from your existing external authentication server using the authentication protocols like LDAP, RADIUS, or TACACS.

Why do we need to cascade external authentication servers?

Cascaded external authentication servers provide uninterrupted authentication processing, allowing access to legitimate users if an authentication server fails. There is no limitation on which types of authentication servers you can cascade. You can have all RADIUS servers, or all LDAP servers, or a combination of RADIUS and LDAP servers.

How many external authentication servers can I cascade?

You can cascade up to 32 external authentication servers in NetScaler ADM.

Do I have an alternative when external authentication fails?

There can be a situation when external authentication completely fails, even when you have cascaded several servers. For example, the external servers can become unreachable, or a new user's credentials might not have been entered in any of the external authentication servers. To prevent locking

users out in such a situation, you can enable fallback local authentication. For more details, see Fallback Local Authentication.

What is fallback local authentication?

Fallback local authentication is an option to authenticate your users locally when external authentication fails. If external authentication fails, NetScaler ADM accesses the local user database to authenticate your users.

In NetScaler ADM, navigate to **Settings > Authentication > Authentication Configuration**. On this page, you can add multiple external authentication servers in a cascade, and you can select the **Enable fallback local authentication** option.

What is an extraction of external user groups?

If you have added external servers for authenticating the users, you can import (extract) existing user groups into NetScaler ADM. You have to import user groups once and provide a group permission to a user group rather than importing individual users and giving them individual permissions. You do not have to recreate the users on NetScaler ADM.

Why do we need to assign group permissions?

When you are using the load balancing feature of NetScaler, you can integrate NetScaler ADM with external authentication servers, and import user group information from the authentication servers. Log in to NetScaler ADM and manually create the same group information in NetScaler ADM and assign permission to those groups. The user and user group permission is managed in NetScaler ADM and not in the external server. The users have different role-based access permissions on the external servers. Configure the same permissions for the users in NetScaler ADM also. Instead of configuring permissions individually for each user, you can configure a group-level permission so that the user-group members can access specific services on the load balanced virtual servers. The typical permissions that you can assign are permissions to manage NetScaler instances, NetScaler SDX instances, virtual servers, and so on, so that the users of that group can manage only those instances or virtual servers. You can later edit the permissions given to the users at the group level. You can even remove one or more user groups; other group users still function on NetScaler ADM.

Configuration Management

Can I perform configuration across multiple NetScaler instances simultaneously using NetScaler ADM?

Yes, you can use configuration jobs to perform configuration across multiple NetScaler instances.

What are configuration jobs on NetScaler ADM?

A job is a set of configuration commands that you can create and run on one or more managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler ADM GUI. You can also convert the recorded tasks into CLI commands.

You can use the Configuration Jobs feature of NetScaler ADM to create a configuration job, send email notifications, and check execution logs of the jobs created.

Can I schedule jobs using built-in templates in NetScaler ADM?

Yes! You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can choose to run the job immediately, or schedule the job to be run later.

You can save the configuration of a job that was previously created, and run the job again after modifying the commands, the parameters, the configuration source, and targeted instances. This is useful when the same set of commands has to be run on a different instance, or when the job encounters an error and stops further execution.

Certificate Management

Does the deletion of SSL certificates from NetScaler ADM lead to the deletion of certificates from NetScaler instances?

No

Deployment

What is the default user name and password?

- After you complete the initial network configuration, you can log on to NetScaler ADM from the hypervisor or SSH console, using the default user name and password (nsrecover/nsroot).
- The default user name and password to log on from the GUI is *nsroot/nsroot*.

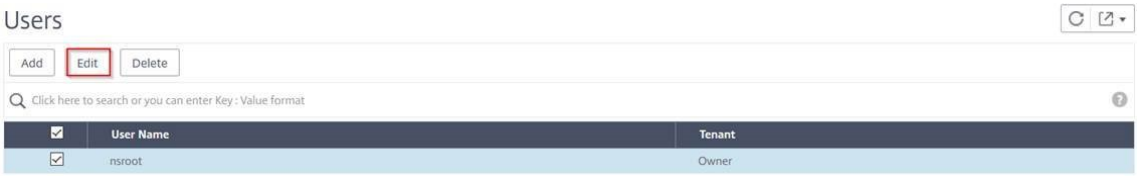
How to change the default password?

To change the password:

1. In NetScaler ADM, navigate to **Settings > User Administration > Users**.

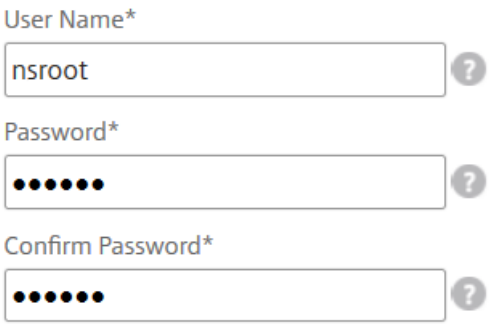
   The **Users page** is displayed.

2. Select the user name **nsroot** and click **Edit**.



   The **Configure System User** page is displayed.

3. Select **Change Password** and create a password of your choice.



4. Click **OK**.

   You can now use the new password to log on from the GUI, hypervisor, or SSH console.

> Note
>
> You cannot modify the user name.

How to reset the password?

You can see this documentation to reset the password.

In a HA pair, if the password is changed in the primary node and if the Break HA pair option is selected later, what is the behavior?

You can log on to both standalone nodes using your new password.

If two standalone servers have different passwords, what is the impact in deploying these two servers in HA pair?

It is recommended to have default password for both servers when you deploy two standalone servers to HA pair.

The HA configuration is complete, but the primary node GUI is not accessible. What can be the reason?

It takes a few minutes for the configuration to take effect. You can try accessing again after a few minutes.

The HA configuration is complete, but the floating IP address GUI is not accessible. What can be the reason?

After the HA configuration, you need to first access the primary node GUI and complete the deployment. For more information, see Deploy the primary and secondary node as a high availability pair. After the deployment is complete, the server reboots and gets ready for high availability deployment. You can then access the floating IP address GUI.

What DB is supported in NetScaler ADM standalone and NetScaler ADM HA?

Both NetScaler ADM standalone and NetScaler ADM HA support PostgreSQL.

What is the potential data loss to the secondary node?

The secondary node listens to the heartbeat messages that the primary node sends through the NetScaler ADM database. If the secondary node does not receive the heartbeats for more than

180 seconds, then the secondary node performs an SSH-based check on the primary node. If the heartbeat and SSH-based check fail, the primary node is considered to be down.

In this scenario, the secondary node takes over as the primary node and the 180 seconds timeframe can be considered as the possible data loss to the secondary node.

What happens if the primary node is down?

The secondary node takes over and becomes the primary node.

How to reinstall the failed node?

It is recommended to install a fresh VM build. To reinstall:

1. Break the HA pair. Navigate to **Settings > Deployment**

   The deployment page is displayed. Click **Break HA**
2. Delete the failed node from the hypervisor.
3. Import the .XVA image file to the hypervisor.
4. From the Console tab, configure NetScaler ADM with the initial network configurations. For more information, see Register and deploy the first server (primary node) and Register and deploy the second server (secondary node).
5. Redeploy the HA pair.

Does NetScaler ADM support SAN Storage?

Citrix recommends you to host the NetScaler ADM VHD on a local storage. When hosted on storage devices in a SAN, NetScaler ADM might not work as expected. So, ADM deployment on SAN is not supported.

Does NetScaler ADM support an extra disk?

Yes. A new installation of NetScaler ADM HA pair allocates 120 GB of storage by default. For more than 120 GB storage, you can add one extra disk for a maximum of 3 TB storage. Adding more than one extra disk is not supported.

After disabling the HA pair, what happens to the floating IP address configured?

The floating IP address is no longer accessible and you need to redeploy the high availability pair.

Can I give a different floating IP address while redeploy?

Yes. You can configure a new floating IP address.

Why is secondary node GUI not accessible?

Secondary node is only a read-replica server and acts as a primary node only if the primary node is down for any reason. Citrix recommends accessing either the primary node GUI or the floating IP address GUI.

If the primary node is down for a long duration, can the configurations still be done using the floating IP address GUI?

Yes. You can still continue to do configurations and the configurations get saved in the secondary node. After the primary node is back, all the configurations are synchronized.

If there is a necessity to change the primary node IP address or secondary node IP address or floating IP address in the future (for example, changing it to IPv6), what are the recommended solutions to follow?

Changing the IP addresses in HA pair is not supported without breaking the HA pair.

To update the primary node or the secondary node IP address:

1. Break the HA pair. Navigate to **Settings > Deployment**.

   The Deployment page is displayed. Click **Break HA**

   a) Log on to the primary node using an SSH client or from the hypervisor.

   b) Use `nsrecover` as the user name and enter the password that you have set.

   c) Enter **networkconfig**. Perform the procedure from **step 3** available at Register and deploy the first server (primary node).

      During the initial network configuration, you can provide a different IP address.

   d) Perform the same procedure for secondary node and continue with the procedure from **step 3** available at Register and deploy the second server (secondary node).

To update the floating IP address:

1. Navigate to **Settings > Deployment**.

   The Deployment page is displayed.

a) Click **HA Settings**.

b) Click **Configure Floating IP Address for High Availability Mode**.

c) Enter the floating IP address and click **OK**.

Does ADM support AMD processors?

AMD processor is supported in:

- **NetScaler ADM 13.1 build 4.43 or later**.
- **NetScaler agent 13.1 build 17.42 or later**.

Deployment (Disaster Recovery)

How frequent does the replication happens between the primary site and disaster recovery site?

The replication between the primary site and the disaster recovery site is real time.

After initiating the backup script at the DR site, does the DR site becomes the temporary primary site, until the primary site is recovered and fully operational?

No. The DR site will now become the primary site. To revert the HA pair as the primary site, see Revert configurations to the original primary site

If the Break HA pair option is selected, both nodes operate as a standalone server. Since DR support is not applicable for standalone server, what happens to the DR site if Break HA pair is selected?

If you select Break HA pair option, the replication between the primary site and the DR site is terminated. You need to reconfigure the DR site as part of redeploying HA pair.

Event Management

How can I keep track of all the events that have been generated on my managed NetScaler instances using NetScaler ADM?

As a network administrator, you can view details such as configuration changes, log on conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along

with events and their severity on specific instances. You can use the NetScaler ADM events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

What are event rules?

Using NetScaler ADM, you can configure rules to monitor specific events. Event Rules make it easier to monitor many events generated across your NetScaler ADM infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run.

The conditions for which you can create filters are severity, NetScaler instances, category, and failure objects. The actions you can assign to the events are sending an email notification, forwarding SNMP traps from managed NetScaler instances to the NetScaler ADM, and sending an SMS notification.

Instance Management

What happens if an ADC instance cannot connect to ADM after bandwidth allocation when you use NetScaler pooled capacity licensing?

If the heartbeat between the ADC instance and ADM fails, the instance enters a grace period of 30 days. And after communication is re-established, pooled capacity licensing starts working. When in grace period, ADC functions are not affected. After 30 days of grace period, the ADC instance initiates warm restart and is unlicensed.

What are data centers in NetScaler ADM?

A NetScaler ADM data center is a logical grouping of the NetScaler instances in a specific geographical location. Each server can monitor and manage several NetScaler instances within a data center. You can use the NetScaler ADM server to manage data such as syslog, application traffic flow, and SNMP traps from the managed instances. For more details on configuring data centers, see How to Configure Data Centers for Geomaps in NetScaler ADM.

What are the different NetScaler ADC appliances that are supported by NetScaler ADM?

Instances are the NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler ADM. You must add these instances to the NetScaler ADM server. You can add the following NetScaler ADC appliances and virtual appliances to NetScaler ADM:

- NetScaler MPX

- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

You can add instances either while setting up the NetScaler ADM server for the first time or later.

What is an instance profile?

An instance profile is used by NetScaler ADM to access an instance.

An instance profile contains the user name and password for access to one or more instances. A default profile is available for each instance type. For example, the ns-root-profile is the default profile for NetScaler instances. It contains the default NetScaler administrator credentials. When you change the credentials required for access to instances, you can define custom instance profiles for those instances.

Can I rediscover multiple NetScaler VPX instances in NetScaler ADM?

Yes, you can rediscover multiple Citrix **VPX** instances in NetScaler ADM to learn the latest states and configurations of the instances.

Navigate to **Infrastructure > Instances > NetScaler > VPX**, select the instances that you want to rediscover, and in the **Action** list click **Rediscover**. For more information, see How to Rediscover Multiple VPX Instances.

Can NetScaler ADM be installed on NetScaler SDX?

No

Can I add a NetScaler instance on the ADM software by using a public IP address?

Yes, you can by using network address translation (NAT).

- For adding a single instance: use NAT IP of the public IP address of the ADC instance.
- For adding an ADC HA pair: add the NAT IP addresses of the HA pair in this format:

  <NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>

- For adding an ADC cluster: add all the NAT public IP addresses of all the instances in the cluster, each separated by a comma, and add the NAT IP of the CLUSTER IP inside parentheses or round brackets. An example format: NAT1, NAT2, NAT3,(NATIP of CLUSTERIP).

For more information, see the following topics:

- Add instances to NetScaler ADM
- Configuring Network Address Translation

How to register a disaster recovery node if the DR node credentials are changed?

Reset the disaster recovery (DR) node credentials to `nsrecover`/`nsroot` using the following command:

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

To register a DR node, follow the steps in Deploy and register the NetScaler ADM DR node using DR console.

StyleBooks

Can StyleBooks be used to configure different NetScaler instances running on different versions of the NetScaler software?

Yes, you can use StyleBooks to configure different NetScaler instances running on different versions if there is no discrepancy between the commands across different versions.

When a StyleBook is used to configure multiple NetScaler instances at the same time, and configuration of one NetScaler instance fails, what happens?

If applying the configuration to a NetScaler instance fails, the configuration is not applied to any more instances, and already-applied configurations are rolled back.

Do NetScaler backups made through NetScaler include configurations applied through StyleBooks?

Yes

System Management

Can I assign a host name to my NetScaler ADM server?

Yes, you can assign a host name to identify your NetScaler ADM server. To assign a host name, navigate to **System**> **System Administration** > **System Settings**, and click **Change Hostname**.

The host name is displayed on the Universal license for NetScaler ADM. For more information, see How to Assign a Host Name to a NetScaler ADM Server.

Can I back up and restore my NetScaler ADM configuration?

Yes, you can back up configuration files (NTP files and SSL certificates), system data, infrastructure and application data, and all your **SNMP** settings. If your NetScaler ADM ever becomes unstable, you can use the backed-up files to restore your NetScaler ADM to a stable state.

To back up and restore your NetScaler ADM configuration, navigate to **System** > **Advanced Settings** > **Backup Files**, and click **Back Up** or **Restore** as the case might be. For more information, see How to back up and Restore Configuration on NetScaler ADM.

Citrix recommends that you use this feature before performing an upgrade or for precautionary reasons.

What are Thresholds and Alerts on NetScaler ADM?

You can set thresholds and alerts to monitor the state of a NetScaler instance and monitor entities on managed instances.

When the value of a counter exceeds the threshold, NetScaler ADM generates an alert to signify a performance-related issue. When the counter value returns to the clear value specified in the threshold, the event is cleared.

Can I generate a technical support file for NetScaler ADM?

Yes. Citrix recommends that you generate an archive of NetScaler ADM data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

You can generate a technical support file that contains debug logs, the duration for which debug logs were collected, and distinct and diverse logs from the NetScaler ADM database.

To configure and send a technical support file, navigate to **System** > **Diagnostics** > **Technical Support**, and then, click **Generate Technical Support File**. For more information, see How to Generate a Tech Support File for NetScaler ADM.

What is syslog purging?

Syslog is a standard protocol for logging. Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which all Generic Syslog data, AppFirewall data, and NetScaler Gateway data will be deleted from NetScaler ADM.

Can I configure NTP server on NetScaler ADM?

You can configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize the NetScaler ADM clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server, navigate to **System** > **NTP Servers**, and then click **Add**. For more information, see How to Configure NTP Server on NetScaler ADM.

From which version is the NetScaler ADM active-passive HA deployment supported?

The NetScaler ADM active-passive HA deployment mode is supported from NetScaler ADM version 12.0 build 51.24.

I had a NetScaler ADM active-active HA setup and had configured a NetScaler appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration?

After you upgrade the NetScaler ADM HA pair to active-passive mode, you have to run the following command on the NetScaler appliance to update the load balancing configuration:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n\"\"-recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

Can I configure load balancing of the NetScaler ADM HA pair on a NetScaler Instance using port 443?

No, you cannot configure load balancing of the NetScaler ADM HA pair on a NetScaler Instance using port 443.

When you configure the `http-ecv` and `https-ecv` monitors on NetScaler, it does not monitor the NetScaler ADM HA nodes correctly.

Can a NetScaler ADM server backup file be used to restore the configuration of another NetScaler ADM server?

Yes

After NetScaler ADM backs up a NetScaler instance, can that backup file be used to restore the configuration of another NetScaler instance through NetScaler ADM?

Yes. Download the NetScaler ADM backup file, upload it into another NetScaler instance's backup repository, and restore that instance. Make sure that the network information and authentication information do not conflict. For example, check for IP-address or port conflicts, mismatched password profiles. Also make sure that the restored VPX instance has the same NSIP address and NetScaler license as the one that was backed up.

Before restoring an instance in a high availability pair, make sure the IP addresses and state (primary or secondary) stored in the backup file match those of the original HA configuration. Also verify that the new primary and secondary have the same type of NetScaler license.

Can we force NetScaler ADM to use a SNIP address to communicate with the NetScaler instances, instead of using the NSIP address of the NetScaler ADM server?

Yes, you can add a SNIP address (with management enabled) in NetScaler ADM for communication with NetScaler instances.

When I back up NetScaler Instances in NetScaler ADM, is the result a full back-up or a basic back-up?

Backups of NetScaler instances by NetScaler ADM are full backups.

Is there a troubleshooting guide for NetScaler ADM?

Yes. See https://support.citrix.com/article/CTX224502.

How are NetScaler instances managed when a NetScaler ADM HA failover occurs?

If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node. All the NetScaler instances are updated with the latest primary node details as their SNMP trap destination by default.

The new primary (active) NetScaler ADM node checks to determine whether the previously active node was configured as the AppFlow collector or syslog server, if it was, the new primary adds the AppFlow collector or syslog server details to the information sent to the instances.

For syslog it replaces the old server details.

What happens when the NetScaler ADM HA node that went down comes back up?

After returning to service, the NetScaler ADM node remains passive unless the active node fails over

How are NetScaler instances distributed across NetScaler ADM HA nodes?

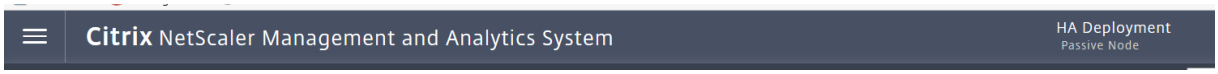
All the NetScaler instances are managed by the primary NetScaler ADM node.

How are virtual server licenses managed if there is NetScaler ADM HA failover?

If the NetScaler ADM primary node on which virtual server licenses are applied goes down, the new primary node manages the virtual server licenses for a grace period of 30 days. Reapply the licenses on the new primary before the end of the grace period. For alternatives, contact NetScaler support.

Is a load balancer mandatory for a NetScaler ADM HA setup?

No, but if there is no load balancer, NetScaler ADM nodes must be accessed through their own IP addresses. The passive node is marked with the tag "Passive", and Citrix recommends not to create any configurations on the passive node.



Does NetScaler ADM support an external database?

No

Can a NetScaler instance that is being managed by NetScaler ADM be used as a Load balancer for NetScaler ADM HA?

Yes

What data is synchronized between NetScaler ADM HA nodes?

Complete NetScaler ADM database is synchronized, and the following folders are synchronized:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/