Citrix Application Delivery Management service

Contents

Overview

September 25, 2021

Citrix Application Delivery and Management is a web-based solution for managing all Citrix deployments that include Citrix ADC MPX, Citrix ADC VPX, Citrix ADC SDX, Citrix ADC CPX, Citrix ADC BLX, Citrix Gateway, and Citrix Secure Web Gateway that are deployed on-premises or on the cloud.

You can use this cloud solution to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified, and centralized cloud-based console. Citrix Application Delivery and Management provides all the capabilities required to quickly set up, deploy, and manage application delivery in Citrix ADC deployments and with rich analytics of application health, performance, and security.

Citrix Application Delivery and Management provides the following benefits:

- **Agile** – Easy to operate, update, and consume. The service model of Citrix Application Delivery and Management is available over the cloud, making it is easy to operate, update, and use the features provided by Citrix Application Delivery and Management. The frequency of updates, combined with the automated update feature, quickly enhances your Citrix ADC deployment.
- **Faster time to value** – Quicker business goals achievement. Unlike with the traditional on-premises deployment, you can use your Citrix Application Delivery and Management with a few clicks. You not only save the installation and configuration time, but also avoid wasting time and resources on potential errors.
- **Multi-Site Management** – Single pane of glass for instances across multi-site data centers. With the Citrix Application Delivery and Management, you can manage and monitor Citrix ADCs that are in various types of deployments. You have one-stop management for Citrix ADCs deployed on-premises and in the cloud.
- **Operational Efficiency** – Optimized and automated way to achieve higher operational productivity. With the Citrix Application Delivery and Management, your operational costs are reduced by saving your time, money, and resources on maintaining and upgrading the traditional hardware deployments.

How Citrix Application Delivery and Management works

Citrix Application Delivery and Management is available as a service on the Citrix Cloud. After you sign up for Citrix Cloud and start using the service, install agents in your network environment or initiate the built-in agent in the instances. Then, add the instances you want to manage to the service.

An agent enables communication between the Citrix Application Delivery and Management and the managed instances in your data center. The agent collects data from the managed instances in your network and sends it to the Citrix Application Delivery and Management.

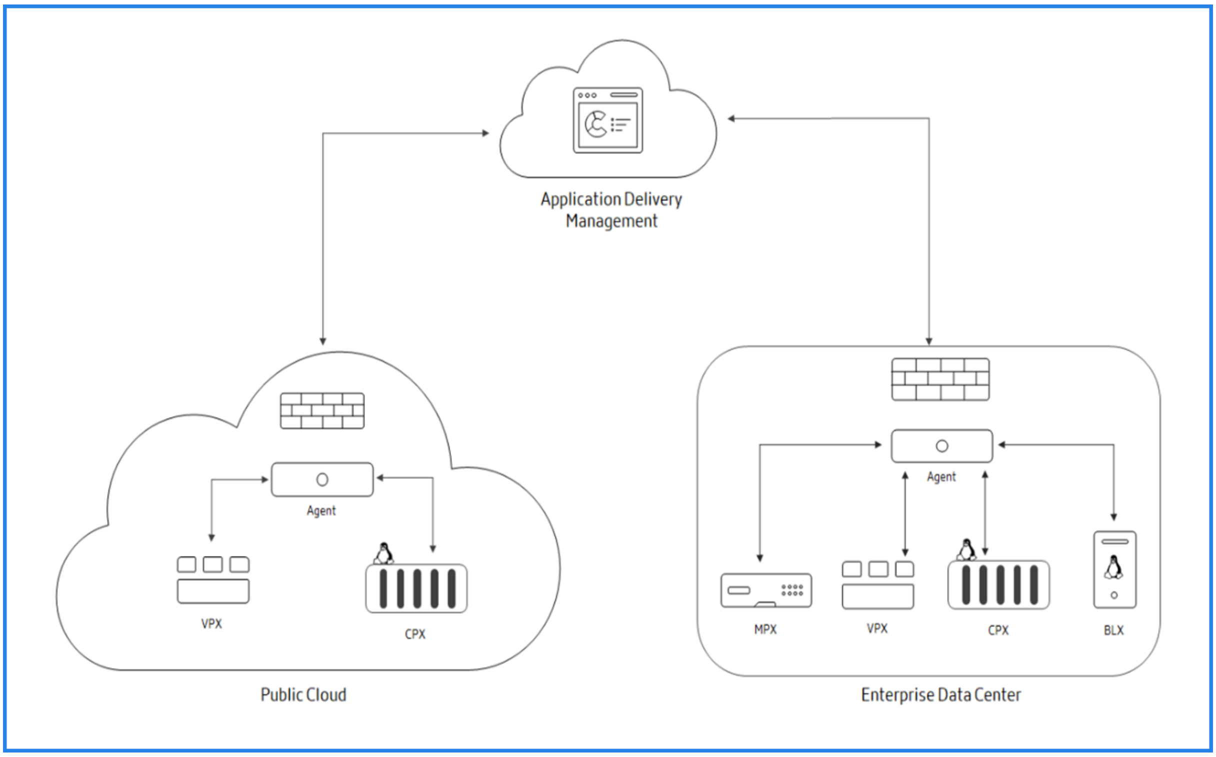
When you add an instance to Citrix Application Delivery and Management, it implicitly adds itself as a trap destination and collects inventory of the instance.

The service collects instance details such as:

- Host name
- Software version
- Running and saved configuration
- Certificates
- Entities configured on the instance, and so on.

Citrix Application Delivery and Management periodically polls managed instances to collect information.

The following image illustrates the communication between the service, agents, and instances:



Features and solutions

September 28, 2021

This document describes the features that are supported on the Citrix Application Delivery and Management.

Application analytics and management

Application Analytics and Management feature of Citrix Application Delivery and Management strengthens the application-centric approach to help you address various application delivery challenges. This approach gives you visibility into the health scores of applications, helps you determine the security risks, and helps you detect anomalies in the application traffic flows and take corrective actions.

- 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 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 Citrix ADC instances.
- Intelligent App Analytics: The Intelligent App Analytics feature provides an easy and scalable solution for monitoring and troubleshooting applications that are delivered through Citrix ADC appliances. Intelligent App Analytics not only monitors all the levels of application transactions, but also uses machine learning techniques to define normal traffic patterns in your network and detect anomalies. This feature reduces the overall turnaround time and improves the overall application uptime.

StyleBooks

StyleBooks simplify the task of managing complex Citrix ADC configurations for your applications. A StyleBook is a template that you can use to create and manage Citrix ADC configurations. You can create a StyleBook for configuring a specific feature of Citrix ADC, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Skype for Business.

Instance management

Enables you to manage the Citrix ADC, Citrix Gateway, and Citrix Secure Web Gateway instances.

Event management

Events represent occurrences of events or errors on a managed Citrix ADC instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on Citrix Application Delivery and Management. Following are the related features that you can configure or view by using Citrix Application Delivery and Management:

- Creating event rules
- Using Citrix Application Delivery and Management to export syslog messages

Certificate management

Citrix Application Delivery and Management 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.

Configuration management

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management.

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.

License management

Allows you to manage Citrix ADC licenses by configuring Citrix Application Delivery and Management as license manager.

- Citrix ADC pooled capacity: A common license pool from which your Citrix ADC instance can check out one instance license and only as much bandwidth as it needs. When the instance no longer requires these resources, it checks them back in to the common pool, making the resources available to other instances that need them.
- Citrix ADC VPX check-in and check-out licensing: Citrix Application Delivery and Management allocates licenses Citrix ADC VPX instances on demand. A Citrix ADC VPX instance can check out the license from the Citrix Application Delivery and Management when a Citrix ADC VPX instance is provisioned, or check back in its license to Citrix Application Delivery and Management when an instance is removed or destroyed.

Network reporting

You can optimize resource usage by monitoring your network reporting on Citrix Application Delivery and Management.

Analytics

Provides an easy and scalable way to look into the various insights of the Citrix ADC instances' data to describe, predict, and improve application performance. You can use one or more analytics features simultaneously.

- HDX Insight: Provides end-to end visibility for ICA traffic passing through Citrix ADC. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, end-to-end performance data, and troubleshoot performance issues.
- Web Insight: Provides visibility into enterprise web applications. It allows IT administrators to monitor all web applications served by the Citrix ADC by providing integrated and real-time monitoring of applications. Web Insight processes data from Citrix ADC using an approximation algorithm. It provides top 1,000 records of the metrics related to the web applications in your enterprise.
- 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: Provides visibility into secure transactions on the web (HTTPs). It allows IT administrators to monitor all web applications served by the Citrix ADC by providing integrated, real-time, and historic monitoring of web transactions. SSL insight processes data from Citrix ADC using an approximation algorithm. It provides top 1,000 records of the metrics related to the web transactions in your enterprise.

Role-based access control

Role-based access control (RBAC) allows you to grant access permissions based on the roles of individual users within your enterprise. The first user of an organization who logs on with Citrix Cloud credentials has the super admin role who, by default, has all access permissions. The other users of that organization, who are later created by the admin, are granted non-admin roles.

Subscriptions

Provides a dashboard view of the subscriptions that you have purchased.

You are assigned to an Express account by default. With this account, you can manage limited Citrix Application Delivery and Management resources. For more information, see Manage Citrix Application Delivery and Management resources using Express account.

The following Citrix Application Delivery and Management features are currently not available:

- Deployment
  - Migrating from Citrix Insight Center to Citrix Application Delivery and Management

  - Integrating Citrix Application Delivery and Management with Citrix Virtual Desktop Director
- Analytics: TCP Insight, Video Insight, and WAN Insight
- Limited System Settings
- Orchestration
  - Integration with OpenStack and VMware NSX Manager
  - Citrix ADC Automation in Cisco ACI's Hybrid Mode
  - Container Orchestration: Integration with Mesos/Marathon and Kubernetes

Release notes

October 27, 2021

The Citrix Application Delivery Management (Citrix ADM) release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release.

The Citrix Application Delivery Manager (ADM) agents are, by default, automatically upgraded to Citrix ADM latest build. You can view the agent details on the **Infrastructure > Instances > Agents** page. You can also specify the time when you want the agent upgrades to happen. For more information, see Configuring Agent Upgrade Settings.

Publication Date	Version
October 26, 2021	Release notes version 1.0
October 14, 2021	Release notes version 1.0
September 29, 2021	Release notes version 1.0
September 15, 2021	Release notes version 1.0
September 06, 2021	Release notes version 1.0
August 20, 2021	Release notes version 1.0
July 27, 2021	Release notes version 1.0
July 19, 2021	Release note version: 2.0
July 01, 2021	Release note version: 1.0
June 08, 2021	Release note version: 1.0
May 17, 2021	Release note version: 1.0

Publication Date	Version
April 27, 2021	Release note version: 1.0
Previous Releases	Release note version: 1.0

Release Notes for Citrix ADM service Oct 26, 2021 Release

October 27, 2021

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build Oct 26, 2021.

Notes

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

What's New

The enhancements and changes that are available in Build Oct 26, 2021.

Analytics

A unified process to enable analytics on virtual servers

Apart from the existing process to enable analytics, you can now 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.

For more information, see A unified process to enable analytics on virtual servers.

[NSADM-74747]

Improvements to application slowness in Web Insight

In **Applications > Web Insight**, when you drill down an application from the **Applications with Response Time Anomalies** metric, the **Client Network Latency** and **Server Network Latency** now enables you to view:

- A search bar - Click the search bar to view the IP address of all clients (in Client Network Latency) and servers (in Server Network Latency). You can select the IP address to filter the results.
- An export option - Click **Download CSV** to export the details in CSV format.

For more information, see Analyze the root cause for application slowness

[NSADM-71521]

StyleBooks

StyleBooks meta-properties support expressions

Meta-properties define the actions to be taken on ADC objects. You can now specify expressions for a meta-property. These expressions dynamically apply the valid meta-property actions for ADC objects. Earlier, the meta-property action was only able to take static values.**Example**:

```
parameters: -
 name: meta-action-lbvserver
 type: string
 default: disable

components:  -
 name: c1
 type: ns::lbvserver
 meta-properties:  action: $parameters.meta-action-lbvserver
 properties:  name: $parameters.lbvserver
 ipv46: $parameters.ip
 port: 80
 servicetype: HTTP

 <!--NeedCopy-->
```

In this example, a StyleBook user can specify a valid meta property action while creating a configuration pack.

StyleBook supports these meta property actions - `enable`, `disable`, `link`, `unlink`, **`import`**, `export`, `create`, `archive`, and `apply`.

[NSADM-77230]

Release Notes for Citrix ADM service Oct 14, 2021 Release

October 26, 2021

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build Oct 14, 2021.

Notes

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

What's New

The enhancements and changes that are available in Build Oct 14, 2021.

Management and Monitoring

Buy ADM virtual server licenses from the ADM GUI

You can now use the ADM GUI to buy ADM virtual server licenses from Microsoft Azure cloud. Select **Buy ADM License** from the navigation menu. Alternatively, you can navigate to **Settings > Licensing & Analytics** and select **Buy ADM License**. Earlier, to buy the server license, you had to visit Citrix Cloud or contact Technical Support. For more information, see Buy ADM Licenses.

[NSADM-78172]

Changes to Citrix ADM express account

With Citrix ADM express account, you can now avail the following benefits:

- No limit to use configuration jobs and StyleBook configuration packs. Earlier, you were only able to use up to two configuration jobs and StyleBook configuration packs.
- View all discovered virtual servers in **Network Functions** and **Network Reporting**. Earlier, you were able to view only licensed virtual servers.

For more information, see Manage Citrix ADM resources using Express account.

[NSADM-76506]

Fixed Issues

The issues that are addressed in Build Oct 14, 2021.

Infrastructure

When you are monitoring many virtual servers, the Network Functions dashboard takes longer time to load or it becomes unresponsive.

[NSHELP-29274]

Release Notes for Citrix ADM service Sep 29, 2021 Release

October 26, 2021

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build Sep 29, 2021.

Notes

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

What's New

The enhancements and changes that are available in Build Sep 29, 2021.

Management and Monitoring

ADM service now supports maximum 50 instance backup files.

[NSADM-76475]

StyleBooks

StyleBooks support implicit typecasting of datatypes

When you use StyleBook expressions for different datatypes, the StyleBook engine now implicitly typecasts the output to an appropriate datatype. For example, if you do an add operation between 'string' and 'integer' types, the StyleBook engine sets the output datatype to 'string'.

[NSADM-77219]

Fixed Issues

The issues that are addressed in Build Sep 29, 2021.

Miscellaneous

- In **Web Insight**, the scheduled export option is temporarily disabled because the report appears blank.

  [NSADM-77966]

- ADM agent displays an error message "Invalid PEM key: Incorrect password", when you upload a password-protected certificate.

  [NSHELP-28983]

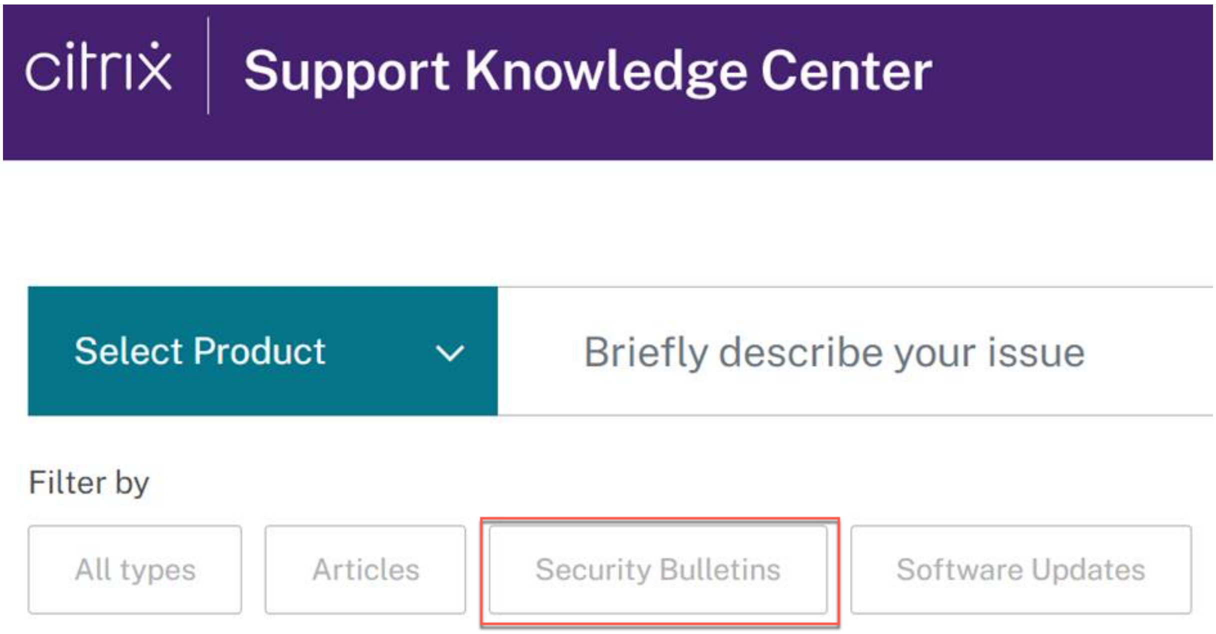
Release Notes for Citrix ADM service Sep 15, 2021 Release

September 27, 2021

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build Sep 15, 2021.

Notes

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin. To check security bulletins for a particular product, log on to `https://support.citrix.com/search##/`, select the product, and click **Security Bulletins**.



What's New

The enhancements and changes that are available in Build Sep 15, 2021.

StyleBooks

Some internal configuration packs and StyleBooks do not appear on the ADM GUI

If the default StyleBook has `type:apisec`, the StyleBook and its configuration packs do not appear on the ADM GUI. However, you can create configuration packs for such StyleBooks using their API.

[NSADM-77222]

Case-insensitive ADM StyleBooks

ADM StyleBooks now treats all the variables and parameters with uppercase and lowercase as the same.

[NSADM-64246]

Getting started

September 25, 2021

This document walks you through how to get started with onboarding and setting up Citrix Application Delivery and Management for the first time. This document is intended for network and application administrators who manage Citrix network devices (Citrix ADC, SD-WAN WO, Citrix Gateway, Citrix Secure Web Gateway, and so on). Follow the steps in this document irrespective of the type of device you plan to manage using Citrix Application Delivery and Management.

Before you begin onboarding, make sure you review the browser requirements, the agent installation requirements, and the port requirements.

Step 1: Sign Up for Citrix Cloud

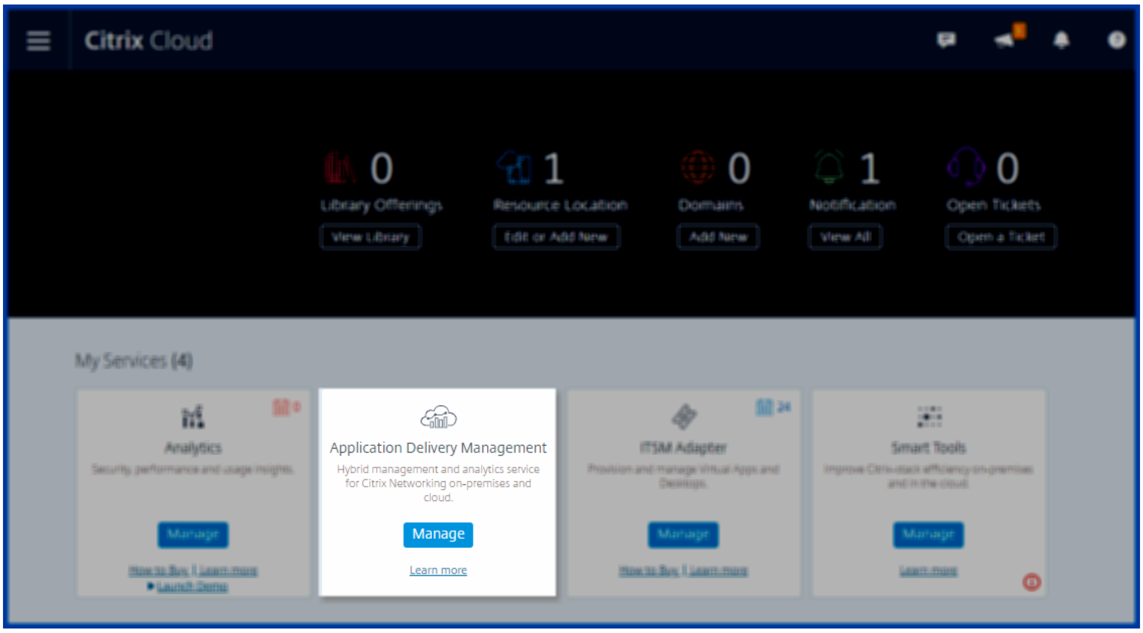
To start using Citrix Application Delivery and Management, you must first create a Citrix Cloud company account or join an existing one that someone else in your company has created. For detailed processes and instructions on how to proceed, see Signing Up for Citrix Cloud.

Step 2: Manage Citrix Application Delivery and Management with an Express account

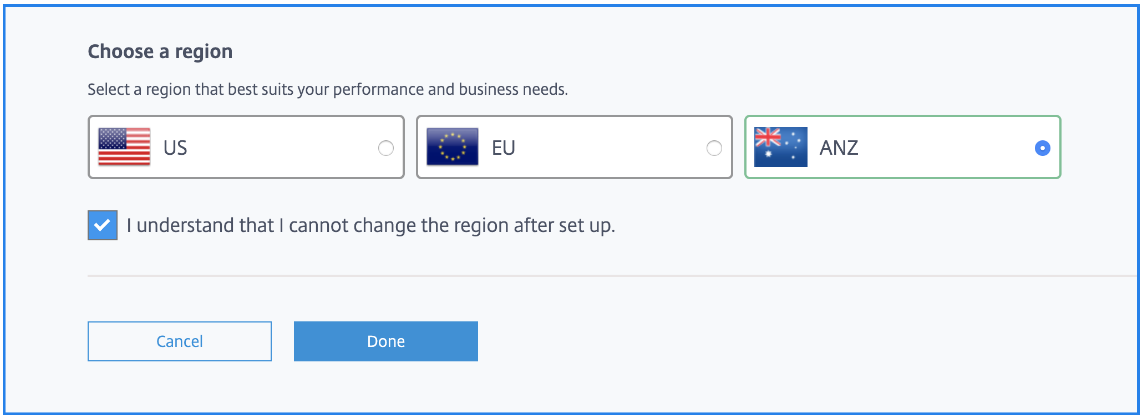
After you log on to Citrix Cloud, do the following:

1. Go to the **Available Services** section.
2. On the **Application Delivery Management** tile, click **Manage**.

   The **Application Delivery Management** tile moves to the **My Services** section.



3. Select one of the following regions that suits your business need:
   - United States (US)
   - Europe (EU)
   - Australia (ANZ)



Choose a region

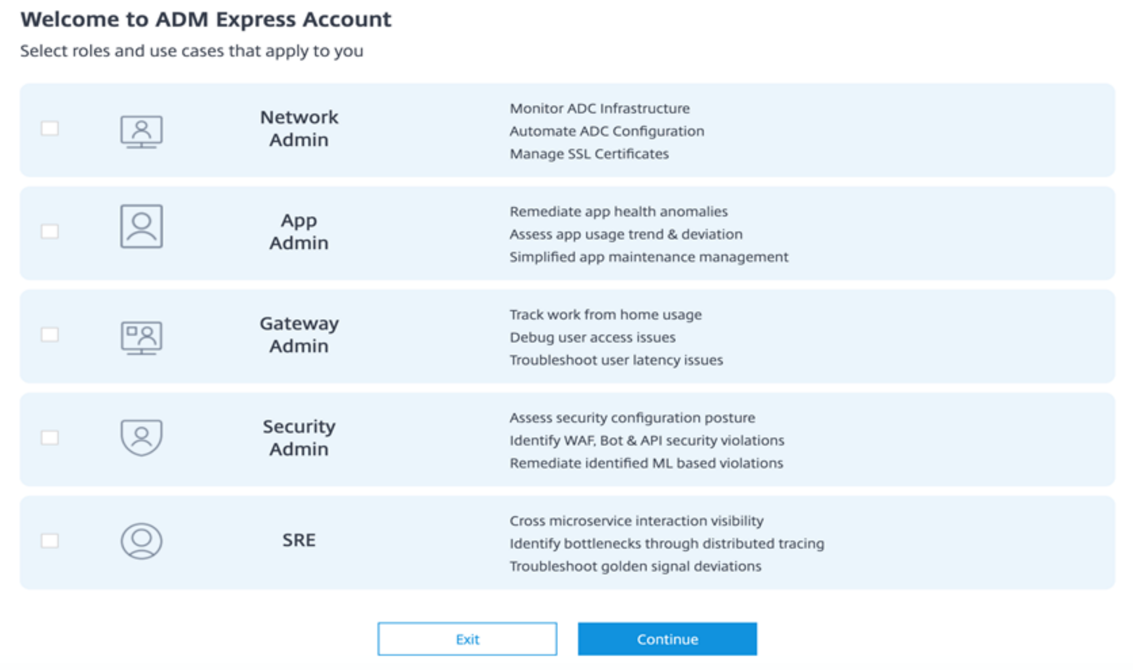
Select a region that best suits your performance and business needs.

US ○ EU ○ ANZ ●

☑ I understand that I cannot change the region after set up.

> **Important**
>
> You cannot change the region later.

4. Select roles and use cases that apply to you.



Welcome to ADM Express Account

Select roles and use cases that apply to you

□ Network Admin
- Monitor ADC Infrastructure
- Automate ADC Configuration
- Manage SSL Certificates

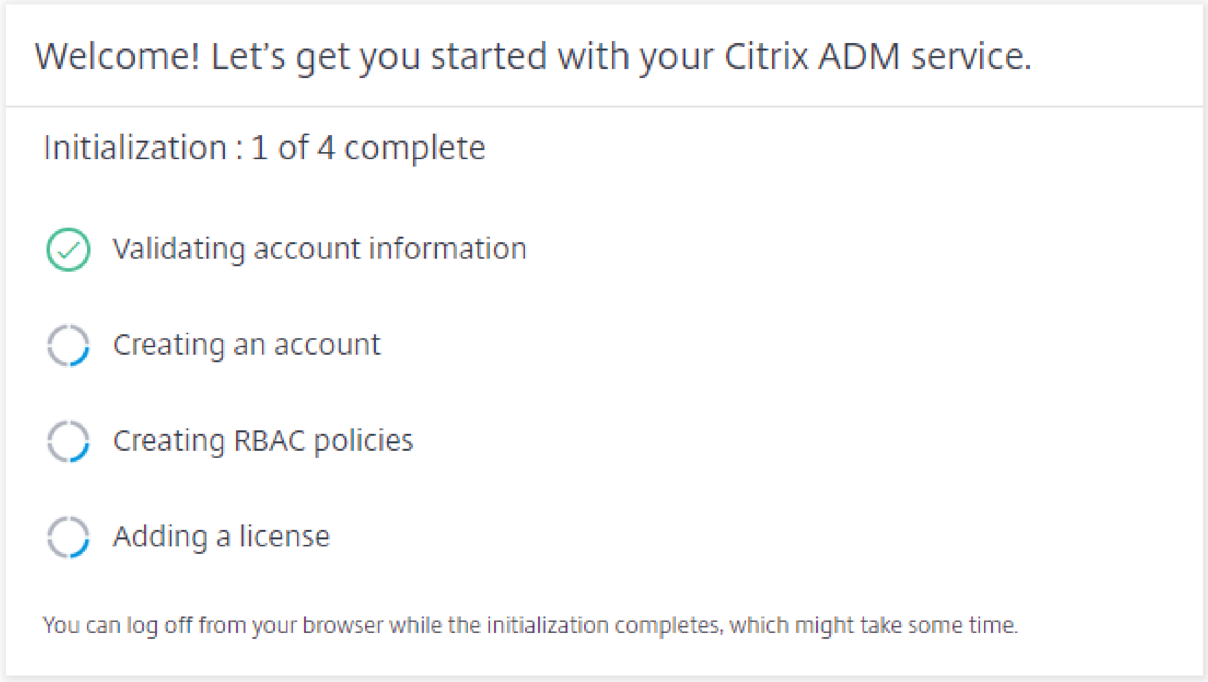
□ App Admin
- Remediate app health anomalies
- Assess app usage trend & deviation
- Simplified app maintenance management

□ Gateway Admin
- Track work from home usage
- Debug user access issues
- Troubleshoot user latency issues

□ Security Admin
- Assess security configuration posture
- Identify WAF, Bot & API security violations
- Remediate identified ML based violations

□ SRE
- Cross microservice interaction visibility
- Identify bottlenecks through distributed tracing
- Troubleshoot golden signal deviations

You can log off from the browser while the initialization completes in the background, which might take some time.



Welcome! Let's get you started with your Citrix ADM service.

Initialization : 1 of 4 complete

✓ Validating account information

○ Creating an account

○ Creating RBAC policies

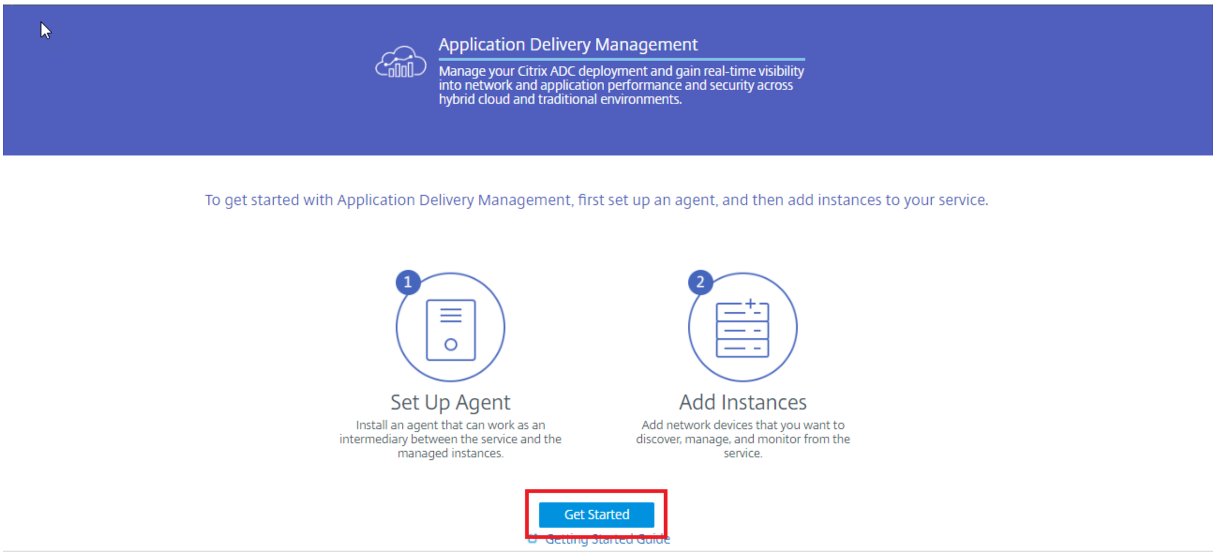
○ Adding a license

You can log off from your browser while the initialization completes, which might take some time.

> **Note**
>
> Citrix assigns an Express account to manage Citrix Application Delivery and Management resources. If your Citrix Application Delivery and Management Express account remains inactive for 90 days, the account gets deleted. For more information, see Manage Citrix Application

> Delivery and Management using Express account.

When you log back on to your Citrix Cloud account, the **Citrix Application Delivery and Management GUI** screen appears. Click **Get Started** to begin setting up the service for the first time.



Application Delivery Management

Manage your Citrix ADC deployment and gain real-time visibility into network and application performance and security across hybrid cloud and traditional environments.

To get started with Application Delivery Management, first set up an agent, and then add instances to your service.

1 Set Up Agent

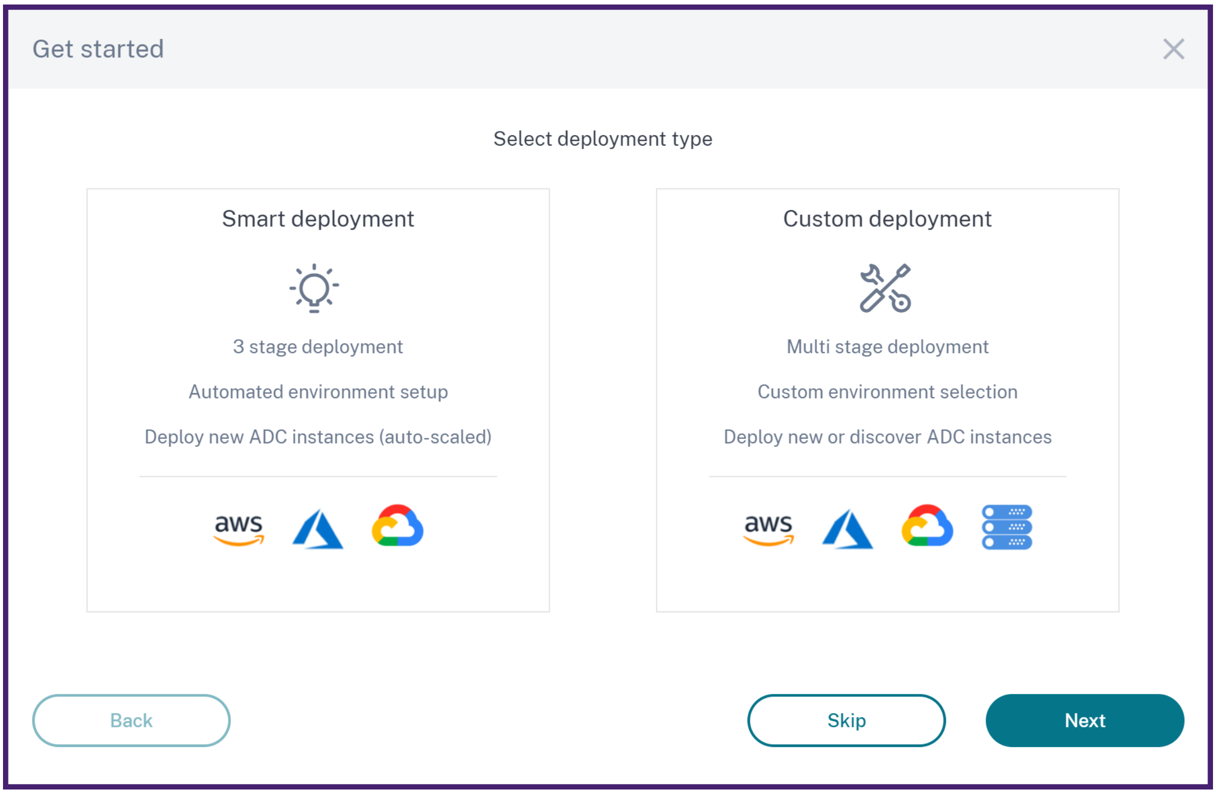
Install an agent that can work as an intermediary between the service and the managed instances.

2 Add Instances

Add network devices that you want to discover, manage, and monitor from the service.

Step 3: Select an ADC deployment type

Select one of the following deployment options that suits your business requirement:



Get started

Select deployment type

Smart deployment

3 stage deployment

Automated environment setup

Deploy new ADC instances (auto-scaled)

Custom deployment

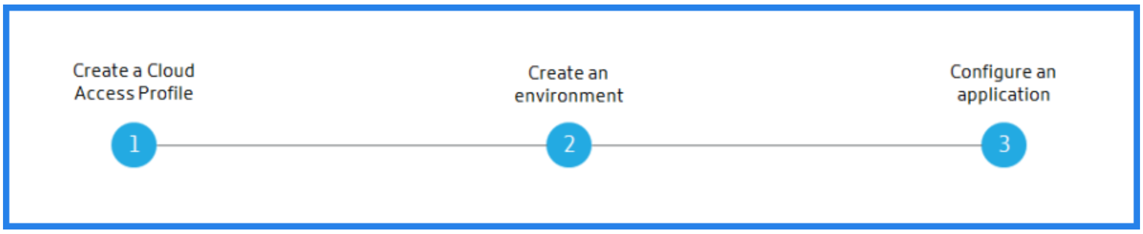
Multi stage deployment

Custom environment selection

Deploy new or discover ADC instances

- **Smart deployment** - This option is an automated environment setup to deploy new ADC instances. It automatically installs an agent to enable communication between the Citrix Application Delivery and Management and the managed instances.

  This option supports AWS, Microsoft Azure, and Google Cloud environments. In three steps, you can deliver an application that is present in the cloud using ADC instances.

- **Custom deployment** - This option is a multi-stage deployment. You can select each environment option and deploy or discover ADC instances.

Select smart deployment for AWS

This deployment option creates the following infrastructure in AWS:

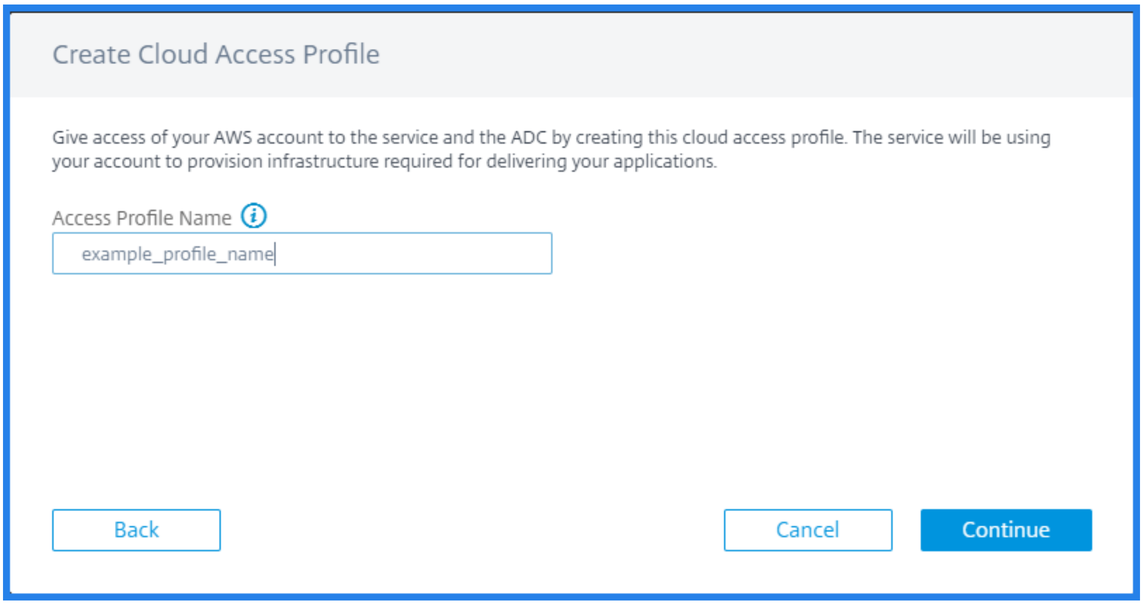
- A CloudFormation stack in AWS to create the required infrastructure that includes subnets, security groups, NAT gateways, and so on.
- An Citrix Application Delivery and Management Agent in the VPC to manage ADC instances.
- An ADC Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

Before deploying ADC instances, ensure the following:

1. You already possess an AWS account.
2. You have created an IAM user with all administrative permissions.

To deploy ADC instances, perform the following steps:

1. In **Create Cloud Access profile**, select **AWS** as a deployment environment. Specify **Access Profile Name** and **Role ARN** to create a Cloud Access Profile.

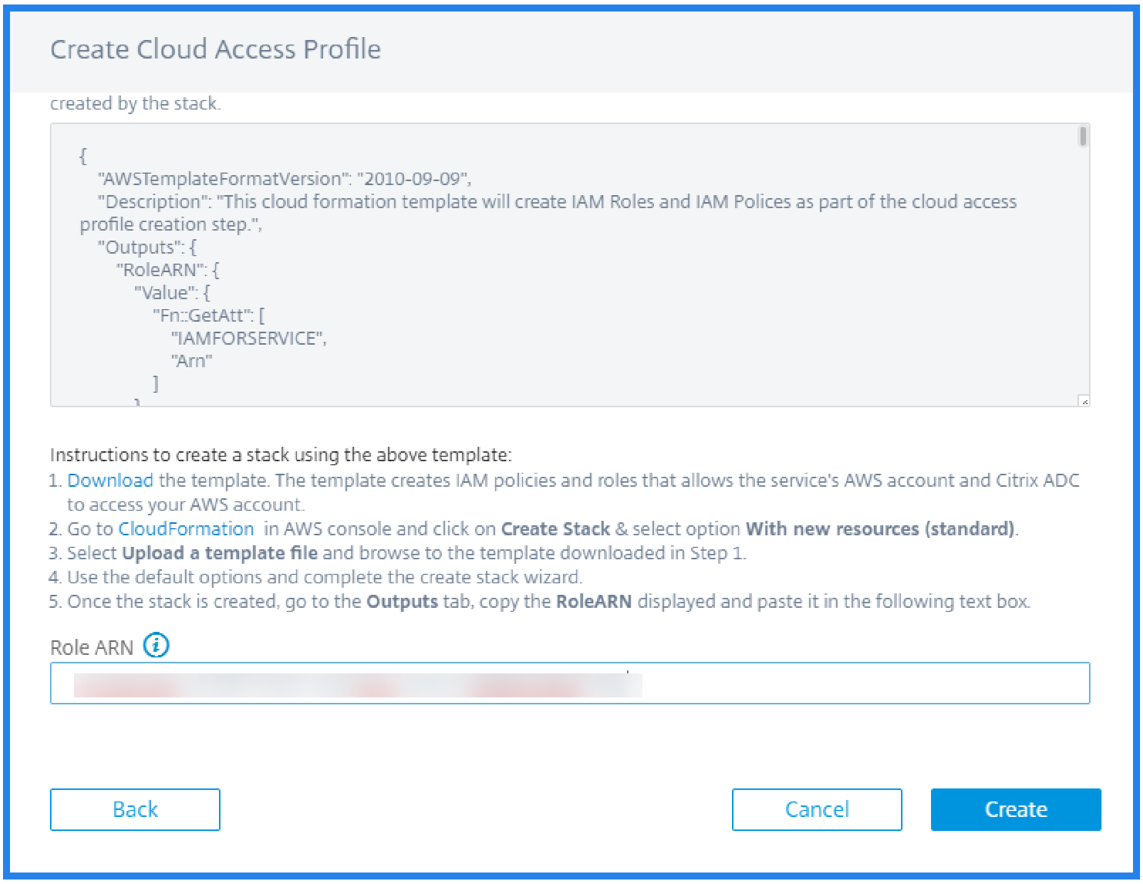


Create Cloud Access Profile

Give access of your AWS account to the service and the ADC by creating this cloud access profile. The service will be using your account to provision infrastructure required for delivering your applications.

Access Profile Name ⓘ

example_profile_name



Create Cloud Access Profile

created by the stack.

```
{
   "AWSTemplateFormatVersion": "2010-09-09",
   "Description": "This cloud formation template will create IAM Roles and IAM Polices as part of the cloud access
profile creation step.",
   "Outputs": {
      "RoleARN": {
         "Value": {
            "Fn::GetAtt": [
               "IAMFORSERVICE",
               "Arn"
            ]
```

Instructions to create a stack using the above template:

1. Download the template. The template creates IAM policies and roles that allows the service's AWS account and Citrix ADC to access your AWS account.
2. Go to CloudFormation in AWS console and click on **Create Stack** & select option **With new resources (standard)**.
3. Select **Upload a template file** and browse to the template downloaded in Step 1.
4. Use the default options and complete the create stack wizard.
5. Once the stack is created, go to the **Outputs** tab, copy the **RoleARN** displayed and paste it in the following text box.

Role ARN ⓘ

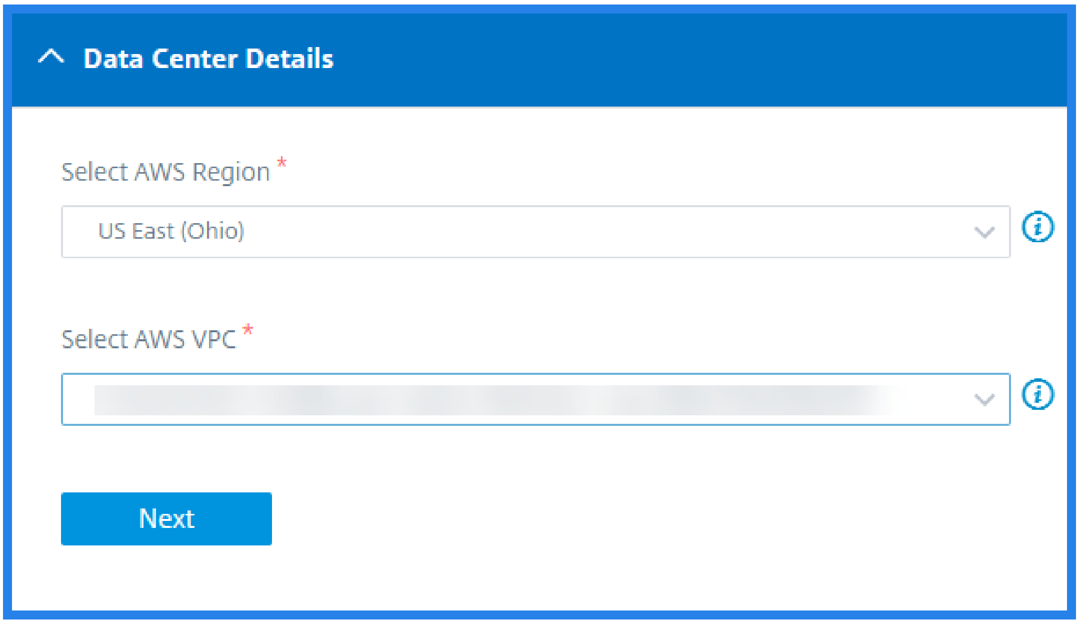
[redacted]

The Citrix Application Delivery and Management uses the Cloud Access Profile to access an AWS account.

2. Specify the following details to prepare the AWS environment:

   a) In **Data Center Details**, select **AWS Region** and **AWS VPC** where you want to deploy ADC instances.

AWS VPC lists the VPCs present in the selected **AWS Region**.



Data Center Details

Select AWS Region *

US East (Ohio)

Select AWS VPC *

b) In **ADC AutoScale Group Details**, specify the following to Autoscale ADC instances in the AWS cloud:

- **AutoScale Group Name** - A name to identify an Autoscale group.
- **Availability Zones** - Select the zones in which you want to create the Autoscale groups.

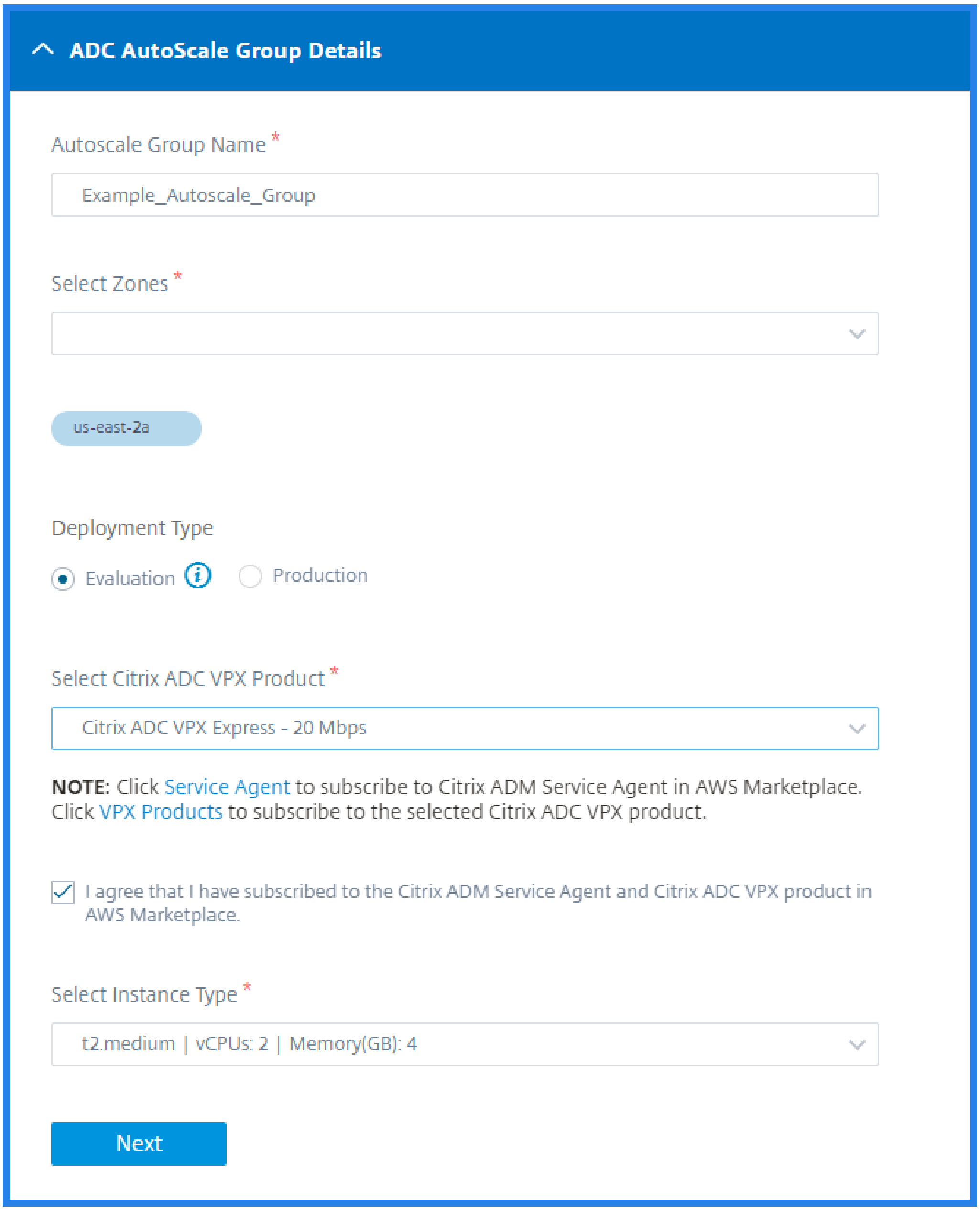
  You can select multiple zones from the list.
- **Deployment Type** - Select either **Evaluation** or **Production** option.

  If you want to evaluate the Citrix Application Delivery and Management Autoscale solution before purchasing the production license, select the **Evaluation** option.

  > **Important**
  >
  > - The evaluation option supports only one availability zone.
  > - With the evaluation option, you can select only Citrix ADC VPX Express. And, the Citrix Application Delivery and Management Autoscale solution can scale up to three ADC instances.
- **Citrix ADC VPX product** - Select licenses to provision ADC instances.

  Subscribe to the selected license in the AWS marketplace and return to this page.

  Review and select the user consent message.
- **Instance type** - Select the required instance type.



ADC AutoScale Group Details

Autoscale Group Name *

Example_Autoscale_Group

Select Zones *

us-east-2a

Deployment Type

● Evaluation ○ Production

Select Citrix ADC VPX Product *

Citrix ADC VPX Express - 20 Mbps

NOTE: Click Service Agent to subscribe to Citrix ADM Service Agent in AWS Marketplace. Click VPX Products to subscribe to the selected Citrix ADC VPX product.

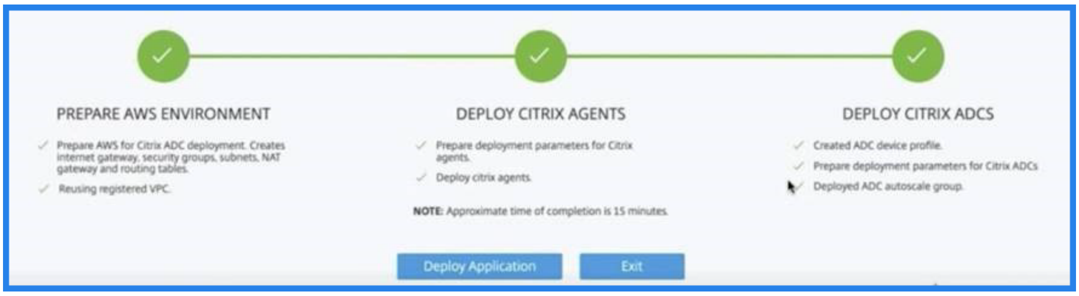
☑ I agree that I have subscribed to the Citrix ADM Service Agent and Citrix ADC VPX product in AWS Marketplace.

Select Instance Type *

t2.medium | vCPUs: 2 | Memory(GB): 4

c) Click **Next**.

After successful validation, click **Create** to deploy ADC instances in AWS and create an Autoscale group.



PREPARE AWS ENVIRONMENT

- ✓ Prepare AWS for Citrix ADC deployment. Creates internet gateway, security groups, subnets, NAT gateway and routing tables.
- ✓ Reusing registered VPC.

DEPLOY CITRIX AGENTS

- ✓ Prepare deployment parameters for Citrix agents.
- ✓ Deploy citrix agents.

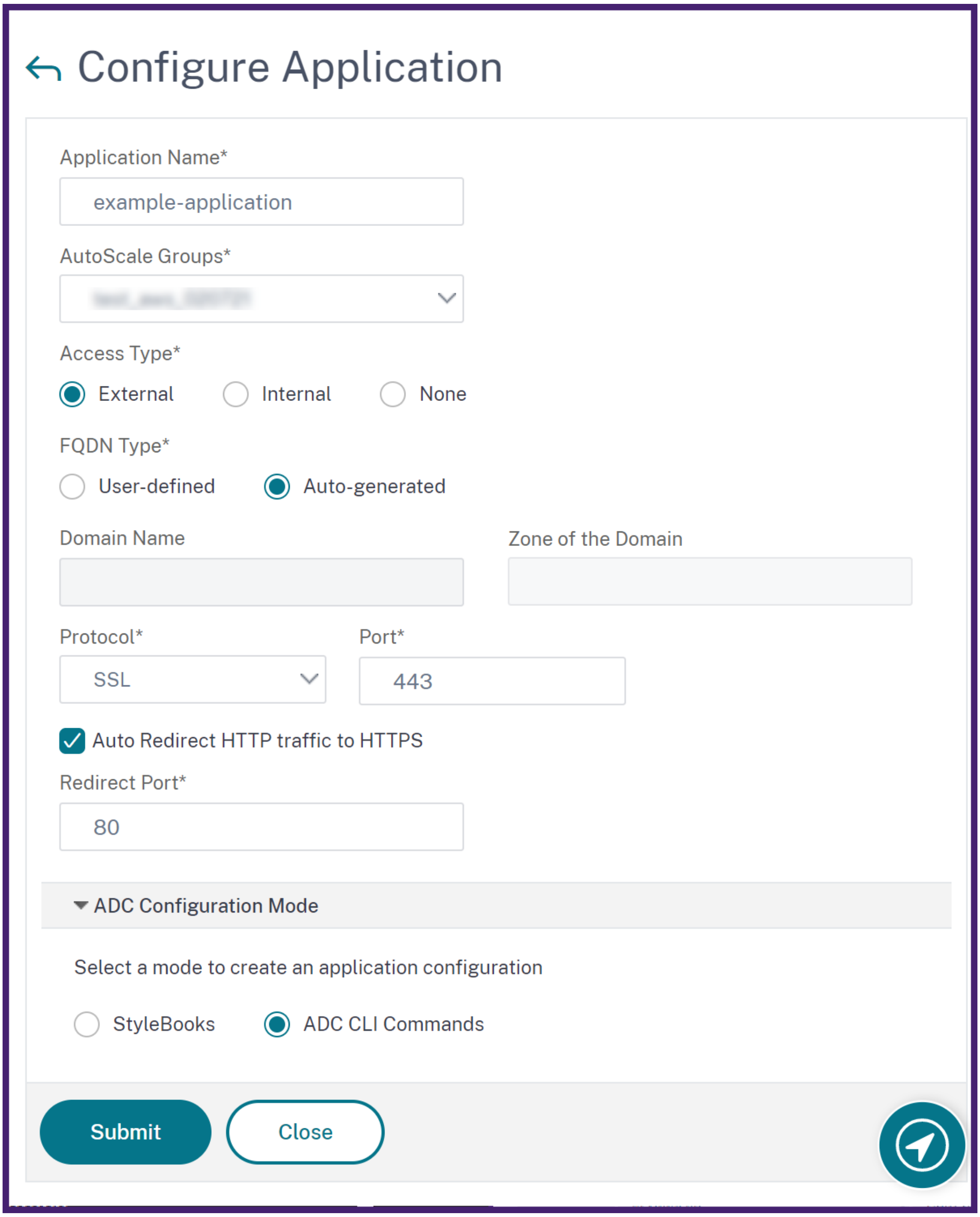
NOTE: Approximate time of completion is 15 minutes.

DEPLOY CITRIX ADCS

- ✓ Created ADC device profile.
- ✓ Prepare deployment parameters for Citrix ADCs
- ✓ Deployed ADC autoscale group.

3. After the successful ADC deployment, click **Deploy Application**.

   In **Configure Application**, specify the necessary details and click **Submit**.



Configure Application

Application Name*

example-application

AutoScale Groups*

[redacted]

Access Type*

● External ○ Internal ○ None

FQDN Type*

○ User-defined ● Auto-generated

Domain Name

Zone of the Domain

Protocol*

SSL

Port*

443

☑ Auto Redirect HTTP traffic to HTTPS

Redirect Port*

80

ADC Configuration Mode

Select a mode to create an application configuration

○ StyleBooks ● ADC CLI Commands

For more information, see Configure an application for the Autoscale group.

Select smart deployment for Microsoft Azure

This deployment option creates the following infrastructure in Azure:

- An Azure Resource Manager (ARM) template to create the required infrastructure that includes subnets, security groups, NAT gateways, and so on.

- An Citrix Application Delivery and Management Agent in the VPC to manage ADC instances.
- An ADC Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

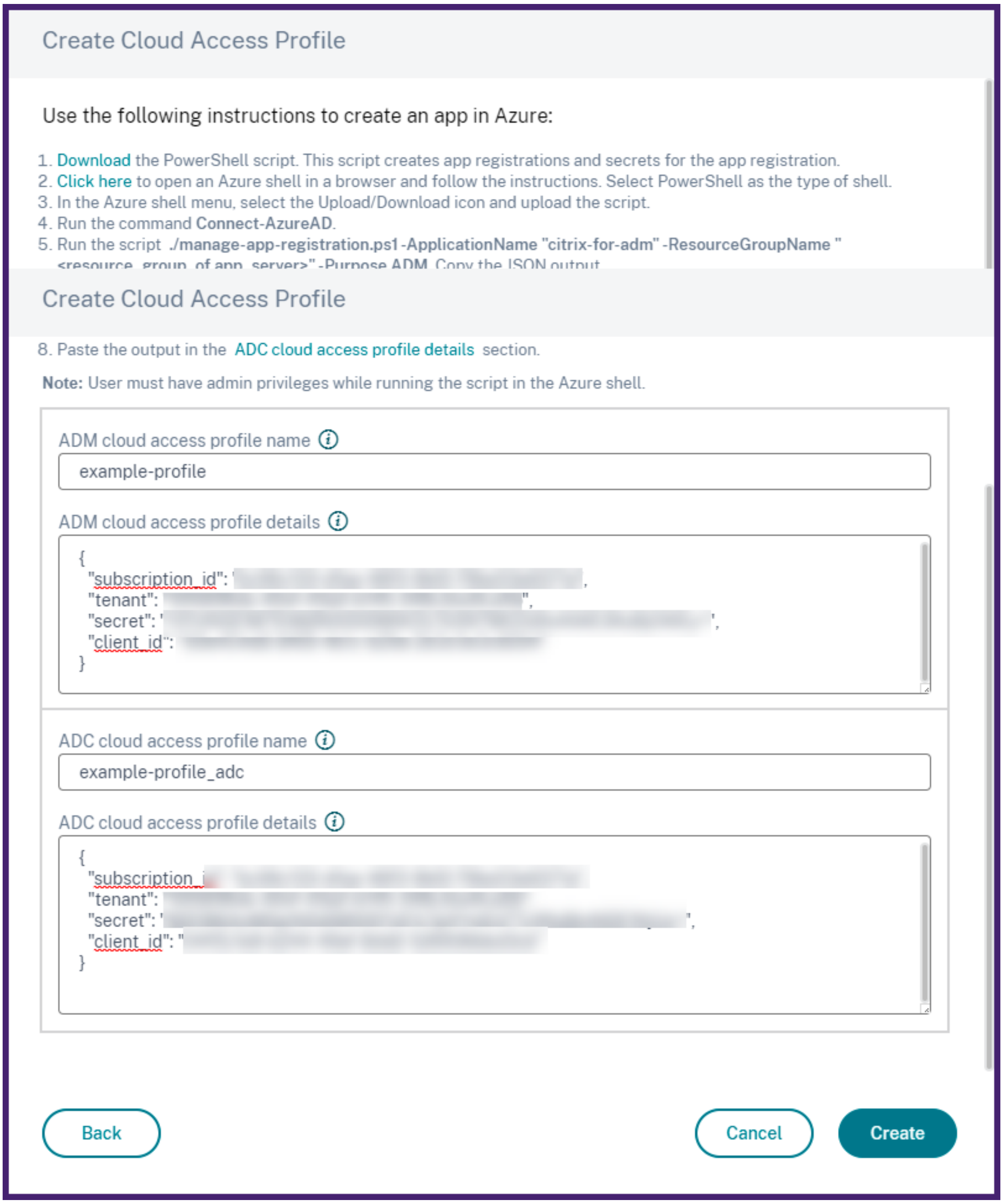
Before deploying ADC instances, ensure the following:

- You possess a Microsoft Azure account that supports the Azure Resource Manager deployment model.
- You have a resource group in Microsoft Azure.

For more information on how to create an account and other tasks, see Microsoft Azure Documentation.

To deploy ADC instances, perform the following steps:

1. In **Create Cloud Access profile**, select **Microsoft Azure** as a deployment environment. Specify Citrix Application Delivery and Management and ADC cloud access profile details.



Create Cloud Access Profile

Use the following instructions to create an app in Azure:

1. **Download** the PowerShell script. This script creates app registrations and secrets for the app registration.
2. **Click here** to open an Azure shell in a browser and follow the instructions. Select PowerShell as the type of shell.
3. In the Azure shell menu, select the Upload/Download icon and upload the script.
4. Run the command **Connect-AzureAD**.
5. Run the script **./manage-app-registration.ps1 -ApplicationName "citrix-for-adm" -ResourceGroupName "<resource_group_of app_server>" -Purpose ADM**. Copy the JSON output

Create Cloud Access Profile

8. Paste the output in the **ADC cloud access profile details** section.

Note: User must have admin privileges while running the script in the Azure shell.

ADM cloud access profile name: example-profile

ADM cloud access profile details:

```
{
 "subscription_id": [redacted],
 "tenant": [redacted]",
 "secret": [redacted]",
 "client_id": [redacted]
}
```

ADC cloud access profile name: example-profile_adc

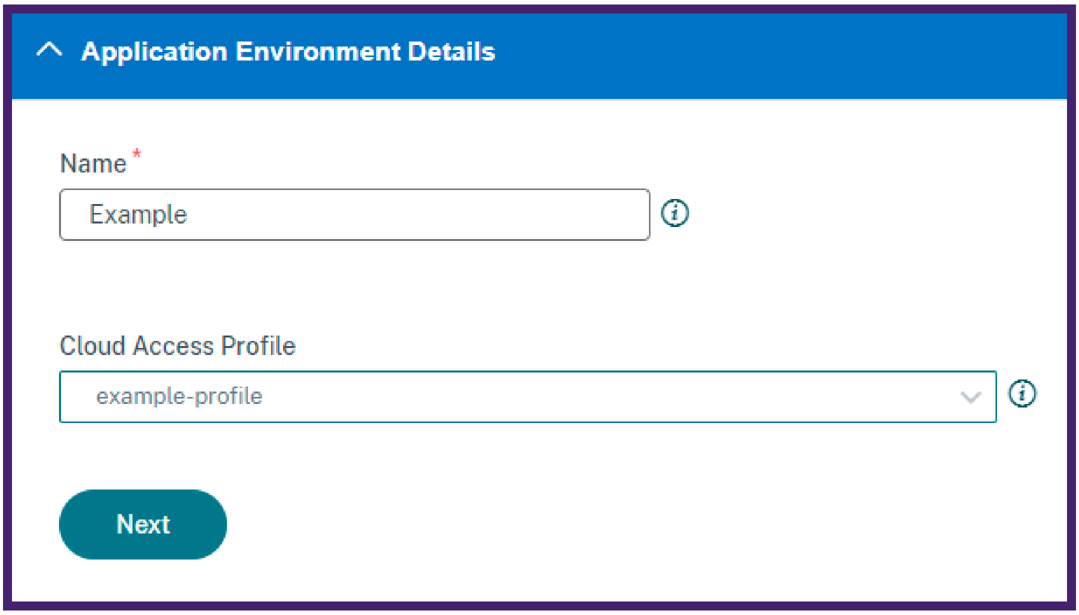
ADC cloud access profile details:

```
{
 "subscription_[redacted]
 "tenant": [redacted]
 "secret": [redacted]",
 "client_id": "[redacted]
}
```

The Citrix Application Delivery and Management uses the Citrix Application Delivery and Management Cloud Access Profile to access a Microsoft Azure account. And, an ADC Cloud Access Profile is used to provision ADC VPX instances.

2. Specify the following details to prepare the Azure environment:

   a) In **Application Environment Details**, specify a name for your deployment. And, ensure that the correct Cloud Access Profile is selected.



Application Environment Details

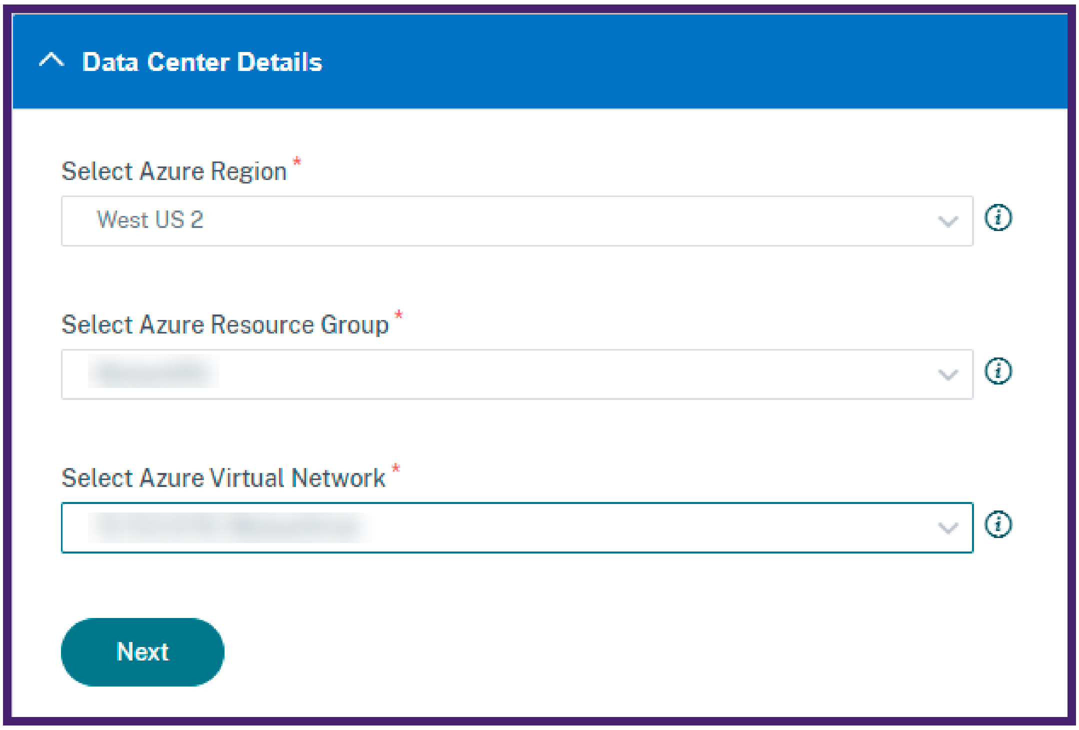
Name *

Example

Cloud Access Profile

example-profile

b) In **Data Center Details**, specify the region, resource group, and virtual network details where you want to deploy ADC instances.



Data Center Details

Select Azure Region *

West US 2

Select Azure Resource Group *

[redacted]

Select Azure Virtual Network *

[redacted]

c) In **ADC AutoScale Group Details**, specify the following:

- **Availability** - Select the availability zone or set in which you want to create the Autoscale groups. Depending on the cloud access profile that you have selected, availability zones appear on the list.
- **Deployment Type** - Select either **Evaluation** or **Production** option.

If you want to evaluate the Citrix Application Delivery and Management Autoscale solution before purchasing the production license, select the **Evaluation** option.

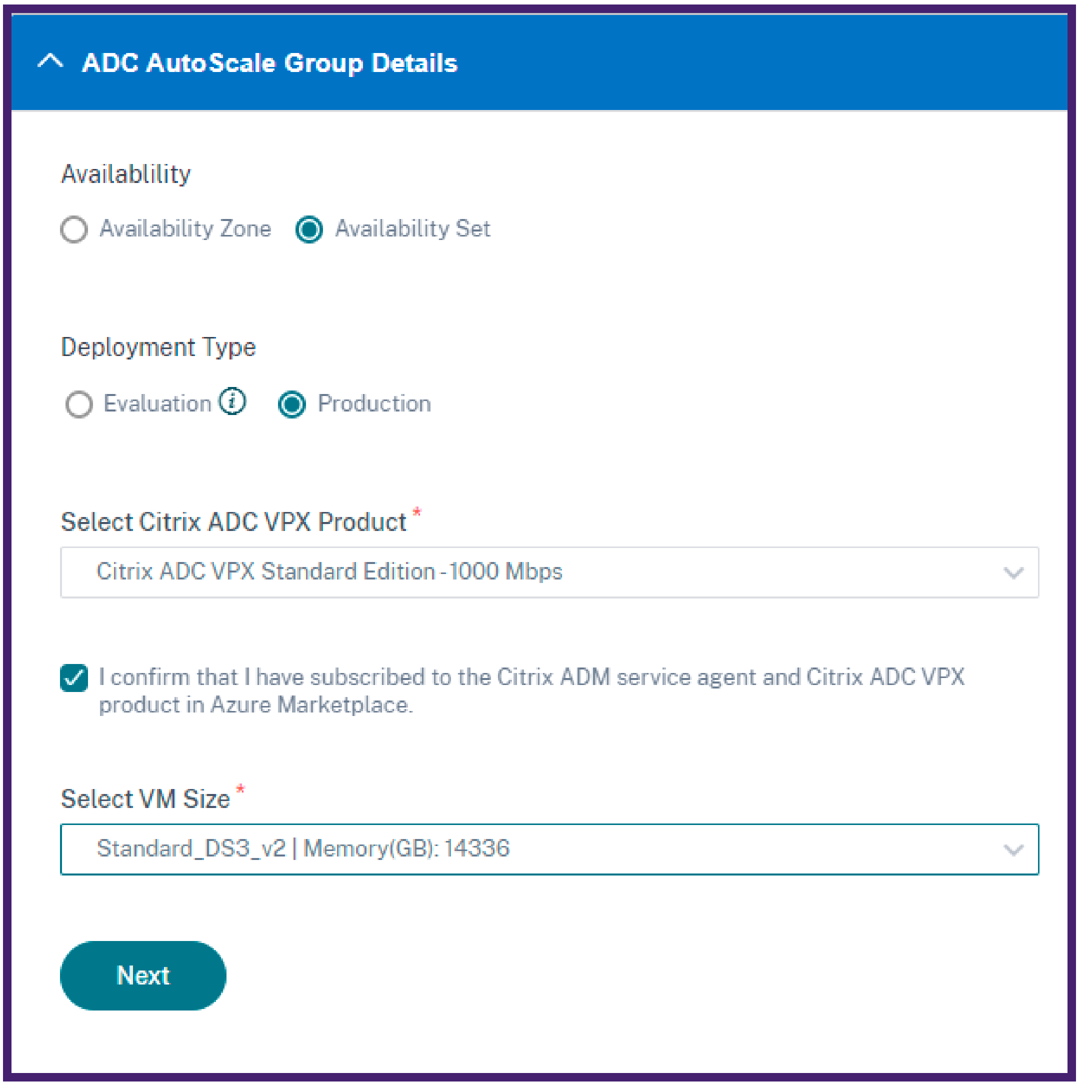
> **Important**
>
> - The evaluation option supports only one availability zone or set.
> - With the evaluation option, you can select only Citrix ADC VPX Express. And, the Citrix Application Delivery and Management Autoscale solution can scale up to three ADC instances.

- **Select Citrix ADC VPX product** - Select licenses to provision ADC instances.

  Subscribe to this Azure Marketplace license and return to the page.

  Review and select the user consent message.

- **Select VM size** - Select the required virtual machine size.



ADC AutoScale Group Details

Availablility

○ Availability Zone ● Availability Set

Deployment Type

○ Evaluation ● Production

Select Citrix ADC VPX Product *

Citrix ADC VPX Standard Edition - 1000 Mbps

☑ I confirm that I have subscribed to the Citrix ADM service agent and Citrix ADC VPX product in Azure Marketplace.

Select VM Size *

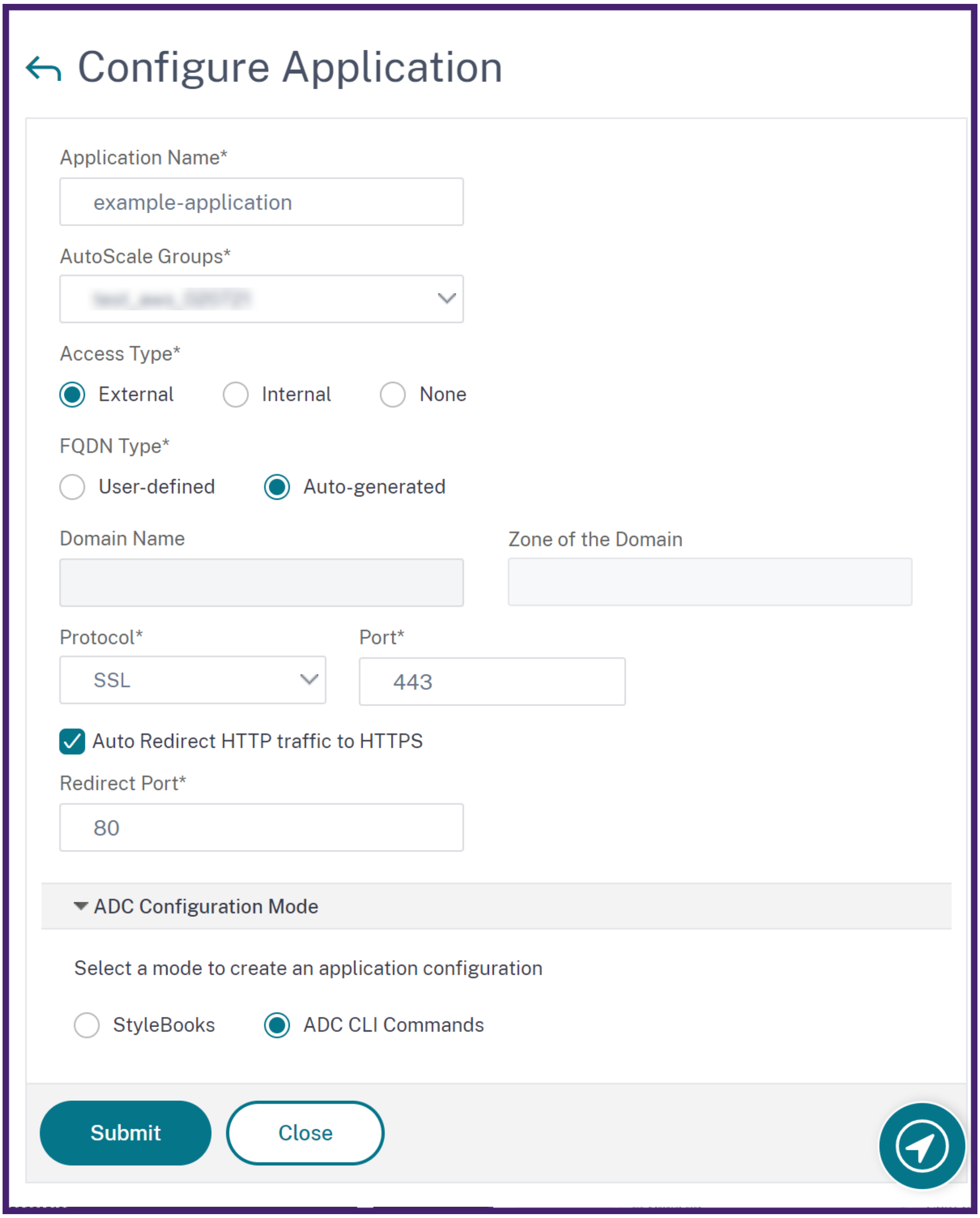
Standard_DS3_v2 | Memory(GB): 14336

d) Click **Next**.

After successful validation, click **Create** to deploy ADC instances in Microsoft Azure and create an Autoscale group.

3. After the successful ADC deployment, click **Deploy Application**.

   In **Configure Application**, specify the necessary details and click **Submit**.



Configure Application

Application Name*
example-application

AutoScale Groups*
[redacted]

Access Type*
● External ○ Internal ○ None

FQDN Type*
○ User-defined ● Auto-generated

Domain Name	Zone of the Domain

Protocol*	Port*
SSL	443

☑ Auto Redirect HTTP traffic to HTTPS

Redirect Port*
80

▾ ADC Configuration Mode

Select a mode to create an application configuration

○ StyleBooks ● ADC CLI Commands

For more information, see Configure an application for the Autoscale group.

Select smart deployment for Google Cloud

This deployment option creates the following infrastructure in Google Cloud:

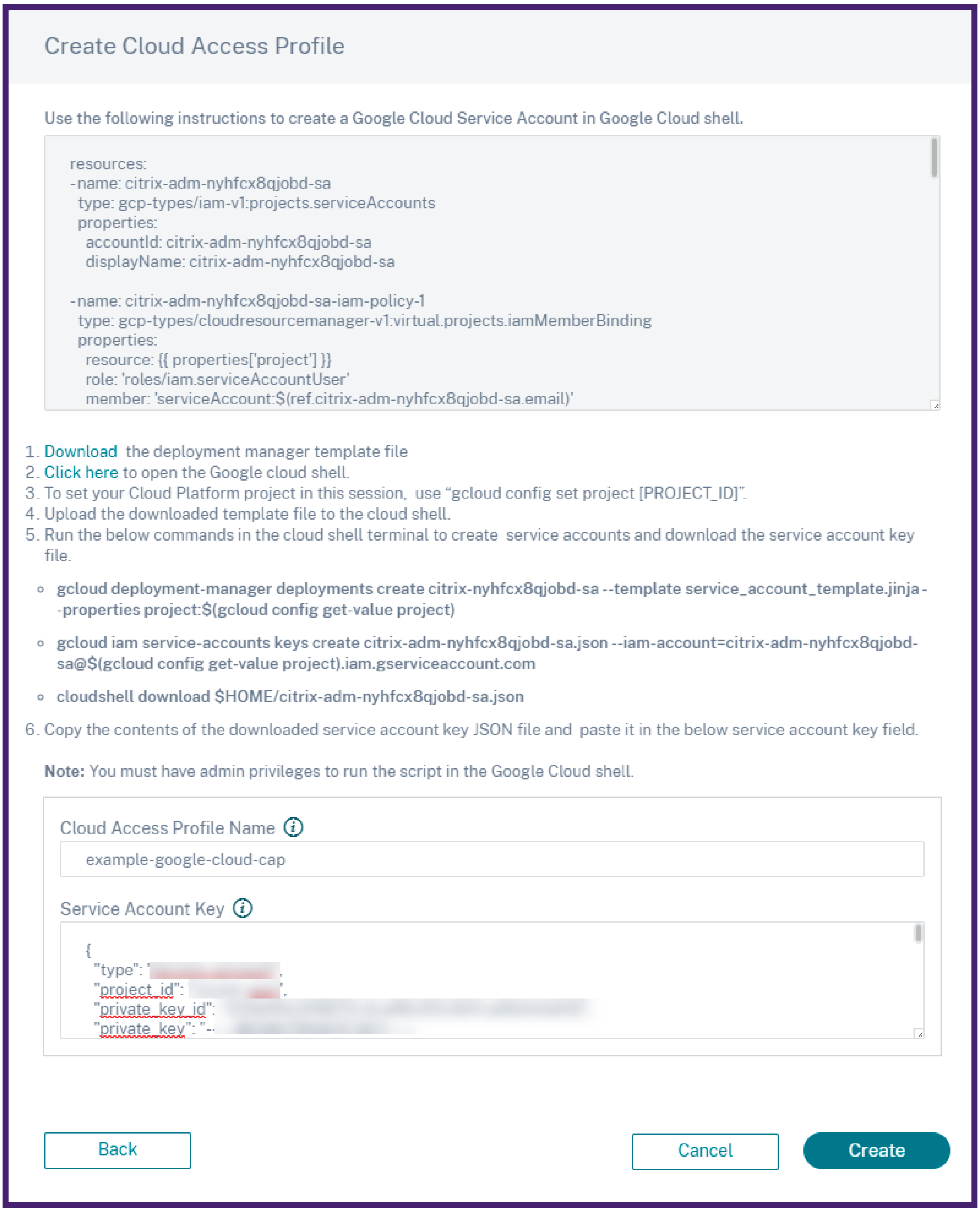
- A Google Cloud Deployment Manager to create the required infrastructure that includes VPC networks, subnets, Cloud NAT, Cloud Router gateways, and firewall rules.
- An Citrix Application Delivery and Management Agent in the VPC to manage ADC instances.
- An ADC Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

Before deploying ADC instances, ensure that you already possess a Google Cloud account. For more information on how to create an account, see Google Cloud Documentation.

To deploy ADC instances, perform the following steps:

1. In **Create Cloud Access profile**, select **Google Cloud** as a deployment environment.

   Specify **Cloud Access Profile Name** and **Service Account Key**.



Create Cloud Access Profile

Use the following instructions to create a Google Cloud Service Account in Google Cloud shell.

```
resources:
-name: citrix-adm-nyhfcx8qjobd-sa
 type: gcp-types/iam-v1:projects.serviceAccounts
 properties:
  accountId: citrix-adm-nyhfcx8qjobd-sa
  displayName: citrix-adm-nyhfcx8qjobd-sa

-name: citrix-adm-nyhfcx8qjobd-sa-iam-policy-1
 type: gcp-types/cloudresourcemanager-v1:virtual.projects.iamMemberBinding
 properties:
  resource: {{ properties['project'] }}
  role: 'roles/iam.serviceAccountUser'
  member: 'serviceAccount:$(ref.citrix-adm-nyhfcx8qjobd-sa.email)'
```

1. Download the deployment manager template file
2. Click here to open the Google cloud shell.
3. To set your Cloud Platform project in this session, use "gcloud config set project [PROJECT_ID]".
4. Upload the downloaded template file to the cloud shell.
5. Run the below commands in the cloud shell terminal to create service accounts and download the service account key file.
   - **gcloud deployment-manager deployments create citrix-nyhfcx8qjobd-sa --template service_account_template.jinja --properties project:$(gcloud config get-value project)**
   - **gcloud iam service-accounts keys create citrix-adm-nyhfcx8qjobd-sa.json --iam-account=citrix-adm-nyhfcx8qjobd-sa@$(gcloud config get-value project).iam.gserviceaccount.com**
   - **cloudshell download $HOME/citrix-adm-nyhfcx8qjobd-sa.json**
6. Copy the contents of the downloaded service account key JSON file and paste it in the below service account key field.

Note: You must have admin privileges to run the script in the Google Cloud shell.

Cloud Access Profile Name ⓘ

example-google-cloud-cap

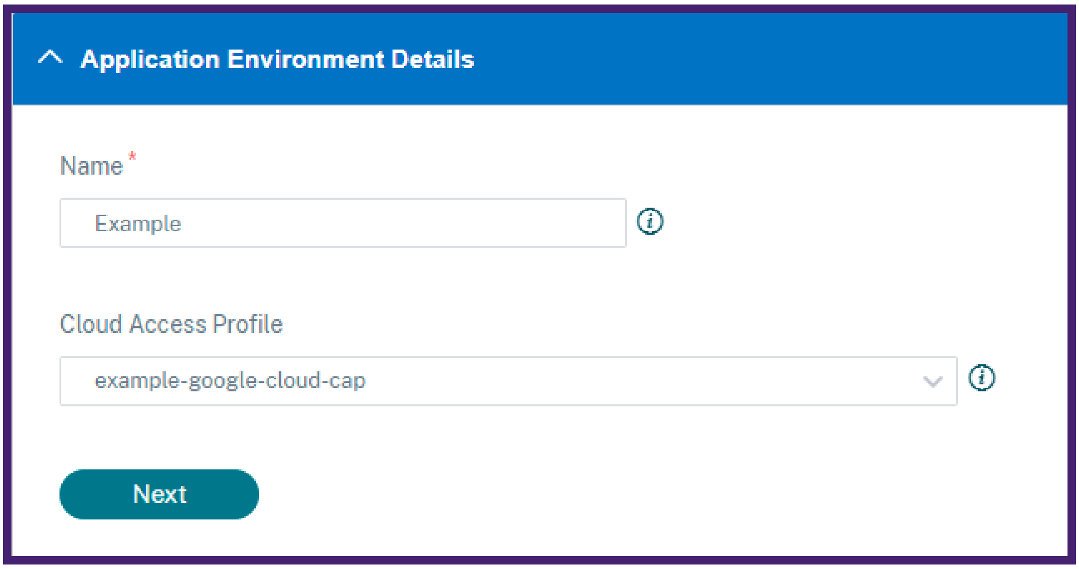
Service Account Key ⓘ

```
{
 "type": "[redacted]",
 "project_id": "[redacted]",
 "private_key_id": "[redacted]
 "private_key": "-[redacted]
```

The Citrix Application Delivery and Management uses the Cloud Access Profile to access a Google Cloud account.

2. Specify the following details to prepare the Google Cloud environment:

   a) In **Application Environment Details**, specify a name for your deployment. And, ensure that the correct Cloud Access Profile is selected.



Application Environment Details

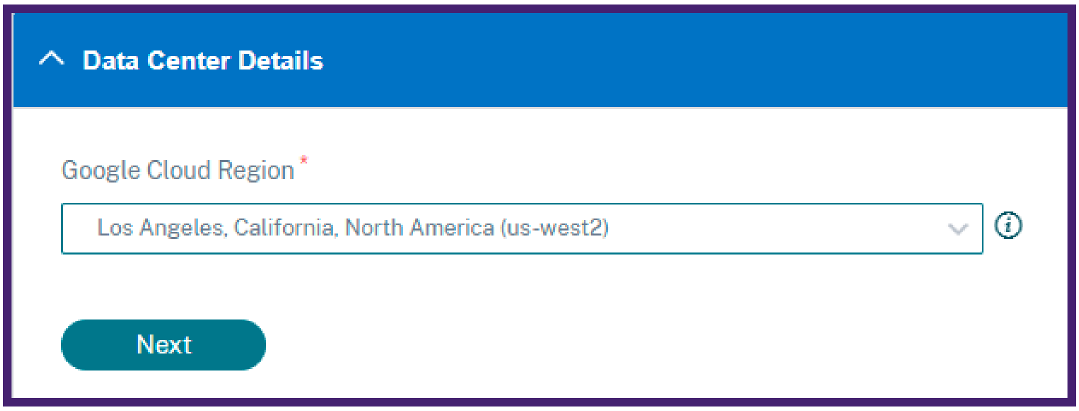
Name *

Example

Cloud Access Profile

example-google-cloud-cap

b) In **Data Center Details**, select **Google Cloud Region** where you want to deploy ADC instances.



Data Center Details

Google Cloud Region *

Los Angeles, California, North America (us-west2)

c) In **ADC AutoScale Group Details**, specify the following to Autoscale ADC instances in Google Cloud:

- **VPC Network's Subnet CIDR** - Specify a VPC network created for management, client, and server traffic. However, you can select the existing network for server.
- **Zones** - Select the zones in which you want to create the Autoscale groups.

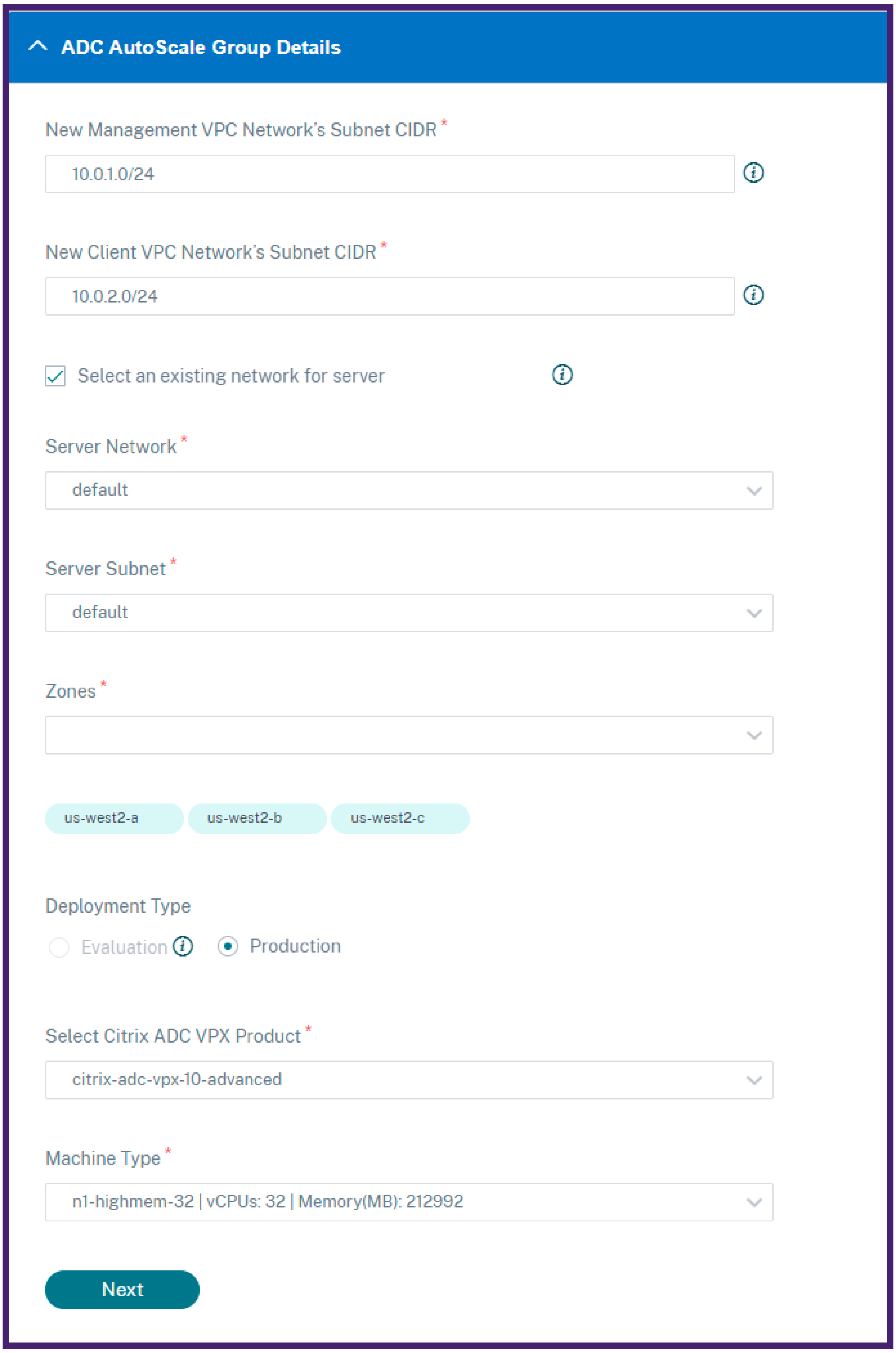
  You can select multiple zones from the list.
- **Deployment Type** - Select either **Evaluation** or **Production** option.

  If you want to evaluate the Citrix Application Delivery and Management Autoscale solution before purchasing the production license, select the **Evaluation** option.

  > **Important**
  >
  > – The evaluation option supports only one availability zone.

> - With the evaluation option, you can select only Citrix ADC VPX Express. And, the Citrix Application Delivery and Management Autoscale solution can scale up to three ADC instances.

- **Citrix ADC VPX product** - Select licenses to provision ADC instances.
- **Machine type** - Select the required instance type.



ADC AutoScale Group Details

New Management VPC Network's Subnet CIDR *

10.0.1.0/24

New Client VPC Network's Subnet CIDR *

10.0.2.0/24

☑ Select an existing network for server

Server Network *

default

Server Subnet *

default

Zones *

us-west2-a us-west2-b us-west2-c

Deployment Type

○ Evaluation ● Production

Select Citrix ADC VPX Product *

citrix-adc-vpx-10-advanced

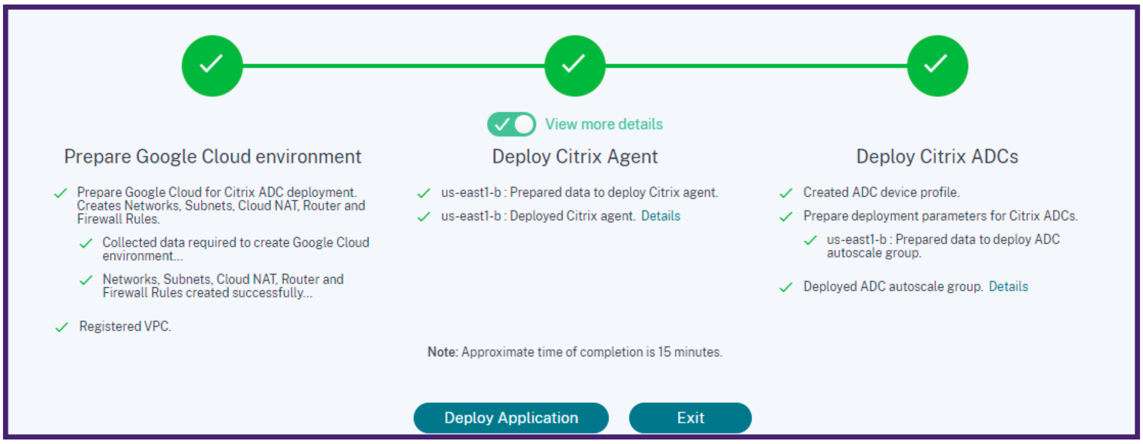
Machine Type *

n1-highmem-32 | vCPUs: 32 | Memory(MB): 212992

d) Click **Next**.

After successful validation, click **Create** to deploy ADC instances in Google Cloud and create an Autoscale group.

3. After the successful ADC deployment, click **Deploy Application**.



Prepare Google Cloud environment

- ✓ Prepare Google Cloud for Citrix ADC deployment. Creates Networks, Subnets, Cloud NAT, Router and Firewall Rules.
  - ✓ Collected data required to create Google Cloud environment...
  - ✓ Networks, Subnets, Cloud NAT, Router and Firewall Rules created successfully...
- ✓ Registered VPC.

Deploy Citrix Agent

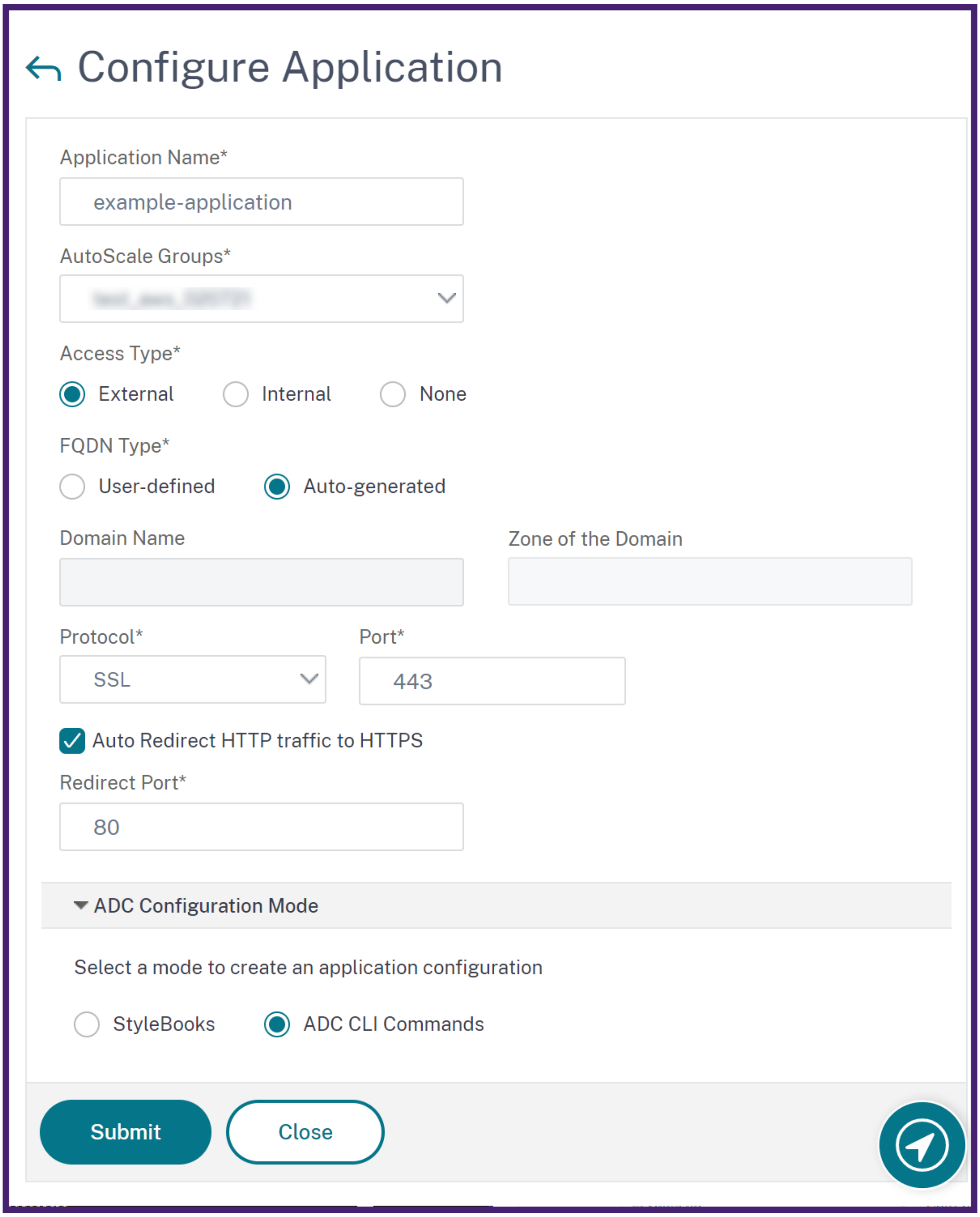
- ✓ us-east1-b : Prepared data to deploy Citrix agent.
- ✓ us-east1-b : Deployed Citrix agent. Details

Deploy Citrix ADCs

- ✓ Created ADC device profile.
- ✓ Prepare deployment parameters for Citrix ADCs.
  - ✓ us-east1-b : Prepared data to deploy ADC autoscale group.
- ✓ Deployed ADC autoscale group. Details

Note: Approximate time of completion is 15 minutes.

In **Configure Application**, specify the necessary details and click **Submit**.



Configure Application

Application Name*

example-application

AutoScale Groups*

[redacted]

Access Type*

● External ○ Internal ○ None

FQDN Type*

○ User-defined ● Auto-generated

Domain Name

Zone of the Domain

Protocol*: SSL

Port*: 443

☑ Auto Redirect HTTP traffic to HTTPS

Redirect Port*

80

ADC Configuration Mode

Select a mode to create an application configuration

○ StyleBooks ● ADC CLI Commands

For more information, see Configure an application for the Autoscale group.

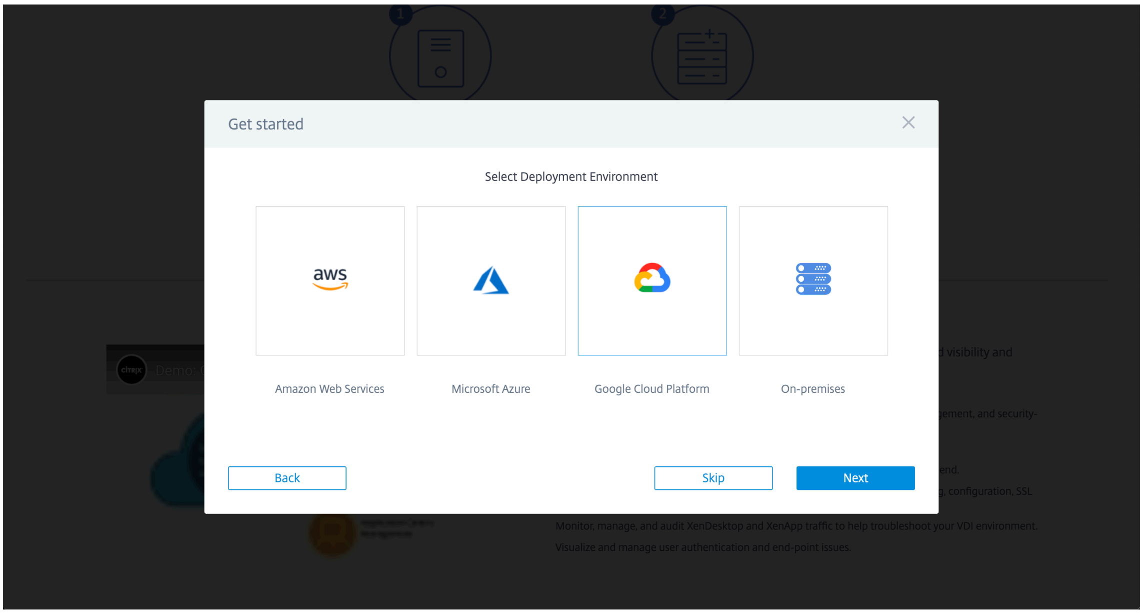
Select custom deployment

This option provides a multi stage deployment. Select this option to discover ADC instances from various environments. With this option, you can also deploy new instances by specifying custom environment options.

Perform the following steps to deploy or discover ADC instances:

1. Select any of the following environments:

   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - **On-premises**

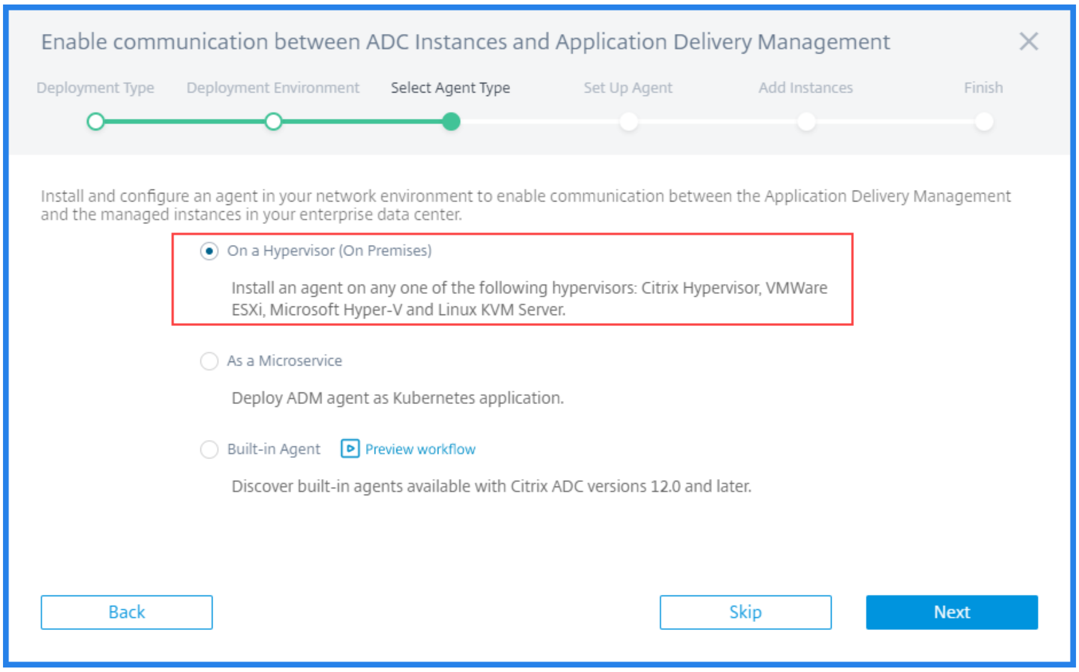
   

2. Install the Citrix Application Delivery and Management Agent to enable communication between the Citrix Application Delivery and Management and the managed instances in your data center or cloud.

   The **Select Agent Type** step varies the agent installation options depending on the selected environment.

   - **On-premises** - If you select **On-premises**, you can install an agent on the following hypervisors:

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



Enable communication between ADC Instances and Application Delivery Management

Install and configure an agent in your network environment to enable communication between the Application Delivery Management and the managed instances in your enterprise data center.

● On a Hypervisor (On Premises)

Install an agent on any one of the following hypervisors: Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V and Linux KVM Server.

○ As a Microservice

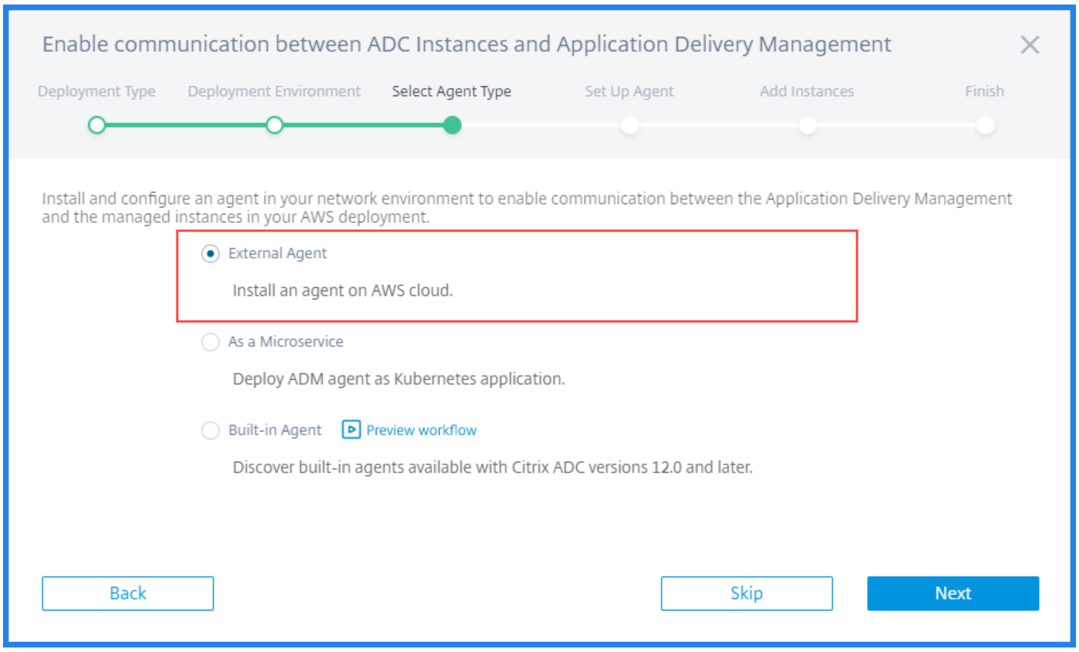
Deploy ADM agent as Kubernetes application.

○ Built-in Agent Preview workflow

Discover built-in agents available with Citrix ADC versions 12.0 and later.

- **Public clouds** - If you select **AWS**, **Microsoft Azure** or **Google Cloud Platform**, you can externally install an agent on the selected cloud.

  The following is an example image for the AWS environment.



Enable communication between ADC Instances and Application Delivery Management

Install and configure an agent in your network environment to enable communication between the Application Delivery Management and the managed instances in your AWS deployment.

● External Agent

Install an agent on AWS cloud.

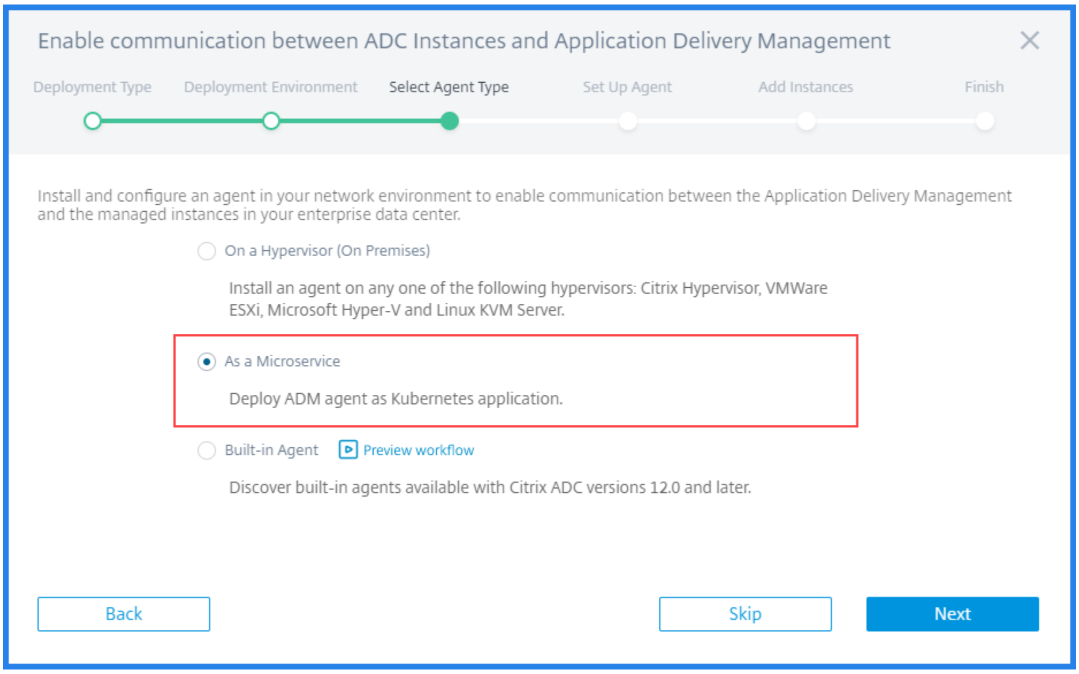
○ As a Microservice

Deploy ADM agent as Kubernetes application.

○ Built-in Agent Preview workflow

Discover built-in agents available with Citrix ADC versions 12.0 and later.

- **As a microservice** - To deploy an agent as a Kubernetes application.



Enable communication between ADC Instances and Application Delivery Management

Install and configure an agent in your network environment to enable communication between the Application Delivery Management and the managed instances in your enterprise data center.

○ On a Hypervisor (On Premises)

Install an agent on any one of the following hypervisors: Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V and Linux KVM Server.

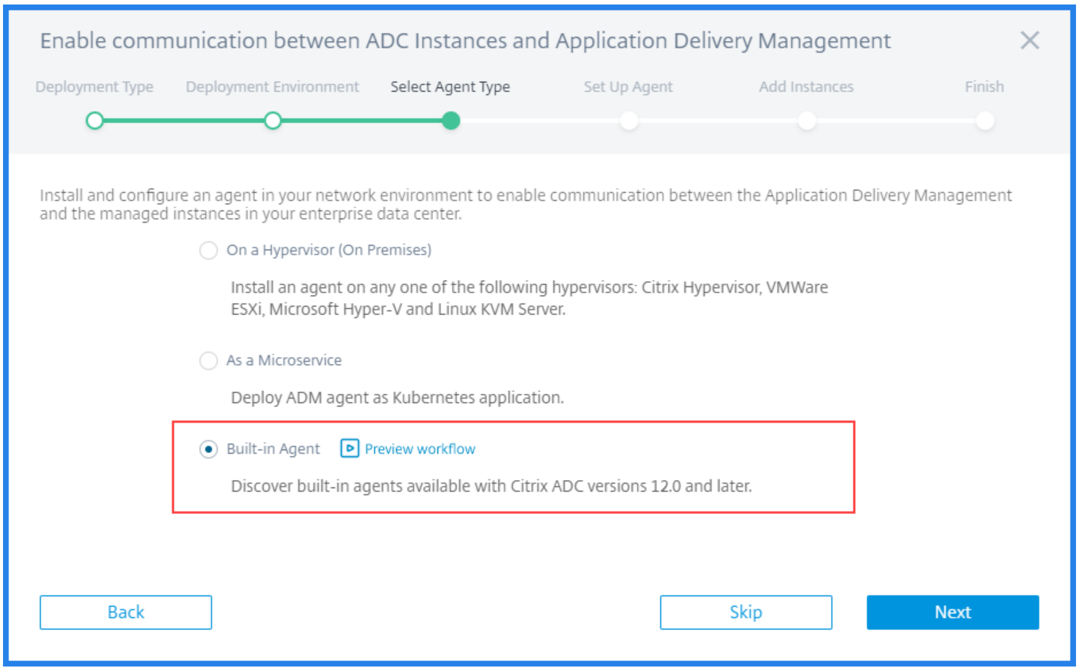
● As a Microservice

Deploy ADM agent as Kubernetes application.

○ Built-in Agent Preview workflow

Discover built-in agents available with Citrix ADC versions 12.0 and later.

- **Built-in agent** - To discover built-in agents available with Citrix ADC version 12.0 or later.



Enable communication between ADC Instances and Application Delivery Management

Install and configure an agent in your network environment to enable communication between the Application Delivery Management and the managed instances in your enterprise data center.

○ On a Hypervisor (On Premises)

Install an agent on any one of the following hypervisors: Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V and Linux KVM Server.

○ As a Microservice

Deploy ADM agent as Kubernetes application.

● Built-in Agent Preview workflow

Discover built-in agents available with Citrix ADC versions 12.0 and later.

3. Click **Next**

   Steps to install an agent vary for every option. The following links guide you to the specific steps to install an agent:

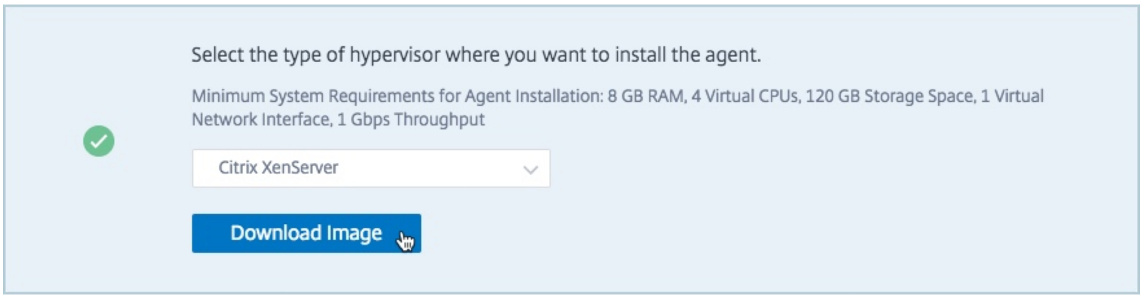
   - Hypervisor
   - External agent
   - As a microservice

- Built-in agent

Install an agent on a hypervisor

Perform the following steps to set up an Citrix Application Delivery and Management agent on a hypervisor:

1. Select the hypervisor and click **Download Image** to download the agent image to your local system.

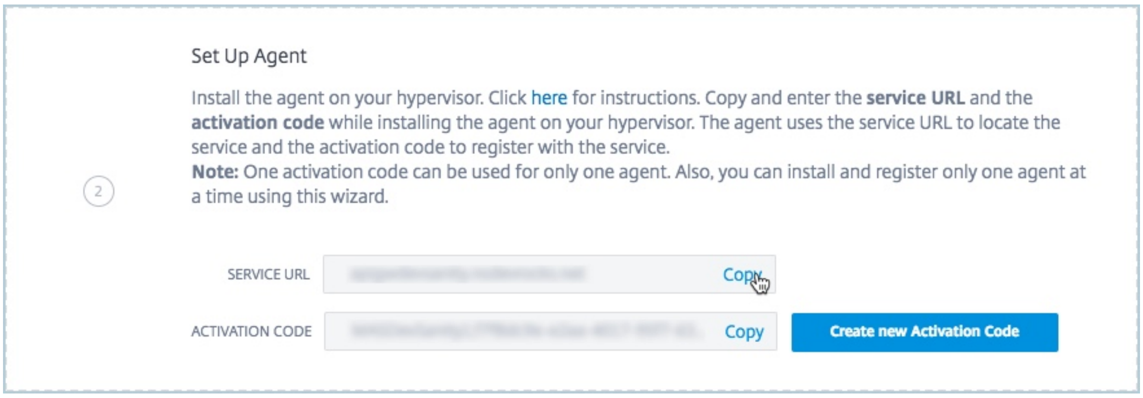
   

   Select the type of hypervisor where you want to install the agent.

   Minimum System Requirements for Agent Installation: 8 GB RAM, 4 Virtual CPUs, 120 GB Storage Space, 1 Virtual Network Interface, 1 Gbps Throughput

   A service URL and an activation code are generated and displayed on the GUI.

2. Copy the service URL and an activation code.

   Set Up Agent

   Install the agent on your hypervisor. Click here for instructions. Copy and enter the **service URL** and the **activation code** while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.
   Note: One activation code can be used for only one agent. Also, you can install and register only one agent at a time using this wizard.

   SERVICE URL [redacted] Copy

   ACTIVATION CODE [redacted] Copy

3. Specify the copied service URL and the activation code while installing the agent on your hypervisor.

   The agent uses the service URL to locate the service and the activation code to register with the service. For detailed instructions about installing an agent on your on-premises hypervisor, see Install Citrix Application Delivery and Management agent on-premises.

4. After successful agent installation, return to the **Set Up Agent** page and click **Register Agent**.

Next step: Add instances.

> **Note**
>
> If you do not want to add agents during the initial setup, click **Skip** to check the features provided

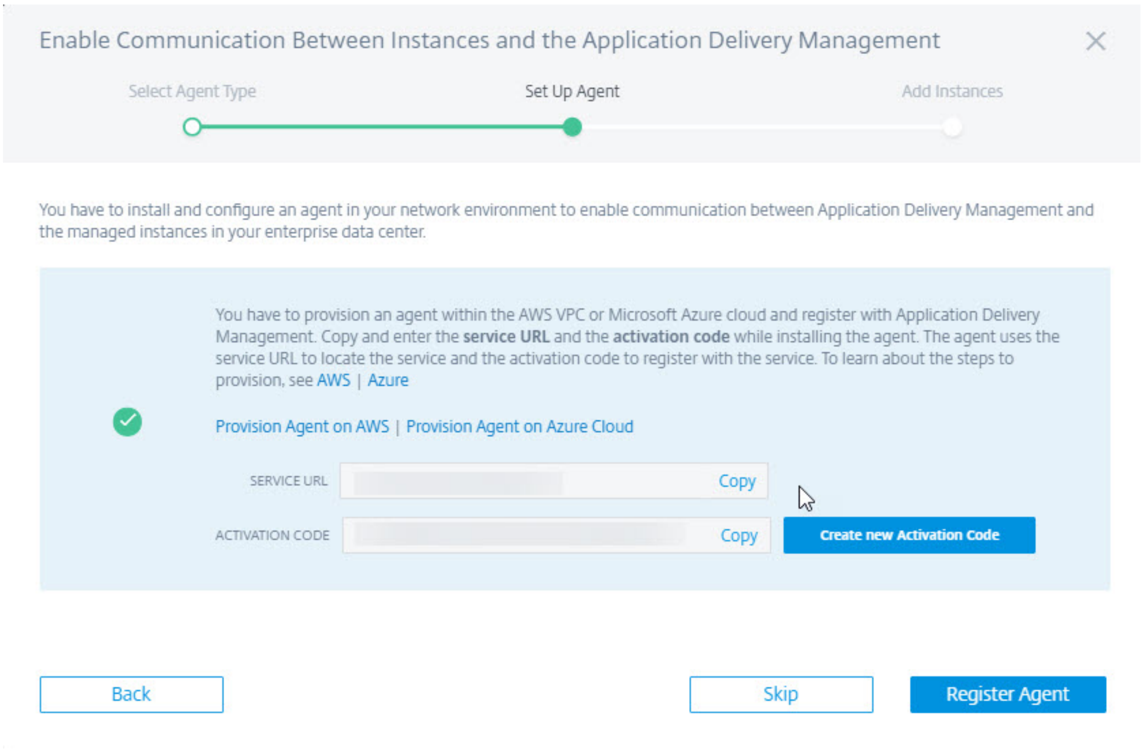
> by Citrix Application Delivery and Management. You can add the agents and instances later. To add agents later, navigate to **Settings > Set up Agents**. For instructions about how to add instances later, see Adding Instances.

Install an agent on a public cloud

You do not have to download the agent image from the **Set Up Agent** page. The agent image is available on the respective cloud marketplace.

1. Copy and save the service URL and the activation code to use during agent installation.

   If you want a new activation code, click **Create new Activation Code**, and then copy and save the code to use during agent installation.

   Enable Communication Between Instances and the Application Delivery Management

   You have to install and configure an agent in your network environment to enable communication between Application Delivery Management and the managed instances in your enterprise data center.

   You have to provision an agent within the AWS VPC or Microsoft Azure cloud and register with Application Delivery Management. Copy and enter the **service URL** and the **activation code** while installing the agent. The agent uses the service URL to locate the service and the activation code to register with the service. To learn about the steps to provision, see AWS | Azure

   SERVICE URL [redacted]

   ACTIVATION CODE [redacted]

   Select Agent Type
Set Up Agent
Add Instances
Provision Agent on AWS | Provision Agent on Azure Cloud
Copy
Copy
Create new Activation Code
Back
Skip
Register Agent

   - For detailed instructions about installing an agent on Microsoft Azure cloud, see Installing Citrix Application Delivery and Management Agent on Microsoft Azure Cloud.
   - For detailed instructions about installing an agent on AWS, see Installing Citrix Application Delivery and Management Agent on AWS.
   - For detailed instructions about installing an agent on Google Cloud, see Install Citrix Application Delivery and Management agent on GCP.

2. After successful agent installation, return to the **Set Up Agent** page and click **Register Agent**.

Next step: Add instances.

Install an agent as a microservice

You can deploy a Citrix Application Delivery and Management agent as a microservice in the Kubernetes cluster to view **service graph** in Citrix Application Delivery and Management.

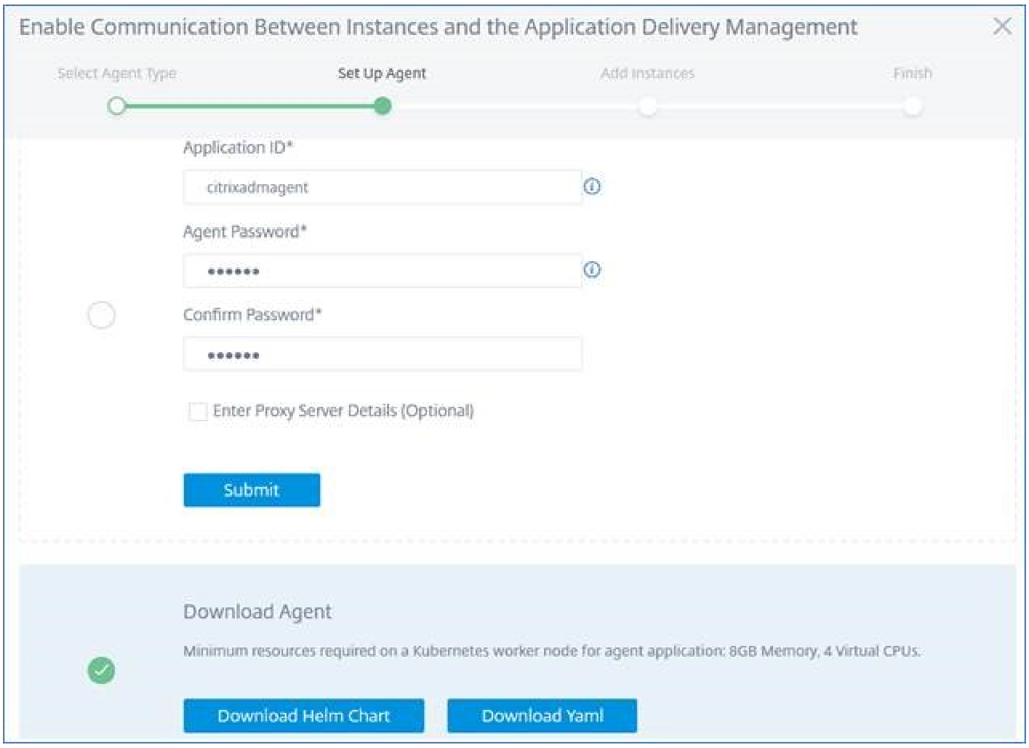
For more information to get started with service graph, see Setting up service graph.

1. 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) **Agent Password** – Specify a password for CPX to use this password to onboard CPX to Citrix Application Delivery and Management through the agent.

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



Enable Communication Between Instances and the Application Delivery Management

Application ID*: citrixadmagent

Agent Password*: ••••••

Confirm Password*: ••••••

□ Enter Proxy Server Details (Optional)

Download Agent

Minimum resources required on a Kubernetes worker node for agent application: 8GB Memory, 4 Virtual CPUs.

    d) Click **Submit**.

2. After you click **Submit**, you can download the YAML or Helm Chart.

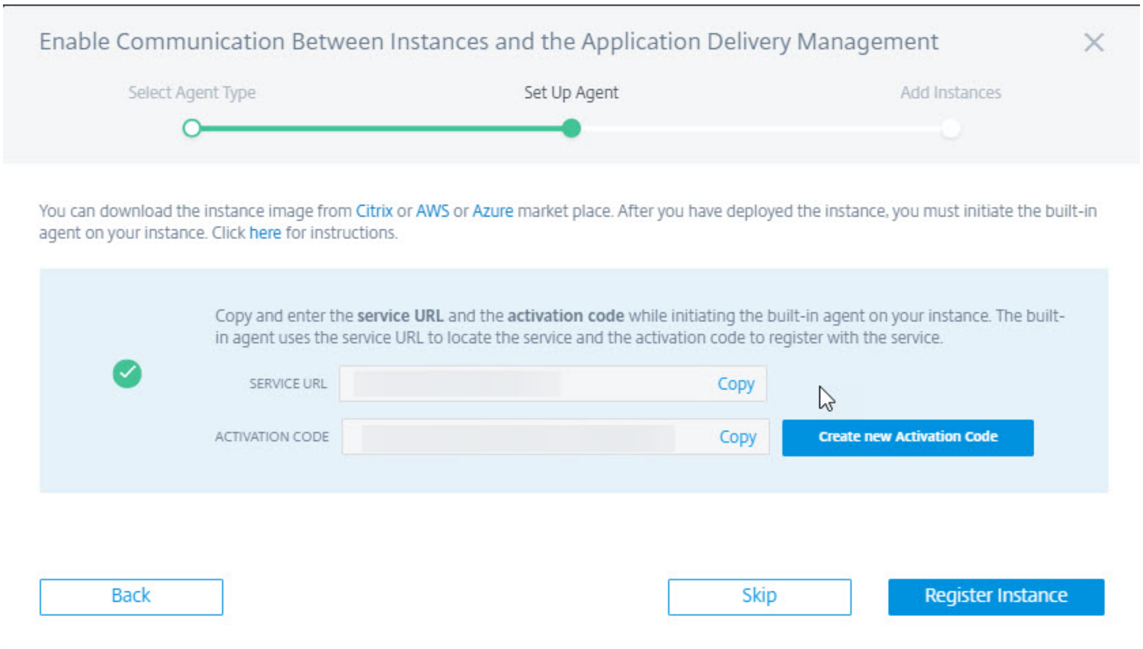
3. Click **Close**.

    For more information, see Install Citrix Application Delivery and Management agent in Kubernetes cluster.

Use the built-in agent in the Citrix ADC instance

The Citrix ADC instances in your environment include a built-in agent. You can initiate the built-in agent and use it to establish communication between the instance and Citrix Application Delivery and Management.

1. Copy the generated **Service URL** and the **Activation Code**. Save them to use while initiating the built-in agent on your Citrix ADC instance.



Enable Communication Between Instances and the Application Delivery Management

You can download the instance image from Citrix or AWS or Azure market place. After you have deployed the instance, you must initiate the built-in agent on your instance. Click here for instructions.

Copy and enter the **service URL** and the **activation code** while initiating the built-in agent on your instance. The built-in agent uses the service URL to locate the service and the activation code to register with the service.

   For detailed instructions about initiating the built-in agent on your Citrix ADC instance, see Initiate Built-in Agent on the Citrix ADC instance.

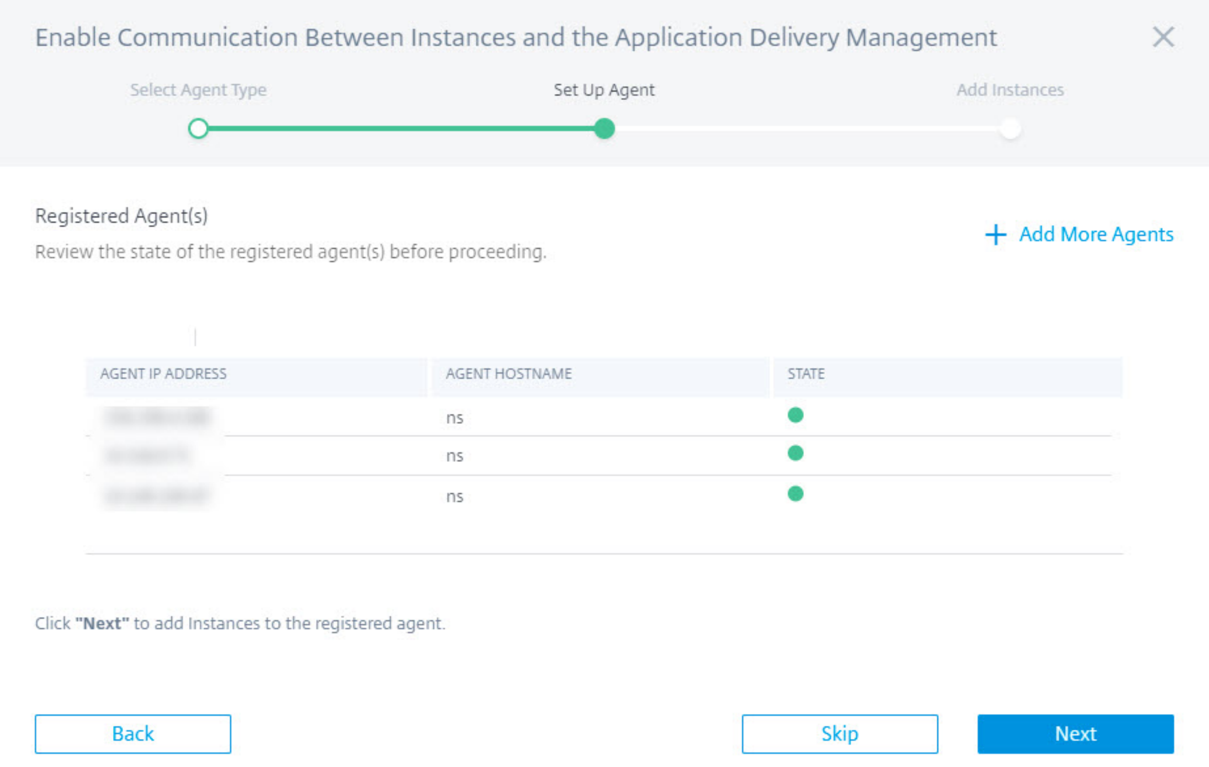
2. After the built-in agent is initiated, return to the **Set Up Agent** page and click **Register Instance**.

Next step: Add instances.

Add instances to Citrix Application Delivery and Management

Instances are network appliances or virtual appliances that you want to discover, manage, and monitor from Citrix Application Delivery and Management. To manage and monitor these instances, you must add the instances to the service.

After the successful agent installation and registration, the agents are displayed on the **Set Up Agent** page. When the agent status is in the UP state denoted by a green dot next to it, click **Next** to start adding instances to the service.



Enable Communication Between Instances and the Application Delivery Management

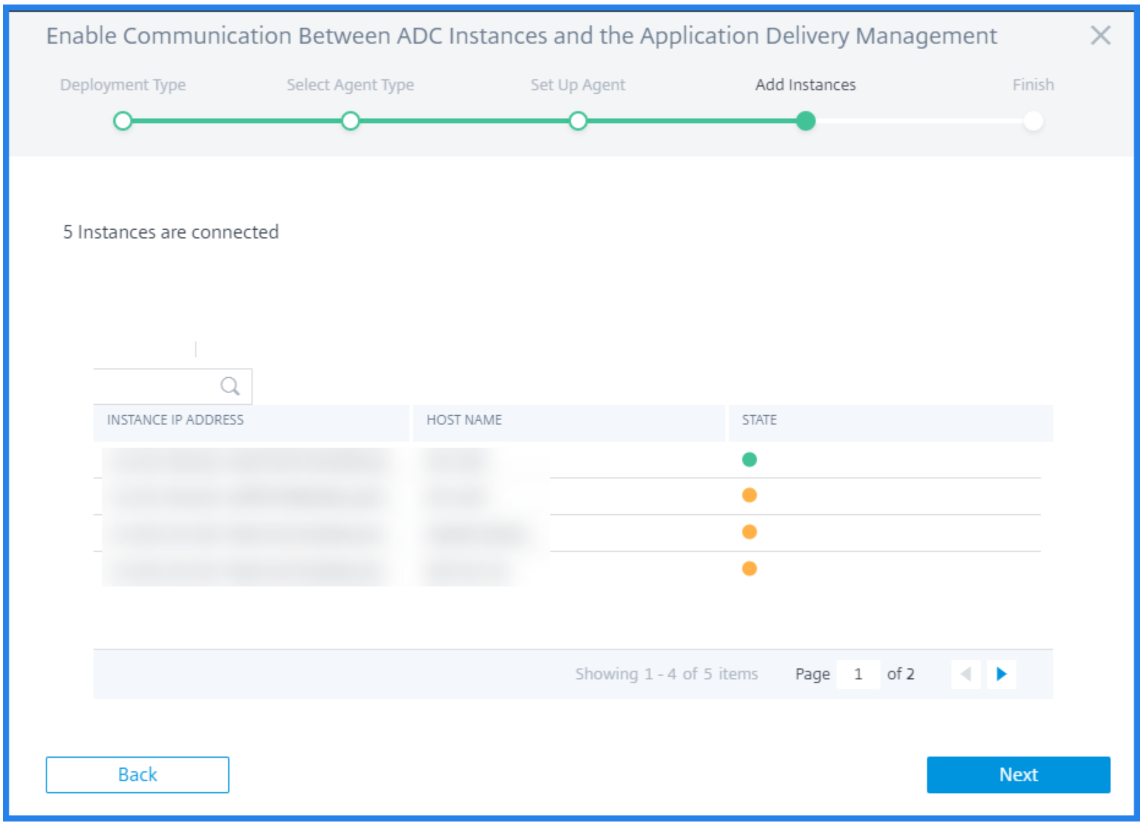
Registered Agent(s)

Review the state of the registered agent(s) before proceeding.

AGENT IP ADDRESS	AGENT HOSTNAME	STATE
[redacted]	ns	●
[redacted]	ns	●
[redacted]	ns	●

Click **"Next"** to add Instances to the registered agent.

1. In the **Add Instances** page, view the ADC instances that are connected to the registered agent. Ensure that the instance is in the **Up** status and click **Next**.



Enable Communication Between ADC Instances and the Application Delivery Management

5 Instances are connected

INSTANCE IP ADDRESS	HOST NAME	STATE
[redacted]	[redacted]	●
[redacted]	[redacted]	●
[redacted]	[redacted]	●
[redacted]	[redacted]	●

Showing 1 - 4 of 5 items Page 1 of 2

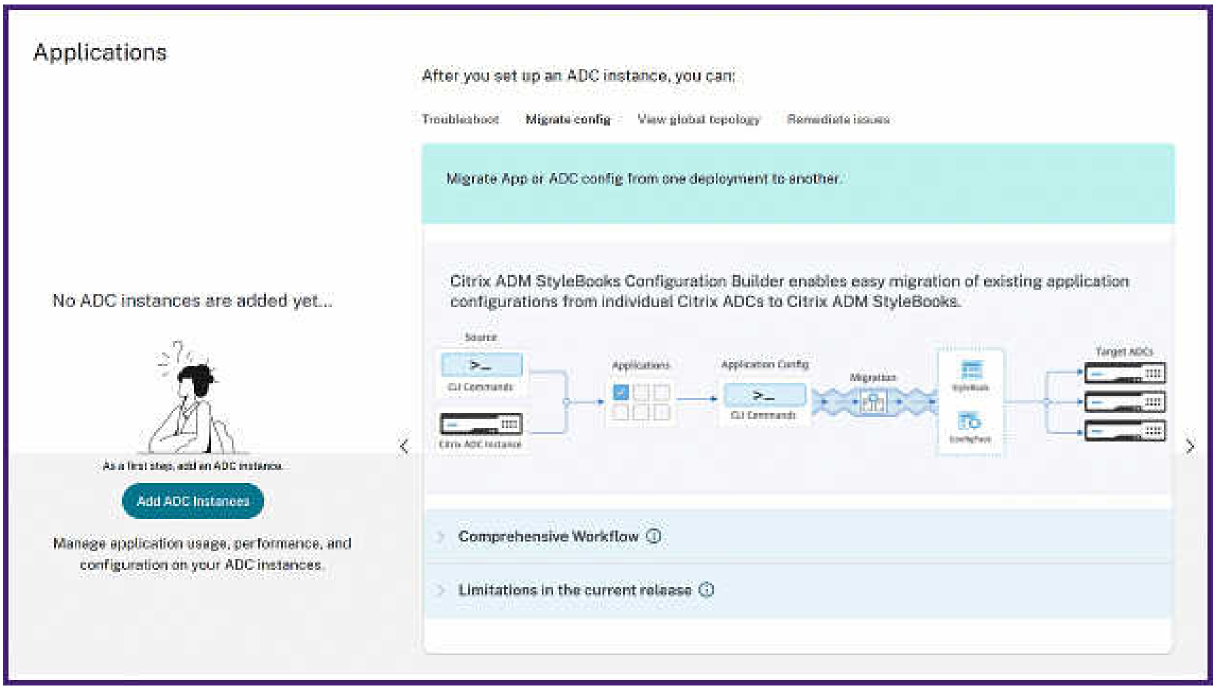
2. Click **Done** to complete your initial setup and start managing your deployment.

> **Note**
>
> If you do not want to add instances during the initial setup, you can click **Done** to complete the setup and add the instances later. For instructions about how to add instances later to Citrix Application Delivery and Management, see Adding Instances.

Onboard ADC instances by using the Citrix Application Delivery and Management GUI dashboard

If you've skipped onboarding the ADC instances in the **Getting Started** workflow while setting up Citrix Application Delivery and Management for the first time, you can onboard the instances from the Citrix Application Delivery and Management GUI dashboard. If ADC instances are not yet added, the GUI prompts you to add the instances.

When you click any module on the left-hand navigation bar, on the right-hand side a tabular preview of the features and benefits of that module appears. These features and benefits help you better manage ADC instances by using Citrix Application Delivery and Management.



Applications

After you set up an ADC instance, you can:

Migrate App or ADC config from one deployment to another.

Citrix ADM StyleBooks Configuration Builder enables easy migration of existing application configurations from individual Citrix ADCs to Citrix ADM StyleBooks.

No ADC instances are added yet...

As a first step, add an ADC instance.

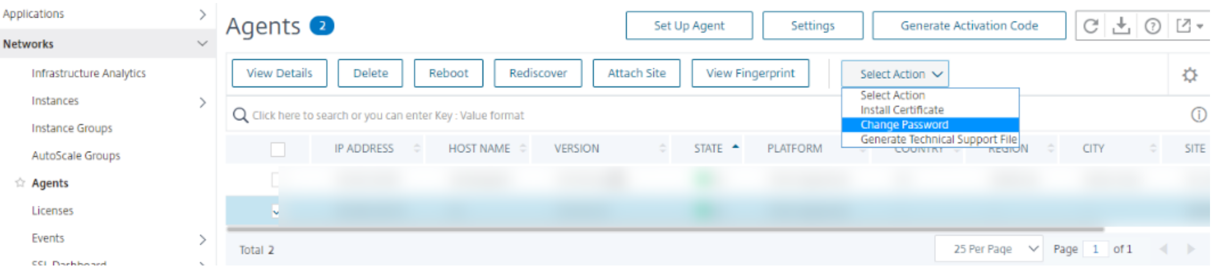
Manage application usage, performance, and configuration on your ADC instances.

Click **Add ADC instances** to onboard the instances. The **Get Started** workflow restarts. Follow the steps from Step 3: Select an ADC deployment type onwards, given in this document, to onboard the instances.

If the ADC instances are already onboarded, after you log on to Citrix Application Delivery and Management, you see only the Citrix Application Delivery and Management landing page with the navigation bar on the left.

Agent actions

After you've set up your Citrix Application Delivery and Management, you can apply various actions to an agent. Navigate to **Infrastructure > Instances > Agents**.



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 Citrix Application Delivery and Management agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

Configure the ADC built-in agent to manage instances

October 14, 2021

A built-in agent is available on Citrix ADC MPX, VPX, Gateway instances running the version `12.1.48.13` and later and on Citrix ADC SDX instances running version 13.0 61.x and later and 12.1 58.x and later. You can initiate this agent on the ADC instance instead of installing a dedicated agent in your data center or public cloud. The built-in agent enables communication between the instance and Citrix Application Delivery and Management.

> **Note**
>
> Built-in agent is available only on the following Citrix ADC instance types:
>
> - Citrix ADC MPX
> - Citrix ADC VPX
> - Citrix ADC SDX
> - Citrix Gateway

The built-in agent is ideal for smaller ADC standalone or HA pair deployments. If you have multiple ADC instances, use a dedicated agent for deployments. This agent ensures you have better data aggregation capabilities than the built-in agent. For more information, see Install an agent on-premises.

Citrix Application Delivery and Management supports management and monitoring of Citrix ADC instances using built-in agents. However, the following features are not supported in the built-in agent:

- Application dashboard
- Web Insight
- SSL insight
- HDX insight
- Gateway insight
- Security insight
- Advanced analytics
- Pooled licensing

You can transition from a built-in agent to an external agent. For more information, see Transition from a built-in agent to an external agent.

Prerequisites

Before you configure a built-in agent on the Citrix ADC instance, ensure the following:

- The Citrix ADC (MPX, VPX, or Gateway) instance is running on the version `12.1.48.13` or later. The SDX instance is running version `13.0.61.x` and later.
- A DNS name server is added on the Citrix ADC instance.

  For more information, see Add a name server.
- You have a Citrix Cloud account. For more information, see Sign up for Citrix Cloud.

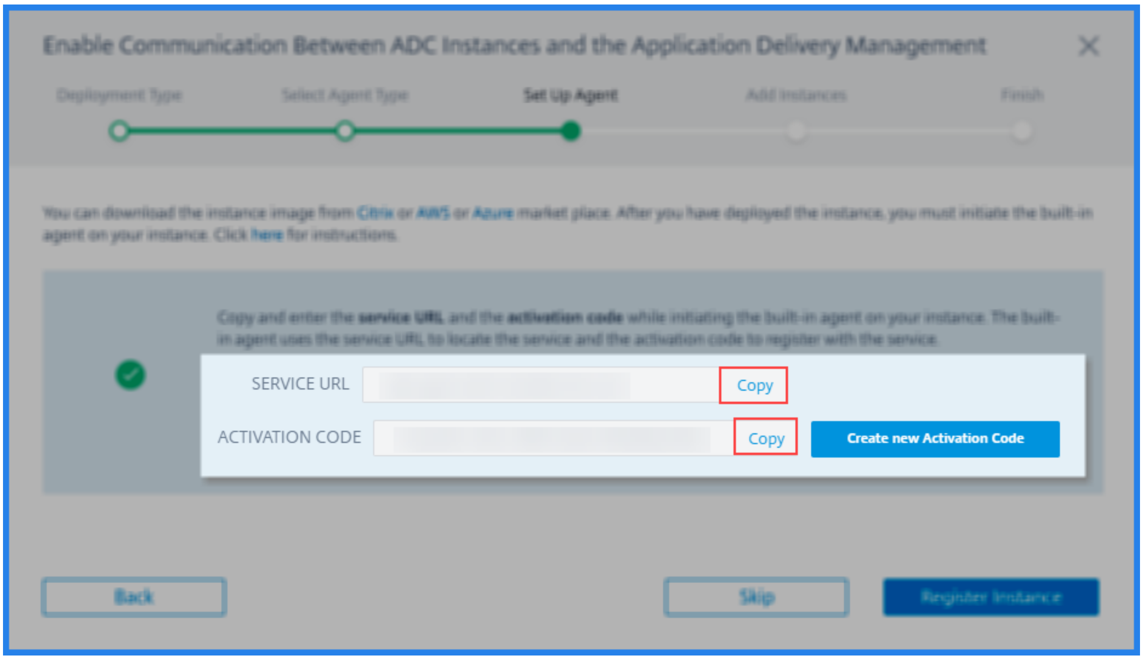
> **Note**
>
> For all information related to ports and other system requirements, see System Requirements.

Configure the built-in agent

Perform the following tasks to configure the ADC built-in agent:

1. Select the Built-in agent option as instructed in Getting Started.
2. Copy the **Service URL** and **Activation code**.

   The agent uses the service URL to locate the service and the activation code to register with the service. Skip step 7 if you are an MPX or a Gateway customer.

   Enable Communication Between ADC Instances and the Application Delivery Management

   You can download the instance image from Citrix or AWS or Azure market place. After you have deployed the instance, you must initiate the built-in agent on your instance. Click here for instructions.

   Copy and enter the **service URL** and the **activation code** while initiating the built-in agent on your instance. The built-in agent uses the service URL to locate the service and the activation code to register with the service.

3. Initiate the built-in agent using an SSH client. Gateway users must skip this step.

   a) Log on to your Citrix ADC instance. For more information, see Access a Citrix ADC.

b) Navigate to the `/var/mastools/scripts` directory and type the following command:

On the SDX instance

```
./mastools_init.sh <user_name> <service-url> <activation-code>
    -sdx
<!--NeedCopy-->
```

- In `<user_name>`, enter Citrix ADC user name.

```
./mastools_init.sh <device-profile-name> <service-url> <
    activation-code> -sdx -profile

<!--NeedCopy-->
```

> Note
>
> Citrix Application Delivery and Management discovers all VPX instances running on that SDX and you don't have to register the VPX instances individually.

On VPX instances not running on an SDX appliance and MPX and Gateway instances:

If the ADC image version is lower than 13.0 61.x or 12.1 57.x, you must check the `mastools` version by typing the command `cat /var/mastools/version.conf`. If the output is `0.0-0.0`, it is the first time.

Type one of the following commands given in the following, depending on the software version.

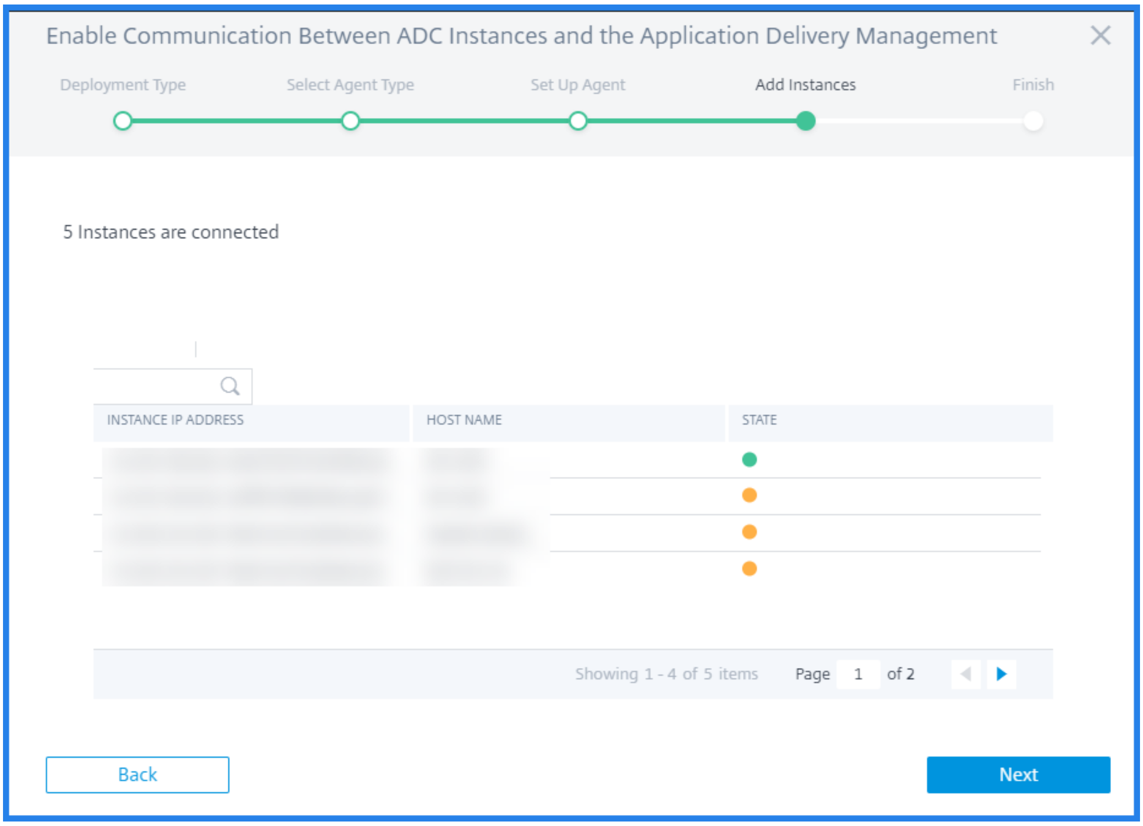
ADC image version	Is mastools_version `0.0-0.0`?	Command for registration with profile	Command for registration without profile
Lower than 13.0 61.xx and 12.1 57.xx	Yes	`./mastools_init.sh <device_profile_nam > <service_url> "MAS;<activation_code> "-profile`	`./mastools_init.sh <user_name> <pwd> <service_url> "MAS;<activation_code> "`
Lower than 13.0 61.xx and 12.1 57.xx	No	`./mastools_init.sh <device_profile_name > <service_url> <activation_code > -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

ADC image version	Is mastools_version `0.0-0.0`?	Command for registration with profile	Command for registration without profile
Higher than 13.0 61.x and 12.1 57.xx	Not applicable	`./mastools_init.sh <device_profile_nam> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

- In `<user_name>`, enter Citrix ADC user name.

> **Note**
>
> In an HA pair, complete the registration on the primary node. If you run the registration on the secondary node, the following message appears:
>
> **Please run the registration command on the primary node.**

4. Return to the Citrix Application Delivery and Management page and click **Register Instance**.
5. In **Add Instances**, view the instance where you initiated the built-in agent. Ensure the instance is in the **Up** status and click **Next**.



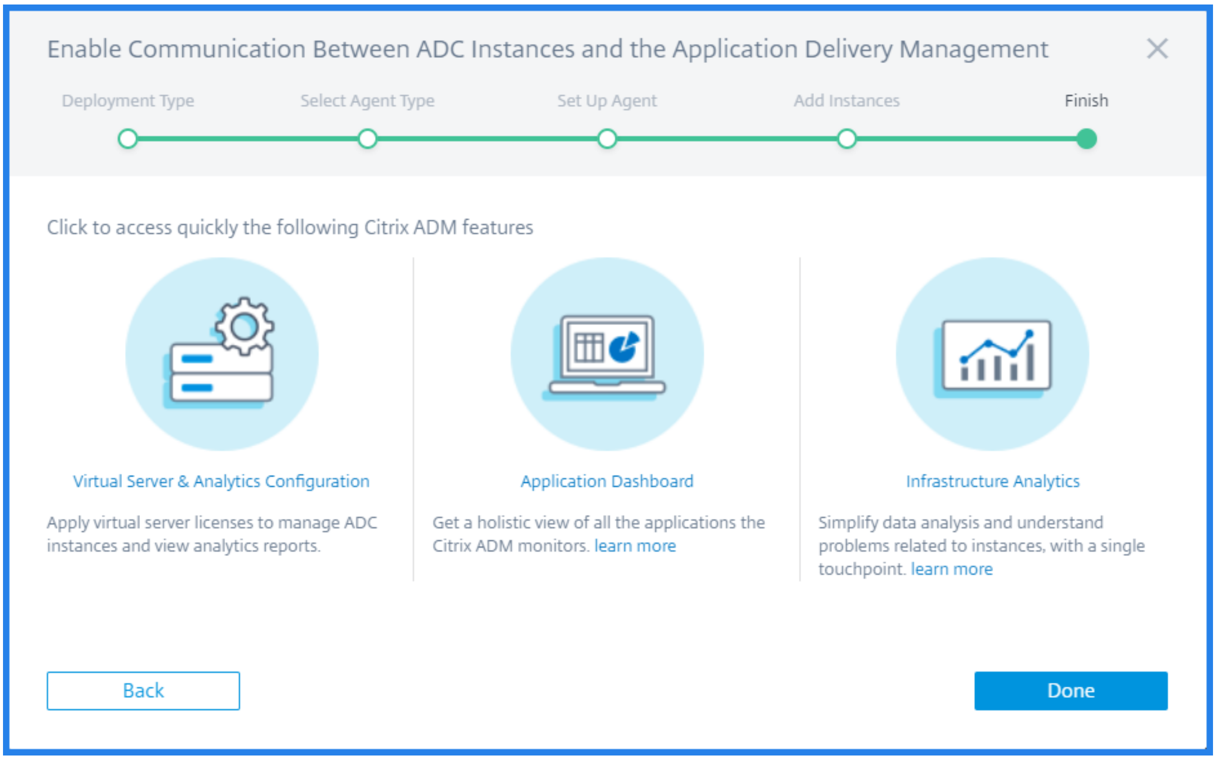
Enable Communication Between ADC Instances and the Application Delivery Management

5 Instances are connected

INSTANCE IP ADDRESS	HOST NAME	STATE
[redacted]	[redacted]	●
[redacted]	[redacted]	●
[redacted]	[redacted]	●
[redacted]	[redacted]	●

Showing 1 - 4 of 5 items Page 1 of 2

6. Click **Done**.



Enable Communication Between ADC Instances and the Application Delivery Management

Click to access quickly the following Citrix ADM features

Virtual Server & Analytics Configuration

Apply virtual server licenses to manage ADC instances and view analytics reports.

Application Dashboard

Get a holistic view of all the applications the Citrix ADM monitors. learn more

Infrastructure Analytics

Simplify data analysis and understand problems related to instances, with a single touchpoint. learn more

After successful built-in agent configuration, you can access the Citrix Application Delivery and Management features such as:

- **Virtual server and analytics** – Apply licenses to your virtual server to manage ADC instances. For more information, see Manage subscriptions.
- **Application dashboard** – To view all applications in a holistic way. For more information, see Application management and dashboard.
- **Infrastructure analytics** – This feature helps you to visualize the factors that resulted or might result in an issue on the instances. For more information, see Infrastructure Analytics.

> Note
>
> You can also configure the built-in agent by navigating to the **Infrastructure > Instances > Agents > Generate Activation code** page. Copy and paste the URL and activation code to an ADC instance and discover that instance.

After the built-in agent is initiated, navigate to **Infrastructure > Instances > Citrix ADC**. This page displays the details about the managed instance discovered using the built-in agent.

Troubleshooting

You can check logs if registration fails or if registration succeeds but the built-in agent does not appear in the Citrix Application Delivery and Management GUI.

- If registration fails, check logs in `/var/mastools/logs/mastools_reg.py.log`
- If registration succeeds, but the built-in agent does not appear in the Citrix Application Delivery and Management GUI, check:
  - **Mastools_upgrade** logs in `/var/mastools/logs/mastools_upgrade.log`
  - **Binary logs** in `/var/log/mastoolsd.log`.

Install an agent on-premises

October 14, 2021

The agent works as an intermediary between the Citrix Application Delivery and Management and the discovered instances in the data center.

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

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

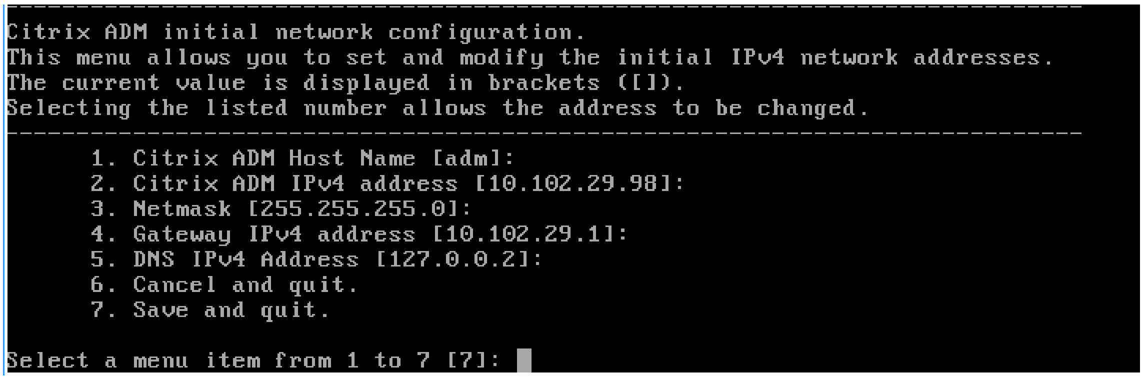
> **Note**
>
> For all information related to ports and other requirements, see System Requirements.

To install the Citrix ADM agent:

1. Download the agent image as instructed in Getting Started.

2. Import the agent image file to your hypervisor.

3. From the **Console** tab, configure the initial network configuration options as shown in the following example:

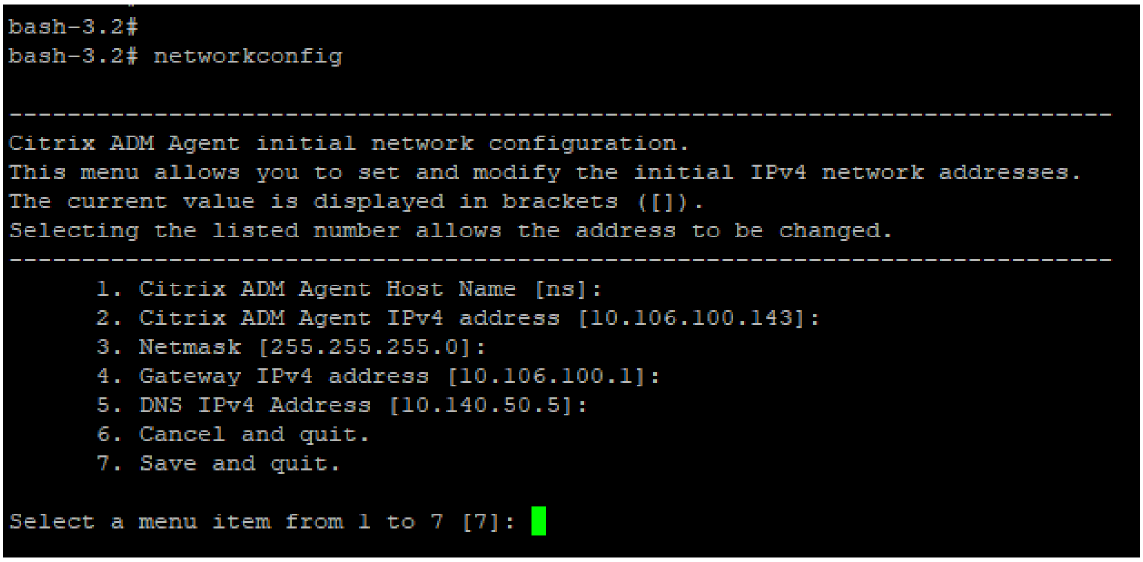


```
------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------
      1. Citrix ADM Host Name [adm]:
      2. Citrix ADM IPv4 address [10.102.29.98]:
      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]:
```

> **Note**
>
> Ensure that you configure your DNS to allow Internet access to your Citrix ADM agent.

4. After completing the initial network configuration, save the configuration settings. When prompted, log on using the default (`nsrecover`/`nsroot`) credentials.

   If you want to change the configured network settings on the agent, type the `networkconfig` command and follow the prompts in the CLI.



```
bash-3.2#
bash-3.2# 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 [10.106.100.143]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.106.100.1]:
      5. DNS IPv4 Address [10.140.50.5]:
      6. Cancel and quit.
      7. Save and quit.

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

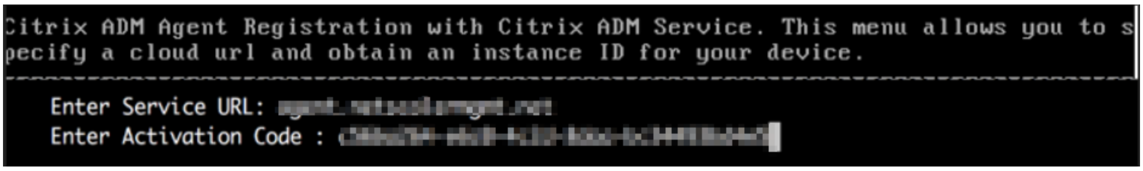
5. If there is no prompt to enter the Service URL, navigate to /mps in the Citrix ADM agent and then run any one of the following scripts:

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

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

6. Enter the **Service URL** and the **Activation Code** that you saved when you had downloaded the

agent image. The agent uses the Service URL to locate the service and the activation code to register with the service.

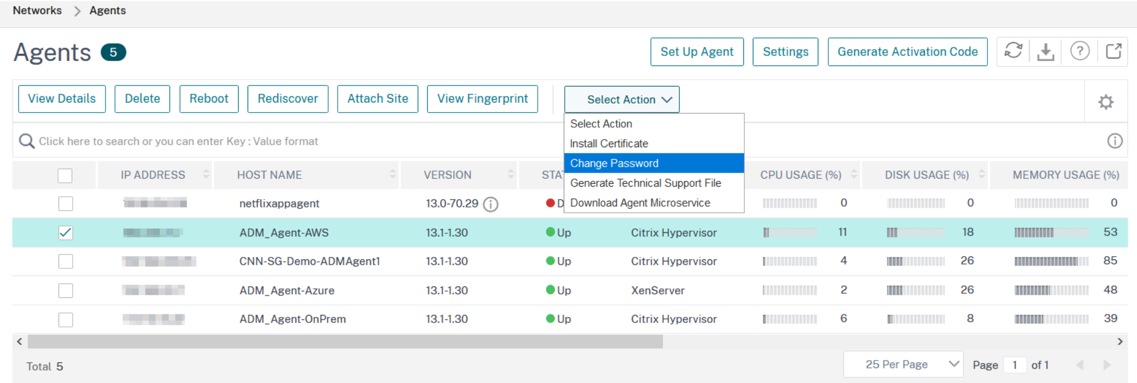


```
itrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
--------------------------------------------------------------------------------
   Enter Service URL: [redacted]
   Enter Activation Code : [redacted]
```

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

After the agent has restarted, access the Citrix Application Delivery and Management GUI and navigate to **Infrastructure > Instances > Agents** to verify the status of the agent. After the agent is configured, you must change the password.

1. Navigate to **Infrastructure > Instances > Agents**
2. Select the agent and from the **Select Action** list, click **Change Password**.



	IP ADDRESS	HOST NAME	VERSION	STAT		CPU USAGE (%)	DISK USAGE (%)	MEMORY USAGE (%)
□	[redacted]	netflixappagent	13.0-70.29 ⓘ	● D		0	0	0
☑	[redacted]	ADM_Agent-AWS	13.1-1.30	● Up	Citrix Hypervisor	11	18	53
□	[redacted]	CNN-SG-Demo-ADMAgent1	13.1-1.30	● Up	Citrix Hypervisor	4	26	85
□	[redacted]	ADM_Agent-Azure	13.1-1.30	● Up	XenServer	2	26	48
□	[redacted]	ADM_Agent-OnPrem	13.1-1.30	● Up	Citrix Hypervisor	6	8	39

3. Enter the current password (`nsroot`), then specify a new password, and click **OK** to change the password.

   The password must:

   - Be at least six characters in length
   - Have at least one special character
   - Have at least one upper case character
   - Have at least one lower case character
   - Have at least one numeric character

Install an agent on Microsoft Azure cloud

October 14, 2021

The agent works as an intermediary between the Citrix Application Delivery and Management and the managed instances in the enterprise data center, or on the cloud.

To install the Citrix ADM agent on the Microsoft Azure cloud, you have to create an instance of the agent in the virtual network. Obtain the Citrix ADM agent image from the Azure Marketplace, and then use the Azure Resource Manager portal to create the agent.

Before you begin creating the Citrix ADM agent instance, make sure that you have created a virtual network with the required subnets where the instance will reside. You can create virtual networks during VM provisioning, but without the flexibility to create different subnets. For information about creating virtual networks, see http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network.

Configure DNS server and VPN connectivity that allows a virtual machine to access Internet resources.

Prerequisites

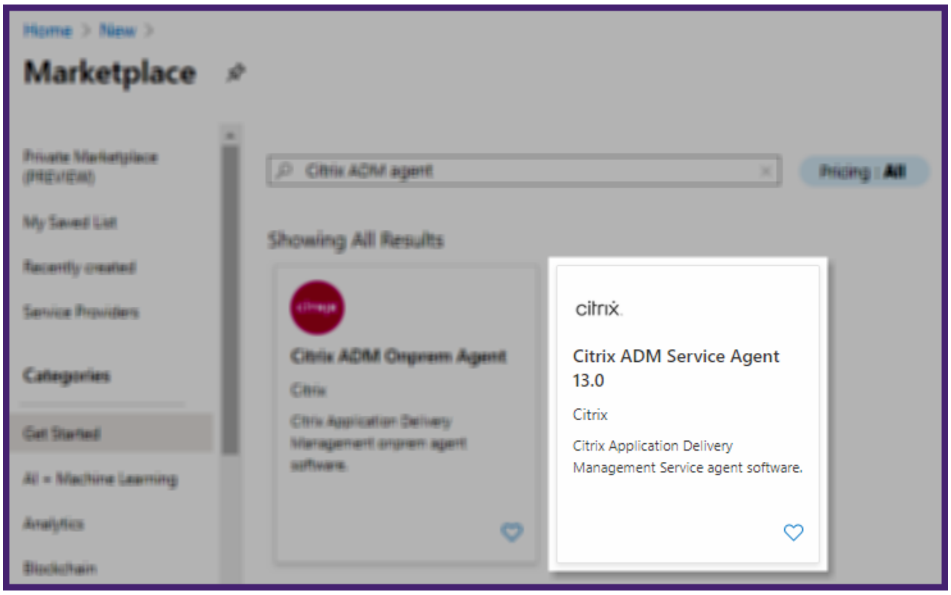
Make sure that you have the following:

- A Microsoft Azure user account
- Access to Microsoft Azure Resource Manager

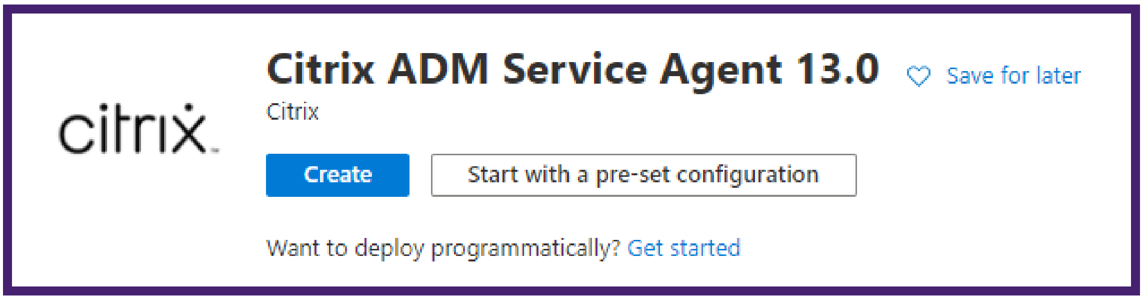
> **Note**
>
> - Citrix recommends that you create resource group, network security group, virtual network, and other entities before you provision the Citrix ADM agent virtual machine, so that the network information is available during provisioning.
> - For the Citrix ADM agent to communicate with Citrix Application Delivery and Management and the Citrix ADC instances, ensure that the recommended ports are open. For complete details about the port requirements for the Citrix ADM agent, see Ports.

To install the Citrix ADM agent on Microsoft Azure Cloud:

1. Log on to the Azure portal (https://portal.azure.com) by using your Microsoft Azure credentials.
2. Click **+Create a resource**.
3. Type `Citrix ADM agent` in the search bar and select **Citrix ADM agent**.



4. Click **Create**.

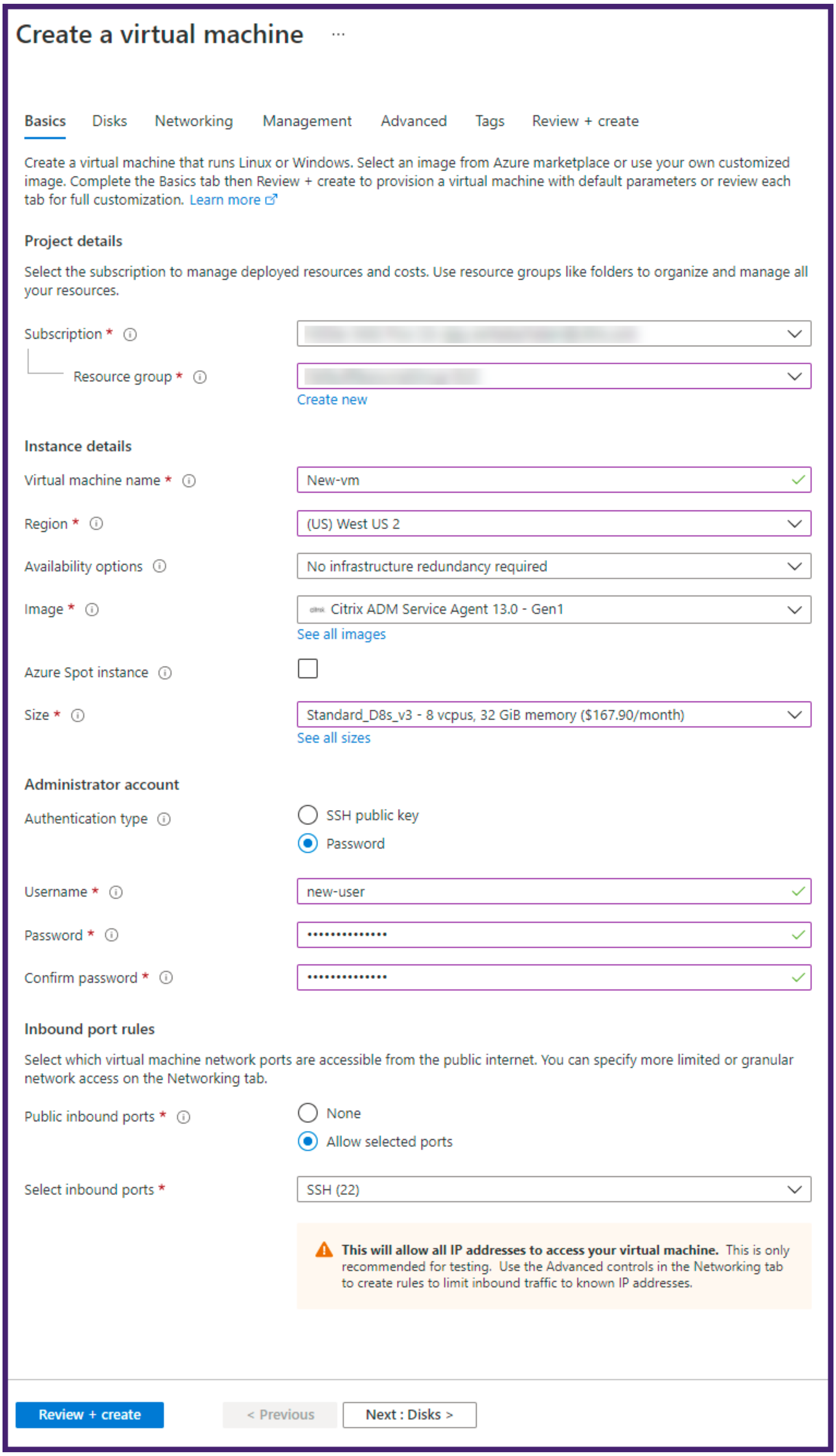

citrix
Citrix ADM Service Agent 13.0
Save for later
Citrix
Create
Start with a pre-set configuration

Want to deploy programmatically? Get started

5. In the **Create virtual machine** pane, specify the required values in each section to create a virtual machine.

   Basics:

   In this tab, specify **Project details**, **Instance details**, and **Administrator account**.



Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [redacted]

Resource group * [redacted]

Create new

Instance details

Virtual machine name * New-vm ✓

Region * (US) West US 2

Availability options No infrastructure redundancy required

Image * Citrix ADM Service Agent 13.0 - Gen1

See all images

Azure Spot instance □

Size * Standard_D8s_v3 - 8 vcpus, 32 GiB memory ($167.90/month)

See all sizes

Administrator account

Authentication type ○ SSH public key ● Password

Username * new-user ✓

Password * •••••••••••••• ✓

Confirm password * •••••••••••••• ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ○ None ● Allow selected ports

Select inbound ports * SSH (22)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

- **Resource group** – Select the resource group you have created from the drop-down list.

  > **Note**
  >
  > You can create a resource group at this point, but Citrix recommends that you create a resource group from Resource groups in the Azure Resource Manager and then select the group from the drop-down list.

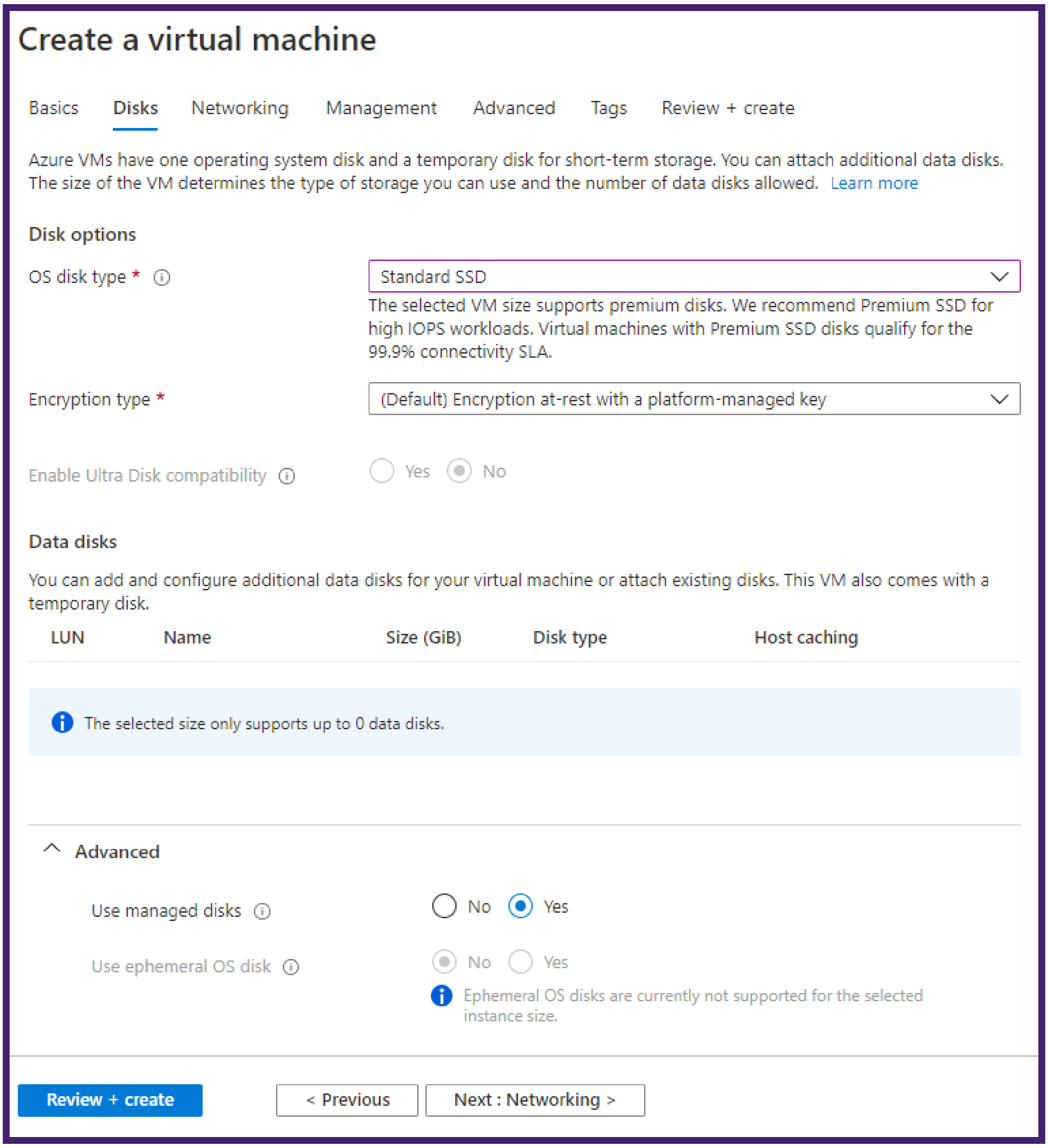
- **Virtual machine name** – Specify a name for the Citrix ADM agent instance.
- **Region** - Select the region where you want to deploy an agent.
- **Availability options** – Select the availability set from the list.
- **Image** - This field displays the already selected agent image. If you want to change to a different agent image, select the required image from the list.
- **Size** - Specify the type and size of the virtual disk for deploying your Citrix ADM agent.

  Select the Supported virtual disk type (**HDD** or **SSD**) from the list.

- **Authentication Type** – Select Password.
- **User name and Password** – Specify a user name and password to access the resources in the resource group that you have created.

Disks:

In this tab, specify **Disk options** and **Data disks**.



Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Standard SSD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * : (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility: ○ Yes ● No

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

The selected size only supports up to 0 data disks.

Advanced

Use managed disks: ○ No ● Yes

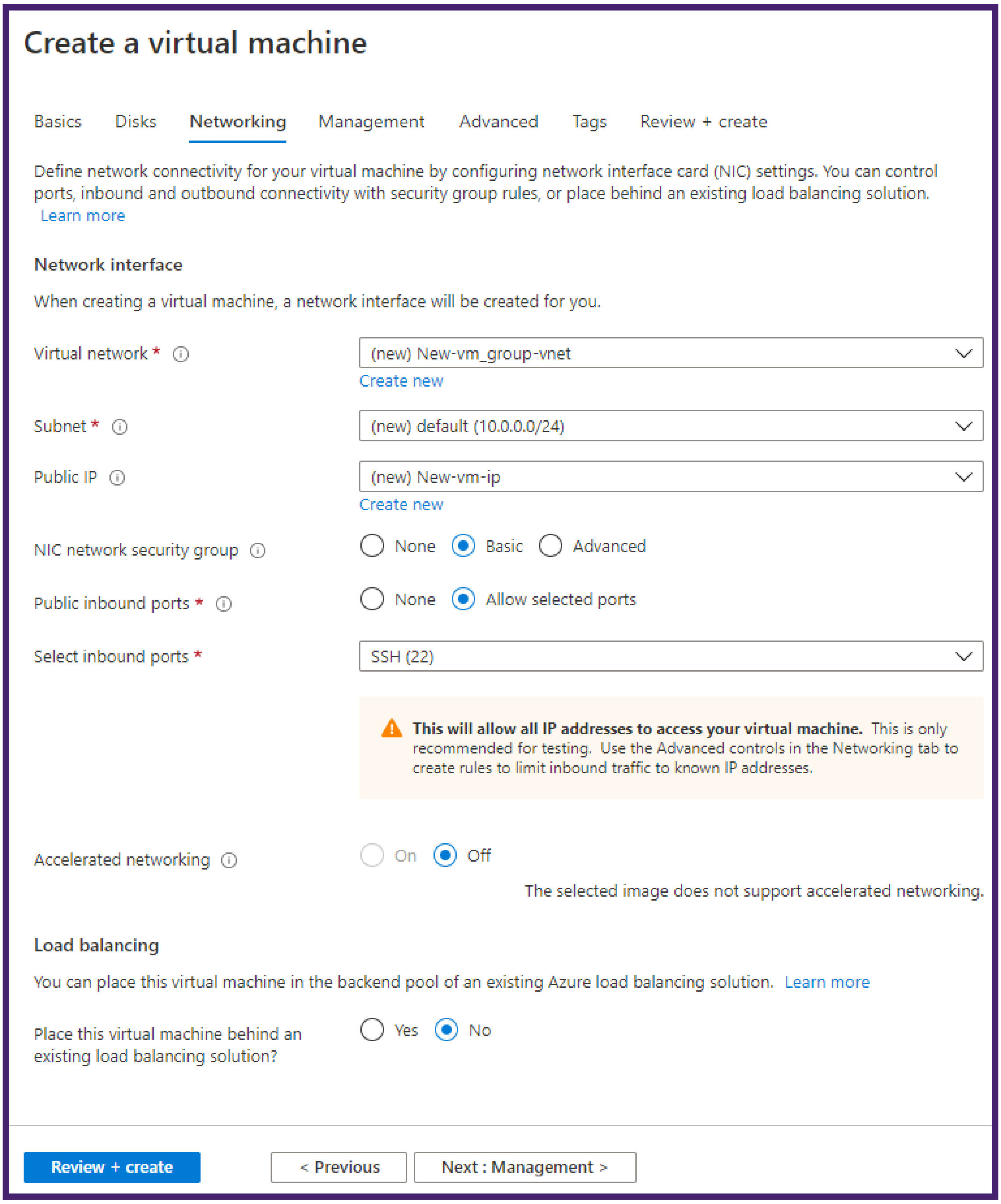
Use ephemeral OS disk: ● No ○ Yes

Ephemeral OS disks are currently not supported for the selected instance size.

- **OS disk type** - Select the virtual disk type (HDD or SSD).

Networking:

Specify the required networking details:



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : (new) New-vm_group-vnet
Create new

Subnet * : (new) default (10.0.0.0/24)

Public IP : (new) New-vm-ip
Create new

NIC network security group : ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking : ○ On ● Off

The selected image does not support accelerated networking.

Load balancing

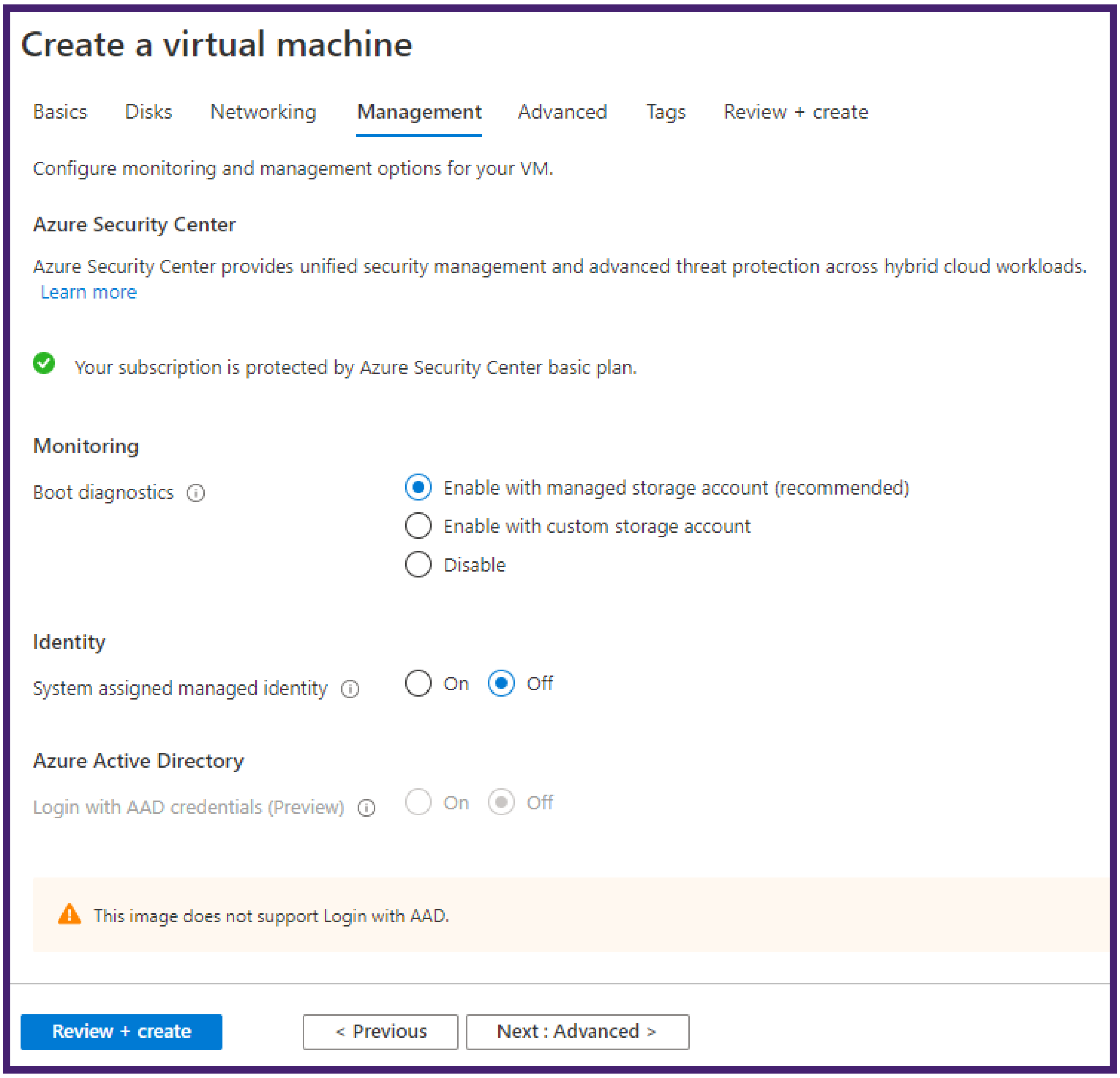
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No

- **Virtual network** – Select the virtual network.
- **Subnet** – Set the subnet address.
- **Public IP address** – Select the IP address.
- **Network security group** – Select the security group that you have created.
- **Select inbound ports** - If you allow public inbound ports, ensure the inbound and outbound rules are configured in the security group. Then, select the inbound ports from the list. For more details, see Prerequisites.

Management:

Specify **Azure Security Center**, **Monitoring**, and **Identity**.



Create a virtual machine

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ
● Enable with managed storage account (recommended)
○ Enable with custom storage account
○ Disable

Identity

System assigned managed identity ⓘ ○ On ● Off

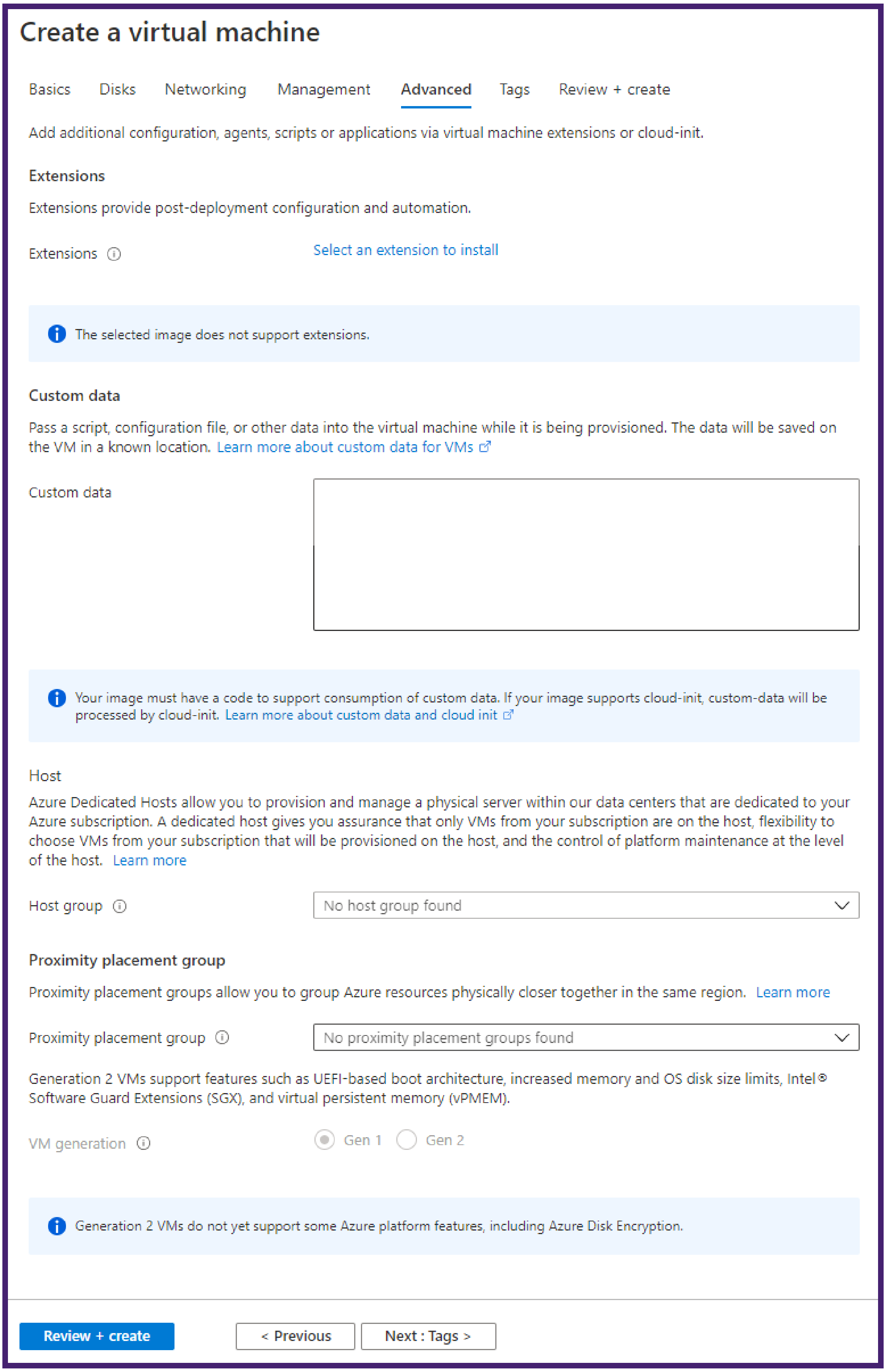
Azure Active Directory

Login with AAD credentials (Preview) ⓘ ○ On ● Off

⚠ This image does not support Login with AAD.

Advanced:

Optional, specify **Extensions**, **Custom Data**, and **Proximity placement group**.



Create a virtual machine

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

ⓘ The selected image does not support extensions.

Custom data

Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

ⓘ Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data and cloud init

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more

Host group ⓘ No host group found

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. Learn more

Proximity placement group ⓘ No proximity placement groups found

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM).

VM generation ⓘ ● Gen 1 ○ Gen 2

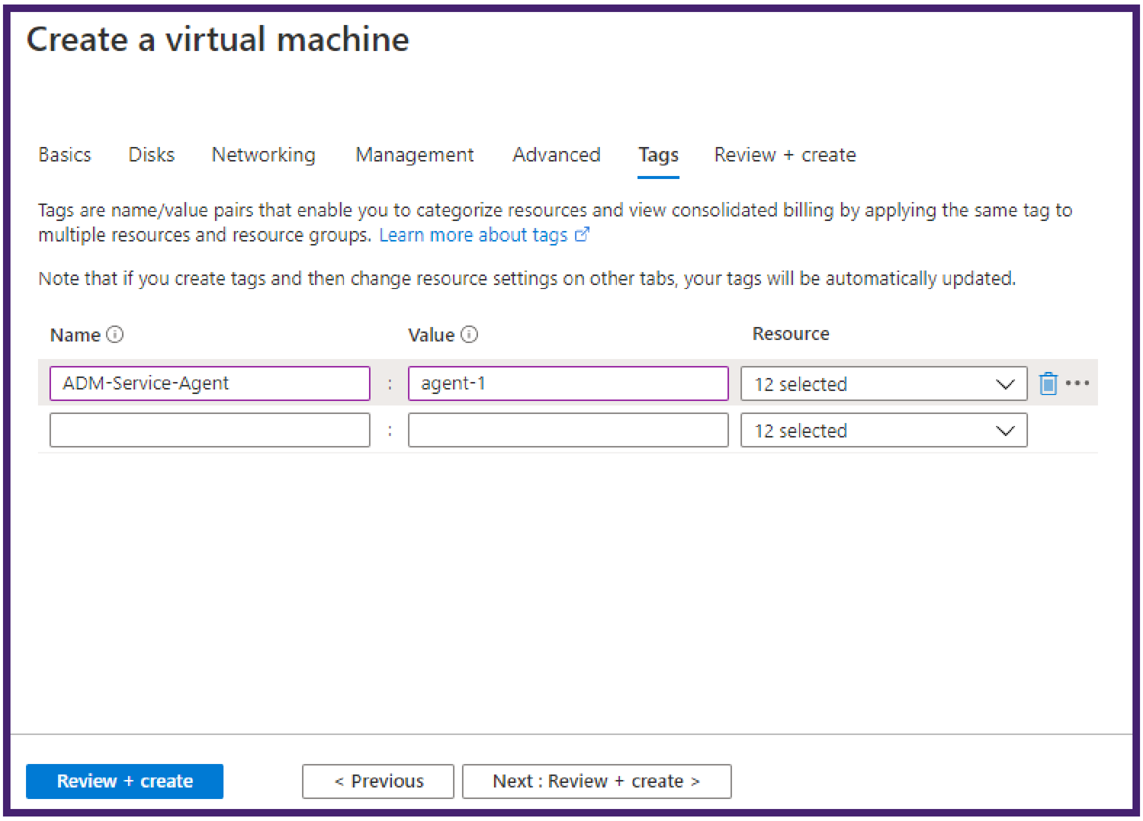
ⓘ Generation 2 VMs do not yet support some Azure platform features, including Azure Disk Encryption.

> **Note**
>
> In **Custom Data**, specify the **Service-URL** and **Activation code** that you copied from the **Set Up Agents** page in Citrix Application Delivery and Management as instructed in Getting Started. Enter the details in the following format:
>
> ```
> registeragent -serviceurl <apigatewayurl> -activationcode <
>     activationcodevalue>
> <!--NeedCopy-->
> ```
>
> Agent uses this information to auto-register with the Citrix Application Delivery and Management during boot-up.

If you specify this auto-registration script, skip step 7 and 8.

Tags:

Type the key-value pair for the Citrix ADM agent tags. A tag consists of a case-sensitive key-value pair. These tags enable you to organize and identify the agent easily. The tags are applied to both Azure and Citrix Application Delivery and Management.



Create a virtual machine

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

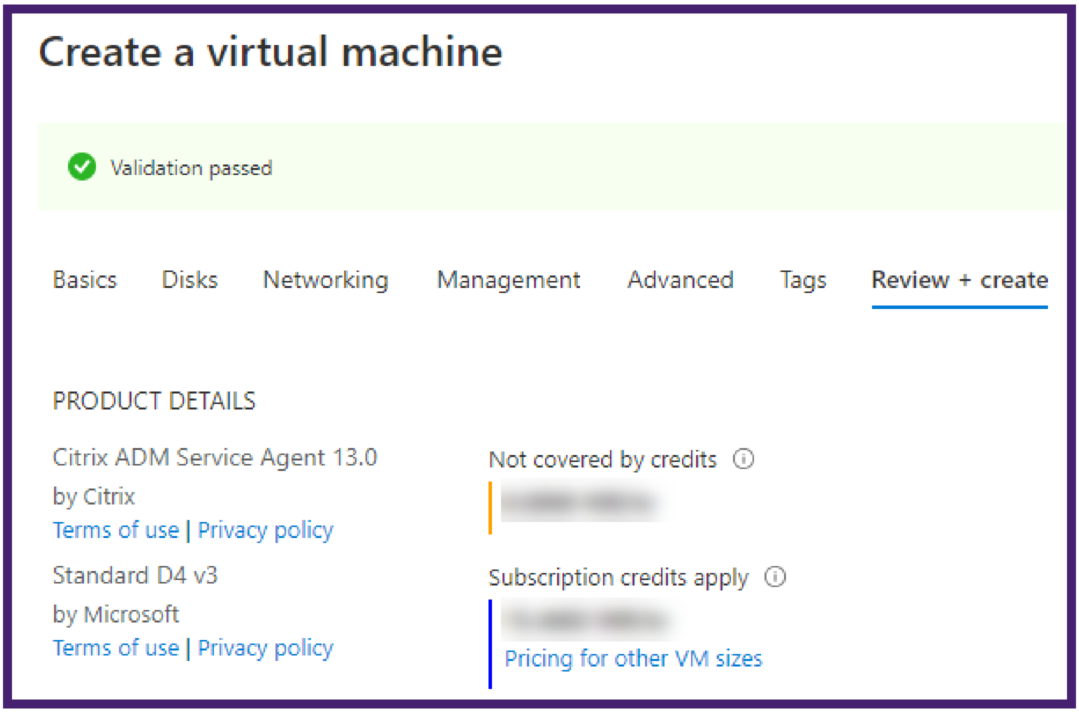
Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name		Value	Resource
ADM-Service-Agent	:	agent-1	12 selected
	:		12 selected

The configuration settings are validated and the **Review and create** tab displays the result of the validation.

- If the validation fails, this tab displays the reason for the failure. Go back to the particular section and make changes as required.

- If the validation passes, click **Create**. The agent deployment process begins.



Create a virtual machine

✓ Validation passed

PRODUCT DETAILS

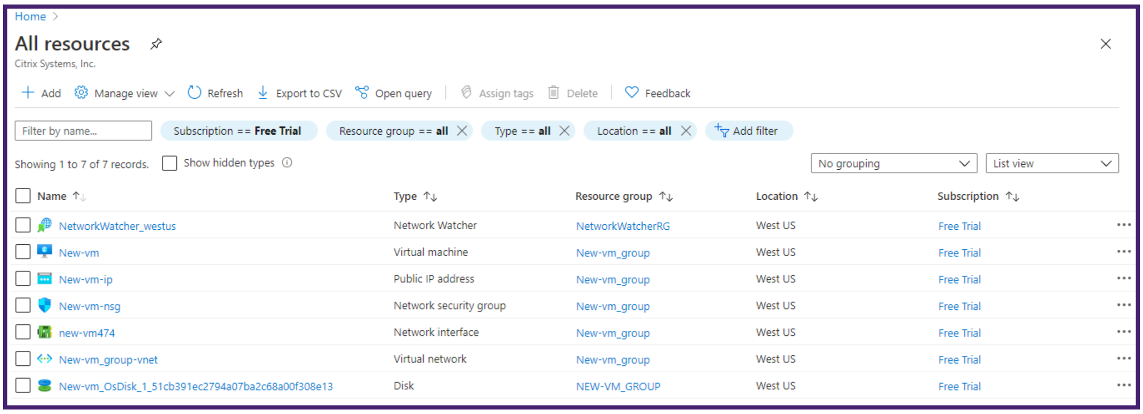
Citrix ADM Service Agent 13.0
by Citrix
Terms of use | Privacy policy

Not covered by credits ⓘ
[redacted]

Standard D4 v3
by Microsoft
Terms of use | Privacy policy

Subscription credits apply ⓘ
[redacted]
Pricing for other VM sizes

The deployment process might take approximately 10–15 minutes. Once the deployment is successfully completed, you can view your Citrix ADM agent virtual machine in your Microsoft Azure account.



Home >

All resources

Citrix Systems, Inc.

Filter by name... | Subscription == **Free Trial** | Resource group == **all** | Type == **all** | Location == **all** | Add filter

Showing 1 to 7 of 7 records. □ Show hidden types | No grouping | List view

□ Name	Type	Resource group	Location	Subscription
□ NetworkWatcher_westus	Network Watcher	NetworkWatcherRG	West US	Free Trial
□ New-vm	Virtual machine	New-vm_group	West US	Free Trial
□ New-vm-ip	Public IP address	New-vm_group	West US	Free Trial
□ New-vm-nsg	Network security group	New-vm_group	West US	Free Trial
□ new-vm474	Network interface	New-vm_group	West US	Free Trial
□ New-vm_group-vnet	Virtual network	New-vm_group	West US	Free Trial
□ New-vm_OsDisk_1_51cb391ec2794a07ba2c68a00f308e13	Disk	NEW-VM_GROUP	West US	Free Trial

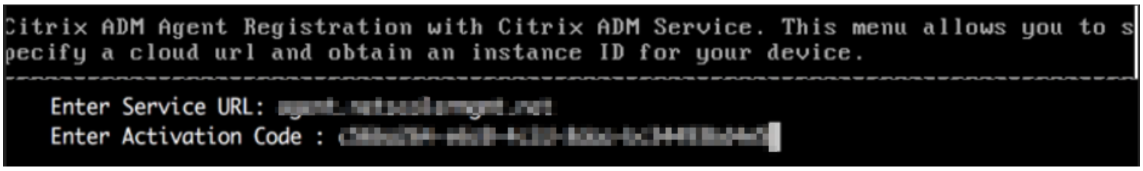
6. Once the agent is up and running, using an SSH client, log on to your Citrix ADM agent using the **Public IP address**.

> **Note**
>
> - If you specified the user name as `nsrecover`, use the default Citrix ADM agent credentials (**nsrecover/nsroot**) to log on to the virtual machine.
> - Citrix recommends that you change your default password after the first logon. To

> change the password, at shell type: **passwd nsroot**.

7. Enter the following command to invoke the deployment screen: **deployment_type.py**

8. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in Citrix Application Delivery and Management as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.



```
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
--------------------------------------------------------------------------------

   Enter Service URL: [redacted]
   Enter Activation Code : [redacted]
```

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

After the agent has restarted, access Citrix Application Delivery and Management and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Install an agent on Amazon Web Services (AWS)

October 18, 2021

The Citrix ADM agent works as an intermediary between the Citrix Application Delivery and Management and the discovered instances in the data center or on the cloud.

Prerequisites

To launch a Citrix ADM agent AMI within an Amazon Web Services (AWS) Virtual Private Cloud (VPC) by using the Amazon GUI, you need:

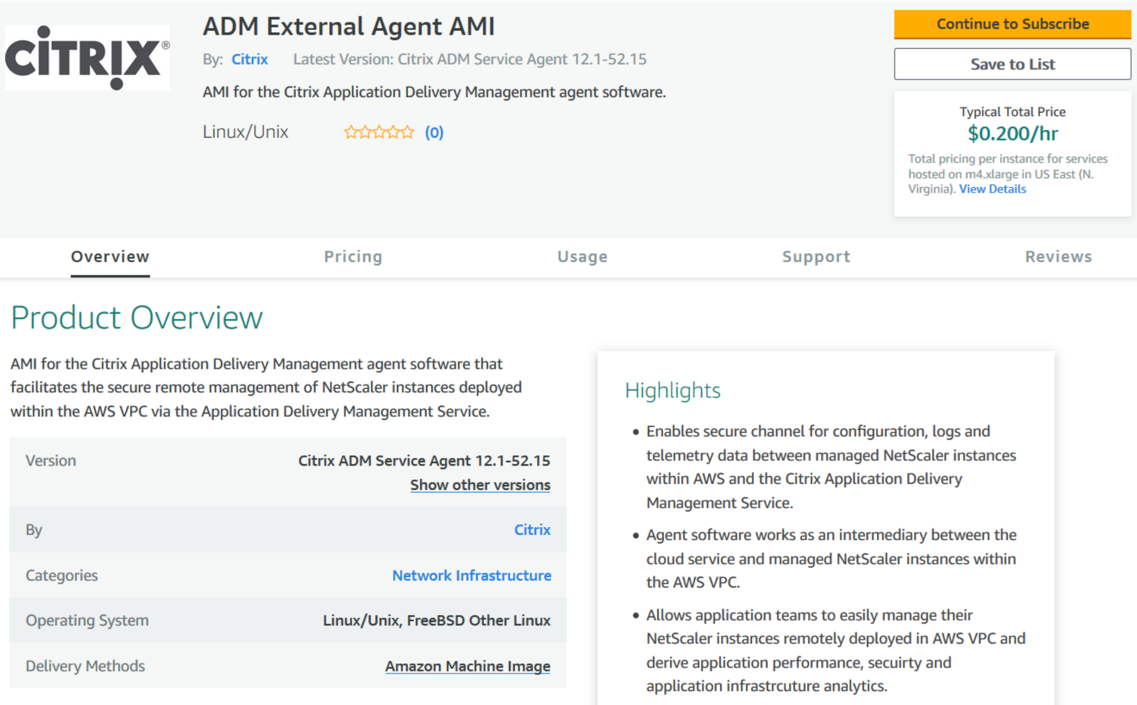
- An AWS account
- An AWS virtual private cloud (VPC)
- An IAM account

> **Note**
>
> - Before you provision a Citrix ADM agent virtual machine, Citrix recommends creating security group, virtual private network, key pair, subnet, and other entities. So, the network information is available during provisioning.
> - For a Citrix ADM agent to communicate with the Citrix Application Delivery and Manage-

> ment, and the Citrix ADC instances, ensure that the recommended ports are open. For complete details about the port requirements for a Citrix ADM agent, see Ports.

To install the Citrix ADM agent on AWS:

1. Log on to the AWS marketplace by using your AWS credentials.
2. In the search field, type **Citrix ADM agent** to search for the Citrix ADM agent AMI, and click **Go**.
3. On the search result page, click the **Citrix Application Delivery and Management External agent AMI** from the available list.
4. On the **Citrix Application Delivery and Management External Agent AMI** page, click **Continue to Subscribe**.



ADM External Agent AMI

By: Citrix Latest Version: Citrix ADM Service Agent 12.1-52.15

AMI for the Citrix Application Delivery Management agent software.

Linux/Unix

Typical Total Price
$0.200/hr
Total pricing per instance for services hosted on m4.xlarge in US East (N. Virginia). View Details

Product Overview

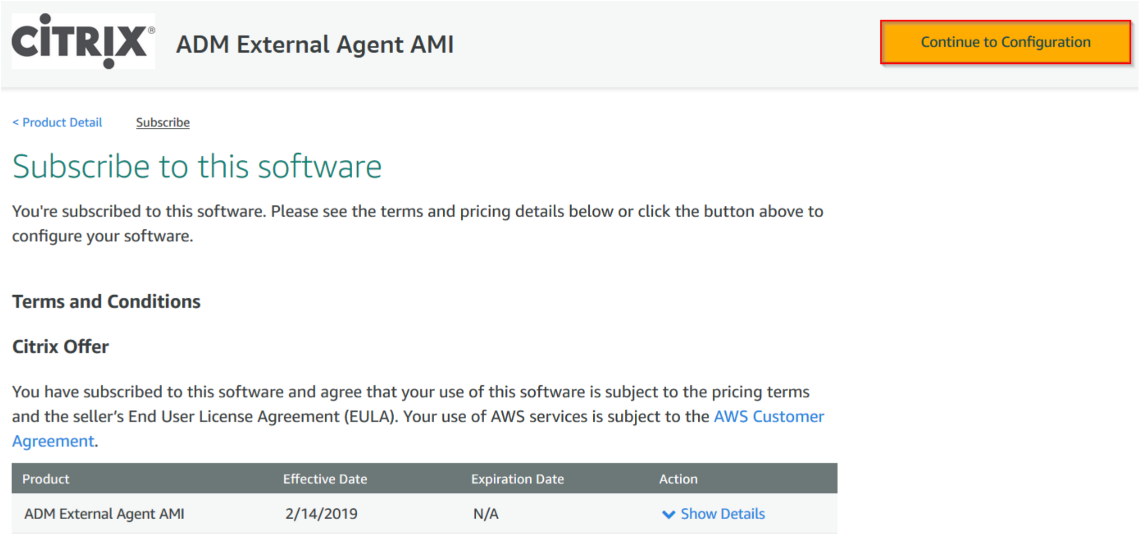
AMI for the Citrix Application Delivery Management agent software that facilitates the secure remote management of NetScaler instances deployed within the AWS VPC via the Application Delivery Management Service.

Version	Citrix ADM Service Agent 12.1-52.15 Show other versions
By	Citrix
Categories	Network Infrastructure
Operating System	Linux/Unix, FreeBSD Other Linux
Delivery Methods	Amazon Machine Image

Highlights

- Enables secure channel for configuration, logs and telemetry data between managed NetScaler instances within AWS and the Citrix Application Delivery Management Service.
- Agent software works as an intermediary between the cloud service and managed NetScaler instances within the AWS VPC.
- Allows application teams to easily manage their NetScaler instances remotely deployed in AWS VPC and derive application performance, secuirty and application infrastrcuture analytics.

5. After the subscription is successful, click **Continue to Configuration**.



Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

Citrix Offer

You have subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). Your use of AWS services is subject to the AWS Customer Agreement.

Product	Effective Date	Expiration Date	Action
ADM External Agent AMI	2/14/2019	N/A	Show Details

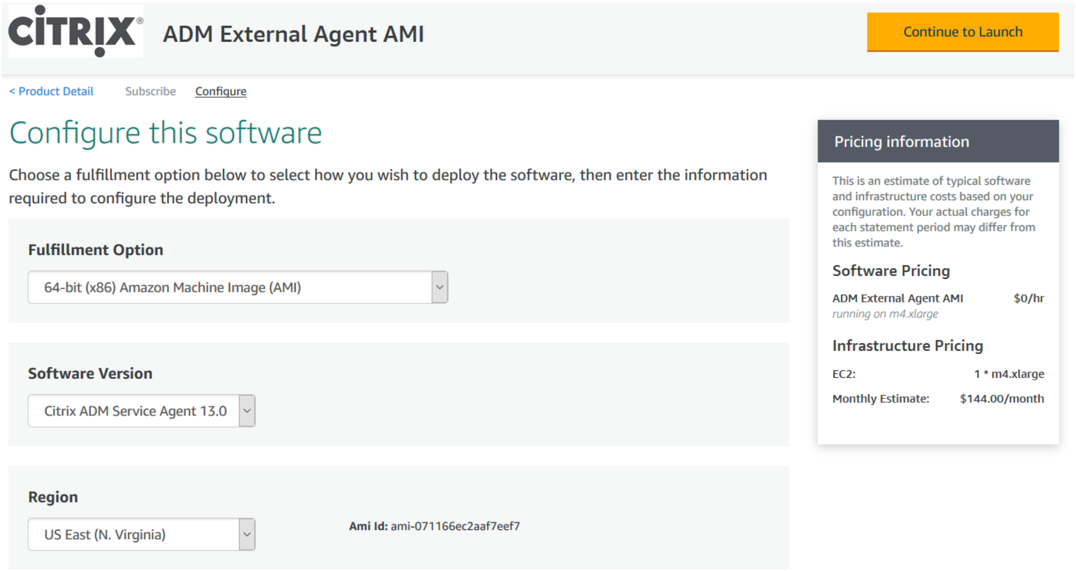
6. On the **Configure this software** page:

   a) Select the AMI from the **Fulfillment option** list.

   b) Select the latest Citrix ADM agent version from the **Software Version** list.

   c) Select your region from the **Region** list.

   d) Click **Continue to Launch**



Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option: 64-bit (x86) Amazon Machine Image (AMI)

Software Version: Citrix ADM Service Agent 13.0

Region: US East (N. Virginia)

Ami Id: ami-071166ec2aaf7eef7

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

ADM External Agent AMI *running on m4.xlarge*	$0/hr

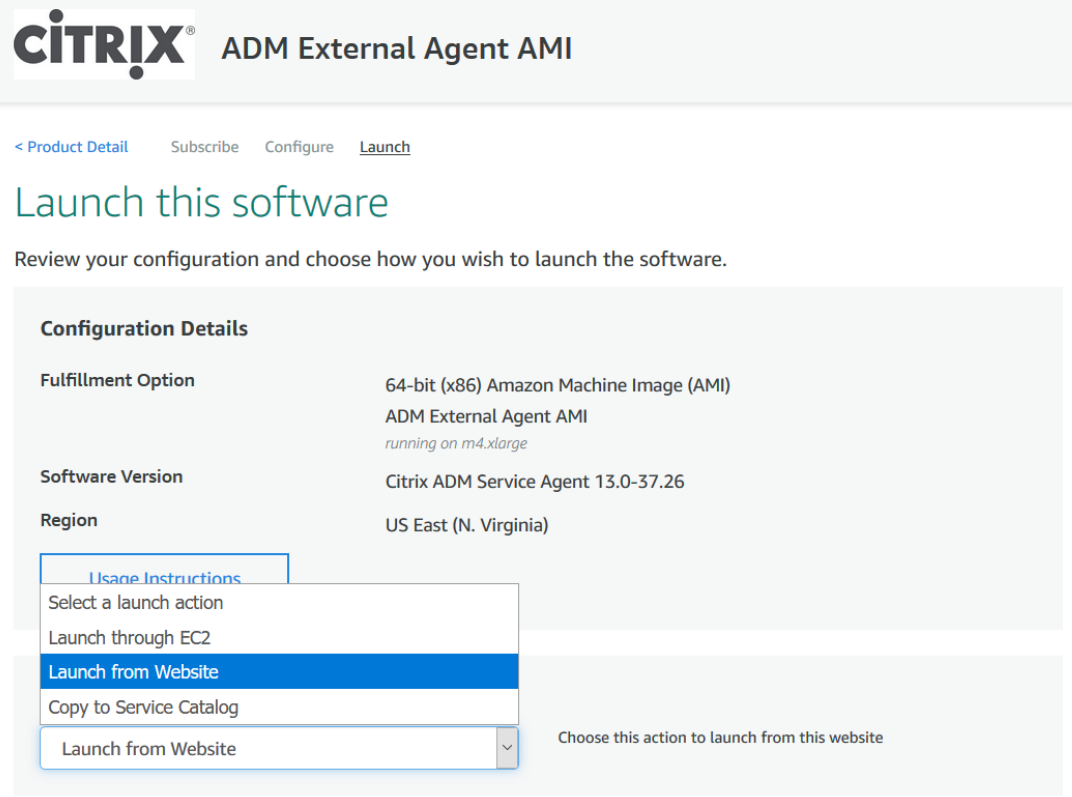
Infrastructure Pricing

EC2:	1 * m4.xlarge
Monthly Estimate:	$144.00/month

7. On the **Launch this software** page, you have two options to register the Citrix ADM agent:

   a) **Launch from Website**

   b) **Launch with EC2**



Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option: 64-bit (x86) Amazon Machine Image (AMI)
ADM External Agent AMI
running on m4.xlarge

Software Version: Citrix ADM Service Agent 13.0-37.26

Region: US East (N. Virginia)

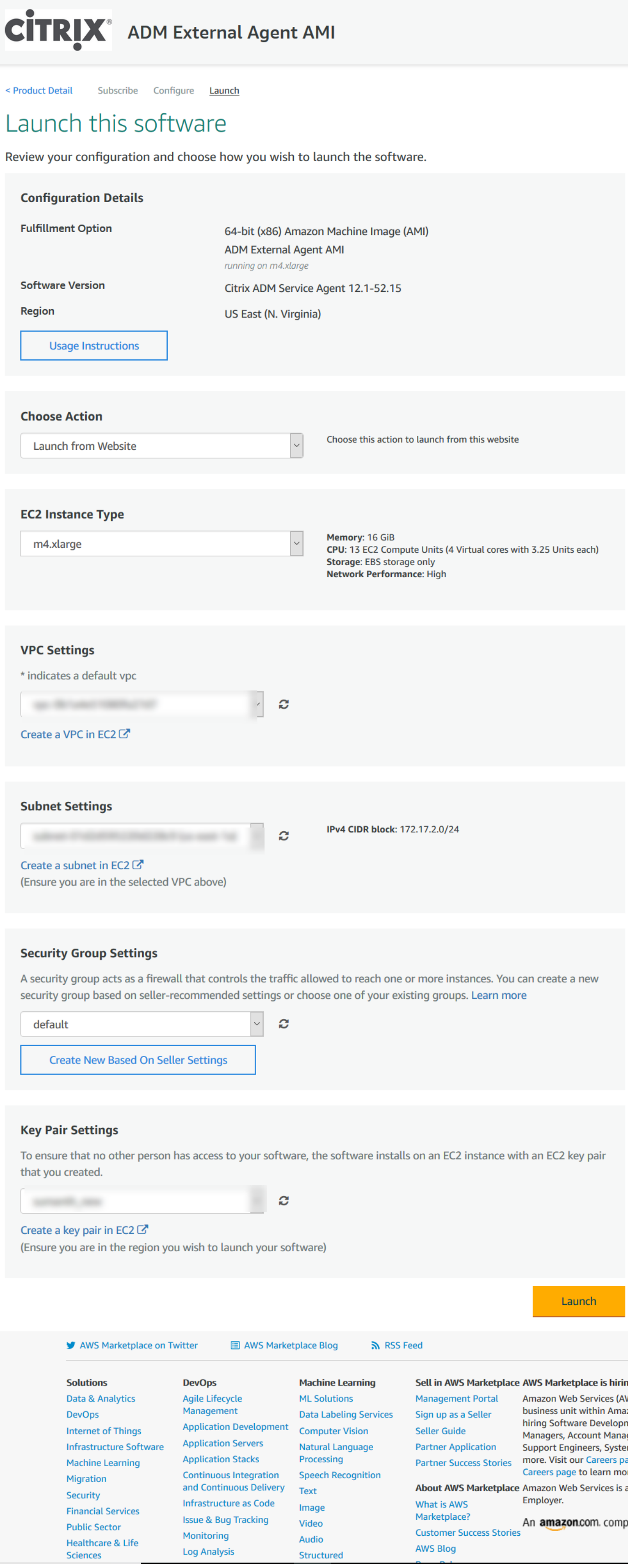
Launch from Website

Choose this action to launch from this website

Launch from a Website

To launch from a Website, select:

1. An EC2 instance type from the **EC2 Instance Type** list
2. A VPC from the **VPC Settings** list. Click **Create a VPC in EC2** to create a VPC for your software.
3. A Subnet from the **Subnet Settings** list. Click **Create a subnet in EC2** to create a subnet after you selected the VPC.
4. A security group for the firewall from the **Security Group Settings** list. Click **Create New Based On Seller Settings** to create a security group.
5. A key pair to ensure access security from the **Key Pair Settings** list. Click **Create a key pair in EC2** to create a key pair for your software.
6. Click **Launch**



ADM External Agent AMI

< Product Detail Subscribe Configure Launch

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option: 64-bit (x86) Amazon Machine Image (AMI)
ADM External Agent AMI
running on m4.xlarge

Software Version: Citrix ADM Service Agent 12.1-52.15

Region: US East (N. Virginia)

Usage Instructions

Choose Action

Launch from Website

Choose this action to launch from this website

EC2 Instance Type

m4.xlarge

Memory: 16 GiB
CPU: 13 EC2 Compute Units (4 Virtual cores with 3.25 Units each)
Storage: EBS storage only
Network Performance: High

VPC Settings

* indicates a default vpc

[redacted]

Create a VPC in EC2

Subnet Settings

[redacted]

IPv4 CIDR block: 172.17.2.0/24

Create a subnet in EC2
(Ensure you are in the selected VPC above)

Security Group Settings

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. You can create a new security group based on seller-recommended settings or choose one of your existing groups. Learn more

default

Create New Based On Seller Settings

Key Pair Settings

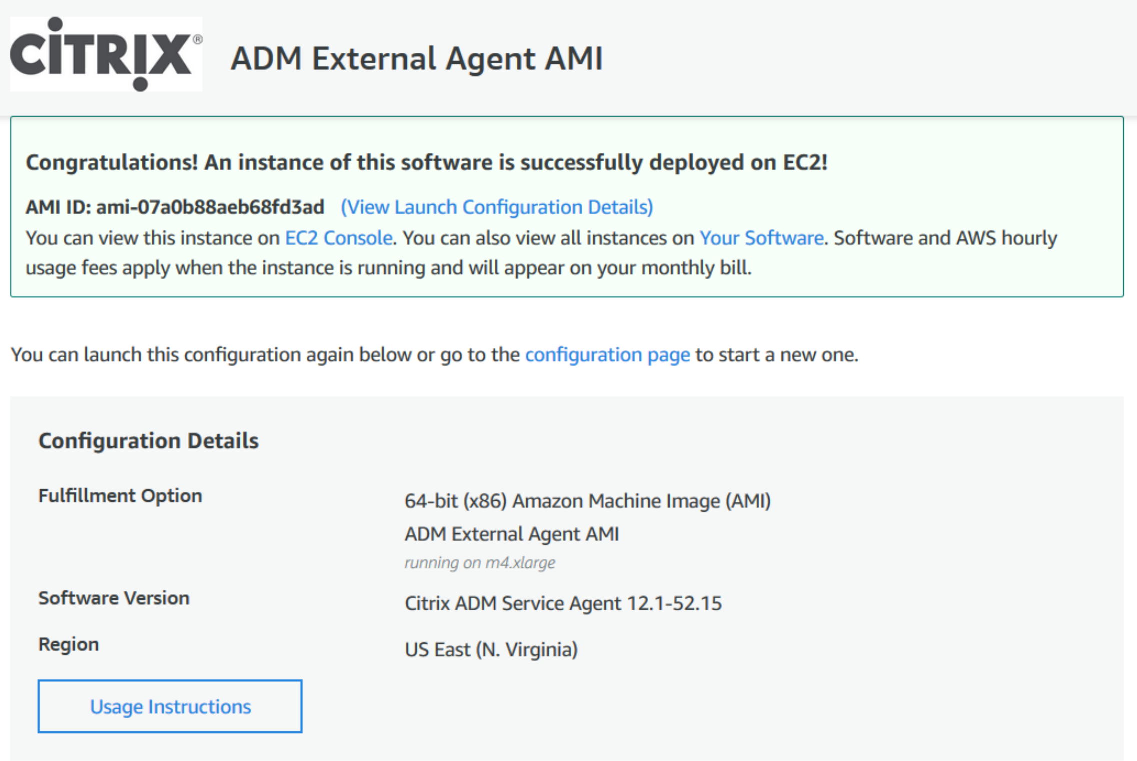
To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created.

[redacted]

Create a key pair in EC2
(Ensure you are in the region you wish to launch your software)

Launch

7. The launch from a Website is successful.



ADM External Agent AMI

Congratulations! An instance of this software is successfully deployed on EC2!

AMI ID: ami-07a0b88aeb68fd3ad (View Launch Configuration Details)

You can view this instance on EC2 Console. You can also view all instances on Your Software. Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.

You can launch this configuration again below or go to the configuration page to start a new one.

Configuration Details

Fulfillment Option	64-bit (x86) Amazon Machine Image (AMI) ADM External Agent AMI *running on m4.xlarge*
Software Version	Citrix ADM Service Agent 12.1-52.15
Region	US East (N. Virginia)

> **Note**
>
> The deployment process might take approximately 10–15 minutes. After the deployment is successfully completed, you can view your Citrix ADM agent virtual machine on your AWS account.

8. Once the agent is deployed, assign a name for your Citrix ADM agent.

9. Once the agent is up and running, assign an elastic IP address for your Citrix ADM agent.

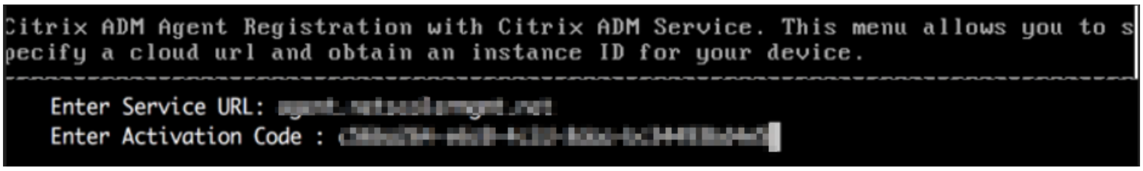
> **Note**
>
> Elastic IP address enables Citrix ADM agent to communicate with Citrix Application Delivery and Management. But, an elastic IP address might not be required if you have configured NAT Gateway to route the traffic to the Internet.

10. Using an SSH client, log on to your Citrix ADM agent using the public IP address.

> **Note**
>
> You can log on to the Citrix ADM agent using one of the following ways:
>
> - Use `nsrecover` as the user name and AWS instance ID as the password.
> - Use `nsroot` as the user name and a valid keypair as the password.

11. Enter the following command to invoke the deployment screen: **deployment_type.py**

12. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in Citrix Application Delivery and Management as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.



```
itrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
--------------------------------------------------------------------------------
   Enter Service URL: [redacted]
   Enter Activation Code : [redacted]
```

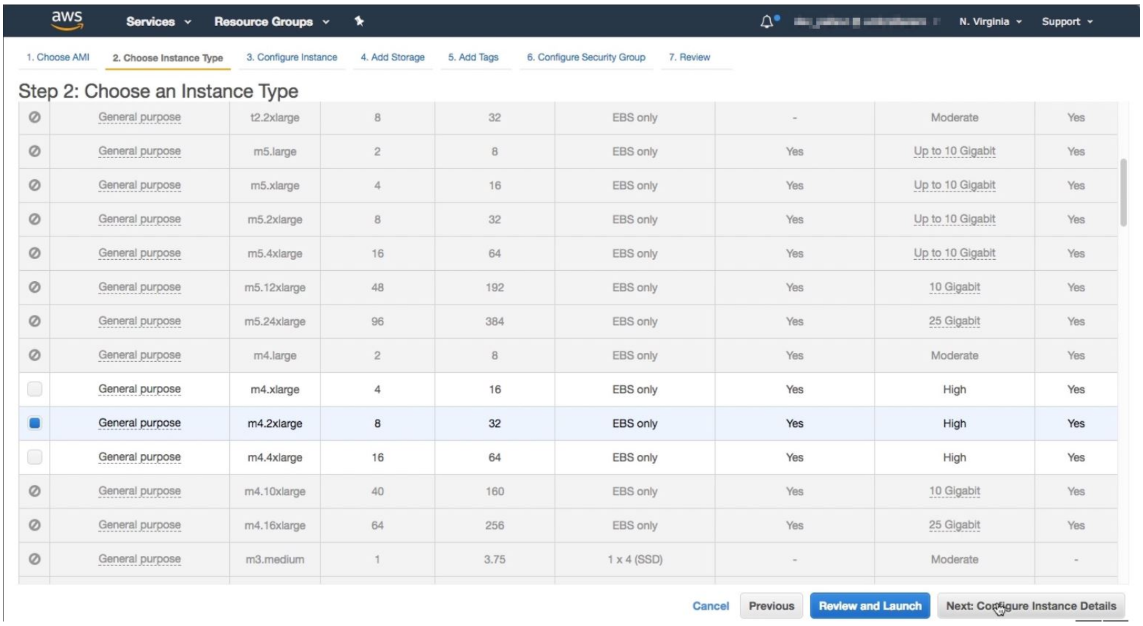
After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access Citrix Application Delivery and Management and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Launch with EC2

To launch with EC2, select **Launch through EC2** from the **Choose Action** list, and then click **Launch**.

1. On the **Choose an Instance Type** page, select the instance, and click **Next: Configure Instance Details**.



Step 2: Choose an Instance Type

⊘	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
⊘	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
⊘	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
⊘	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
⊘	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
☐	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
■	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
☐	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes
⊘	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit	Yes
⊘	General purpose	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes
⊘	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate	-

2. On the **Configure Instance Details** page, specify the required parameters.

   Under the **Advanced Details** section, you can enable a zero-touch agent by specifying authentication details or a script in the **User data** field.

   - **Authentication details** - Specify the **Service-URL** and **Activation code** that you copied from the **Set Up Agents** page in Citrix Application Delivery and Management as instructed in Getting Started. Enter the details in the following format.

```
registeragent -serviceurl <apigatewayurl> -activationcode <activationcodevalue>
<!--NeedCopy-->
```

Agent uses this information to auto-register with the Citrix Application Delivery and Management during boot-up.

- **Script** - Specify an agent auto-registration script as user data. The following is an example script:

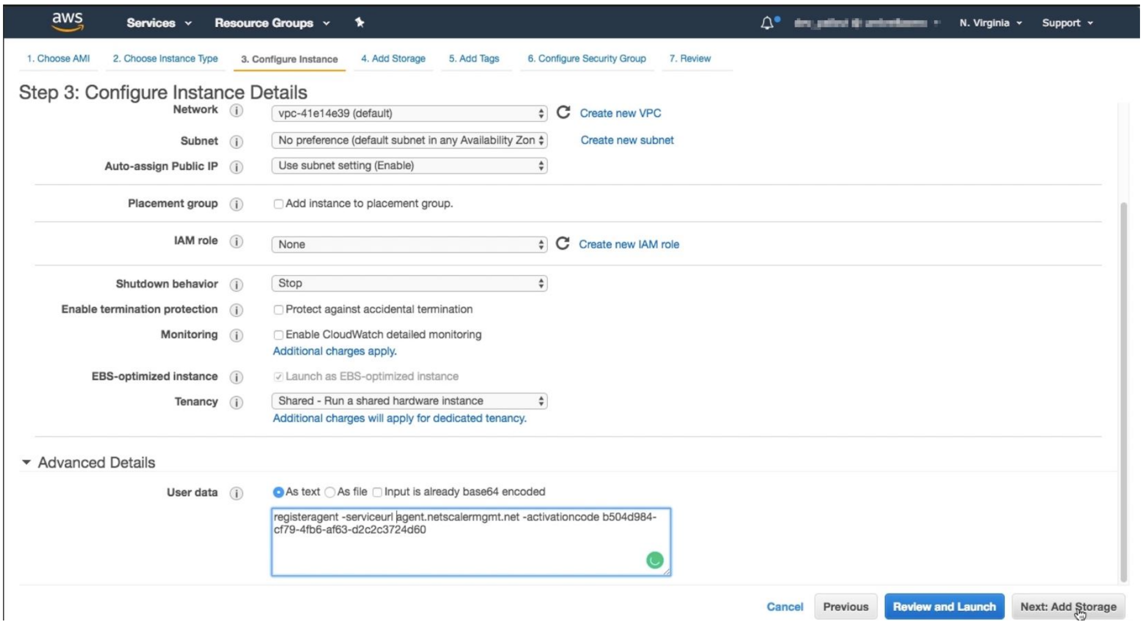
```
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Overview of the Script:
The script helps to register a Citrix ADM agent with Citrix Application Delivery and Management. Pass it in userdata to make Citrix ADM agent in AWS to autoregister on bootup.  The workflow is as follows
1)  Fetch the Citrix Application Delivery and Management API credentials (ID and secret) from AWS secret store (NOTE: you have to assign IAM role to the Citrix ADM agent that will give permission to fetch secrets from AWS secret store)
2)  Login to Citrix Application Delivery and Management with credentials fetched in step 1
3)  Call Citrix Application Delivery and Management to fetch credentials (serviceURL and token) for agent registration
4)  Calls registration by using the credentials fetched in step 3
'''

'''
These are the placeholders which you need to replace according to your setup configurations
aws_secret_id: Id of the AWS secret where you have stored Citrix Application Delivery and Management Credentials
```

```
The secrets value should be in the following json format
{
 "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "YOUR_SECRET" }

'''


aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Set up a specific logger with your desired output level and log file name
'''
log_file_name_local = os.path.basename(__file__)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50*1024*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(__name__)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s', datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def __init__(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def __str__(self):
        return self.message + ". Error code '" + str(self.error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
"errorcode": "500", "message": "Error while reading response.
```

```
    " }

            return resp

        if print_response:
            logger.debug('Response text for %s is %s' % (url, response.text))

        response = json.loads(response.text)
        logger.debug("ErrorCode - " + str(response['errorcode']) + ". Message -" + str(response['message']))
        raise APIHandlerException(response['errorcode'], str(response['message']))
    elif response.text:
        if print_response:
            logger.debug('Response text for %s is %s' % (url, response.text))

        result = json.loads(response.text)
        if 'errorcode' in result and result['errorcode'] > 0:
            raise APIHandlerException(result['errorcode'], str(result['message']))
        return result

def _request(method, url, data=None, headers=None, retry=3, print_response=True):
    try:
        response = requests.request(method, url, data=data, headers=headers)
        result = parse_response(response, url, print_response=print_response)
        return result
    except [requests.exceptions.ConnectionError, requests.exceptions.ConnectTimeout]:
        if retry > 0:
            return _request(method, url, data, headers, retry -1, print_response=print_response)
        else:
            raise APIHandlerException(503, 'ConnectionError')
    except requests.exceptions.RequestException as e:
        logger.debug(str(e))
        raise APIHandlerException(500, str(e))
    except APIHandlerException as e:
        logger.debug("URL: %s, Error: %s, Message: %s" % (url, e.error_code, e.message))
        raise e
    except Exception as e:
        raise APIHandlerException(500, str(e))

try:
    '''Get the AWS Region'''
    client = boto3.client('s3')
    my_region = client.meta.region_name
    logger.debug("The rgion is %s" % (my_region))

    '''Creating a Boto cleint session'''
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=my_region
    )

    '''Getting the values stored in the secret with id: <aws_secret_id>'''
    get_id_value_response = client.get_secret_value(
        SecretId = aws_secret_id
    )
    adm_user_id = json.loads(get_id_value_response["SecretString"])["adm_user_id_key"]
    adm_user_secret = json.loads(get_id_value_response["SecretString"])["adm_user_secret_key"]

except Exception as e:
    logger.debug("Fetching of Citrix Application Delivery and Management credentials from AWS secret failed with error: %s" % (str(e)))
    raise e

'''
Initializing common Citrix Application Delivery and Management API handlers
'''
mas_common_headers = {

    'Content-Type': "application/json",
    'Accept-type': "application/json",
    'Connection': "keep-alive",
    'isCloud': "true"
 }

```

```

    '''
    API to login to the Citrix Application Delivery and Management and fetch the Session ID and Tenant ID
    '''
    url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/login"
    payload = 'object={
    "login":{
    "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"}
     }
    '
    try:
        response = _request("POST", url, data=payload, headers=mas_common_headers)
        sessionid = response["login"][0]["sessionid"]
        tenant_id = response["login"][0]["tenant_name"]
    except Exception as e:
        logger.debug("Login call to the Citrix Application Delivery and Management failed with error: %s" % (str(e)))
        raise e

    '''
    API to fetch the service URL and Token to be used for registering the agent with the Citrix Application Delivery and Management
    '''
    mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
    url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/trust_preauthtoken/" + tenant_id +"?customer="+tenant_id
    logger.debug("Fetching Service URL and Token.")
    try:
        response = _request("GET", url, data=None, headers=mas_common_headers)
        service_name  = response["trust_preauthtoken"][0]["service_name"]
        token = response["trust_preauthtoken"][0]["token"]
        api_gateway_url = response["trust_preauthtoken"][0]["api_gateway_url"]
    except Exception as e:
        logger.debug("Fetching of the Service URL Passed with error. %s" % (str(e)))
        raise e

    '''
    Running the register agent command using the values we retrieved earlier
    '''
    try:
        registeragent_command = "registeragent -serviceurl "+api_gateway_url+" -activationcode "+service_name+"\;"+token
        file_run_command = "/var/python/bin/python2.7 /mps/register_agent_cloud.py "+registeragent_command
        logger.debug("Executing registeragent command: %s" % (file_run_command))
        os.system(file_run_command)
    except Exception as e:
        logger.debug("Agent Registeration failed with error: %s" % (str(e)))
            raise e
    <!--NeedCopy-->
```

This script fetches the authentication details from the AWS secrets manager and runs the `deployment.py` script to register the agent with the Citrix Application Delivery and Management.



Step 3: Configure Instance Details

Network: vpc-41e14e39 (default)

Subnet: No preference (default subnet in any Availability Zon

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group.

IAM role: None

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring

EBS-optimized instance: ☑ Launch as EBS-optimized instance

Tenancy: Shared - Run a shared hardware instance

Advanced Details

User data: ● As text ○ As file □ Input is already base64 encoded

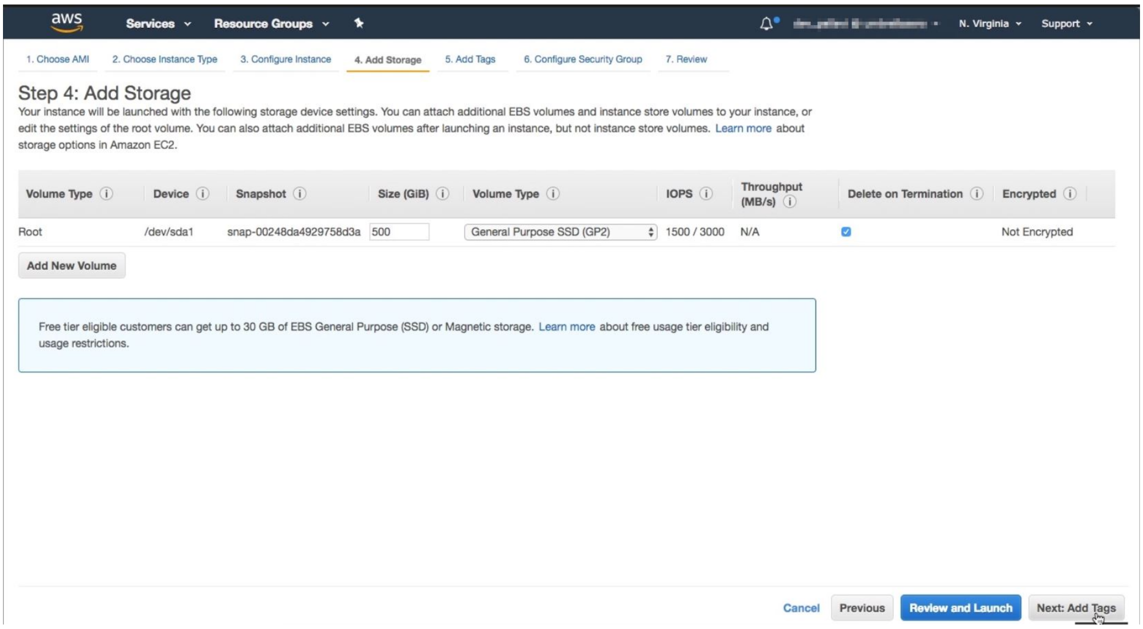
```
registeragent -serviceurl agent.netscalermgmt.net -activationcode b504d984-cf79-4fb6-af63-d2c2c3724d60
```

> **Note**
>
> While you can auto-assign public IP address, you can also assign elastic IP address. Assign-

> ing an elastic IP address is required when NAT Gateway is not configured.
>
> If the elastic IP address is not set in this step, you can still do it on the EC2 console. You can create a new elastic IP address and associate that with the Citrix ADM agent using the instance ID or ENI-ID.

Click **Add Storage**.

3. On the **Add Storage** page, configure the storage device settings for the instance, and click **Next: Add Tags**.



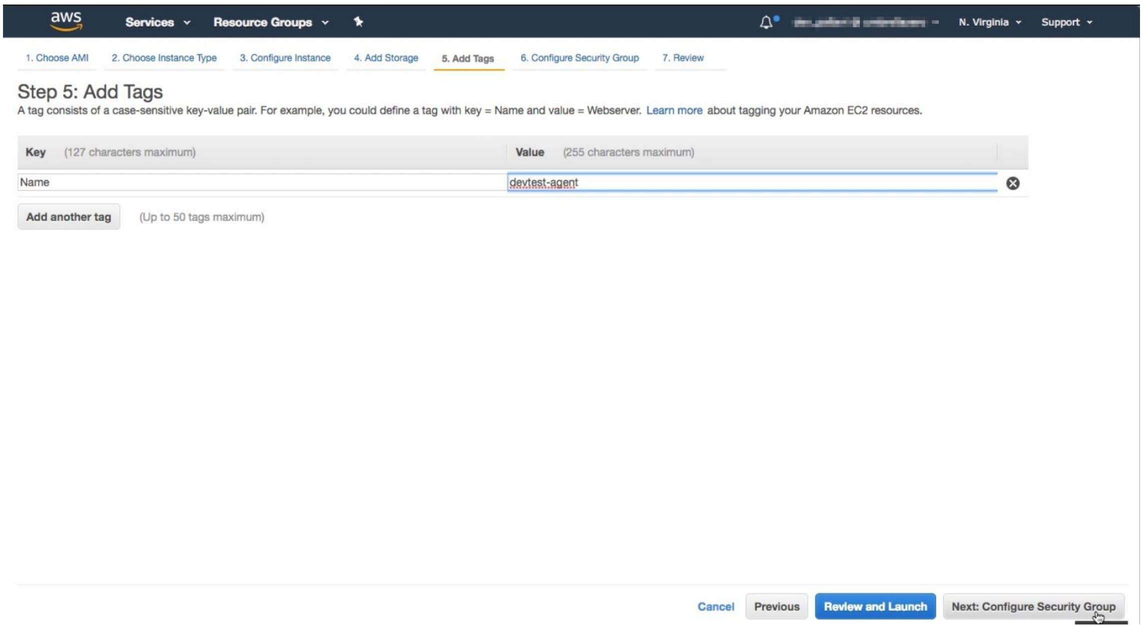
Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-00248da4929758d3a	500	General Purpose SSD (GP2)	1500 / 3000	N/A	☑	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

4. On the **Add Tags** page, define the tag for the instance, and click **Next: Configure Security Group**.



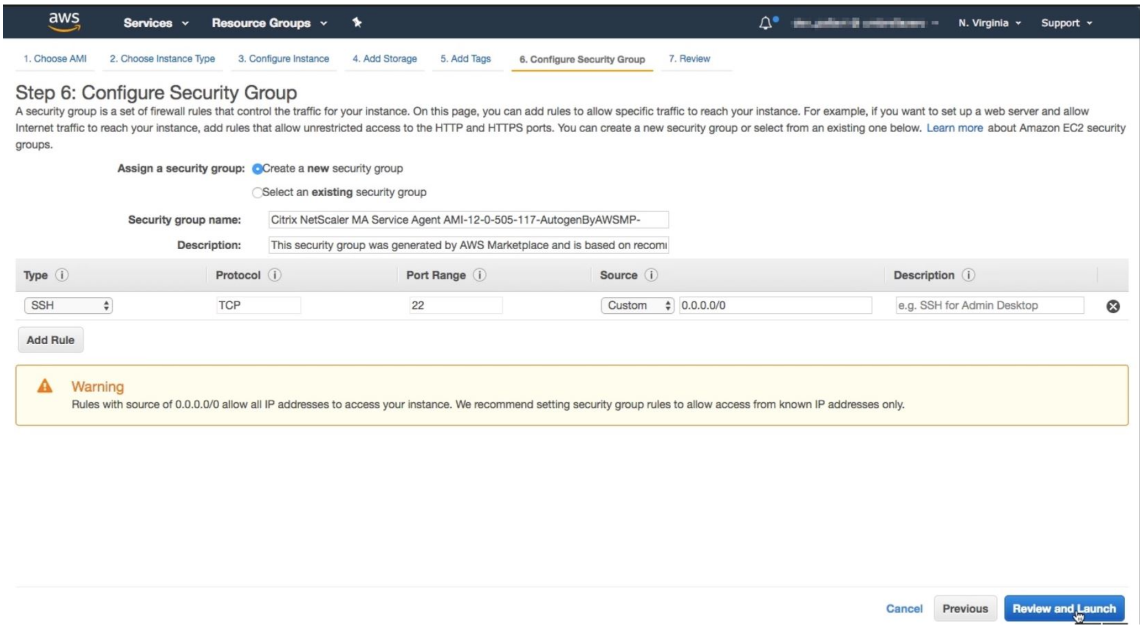
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	devtest-agent

(Up to 50 tags maximum)

5. On the **Configure Security Group** page, add rules to allow specific traffic to your instance and click **Review and Launch**.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Citrix NetScaler MA Service Agent AMI-12-0-505-117-AutogenByAWSMP-

Description: This security group was generated by AWS Marketplace and is based on recomi

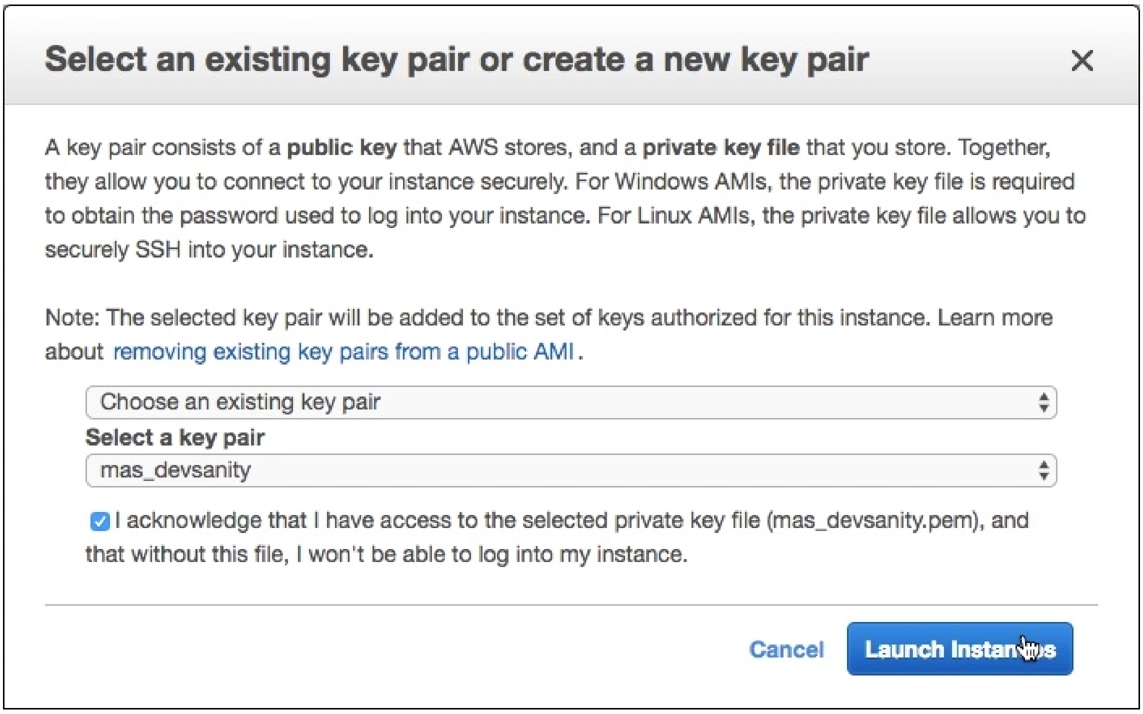
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

6. On the **Review Instance Launch** page, review the instance settings and click **Launch**.

7. In the **Select an existing key pair or create a new key pair** dialog box, create a key pair. You can also select from the existing key pairs.

   Accept the acknowledgment and click **Launch Instances**.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair
mas_devsanity

☑ I acknowledge that I have access to the selected private key file (mas_devsanity.pem), and that without this file, I won't be able to log into my instance.

The deployment process might take approximately 10–15 minutes. After the deployment is successfully completed, you can view your Citrix ADM agent virtual machine on your AWS account.

Install an agent on GCP

October 18, 2021

The Citrix ADM agent works as an intermediary between the Citrix Application Delivery and Management and the discovered instances in the data center or on the cloud. You can deploy the agent on the Google Cloud Platform (GCP) to facilitate the secure remote management of Citrix ADC instances deployed within the Google cloud virtual network through Citrix Application Delivery and Management. For more information about how the Citrix ADM agent on GCP delivers for IT admins, read the blog Citrix ADM agent is now available on the Google Cloud Platform Marketplace.

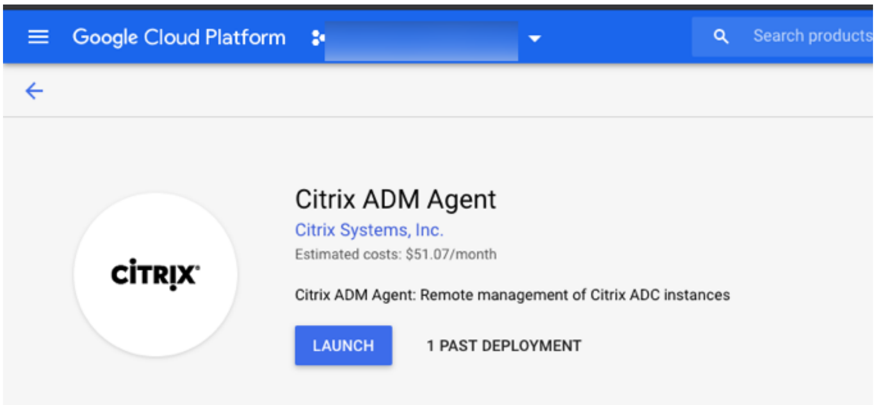
Prerequisites

To install a Citrix ADM agent on GCP, you need a GCP account.

Install the Citrix ADM agent on GCP

Follow these steps to install a Citrix ADM agent on GCP.

1. Log on to the GCP console (console.cloud.google.com) using your credentials and go to the marketplace.
2. In the search field, type **Citrix ADM agent**.
3. Click **Citrix ADM agent** from the results field and then click **Launch**.



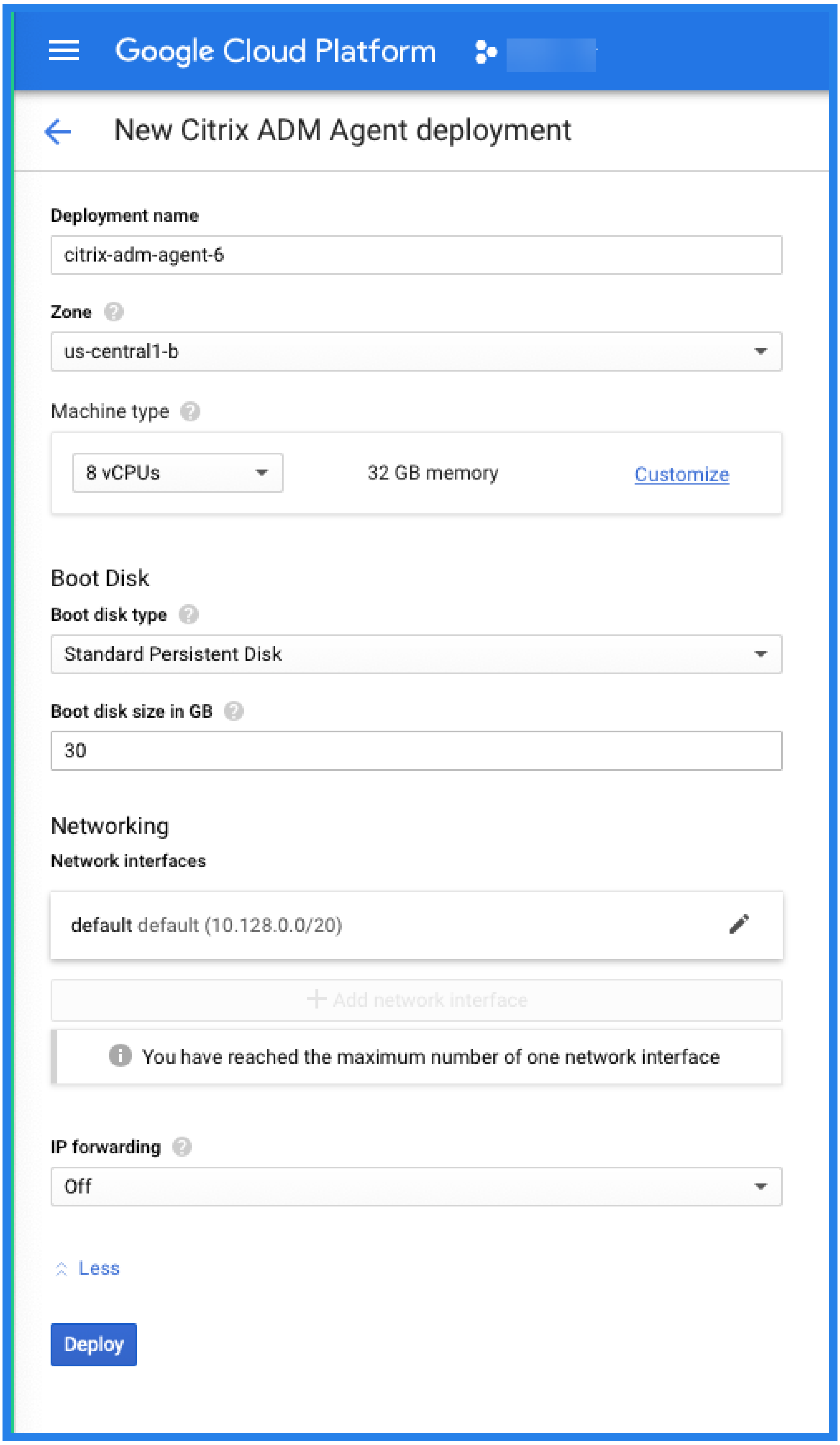
Citrix ADM Agent

Citrix Systems, Inc.

Estimated costs: $51.07/month

Citrix ADM Agent: Remote management of Citrix ADC instances

4. In the **New Citrix ADM agent deployment** page, most of the options are set by default. You can change the default configurations as required and click **Deploy**.



New Citrix ADM Agent deployment

Deployment name: citrix-adm-agent-6

Zone: us-central1-b

Machine type: 8 vCPUs, 32 GB memory

Boot Disk

Boot disk type: Standard Persistent Disk

Boot disk size in GB: 30

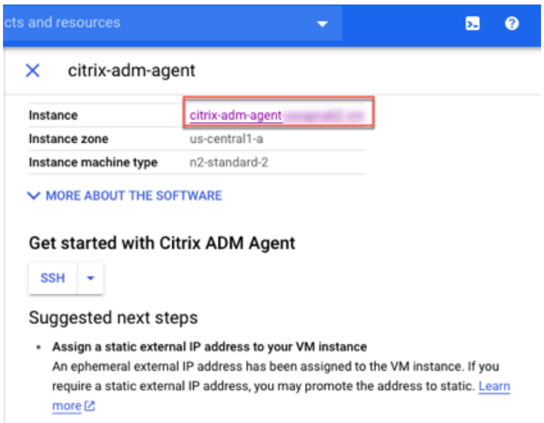
Networking

Network interfaces: default default (10.128.0.0/20)

You have reached the maximum number of one network interface

IP forwarding: Off

5. After the agent is deployed, click the instance link and check the details in the **VM instance details page**.

   citrix-adm-agent

Instance	citrix-adm-agent[redacted]
Instance zone	us-central1-a
Instance machine type	n2-standard-2

   Get started with Citrix ADM Agent

   Suggested next steps

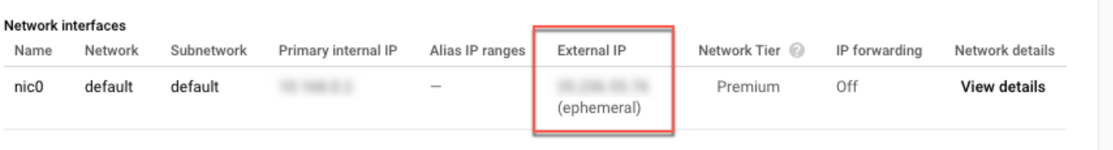
   - **Assign a static external IP address to your VM instance**
     An ephemeral external IP address has been assigned to the VM instance. If you require a static external IP address, you may promote the address to static. Learn more

6. Log on to the agent through an SSH client using the agent external IP address. Use the following commands:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

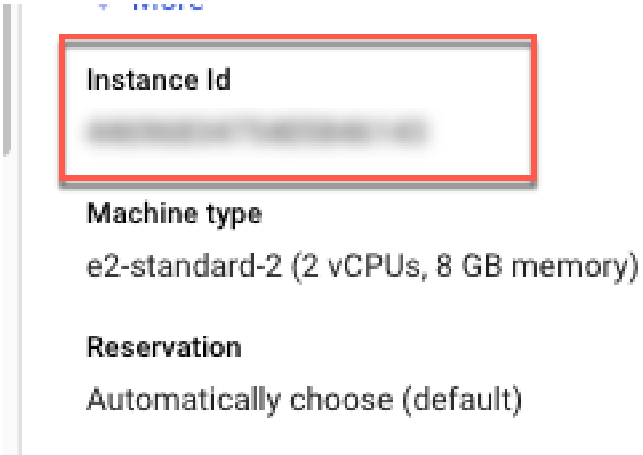
   Password: Instance ID

   Can you find the external IP address and the instance ID in the **VM instance details** page.

   Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	[redacted]	–	[redacted] (ephemeral)	Premium	Off	View details

   Instance Id

   [redacted]

   Machine type

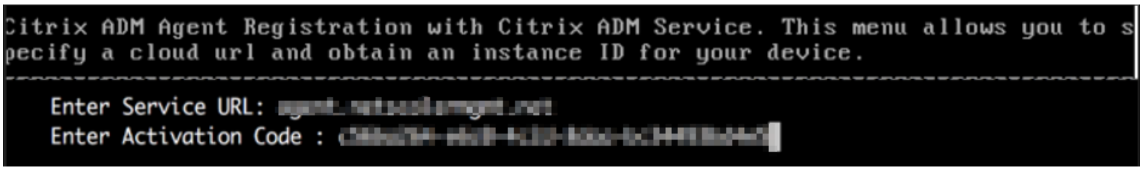
   e2-standard-2 (2 vCPUs, 8 GB memory)

   Reservation

   Automatically choose (default)

7. Enter the following command to invoke the deployment screen: **deployment_type.py**

8. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in Citrix Application Delivery and Management as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.



```
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
--------------------------------------------------------------------------------
    Enter Service URL: [redacted]
    Enter Activation Code : [redacted]
```

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

After the agent has restarted, access Citrix Application Delivery and Management and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Install an agent in Kubernetes cluster

October 14, 2021

> **Note**
>
> The procedure to install an agent as a microservice is available in the Getting Started section.

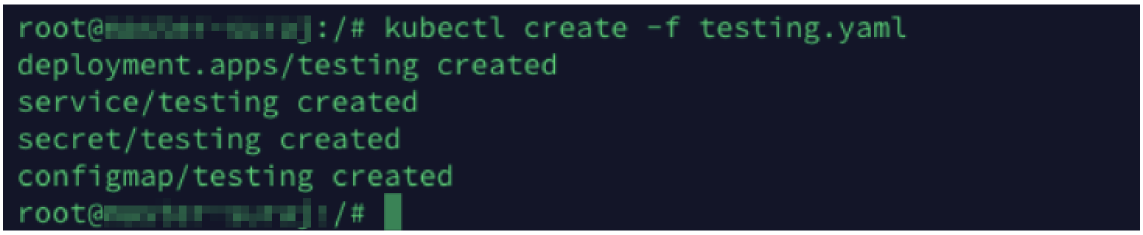
In the Kubernetes master node:

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

   `kubectl create -f <yaml file>`

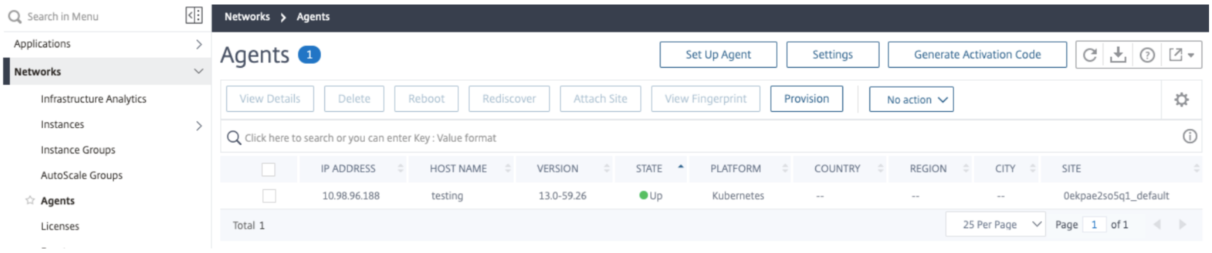
   For example, `kubectl create -f testing.yaml`

   The agent is successfully created.



```
root@[redacted]:/# kubectl create -f testing.yaml
deployment.apps/testing created
service/testing created
secret/testing created
configmap/testing created
root@[redacted]:/#
```

In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Agents** to see the agent status.



□	IP ADDRESS	HOST NAME	VERSION	STATE	PLATFORM	COUNTRY	REGION	CITY	SITE
□	10.98.96.188	testing	13.0-59.26	● Up	Kubernetes	--	--	--	0ekpae2so5q1_default

Total 1   25 Per Page   Page 1 of 1

How to Get Help and Support

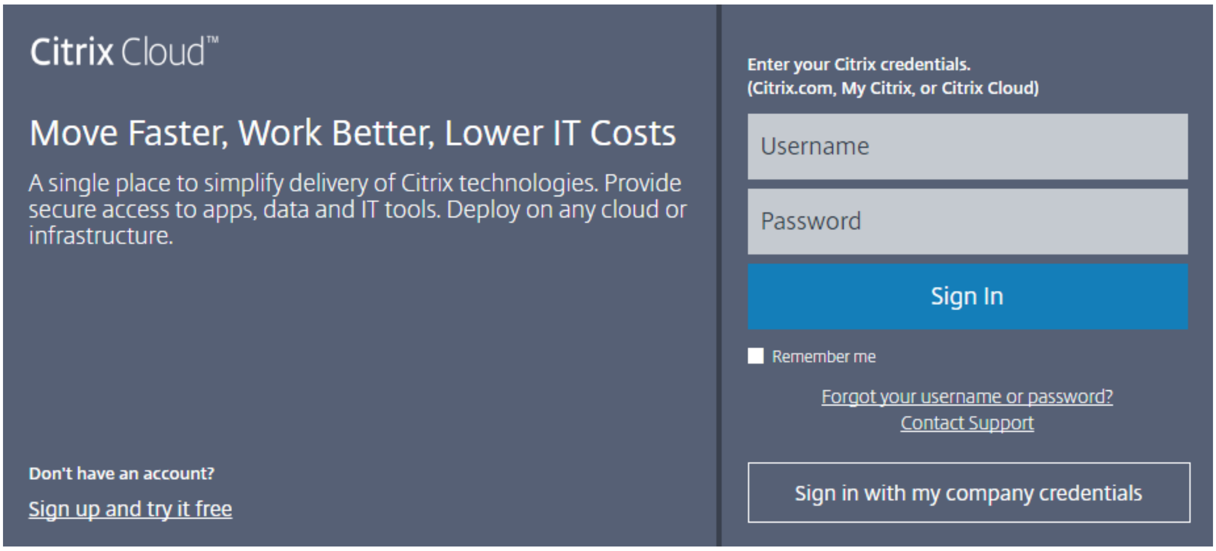
September 23, 2021

As a Citrix Cloud user, sometimes you might need help with making sure a smooth functioning of our infrastructure. This topic provides more information about the different help and supports options and how to access them.

Create a Citrix Cloud account

If you encounter an error when signing up for a Citrix Cloud account, contact Citrix Customer Service.

Sign in to your account



Citrix Cloud™

Move Faster, Work Better, Lower IT Costs

A single place to simplify delivery of Citrix technologies. Provide secure access to apps, data and IT tools. Deploy on any cloud or infrastructure.

Don't have an account?

Sign up and try it free

Enter your Citrix credentials.
(Citrix.com, My Citrix, or Citrix Cloud)

Username
Password
Sign In
□ Remember me
Forgot your username or password?
Contact Support
Sign in with my company credentials

If you're having trouble signing in to your Citrix Cloud account:

- Make sure you sign in with the email address and password you provided when you signed up for your account.
- Citrix Cloud automatically prompts you to reset your password before you can sign in, if:
  - You haven't signed in to Citrix Cloud in a while
  - Your password doesn't meet Citrix Cloud's requirements
- For more information, see Changing your password in this article.
- If your company allows users to sign in to Citrix Cloud using their company credentials instead of a Citrix account, click **Sign in with my company credentials** and enter your company's sign-in URL. You can then enter your company credentials to access your company's Citrix Cloud

account. If you don't know your company's sign-in URL, contact your company's administrator for assistance.

Change your password

If you've forgotten your Citrix Cloud account password, click **Forgot your username or password?**, and you can enter your account email address. You receive an email to reset your password. If you do not receive the password reset email, or you need more assistance, contact Citrix Customer Service.

To help you keep your account password safe and secure, Citrix Cloud might prompt you to reset your password when you attempt to sign in. This prompt occurs if:

- Your password doesn't meet Citrix Cloud's complexity requirements. Passwords must be at least 8 characters long and include:
  - At least one number
  - At least one upper-case letter
  - At least one symbol: `! @ ## $ % ^ * ? + = -`
- Your password includes dictionary words.
- Your password is listed in a known database of compromised passwords.
- You haven't signed in to Citrix Cloud in the last six months.

When prompted, select **Reset Password** to create a new strong password for your account.

Citrix Cloud support forums

On the Citrix Cloud support forums you can get help, provide feedback and improvement suggestions, view conversations from other users, or start your own topics.

Citrix support staff members track these forums and are ready to answer your questions. Other Citrix Cloud community members might also offer help or join the discussion.

You do not need to log in to read forum topics. However, you must log in to post or reply to a topic. To log in, use your existing Citrix account credentials or use the email address and password you provided when you created your Citrix Cloud account. To create a Citrix account, go to Create or request an account.

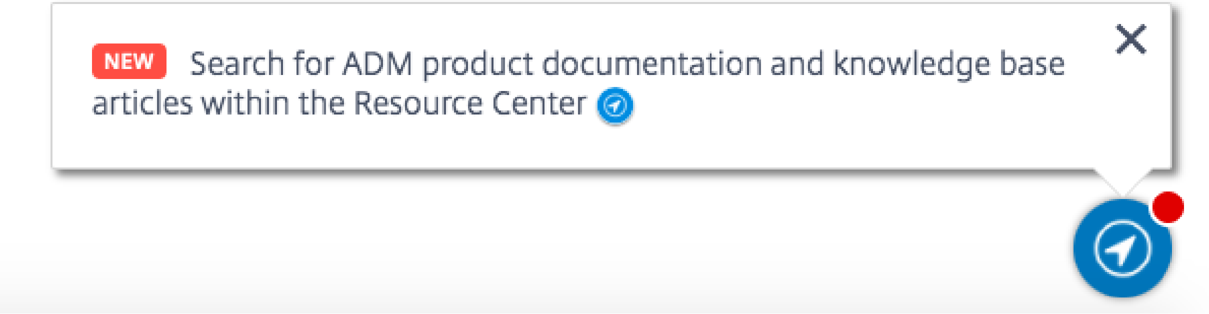
Support articles and documentation

Citrix provides a wealth of product and support content to help you get the most out of Citrix Cloud and resolve many issues you might experience with Citrix products.

Citrix Cloud Resource Center

The Citrix Cloud Resource Center provides several resources to help you get started with Citrix Cloud services, learn more about features, and resolve issues. The resources that appear are applicable to the feature or service in Citrix Cloud that you are currently working with. For example, if you're in the Virtual Apps and Desktops service management console, the Resource Center shows you the following resources.

Access the Resource Center anytime by clicking the blue compass icon in the bottom-right of the Citrix Cloud console.



NEW Search for ADM product documentation and knowledge base articles within the Resource Center

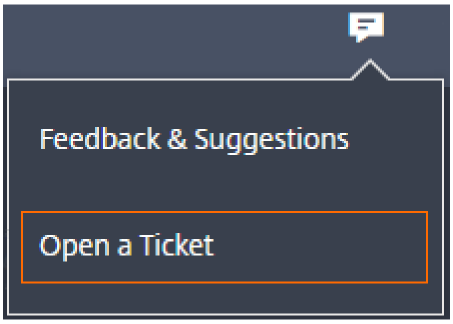
- **Get Started**: Provides a brief guided walkthrough of key tasks specific to the service you're currently working with. You also find links to training and onboarding resources to help you learn more about service capabilities and set up your end-users for success.
- **Announcements**: Provides notifications of newly released features and links to essential Citrix communications. Click a feature notification to receive a brief guided walkthrough of the feature.
- **Search Articles**: Provides a list of product documentation and Knowledge Center articles for common tasks and helps you find more articles, without leaving Citrix Cloud. Enter a search query in the **How do I…** box for a filtered list of articles based on the service you're working with. In general, support articles appear first in the list, followed by product documentation articles.

Citrix Tech Zone

Citrix Tech Zone contains a wealth of information to help you learn more about Citrix Cloud and other Citrix products. Here you find reference architectures, diagrams, videos, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

Technical Support

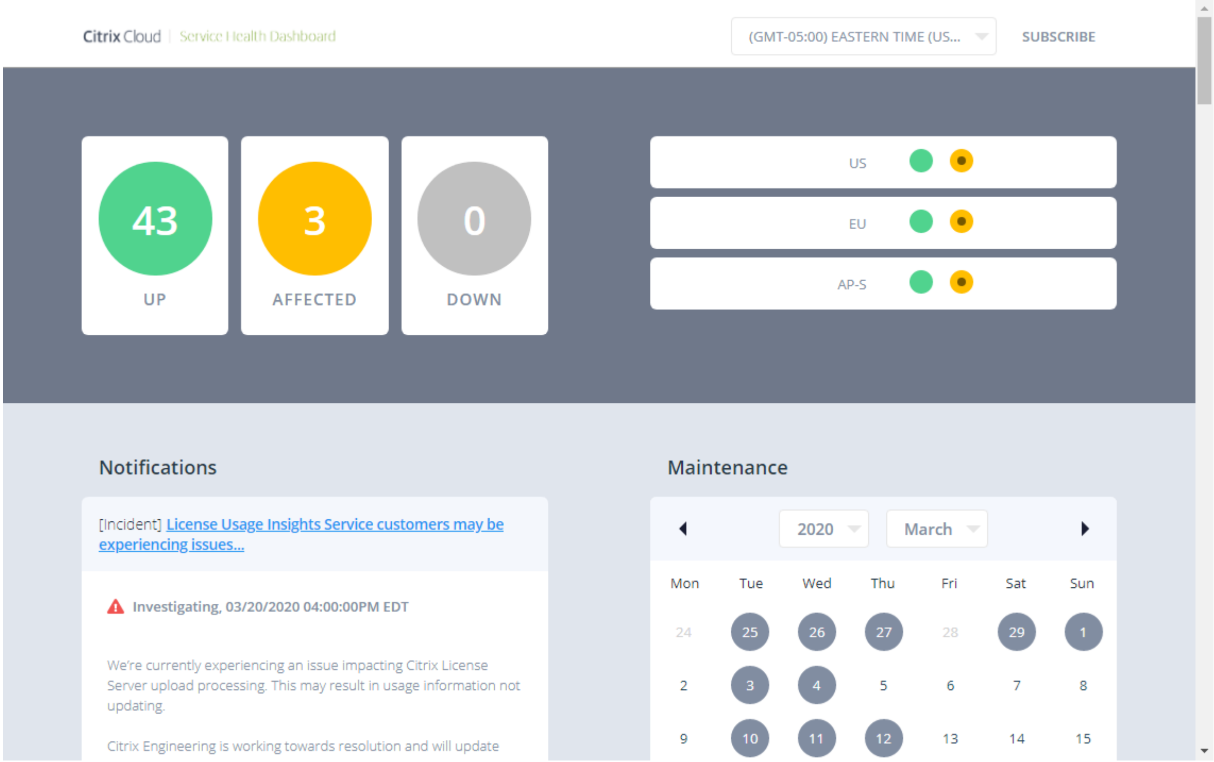
If you're experiencing an issue that requires technical help, click the **Feedback and Support** icon near the top-right of the screen, and then select **Open a Ticket.**



Click **Go to My Support** and then **My Support** to open a ticket through the My Support portal. You can also use the My Support portal to track your existing tickets and view your current product entitlements.

Service Health Dashboard

The Citrix Cloud Service Health Dashboard provides an overview of real-time availability of the Citrix Cloud platform and services in each geographical region. If you experience any issues with Citrix Cloud, check the Service Health Dashboard to verify that Citrix Cloud or specific services are operating normally.


Citrix Cloud | Service Health Dashboard
(GMT-05:00) EASTERN TIME (US...
SUBSCRIBE
43
UP
3
AFFECTED
0
DOWN
US
EU
AP-S
Notifications
Maintenance
2020
March

[Incident] License Usage Insights Service customers may be experiencing issues...

Investigating, 03/20/2020 04:00:00PM EDT

We're currently experiencing an issue impacting Citrix License Server upload processing. This may result in usage information not updating.

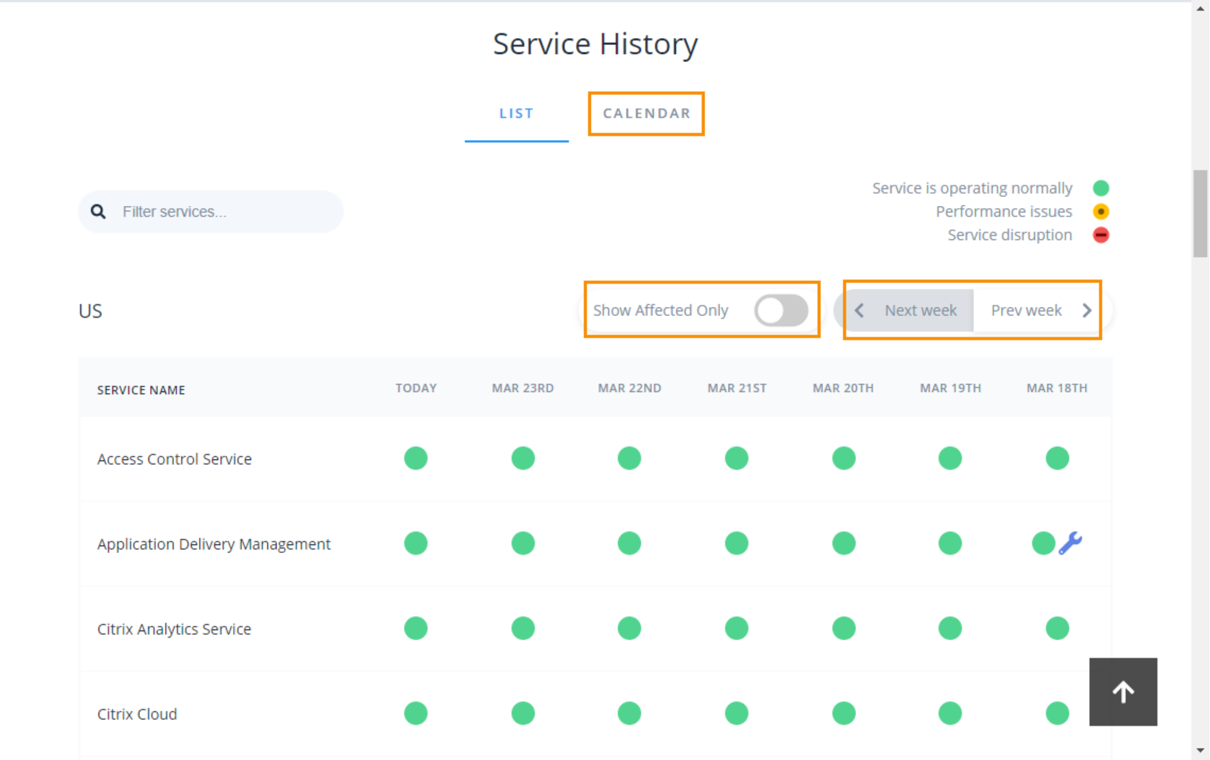
Citrix Engineering is working towards resolution and will update

Mon	Tue	Wed	Thu	Fri	Sat	Sun
24	25	26	27	28	29	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15

Use the dashboard to learn more about the following conditions:

- The current availability status of all Citrix Cloud services, grouped by geographical region
- The service health history of each service for the last seven days (default) or for previous seven-day increments
- Maintenance windows for specific services

By default, service health status is displayed as a list, but you can also display the status in a calendar view. Select **Next** or **Previous** to scroll through the service health history in seven-day increments. You can also filter the list to display affected services only.



Service History

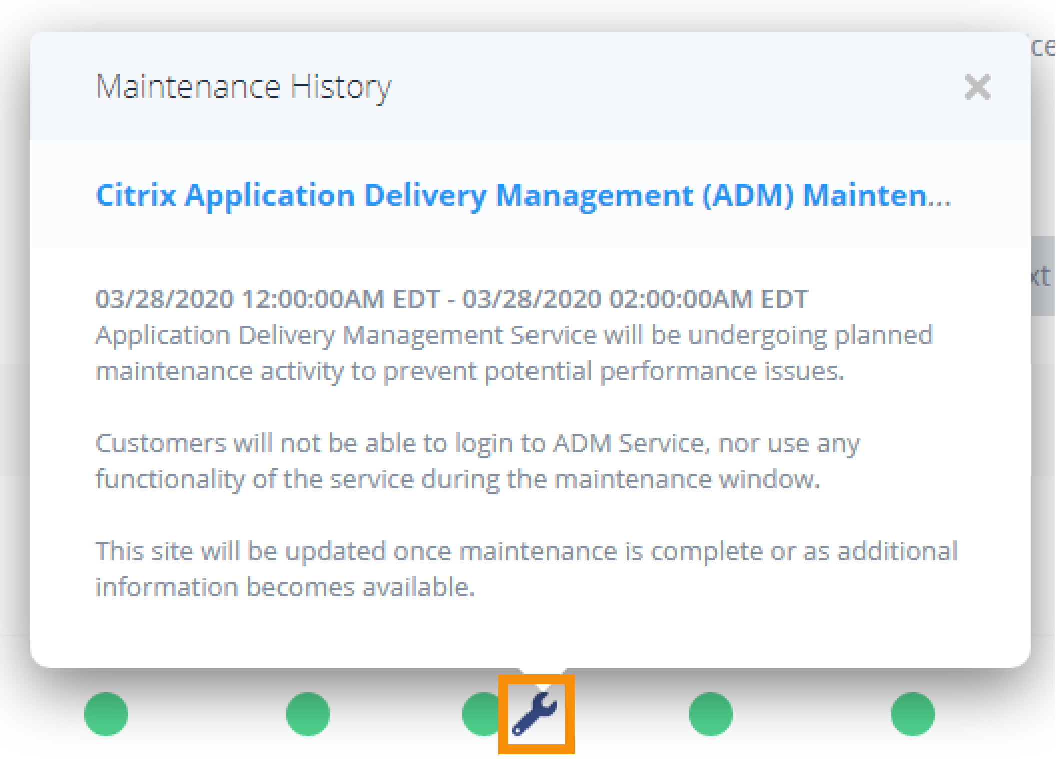
Service is operating normally ●
Performance issues ●
Service disruption ●

US

SERVICE NAME	TODAY	MAR 23RD	MAR 22ND	MAR 21ST	MAR 20TH	MAR 19TH	MAR 18TH
Access Control Service	●	●	●	●	●	●	●
Application Delivery Management	●	●	●	●	●	●	● 🔧
Citrix Analytics Service	●	●	●	●	●	●	●
Citrix Cloud	●	●	●	●	●	●	●

To view more detailed information about the service health incident for an affected service:

- From the list view, click the icon next to the service indicator to view more detailed information about the service health incident.



Maintenance History

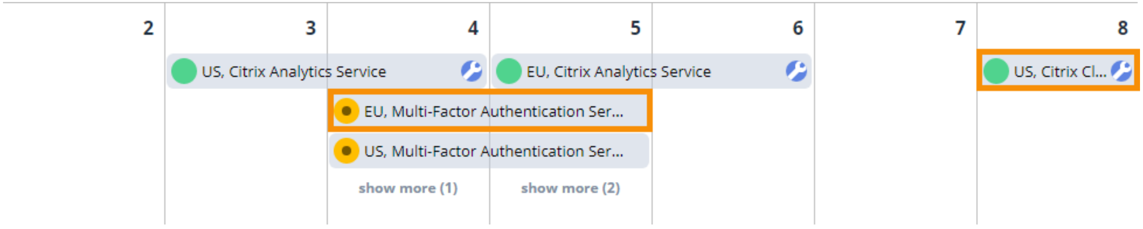
Citrix Application Delivery Management (ADM) Mainten...

03/28/2020 12:00:00AM EDT - 03/28/2020 02:00:00AM EDT
Application Delivery Management Service will be undergoing planned maintenance activity to prevent potential performance issues.

Customers will not be able to login to ADM Service, nor use any functionality of the service during the maintenance window.

This site will be updated once maintenance is complete or as additional information becomes available.

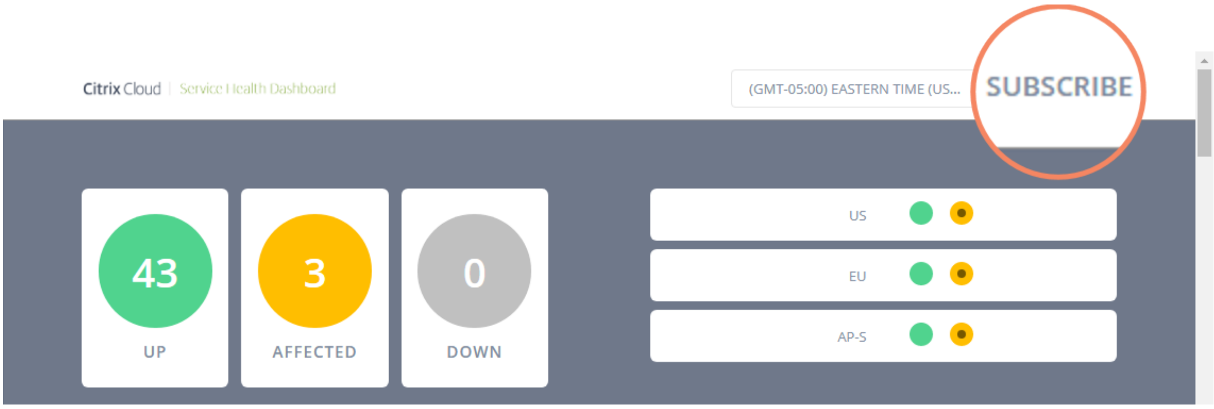
- From the calendar view, click the service entry to view the status for the service health incident.



2
3
4
5
6
7
8
US, Citrix Analytics Service
EU, Citrix Analytics Service
EU, Multi-Factor Authentication Ser...
US, Multi-Factor Authentication Ser...
show more (1)
show more (2)
US, Citrix Cl...

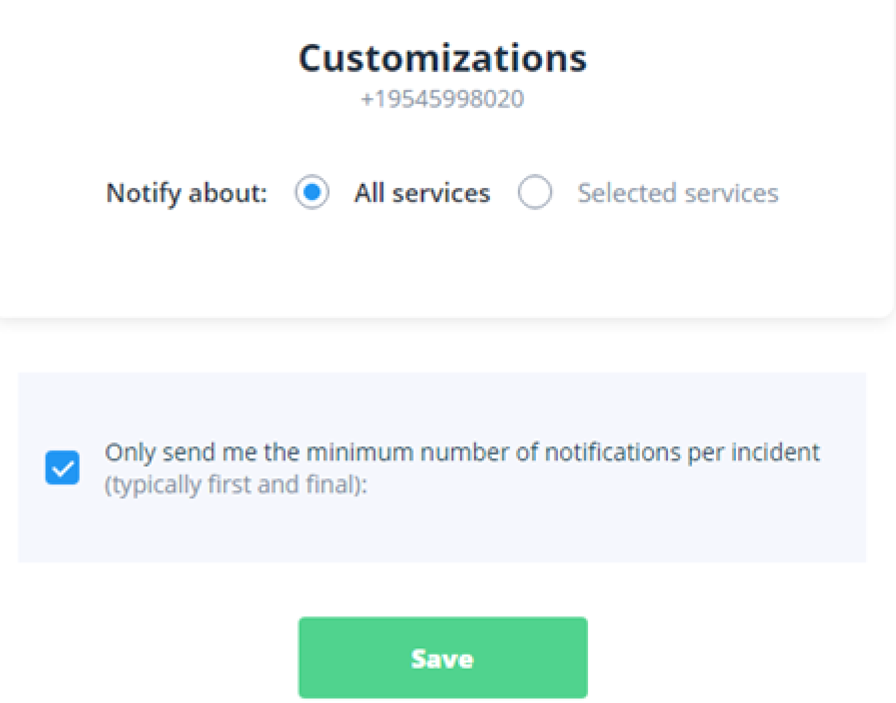
Service health subscriptions

To receive service health notifications, click **Subscribe** in the upper-right of the dashboard and select the notification method you want to use.



Citrix Cloud | Service Health Dashboard
(GMT-05:00) EASTERN TIME (US...
SUBSCRIBE
43
UP
3
AFFECTED
0
DOWN
US
EU
AP-S

You can subscribe to notifications for all services or only the services you select. By default, you receive all notifications for a service health incident. To limit the frequency of notifications during an incident, you can choose to receive only the first and final notifications.



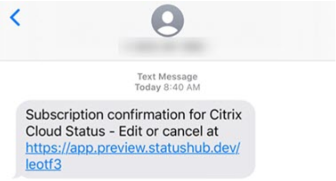
Customizations

+19545998020

Notify about: ● All services ○ Selected services

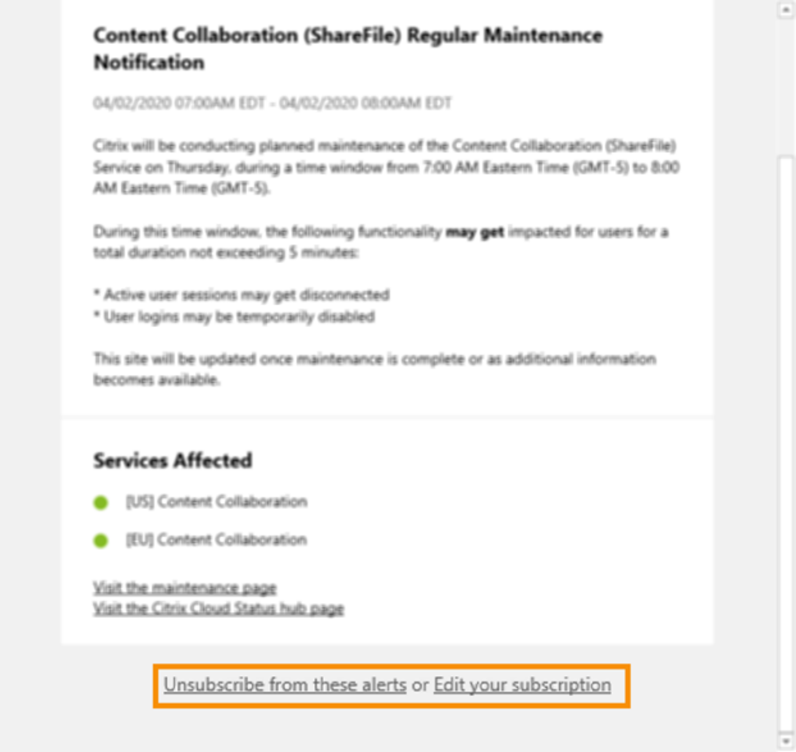
☑ Only send me the minimum number of notifications per incident (typically first and final):

Depending on the subscription method, links to unsubscribe and to change your preferences are included in the subscription confirmation message you receive (for example, when subscribing to phone notifications) or in each notification message (for example, when you subscribe to email notifications).



Text Message
Today 8:40 AM

Subscription confirmation for Citrix Cloud Status - Edit or cancel at https://app.preview.statushub.dev/leotf3



Content Collaboration (ShareFile) Regular Maintenance Notification

04/02/2020 07:00AM EDT - 04/02/2020 08:00AM EDT

Citrix will be conducting planned maintenance of the Content Collaboration (ShareFile) Service on Thursday, during a time window from 7:00 AM Eastern Time (GMT-5) to 8:00 AM Eastern Time (GMT-5).

During this time window, the following functionality **may get** impacted for users for a total duration not exceeding 5 minutes:

* Active user sessions may get disconnected
* User logins may be temporarily disabled

This site will be updated once maintenance is complete or as additional information becomes available.

Services Affected

● [US] Content Collaboration

● [EU] Content Collaboration

Visit the maintenance page
Visit the Citrix Cloud Status hub page

Unsubscribe from these alerts or Edit your subscription

To unsubscribe or change your subscription preferences:

1. Locate an existing notification and select the link to unsubscribe or change your notification preferences.
2. If unsubscribing, select **Unsubscribe** and then select the notification method you want to cancel. To subscribe from all notification methods, select **Remove all subscriptions**.
3. If changing preferences, select the notification method, make the appropriate changes to the services and minimum incident notifications, and then select **Save**.

Low-touch onboarding of Citrix ADC instances using service connect

October 20, 2021

As your hybrid multi-cloud (HMC) infrastructure grows, the challenges to manage, monitor, analyze, and troubleshoot ADC instances become multifold. A centralized controller providing visibility into your complete infrastructure and all the applications running on it becomes the need of the hour.

In today's world, onboarding your instances to a central controller needs to be done in a fast, easy, and low-touch manner. Keeping this need in mind, Citrix Application Delivery and Management launches a new onboarding workflow, which provides you a faster way to get complete visibility into your HMC deployment.

Overview: components of Citrix Application Delivery and Management onboarding workflow

The building blocks of this workflow are two ADC-side components: ADC service connect and Call Home.

- **Citrix Application Delivery and Management connect**: it is a new feature in ADC that helps enable seamless onboarding of Citrix ADC instances onto Citrix Application Delivery and Management. This feature lets the Citrix ADC instance automatically connect with Citrix Application Delivery and Management and send system, usage, and telemetry data to Citrix Application Delivery and Management. Based on this data, the Citrix Application Delivery and Management gives you insights and recommendations on your Citrix ADC infrastructure. Such as quick identification of performance issues, high resource usage, and critical errors.

  Citrix Application Delivery and Management connect is available on the following ADC versions:

  - Citrix ADC MPX and VPX image version 12.1 57.18 and later and 13.0 61.48 and later. For more information, see Introduction to Citrix Application Delivery and Management connect for Citrix ADC appliances.
  - Citrix ADC SDX version image 12.1 58.14 and later and 13.0 61.48 and later. For more information, see Introduction to Citrix Application Delivery and Management connect for Citrix ADC SDX appliances.

- **Call Home**: it is an existing feature in ADC, which periodically monitors the instances and automatically uploads data to the Citrix technical support server. For more details, see Call Home. The data collected by Call Home is also routed to Citrix Application Delivery and Management to enable this new workflow.

All ADC instances with internet connectivity or Call Home, or instances enabled with Citrix Application Delivery and Management connect are connected to Citrix Application Delivery and Management. Citrix Application Delivery and Management starts collecting relevant metrics from these ADC instances through Call Home route, Citrix Application Delivery and Management connect route, or both. For more information, see Data governance for MPX and VPX instances and Data governance for SDX instances.

Using this data, Citrix Application Delivery and Management creates an inventory of ADC instances for every customer (unique org ID), which shows you a consolidated list of your ADC instances. Citrix Application Delivery and Management also uses this data to create insights on your ADC and Gateway instances, which give meaningful insights into your HMC deployments, identifies issues, and recommends actions to mitigate the issues. Before you can mitigate the issues, you must onboard the ADC instances to Citrix Application Delivery and Management.
You can check **Select ADC and Gateway instances to onboard** and select the ADC instances you want to onboard to Citrix Application Delivery and Management. After you start, you are guided to the onboarding process.

The auto-onboarding process uses Citrix Application Delivery and Management connect, which makes the experience automated, seamless, and faster. For ADC instances on versions that do not support Citrix Application Delivery and Management connect and auto-onboarding, Citrix Application Delivery and Management provides use script-based onboarding, which is a semi-automated process.

> **Note**
>
> The auto and script-based onboarding use a built-in agent. However, this workflow also gives you the flexibility to use an external agent for onboarding. You can use the external agent-based onboarding if you want to use pooled licensing or the complete analytics suite in Citrix Application Delivery and Management. Or if you want both use pooled licensing and the complete analytics suite. The built-in agent supports only management and monitoring.

A quick tour of onboarding

Your first touchpoint in the onboarding journey is a product-initiated email. Here's a quick tour of the onboarding journey:

1. A **Citrix product-initiated email**: You receive an email from Citrix Application Delivery and Management showing some key insights of your ADC infrastructure and inviting you to get started with Citrix Application Delivery and Management. Click the link given in email.
2. **Citrix Cloud login page**: You must sign in to Citrix Cloud using your **My Citrix** credentials.
3. **Citrix Application Delivery and Management welcome page**: You get an overview of Citrix Application Delivery and Management and its benefits.
4. **Insights on your ADC and Gateway instances**: You get detailed insights into your overall ADC infrastructure including security advisory (advice on current Citrix CVEs), upgrade advisory (advice based on EOM/EOL timelines) , key metrics, trends, and highlights the issues affecting ADC performance and health and recommends way to mitigate the issues.
5. **Select ADC and Gateway instances to onboard**: You get a consolidated view of your ADC inventory. You can select which ADC instances you want to onboard to Citrix Application Delivery and Management.
6. **Onboard ADC instances to Citrix Application Delivery and Management**: Based on the ADC instances selected for onboarding, Citrix Application Delivery and Management guides you with the onboarding process. By default, built-in agent is selected for auto-onboarding.
7. **Citrix Application Delivery and Management GUI dashboard**: After onboarding completes, you are guided to the Citrix Application Delivery and Management instance dashboard.

> **Note**
>
> This workflow is rolled out (GA) in a phased manner, through canary release. You receive an email

> when this feature is available in your Citrix Application Delivery and Management environment.

For more details on each of these onboarding methods, see Onboard Citrix ADC instances using Citrix Application Delivery and Management connect.

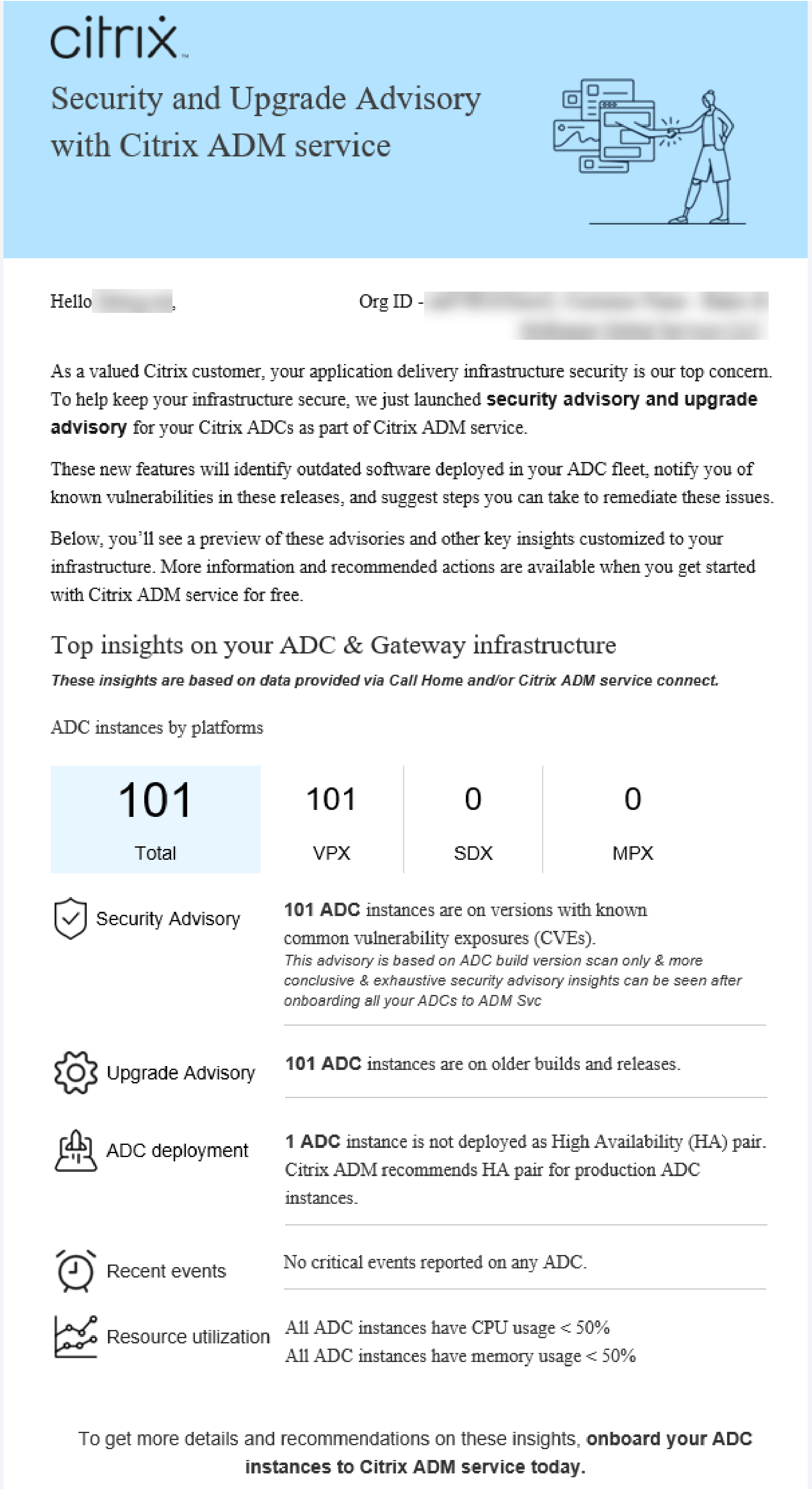
Onboard Citrix ADC instances using service connect

October 20, 2021

Following is a step-by-step guide to help you get started with Citrix Application Delivery and Management. Before you start, read how the Citrix Application Delivery and Management launches a new onboarding workflow, which provides you a faster way to get complete visibility into your hybrid multi-cloud (HMC) deployment. See Low-touch onboarding of Citrix ADC instances using Citrix Application Delivery and Management connect.

Step 1: Get started

You receive an email from Citrix Application Delivery and Management showing some key insights of your ADC infrastructure and inviting you to get started with Citrix Application Delivery and Management.



Security and Upgrade Advisory with Citrix ADM service

Hello [redacted],

Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs as part of Citrix ADM service.

These new features will identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you get started with Citrix ADM service for free.

Top insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM service connect.

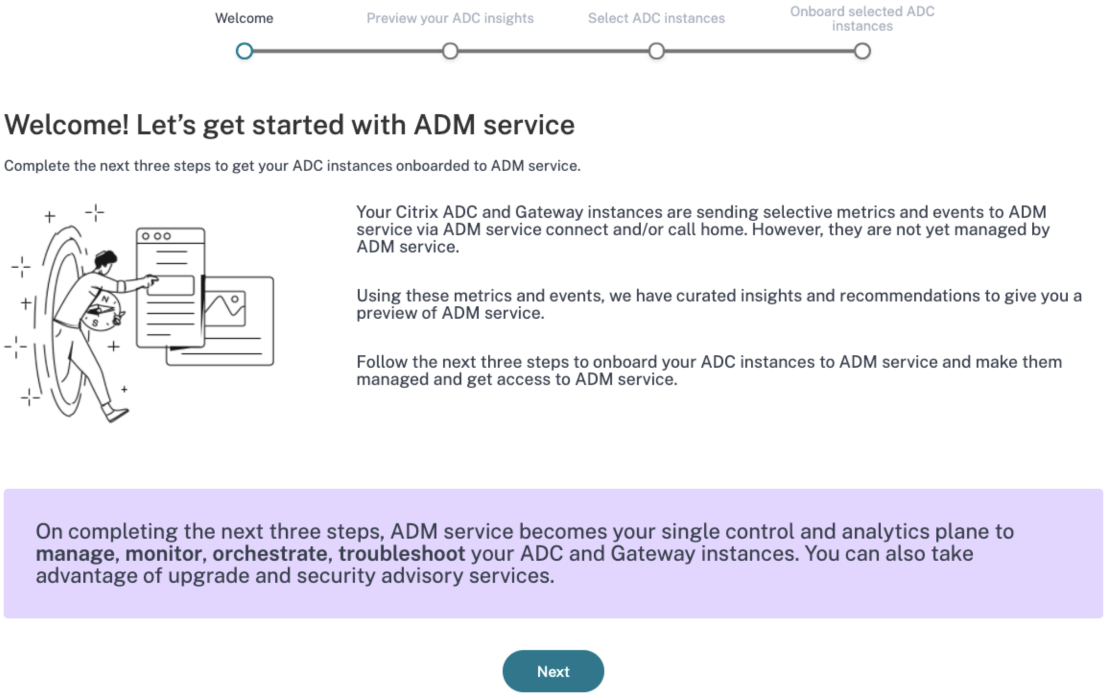
ADC instances by platforms

Total	VPX	SDX	MPX
101	101	0	0

Security Advisory	**101 ADC** instances are on versions with known common vulnerability exposures (CVEs). *This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc*
Upgrade Advisory	**101 ADC** instances are on older builds and releases.
ADC deployment	**1 ADC** instance is not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.
Recent events	No critical events reported on any ADC.
Resource utilization	All ADC instances have CPU usage < 50% All ADC instances have memory usage < 50%

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service today.**

1. In the email, click **Get Started** to initiate the onboarding process.
2. Sign in to Citrix Cloud using your My Citrix/Citrix Cloud credentials.
3. In the Citrix Application Delivery and Management landing page, take a moment to read why you are there and the benefits of using Citrix Application Delivery and Management.



Welcome! Let's get started with ADM service

Complete the next three steps to get your ADC instances onboarded to ADM service.

Your Citrix ADC and Gateway instances are sending selective metrics and events to ADM service via ADM service connect and/or call home. However, they are not yet managed by ADM service.

Using these metrics and events, we have curated insights and recommendations to give you a preview of ADM service.

Follow the next three steps to onboard your ADC instances to ADM service and make them managed and get access to ADM service.

On completing the next three steps, ADM service becomes your single control and analytics plane to **manage, monitor, orchestrate, troubleshoot** your ADC and Gateway instances. You can also take advantage of upgrade and security advisory services.

> **Note**
>
> The security advisory insights in the email are based on ADC build version scan only. You can see more conclusive and exhaustive security advisory insights after onboarding your ADC instances to Citrix Application Delivery and Management.

1. Click **Next**. The **Insights on your ADC and Gateway instances** page opens.

The next few steps act as a guided workflow to give you a preview into what Citrix Application Delivery and Management can offer and help you onboard your ADC instances onto Citrix Application Delivery and Management seamlessly.

Step 2: Insights on your ADC and Gateway instances

This insights page uses the data collected through Call Home or Citrix Application Delivery and Management connect or both Call Home and Citrix Application Delivery and Management connect to provide insights on your ADC instances. This page gives you insights into your overall ADC infrastructure including security advisory (advice on current Citrix CVEs), upgrade advisory (advice based on EOM/EOL timelines) , key metrics, trends, and highlights the issues affecting ADC performance and health and recommends way to mitigate the issues. These insights and recommendations are only a small preview of the plethora of benefits and value-add that Citrix Application Delivery and Management has to offer. To get many more benefits, detailed insights and to be able to run the recommended actions, you need to onboard the ADC instances onto Citrix Application Delivery and Management.

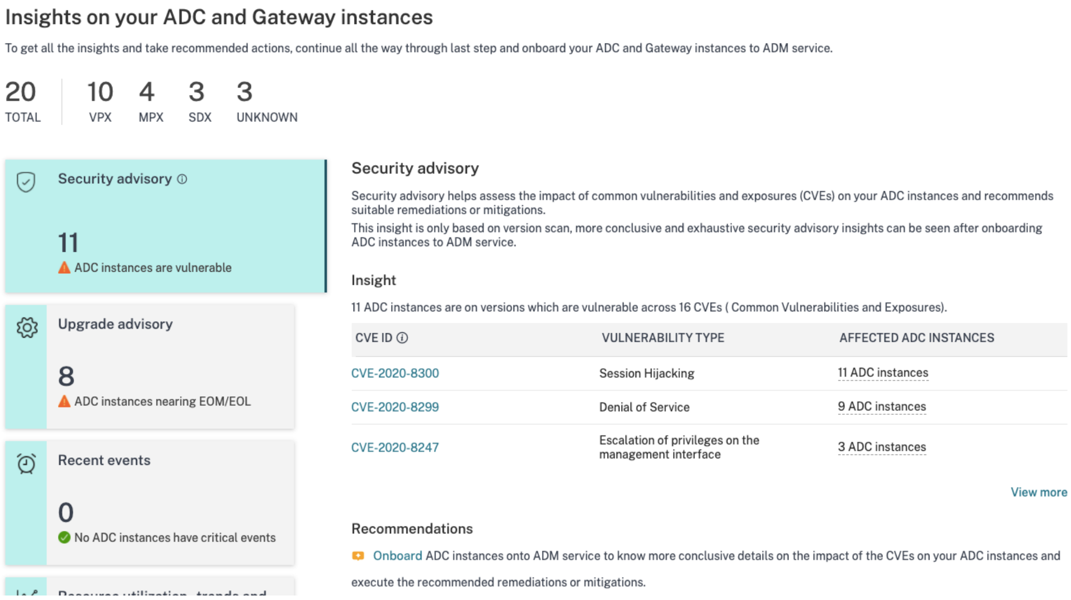
The insights and recommendations are categorized into the following types:

- **Security advisory**: onboard ADC instances to get the CVE impact details on your ADC instances and run the recommended remediations or mitigations.
- **Upgrade advisory**: onboard ADC instances onto Citrix Application Delivery and Management and upgrade your ADC instances that have reached or are reaching EOM/EOL or are on older releases/builds.
- **Recent events**: onboard ADC instances to Citrix Application Delivery and Management to monitor 200+ events on a regular basis, and create rules to get notified over email, PagerDuty, Slack, ServiceNow, take appropriate action.
- **Resource utilization - trends and anomalies**: onboard ADC instances to Citrix Application Delivery and Management to get a comprehensive view of ADC instance health, performance issues, and recommendations to mitigate those issues. You can also assess predicted CPU and memory usage for your ADC instances.
- **ADC deployment guidance**: onboard ADC instances to Citrix Application Delivery and Management and configure them as HA pair, using configuration jobs on Citrix Application Delivery and Management.

1. **Security advisory**: Citrix Application Delivery and Management Security Advisory alerts you about vulnerabilities putting your ADC instances at risk and recommends mitigations and remediations.

   > **Note**
   >
   > Security advisory insights in the onboarding email and guided workflow are based on ADC build version scan only. You can see conclusive and exhaustive security advisory insights after onboarding your ADC instances to Citrix Application Delivery and Management **Example**: If a CVE needs both version scan and config scan for vulnerability assessment, the onboarding email and guided workflow shows the results based on version scan. So, there might be false positives. To know a more conclusive and accurate assessment of the impact, onboard ADC to Citrix Application Delivery and Management. After onboarding, Citrix Application Delivery and Management security advisory shows the impact assessment, which vulnerable ADC assessment, based on versions scan and config scan.

   You can check the CVE ID, vulnerability type, and affected ADC instances. The CVE ID link takes to the security bulletin article.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20 TOTAL | 10 VPX | 4 MPX | 3 SDX | 3 UNKNOWN

Security advisory ⓘ

11

⚠ ADC instances are vulnerable

Upgrade advisory

8

⚠ ADC instances nearing EOM/EOL

Recent events

0

✓ No ADC instances have critical events

Resource utilization - trends and

Security advisory

Security advisory helps assess the impact of common vulnerabilities and exposures (CVEs) on your ADC instances and recommends suitable remediations or mitigations.

This insight is only based on version scan, more conclusive and exhaustive security advisory insights can be seen after onboarding ADC instances to ADM service.

Insight

11 ADC instances are on versions which are vulnerable across 16 CVEs (Common Vulnerabilities and Exposures).

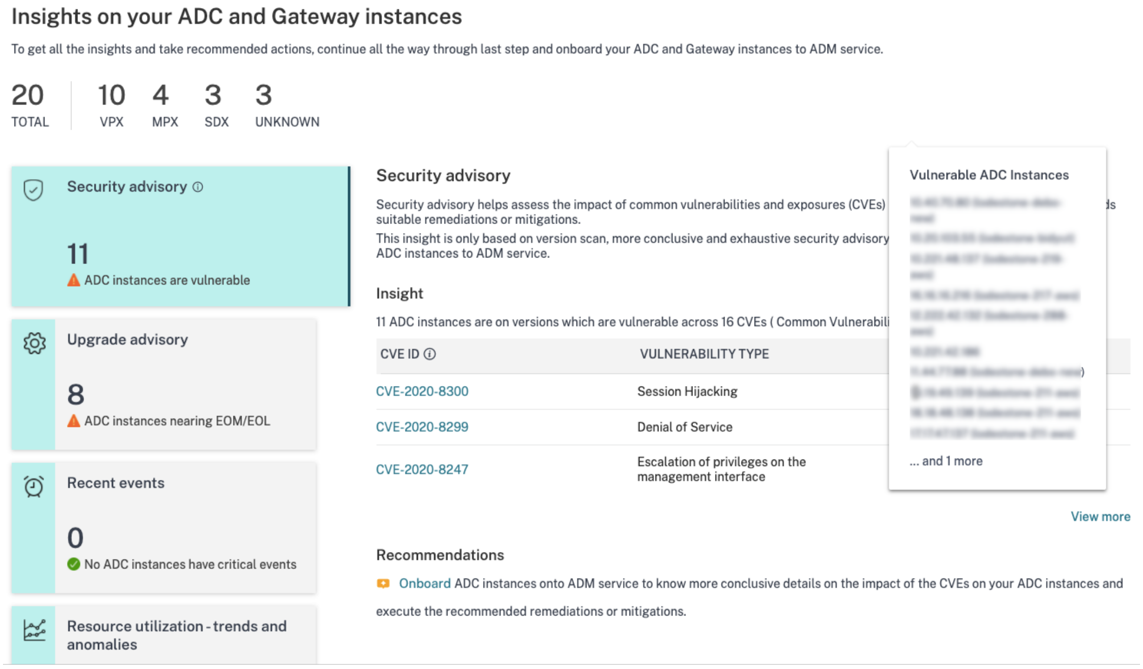
CVE ID ⓘ	VULNERABILITY TYPE	AFFECTED ADC INSTANCES
CVE-2020-8300	Session Hijacking	11 ADC instances
CVE-2020-8299	Denial of Service	9 ADC instances
CVE-2020-8247	Escalation of privileges on the management interface	3 ADC instances

View more

Recommendations

Onboard ADC instances onto ADM service to know more conclusive details on the impact of the CVEs on your ADC instances and execute the recommended remediations or mitigations.

The recommendation guides you to onboard your ADC instances to Citrix Application Delivery and Management to get more details of the CVE impact on your ADC instances and run the recommended mitigation or remediation. Click the affected ADC instances to see the IP addresses of the impacted instances.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20 TOTAL | 10 VPX | 4 MPX | 3 SDX | 3 UNKNOWN

Security advisory ⓘ

11

⚠ ADC instances are vulnerable

Upgrade advisory

8

⚠ ADC instances nearing EOM/EOL

Recent events

0

✓ No ADC instances have critical events

Resource utilization - trends and anomalies

Security advisory

Security advisory helps assess the impact of common vulnerabilities and exposures (CVEs)
suitable remediations or mitigations.

This insight is only based on version scan, more conclusive and exhaustive security advisory
ADC instances to ADM service.

Insight

11 ADC instances are on versions which are vulnerable across 16 CVEs (Common Vulnerabili

CVE ID ⓘ	VULNERABILITY TYPE
CVE-2020-8300	Session Hijacking
CVE-2020-8299	Denial of Service
CVE-2020-8247	Escalation of privileges on the management interface

Vulnerable ADC Instances

[redacted]

... and 1 more

View more

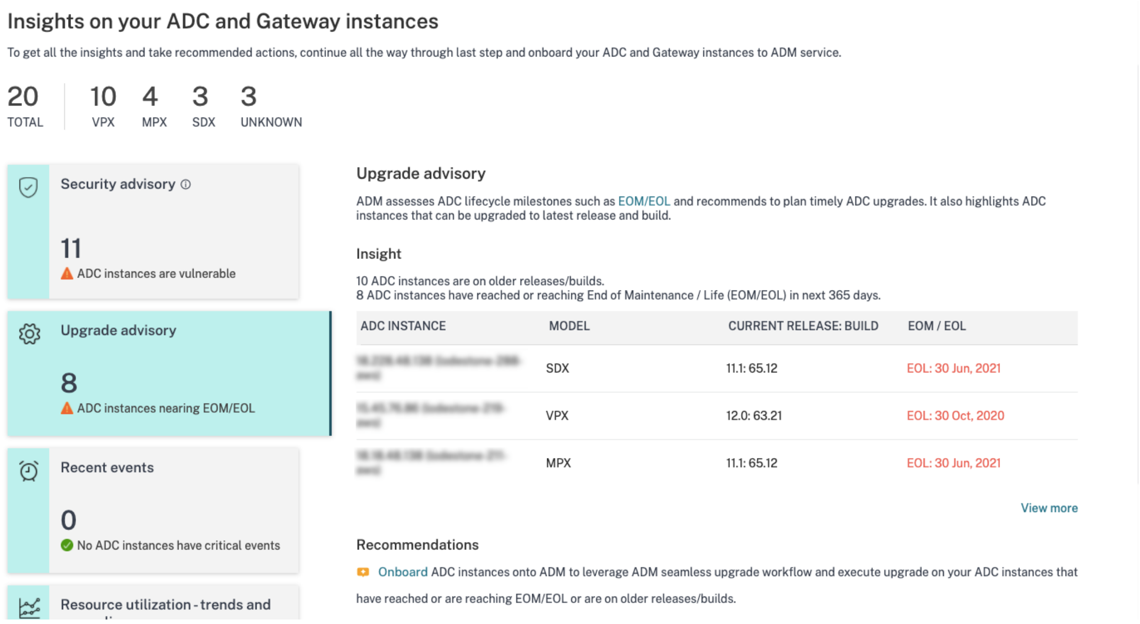
Recommendations

Onboard ADC instances onto ADM service to know more conclusive details on the impact of the CVEs on your ADC instances and execute the recommended remediations or mitigations.

2. **Upgrade advisory**: Use this advisory to check which ADC instances are nearing EOM/EOL or are on older builds.

   Based on these insights, Citrix Application Delivery and Management recommends you to plan a timely upgrade before EOM/EOL or to benefit from the latest features and fixes.

To perform the upgrade, you need to onboard your ADC instances on to Citrix Application Delivery and Management.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20 TOTAL | 10 VPX | 4 MPX | 3 SDX | 3 UNKNOWN

Security advisory ⓘ

11

⚠ ADC instances are vulnerable

Upgrade advisory

8

⚠ ADC instances nearing EOM/EOL

Recent events

0

✓ No ADC instances have critical events

Resource utilization - trends and

Upgrade advisory

ADM assesses ADC lifecycle milestones such as EOM/EOL and recommends to plan timely ADC upgrades. It also highlights ADC instances that can be upgraded to latest release and build.

Insight

10 ADC instances are on older releases/builds.
8 ADC instances have reached or reaching End of Maintenance / Life (EOM/EOL) in next 365 days.

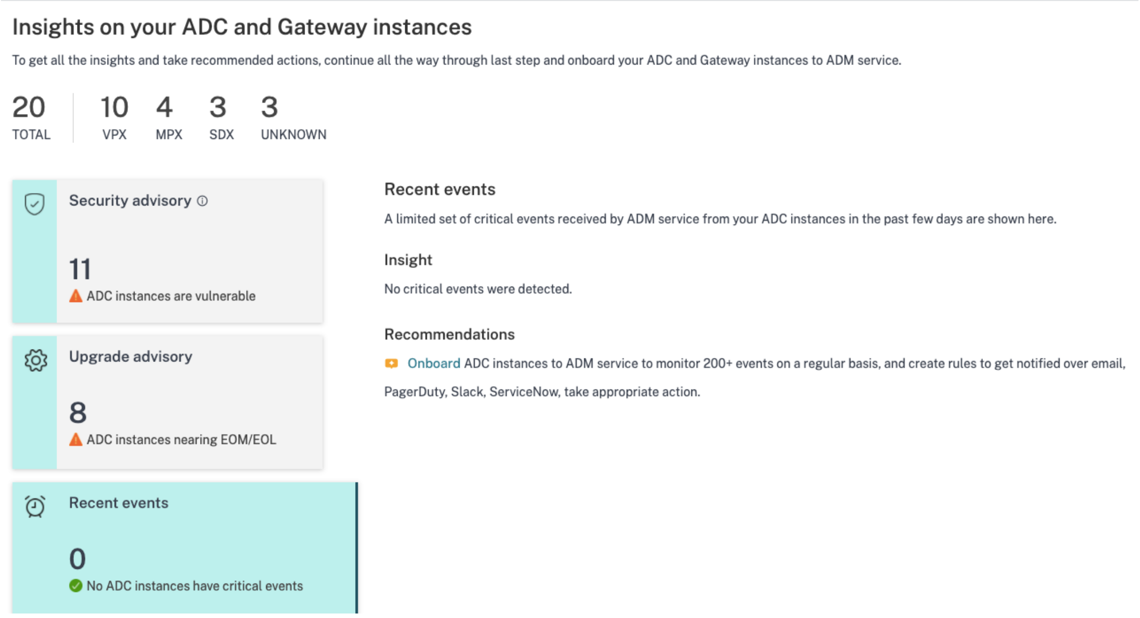
ADC INSTANCE	MODEL	CURRENT RELEASE: BUILD	EOM / EOL
[redacted]	SDX	11.1: 65.12	EOL: 30 Jun, 2021
[redacted]	VPX	12.0: 63.21	EOL: 30 Oct, 2020
[redacted]	MPX	11.1: 65.12	EOL: 30 Jun, 2021

View more

Recommendations

Onboard ADC instances onto ADM to leverage ADM seamless upgrade workflow and execute upgrade on your ADC instances that have reached or are reaching EOM/EOL or are on older releases/builds.

3. **Recent events**: Get details of some critical errors that have happened on the ADC instances and a list of ADC instances on which the errors have occurred.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20 TOTAL | 10 VPX | 4 MPX | 3 SDX | 3 UNKNOWN

Security advisory ⓘ

11

⚠ ADC instances are vulnerable

Upgrade advisory

8

⚠ ADC instances nearing EOM/EOL

Recent events

0

✓ No ADC instances have critical events

Recent events

A limited set of critical events received by ADM service from your ADC instances in the past few days are shown here.

Insight

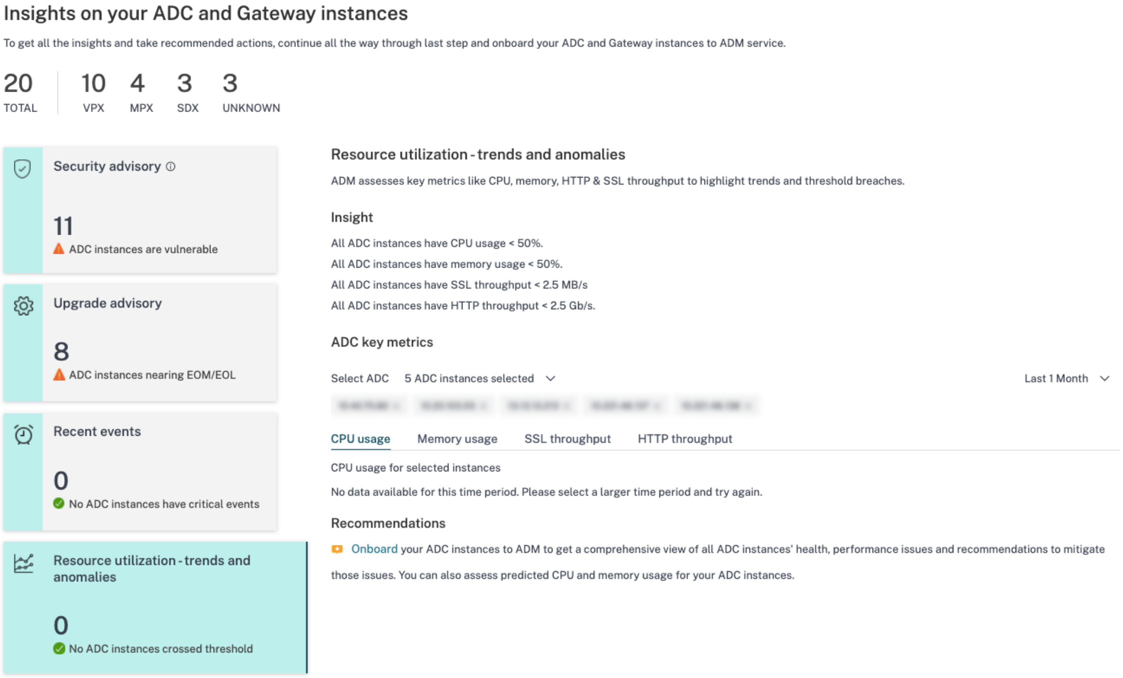
No critical events were detected.

Recommendations

Onboard ADC instances to ADM service to monitor 200+ events on a regular basis, and create rules to get notified over email, PagerDuty, Slack, ServiceNow, take appropriate action.

4. **Resource utilization - trends and anomalies**: Find insights about high resource utilization for CPU, memory, HTTP throughput, and SSL throughput. For each insight, Citrix Application Delivery and Management suggests recommended action. To have more visibility into these insights and recommendations, you need to onboard your ADC instances onto Citrix Application Delivery and Management. Some benefits after onboarding are:

- CPU: Predict CPU utilization for the next 24 hours on Citrix Application Delivery and Management.
- Memory: Predict memory utilization for the next 24 hours on Citrix Application Delivery and Management.
- SSL throughput: View SSL real time optimization with intelligent App Analytics on Citrix Application Delivery and Management.
- HTTP Throughput: Troubleshoot ADC throughput capacity issues with Infrastructure Analytics.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20	10	4	3	3
TOTAL	VPX	MPX	SDX	UNKNOWN

Security advisory ⓘ

11

ADC instances are vulnerable

Upgrade advisory

8

ADC instances nearing EOM/EOL

Recent events

0

No ADC instances have critical events

Resource utilization - trends and anomalies

0

No ADC instances crossed threshold

Resource utilization - trends and anomalies

ADM assesses key metrics like CPU, memory, HTTP & SSL throughput to highlight trends and threshold breaches.

Insight

All ADC instances have CPU usage < 50%.

All ADC instances have memory usage < 50%.

All ADC instances have SSL throughput < 2.5 MB/s

All ADC instances have HTTP throughput < 2.5 Gb/s.

ADC key metrics

Select ADC: 5 ADC instances selected

Last 1 Month

[redacted]

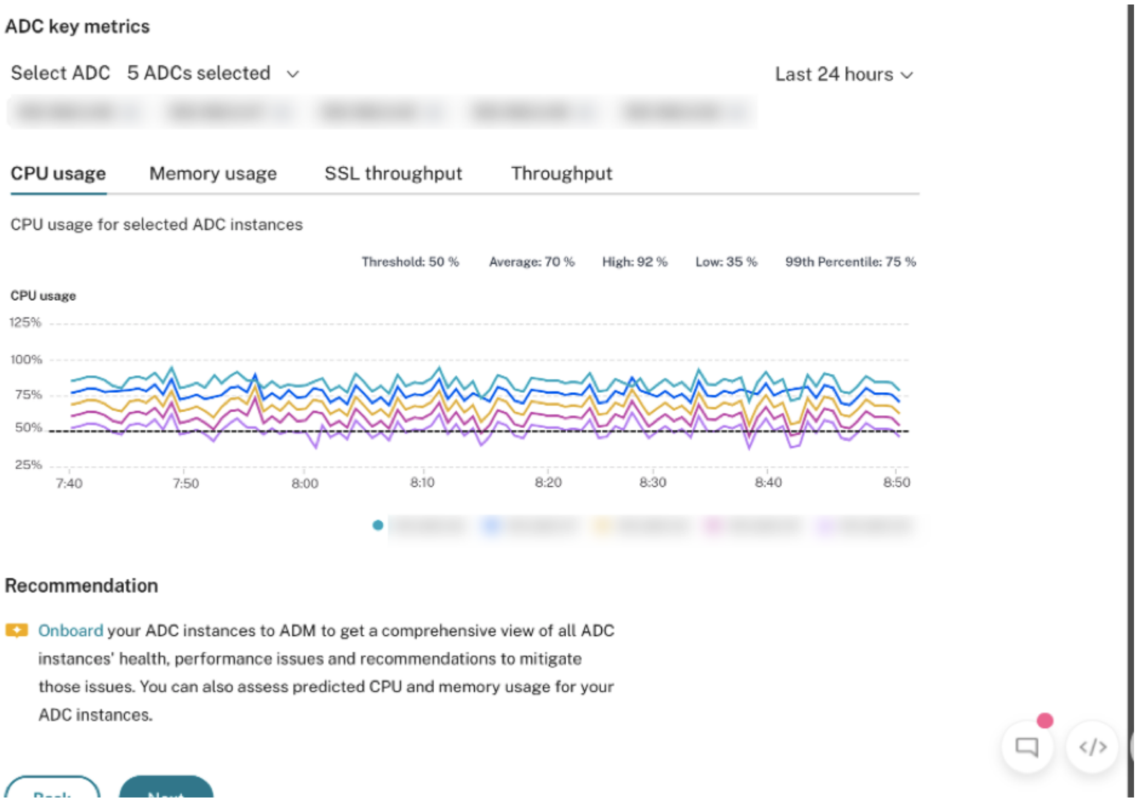
CPU usage for selected instances

No data available for this time period. Please select a larger time period and try again.

Recommendations

Onboard your ADC instances to ADM to get a comprehensive view of all ADC instances' health, performance issues and recommendations to mitigate those issues. You can also assess predicted CPU and memory usage for your ADC instances.

- **Key Metrics**: Get details of key metrics related to CPU, memory, HTTP throughput, SSL throughput, and uncover anomalous trends in metrics.



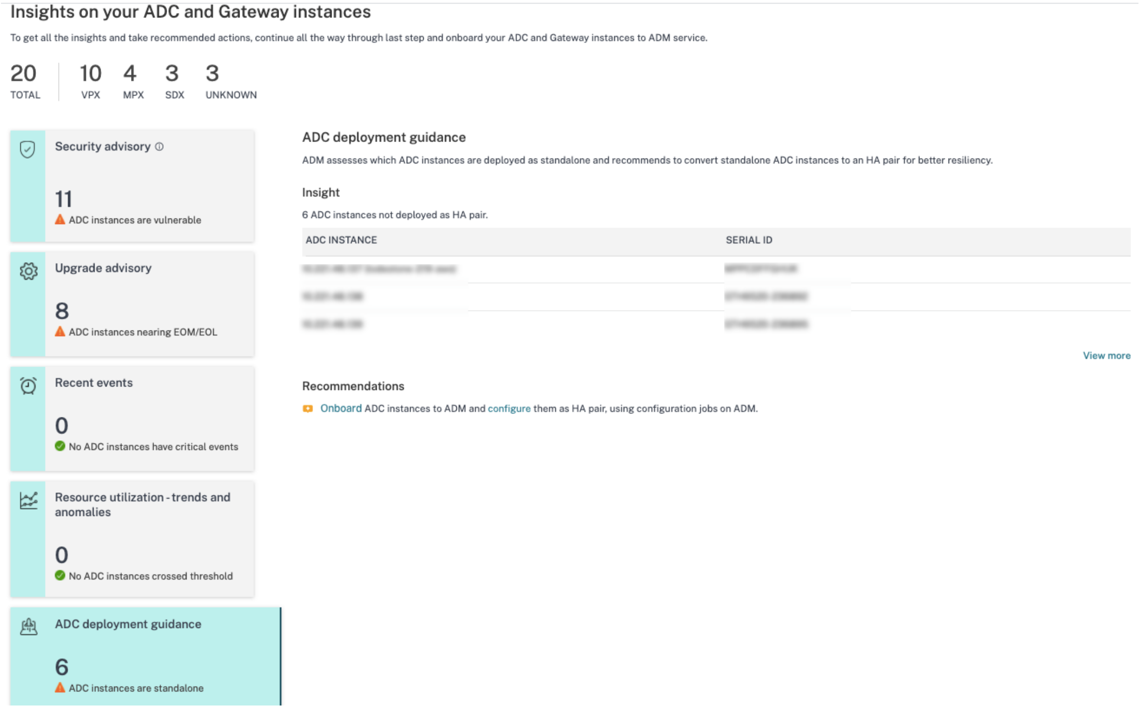
ADC key metrics

CPU usage for selected ADC instances

Recommendation

Onboard your ADC instances to ADM to get a comprehensive view of all ADC instances' health, performance issues and recommendations to mitigate those issues. You can also assess predicted CPU and memory usage for your ADC instances.

5. **Deployment guidance**: Have visibility into ADC instances that are deployed as a standalone ADC. Citrix Application Delivery and Management gives recommendation to configure these ADC instances as an HA pair for better resiliency. This requires you to onboard your ADC instances to Citrix Application Delivery and Management and then use maintenance jobs to configure the instances as an HA pair.



Insights on your ADC and Gateway instances

To get all the insights and take recommended actions, continue all the way through last step and onboard your ADC and Gateway instances to ADM service.

20	10	4	3	3
TOTAL	VPX	MPX	SDX	UNKNOWN

Security advisory ⓘ
11
ADC instances are vulnerable

Upgrade advisory
8
ADC instances nearing EOM/EOL

Recent events
0
No ADC instances have critical events

Resource utilization - trends and anomalies
0
No ADC instances crossed threshold

ADC deployment guidance
6
ADC instances are standalone

ADC deployment guidance

ADM assesses which ADC instances are deployed as standalone and recommends to convert standalone ADC instances to an HA pair for better resiliency.

Insight

6 ADC instances not deployed as HA pair.

ADC INSTANCE	SERIAL ID
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

View more

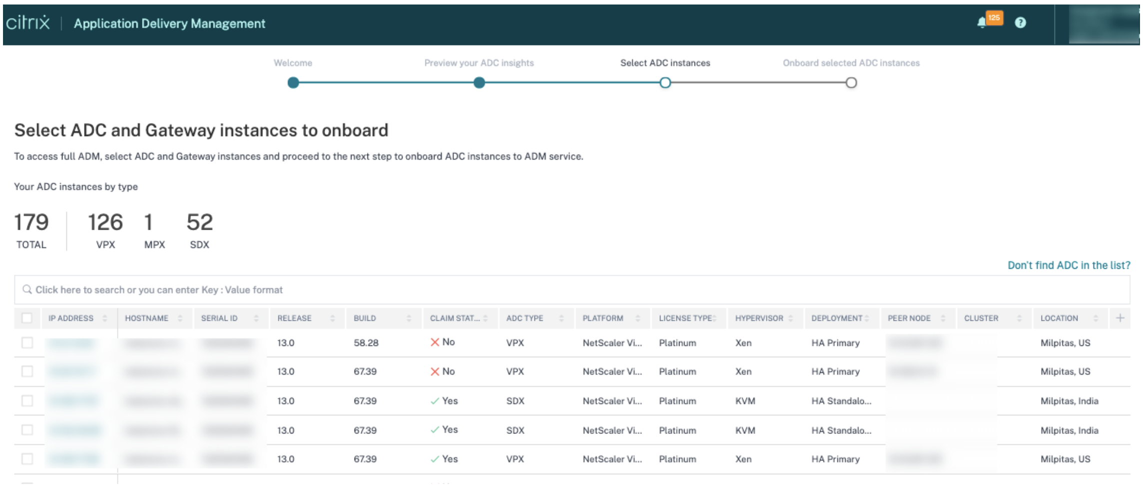
Recommendations

Onboard ADC instances to ADM and configure them as HA pair, using configuration jobs on ADM.

Step 3: Select ADC and Gateway instances to onboard

This page displays all the ADC and Gateway instances in your environment. View and select the ADC and Gateway instances you want to onboard to Citrix Application Delivery and Management and click **Next**.

1. View and select the ADC instances you want to onboard to Citrix Application Delivery and Management.



citrix
Application Delivery Management
Welcome
Preview your ADC insights
Select ADC instances
Onboard selected ADC instances

Select ADC and Gateway instances to onboard

To access full ADM, select ADC and Gateway instances and proceed to the next step to onboard ADC instances to ADM service.

Your ADC instances by type

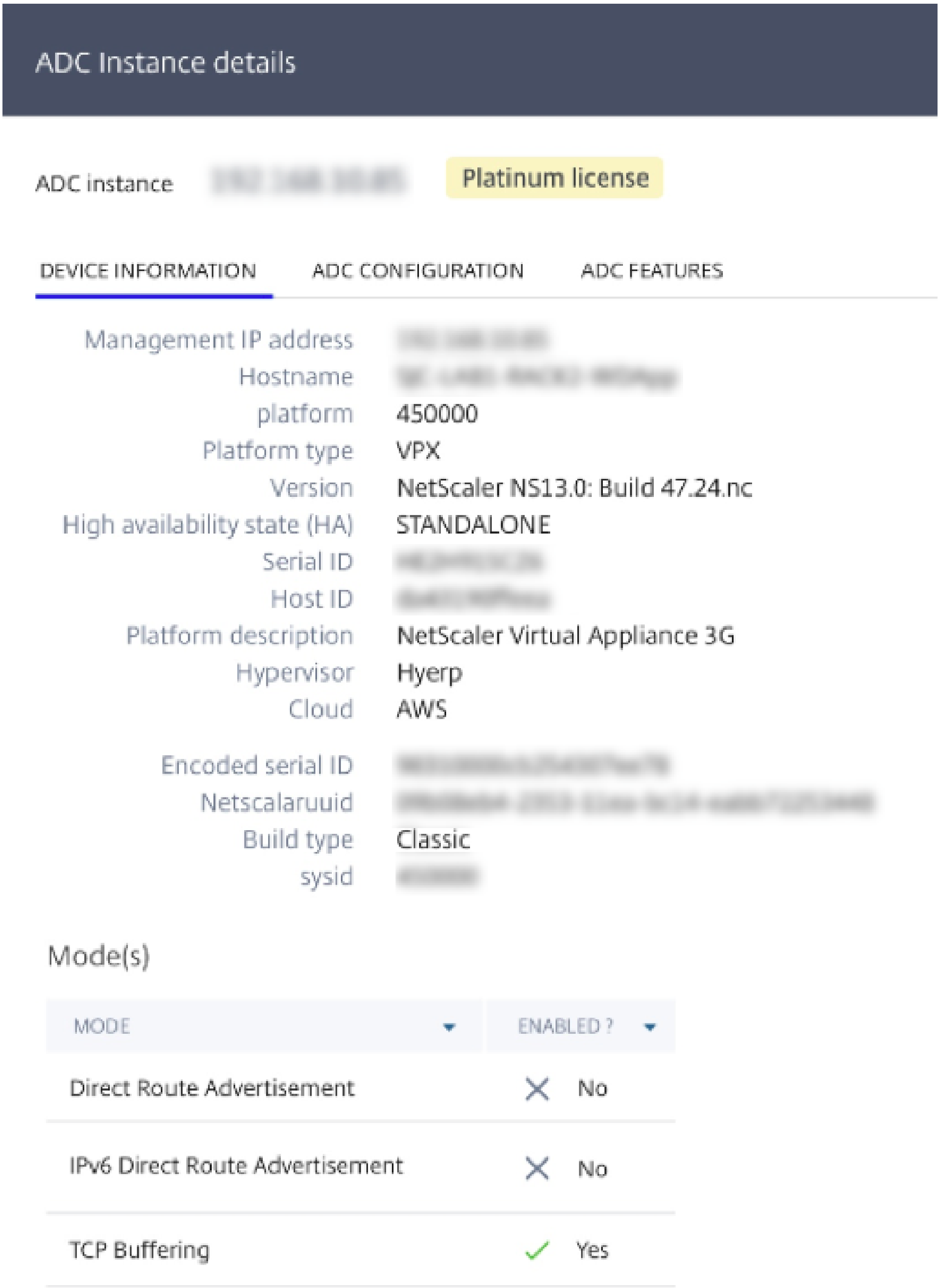
179	126	1	52
TOTAL	VPX	MPX	SDX

Don't find ADC in the list?

Click here to search or you can enter Key : Value format

□	IP ADDRESS	HOSTNAME	SERIAL ID	RELEASE	BUILD	CLAIM STAT...	ADC TYPE	PLATFORM	LICENSE TYPE	HYPERVISOR	DEPLOYMENT	PEER NODE	CLUSTER	LOCATION
□	[redacted]	[redacted]	[redacted]	13.0	58.28	✗ No	VPX	NetScaler Vi...	Platinum	Xen	HA Primary	[redacted]		Milpitas, US
□	[redacted]	[redacted]	[redacted]	13.0	67.39	✗ No	VPX	NetScaler Vi...	Platinum	Xen	HA Primary	[redacted]		Milpitas, US
□	[redacted]	[redacted]	[redacted]	13.0	67.39	✓ Yes	SDX	NetScaler Vi...	Platinum	KVM	HA Standalo...			Milpitas, India
□	[redacted]	[redacted]	[redacted]	13.0	67.39	✓ Yes	SDX	NetScaler Vi...	Platinum	KVM	HA Standalo...			Milpitas, India
□	[redacted]	[redacted]	[redacted]	13.0	67.39	✓ Yes	VPX	NetScaler Vi...	Platinum	Xen	HA Primary	[redacted]		Milpitas, US

If you need details about any instance such as device information, ADC configuration, ADC features available, or license information, click the instance IP address under the ADC instance.



ADC Instance details

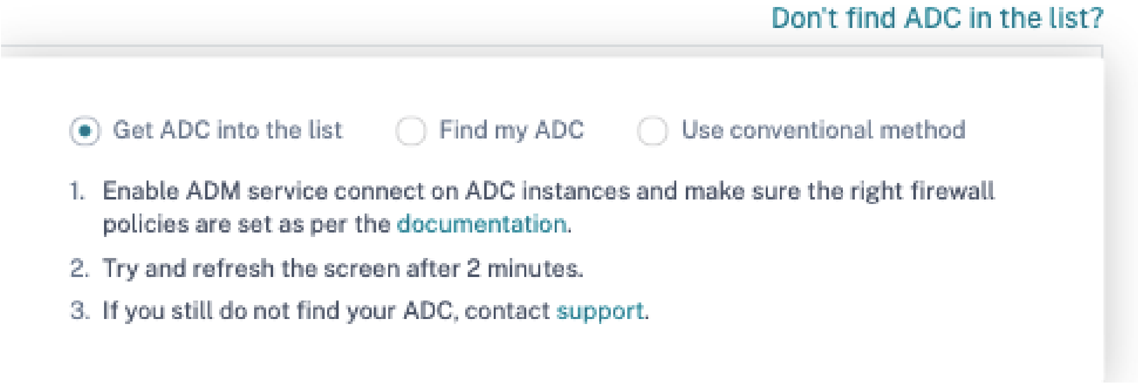
ADC instance [redacted] Platinum license

Management IP address	[redacted]
Hostname	[redacted]
platform	450000
Platform type	VPX
Version	NetScaler NS13.0: Build 47.24.nc
High availability state (HA)	STANDALONE
Serial ID	[redacted]
Host ID	[redacted]
Platform description	NetScaler Virtual Appliance 3G
Hypervisor	Hyerp
Cloud	AWS
Encoded serial ID	[redacted]
Netscalaruuid	[redacted]
Build type	Classic
sysid	[redacted]

Mode(s)

MODE	ENABLED ?
Direct Route Advertisement	✕ No
IPv6 Direct Route Advertisement	✕ No
TCP Buffering	✓ Yes

If your instance is not listed, use the **Don’t find ADC in the list** on the upper-right corner.



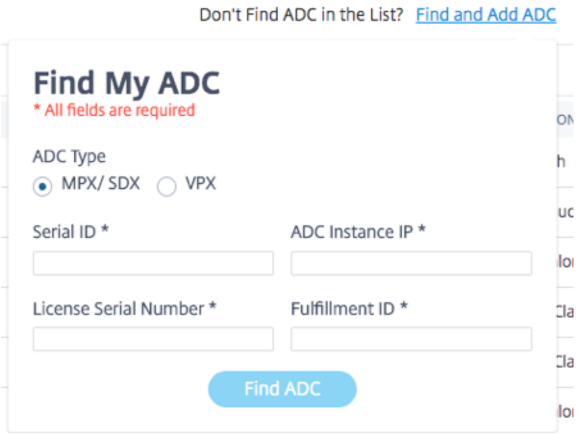
Don't find ADC in the list?

○ Get ADC into the list ● ○ Find my ADC ○ Use conventional method

1. Enable ADM service connect on ADC instances and make sure the right firewall policies are set as per the documentation.
2. Try and refresh the screen after 2 minutes.
3. If you still do not find your ADC, contact support.

You can proceed in three ways:follow the steps given under **Get ADC into the list** or use the **Find my ADC option**. If these two steps do not help, click **Use conventional method** option, which skips the workflow and takes you through the traditional way of onboarding ADC instances.

For the **Find my ADC option**, enter the details in the mandatory fields (serial ID, ADC instance IP address, license serial number, and fulfillment ID) and search.



Don't Find ADC in the List? Find and Add ADC

Find My ADC

* All fields are required

ADC Type

● MPX/ SDX ○ VPX

Serial ID *

ADC Instance IP *

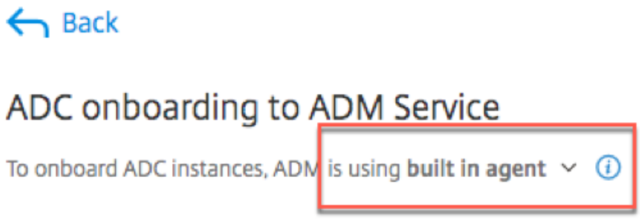
License Serial Number *

Fulfillment ID *

Find ADC

Step 4: Onboard ADC instances to Citrix Application Delivery and Management

You can onboard your instances using the built-agent (default option) or an external agent.



Back

ADC onboarding to ADM Service

To onboard ADC instances, ADM is using **built in agent**

Onboard ADC instances using a built-in agent

Auto- and script-based onboarding use the built-in agent, which is set by default.

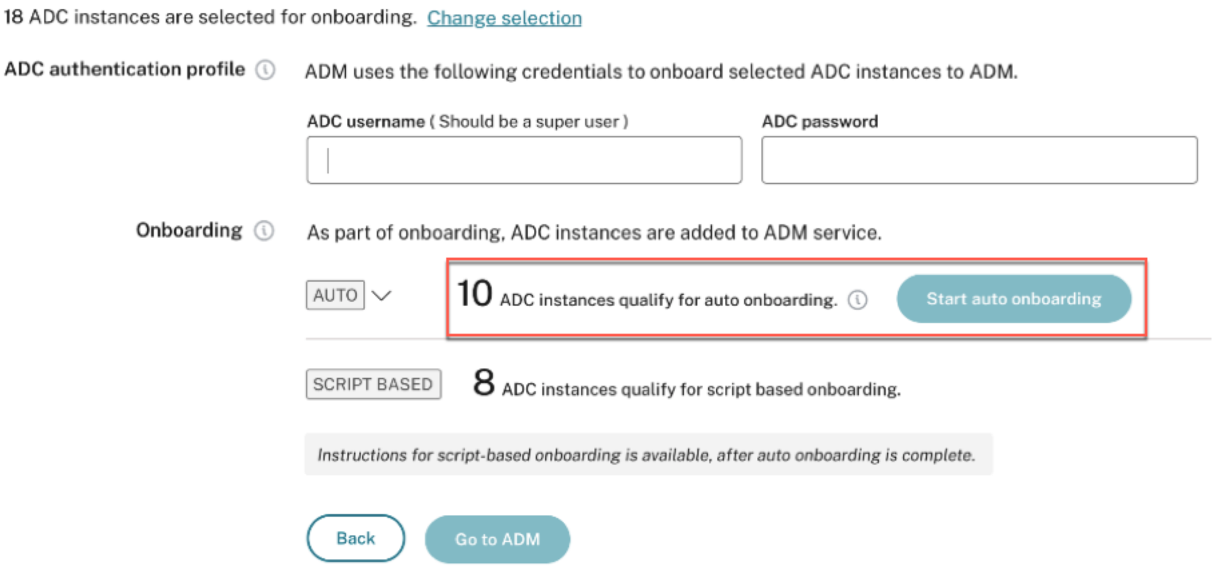
Auto-onboarding: it is supported only on the following ADC versions:

- Citrix ADC MPX and VPX image version 12.1 57.18 and later and 13.0 61.48 and later
- SDX version image 13.0 61.48 and later and 12.1 58.14 and later

To select a different ADC instance, click **Change selection**.

Out of the total selected ADC instances, some instances might qualify for auto-onboarding (based on minimum version criteria). You can see the instances that qualify for auto-onboarding.

Enter the ADC user name and password. These credentials must be ADC user admin credentials, and Citrix Application Delivery and Management uses these credentials to onboard ADC. Click **Start onboarding** to onboard your ADC instances on Citrix Application Delivery and Management.



18 ADC instances are selected for onboarding. Change selection

ADC authentication profile ⓘ ADM uses the following credentials to onboard selected ADC instances to ADM.

ADC username (Should be a super user)

ADC password

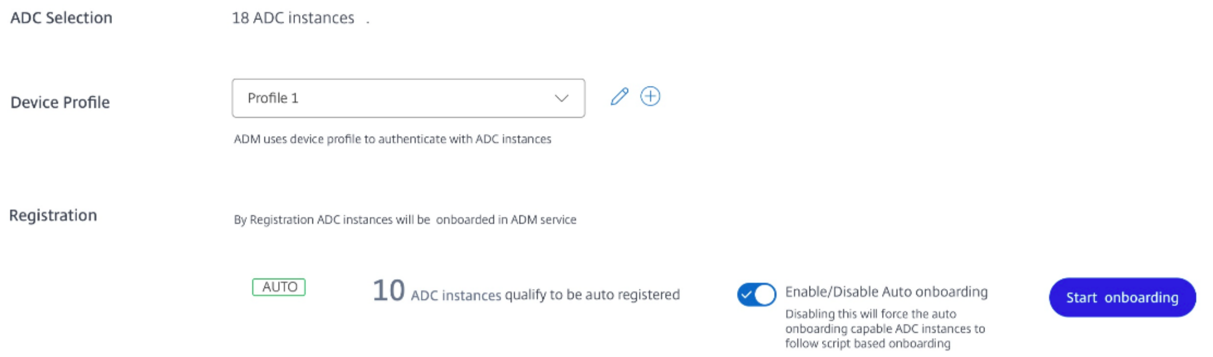
Onboarding ⓘ As part of onboarding, ADC instances are added to ADM service.

AUTO 10 ADC instances qualify for auto onboarding. ⓘ Start auto onboarding

SCRIPT BASED 8 ADC instances qualify for script based onboarding.

Instructions for script-based onboarding is available, after auto onboarding is complete.

Back Go to ADM



ADC Selection 18 ADC instances .

Device Profile Profile 1

ADM uses device profile to authenticate with ADC instances

Registration By Registration ADC instances will be onboarded in ADM service

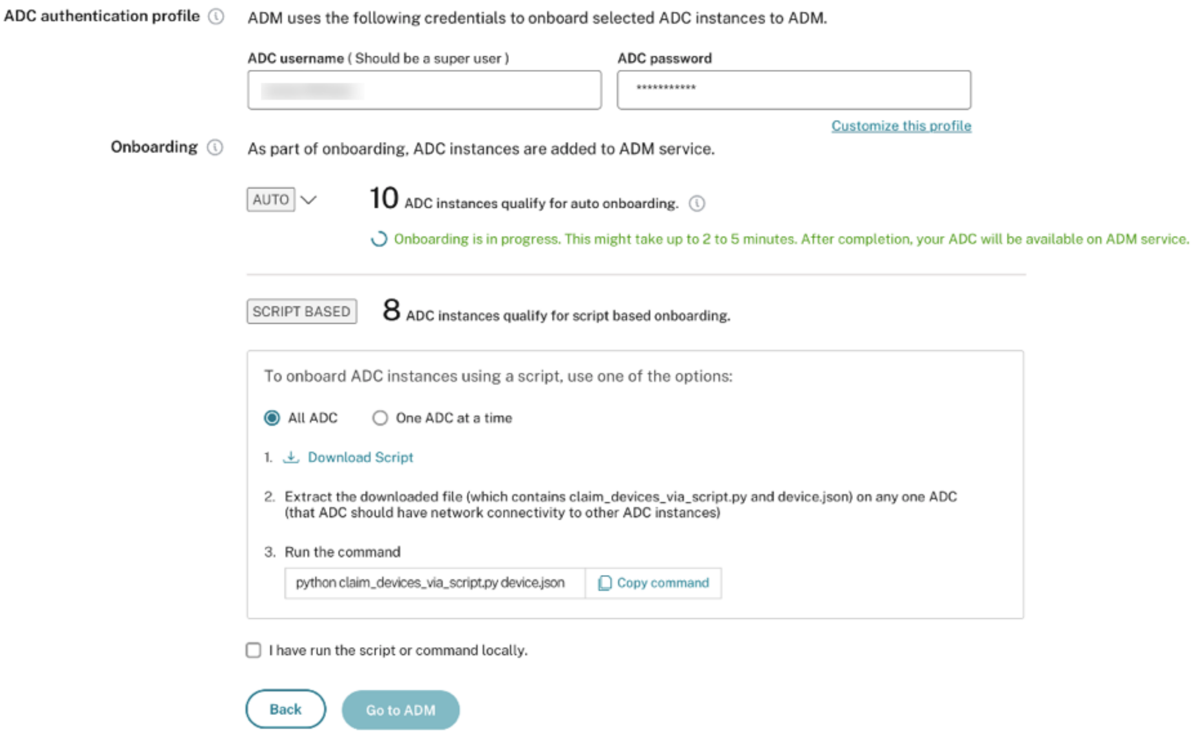
AUTO 10 ADC instances qualify to be auto registered

Enable/Disable Auto onboarding

Disabling this will force the auto onboarding capable ADC instances to follow script based onboarding

Start onboarding

Auto-onboarding might take up to 2-5 minutes to complete.



ADC authentication profile ⓘ ADM uses the following credentials to onboard selected ADC instances to ADM.

ADC username (Should be a super user): [redacted]

ADC password: ***********

Customize this profile

Onboarding ⓘ As part of onboarding, ADC instances are added to ADM service.

AUTO 10 ADC instances qualify for auto onboarding. ⓘ

Onboarding is in progress. This might take up to 2 to 5 minutes. After completion, your ADC will be available on ADM service.

SCRIPT BASED 8 ADC instances qualify for script based onboarding.

To onboard ADC instances using a script, use one of the options:

● All ADC ○ One ADC at a time

1. Download Script
2. Extract the downloaded file (which contains claim_devices_via_script.py and device.json) on any one ADC (that ADC should have network connectivity to other ADC instances)
3. Run the command

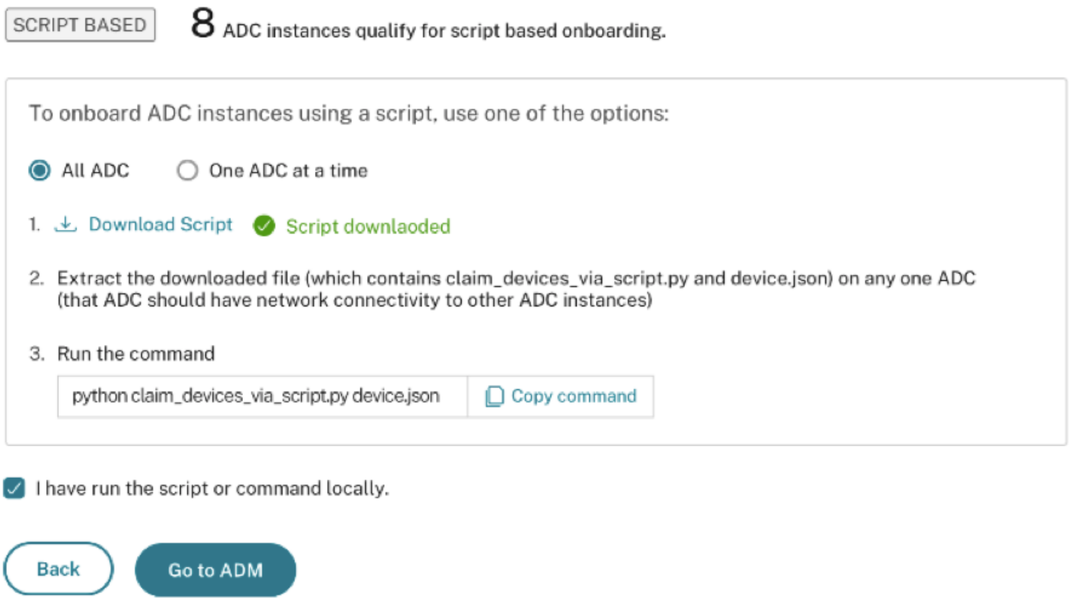
```
python claim_devices_via_script.py device.json
```

□ I have run the script or command locally.

> **Note**
>
> If you don't want the ADC instances to auto-onboard to Citrix Application Delivery and Management, you can disable auto-onboarding and you use the script-based option for on onboarding.

Script-based onboarding: after auto-onboarding completes, you can onboard the rest of the instances using the script-based onboarding. Use one of the following options:

- **Option 1**: download the script, extract the tar file, and run it on any one of the ADC instances, using the command given on the UI. Ensure that the ADC instance on which you run this script has network connectivity to all the other selected ADC instances.
- **Option 2**: Log in to the CLI console of each ADC instance and run the commands given on the UI. For more details, refer to step 7 in the doc Configure the ADC built-in agent to manage instances. Ensure that you generate a new unique activation code for each of the ADC instances.



SCRIPT BASED 8 ADC instances qualify for script based onboarding.

To onboard ADC instances using a script, use one of the options:

● All ADC ○ One ADC at a time

1. Download Script ✓ Script downlaoded
2. Extract the downloaded file (which contains claim_devices_via_script.py and device.json) on any one ADC (that ADC should have network connectivity to other ADC instances)
3. Run the command

```
python claim_devices_via_script.py device.json
```

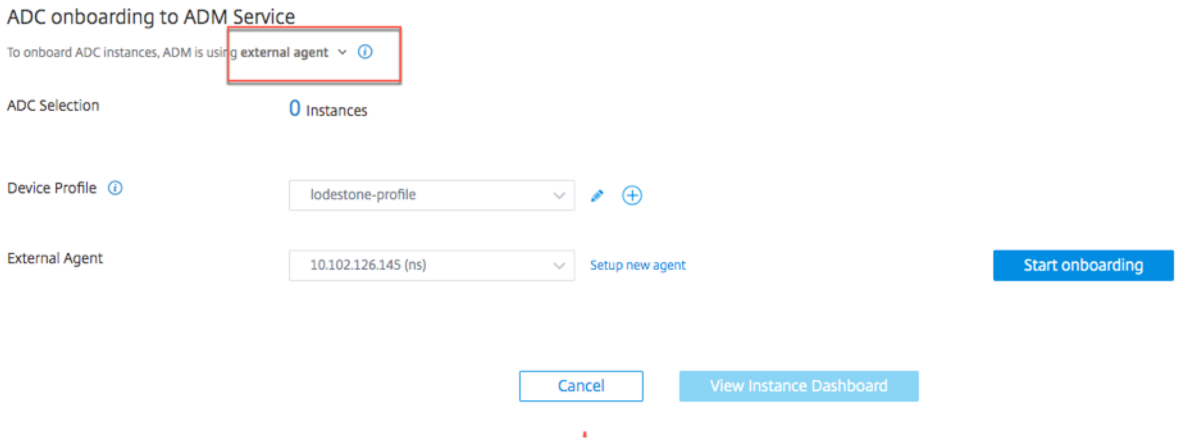
☑ I have run the script or command locally.

After you've onboarded all your instances, click **Go to Citrix Application Delivery and Management** to go to the Citrix Application Delivery and Management instance management UI dashboard and explore the different features.

> **Note**
>
> If you are a new customer on Citrix Application Delivery and Management without an Citrix Application Delivery and Management license, your Citrix service account by default is an Express account. For more information about the Citrix Application Delivery and Management account entitlement, see Manage Citrix Application Delivery and Management resources using Express account.

Onboard ADC instances using an external agent

You can use external agent-based onboarding if you want to use pooled licensing or the complete analytics suite in Citrix Application Delivery and Management or both use pooled licensing and the complete analytics suite.


ADC onboarding to ADM Service

To onboard ADC instances, ADM is using **external agent**

ADC Selection: 0 Instances

Device Profile: lodestone-profile

External Agent: 10.102.126.145 (ns)

Complete the following steps:

1. Select a device profile.

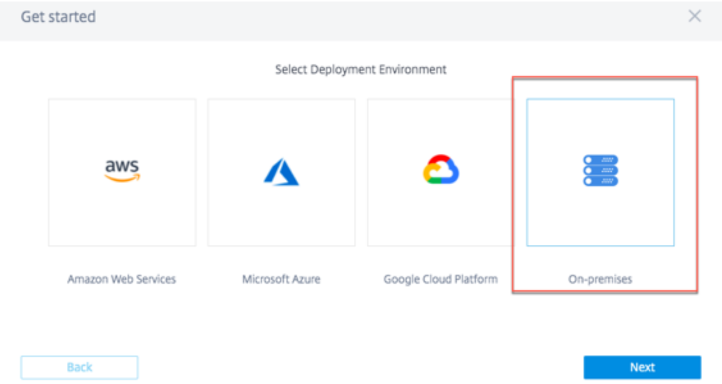
   > **Note**
   >
   > For security reasons, you can't use the default ADC credentials (nsroot/nsroot) for onboarding.

2. Select an external agent and click **Setup new agent**.
3. Select any of the following environments:

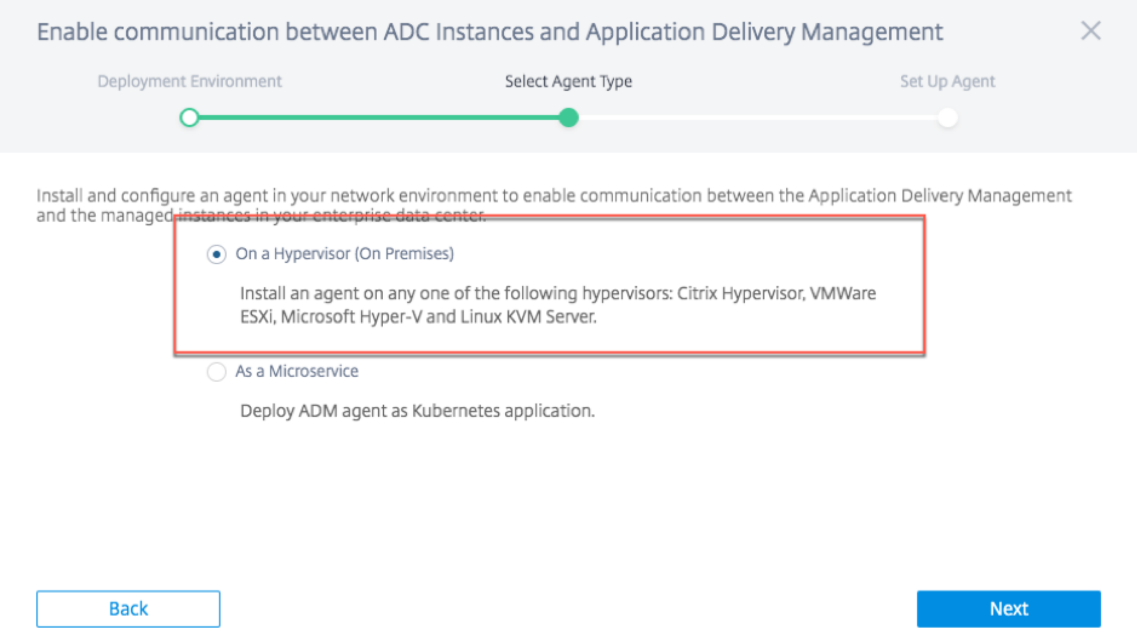
   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - On-premises

Install an agent on your on-premises hypervisor

If you select **On-premises**, you can install the agent on the following hypervisors: Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.



1. Select **On a Hypervisor (On Premises)** and click **Next**.



Enable communication between ADC Instances and Application Delivery Management

Install and configure an agent in your network environment to enable communication between the Application Delivery Management and the managed instances in your enterprise data center.

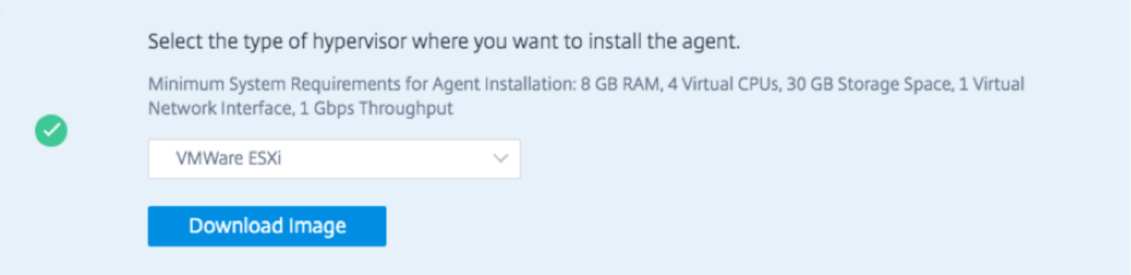
● On a Hypervisor (On Premises)

Install an agent on any one of the following hypervisors: Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V and Linux KVM Server.

○ As a Microservice

Deploy ADM agent as Kubernetes application.

2. Select the hypervisor type and download the image, for example, VMware ESXi.

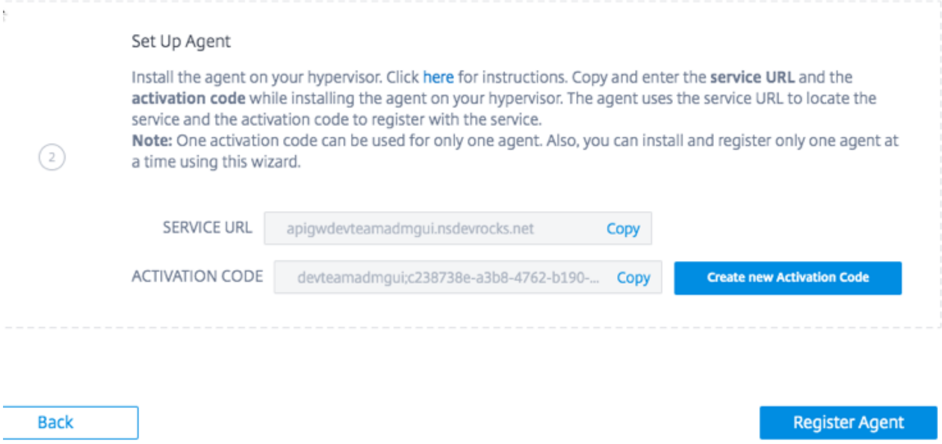


Select the type of hypervisor where you want to install the agent.

Minimum System Requirements for Agent Installation: 8 GB RAM, 4 Virtual CPUs, 30 GB Storage Space, 1 Virtual Network Interface, 1 Gbps Throughput

VMWare ESXi

3. Use the service URL and activation code to configure the agent.



Set Up Agent

Install the agent on your hypervisor. Click here for instructions. Copy and enter the **service URL** and the **activation code** while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.
Note: One activation code can be used for only one agent. Also, you can install and register only one agent at a time using this wizard.

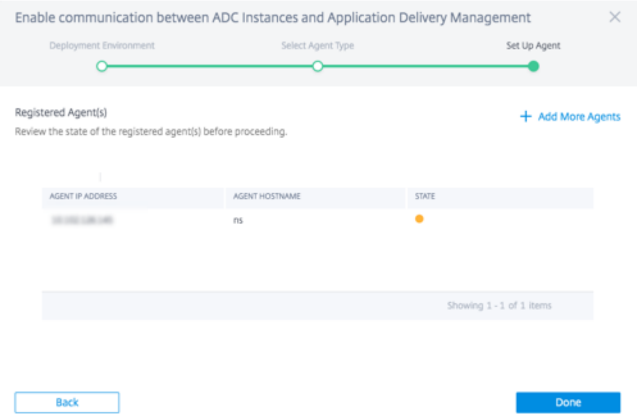
SERVICE URL: apigwdevteamadmgui.nsdevrocks.net

ACTIVATION CODE: devteamadmgui;c238738e-a3b8-4762-b190-...

The agent uses the service URL to locate the service and the activation code to register with the service. For detailed instructions about installing an agent on your on-premises hypervisor, see

   Install Citrix Application Delivery and Management agent on-premises

4. Click **Register Agent**. When completed, and click **Done** to return to the ADC onboarding Citrix Application Delivery and Management page.



Enable communication between ADC Instances and Application Delivery Management

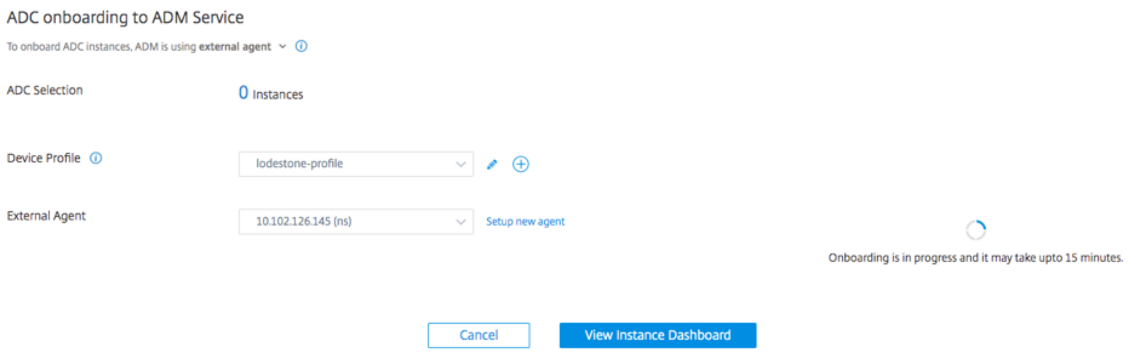
Registered Agent(s)

Review the state of the registered agent(s) before proceeding.

AGENT IP ADDRESS	AGENT HOSTNAME	STATE
[redacted]	ns	●

Showing 1 - 1 of 1 items

5. Click **Start onboarding**. After you've onboarded all your instances, click **View instance dashboard** to go to the Citrix Application Delivery and Management instance management UI dashboard and explore the different features.



ADC onboarding to ADM Service

To onboard ADC instances, ADM is using **external agent**

ADC Selection: 0 Instances

Device Profile: lodestone-profile

External Agent: 10.102.126.145 (ns)

Onboarding is in progress and it may take upto 15 minutes.

Install an agent on a public cloud

You can install the agent in one of the following cloud environments:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

For more information, see the following documents:

- Install Citrix Application Delivery and Management agent on Microsoft Azure cloud
- Install Citrix Application Delivery and Management agent on AWS
- Install Citrix Application Delivery and Management agent on GCP

Troubleshoot issues using the diagnostic tool

September 25, 2021

> Note
>
> The diagnostic tool is applicable only for the ADC instances onboarded or to be onboarded using the Citrix Application Delivery and Management connect based low-touch onboarding.
>
> For more information, see Low-touch onboarding of Citrix ADC instances using Citrix Application Delivery and Management connect.

When you onboard an ADC instance onto Citrix Application Delivery and Management, you might experience few issues that prevent the ADC instance from successful onboarding. As an administrator, you must know the reason for the onboarding failure. You can perform diagnostic checks using the diagnostic tool when you:

- Experience any issues during auto-onboarding or script-based onboarding
- Want to ensure if the ADC instance is ready to onboard
- Want to analyze issues for the already onboarded ADC instances that show "Down" status in the Citrix Application Delivery and Management GUI

After analyzing the issues, you can troubleshoot and then onboard the ADC instances to Citrix Application Delivery and Management. If the issues still persist even after troubleshooting, you can contact Citrix support. When you contact Citrix support, you must provide the Citrix Application Delivery and Management connect configuration information that is displayed after you run the diagnostic tool. You can view the Citrix Application Delivery and Management connect configuration information details in the **Use the diagnostic tool** section in this document.

Use the diagnostic tool

The diagnostic tool is available as part of the `mastools` upgrade (13.1-2.x or later) and accessible at `/var/mastools/scripts`. You can verify the `mastools` version by running the `cat /var/mastools/version.txt` command in the ADC instance.

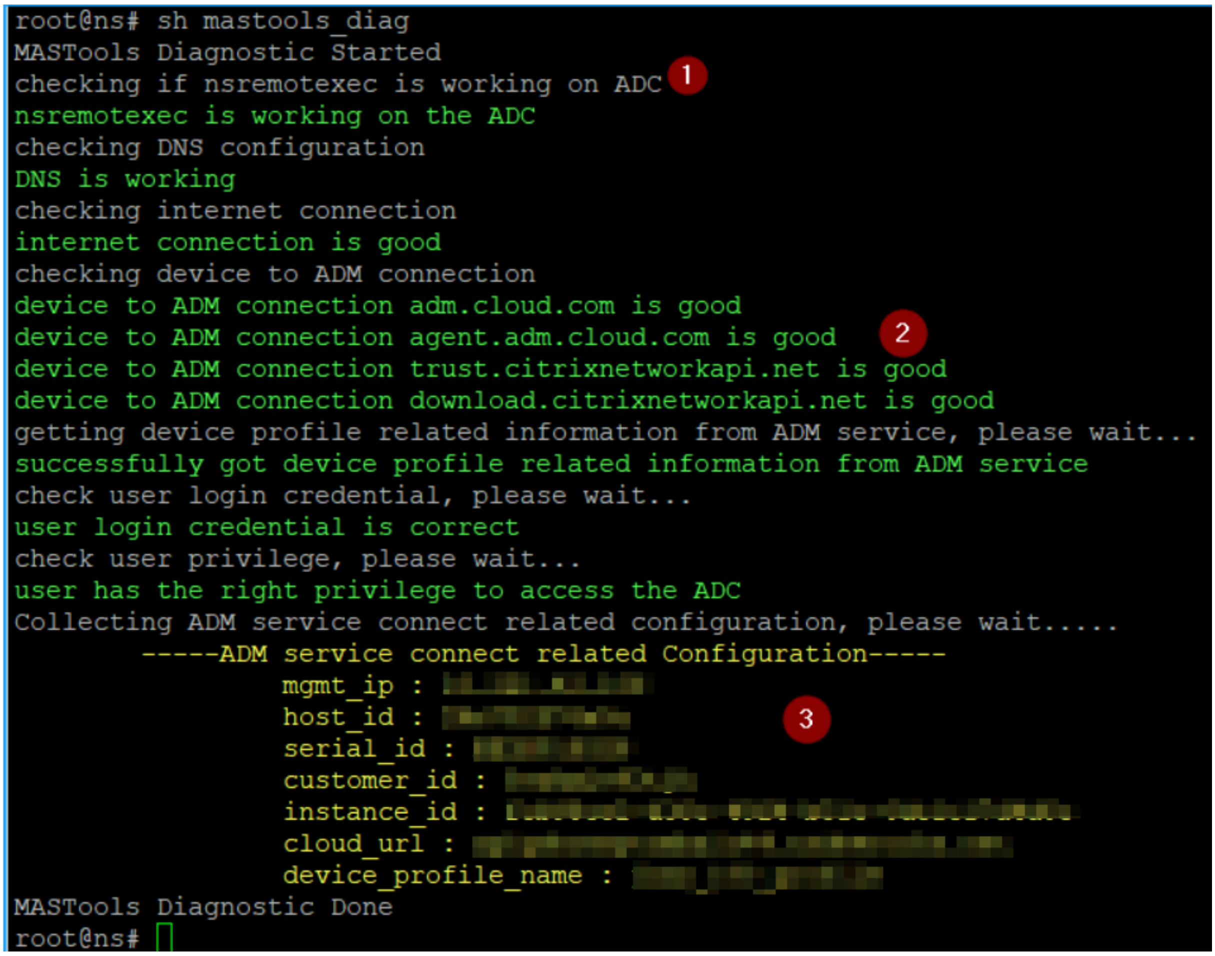
To run the diagnostic tool:

1. Using an SSH client, log on to the ADC instance.
2. Type shell and press Enter to switch to bash mode.
3. Type `cd /var/mastools/scripts`.
4. Type `sh mastools_diag`.

The tool starts and displays the results for the following diagnostic checks:

- **nsremotexec**
- **DNS configuration**
- **Internet connection**
- **Instance to Citrix Application Delivery and Management connection**
- **User privilege**

The following is an example of diagnostic results for an ADC instance that has no issues:

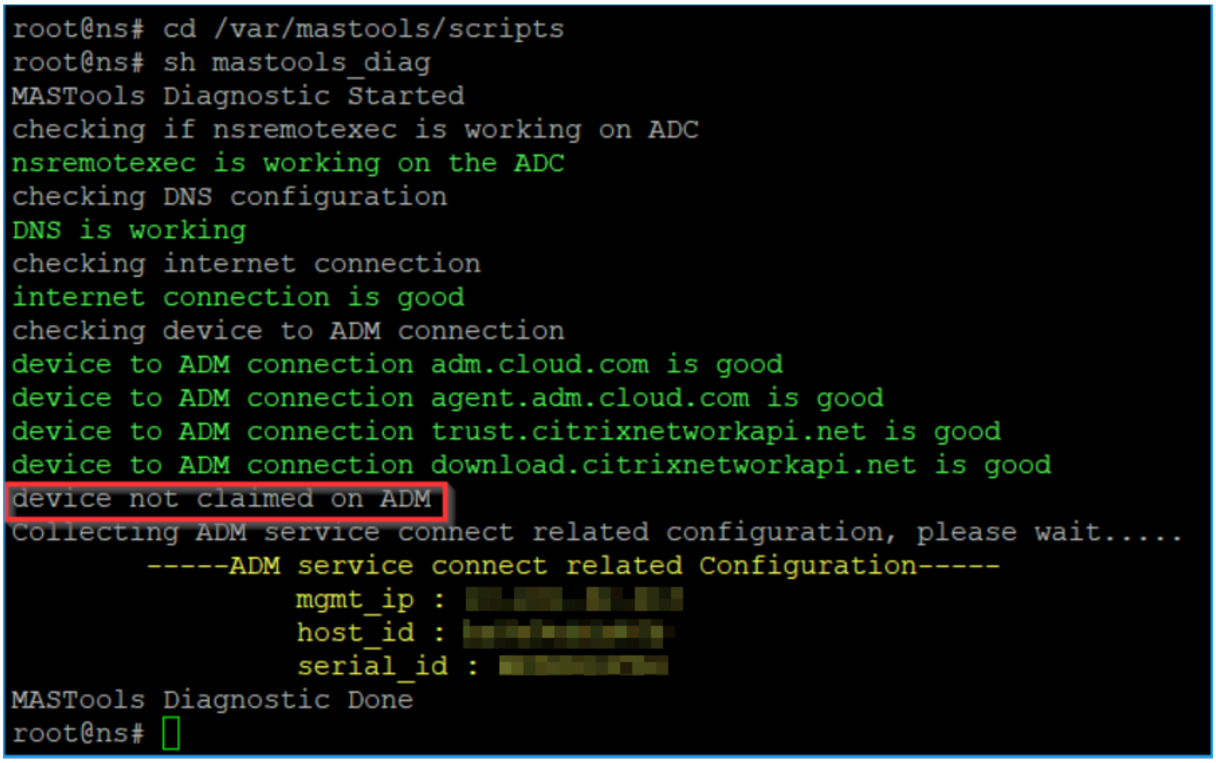


```
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
DNS is working
checking internet connection
internet connection is good
checking device to ADM connection
device to ADM connection adm.cloud.com is good
device to ADM connection agent.adm.cloud.com is good
device to ADM connection trust.citrixnetworkapi.net is good
device to ADM connection download.citrixnetworkapi.net is good
getting device profile related information from ADM service, please wait...
successfully got device profile related information from ADM service
check user login credential, please wait...
user login credential is correct
check user privilege, please wait...
user has the right privilege to access the ADC
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                 mgmt_ip : [redacted]
                 host_id : [redacted]
                 serial_id : [redacted]
                 customer_id : [redacted]
                 instance_id : [redacted]
                 cloud_url : [redacted]
                 device_profile_name : [redacted]
MASTools Diagnostic Done
root@ns# 
```

- **1** – Displays the type of diagnostic check
- **2** – Displays the diagnostic check results either in green or in red. Green indicates the result is successful and red indicates the result is not successful.
- **3** – Displays the Citrix Application Delivery and Management configuration information in yellow each time you run the diagnostic tool. If you want to contact Citrix support, you must provide this information.

Validate the ADC instance readiness for onboarding

Before you onboard the ADC instance to Citrix Application Delivery and Management, you can check the readiness of the ADC instance, by running the diagnostic tool on the ADC instance. If the ADC instance has no issues and ready to onboard, the tool displays the **device not claimed on Citrix Application Delivery and Management** message.

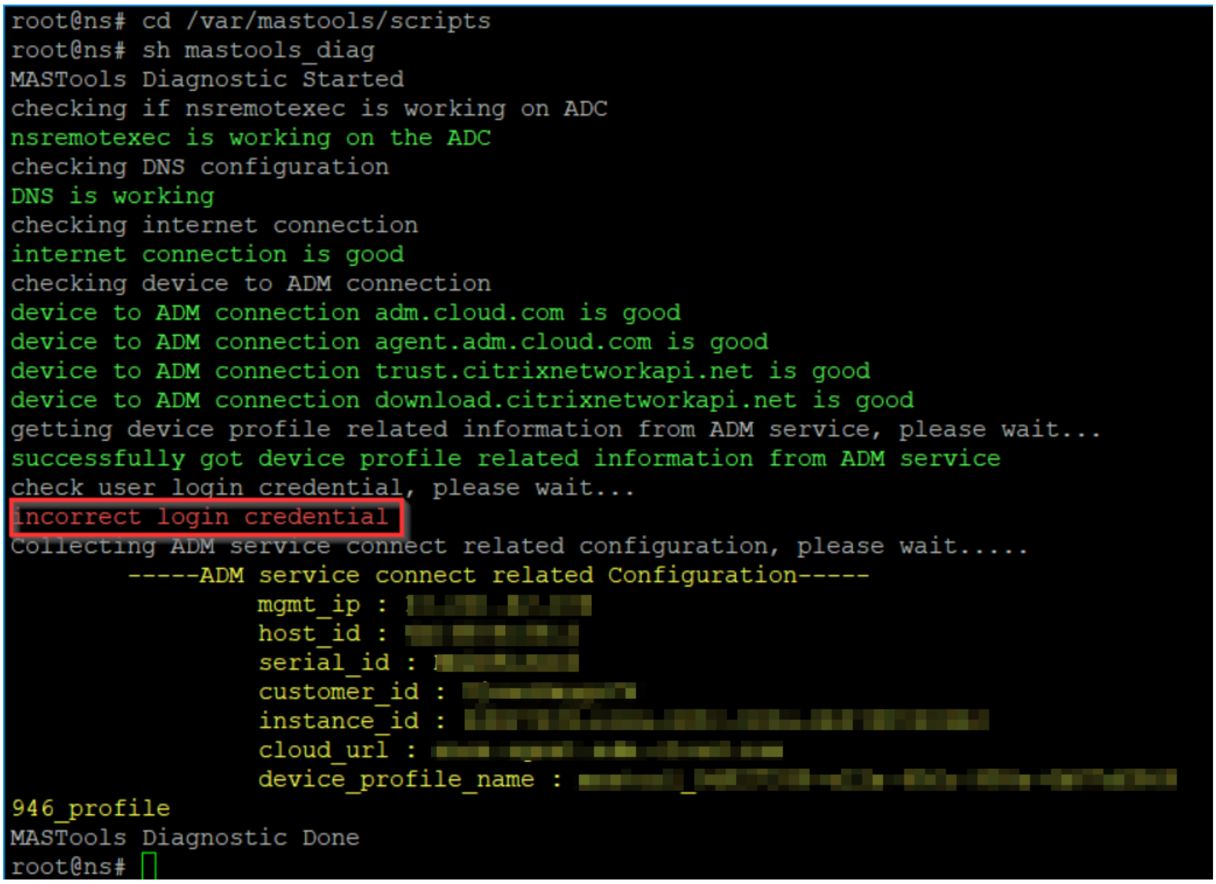


```
root@ns# cd /var/mastools/scripts
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
DNS is working
checking internet connection
internet connection is good
checking device to ADM connection
device to ADM connection adm.cloud.com is good
device to ADM connection agent.adm.cloud.com is good
device to ADM connection trust.citrixnetworkapi.net is good
device to ADM connection download.citrixnetworkapi.net is good
device not claimed on ADM
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                 mgmt_ip : [redacted]
                 host_id : [redacted]
                 serial_id : [redacted]
MASTools Diagnostic Done
root@ns#
```

Troubleshoot

The following are some of the ADC instance issues and their troubleshooting steps:

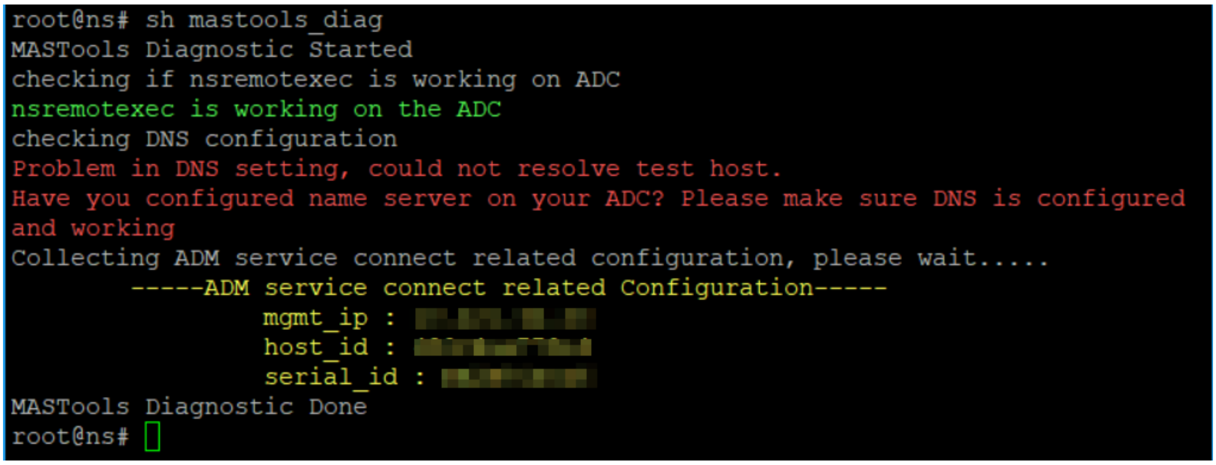
Invalid user name or password



```
root@ns# cd /var/mastools/scripts
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
DNS is working
checking internet connection
internet connection is good
checking device to ADM connection
device to ADM connection adm.cloud.com is good
device to ADM connection agent.adm.cloud.com is good
device to ADM connection trust.citrixnetworkapi.net is good
device to ADM connection download.citrixnetworkapi.net is good
getting device profile related information from ADM service, please wait...
successfully got device profile related information from ADM service
check user login credential, please wait...
incorrect login credential
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                mgmt_ip : [redacted]
                host_id : [redacted]
                serial_id : [redacted]
                customer_id : [redacted]
                instance_id : [redacted]
                cloud_url : [redacted]
                device_profile_name : [redacted]
946_profile
MASTools Diagnostic Done
root@ns#
```

Workaround: Ensure the user name and password provided in the Admin profile are correct. If you have modified the ADC instance password, you must modify the admin profiles of the instances. For more information, see Modify the admin profile.

DNS configuration error



```
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
Problem in DNS setting, could not resolve test host.
Have you configured name server on your ADC? Please make sure DNS is configured
and working
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                mgmt_ip : [redacted]
                host_id : [redacted]
                serial_id : [redacted]
MASTools Diagnostic Done
root@ns#
```

Workaround: Ensure the DNS is configured or the DNS IP address is valid. For more information, see DNS configuration.

No internet connection

Workaround: Ensure that the firewall setting is not blocking the internet access and the required proxy is configured.

No connection to Citrix Application Delivery and Management endpoint

Workaround: Ensure to check firewall settings and the following Citrix Application Delivery and Management endpoints are not blocked in firewall:

```
ADM_GRP_EP = "adm.cloud.com"

ADM_AGENT_EP = "agent.adm.cloud.com"

ADM_TRUST_EP = "trust.citrixnetworkapi.net"

ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
<!--NeedCopy-->
```

If no issue found in the diagnostic checks and the no connection issue still persists, make a note of the Citrix Application Delivery and Management configuration information (available in yellow) and contact Citrix support.

Transition from a built-in agent to an external agent

September 25, 2021

You might have started with using Citrix Application Delivery and Management for management and monitoring only, and later you might want to use other features such as pooled licensing and analytics. For that, you must transition from the built-in Citrix Application Delivery and Management agent to an external agent.

The built-in agent supports only Citrix Application Delivery and Management management and monitoring features. For other Citrix Application Delivery and Management features such as pooled licensing and analytics, you need an external agent. This document covers the steps for transitioning from an existing Citrix Application Delivery and Management built-in agent to an external hypervisor-based agent.

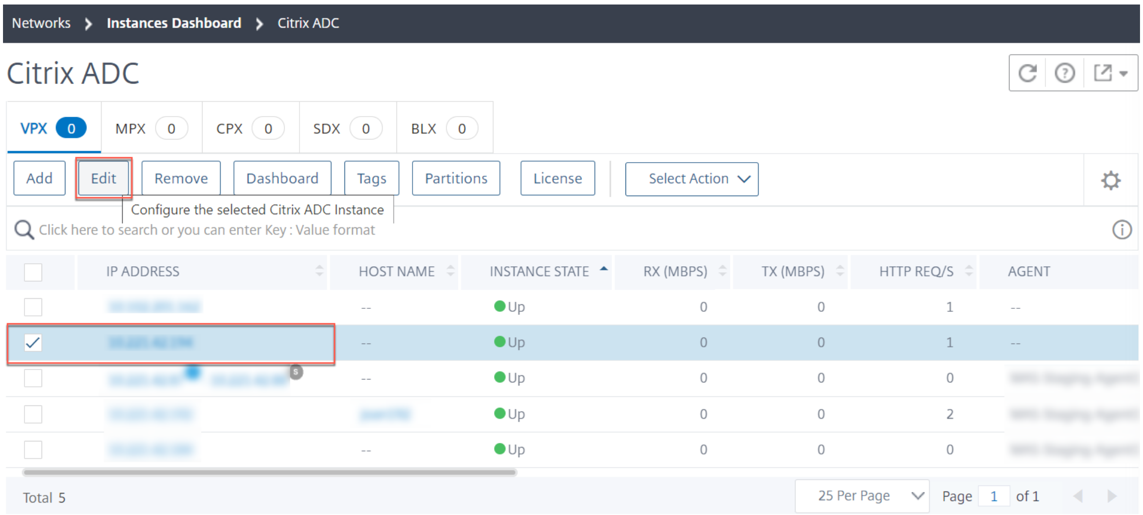
Before you start

Install an external agent before you start transitioning. Follow the procedure given in the topic Install Citrix Application Delivery and Management agent on-premises.

Transition from a built-in agent to an external agent

Follow these steps to transition from a built-in agent to an external agent:

1. In the Citrix Application Delivery and Management GUI, under **Infrastructure > Instances Dashboard > Citrix ADC**, select the Citrix ADC instance and click **Edit**.

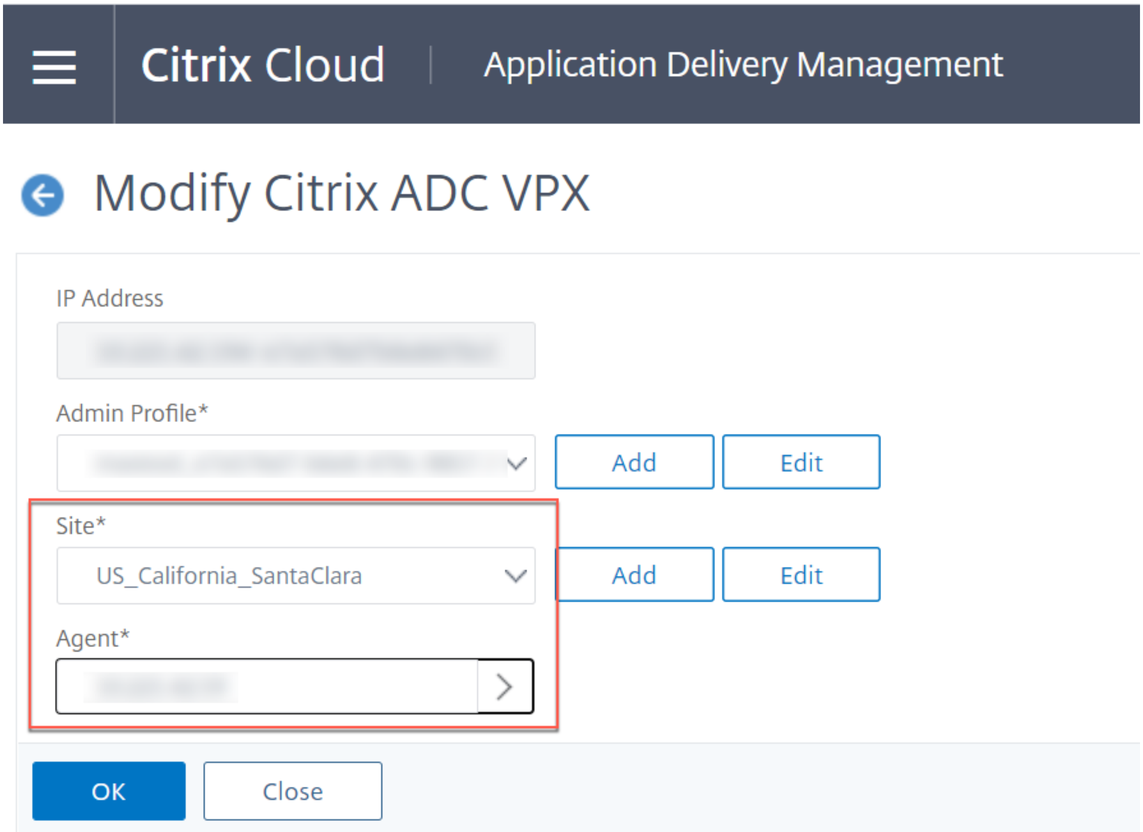


Networks > Instances Dashboard > Citrix ADC
Citrix ADC
VPX 0
MPX 0
CPX 0
SDX 0
BLX 0
Add
Edit
Remove
Dashboard
Tags
Partitions
License
Select Action
Configure the selected Citrix ADC Instance
Click here to search or you can enter Key : Value format

☐	IP ADDRESS	HOST NAME	INSTANCE STATE	RX (MBPS)	TX (MBPS)	HTTP REQ/S	AGENT
☐	[redacted]	--	● Up	0	0	1	--
☑	[redacted]	--	● Up	0	0	1	--
☐	[redacted]	--	● Up	0	0	0	[redacted]
☐	[redacted]	[redacted]	● Up	0	0	2	[redacted]
☐	[redacted]	--	● Up	0	0	0	[redacted]

Total 5
25 Per Page
Page 1 of 1

2. Select the site and agent and click **OK**.



Modify Citrix ADC VPX

IP Address: [redacted]

Admin Profile*: [redacted]

Site*: US_California_SantaClara

Agent*: [redacted]

3. Select the instance again and click **Select Action > Rediscover**.

System requirements

September 25, 2021

Before you begin using Citrix Application Delivery and Management, you must review the software requirements, browser requirements, port information, license information, and limitations.

Supported browsers

To access Citrix Application Delivery and Management, your workstation must have a supported web browser.

The following browsers are supported.

Web Browser	Version
Internet Explorer	11.0 and later
Google Chrome	Chrome 19 and later

Web Browser	Version
Safari	Safari 5.1.1 and later
Mozilla Firefox	Firefox 3.6.25 and later

Agent installation requirements

Install and configure an agent in your network environment to enable communication between the Citrix Application Delivery and Management and the managed instances in your data center. In your data center on-premises, you can install an agent on Citrix XenServer, VMware ESXi, Microsoft Hyper-V, and Linux KVM server.

The agent requirements are the virtual computing resources that the hypervisor must provide for each Citrix Application Delivery and Management agent. The following table lists the agent requirements to avail all Citrix Application Delivery and Management features:

Component	Requirement
RAM	32 GB
Virtual CPU	8
Storage Space	30 GB
Virtual Network interfaces	1
Throughput	1 Gbps

The agent requirements to avail only the pooled licensing feature, see Lightweight agent for pooled licensing.

You can also install an agent on Microsoft Azure or AWS or Google Cloud. Citrix recommends you use the following virtual machine types from the respective cloud marketplaces to avail all Citrix Application Delivery and Management features:

Cloud	Agent requirements	Preferred virtual machine type
AWS	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`m4.2xlarge`
Microsoft Azure	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`Standard_D8s_v3`

Cloud	Agent requirements	Preferred virtual machine type
Google Cloud	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`e2-standard-8`

For instructions about installing an agent, see the following links:

- Installing Citrix Application Delivery and Management Agent on Microsoft Azure Cloud.
- Installing Citrix Application Delivery and Management Agent on AWS.
- Installing Citrix Application Delivery and Management Agent on Google Cloud.

Lightweight agent for pooled licensing

If you plan to use the Citrix Application Delivery and Management only for pooled licensing, you can use an agent with lower specifications, as listed in the following table:

Component	Requirement
RAM	8 GB
Virtual CPU	4
Storage Space	30 GB

Such agents with lower specifications (lightweight) are supported only on Citrix Application Delivery and Management.

Citrix recommends you use the following virtual machine types from the respective cloud marketplaces to avail only the pooled licensing feature:

Cloud	Agent requirements	Preferred virtual machine type
AWS	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`m4.xlarge`. This instance type provides 4 virtual CPU, 16 GB RAM, and 30 GB storage space. Citrix recommends this instance type since it matches most of the agent requirements among existing instance types.

Cloud	Agent requirements	Preferred virtual machine type
Microsoft Azure	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`Standard_F4s_v2`
Google Cloud	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`e2-standard-4`

> **Note**
>
> You must disable the default scheduling jobs by navigating to **Settings > Global Settings > Configurable Features**.

Ports

For communications between Citrix ADC instances and Citrix Application Delivery and Management agent, or Citrix SD-WAN instances and Citrix Application Delivery and Management agent, the following ports must be open in a Citrix Application Delivery and Management agent:

Type	Port	Details	Direction of communication
TCP	80/443	For NITRO communication from Citrix Application Delivery and Management to Citrix ADC or Citrix SD-WAN instance.443. For NITRO communication between Citrix Application Delivery and Management servers in high availability mode.	Citrix Application Delivery and Management to Citrix ADC and Citrix ADC to Citrix Application Delivery and Management

Type	Port	Details	Direction of communication
TCP	22	For SSH communication from Citrix Application Delivery and Management to Citrix ADC or Citrix SD-WAN instance. For synchronization between Citrix Application Delivery and Management servers deployed in high availability mode. And, this port is required for the SSH communication between the Citrix Application Delivery and Management agent and Citrix ADC.	Citrix Application Delivery and Management to Citrix ADC and Citrix Application Delivery and Management agent to Citrix ADC
UDP	4739	For AppFlow communication from Citrix ADC or Citrix SD-WAN instance to Citrix Application Delivery and Management.	Citrix ADC or Citrix SD-WAN to Citrix Application Delivery and Management

Type	Port	Details	Direction of communication
ICMP	No reserved port	To detect network reachability between Citrix Application Delivery and Management and Citrix ADC instances, SD WAN instances, or the secondary Citrix Application Delivery and Management server deployed in high availability mode.	
UDP	161, 162	To receive SNMP events from Citrix ADC instance to Citrix Application Delivery and Management.	**Port 161** - Citrix Application Delivery and Management to Citrix ADC
			Port 162 - Citrix ADC to Citrix Application Delivery and Management
UDP	514	To receive syslog messages from Citrix ADC or Citrix SD-WAN instance to Citrix Application Delivery and Management.	Citrix ADC or Citrix SD-WAN to Citrix Application Delivery and Management
TCP	25	To send SMTP notifications from Citrix Application Delivery and Management to users.	

Type	Port	Details	Direction of communication
TCP	5563	To receive ADC metrics (counters), system events, and Audit Log messages from Citrix ADC instance to Citrix Application Delivery and Management.	Citrix ADC to Citrix Application Delivery and Management
TCP	5557/5558	For **logstream** communication (for Security Insight, Web Insight, and HDX Insight) from Citrix ADC to Citrix Application Delivery and Management.	Citrix ADC to Citrix Application Delivery and Management
TCP	5454	Default port for communication, and database synchronization in between Citrix Application Delivery and Management nodes in high availability mode.	Citrix Application Delivery and Management primary node to Citrix Application Delivery and Management secondary node
TCP	27000 and 7279	License ports for communication between Citrix Application Delivery and Management license server and ADC instance. These ports are also used for ADC pooled licenses.	Citrix ADC to Citrix Application Delivery and Management

Type	Port	Details	Direction of communication
TCP	443/8443/7443	Port for communication between Citrix Application Delivery and Management agent and Citrix Application Delivery and Management. The Citrix Application Delivery and Management agent initiates the communication to Citrix Application Delivery and Management.	Citrix Application Delivery and Management agent to Citrix Application Delivery and Management

For communication between Citrix Application Delivery and Management agent and Citrix Application Delivery and Management, ensure the following port is open in Citrix Application Delivery and Management agent:

Type	Port	Details
HTTPS	443	For communication from Citrix Application Delivery and Management agent to Citrix Application Delivery and Management.

> **Note**
>
> The endpoint of the Citrix Application Delivery and Management is the same as the "Service URL" generated while trying to register the agent. The agent uses the Service URL to locate the Citrix Application Delivery and Management.

Ensure that the following endpoints are whitelisted:

- Download Service:

```
https://download.citrixnetworkapi.net
<!--NeedCopy-->
```

- Trust Service:

```
*.citrixnetworkapi.net
<!--NeedCopy-->
```

- Service URLs:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
<!--NeedCopy-->
```

- ADC backup service:

```
adm-prod-backup-.*\.s3\..*amazonaws\.com
<!--NeedCopy-->
```

For communication between Citrix Application Delivery and Management agent and Citrix Analytics Service, ensure the following endpoints are whitelisted:

Endpoint	US region	EU region
Event Hub	`https://cas-eh-ns-alias.servicebus.windows.net`	`https://cas-eh-ns-eu-alias.servicebus.windows.net`

Deprecated FQDNs

Some FQDNs are deprecated for the following use of the Citrix Application Delivery and Management. To help you switch to the new FQDNs without any interruption, the deprecated FQDNs continue to work for some time and will be phased out slowly.

Citrix Application Delivery and Management Endpoints	Old FQDN	New FQDN
Citrix Application Delivery and Management UI Access	`netscalermas.cloud.com`	`adm.cloud.com`

Citrix Application Delivery and Management Endpoints	Old FQDN	New FQDN
Service URL	`agent.netscalermgmt.net`	`*.agent.adm.cloud.com` **Note**: The value of * would depend on which PoP (point of presence) your data is available.
API interactions	`netscalermas.cloud.com`	`api.adm.cloud.com`

Minimum Citrix ADC versions required

> Note
>
> Citrix ADC versions 10.5, 11.0, and 12.0 have already reached End Of Life (EOL). For more information, see the Product Matrix. The recommended ADC version is 12.1.

Citrix Application Delivery and Management Feature	Citrix ADC Software Version
StyleBooks	10.5 and later
Monitoring/Reporting and Configuring using Jobs	10.5 and later
Analytics	
HDX Insight	10.1 and later
Gateway Insight	11.0.65.31 and later
Security Insight	11.0.65.31 and later

Requirements for Citrix SD-WAN instance management

Minimum Citrix SD-WAN WANOP versions required

Citrix Application Delivery and Management Feature	Citrix CloudBridge / Citrix SD-WAN WO
Monitoring/Reporting and Configuration using Jobs	Citrix CloudBridge 7.4.0 and later
Analytics	
HDX Insight	Citrix CloudBridge 7.4.0 and later

Citrix Application Delivery and Management Feature	Citrix CloudBridge / Citrix SD-WAN WO
WAN Insight	Citrix CloudBridge 7.4.0 and later

Inter-operability matrix of Citrix SD-WAN platform editions and Citrix Application Delivery and Management features

Platform Editions	Discovery	Configuration	Monitoring	Reporting	Event Management (SNMP Traps)	HDX Insight and WAN Insight Analytics	Multi-Hop Insight
Citrix SD-WAN WANOP	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Thin clients supported for Citrix SD-WAN instances

Citrix Application Delivery and Management supports the following thin clients for monitoring Citrix SD-WAN deployments:

- Dell Wyse WTOS Model R10L Rx0L Thin Client
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced SUSE Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

Requirements for Citrix Application Delivery and Management Analytics solution

Minimum Citrix Virtual Apps and Desktops versions required

Citrix Application Delivery and Management Feature	Citrix Virtual Apps and Desktops Version
HDX Insight	Citrix Virtual Apps and Desktops 7.0 and later

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

Citrix Application Delivery and Management can generate reports for applications that are published on a Citrix Virtual App or Desktop and accessed through Citrix Receiver. However, this capability depends on the operating system on which the Receiver is installed. Currently, a Citrix ADC does not parse ICA traffic for applications or desktops that are accessed through Citrix Receiver running on iOS or Android operating systems.

Thin clients supported for HDX Insight

Citrix Application Delivery and Management supports the following thin clients for monitoring Citrix ADC instances running on software version 11.0 Build 65.31 and later:

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux based Thin Clients
- Dell Wyse ThinOS based Thin Clients
- 10ZiG Ubuntu based Thin Clients

Citrix ADC instance license required for HDX Insight

The data collected by Citrix Application Delivery and Management for HDX Insight depends on the version and the installed licenses of the Citrix ADC instances that are monitored. HDX Insight reports are displayed only for Citrix ADC Premium and Enterprise appliances running on software version 10.5 and later.

Citrix ADC 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 operating systems and Citrix Receiver versions

The following table lists the operating systems supported by Citrix Application Delivery and Management, and the Citrix Receiver versions currently supported with each system:

Operating System	Receiver 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*

* Applicable with Citrix CloudBridge release 7.4 and later.

Licenses

October 20, 2021

Citrix Application Delivery and Management requires a verified Citrix Application Delivery and Management license to manage and monitor the Citrix ADC instances.

The following are the license types supported for Citrix Application Delivery and Management for Service:

License type	**Entitled to**
Virtual server	10 virtual servers and 5 GB storage per license
Storage	5 GB per license
Express license	Citrix Application Delivery and Management Express account is a default account to manage Citrix Application Delivery and Management resources.

With an Express account, you can manage limited Citrix Application Delivery and Management resources. For more information, see Manage Citrix Application Delivery and Management resources using Express account.

After the purchased license is expired, you will have 60 days of grace period. During the grace period, you can choose the Citrix Application Delivery and Management resources that can be managed using an Express account.

For more information to get started with an Express account, see Getting Started and to manage subscriptions, see Managing Subscriptions.

Add a license

> Note:
>
> You can add only a pooled license for Citrix ADC instances.

You can add a pooled license for Citrix ADC instances in Citrix Application Delivery and Management. After you add the license, you can verify the license information in **Settings > Licensing & Analytics Config**.

To add a pooled license:

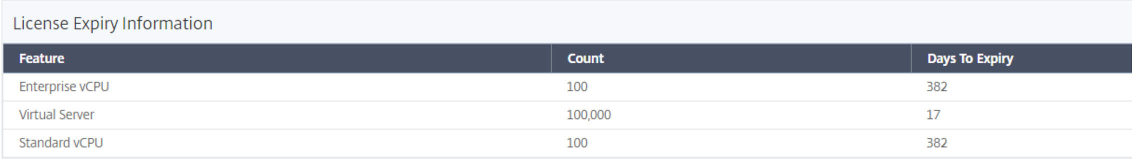
1. Navigate to **Infrastructure > Pooled Licensing**.
2. Click **Browse** to select the license file from your local computer.
3. Select the license file (.lic) and click **OK**.

Expiry checks for virtual server licenses

You can now view the status of and set alerts for license expiry in Citrix Application Delivery and Management.

To view the status of the licenses:

1. Navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Expiry Information** section, you can find the details of the licenses that are going to expire:



License Expiry Information

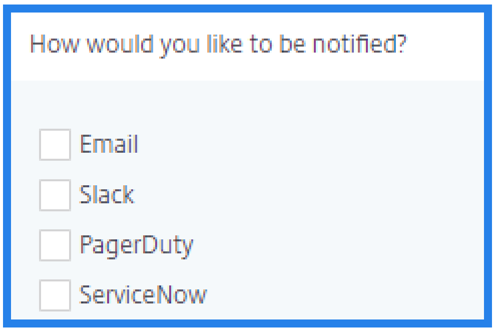
Feature	Count	Days To Expiry
Enterprise vCPU	100	382
Virtual Server	100,000	17
Standard vCPU	100	382

- **Feature**: Type of license that is going to expire.
- **Count**: Number of 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**.
2. In the **Notification Settings** section, click the pencil icon and edit the parameters.
    a) **What would you like to be notified about?** - Specify the percentage of the capacity.
    b) **How would you like to be notified?** - Select the following notification options:
        - **Email** – Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
        - **Slack** - Specify a slack profile. A notification is sent when your licenses are about to expire.
        - **PagerDuty** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your licenses are about to expire.
        - **ServiceNow** - A notification is sent to the default ServiceNow profile when your licenses are about to expire.

        > **Important**
        >
        > Ensure Citrix Cloud ITSM Adapter is configured for ServiceNow and integrated with Citrix Application Delivery and Management. For more information, see Integrate Citrix Application Delivery and Management with ServiceNow instance.

        How would you like to be notified?

        □ Email
        □ Slack
        □ PagerDuty
        □ ServiceNow

    c) **Expiry of licenses** - Specify the days before the license expires, when you want to get notified.

Manage resources using Express account

October 21, 2021

Citrix Application Delivery and Management Express account is a default account to manage Citrix Application Delivery and Management resources. This account is readily available on Citrix Cloud.

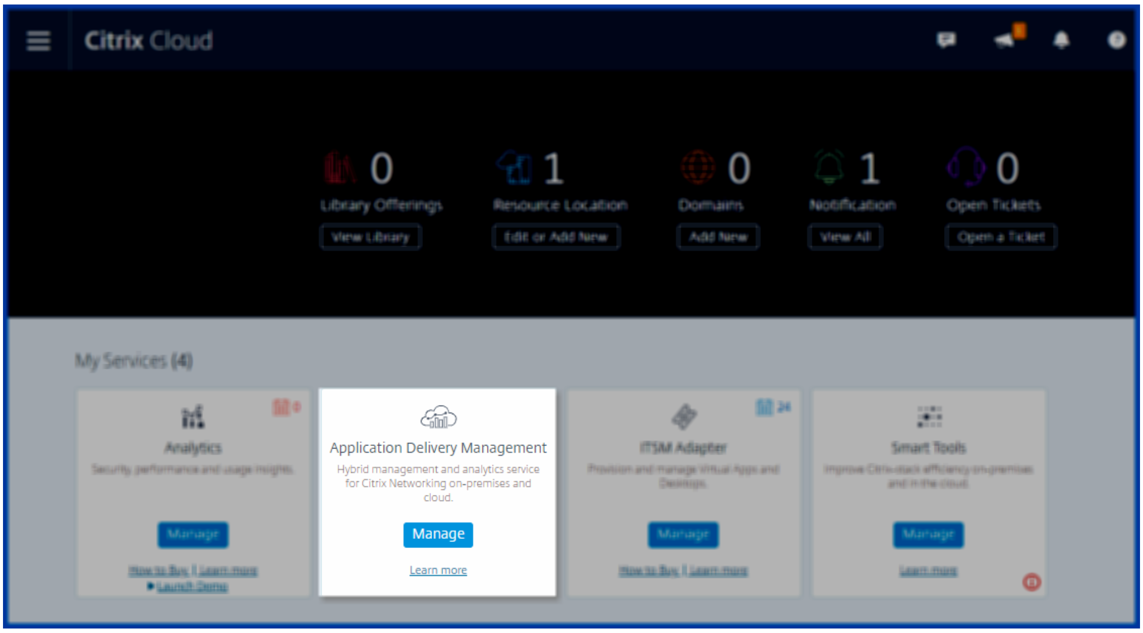
With this account, you can manage up to two virtual servers in Citrix Application Delivery and Management. However, you can monitor all discovered virtual servers in **Network Reporting** and **Network Functions**.

To manage the specific virtual servers with an Express account, you must select the required virtual servers during the grace period. Otherwise, Citrix Application Delivery and Management auto-selects the virtual servers which you can manage with the Express account.

> **Important**
>
> - When your account is converted to an Express account, the Citrix Application Delivery and Management retains the storage data up to 500 MB or one day data, whichever is the lesser.
> - If your Citrix Application Delivery and Management Express account remains inactive for 90 days, the account will be deleted. Citrix sends a reminder after 60 days of inactivity.

To manage the Citrix Application Delivery and Management resources:

1. Log on to Citrix Cloud with your credentials.
2. Click **Manage** on the **Citrix Application Delivery and Management** tile.



After your Citrix Application Delivery and Management subscription license and grace period ends, your account is converted to an Express account unless you renew your license. The Express account helps you continue your business using Citrix Application Delivery and Management. To renew your license, you can do one of the following:

- Buy Citrix Application Delivery and Management license from the GUI.
- Visit Citrix Cloud.
- Contact Technical Support.

When you renew your license, the configurations are retained from your Express account. And, you receive extra virtual servers depending on your license.

Managing subscriptions

September 28, 2021

Citrix Application Delivery and Management requires a verified license to manage and monitor Citrix ADC instances, Citrix Gateway instances, and third party load balancers.

You can manage and monitor any number of instances when you are using an Express account or when you have subscribed to a valid license. However, you can manage the discovered applications on the App Dashboard, view analytics data, and monitor network functions and network reports only for the number of virtual servers for which you have purchased licenses. For more information about the Citrix Application Delivery and Management resources that you can manage with the Express account, see The Citrix Application Delivery and Management Express account.

With each installed license, you receive a limited amount of data and capacity to manage certain virtual servers. However, you can also purchase and apply data-only licenses to top up your data storage.

For information and instructions about buying and upgrading your Citrix Application Delivery and Management licenses, see Citrix Application Delivery and Management.

The following table lists the Citrix licenses that are required to use some of the Citrix Application Delivery and Management features.

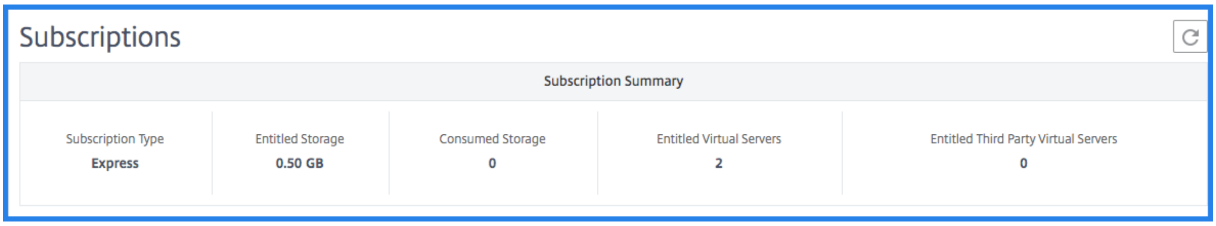
Citrix Application Delivery and Management Feature Group	Citrix Application Delivery and Management Features	Citrix ADC and Gateway License Requirement
Analytics	HDX Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
Analytics	Security Insight	Premium (or) Advanced with App Firewall license
Analytics	Gateway Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)

Citrix Application Delivery and Management Feature Group	Citrix Application Delivery and Management Features	Citrix ADC and Gateway License Requirement
Applications	Application Statistics (App Dashboard, App Security Dashboard)	Citrix Web App Firewall related information on App dashboard, and app security dashboard needs Premium (or) Advanced with App Firewall license
Applications	API gateway	Premium (or) Advanced license
Applications	StyleBooks	N/A
Applications	Inventory Management – Infrastructure Dashboard, Instance groups, Instance dashboards & Sites	N/A
Applications	Event Management & Syslog	N/A
Applications	Configuration Jobs, Configuration Audit, and Configuration Advice	N/A
Applications	Network reporting (Instance level)	N/A
Applications	Network reporting (virtual server level)	N/A
Applications	Network Functions (Plain visibility & Management of virtual servers, services, service groups, server)	N/A
Applications	SSL certificate management (Instance level)	N/A
Applications	SSL certificate management (virtual server level)	N/A
System	RBAC & External Authentication (instance level)	N/A

Citrix Application Delivery and Management Feature Group	Citrix Application Delivery and Management Features	Citrix ADC and Gateway License Requirement
System	RBAC & External Authentication (virtual server level)	N/A

View the subscription details

You can view the licenses installed on your Citrix Application Delivery and Management by navigating to **Account** > **Subscriptions**. You can also view the license summary such as the type of license subscribed to, the entitled data subscription and consumed data subscription, and the allowed and managed virtual servers and third party virtual servers in the **Subscription Summary** section.



Subscriptions

Subscription Summary

Subscription Type	Entitled Storage	Consumed Storage	Entitled Virtual Servers	Entitled Third Party Virtual Servers
Express	0.50 GB	0	2	0

Manage subscriptions for third-party virtual servers

You can manage and monitor any number of hosts when you are on the trial period or when you have subscribed to a valid license. However, you can manage the discovered applications on the App Dashboard, view analytics data, and monitor network functions only for the number of third party virtual servers for which you have purchased licenses. During trial period, you can monitor only 10 third party virtual servers or applications.

Manage virtual servers

You can select the virtual servers or third party virtual servers you want to manage and monitor through Citrix Application Delivery and Management.

Points to note:

- By default, Citrix Application Delivery and Management automatically licenses the virtual servers randomly after each virtual server poll cycle.
- If the total number of virtual servers discovered in your Citrix Application Delivery and Management is lower than the number of installed virtual server licenses, Citrix Application Delivery and Management, by default, licenses all the virtual servers.

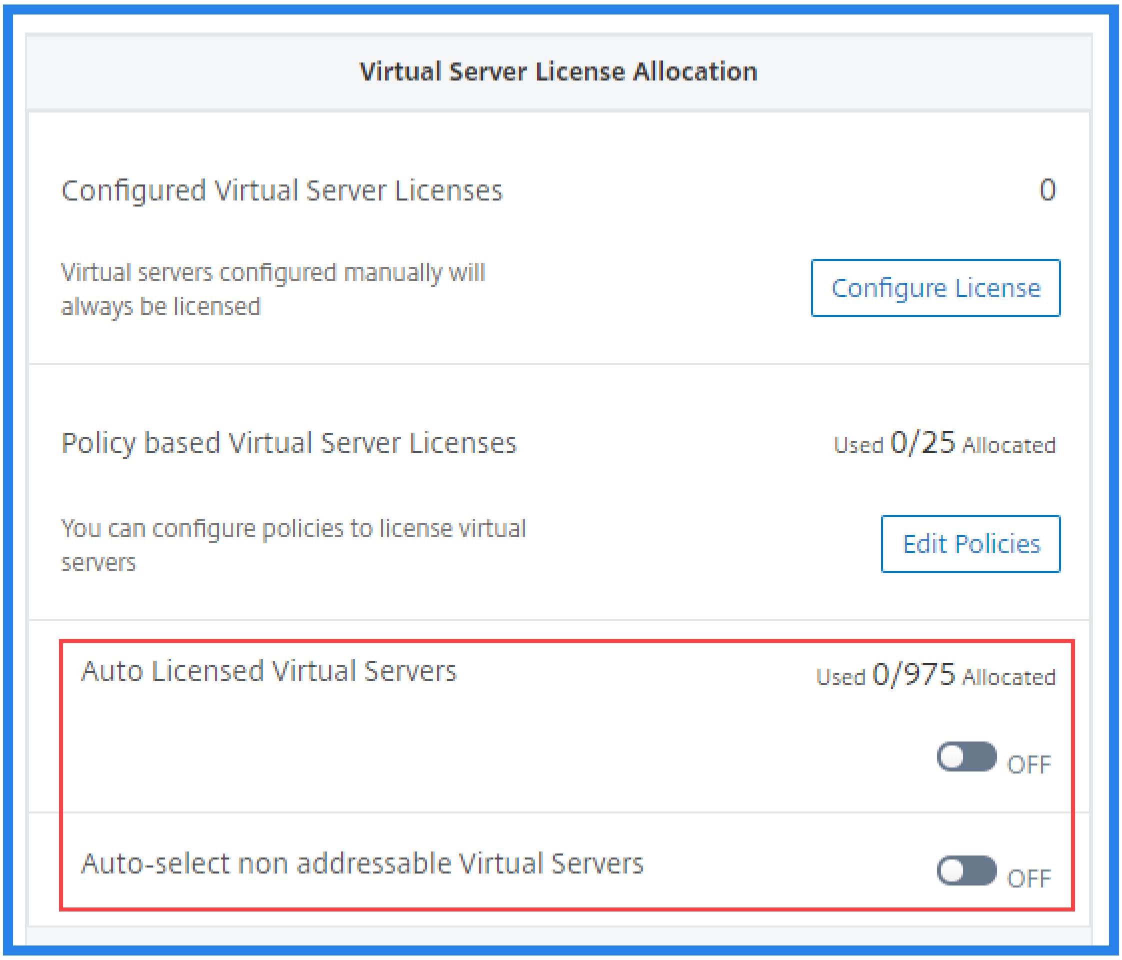
To select the virtual servers manually, or to restrict licensing to limited virtual servers, you have to first disable auto licensing the virtual servers, and then select the virtual servers you want to manage.

To disable auto-licensing virtual servers:

1. Navigate to **Settings > Citrix Application Delivery and Management Licensing & Analytics Config**.

   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**.



Virtual Server License Allocation

Configured Virtual Server Licenses 0

Virtual servers configured manually will always be licensed

Policy based Virtual Server Licenses Used 0/25 Allocated

You can configure policies to license virtual servers

Auto Licensed Virtual Servers Used 0/975 Allocated

OFF

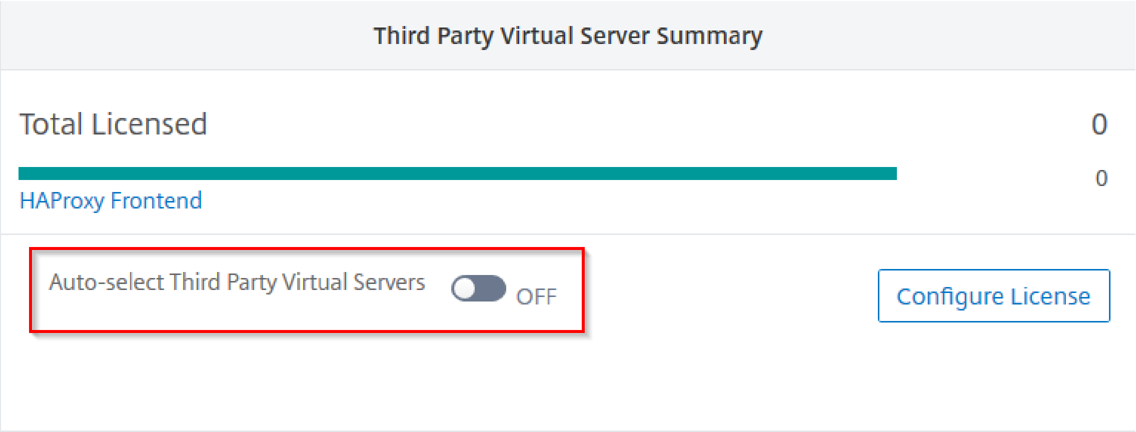
Auto-select non addressable Virtual Servers OFF

To select third party virtual servers for licensing:

1. Navigate to **Account** > **Subscriptions**.

   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**.



Third Party Virtual Server Summary

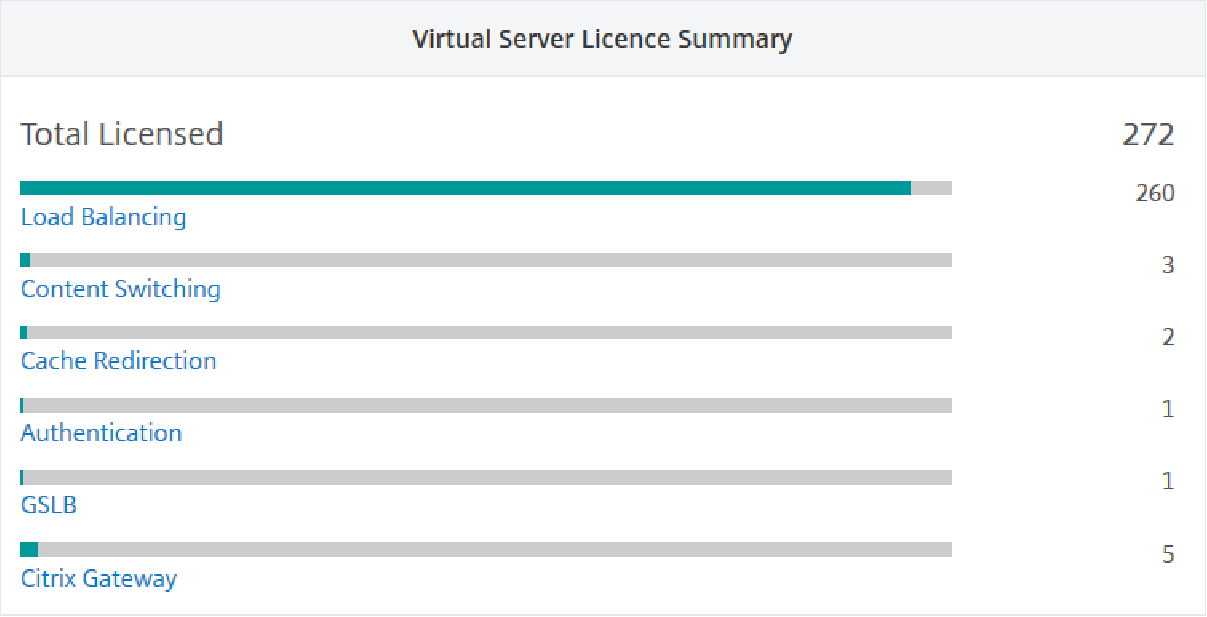
Total Licensed 0

HAProxy Frontend 0

Auto-select Third Party Virtual Servers OFF

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 from the **Subscriptions** page. To view the licensed virtual servers, navigate to **Settings > Citrix Application Delivery and Management Licensing & Analytics Config** and click the virtual server type in the **Total Licensed** section in the **Virtual Servers License Summary**.



Virtual Server Licence Summary

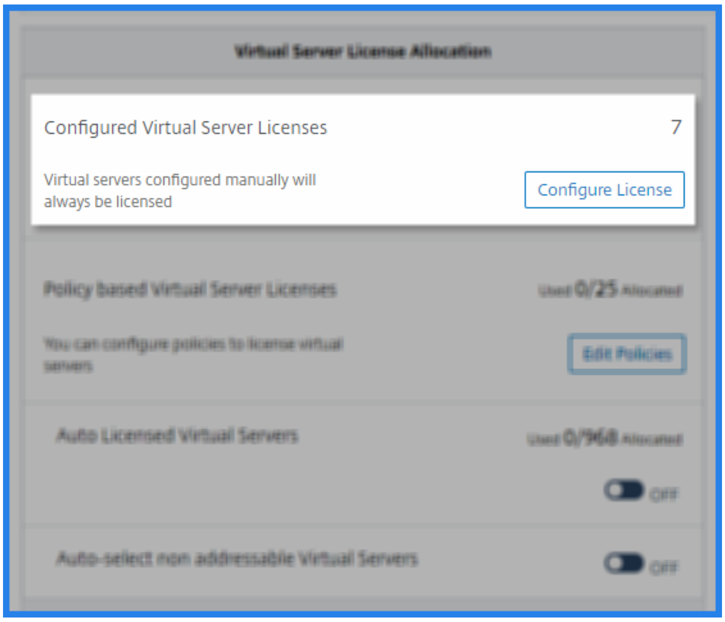
Total Licensed 272

Load Balancing	260
Content Switching	3
Cache Redirection	2
Authentication	1
GSLB	1
Citrix Gateway	5

Apply virtual server licenses manually

You can manually apply licenses to an individual virtual server.

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



Virtual Server License Allocation

Configured Virtual Server Licenses 7

Virtual servers configured manually will always be licensed

Policy based Virtual Server Licenses Used 0/25 Allocated

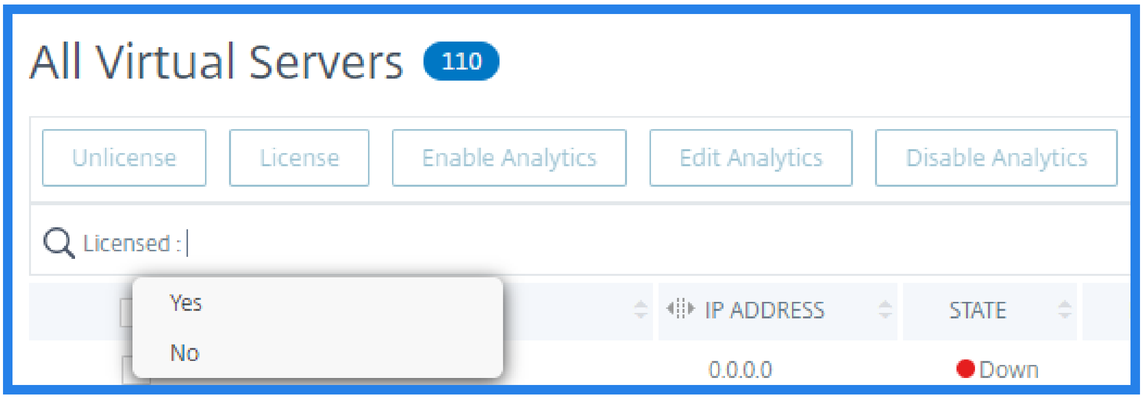
You can configure policies to license virtual servers

Auto Licensed Virtual Servers Used 0/968 Allocated

Auto-select non addressable Virtual Servers

The **All Virtual Servers** page is displayed.

2. Filter unlicensed virtual servers using the property: `Licensed: No`.



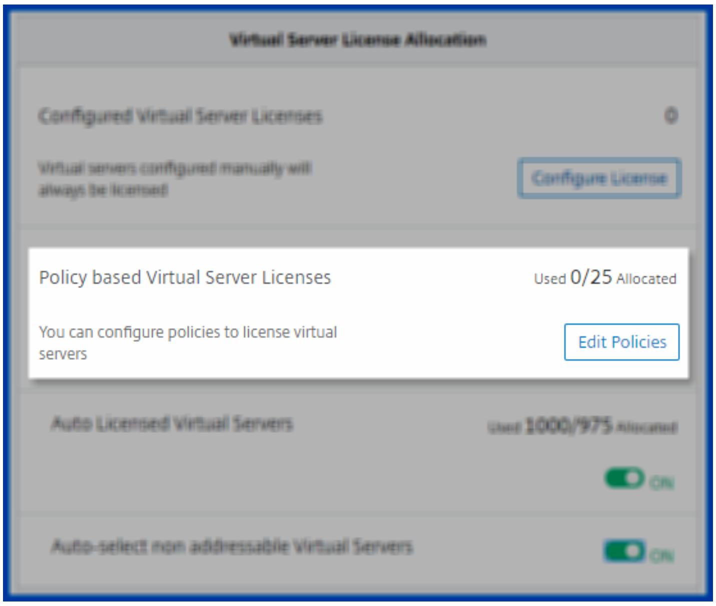
All Virtual Servers 110

Licensed :

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 you want to auto-license. It also applies licenses to selected instances' virtual servers only.



Virtual Server License Allocation

Configured Virtual Server Licenses 0

Virtual servers configured manually will always be licensed

Configure License

Policy based Virtual Server Licenses Used 0/25 Allocated

You can configure policies to license virtual servers

Edit Policies

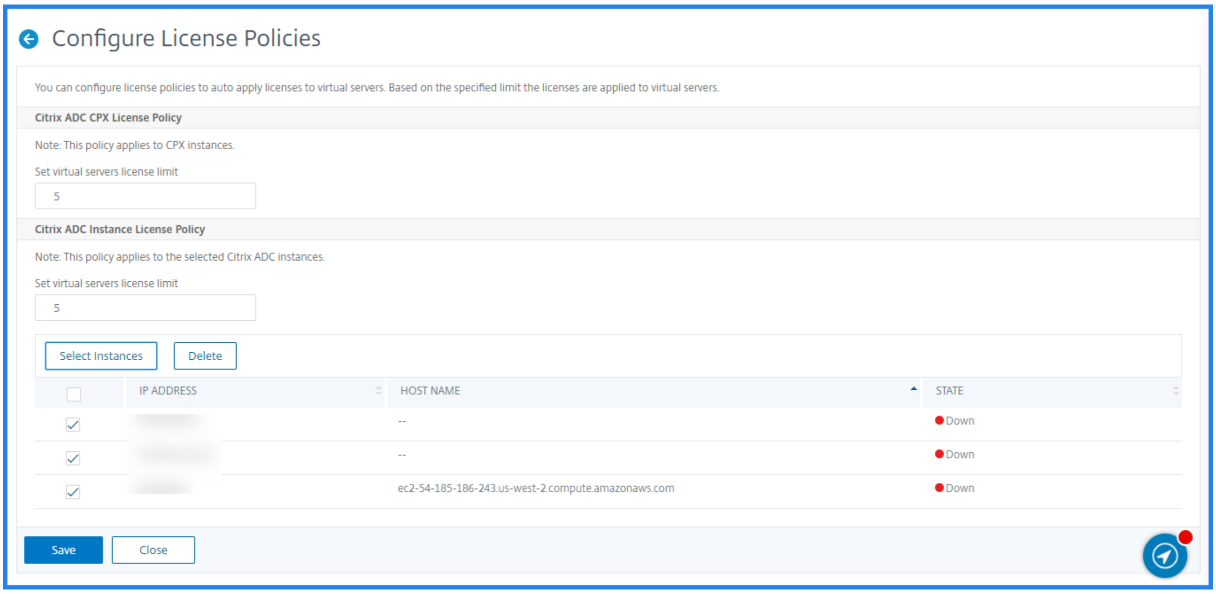
Auto Licensed Virtual Servers Used 1000/975 Allocated

ON

Auto-select non addressable Virtual Servers ON

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

- Set virtual servers limit on CPX instances separately to apply licenses. The Citrix Application Delivery and Management applies license to virtual servers on CPX instances up to a specified limit.
- Set virtual servers limit on selected ADC instances (MPX/VPX/BLX) to apply licenses. The Citrix Application Delivery and Management 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 Citrix Application Delivery and Management can apply license to selected instances' virtual servers only.



Configure License Policies

You can configure license policies to auto apply licenses to virtual servers. Based on the specified limit the licenses are applied to virtual servers.

Citrix ADC CPX License Policy

Note: This policy applies to CPX instances.

Set virtual servers license limit: 5

Citrix ADC Instance License Policy

Note: This policy applies to the selected Citrix ADC instances.

Set virtual servers license limit: 5

Select Instances | Delete

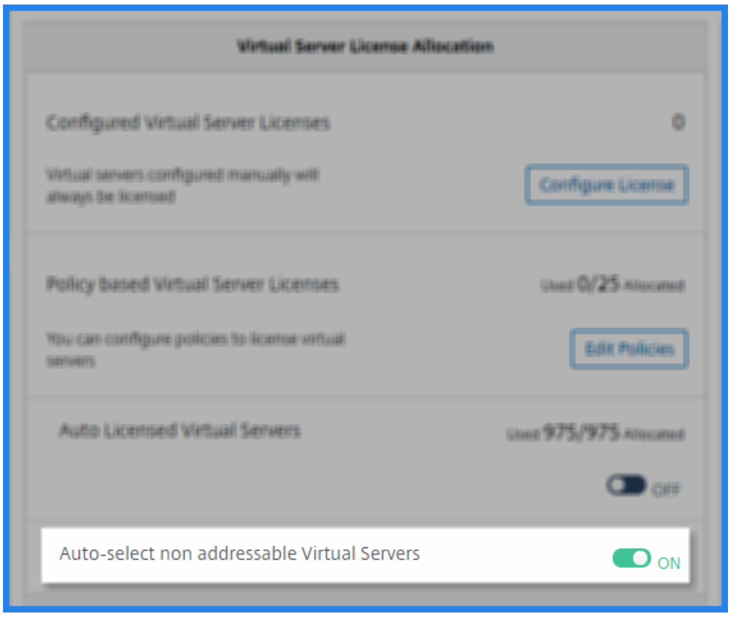
□	IP ADDRESS	HOST NAME	STATE
✓	[redacted]	--	● Down
✓	[redacted]	--	● Down
✓	[redacted]	ec2-54-185-186-243.us-west-2.compute.amazonaws.com	● Down

Save | Close

Configure auto license support for non-addressable virtual servers

Citrix Citrix Application Delivery and Management, 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.

Citrix Application Delivery and Management provides an option in Citrix Application Delivery and Management under **Virtual Server License Allocation**. If you enable **Auto-select non addressable Virtual Servers** option, automatically apply licenses non-addressable virtual servers.



Virtual Server License Allocation

Configured Virtual Server Licenses 0

Virtual servers configured manually will always be licensed

Policy based Virtual Server Licenses Used 0/25 Allocated

You can configure policies to license virtual servers

Auto Licensed Virtual Servers Used 975/975 Allocated

OFF

Auto-select non addressable Virtual Servers ON

> **Note**
>
> - Citrix Application Delivery and Management, by default, still does not select non-addressable virtual servers automatically for licensing.
> - Application analytics (App Dashboard) is the only analytics supported currently on licensed non-addressable virtual servers.

View expiry checks for virtual server subscriptions

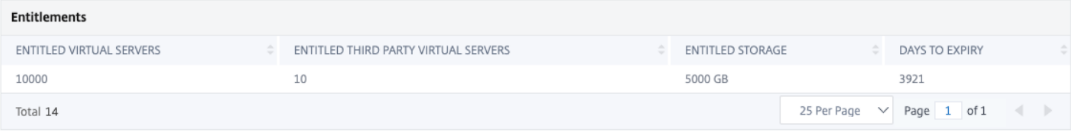
You can view the status of installed licenses with the expiry and the allowed storage limit to the licenses in Citrix Application Delivery and Management.

To view the status of the licenses:

1. Navigate to **Account** > **Subscriptions**.

2. In the **Entitlements** section, you can view the details of licensed virtual servers and the days to expiry:

   - **Entitled Virtual Servers:** Number of virtual servers available to license.
   - **Entitled Third Party Virtual Servers:** Number of third party virtual servers you can manage with the license.
   - **Entitled Storage:** Storage limit of the license.
   - **Days to Expiry:** Number of days remaining before the license expiry.



Entitlements

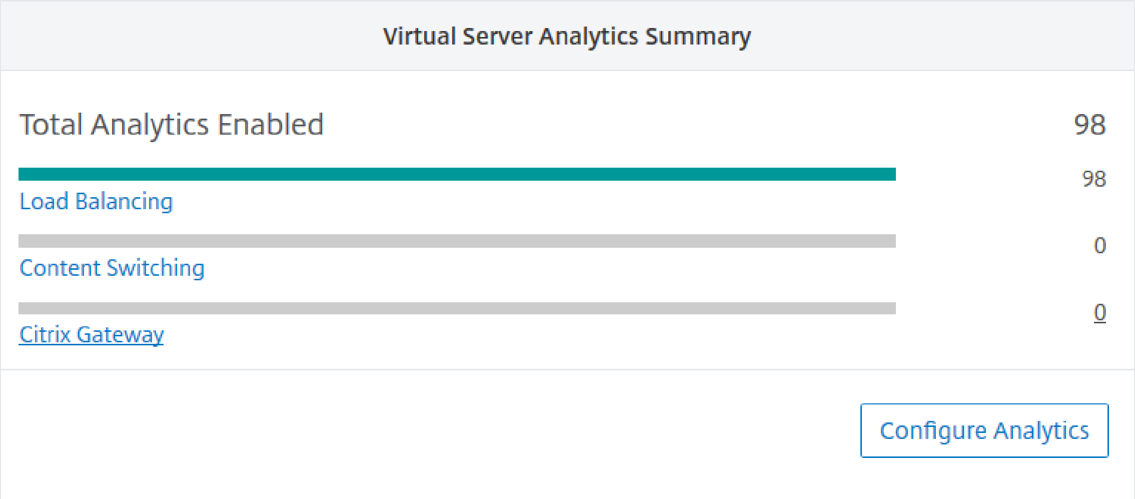
ENTITLED VIRTUAL SERVERS	ENTITLED THIRD PARTY VIRTUAL SERVERS	ENTITLED STORAGE	DAYS TO EXPIRY
10000	10	5000 GB	3921

Total 14 25 Per Page Page 1 of 1

View the type of analytics enabled on the virtual servers

After you enable AppFlow on the selected virtual servers, you can view the type of analytics enabled on the licensed virtual servers or third-party virtual servers from the **Subscriptions** page.

1. Navigate to **Account** > **Subscriptions**.
2. In the **Virtual Server Analytics Summary** section, select the type of licensed virtual servers.



Virtual Server Analytics Summary

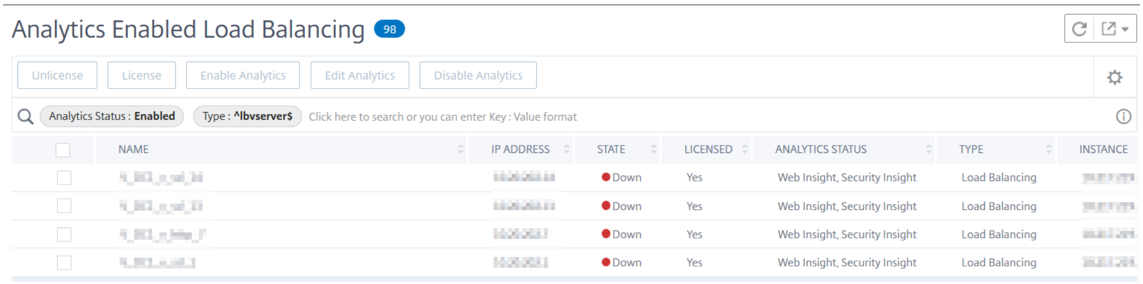
Total Analytics Enabled 98

Load Balancing 98

Content Switching 0

Citrix Gateway 0

3. The licensed virtual servers page displays the list of licensed virtual servers. On this page, the **Analytics Status** column displays the type of analytics enabled on the virtual servers.



Analytics Enabled Load Balancing 98

Analytics Status : **Enabled** Type : **^lbvserver$** Click here to search or you can enter Key : Value format

□	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE
□	[redacted]	[redacted]	● Down	Yes	Web Insight, Security Insight	Load Balancing	[redacted]
□	[redacted]	[redacted]	● Down	Yes	Web Insight, Security Insight	Load Balancing	[redacted]
□	[redacted]	[redacted]	● Down	Yes	Web Insight, Security Insight	Load Balancing	[redacted]
□	[redacted]	[redacted]	● Down	Yes	Web Insight, Security Insight	Load Balancing	[redacted]

Upgrade Advisory

September 25, 2021

As a network administrator, you might manage many ADC instances running on different ADC releases in Citrix Application Delivery and Management. Monitoring the lifecycle of each ADC instance can be a cumbersome task. You must visit Citrix Product Matrix, identify the ADC instances that are reaching or reached End of Life (EOL) or End of Maintenance (EOM). Then, plan their upgrade.

To ease this process, Citrix Application Delivery and Management upgrade advisory helps you monitor the lifecycle of your ADC instances in the following ways:

- Identifies instances reaching or reached EOL or EOM. So, you can plan ADC upgrades ahead of EOL or EOM date.
- Highlights the instances that are not on latest release or build. You can upgrade these instances to latest release or build. With this upgrade, you receive updates on new features and fixed issues.
- Highlights the instances that are not on preferred ADC builds. Some organizations might have a preferred ADC builds for their instances. In Citrix Application Delivery and Management, you can set the preferred build for your organization depending on build stability, features, and other considerations. Then, review and upgrade the instances that are not on preferred builds. Instances running the preferred builds are indicated with a star icon.
- Highlights instances running on the most popular releases or builds. Instances running the popular builds are indicated with a ribbon icon.

The upgrade advisory provides links to corresponding release notes. With this information, you can review and decide an ADC build for upgrade. You can proceed to create a maintenance job to upgrade ADC instances from the Upgrade Advisory page.

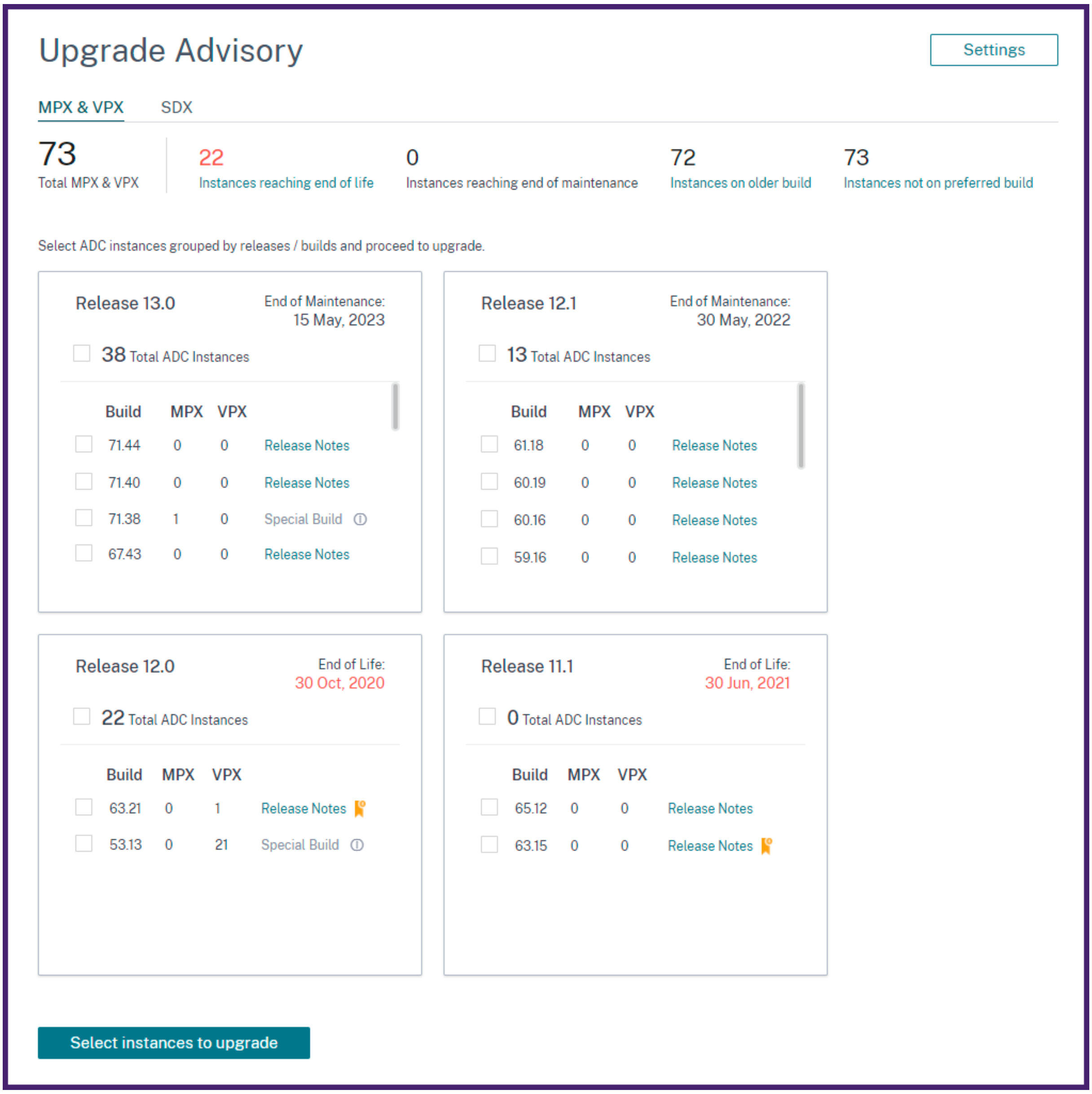
> **Important**

> Upgrade advisory only monitors EOL of ADC software releases. It doesn't check the EOL of ADC appliances.

View upgrade advisory

Navigate **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.
- Instances in older build.
- Instances not in preferred build.
- End of Life and End of Maintenance dates for the various ADC releases.



Upgrade Advisory

73 Total MPX & VPX

22 Instances reaching end of life

0 Instances reaching end of maintenance

72 Instances on older build

73 Instances not on preferred build

Select ADC instances grouped by releases / builds and proceed to upgrade.

Release 13.0 — End of Maintenance: 15 May, 2023

□ 38 Total ADC Instances

	Build	MPX	VPX	
□	71.44	0	0	Release Notes
□	71.40	0	0	Release Notes
□	71.38	1	0	Special Build ⓘ
□	67.43	0	0	Release Notes

Release 12.1 — End of Maintenance: 30 May, 2022

□ 13 Total ADC Instances

	Build	MPX	VPX	
□	61.18	0	0	Release Notes
□	60.19	0	0	Release Notes
□	60.16	0	0	Release Notes
□	59.16	0	0	Release Notes

Release 12.0 — End of Life: 30 Oct, 2020

□ 22 Total ADC Instances

	Build	MPX	VPX	
□	63.21	0	1	Release Notes
□	53.13	0	21	Special Build ⓘ

Release 11.1 — End of Life: 30 Jun, 2021

□ 0 Total ADC Instances

	Build	MPX	VPX	
□	65.12	0	0	Release Notes
□	63.15	0	0	Release Notes

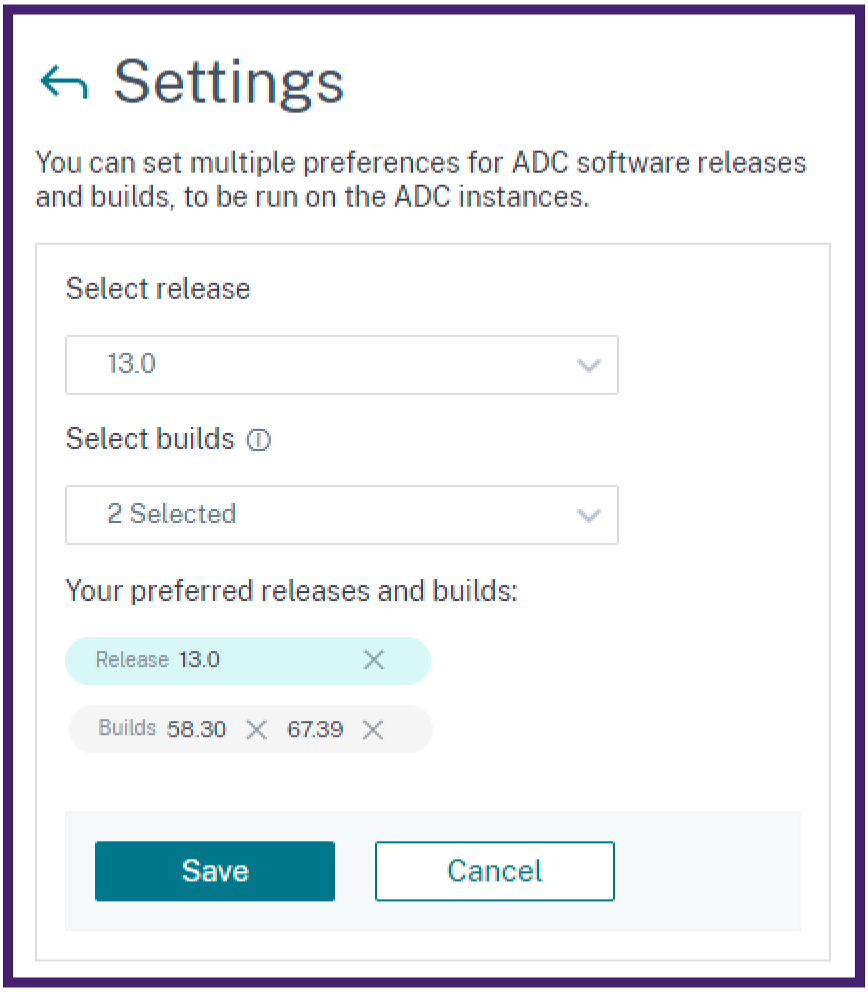
The **Upgrade Advisory** page groups the ADC instances by their releases. The **Release Notes** link guides you to the specific ADC release notes. Review new features, fixed, and known issues before deciding to upgrade. You can select multiple ADC instances across different releases to upgrade at a time. When you proceed with an upgrade, it creates an upgrade job. See, Upgrade ADC instances.

Set the preferred builds

As an administrator, you can define a preferred ADC build for organization. Do the following to set the preferred build:

1. In **Infrastructure > Instance Advisory > Upgrade Advisory**, click **Settings**.

2. Select the preferred release and build.



Settings

You can set multiple preferences for ADC software releases and builds, to be run on the ADC instances.

Select release: 13.0

Select builds: 2 Selected

Your preferred releases and builds:

Release 13.0

Builds 58.30 67.39

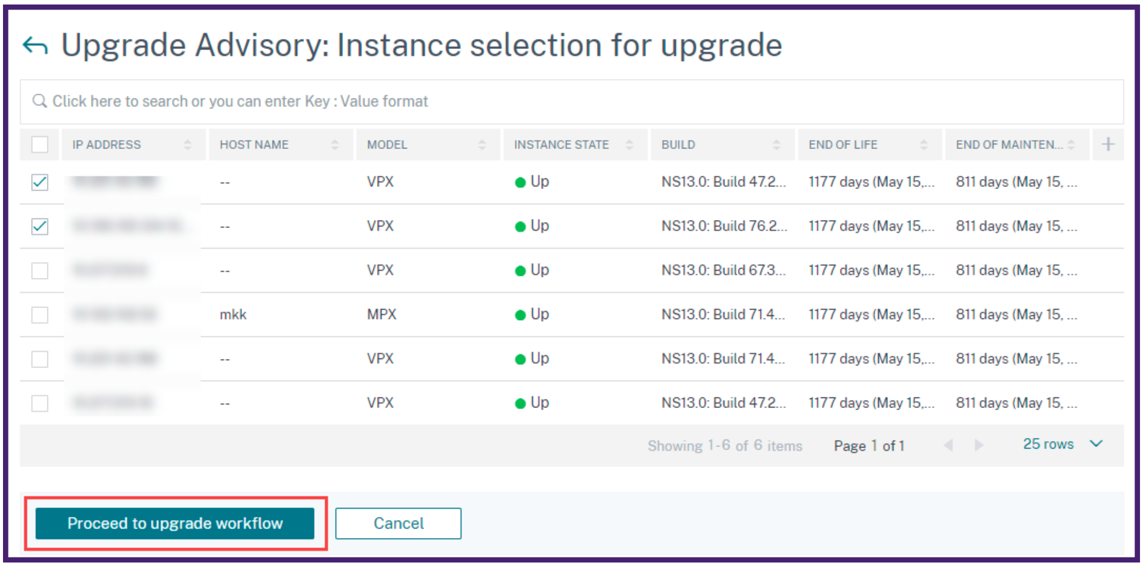
In this example, the preferred builds are `13.0-58.30` and `13.0-67.39`.

3. Click **Save**.

Upgrade ADC instances

In the **Upgrade Advisory** page, after your review, do the following steps to upgrade the required ADC instances:

1. Select the instance builds that you want to upgrade and click **Select instances to upgrade**.
2. Select the ADC instance that you want to upgrade and click **Proceed to upgrade workflow**.



Upgrade Advisory: Instance selection for upgrade

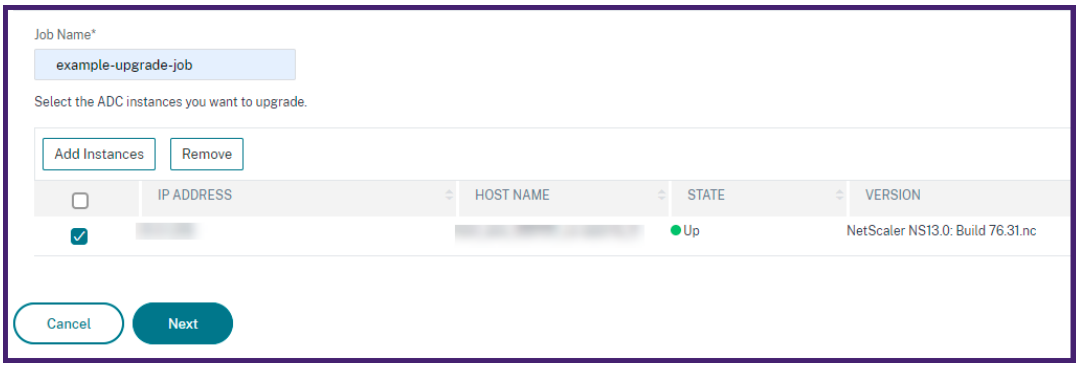
	IP ADDRESS	HOST NAME	MODEL	INSTANCE STATE	BUILD	END OF LIFE	END OF MAINTEN...
☑	[redacted]	--	VPX	● Up	NS13.0: Build 47.2...	1177 days (May 15,...	811 days (May 15, ...
☑	[redacted]	--	VPX	● Up	NS13.0: Build 76.2...	1177 days (May 15,...	811 days (May 15, ...
□	[redacted]	--	VPX	● Up	NS13.0: Build 67.3...	1177 days (May 15,...	811 days (May 15, ...
□	[redacted]	mkk	MPX	● Up	NS13.0: Build 71.4...	1177 days (May 15,...	811 days (May 15, ...
□	[redacted]	--	VPX	● Up	NS13.0: Build 71.4...	1177 days (May 15,...	811 days (May 15, ...
□	[redacted]	--	VPX	● Up	NS13.0: Build 47.2...	1177 days (May 15,...	811 days (May 15, ...

This workflow creates an upgrade job.

3. In the **Select Instance** tab,

   a) Specify a name to the upgrade job.

   b) (Optional) if you want to add other instances, click **Add Instances**.



Job Name*: example-upgrade-job

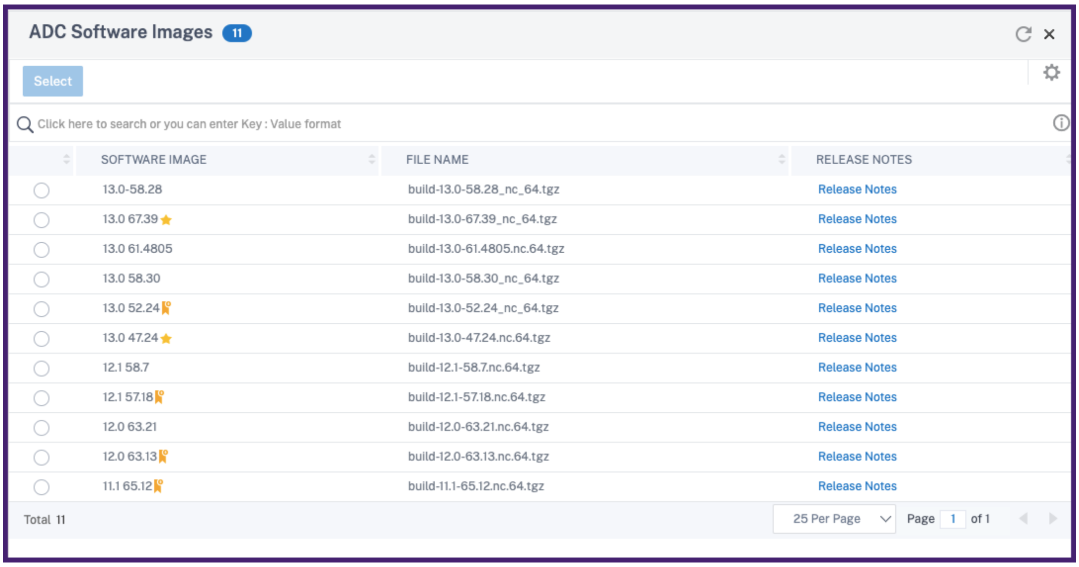
Select the ADC instances you want to upgrade.

□	IP ADDRESS	HOST NAME	STATE	VERSION
☑	[redacted]	[redacted]	● Up	NetScaler NS13.0: Build 76.31.nc

   c) Click **Next**.

4. In the **Select Image** tab, select an ADC image from the image library or local or appliance.

   - **Select from Image Library**: Select an ADC image from the list. This option lists all ADC images that are available in the Citrix Downloads website.



	SOFTWARE IMAGE	FILE NAME	RELEASE NOTES
○	13.0-58.28	build-13.0-58.28_nc_64.tgz	Release Notes
○	13.0 67.39 ★	build-13.0-67.39_nc_64.tgz	Release Notes
○	13.0 61.4805	build-13.0-61.4805.nc.64.tgz	Release Notes
○	13.0 58.30	build-13.0-58.30_nc_64.tgz	Release Notes
○	13.0 52.24 🔖	build-13.0-52.24_nc_64.tgz	Release Notes
○	13.0 47.24 ★	build-13.0-47.24.nc.64.tgz	Release Notes
○	12.1 58.7	build-12.1-58.7.nc.64.tgz	Release Notes
○	12.1 57.18 🔖	build-12.1-57.18.nc.64.tgz	Release Notes
○	12.0 63.21	build-12.0-63.21.nc.64.tgz	Release Notes
○	12.0 63.13 🔖	build-12.0-63.13.nc.64.tgz	Release Notes
○	11.1 65.12 🔖	build-11.1-65.12.nc.64.tgz	Release Notes

Total 11 | 25 Per Page | Page 1 of 1

The ADC software images display the preferred builds with the star icon. And, most downloaded builds with the bookmark icon.

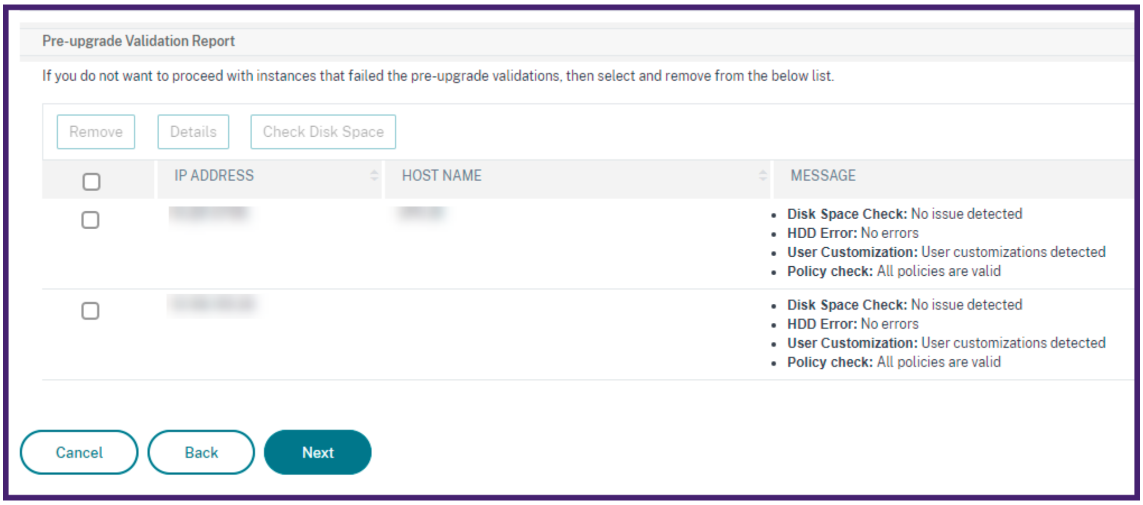
- **Select from local or appliance**: You can upload the image from your local computer or the ADC appliance. When you select ADC appliance, the Citrix Application Delivery and Management GUI displays the instance files that are present in `/var/mps/mps_images`. Select the image from the Citrix Application Delivery and Management GUI.

- **Skip image uploading to ADC if the selected image is already available** - This option checks whether the selected image is available in ADC. Upgrade job skips uploading a new image and uses the image available in ADC.

- **Clean software image from Citrix ADC on successful upgrade** - This option clears the uploaded image in the ADC instance after the instance upgrade.

Click **Next** to start the pre-upgrade validation on the selected instances.

5. The **Pre-upgrade validation** tab displays the failed instances. you can remove the failed instances and click **Next**.



Pre-upgrade Validation Report

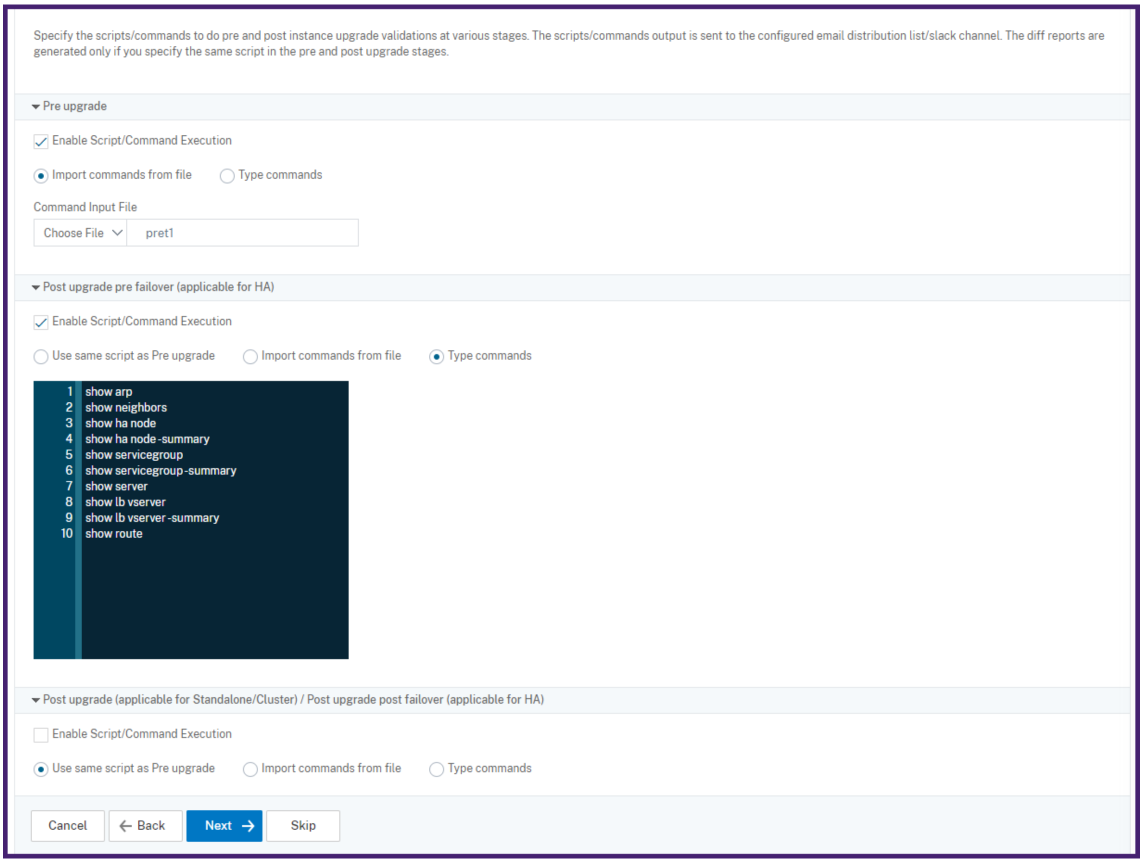
If you do not want to proceed with instances that failed the pre-upgrade validations, then select and remove from the below list.

☐	IP ADDRESS	HOST NAME	MESSAGE
☐	[redacted]	[redacted]	• **Disk Space Check:** No issue detected • **HDD Error:** No errors • **User Customization:** User customizations detected • **Policy check:** All policies are valid
☐	[redacted]		• **Disk Space Check:** No issue detected • **HDD Error:** No errors • **User Customization:** User customizations detected • **Policy check:** All policies are valid

- **Disk Space Check**: If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up ADC disk space.
- **Policy Check**: If Citrix Application Delivery and Management finds unsupported classic policies, you can remove such policies to create an upgrade job.

> **Note**
>
> If you specify cluster IP address, the Citrix Application Delivery and Management does pre-upgrade validation only on the specified instance not on the other cluster nodes.

6. Optional, in the **Custom scripts** tab, specify the scripts to run before and after an instance upgrade.



Specify the scripts/commands to do pre and post instance upgrade validations at various stages. The scripts/commands output is sent to the configured email distribution list/slack channel. The diff reports are generated only if you specify the same script in the pre and post upgrade stages.

▾ Pre upgrade

☑ Enable Script/Command Execution

● Import commands from file ○ Type commands

Command Input File: Choose File — pret1

▾ Post upgrade pre failover (applicable for HA)

☑ Enable Script/Command Execution

○ Use same script as Pre upgrade ○ Import commands from file ● Type commands

```
show arp
show neighbors
show ha node
show ha node -summary
show servicegroup
show servicegroup -summary
show server
show lb vserver
show lb vserver -summary
show route
```

▾ Post upgrade (applicable for Standalone/Cluster) / Post upgrade post failover (applicable for HA)

□ Enable Script/Command Execution

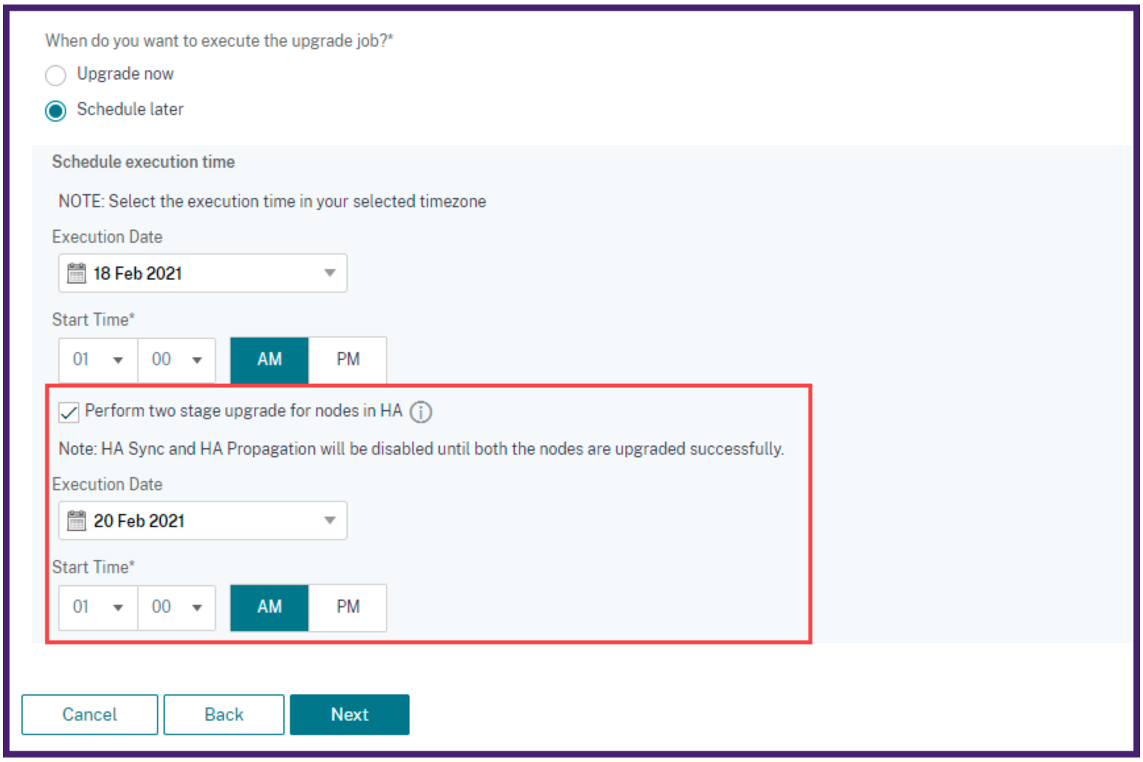
● Use same script as Pre upgrade ○ Import commands from file ○ Type commands

For more information, see Use custom scripts.

7. In the **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 high-availability pair in two stages, select Perform two stage upgrade for nodes in HA.



When do you want to execute the upgrade job?*

○ Upgrade now

● Schedule later

Schedule execution time

NOTE: Select the execution time in your selected timezone

Execution Date: 18 Feb 2021

Start Time*: 01 : 00 AM

☑ Perform two stage upgrade for nodes in HA

Note: HA Sync and HA Propagation will be disabled until both the nodes are upgraded successfully.

Execution Date: 20 Feb 2021

Start Time*: 01 : 00 AM

For more information, see Upgrade ADC high-availability pair.

8. In the **Create Job** tab, specify the following details:

   If you schedule the upgrade job, you can 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.

For more information on the other options, see ADC upgrade options.

Security Advisory

October 30, 2021

A safe, secure, and resilient infrastructure is the lifeline of any organization. So, the organization must track new Common Vulnerabilities and Exposures (CVEs), assess the impact of CVEs on their infrastructure. Understand the mitigation and remediation. Also, the organization must plan for mitigation and remediation to resolve the vulnerabilities.

Citrix Application Delivery and Management security advisory highlights Citrix CVEs putting your ADC instances at risk and recommends mitigations and remediations. You can review the recommendations and take appropriate actions, by using Citrix Application Delivery and Management to apply the mitigations and remediations.

Security advisory features

The following security advisory features help you protect your infrastructure.

- Scan: includes default system scan and on-demand scan.
  - System scan: scans all managed instances by default once a week. Citrix Application Delivery and Management decides the date and time of system scans, and you cannot change them.
  - On-demand scan: enables you to manually scan the instances when required. If the time elapsed after the last system scan is significant, you can run an on-demand scan to assess the current security posture. Or scan after a remediation or mitigation has been applied, to assess the revised posture.
- CVE impact analysis: shows the results of all CVEs impacting your infrastructure and all the ADC instances getting impacted and suggests remediation and mitigation. Use this information to apply mitigation and remediation to fix security risks.
- CVE reports: stores copies of the last five scans. You can download these reports in CSV format and analyze them.
- CVE repository: Gives a detailed view of all the ADC related CVEs that Citrix has announced since Dec 2019, that might impact your ADC infrastructure. You can use this view to understand the CVEs in the security advisory scope and to learn more about the CVE.

Points to note

Keep the following points in mind while using security advisory:

- Instances supported for CVE detection: all ADC (SDX, MPX, VPX, CPX, BLX) and Gateway.
- CVEs supported: all CVEs after Dec 2019.
- Scope of ADC, Gateway releases: the feature is limited to main builds. security advisory does not include any special build in its scope.
  - Security advisory is supported in ADC instances running versions higher than 10.5 and not in instances running 10.5 and lower versions.
  - Security advisory is not supported in Admin partition, SD-WAN devices, HAProxy, or HAProxy host devices.

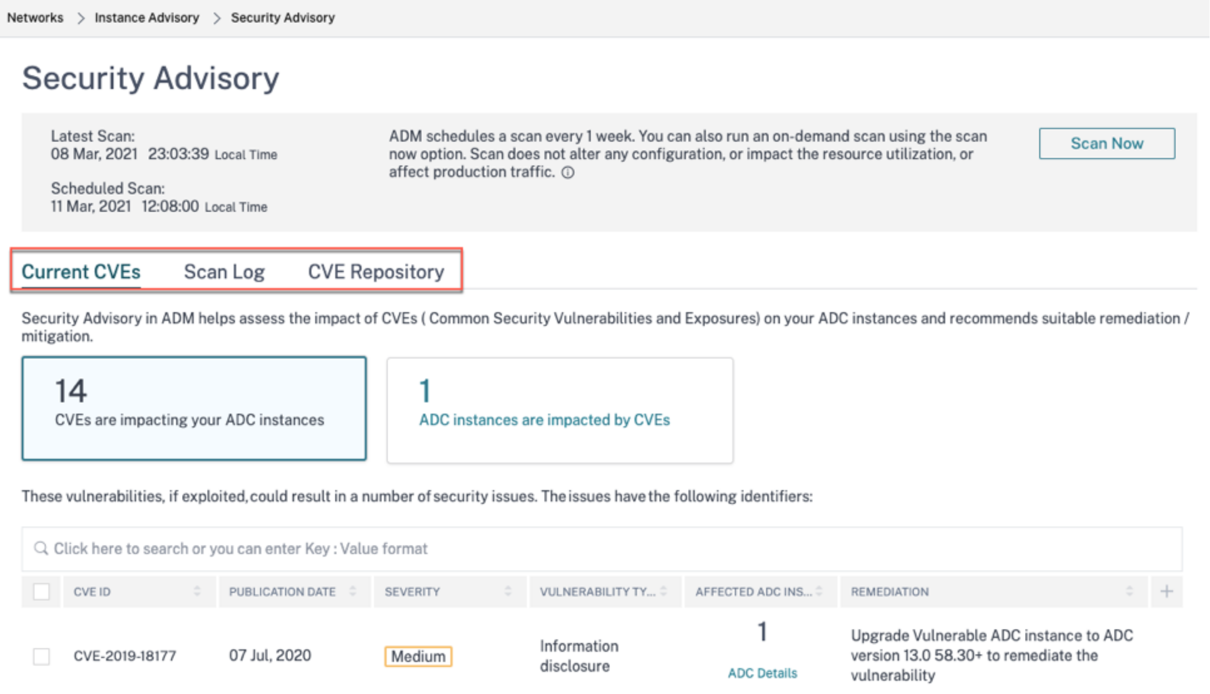
- Types of scan:
  - **Version scan**: This scan needs Citrix Application Delivery and Management to compare the version of an ADC instance with the versions and builds on which the fix is available. This version comparison helps Citrix Application Delivery and Management security advisory identify whether the ADC is vulnerable to the CVE. For example, if a CVE is fixed on ADC release and build xx.yy, security advisory considers all the ADC instances on builds lesser than xx.yy as vulnerable. Version scan is supported today in security advisory.
  - **Config scan**: This scan needs Citrix Application Delivery and Management to match a pattern specific to the CVE scan with ADC config file (nsconf). If the specific config pattern is present in the ADC ns.conf file, the instance is considered vulnerable for that CVE. This scan is typically used with version scan.
Config scan is supported today in security advisory.
  - **Custom scan**: This scan needs Citrix Application Delivery and Management to connect with the managed ADC instance, push a script to it, and run the script. The script output helps Citrix Application Delivery and Management identify whether the ADC is vulnerable to the CVE. Examples include specific shell command output, specific CLI command output, certain logs, and existence or content of certain directories or files. Security Advisory also uses custom scans for multiple config patterns matches, if config scan cannot help with the same. For CVEs that require custom scans, the script runs every time your scheduled or on-demand scan runs. Learn more about the data collected and options for specific custom scans in the Security Advisory documentation for that CVE.
- Scans do not impact production traffic on ADC and do not alter any ADC configuration on ADC.

How to use the security advisory dashboard

To access the **Security Advisory** dashboard, from the Citrix Application Delivery and Management GUI, navigate to **Infrastructure > Instance Advisory > Security Advisory**. The dashboard shows the vulnerability status of all the ADC instances that you manage through Citrix Application Delivery and Management. The instances are scanned once a week; however, you can scan them anytime by clicking **Scan Now**.

The dashboard includes three tabs:

- Current CVEs
- Scan Log
- CVE Repository



Networks > Instance Advisory > Security Advisory

Security Advisory

Latest Scan:
08 Mar, 2021 23:03:39 Local Time

Scheduled Scan:
11 Mar, 2021 12:08:00 Local Time

ADM schedules a scan every 1 week. You can also run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

14 CVEs are impacting your ADC instances

1 ADC instances are impacted by CVEs

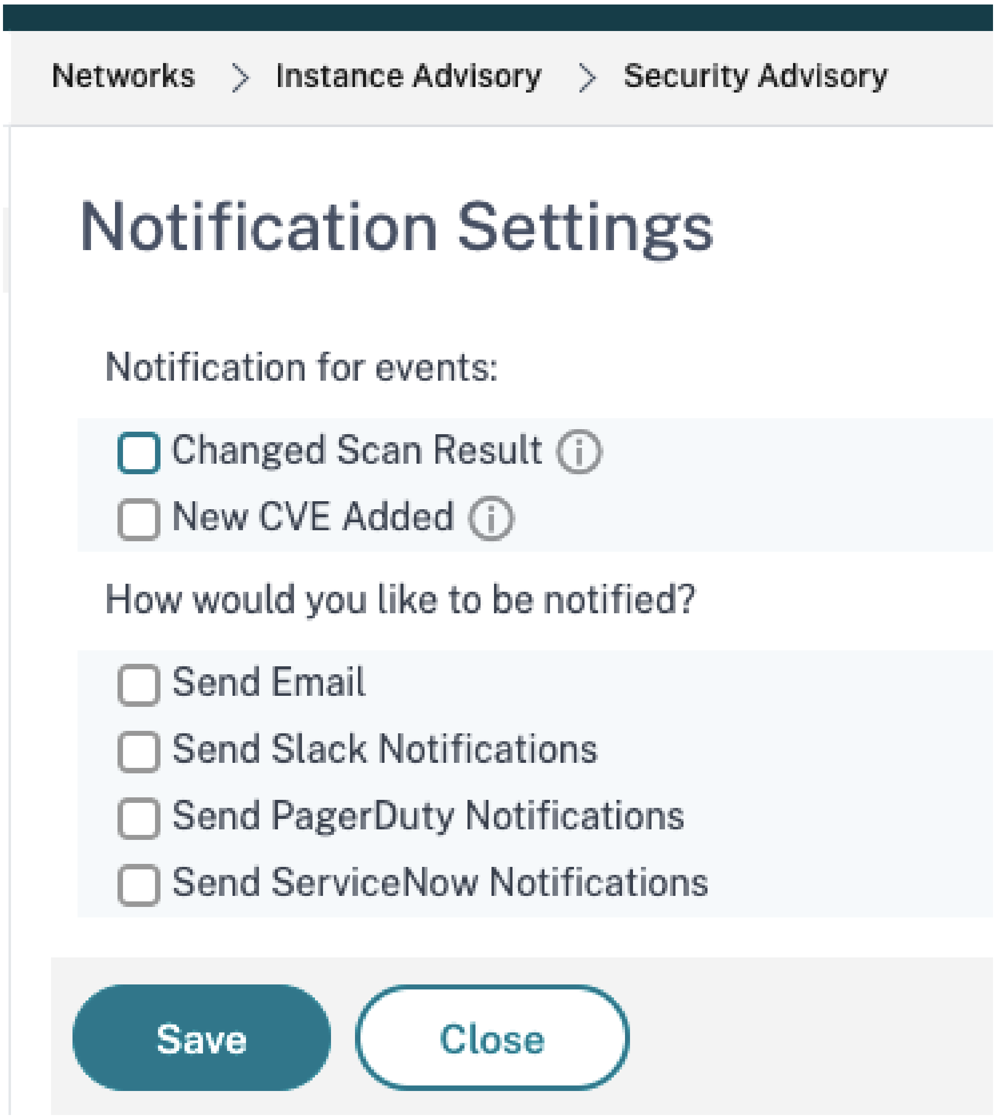
These vulnerabilities, if exploited, could result in a number of security issues. The issues have the following identifiers:

	CVE ID	PUBLICATION DATE	SEVERITY	VULNERABILITY TY...	AFFECTED ADC INS...	REMEDIATION
□	CVE-2019-18177	07 Jul, 2020	Medium	Information disclosure	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 58.30+ to remediate the vulnerability

> **Important**
>
> In the **Security Advisory** GUI or report, all CVEs might not appear, and you might only see one CVE. As a workaround, click **Scan Now** to run an on-demand scan. After the scan is complete, all the CVEs in scope (approximately 15) appear in the UI or report.

On the upper-right corner of the dashboard is the settings icon, which allows you to enable and disable notifications. You can receive the following notifications for Citrix Application Delivery and Management security advisory activities:

- Email, Slack, PagerDuty, and ServiceNow notifications for scan result changes and new CVEs that are added in security advisory repository
- Cloud notification for scan result changes



Notification Settings

Notification for events:

□ Changed Scan Result ⓘ
□ New CVE Added ⓘ

How would you like to be notified?

□ Send Email
□ Send Slack Notifications
□ Send PagerDuty Notifications
□ Send ServiceNow Notifications

Current CVEs

This tab shows the number of CVEs impacting your instances and also the instances that are impacted by CVEs. The tabs are not sequential, and as an admin, you can switch between these tabs depending on your use case.

The table showing the number of CVEs impacting the ADC instances has the following details.

CVE ID: the ID of the CVE impacting the instances.

Publication date: the date the security bulletin was released for that CVE.

Severity score: the severity type (high/medium/critical) and score. To see the score, hover over the severity type.

Vulnerability type: the type of vulnerability for this CVE.

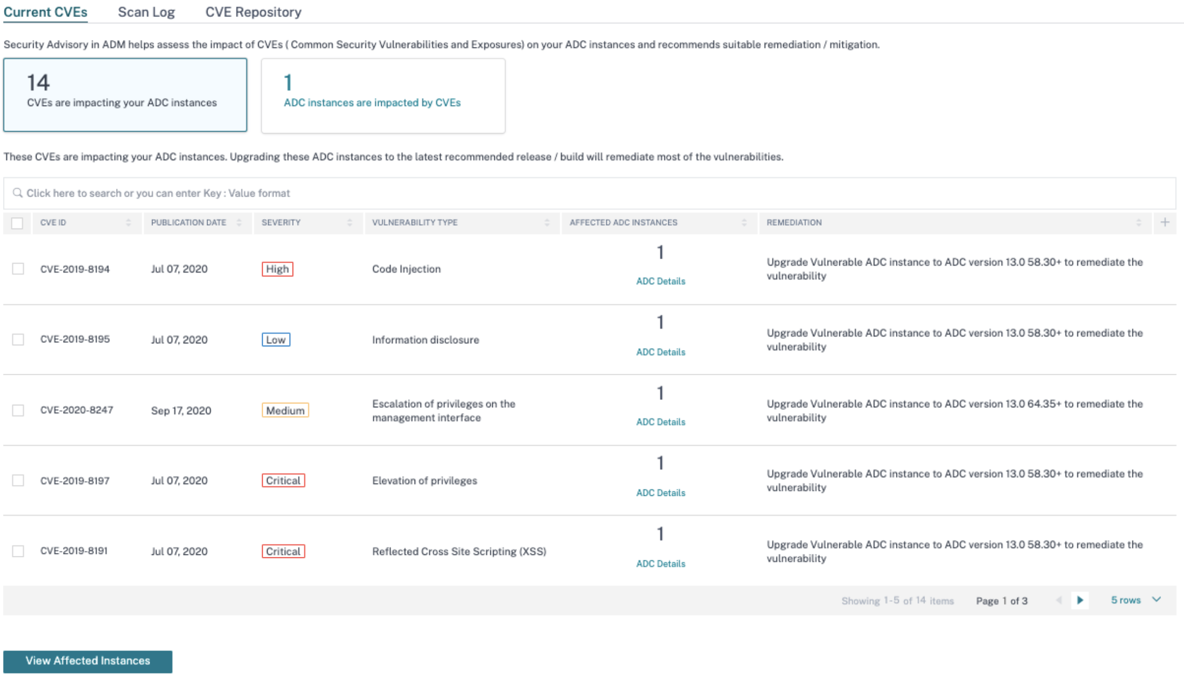
Affected ADC instances: the instance count that the CVE ID is impacting. On hover over, the list of ADC instances appears.

Remediation: the available remediations, which are upgrading the instance (usually) or applying configuration packs.

The same instance can be impacted by multiple CVEs. This table helps you see how many instances one particular CVE or multiple selected CVEs are impacting. To check the IP address of the impacted instance, hover over ADC Details under **Affected ADC Instances**. To check the details of the impacted instance, click **View Affected Instances** at the bottom of the table.
You can also add or remove columns in the table by clicking the plus sign.

Figure. Current CVEs

In this screen the number of CVEs impacting your instances is 14 CVEs and the instances that are impacted by these CVEs is one.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

14
CVEs are impacting your ADC instances

1
ADC instances are impacted by CVEs

These CVEs are impacting your ADC instances. Upgrading these ADC instances to the latest recommended release / build will remediate most of the vulnerabilities.

Click here to search or you can enter Key : Value format

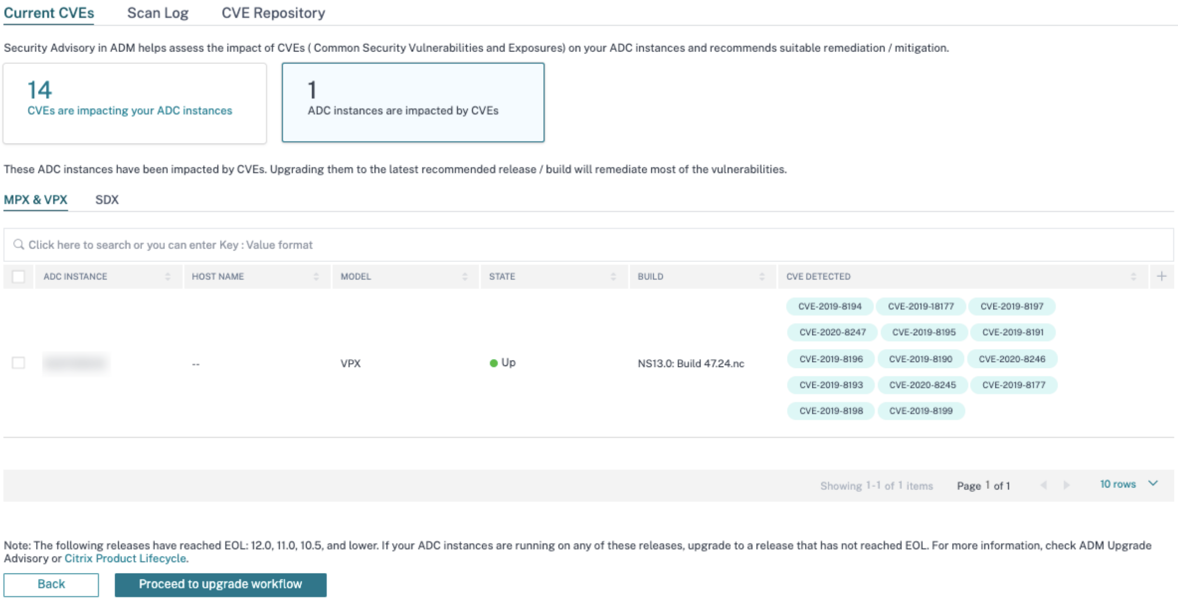
□	CVE ID	PUBLICATION DATE	SEVERITY	VULNERABILITY TYPE	AFFECTED ADC INSTANCES	REMEDIATION
□	CVE-2019-8194	Jul 07, 2020	High	Code Injection	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 58.30+ to remediate the vulnerability
□	CVE-2019-8195	Jul 07, 2020	Low	Information disclosure	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 58.30+ to remediate the vulnerability
□	CVE-2020-8247	Sep 17, 2020	Medium	Escalation of privileges on the management interface	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 64.35+ to remediate the vulnerability
□	CVE-2019-8197	Jul 07, 2020	Critical	Elevation of privileges	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 58.30+ to remediate the vulnerability
□	CVE-2019-8191	Jul 07, 2020	Critical	Reflected Cross Site Scripting (XSS)	1 ADC Details	Upgrade Vulnerable ADC instance to ADC version 13.0 58.30+ to remediate the vulnerability

Showing 1-5 of 14 items Page 1 of 3 5 rows

The `<number of>` **ADC instances are impacted by CVEs** tab shows you all the affected Citrix Application Delivery and Management ADC instances. The table shows the following details:

- ADC IP address
- Host name
- ADC model number
- State of the ADC
- Software version and build
- List of CVEs impacting the ADC.

In the following screen capture, one ADC instance is impacted. You add or remove any of these columns according to your need, by clicking the + sign.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

14
CVEs are impacting your ADC instances

1
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED	+
□	[redacted]	--	VPX	● Up	NS13.0: Build 47.24.nc	CVE-2019-8194 CVE-2019-18177 CVE-2019-8197 CVE-2020-8247 CVE-2019-8195 CVE-2019-8191 CVE-2019-8196 CVE-2019-8190 CVE-2020-8246 CVE-2019-8193 CVE-2020-8245 CVE-2019-8177 CVE-2019-8198 CVE-2019-8199	

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

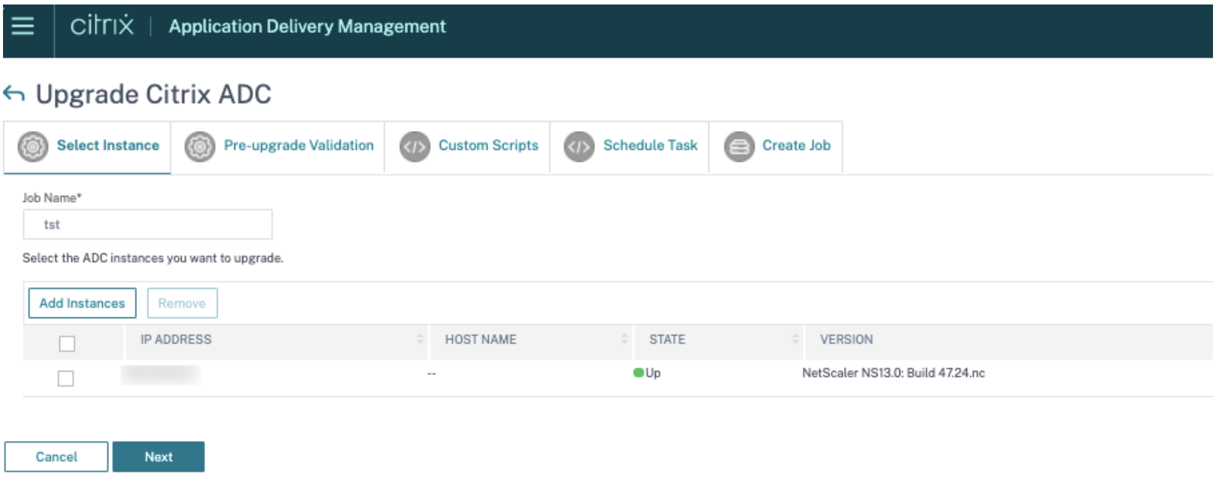
To fix the vulnerability issue, select the ADC instance and apply the recommended remediation. While most of the CVEs need upgrade as a remediation, CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920 need upgrade and another step as remediation. For CVE-2020-8300 remediation, see Remediate vulnerabilities for CVE-2020-8300. For CVE-2021-22927 and CVE-2021-22920, see Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920.

- **Upgrade**: You can upgrade the vulnerable ADC instances to a release and build that has the fix. This detail can be seen in the remediation column. To upgrade, select the instance and then click **Proceed to upgrade workflow**. In the upgrade workflow, the vulnerable ADC is auto-populated as the target ADC.

> **Note**
>
> The releases 12.0, 11,0, 10.5 and lower are already end of life (EOL). If your ADC instances are running on any of these releases, upgrade to a supported release.

The upgrade workflow starts. For more information on how to use Citrix Application Delivery and Management to upgrade ADC instances, see Create an ADC upgrade job.

> **Note**
>
> The release and build to which you want to upgrade is at your discretion. See the advice under the remediation column to know which release and builds have the security fix. And accordingly select a supported release and build, which has not reached end of life yet.



Job Name*

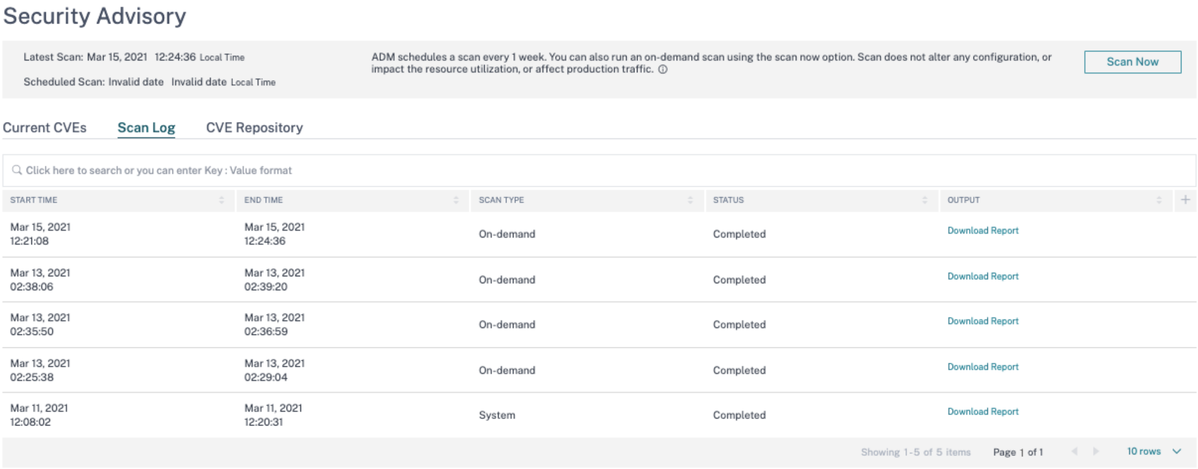
tst

Select the ADC instances you want to upgrade.

	IP ADDRESS	HOST NAME	STATE	VERSION
□	[redacted]	--	● Up	NetScaler NS13.0: Build 47.24.nc

Scan Log

The tab shows reports of the last five scans, which include both default system scans and on-demand user-initiated scans. You can download the report of each scan in CSV format. If an on-demand scan is in progress, you can see the completion status here. If any scan has failed, the status indicates that.



Latest Scan: Mar 15, 2021 12:24:36 Local Time

Scheduled Scan: Invalid date Invalid date Local Time

ADM schedules a scan every 1 week. You can also run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

START TIME	END TIME	SCAN TYPE	STATUS	OUTPUT
Mar 15, 2021 12:21:08	Mar 15, 2021 12:24:36	On-demand	Completed	Download Report
Mar 13, 2021 02:38:06	Mar 13, 2021 02:39:20	On-demand	Completed	Download Report
Mar 13, 2021 02:35:50	Mar 13, 2021 02:36:59	On-demand	Completed	Download Report
Mar 13, 2021 02:25:38	Mar 13, 2021 02:29:04	On-demand	Completed	Download Report
Mar 11, 2021 12:08:02	Mar 11, 2021 12:20:31	System	Completed	Download Report

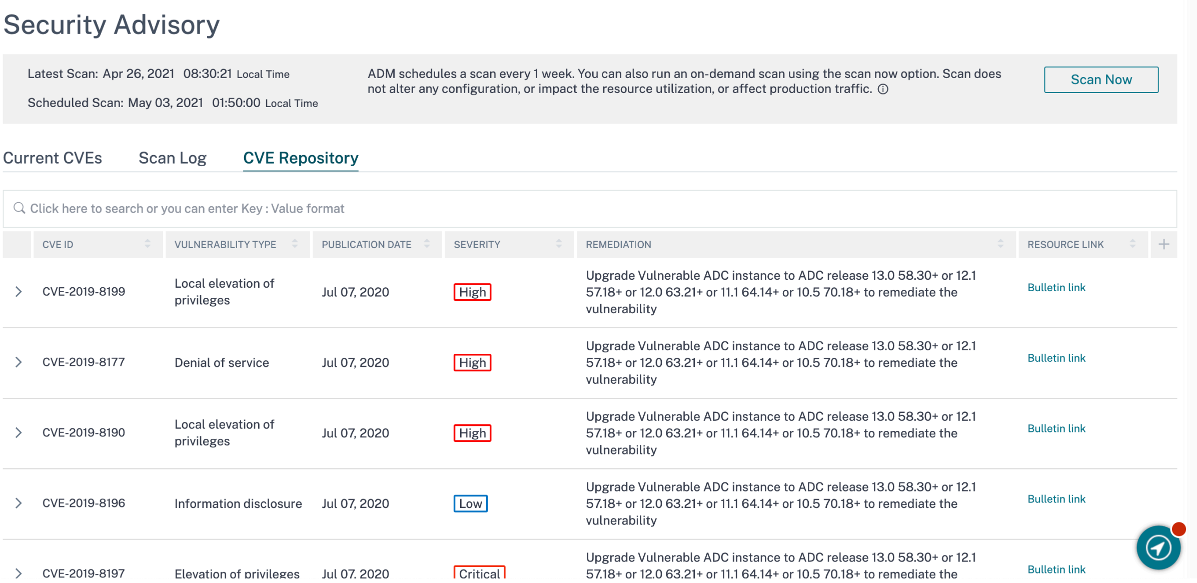
Showing 1-5 of 5 items Page 1 of 1 10 rows

CVE Repository

This tab includes the latest information of all CVEs from December 2019, along with the following details:

- CVE IDs
- Vulnerability type
- Publication date

- Severity level
- Remediation
- Links to security bulletins



Security Advisory

Latest Scan: Apr 26, 2021 08:30:21 Local Time

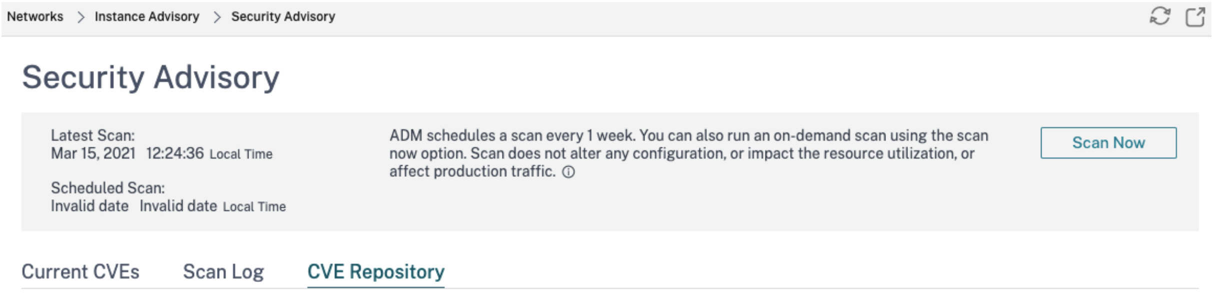
Scheduled Scan: May 03, 2021 01:50:00 Local Time

ADM schedules a scan every 1 week. You can also run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic. ⓘ

	CVE ID	VULNERABILITY TYPE	PUBLICATION DATE	SEVERITY	REMEDIATION	RESOURCE LINK
›	CVE-2019-8199	Local elevation of privileges	Jul 07, 2020	High	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ or 12.0 63.21+ or 11.1 64.14+ or 10.5 70.18+ to remediate the vulnerability	Bulletin link
›	CVE-2019-8177	Denial of service	Jul 07, 2020	High	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ or 12.0 63.21+ or 11.1 64.14+ or 10.5 70.18+ to remediate the vulnerability	Bulletin link
›	CVE-2019-8190	Local elevation of privileges	Jul 07, 2020	High	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ or 12.0 63.21+ or 11.1 64.14+ or 10.5 70.18+ to remediate the vulnerability	Bulletin link
›	CVE-2019-8196	Information disclosure	Jul 07, 2020	Low	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ or 12.0 63.21+ or 11.1 64.14+ or 10.5 70.18+ to remediate the vulnerability	Bulletin link
›	CVE-2019-8197	Elevation of privileges	Jul 07, 2020	Critical	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ or 12.0 63.21+ or 11.1 64.14+ or 10.5 70.18+ to remediate the	Bulletin link

Scan Now

The security advisory shows when the instances were last scanned and when the next schedule is due. You can also scan the instances anytime, according to your need. Click **Scan Now** to get the latest security report of your instance. Citrix Application Delivery and Management takes a few minutes to complete the scan.



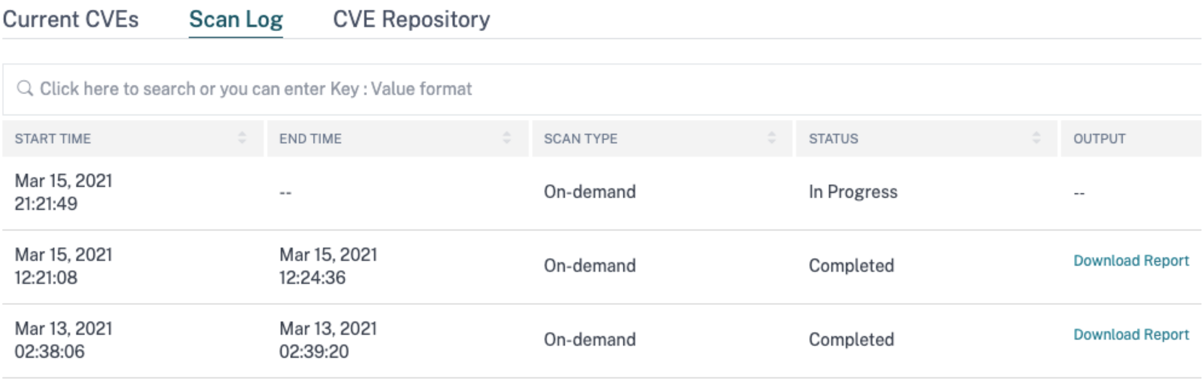
Security Advisory

Latest Scan:
Mar 15, 2021 12:24:36 Local Time

Scheduled Scan:
Invalid date Invalid date Local Time

ADM schedules a scan every 1 week. You can also run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic. ⓘ

Once scanning is complete, the revised security details appears in the security advisory GUI. You can also find the report under **Scan Log**, which you can also download.

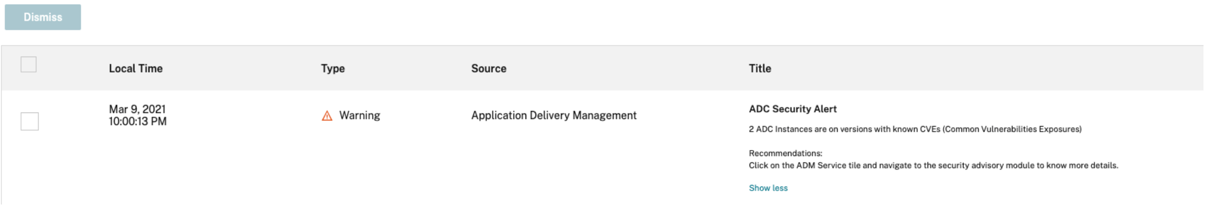


START TIME	END TIME	SCAN TYPE	STATUS	OUTPUT
Mar 15, 2021 21:21:49	--	On-demand	In Progress	--
Mar 15, 2021 12:21:08	Mar 15, 2021 12:24:36	On-demand	Completed	Download Report
Mar 13, 2021 02:38:06	Mar 13, 2021 02:39:20	On-demand	Completed	Download Report

> **Note**
>
> Scan Log shows the logs of only the last five scans, which can be both scheduled or on demand.

Notification

As an admin, you receive Citrix Cloud notifications, which tell how many ADC instances are vulnerable. To see the notifications, click the bell icon on the upper-right corner of the Citrix Application Delivery and Management GUI.

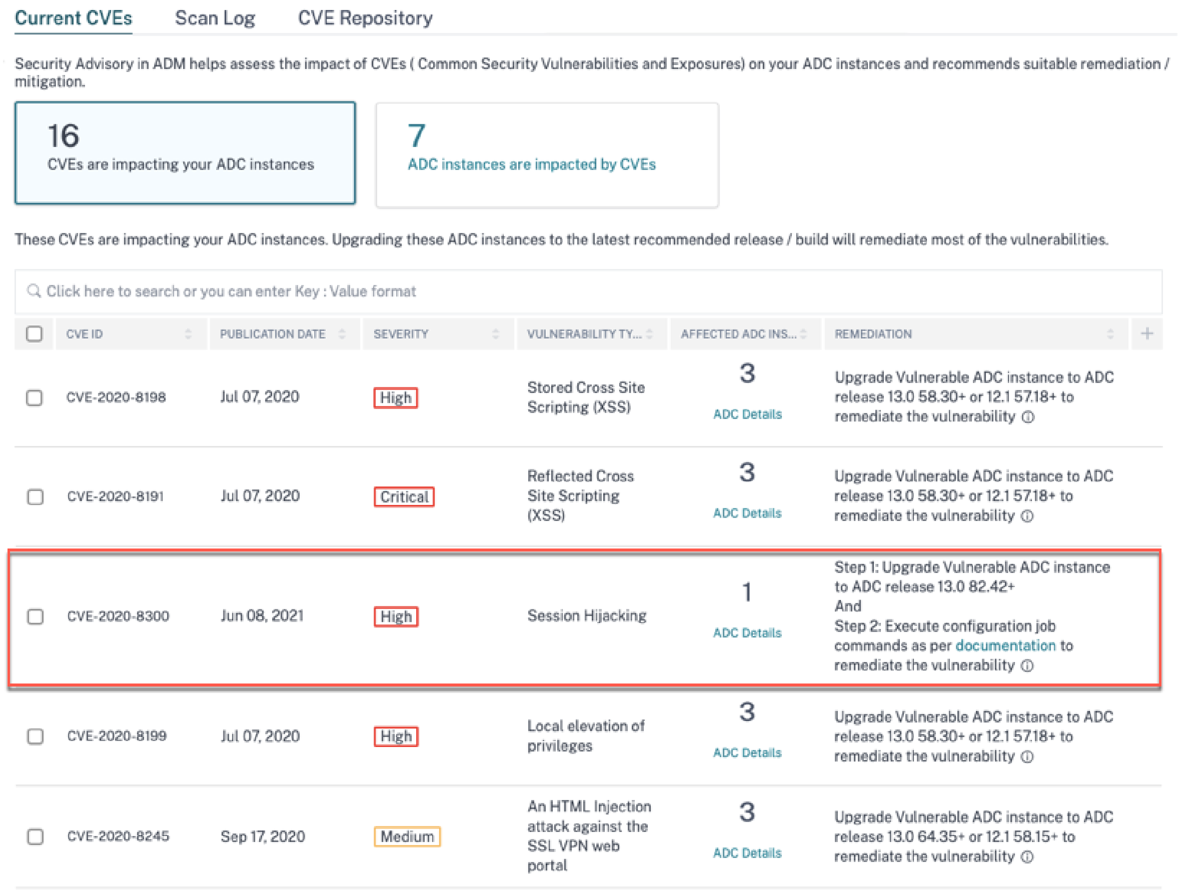


□	Local Time	Type	Source	Title
□	Mar 9, 2021 10:00:13 PM	⚠ Warning	Application Delivery Management	ADC Security Alert 2 ADC Instances are on versions with known CVEs (Common Vulnerabilities Exposures) Recommendations: Click on the ADM Service tile and navigate to the security advisory module to know more details. Show less

Remediate vulnerabilities for CVE-2020-8300

September 25, 2021

In the Citrix Application Delivery and Management security advisory dashboard, under **Current CVEs > <`number of`> ADC instances are impacted by CVEs**, you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2020-8300 impacted instances, select **CVE-2020-8300** and click View **Affected Instances**.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

16
CVEs are impacting your ADC instances

7
ADC instances are impacted by CVEs

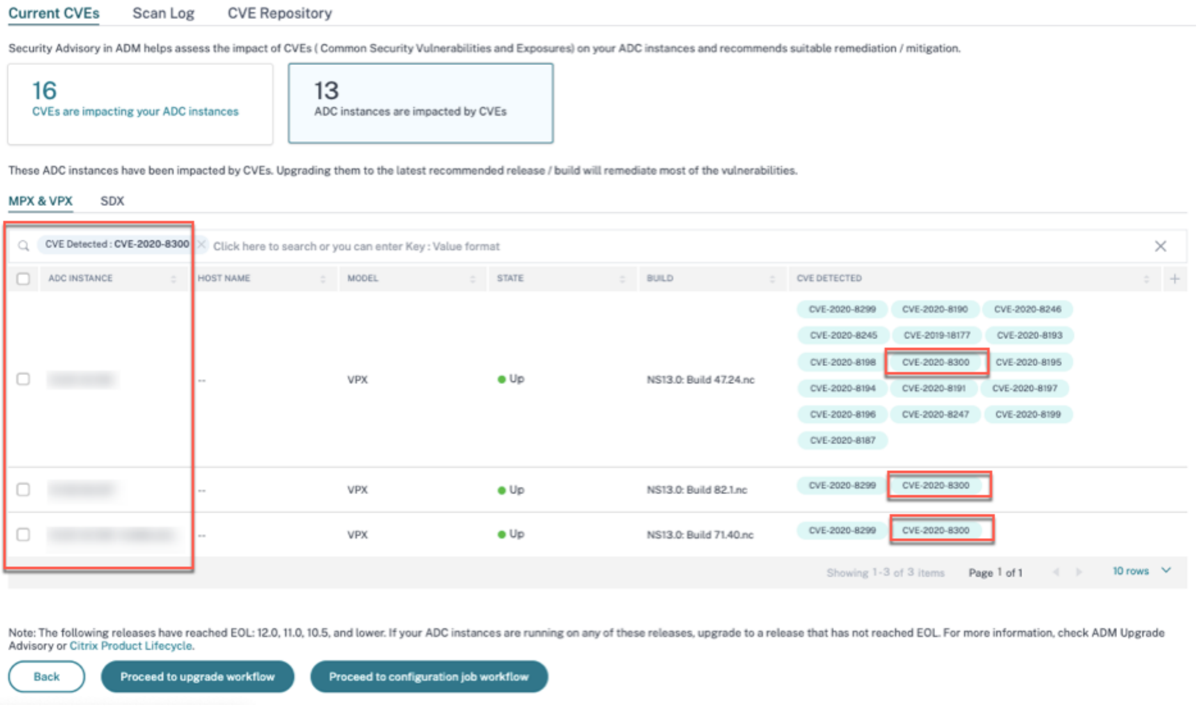
These CVEs are impacting your ADC instances. Upgrading these ADC instances to the latest recommended release / build will remediate most of the vulnerabilities.

Click here to search or you can enter Key : Value format

□	CVE ID	PUBLICATION DATE	SEVERITY	VULNERABILITY TY...	AFFECTED ADC INS...	REMEDIATION
□	CVE-2020-8198	Jul 07, 2020	High	Stored Cross Site Scripting (XSS)	3 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ to remediate the vulnerability ⓘ
□	CVE-2020-8191	Jul 07, 2020	Critical	Reflected Cross Site Scripting (XSS)	3 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ to remediate the vulnerability ⓘ
□	CVE-2020-8300	Jun 08, 2021	High	Session Hijacking	1 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.42+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability ⓘ
□	CVE-2020-8199	Jul 07, 2020	High	Local elevation of privileges	3 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ to remediate the vulnerability ⓘ
□	CVE-2020-8245	Sep 17, 2020	Medium	An HTML Injection attack against the SSL VPN web portal	3 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 64.35+ or 12.1 58.15+ to remediate the vulnerability ⓘ

> **Note**
>
> For more information about the security advisory dashboard see, Security Advisory.

The <`number of`> **ADC instances impacted by CVEs** window appears. Here you see the count and details of the ADC instances impacted by CVE-2020-8300.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

16
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

CVE Detected : CVE-2020-8300 Click here to search or you can enter Key : Value format

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
□	[redacted]	--	VPX	● Up	NS13.0: Build 47.24.nc	CVE-2020-8299 CVE-2020-8190 CVE-2020-8246 CVE-2020-8245 CVE-2019-18177 CVE-2020-8193 CVE-2020-8198 CVE-2020-8300 CVE-2020-8195 CVE-2020-8194 CVE-2020-8191 CVE-2020-8197 CVE-2020-8196 CVE-2020-8247 CVE-2020-8199 CVE-2020-8187
□	[redacted]	--	VPX	● Up	NS13.0: Build 82.1.nc	CVE-2020-8299 CVE-2020-8300
□	[redacted]	--	VPX	● Up	NS13.0: Build 71.40.nc	CVE-2020-8299 CVE-2020-8300

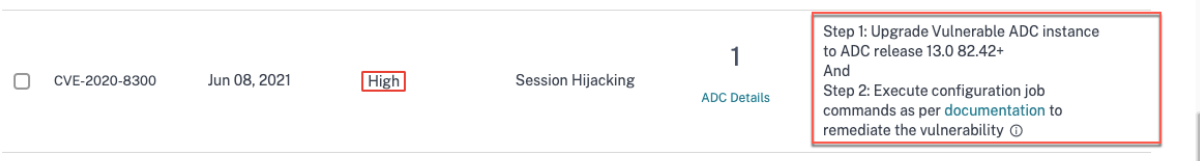
Showing 1-3 of 3 items Page 1 of 1 10 rows

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back
Proceed to upgrade workflow
Proceed to configuration job workflow

Remediate CVE-2020-8300

For CVE-2020-8300-impacted ADC instances, the remediation is a two-step process. In the GUI, under **Current CVEs > ADC instances are impacted by CVEs**, you can see step 1 and 2.

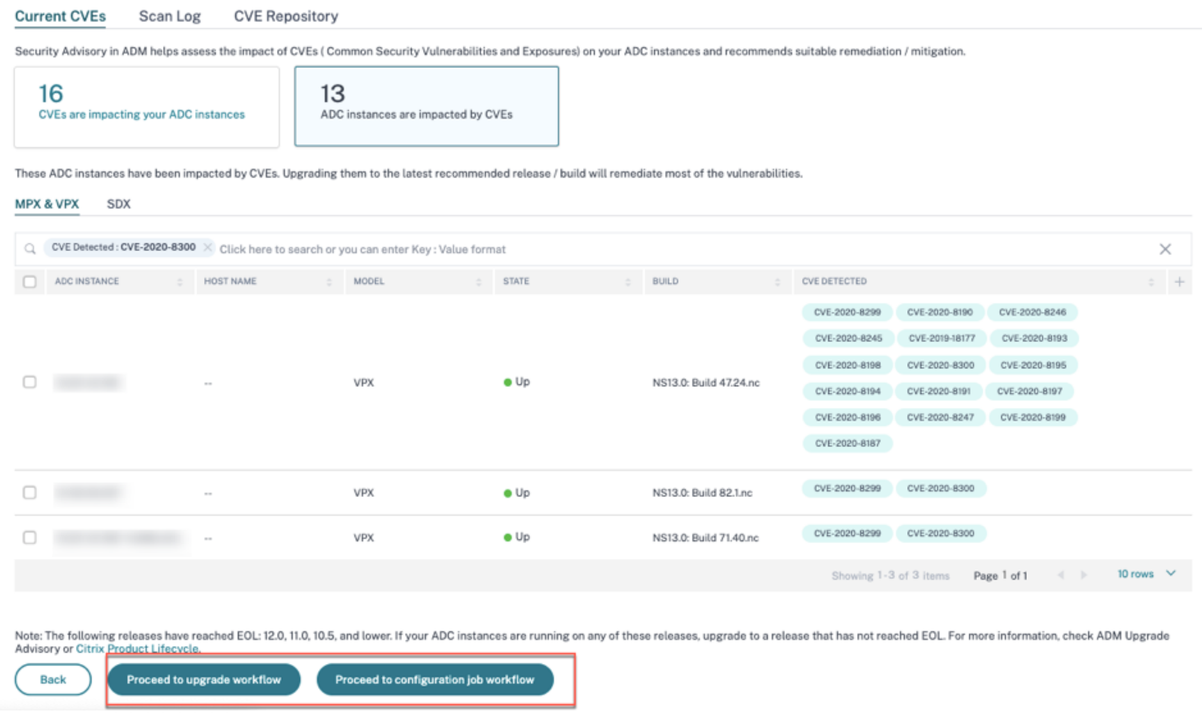


□	CVE-2020-8300	Jun 08, 2021	High	Session Hijacking	1 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.42+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability ⓘ

The two steps include:

1. Upgrading the vulnerable ADC instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs. Follow this step for each vulnerable ADC one at a time and include all SAML actions and SAML profiles for that ADC.

Under **Current CVEs> ADC instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.



Current CVEs | Scan Log | CVE Repository

Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

16
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

MPX & VPX | SDX

CVE Detected : CVE-2020-8300 ✕ Click here to search or you can enter Key : Value format

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
□	[redacted]	--	VPX	● Up	NS13.0: Build 47.24.nc	CVE-2020-8299 CVE-2020-8190 CVE-2020-8246 CVE-2020-8245 CVE-2019-18177 CVE-2020-8193 CVE-2020-8198 CVE-2020-8300 CVE-2020-8195 CVE-2020-8194 CVE-2020-8191 CVE-2020-8197 CVE-2020-8196 CVE-2020-8247 CVE-2020-8199 CVE-2020-8187
□	[redacted]	--	VPX	● Up	NS13.0: Build 82.1.nc	CVE-2020-8299 CVE-2020-8300
□	[redacted]	--	VPX	● Up	NS13.0: Build 71.40.nc	CVE-2020-8299 CVE-2020-8300

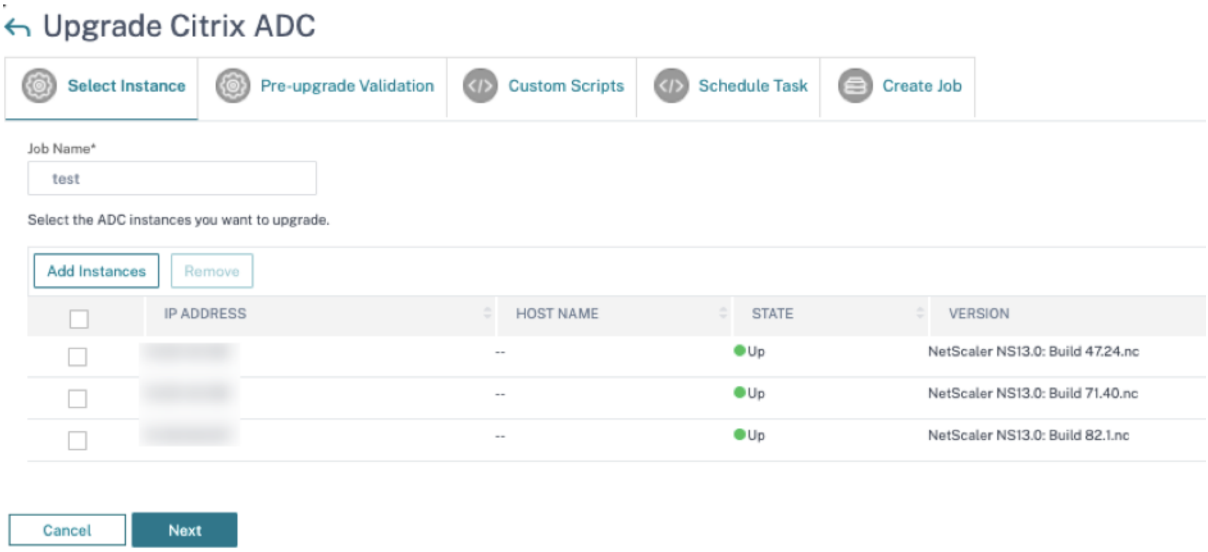
Showing 1-3 of 3 items Page 1 of 1 10 rows

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back
Proceed to upgrade workflow
Proceed to configuration job workflow

Step 1: Upgrade the vulnerable ADC instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable ADC instances already populated.



Upgrade Citrix ADC

Job Name*: test

Select the ADC instances you want to upgrade.

□	IP ADDRESS	HOST NAME	STATE	VERSION
□	[redacted]	--	● Up	NetScaler NS13.0: Build 47.24.nc
□	[redacted]	--	● Up	NetScaler NS13.0: Build 71.40.nc
□	[redacted]	--	● Up	NetScaler NS13.0: Build 82.1.nc

For more information on how to use Citrix Application Delivery and Management to upgrade ADC instances, see Create an ADC upgrade job.

> **Note**
>
> This step can be done at once for all the vulnerable ADC instances.

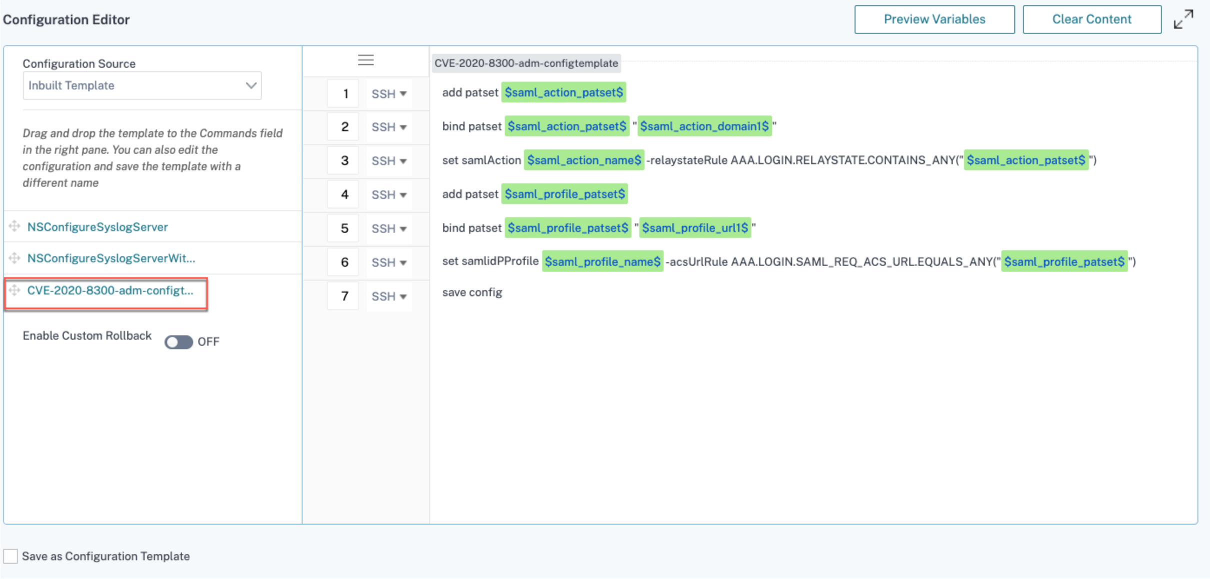
Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **<`number of`> ADC instances impacted by CVEs** window, select one instance impacted by CVE-2020-8300 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration template auto-populates under **Select configuration**.



Configuration Editor
Preview Variables
Clear Content
Configuration Source
Inbuilt Template
Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name
NSConfigureSyslogServer
NSConfigureSyslogServerWit...
CVE-2020-8300-adm-configt...
Enable Custom Rollback
OFF
SSH
CVE-2020-8300-adm-configtemplate
Save as Configuration Template

```
add patset $saml_action_patset$
bind patset $saml_action_patset$ " $saml_action_domain1$ "
set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY(" $saml_action_patset$ ")
add patset $saml_profile_patset$
bind patset $saml_profile_patset$ " $saml_profile_url1$ "
set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY(" $saml_profile_patset$ ")
save config
```

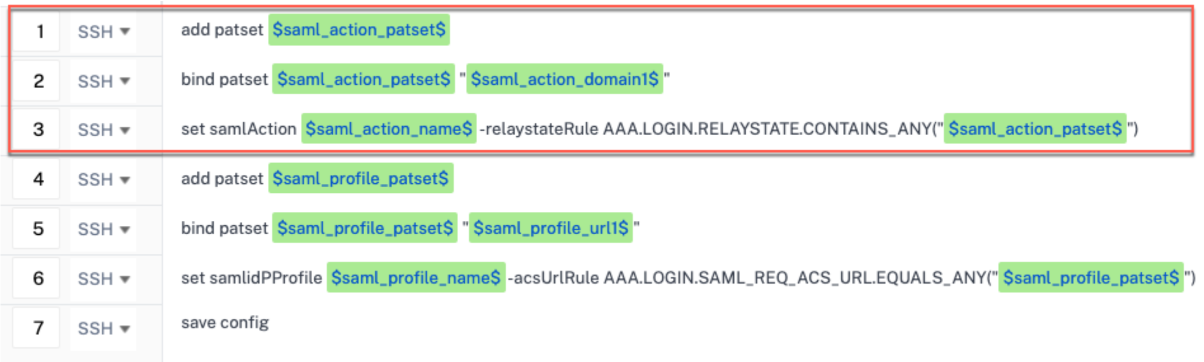
Run a separate configuration job for each impacted ADC instance, one at a time, and include all SAML actions and SAML profiles for that ADC. For example, if you have two vulnerable ADC instances each having two SAML actions and two SAML profiles, you must run this configuration job two times. One time per ADC covering all its SAML actions and SAML profiles.

ADC 1	ADC2
Job 1: two SAML actions +two SAML profiles	Job 2: two SAML actions +two SAML profiles

Give the job a name and customize the template for the following specifications. The built-in configuration template is only an outline or base template. Customize the template based on your deployment for the following requirements:

a. **SAML actions and their associated domains**

Depending on the number of SAML actions you have in your deployment, you must replicate lines 1–3 and customize the domains for each SAML action.



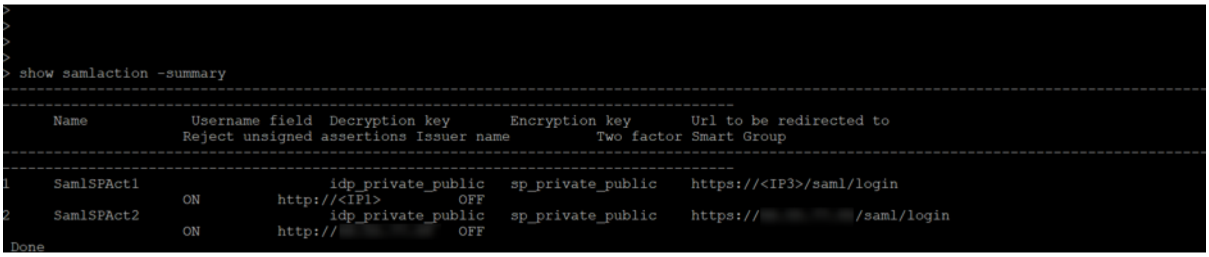
```
1  SSH ▾  add patset $saml_action_patset$
2  SSH ▾  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  SSH ▾  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  SSH ▾  add patset $saml_profile_patset$
5  SSH ▾  bind patset $saml_profile_patset$ "$saml_profile_url1$"
6  SSH ▾  set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset$")
7  SSH ▾  save config
```

For example, if you have two SAML actions, repeat lines 1–3 two times and accordingly customize the variable definitions for each SAML action.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_action_patset$ “$saml_action_domain1$”` multiple times to ensure that line appears N times for that SAML action. And change the following variable definition names:

- `saml_action_patset`: is the config template variable, and it represents the value of name of the pattern set (patset) for the SAML action. You can specify the real value in step 3 of the config job workflow. See the section Step 3: Specify variable values in this doc.
- `saml_action_domain1`: is the config template variable, and it represents the domain name for that specific SAML action. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this doc.

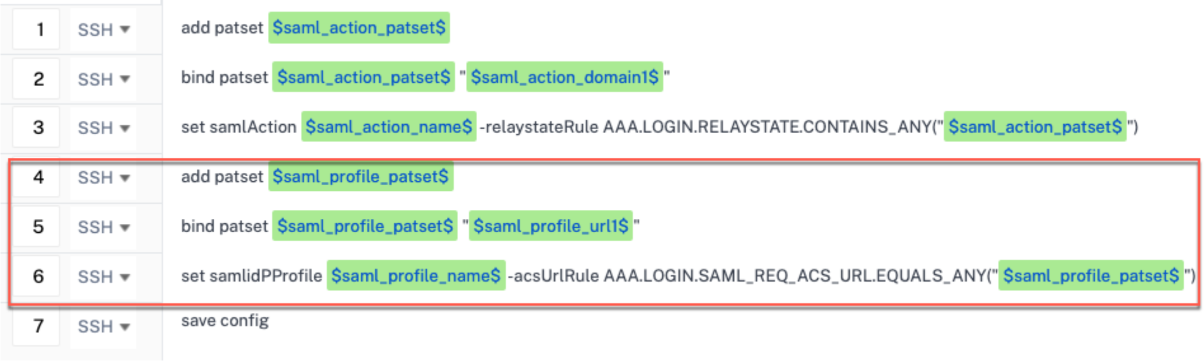
To find all the SAML actions for a device, run the command `show samlaction`.



```
>
>
>
>
> show samlaction -summary
--------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name           Two factor Smart Group
--------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------
1     SamlSPAct1                     idp_private_public   sp_private_public    https://<IP3>/saml/login
                    ON          http://<IP1>          OFF
2     SamlSPAct2                     idp_private_public   sp_private_public    https://[redacted]/saml/login
                    ON          http://[redacted]          OFF
 Done
```

b. **SAML profiles and their associated URLs**

Depending on the number of SAML profiles you have in your deployment, replicate lines 4–6. Customize the URLs for each SAML profile.



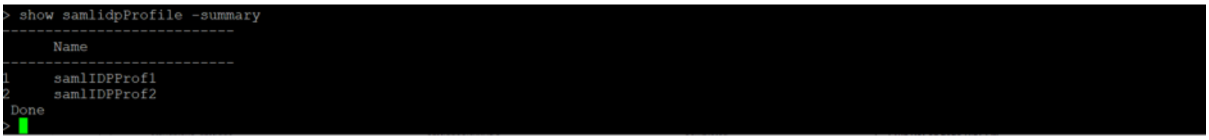
```
1  SSH ▾  add patset $saml_action_patset$
2  SSH ▾  bind patset $saml_action_patset$ " $saml_action_domain1$ "
3  SSH ▾  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY(" $saml_action_patset$ ")
4  SSH ▾  add patset $saml_profile_patset$
5  SSH ▾  bind patset $saml_profile_patset$ " $saml_profile_url1$ "
6  SSH ▾  set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY(" $saml_profile_patset$ ")
7  SSH ▾  save config
```

For example, if you have two SAML profiles, manually enter lines 4–6 two times and accordingly customize the variable definitions for each SAML action.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_profile_patset$ “$saml_profile_url1$”` multiple times to ensure that line appears N times for that SAML profile. And change the following variable definition names:

- `saml_profile_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.
- `saml_profile_url1`: is the config template variable, and it represents the domain name for that specific SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.

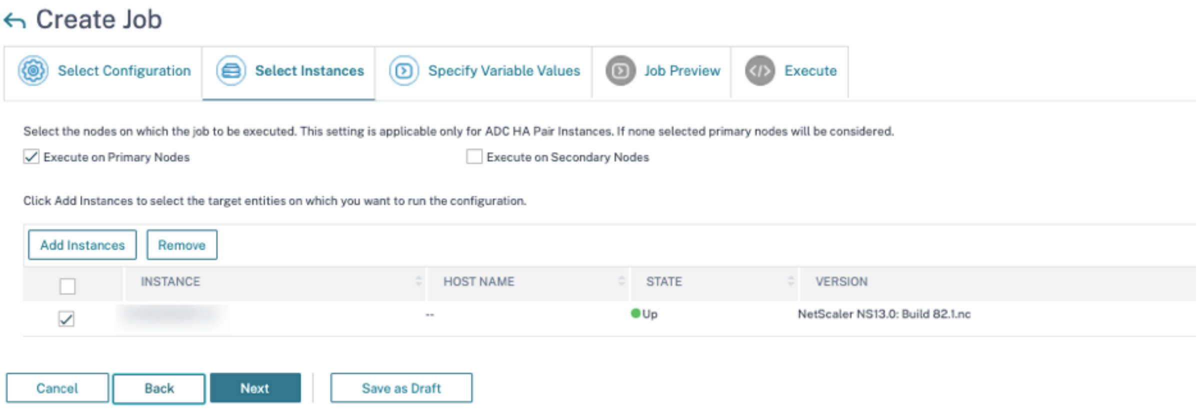
To find all the SAM profiles for a device, run the command `show samlidpProfile`.



```
> show samlidpProfile -summary
--------------------------------
      Name
--------------------------------
1     samlIDPProf1
2     samlIDPProf2
 Done
> 
```

Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.



Select the nodes on which the job to be executed. This setting is applicable only for ADC HA Pair Instances. If none selected primary nodes will be considered.

☑ Execute on Primary Nodes ☐ Execute on Secondary Nodes

Click Add Instances to select the target entities on which you want to run the configuration.

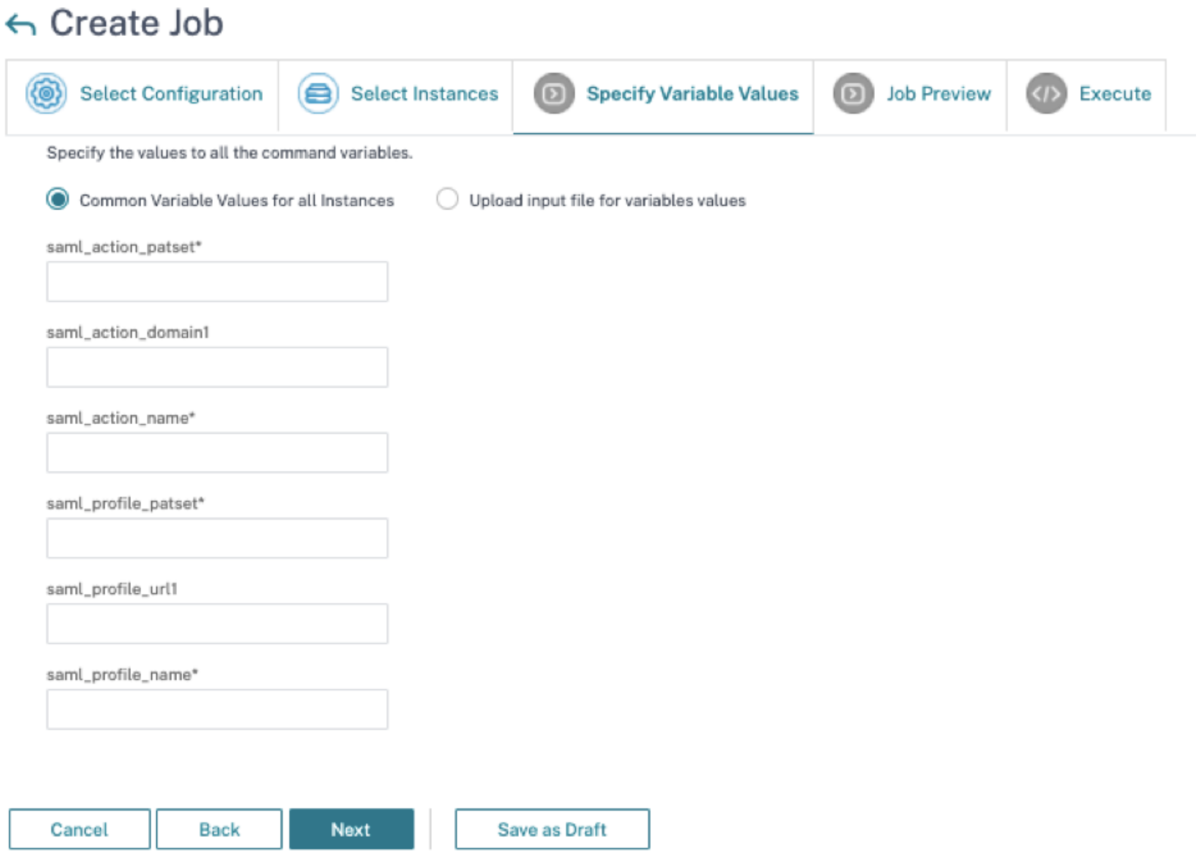
☐	INSTANCE	HOST NAME	STATE	VERSION
☑	[redacted]	--	● Up	NetScaler NS13.0: Build 82.1.nc

Step 3: Specify variable values

Enter the variable values.

- `saml_action_patset`: add a name for the SAML action
- `saml_action_domain1`: enter a domain in the format `https://<example1.com>/`
- `saml_action_name`: enter the same of the SAML action for which you are configuring the job
- `saml_profile_patset`: add a name for the SAML profile
- `saml_profile_url1`: enter the URL is this format `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: enter the same of the SAML profile for which you are configuring the job

> **Note**
>
> For URLs, the extension is not always `cgi/samlauth`. It depends on what third-party authorization you have, and accordingly you must put the extension.



Specify the values to all the command variables.

● Common Variable Values for all Instances ○ Upload input file for variables values

saml_action_patset*

saml_action_domain1

saml_action_name*

saml_profile_patset*

saml_profile_url1

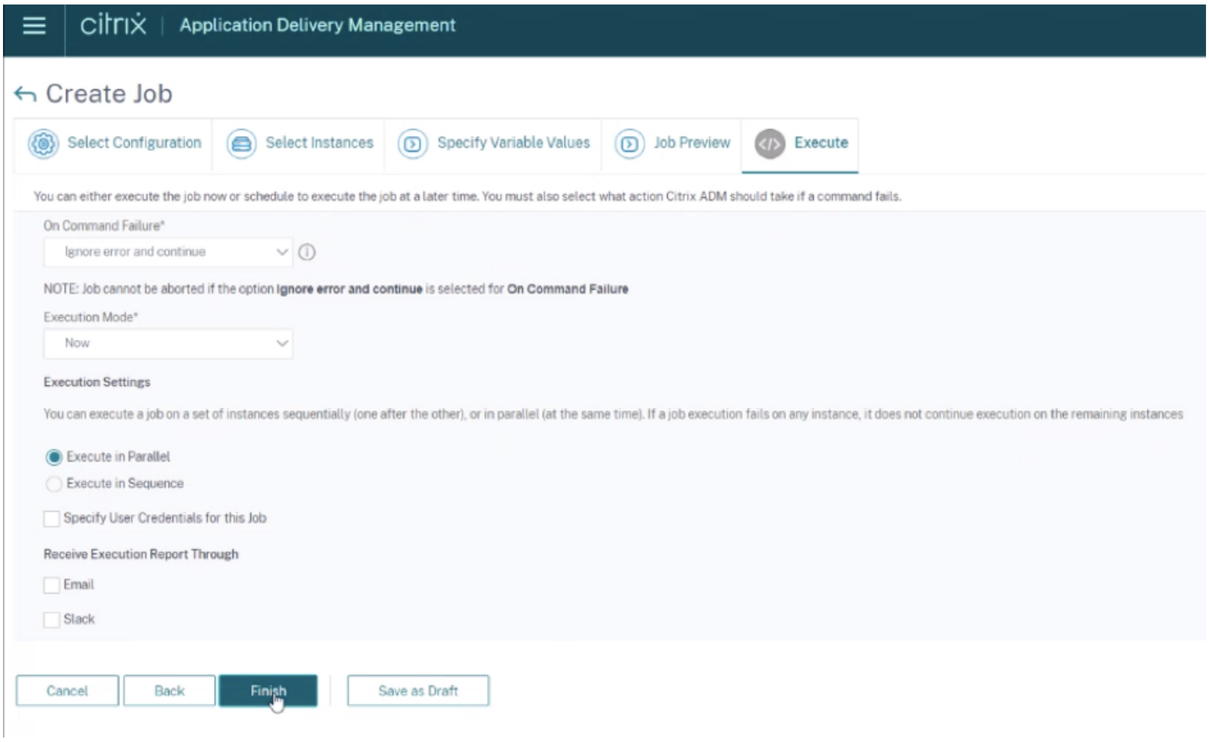
saml_profile_name*

Step 4: Preview the configuration

Previews the variable values having been inserted in the config and click **Next**.

Step 5: Run the job

Click **Finish** to run the configuration job.



Create Job

You can either execute the job now or schedule to execute the job at a later time. You must also select what action Citrix ADM should take if a command fails.

On Command Failure*: Ignore error and continue

NOTE: Job cannot be aborted if the option **Ignore error and continue** is selected for **On Command Failure**

Execution Mode*: Now

Execution Settings

You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances

● Execute in Parallel
○ Execute in Sequence

□ Specify User Credentials for this Job

Receive Execution Report Through

□ Email

□ Slack

After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable ADCs, you can run an on-demand scan to see the revised security posture.

Points to note for Citrix Application Delivery and Management Express account

The Citrix Application Delivery and Management Express account has limited features, which include limitations of two configuration jobs only. To know more about Citrix Application Delivery and Management Express account, see Manage Citrix Application Delivery and Management resources using Express account.
For CVE-2020-8300 remediation, you must run as many configuration jobs as the number of your vulnerable ADC instances. So, if you have an Express account and need to run more than two configuration jobs, follow this workaround.

Workaround: Run two configuration jobs for two vulnerable ADC instances and then delete both the jobs to continue running the next two jobs for the next two vulnerable ADC instances. Continue this until you have covered all vulnerable instances. Before deleting the jobs, you can download the report for future reference. To download the report, under **Network > Jobs**, select the jobs and click **Download** under **Actions**.

Example: If you have six vulnerable ADC instances, run two configuration jobs on two vulnerable instances respectively and then delete both the configuration jobs. Repeat this step another two times. At the end, you would have run six config jobs for six ADC instances respectively. In the Citrix Application Delivery and Management UI under **Infrastructure > Jobs**, you see only the last two configuration jobs.

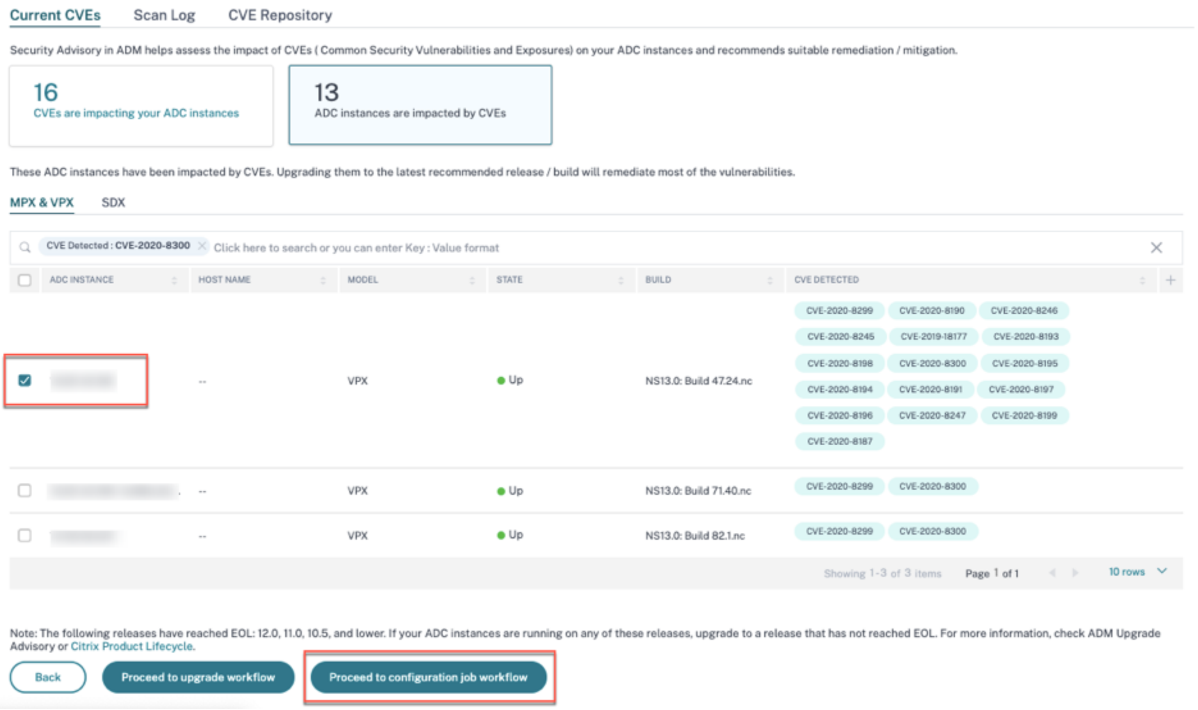
Scenario

In this scenario, three ADC instances are vulnerable to CVE-2020-8300 and you need to remediate all the instances. Follow these steps:

1. Upgrade all the three ADC instances by following the steps given in the "Upgrade an instance" section in this document.
2. Apply config patch to one ADC at a time, using the configuration job workflow. See the steps given in the "Apply configuration commands" section in this document.

The vulnerable ADC 1 has the following configuration:

Two SAML actions	Two SAML profiles
SAML action 1 has one domain, and SAML action 2 has two domains	SAML profile 1 has one URL, and SAML profile 2 has two URLs



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

16
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

CVE Detected : CVE-2020-8300 Click here to search or you can enter Key : Value format

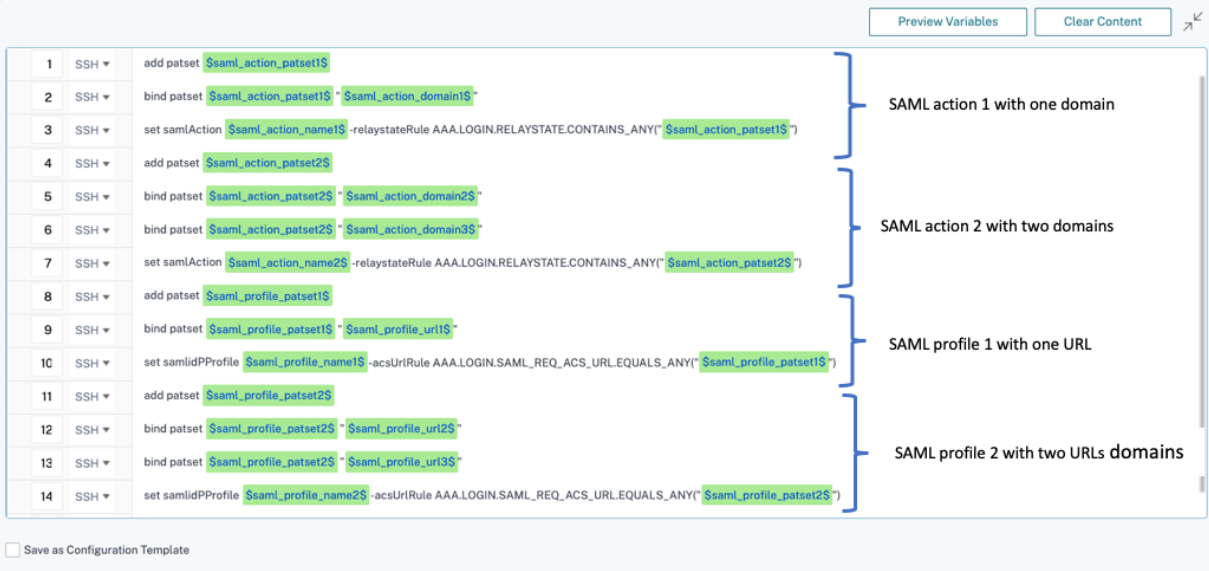
□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
☑	[redacted]	--	VPX	● Up	NS13.0: Build 47.24.nc	CVE-2020-8299 CVE-2020-8190 CVE-2020-8246 CVE-2020-8245 CVE-2019-18177 CVE-2020-8193 CVE-2020-8198 CVE-2020-8300 CVE-2020-8195 CVE-2020-8194 CVE-2020-8191 CVE-2020-8197 CVE-2020-8196 CVE-2020-8247 CVE-2020-8199 CVE-2020-8187
□	[redacted]	--	VPX	● Up	NS13.0: Build 71.40.nc	CVE-2020-8299 CVE-2020-8300
□	[redacted]	--	VPX	● Up	NS13.0: Build 82.1.nc	CVE-2020-8299 CVE-2020-8300

Showing 1-3 of 3 items Page 1 of 1 10 rows

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back
Proceed to upgrade workflow
Proceed to configuration job workflow

Select ADC 1 and click **Proceed to configuration job workflow**. The built-in template auto-populates. Next, give a job name and customize the template according to the given configuration.



```
add patset $saml_action_patset1$
bind patset $saml_action_patset1$ "$saml_action_domain1$"
set samlAction $saml_action_name1$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset1$")
add patset $saml_action_patset2$
bind patset $saml_action_patset2$ "$saml_action_domain2$"
bind patset $saml_action_patset2$ "$saml_action_domain3$"
set samlAction $saml_action_name2$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset2$")
add patset $saml_profile_patset1$
bind patset $saml_profile_patset1$ "$saml_profile_url1$"
set samlidPProfile $saml_profile_name1$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset1$")
add patset $saml_profile_patset2$
bind patset $saml_profile_patset2$ "$saml_profile_url2$"
bind patset $saml_profile_patset2$ "$saml_profile_url3$"
set samlidPProfile $saml_profile_name2$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset2$")
```

SAML action 1 with one domain

SAML action 2 with two domains

SAML profile 1 with one URL

SAML profile 2 with two URLs domains

□ Save as Configuration Template

The following tables list the variable definitions for customized parameters.

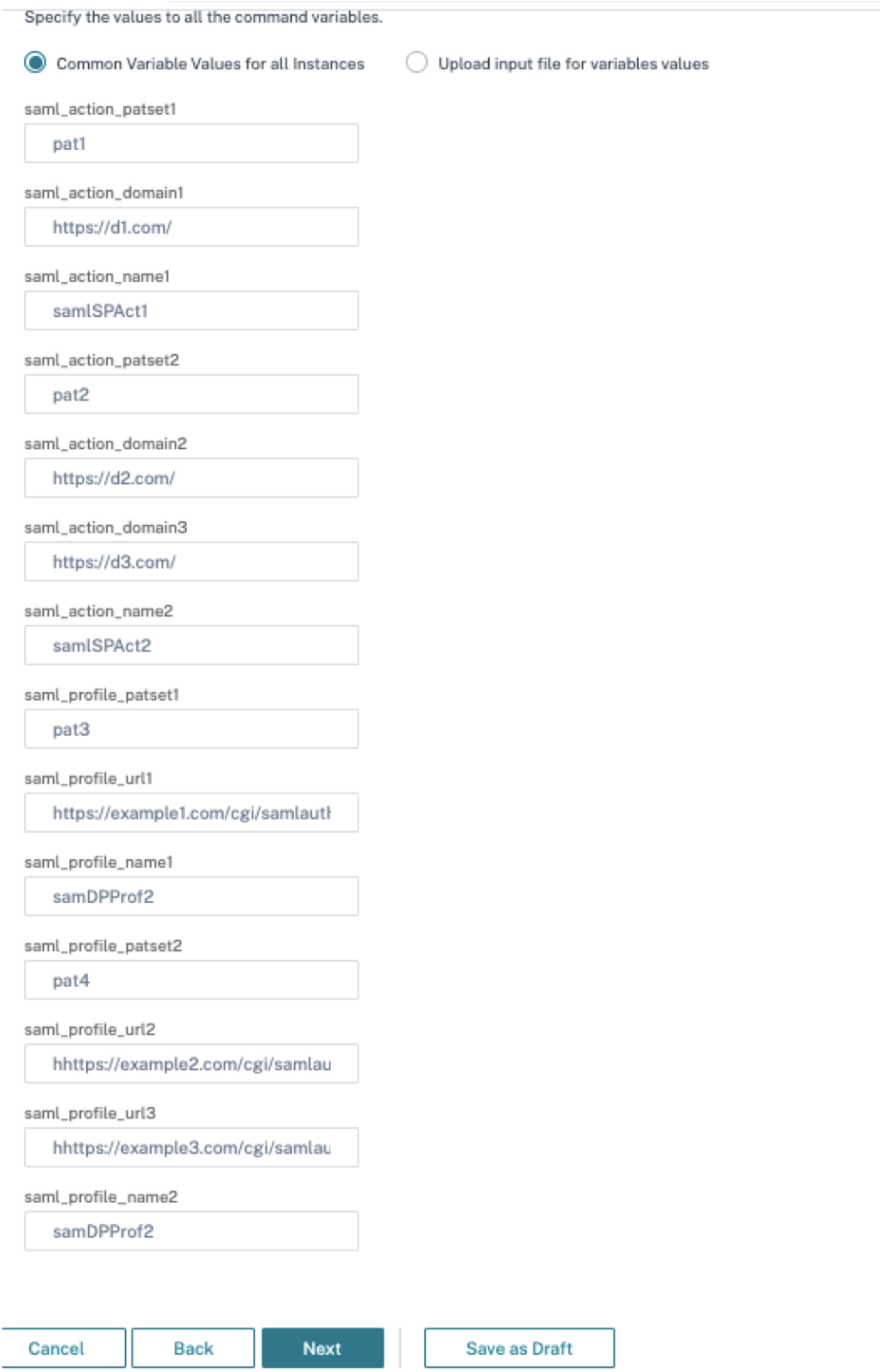
Table 1. Variable definitions for SAML action

ADC configuration	Variable definition for patset	Variable definition for SAML action name	Variable definition for domain
SAML action 1 has one domain	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Table 2. Variable definitions for SAML profile

ADC configuration	Variable definition for patset	Variable definition for SAML profile name	Variable definition for URL
SAML profile 1 has one URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML profile 2 has two URLs	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

Under **Select Instances**, select ADC 1 and click **Next**. The **Specify Variable Values** window appears. In this step, you need to provide values for all the variables defined in the previous step.



Specify the values to all the command variables.

● Common Variable Values for all Instances ○ Upload input file for variables values

saml_action_patset1: pat1

saml_action_domain1: https://d1.com/

saml_action_name1: samlSPAct1

saml_action_patset2: pat2

saml_action_domain2: https://d2.com/

saml_action_domain3: https://d3.com/

saml_action_name2: samlSPAct2

saml_profile_patset1: pat3

saml_profile_url1: https://example1.com/cgi/samlautl

saml_profile_name1: samDPProf2

saml_profile_patset2: pat4

saml_profile_url2: hhttps://example2.com/cgi/samlau

saml_profile_url3: hhttps://example3.com/cgi/samlau

saml_profile_name2: samDPProf2

Next, review the variables.

Click **Next** and then click **Finish** to run the job.

After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for ADC1, follow the same steps to remediate ADC 2 and ADC 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Training video

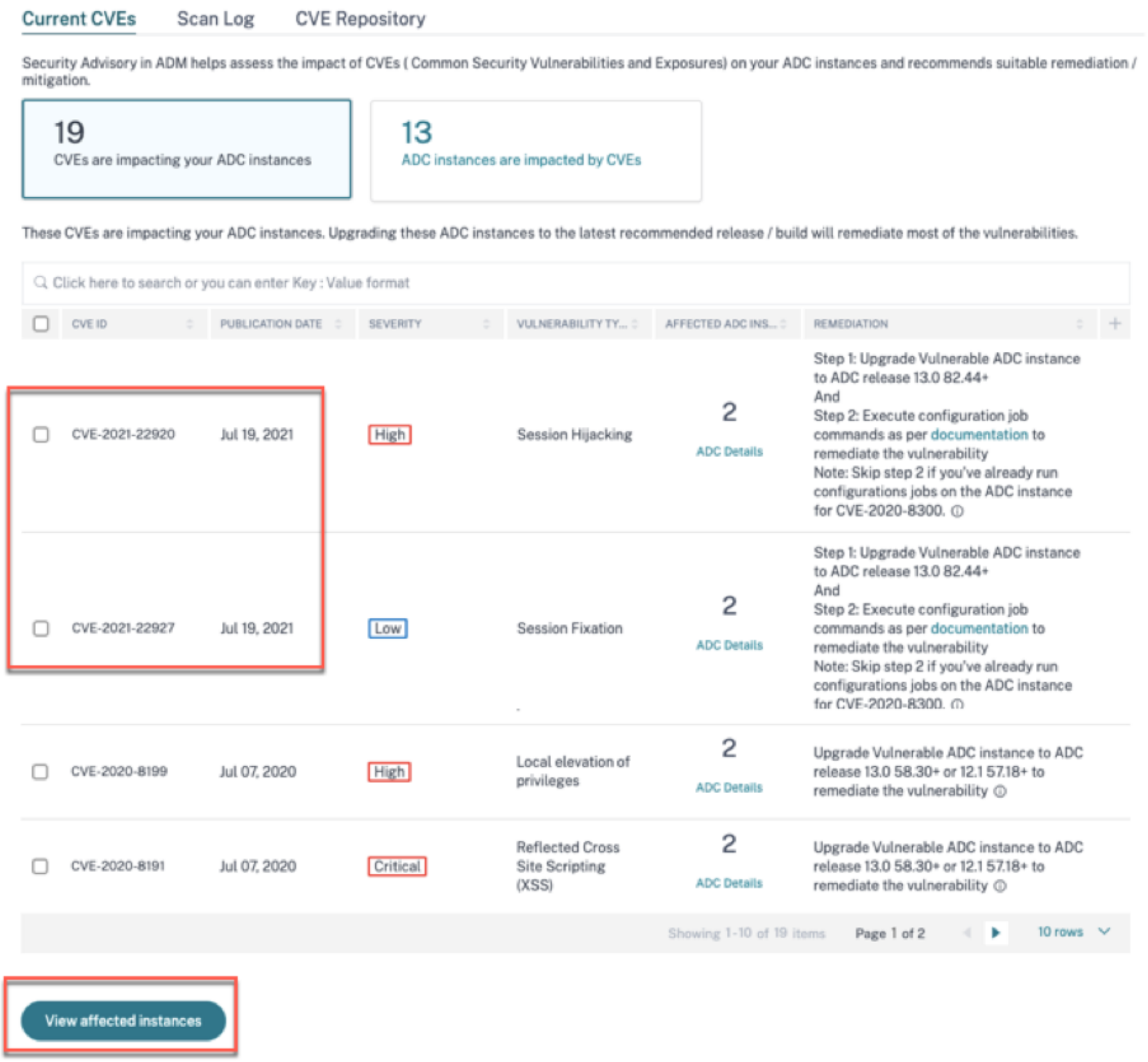
See the following training video to learn more.

Citrix Application Delivery and Management security advisory can help you identify and remediate CVE-2020-8300.

Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920

September 25, 2021

In the Citrix Application Delivery and Management security advisory dashboard, under **Current CVEs > <`number of`> ADC instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2021-22927 and CVE-2021-22920. To check the details of the instances impacted by these two CVEs, select one or more CVEs and click **View Affected Instances**.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

19
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These CVEs are impacting your ADC instances. Upgrading these ADC instances to the latest recommended release / build will remediate most of the vulnerabilities.

Click here to search or you can enter Key : Value format

□	CVE ID	PUBLICATION DATE	SEVERITY	VULNERABILITY TY...	AFFECTED ADC INS...	REMEDIATION
□	CVE-2021-22920	Jul 19, 2021	High	Session Hijacking	2 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.44+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability Note: Skip step 2 if you've already run configurations jobs on the ADC instance for CVE-2020-8300. ⓘ
□	CVE-2021-22927	Jul 19, 2021	Low	Session Fixation	2 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.44+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability Note: Skip step 2 if you've already run configurations jobs on the ADC instance for CVE-2020-8300. ⓘ
□	CVE-2020-8199	Jul 07, 2020	High	Local elevation of privileges	2 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ to remediate the vulnerability ⓘ
□	CVE-2020-8191	Jul 07, 2020	Critical	Reflected Cross Site Scripting (XSS)	2 ADC Details	Upgrade Vulnerable ADC instance to ADC release 13.0 58.30+ or 12.1 57.18+ to remediate the vulnerability ⓘ

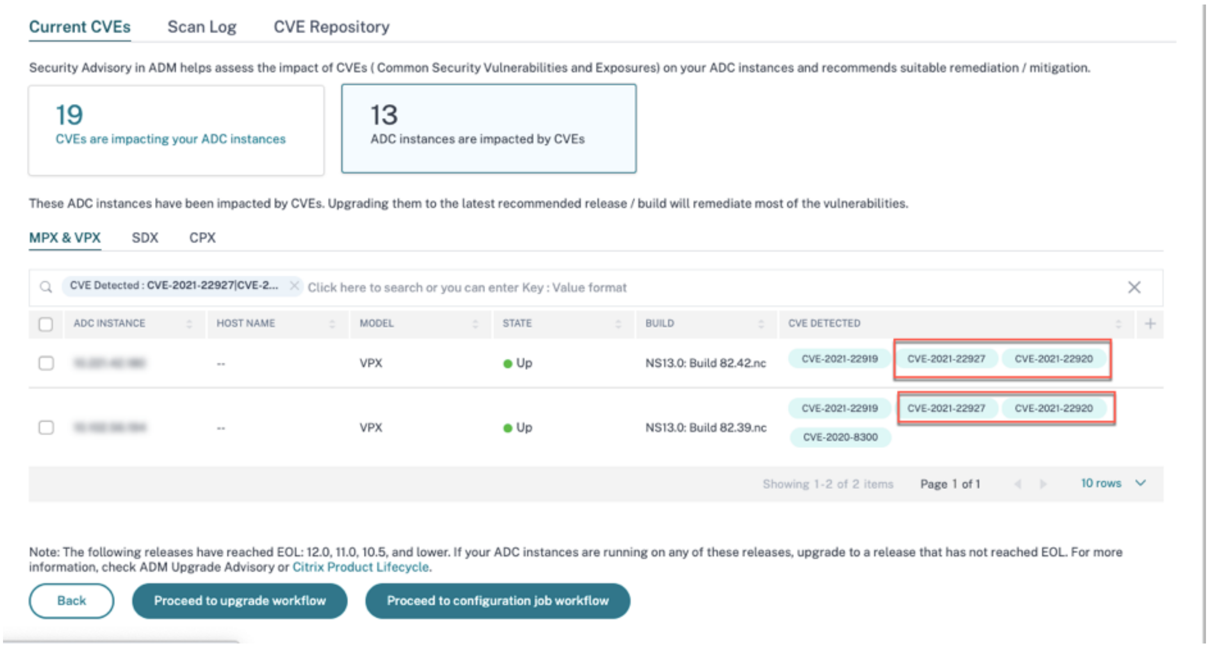
Showing 1-10 of 19 items Page 1 of 2 10 rows

View affected instances

Note

It might take a couple of hours for security advisory system scan to conclude and reflect the impact of CVE-2021-22927 and CVE-2021-22920 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.
For more information about the security advisory dashboard see, Security Advisory.

The <`number of`> **ADC instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the ADC instances impacted by CVE-2021-22927 and CVE-2021-22920.



Current CVEs   Scan Log   CVE Repository

Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

19
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

MPX & VPX   SDX   CPX

CVE Detected : CVE-2021-22927|CVE-2... ✕ Click here to search or you can enter Key : Value format

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
□	[redacted]	--	VPX	● Up	NS13.0: Build 82.42.nc	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920
□	[redacted]	--	VPX	● Up	NS13.0: Build 82.39.nc	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920 CVE-2020-8300

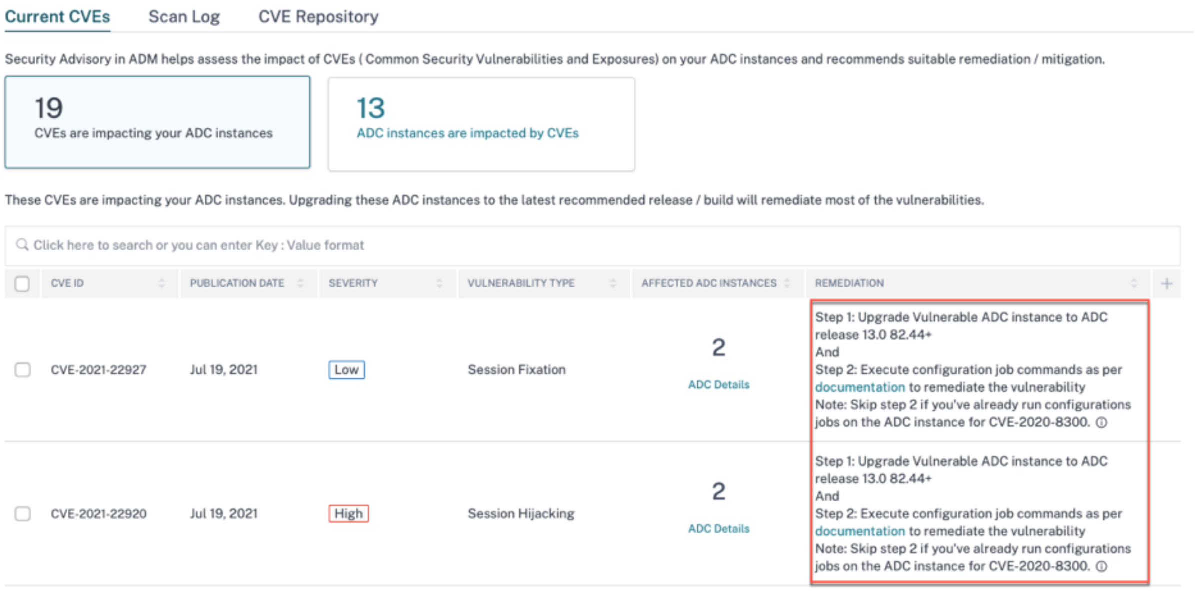
Showing 1-2 of 2 items   Page 1 of 1   10 rows

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back   Proceed to upgrade workflow   Proceed to configuration job workflow

Remediate CVE-2021-22927 and CVE-2021-22920

For CVE-2021-22927 and CVE-2021-22920 impacted ADC instances, the remediation is a two-step process. In the GUI, under **Current CVEs > ADC instances are impacted by CVEs**, you can see step 1 and 2.



Current CVEs   Scan Log   CVE Repository

Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

19
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These CVEs are impacting your ADC instances. Upgrading these ADC instances to the latest recommended release / build will remediate most of the vulnerabilities.

Click here to search or you can enter Key : Value format

□	CVE ID	PUBLICATION DATE	SEVERITY	VULNERABILITY TYPE	AFFECTED ADC INSTANCES	REMEDIATION
□	CVE-2021-22927	Jul 19, 2021	Low	Session Fixation	2 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.44+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability Note: Skip step 2 if you've already run configurations jobs on the ADC instance for CVE-2020-8300. ⓘ
□	CVE-2021-22920	Jul 19, 2021	High	Session Hijacking	2 ADC Details	Step 1: Upgrade Vulnerable ADC instance to ADC release 13.0 82.44+ And Step 2: Execute configuration job commands as per documentation to remediate the vulnerability Note: Skip step 2 if you've already run configurations jobs on the ADC instance for CVE-2020-8300. ⓘ

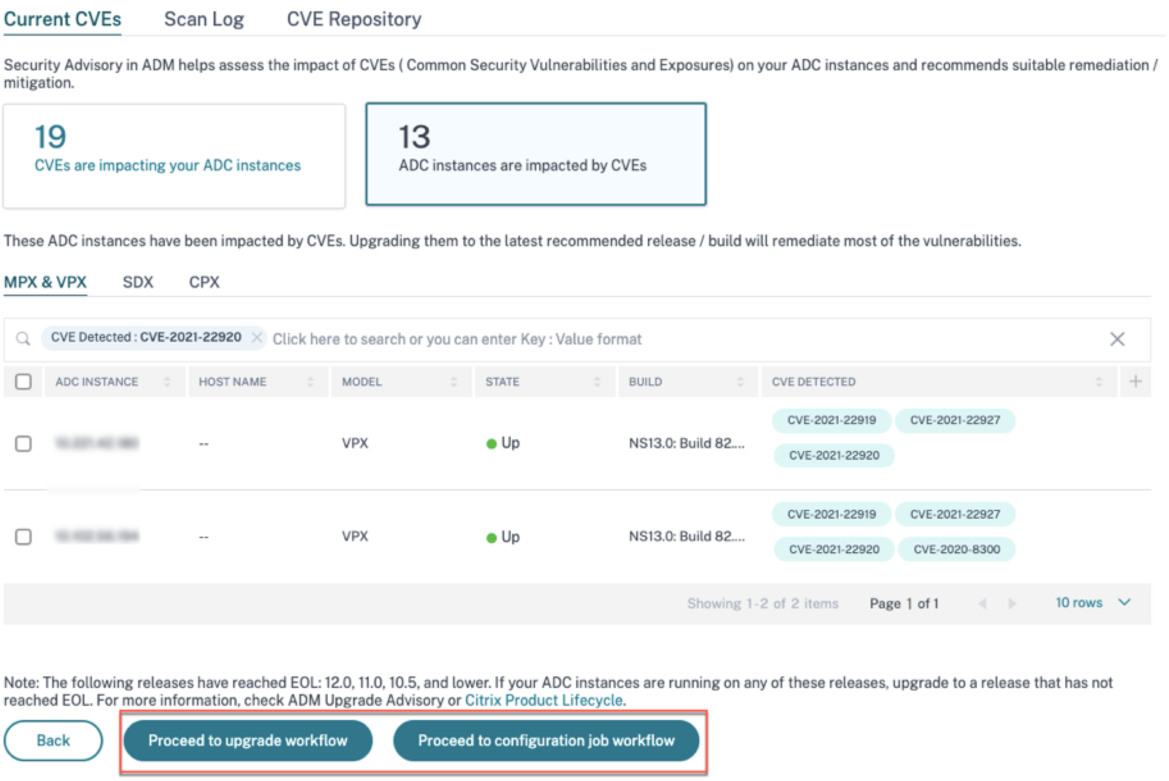
The two steps include:

1. Upgrading the vulnerable ADC instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration

template in configuration jobs. Follow this step for each vulnerable ADC one at a time and include all SAML actions for that ADC.

> **Note**
>
> Skip step 2 if you've already run configuration jobs on the ADC instance for CVE-2020-8300.

Under **Current CVEs> ADC instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

19 CVEs are impacting your ADC instances

13 ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

CVE Detected : CVE-2021-22920 Click here to search or you can enter Key : Value format

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
□	[redacted]	--	VPX	● Up	NS13.0: Build 82....	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920
□	[redacted]	--	VPX	● Up	NS13.0: Build 82....	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920 CVE-2020-8300

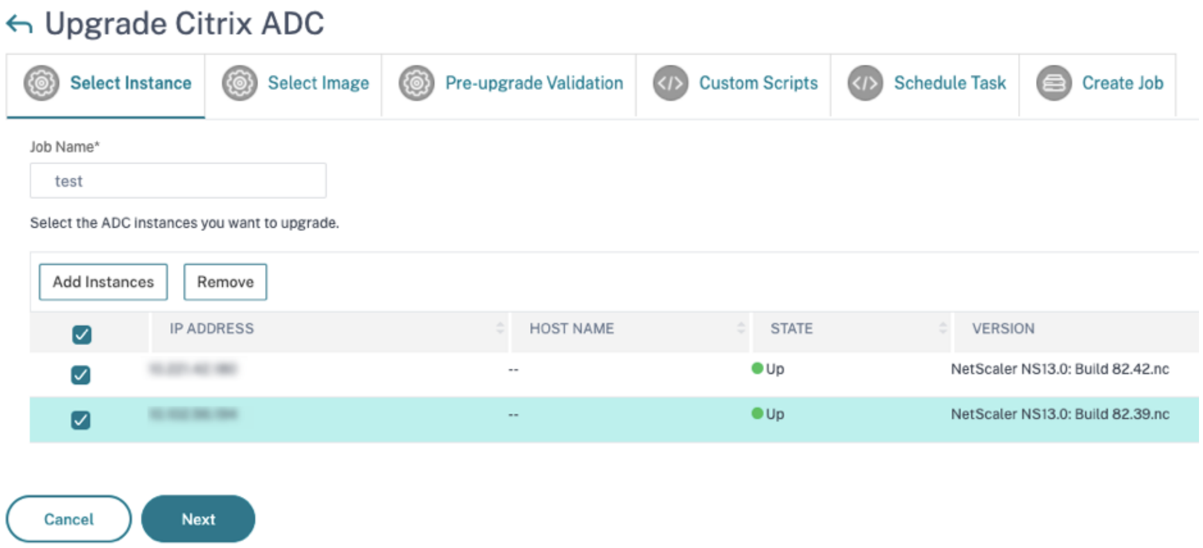
Showing 1-2 of 2 items Page 1 of 1 10 rows

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back
Proceed to upgrade workflow
Proceed to configuration job workflow

Step 1: Upgrade the vulnerable ADC instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable ADC instances already populated.



Job Name*: test

Select the ADC instances you want to upgrade.

☑	IP ADDRESS	HOST NAME	STATE	VERSION
☑	[redacted]	--	● Up	NetScaler NS13.0: Build 82.42.nc
☑	[redacted]	--	● Up	NetScaler NS13.0: Build 82.39.nc

For more information on how to use Citrix Application Delivery and Management to upgrade ADC instances, see Create an ADC upgrade job.

> **Note**
>
> This step can be done at once for all the vulnerable ADC instances.
>
> **Note**
>
> After you have completed step 1 for all the ADC instances vulnerable to CVE-2021-22920 and CVE-2021-22927, do an on-demand scan. The updated security posture under **Current CVEs** helps you understand if the ADC instances are still vulnerable to any of these CVEs. From the new posture, you can also check if you need to run configuration jobs.
> If you've already applied the appropriate configuration jobs to the ADC instance for CVE-2020-8300 and now you have upgraded the ADC instance, after doing the on-demand scan the instance no longer shows as vulnerable for CVE-2020-8300, CVE-2021-22920, and CVE-2021-22927.

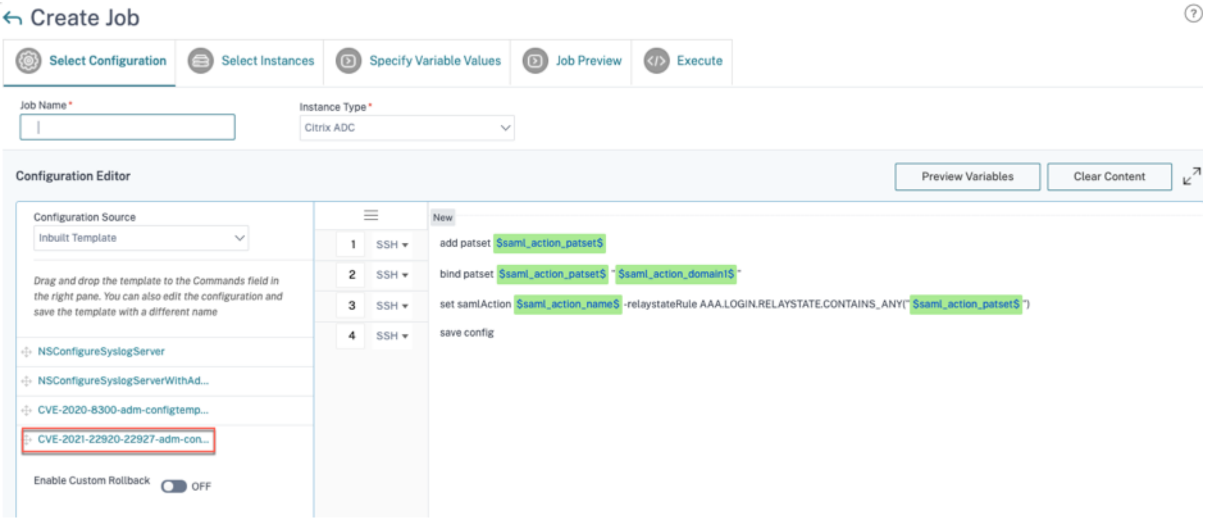
Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **<`number of`> ADC instances impacted by CVEs** window, select one instance impacted by CVE-2021-22927 and CVE-2021-22920 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



Job Name*: |

Instance Type*: Citrix ADC

Configuration Editor

Configuration Source: Inbuilt Template

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name

Enable Custom Rollback: OFF

```
1  add patset $saml_action_patset$
2  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  save config
```

> **Note**
>
> If the ADC instance selected in step 2 for applying configuration commands, is vulnerable to CVE-2021-22927, CVE-2021-22920, and also CVE-2020-8300, the base template for CVE-2020-8300 is auto-populated. The CVE-2020-8300 template is a super set of the config commands required for all the three CVEs. Customize this base template according to your ADC instance deployment and requirement.

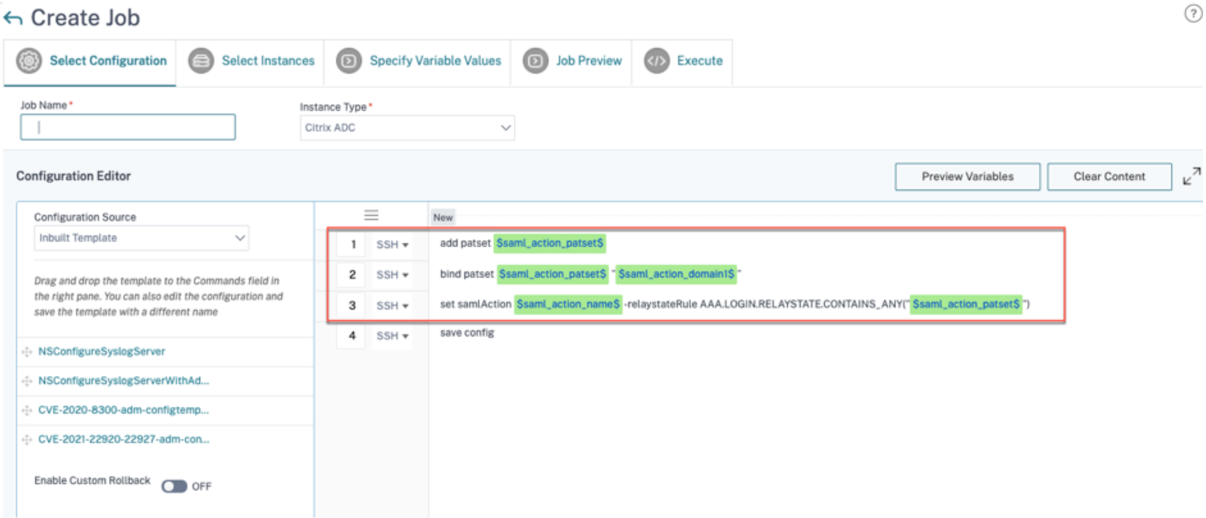
You must run a separate configuration job for each impacted ADC instance, one at a time, and include all SAML actions for that ADC. For example, if you have two vulnerable ADC instances each having two SAML actions, you must run this configuration job two times. One time per ADC covering all its SAML actions.

ADC 1	ADC2
Job 1: two SAML actions	Job 2: two SAML actions

Give the job a name and customize the template for the following specifications. The built-in configuration template is only an outline or base template. Customize the template based on your deployment for the following requirements:

a. **SAML actions and their associated domains**

Depending on the number of SAML actions you have in your deployment, you must replicate lines 1–3 and customize the domains for each SAML action.



Job Name *

Instance Type *: Citrix ADC

Configuration Editor

Configuration Source: Inbuilt Template

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name

- NSConfigureSyslogServer
- NSConfigureSyslogServerWithAd...
- CVE-2020-8300-adm-configtemp...
- CVE-2021-22920-22927-adm-con...

Enable Custom Rollback: OFF

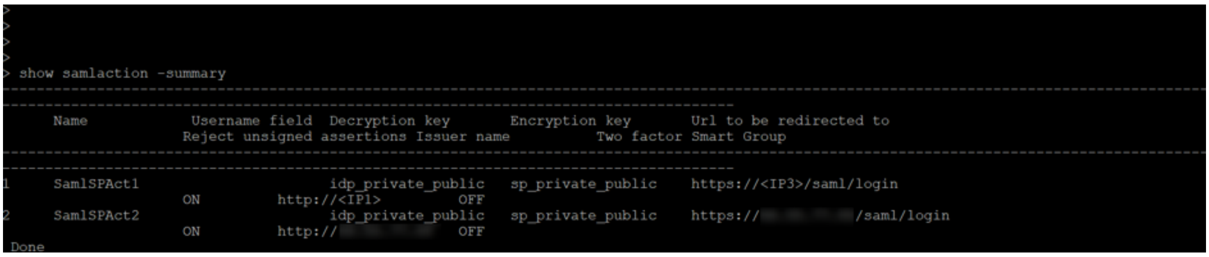
```
1  SSH  add patset $saml_action_patset$
2  SSH  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  SSH  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  SSH  save config
```

For example, if you have two SAML actions, repeat lines 1–3 two times and accordingly customize the variable definitions for each SAML action.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_action_patset$ “$saml_action_domain1$”` multiple times to ensure that the line appears N times for that SAML action. And change the following variable definition names:

- `saml_action_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML action. You can specify the real value in step 3 of the config job workflow. See the section Step 3: Specify variable values in this doc.
- `saml_action_domain1`: is the config template variable, and it represents the domain name for that specific SAML action. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this doc.

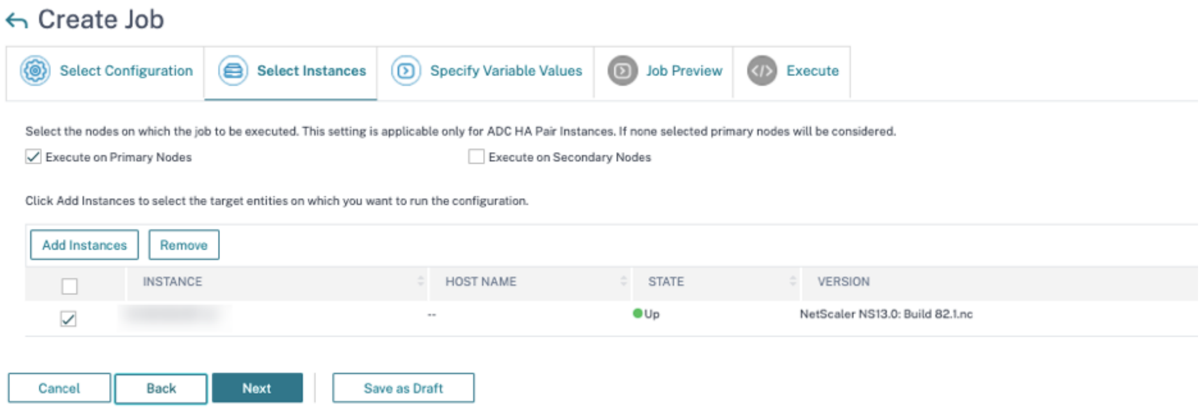
To find all the SAML actions for a device, run the command `show samlaction`.



```
>
>
>
>
> show samlaction -summary
---------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name          Two factor Smart Group
---------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
1     SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                    ON          http://<IP1>          OFF
2     SamlSPAct2                      idp_private_public   sp_private_public    https://[redacted]/saml/login
                    ON          http://[redacted]          OFF
 Done
```

Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.



Select the nodes on which the job to be executed. This setting is applicable only for ADC HA Pair Instances. If none selected primary nodes will be considered.

☑ Execute on Primary Nodes ☐ Execute on Secondary Nodes

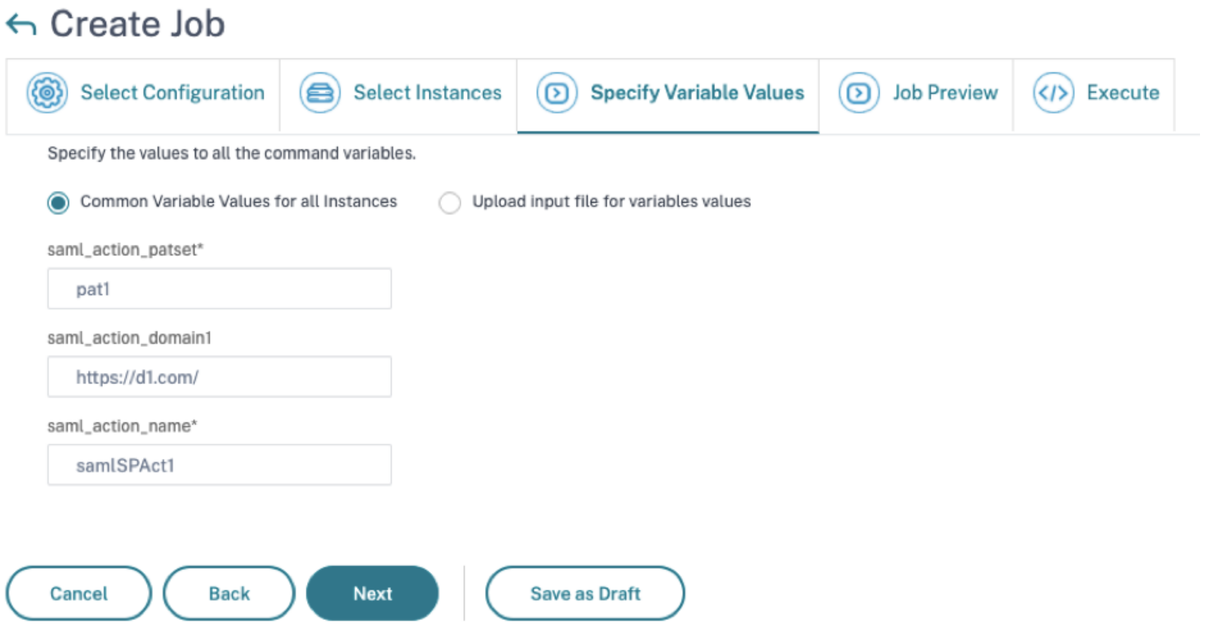
Click Add Instances to select the target entities on which you want to run the configuration.

☐	INSTANCE	HOST NAME	STATE	VERSION
☑	[redacted]	--	● Up	NetScaler NS13.0: Build 82.1.nc

Step 3: Specify variable values

Enter the variable values.

- `saml_action_patset`: add a name for the SAML action
- `saml_action_domain1`: enter a domain in the format `https://<example1.com>/`
- `saml_action_name`: enter the same of the SAML action for which you are configuring the job



Specify the values to all the command variables.

● Common Variable Values for all Instances ○ Upload input file for variables values

saml_action_patset*

pat1

saml_action_domain1

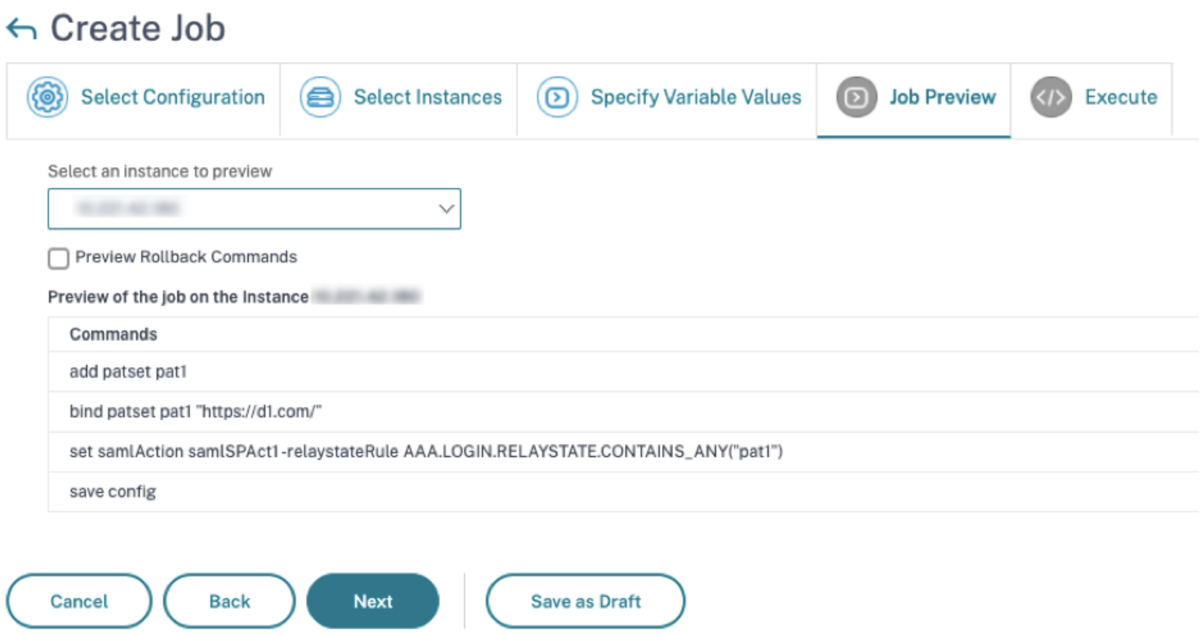
https://d1.com/

saml_action_name*

samlSPAct1

Step 4: Preview the configuration

Previews the variable values having been inserted in the config and click **Next**.



Select an instance to preview

[redacted]

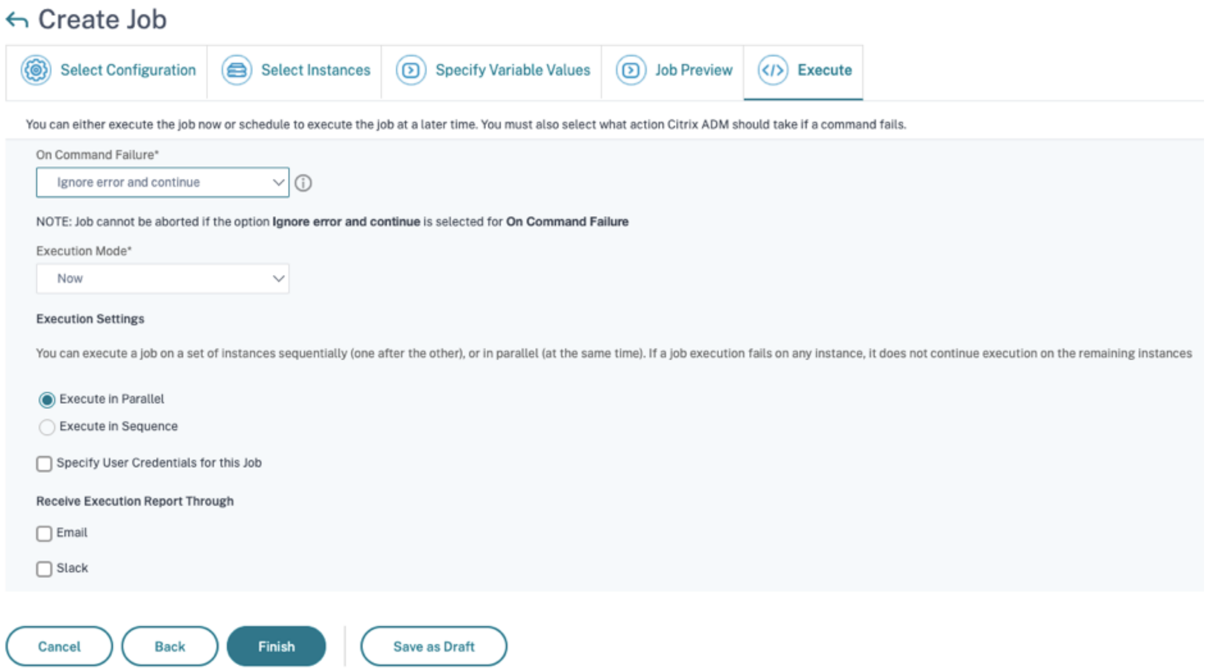
☐ Preview Rollback Commands

Preview of the job on the Instance [redacted]

Commands
add patset pat1
bind patset pat1 "https://d1.com/"
set samlAction samlSPAct1 -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("pat1")
save config

Step 5: Run the job

Click **Finish** to run the configuration job.



You can either execute the job now or schedule to execute the job at a later time. You must also select what action Citrix ADM should take if a command fails.

On Command Failure*

Ignore error and continue

NOTE: Job cannot be aborted if the option **Ignore error and continue** is selected for **On Command Failure**

Execution Mode*

Now

Execution Settings

You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances

● Execute in Parallel

○ Execute in Sequence

☐ Specify User Credentials for this Job

Receive Execution Report Through

☐ Email

☐ Slack

After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable ADCs, you can run an on-demand scan to see the revised security posture.

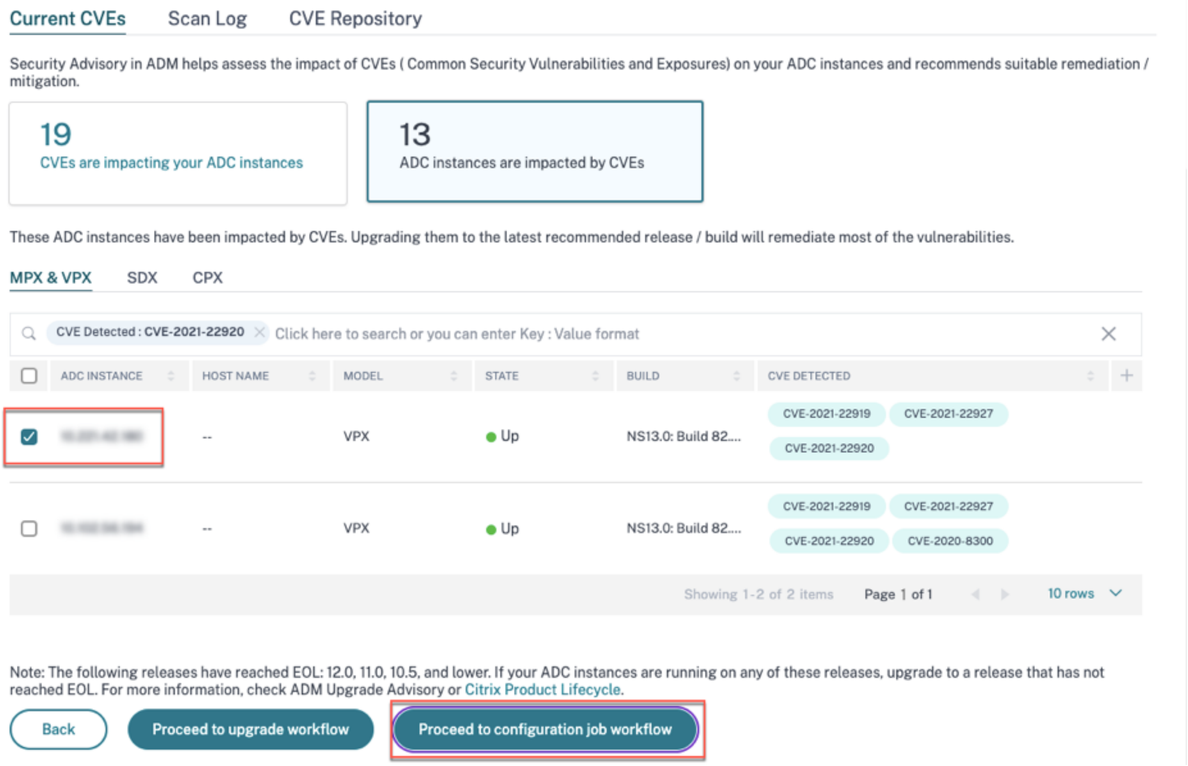
Scenario

In this scenario, two ADC instances are vulnerable to CVE-2021-22920, and you need to remediate all the instances. Follow these steps:

1. Upgrade all the three ADC instances by following the steps given in the "Upgrade an instance" section in this document.
2. Apply the config patch to one ADC at a time, using the configuration job workflow. See the steps given in the "Apply configuration commands" section in this document.

The vulnerable ADC 1 has two SAML actions:

- SAML action 1 has one domain
- SAML action 2 has two domains



Security Advisory in ADM helps assess the impact of CVEs (Common Security Vulnerabilities and Exposures) on your ADC instances and recommends suitable remediation / mitigation.

19
CVEs are impacting your ADC instances

13
ADC instances are impacted by CVEs

These ADC instances have been impacted by CVEs. Upgrading them to the latest recommended release / build will remediate most of the vulnerabilities.

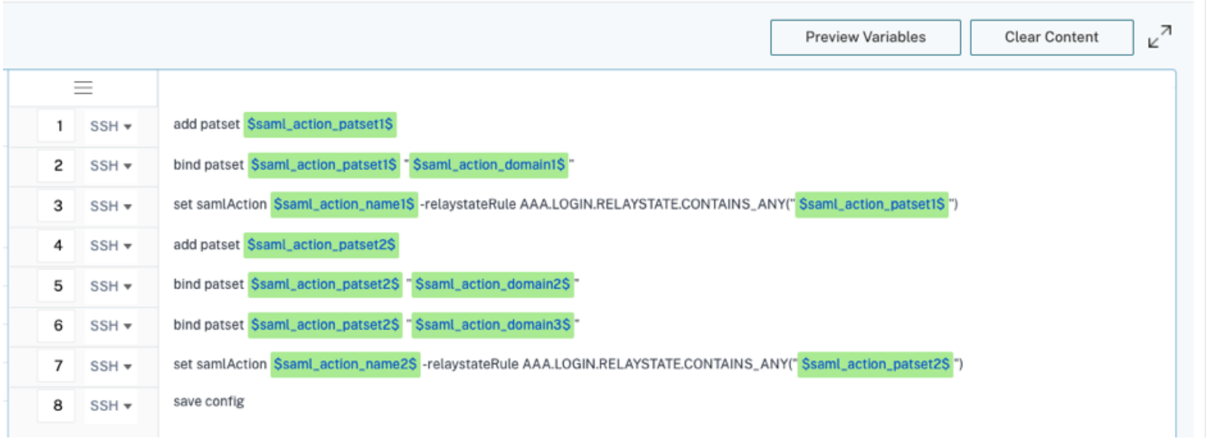
MPX & VPX
SDX
CPX
CVE Detected : CVE-2021-22920
Click here to search or you can enter Key : Value format

□	ADC INSTANCE	HOST NAME	MODEL	STATE	BUILD	CVE DETECTED
☑	[redacted]	--	VPX	● Up	NS13.0: Build 82....	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920
□	[redacted]	--	VPX	● Up	NS13.0: Build 82....	CVE-2021-22919 CVE-2021-22927 CVE-2021-22920 CVE-2020-8300

Note: The following releases have reached EOL: 12.0, 11.0, 10.5, and lower. If your ADC instances are running on any of these releases, upgrade to a release that has not reached EOL. For more information, check ADM Upgrade Advisory or Citrix Product Lifecycle.

Back
Proceed to upgrade workflow
Proceed to configuration job workflow

Select ADC 1 and click **Proceed to configuration job workflow**. The built-in base template auto-populates. Next, give a job name and customize the template according to the given configuration.



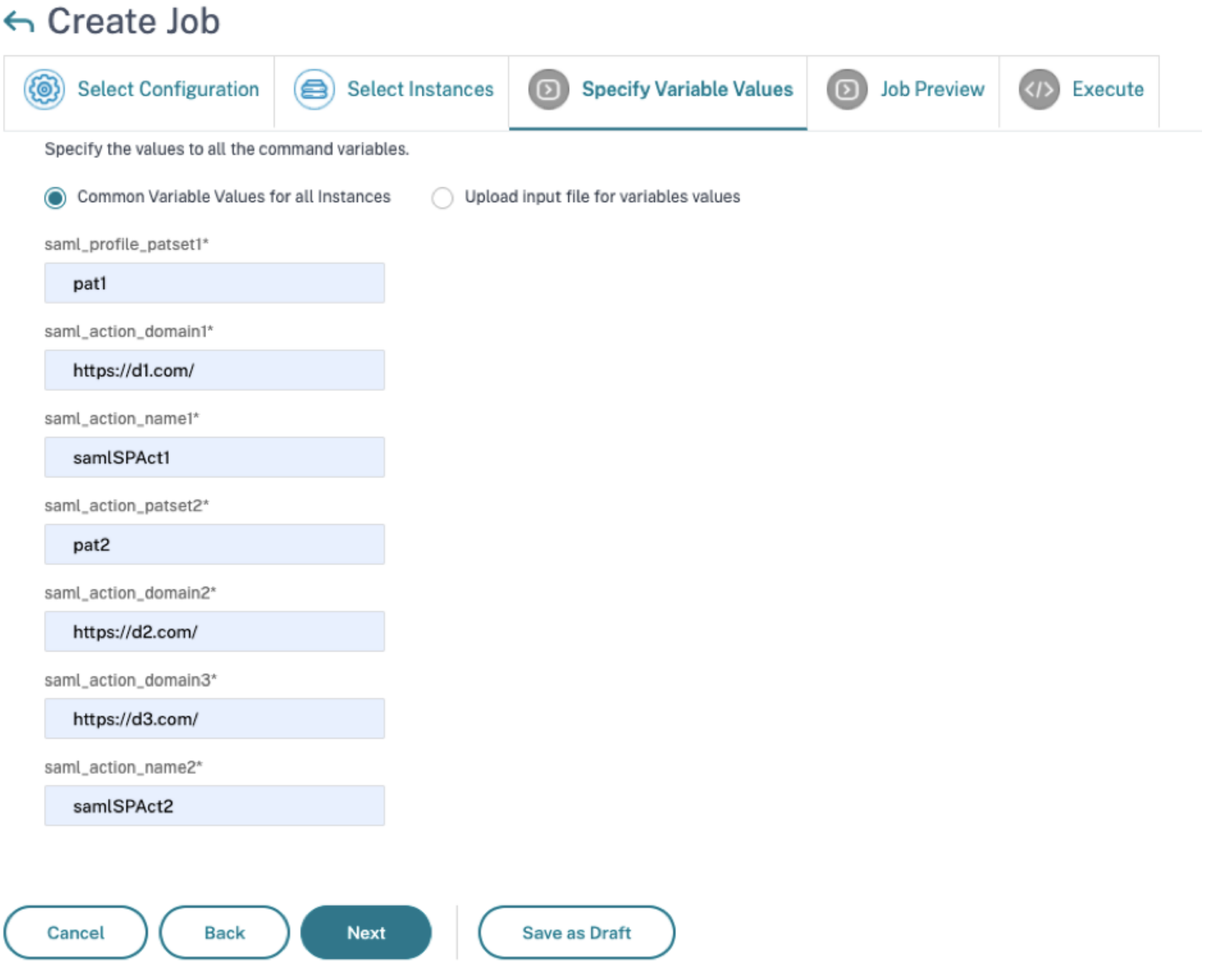
```
add patset $saml_action_patset1$
bind patset $saml_action_patset1$ "$saml_action_domain1$"
set samlAction $saml_action_name1$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset1$")
add patset $saml_action_patset2$
bind patset $saml_action_patset2$ "$saml_action_domain2$"
bind patset $saml_action_patset2$ "$saml_action_domain3$"
set samlAction $saml_action_name2$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset2$")
save config
```

The following table lists the variable definitions for customized parameters.

Table. Variable definitions for SAML action

ADC configuration	Variable definition for patset	Variable definition for SAML action name	Variable definition for domain
SAML action 1 has one domain	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Under **Select Instances**, select ADC 1 and click **Next**. The **Specify Variable Values** window appears. In this step, you need to provide values for all the variables defined in the previous step.



Specify the values to all the command variables.

● Common Variable Values for all Instances ○ Upload input file for variables values

saml_profile_patset1*: pat1

saml_action_domain1*: https://d1.com/

saml_action_name1*: samlSPAct1

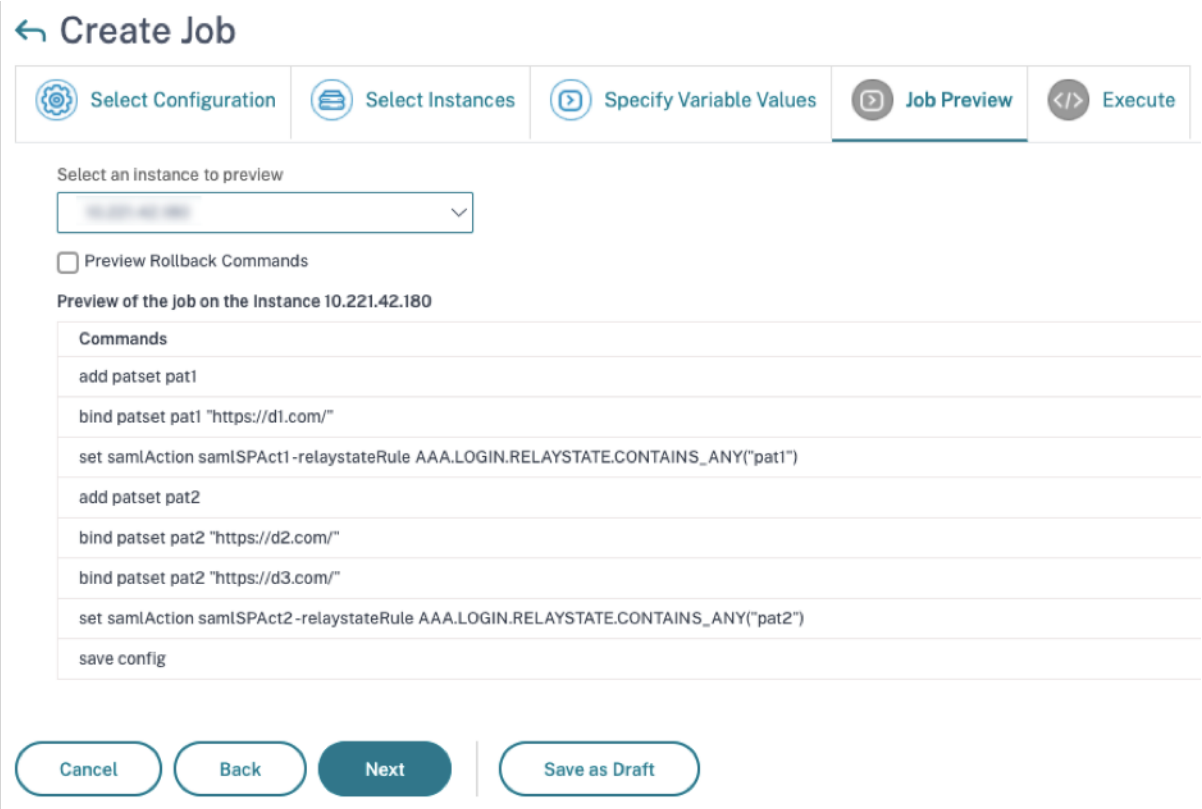
saml_action_patset2*: pat2

saml_action_domain2*: https://d2.com/

saml_action_domain3*: https://d3.com/

saml_action_name2*: samlSPAct2

Next, review the variables.



Select an instance to preview

[redacted]

□ Preview Rollback Commands

Preview of the job on the instance 10.221.42.180

Commands
add patset pat1
bind patset pat1 "https://d1.com/"
set samlAction samlSPAct1 -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("pat1")
add patset pat2
bind patset pat2 "https://d2.com/"
bind patset pat2 "https://d3.com/"
set samlAction samlSPAct2 -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("pat2")
save config

Click **Next** and then click **Finish** to run the job.

After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for ADC1, follow the same steps to remediate ADC 2 and ADC 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Setting up

September 25, 2021

After your initial setup is complete, you have to configure certain settings to start managing your deployment completely.

- Adding multiple agents. The number of agents to be installed depends on the number of managed instances in a data center or cloud and the total throughput. Citrix recommends that you install at least one agent for every data center.
- Adding instances. You can add instances either while setting up the Citrix Application Delivery and Management for the first time or at a later time. You have to add instances to the service

to start managing and monitoring them. After you install multiple agents, you have to add instances and associate them with the agents.

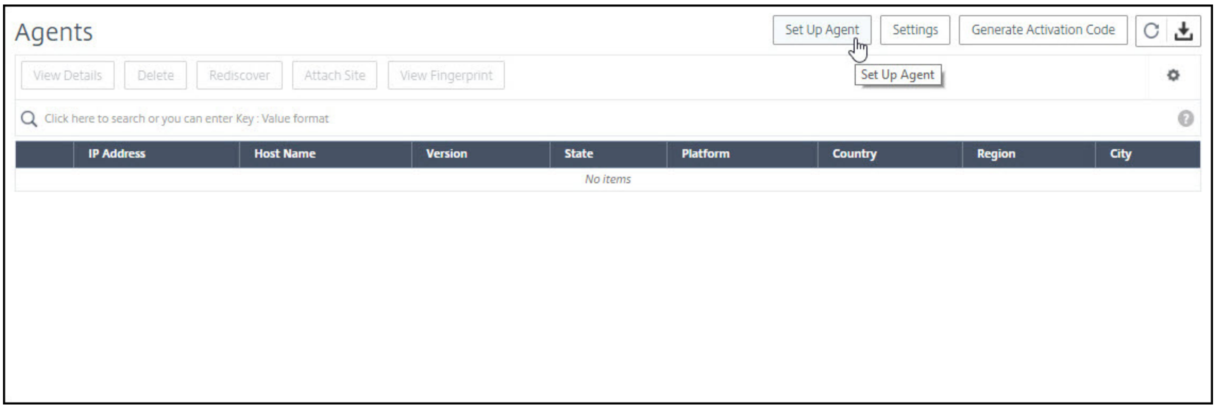
- Enabling Analytics. To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.
- Configuring syslog on instances. You can monitor the syslog events generated on your Citrix ADC instances if you have configured your device to redirect all syslog messages to Citrix Application Delivery and Management. To monitor syslog events, you need to first configure Citrix Application Delivery and Management as the syslog server for your Citrix ADC instance.
- Configuring role-based access control. Citrix Application Delivery and Management 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.
- Configuring Analytics settings. You can configure certain settings to ensure optimal experience with the Analytics feature. For example, you can specify the duration you want to store historical analytics data, and you can also set thresholds and alerts to monitor the desired analytics metrics.

Adding multiple agents

September 25, 2021

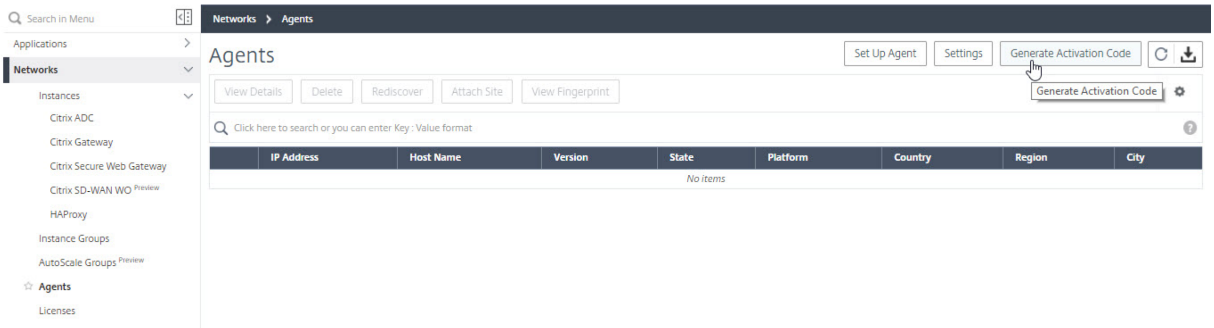
The number of agents to be installed depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Infrastructure > Instances > Agents** and click **Set Up Agent.**



Download the image for the required hypervisor and install the agent by following the instructions in Getting Started. Make sure you copy the service URL and the activation code displayed on the screen because you have to enter the service URL and the activation code while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.

You can use the same image to install multiple agents in your hypervisor. However, you cannot use the same activation code on multiple agents. After you install one agent, generate the activation code again for the next agent. You can generate a new activation code by navigating to **Infrastructure > Instances > Agents**, click **Generate Activation Code**.



	IP Address	Host Name	Version	State	Platform	Country	Region	City
No items								

After the agent is successfully installed and registered, verify the agent status on the service GUI and add instances to it.

> **Note**
>
> You can also install a Citrix Application Delivery and Management agent on Microsoft Azure cloud or AWS cloud. The agent image is available on the respective cloud marketplace.
>
> - For instructions about installing an agent on Microsoft Azure cloud, see Installing Citrix Application Delivery and Management Agent on Microsoft Azure Cloud.
> - For instructions about installing an agent on AWS, see Installing Citrix Application Delivery and Management Agent on AWS.

Configure agents for multisite deployment

October 20, 2021

Agents work as an intermediary between the Citrix Application Delivery and Management and the discovered instances across different data centers and public clouds. Citrix Application Delivery and Management supports agent failover within a data center or a public cloud.

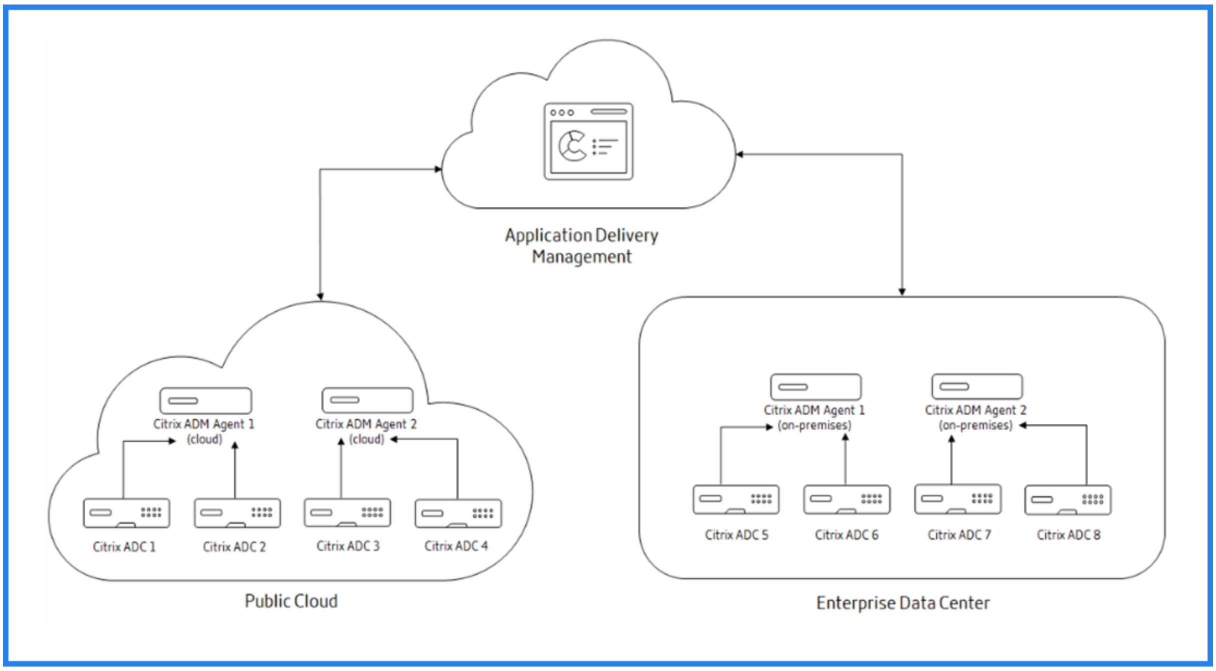
The following are the benefits of installing agents:

- The configured instances to an agent send the unprocessed data directly to the agent instead of Citrix Application Delivery and Management. Agent does the first level of data processing and sends the processed data in compressed format to the Citrix Application Delivery and Management for storage.

- Agents and instances are co-located in the same data center or cloud so that the data processing is faster.
- Clustering the agents provides redistribution of Citrix ADC instances on agent failover. When one agent in a site fails, traffic from Citrix ADC instances switches to another available agent in the same site.

Architecture

The following figure illustrates Citrix ADC instances configured on multiple agents in a data center and public cloud to achieve agent failover:


Application Delivery Management
Citrix ADM Agent 1 (cloud)
Citrix ADM Agent 2 (cloud)
Citrix ADC 1
Citrix ADC 2
Citrix ADC 3
Citrix ADC 4
Public Cloud
Citrix ADM Agent 1 (on-premises)
Citrix ADM Agent 2 (on-premises)
Citrix ADC 5
Citrix ADC 6
Citrix ADC 7
Citrix ADC 8
Enterprise Data Center

The public cloud has four ADC instances and two Citrix Application Delivery and Management agents. The enterprise data center also have four ADC instances and two Citrix Application Delivery and Management agents. Each agent is configured with two ADC instances.

The agents receive data directly from the configured instances. After agent receives the data, agent processes the data and sends to the Citrix Application Delivery and Management in a compressed format. Agents communicate with the Citrix Application Delivery and Management server over a secure channel.

On public cloud, when **Citrix Application Delivery and Management Agent 1** becomes inactive (DOWN state), agent failover occurs. Citrix Application Delivery and Management redistributes the ADC instances of **Citrix Application Delivery and Management Agent 1** with **Citrix Application De-**

livery and Management Agent 2. The instance redistribution occurs on an enterprise data center if one of the agents fails in the data center.

To install a Citrix Application Delivery and Management agent, see Install the Citrix Application Delivery and Management Agent.

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management redistributes the ADC instances of the inactive agent with other active agents.

> **Important**
>
> - Citrix Application Delivery and Management agent failover does not consider CPX instances.
> - Ensure Agent Failover feature is enabled on your account. To enable this feature, see Enable or disable Citrix Application Delivery and Management 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 Citrix Application Delivery and Management GUI:

1. Navigate to **Infrastructure > Instances > Agents**.
2. Select an agent that you want to attach to a site.
3. Specify the site from the list. If you want to add a new site, click **Add**.
4. Click **Save**.

To achieve an agent failover, select Citrix Application Delivery and Management agents one by one and attach to the same site.

For example, two agents 10.106.1xx.2x and 10.106.1xx.7x are attached and operational in the Bangalore site. If one agent becomes inactive, Citrix Application Delivery and Management detects it and displays the state as down.

When a Citrix Application Delivery and Management agent becomes inactive (Down state) in a site, Citrix Application Delivery and Management waits for few minutes for the agent to become active (Up state). If the agent remains inactive, Citrix Application Delivery and Management automatically redistributes the instances among available agents in the same site. This redistribution may take approximately 10-15 minutes.

Citrix Application Delivery and Management triggers instance redistribution every 30 minutes to balance the load among active agents in the site.

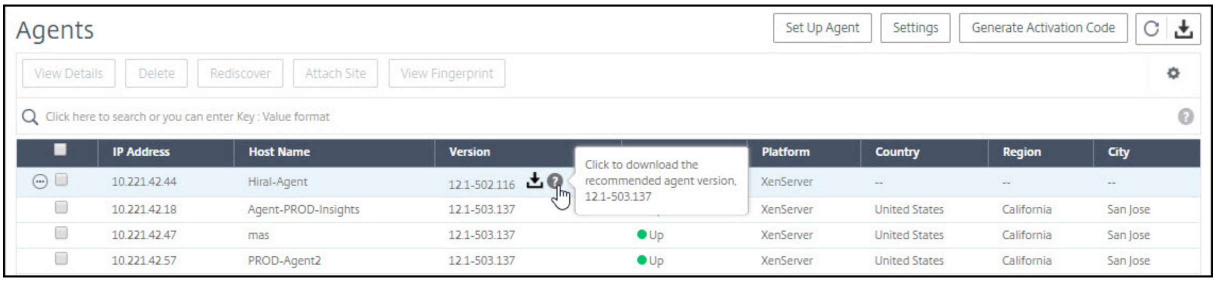
The instances attached and automatically reconfigured to agents in the same site for trap destination, syslog server, and analytics.

Configuring agent upgrade settings

September 24, 2021

In Citrix Application Delivery and Management, agents running on software version 12.0 build 507.110 and later are automatically upgraded to newer and recommended versions by Citrix Application Delivery and Management. The agent is upgraded either when a new version is available or at a time specified by you.

You can view the current version and the recommended version of your agents by navigating to **Infrastructure > Instances > Agents**.



Agents

☐	IP Address	Host Name	Version		Platform	Country	Region	City
☐	10.221.42.44	Hiral-Agent	12.1-502.116		XenServer	--	--	--
☐	10.221.42.18	Agent-PROD-Insights	12.1-503.137		XenServer	United States	California	San Jose
☐	10.221.42.47	mas	12.1-503.137	● Up	XenServer	United States	California	San Jose
☐	10.221.42.57	PROD-Agent2	12.1-503.137	● Up	XenServer	United States	California	San Jose

Click to download the recommended agent version, 12.1-503.137

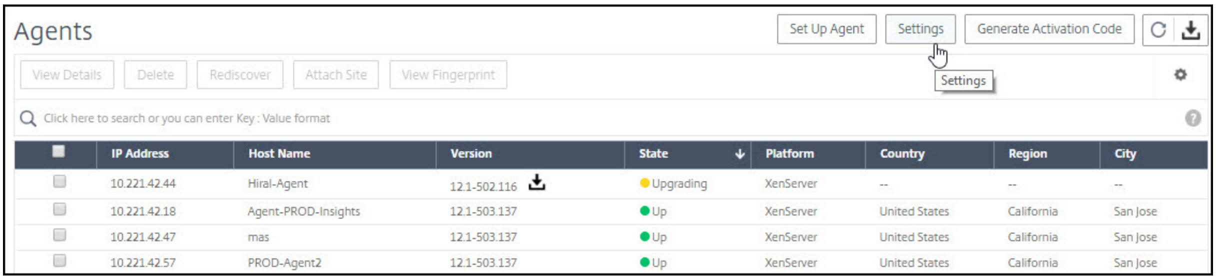
By default, an agent is upgraded automatically when a newer version is available. However, you can specify the time when you want the agent upgrade to happen.

If you select a specific time, the agents are upgraded at that specified time, but in the time zone where your agents are deployed.

During the upgrade, there might be a downtime of approximately 30 minutes.

To configure agent upgrade settings:

Navigate to **Infrastructure > Instances > Agents**, click **Settings**.

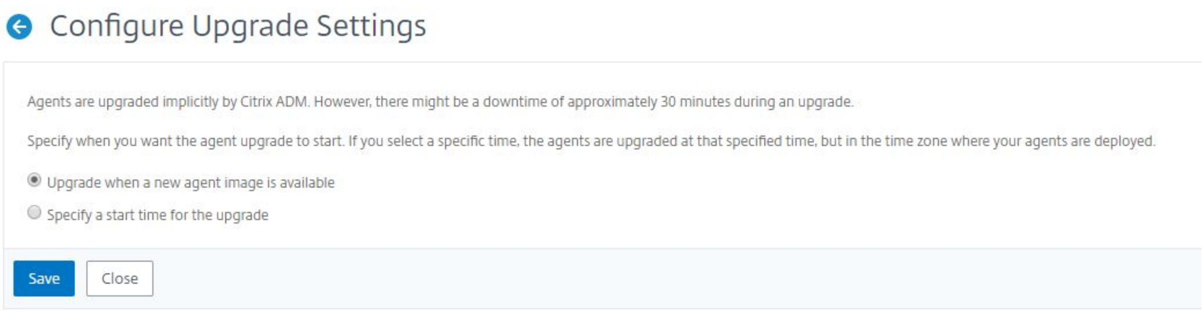


Agents

☐	IP Address	Host Name	Version	State	Platform	Country	Region	City
☐	10.221.42.44	Hiral-Agent	12.1-502.116	● Upgrading	XenServer	--	--	--
☐	10.221.42.18	Agent-PROD-Insights	12.1-503.137	● Up	XenServer	United States	California	San Jose
☐	10.221.42.47	mas	12.1-503.137	● Up	XenServer	United States	California	San Jose
☐	10.221.42.57	PROD-Agent2	12.1-503.137	● Up	XenServer	United States	California	San Jose

Specify when you want the agent upgrade to start. You can choose to upgrade when a new agent is available, or you can set a specific time when you want Citrix Application Delivery and Management to implicitly upgrade the agent. The time you set is specific to the agent time zone.

Click **Save** to save your settings. These settings persist for future agent upgrades until you change the settings.



Configure Upgrade Settings

Agents are upgraded implicitly by Citrix ADM. However, there might be a downtime of approximately 30 minutes during an upgrade.

Specify when you want the agent upgrade to start. If you select a specific time, the agents are upgraded at that specified time, but in the time zone where your agents are deployed.

● Upgrade when a new agent image is available

○ Specify a start time for the upgrade

Adding instances

September 28, 2021

You can add instances either while setting up the Citrix Application Delivery and Management for the first time or later.

Instances are Citrix appliances or virtual appliances that you want to discover, manage, and monitor from Citrix Application Delivery and Management. You can add the following Citrix appliances and virtual appliances to Citrix Application Delivery and Management:

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix Secure Web Gateway

To add instances, you must specify either the host name or IP address of each Citrix ADC instance, or a range of IP addresses. For SD-WAN instances, specify the IP address of each instance, or a range of IP addresses.

Specify an instance profile that Citrix Application Delivery and Management can use to access the instance. This instance profile contains the user name and password of the instances that you want to add to the service. For each instance type, a default profile is available. For example, the ns-root-profile is the default profile for Citrix ADC instances. The default Citrix ADC administrator credentials define this profile. 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 access the GUIs of Citrix ADC instances from the Citrix Application Delivery and Management after adding the instances in the Citrix Application Delivery and Management. To access the Citrix ADC instances from the Citrix Application Delivery and Management, you must be connected to the Citrix network.

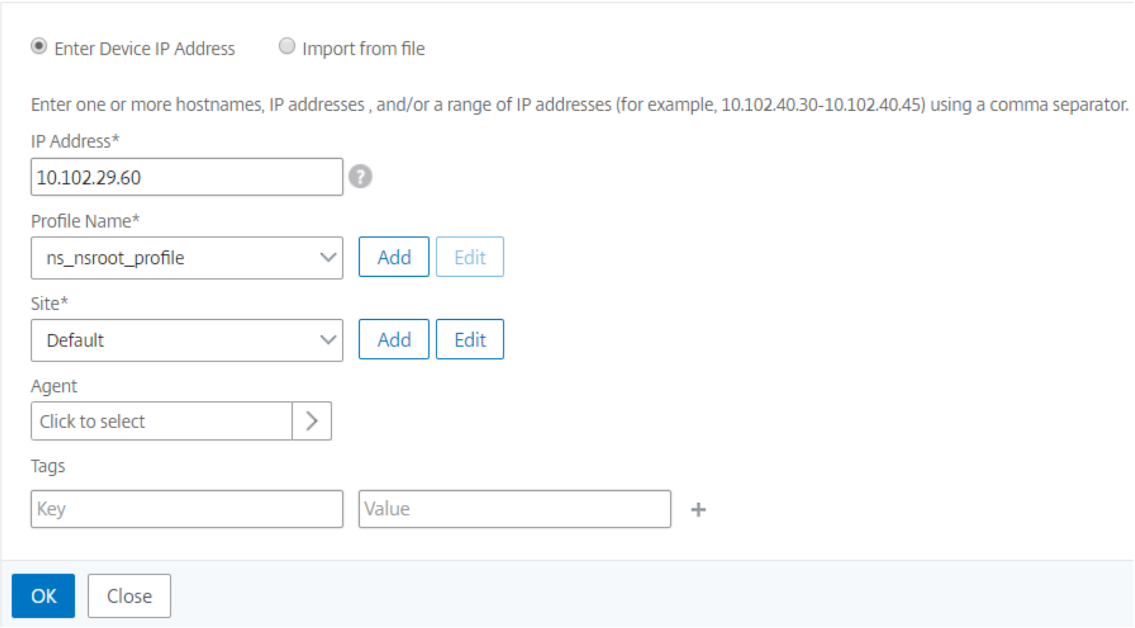
> **Note**
>
> - To add Citrix ADC instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on Citrix Application Delivery and Management, the cluster IP address represents the cluster.
> - For the Citrix ADC instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

To add a Citrix ADC instance to Citrix Application Delivery and Management

> **Note**
>
> Perform this task to add all other ADC instances except the ADC CPX instance.

1. Navigate to **Infrastructure > Instances > Citrix ADC**. Under Instances, select the type of instance you want to add (for example, Citrix ADC VPX) and click **Add**.
2. Select one of the following options:
    - **Enter Device IP address** - For Citrix ADC instances, specify either the host name or IP address of each instance, or a range of IP addresses.
    - **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.
3. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
4. From **Profile** Name, select the appropriate instance profile, or create a profile by clicking the **+** icon.
5. From **Site**, select the site where you want the instance to be added.
6. From **Agent**, select the agent with which you want to associate the instances, and then click **OK**.

    If there is only one agent configured on your Citrix Application Delivery and Management, that agent is selected by default.



● Enter Device IP Address ○ Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

IP Address*: 10.102.29.60

Profile Name*: ns_nsroot_profile

Site*: Default

Agent: Click to select

Tags: Key Value

To add Citrix ADC CPX instance in Citrix Application Delivery and Management

1. Navigate to **Infrastructure > Instances**. Under **Instances**, select **Citrix ADC** and select the CPX tab.

2. Click **Add**.

3. Select one of the following options:

   - **Enter Device IP address**. Specify either the host name or IP address of each instance, or a range of IP addresses.

   - **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. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.

5. In the **Routable IP/Docker IP** field, enter the IP address. The IP address can be either the Citrix ADC CPX instance (if it is reachable) or the Docker host.

6. In the **Profile Name** field, select the appropriate instance profile, or create a profile by clicking the + icon.

   > **Note**
   >
   > When you are creating a profile, ensure to specify the HTTP, HTTPS, SSH, and SNMP port details of the host. You can also specify the range of ports that are published by the host in the Start Port and Number of ports field.

7. As an option, select the site where you want to deploy the CPX instance. You can create a site also by clicking **Add**.
8. If available, select the Citrix Application Delivery and Management agent from the list of agents.
9. Click **OK** to initiate the process of adding instances to Citrix Application Delivery and Management.

   > **Note**
   >
   > If you want to rediscover an instance, perform the following steps:
   >
   > a) Navigate to **Infrastructure > Instances > Citrix ADC** > **CPX**.
   > b) Select the instance you want to rediscover.
   > c) From the **Select Action** list, click **Rediscover**.

To add a standalone Citrix ADC BLX instance in Citrix Application Delivery and Management

A standalone Citrix ADC BLX instance is a single instance that is running on the dedicated host Linux server.

1. Navigate to **Infrastructure > Instances > Citrix ADC**.
2. In the **BLX** tab, click **Add**.
3. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
4. Select the **Standalone** option from the **Instance Type** list.
5. In the **IP address** field, specify the IP address of the BLX instance.
6. In the **Host IP address** field, specify the IP address of the Linux server where the 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.

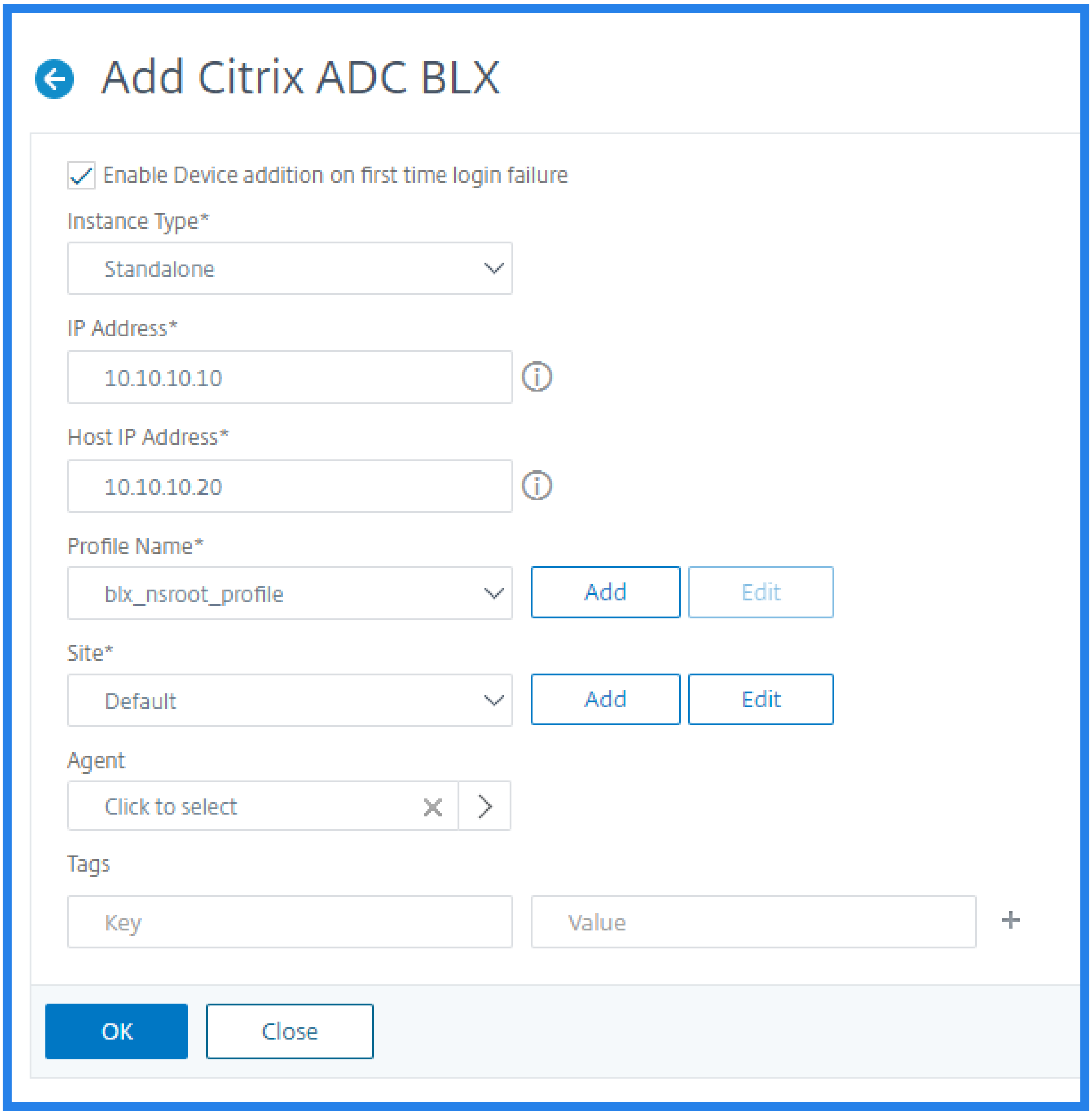
8. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.

9. In the **Agent** list, select the Citrix Application Delivery and Management agent to which you want to associate the instance.

If there is only one agent configured on your Citrix Application Delivery and Management, that agent is selected by default.

10. Click **OK**.



Add Citrix ADC BLX

☑ Enable Device addition on first time login failure

Instance Type*: Standalone

IP Address*: 10.10.10.10

Host IP Address*: 10.10.10.20

Profile Name*: blx_nsroot_profile

Site*: Default

Agent: Click to select

Tags: Key, Value

To add high-availability Citrix ADC BLX instances in Citrix Application Delivery and Management

The high-availability Citrix ADC 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. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
3. Select the **High Availability** 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 **Peer IP address** field, specify the IP address of the peer BLX instance.
7. In the **Peer Host IP address** field, specify the IP address of the Linux server where the peer BLX instance is hosted.
8. 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.

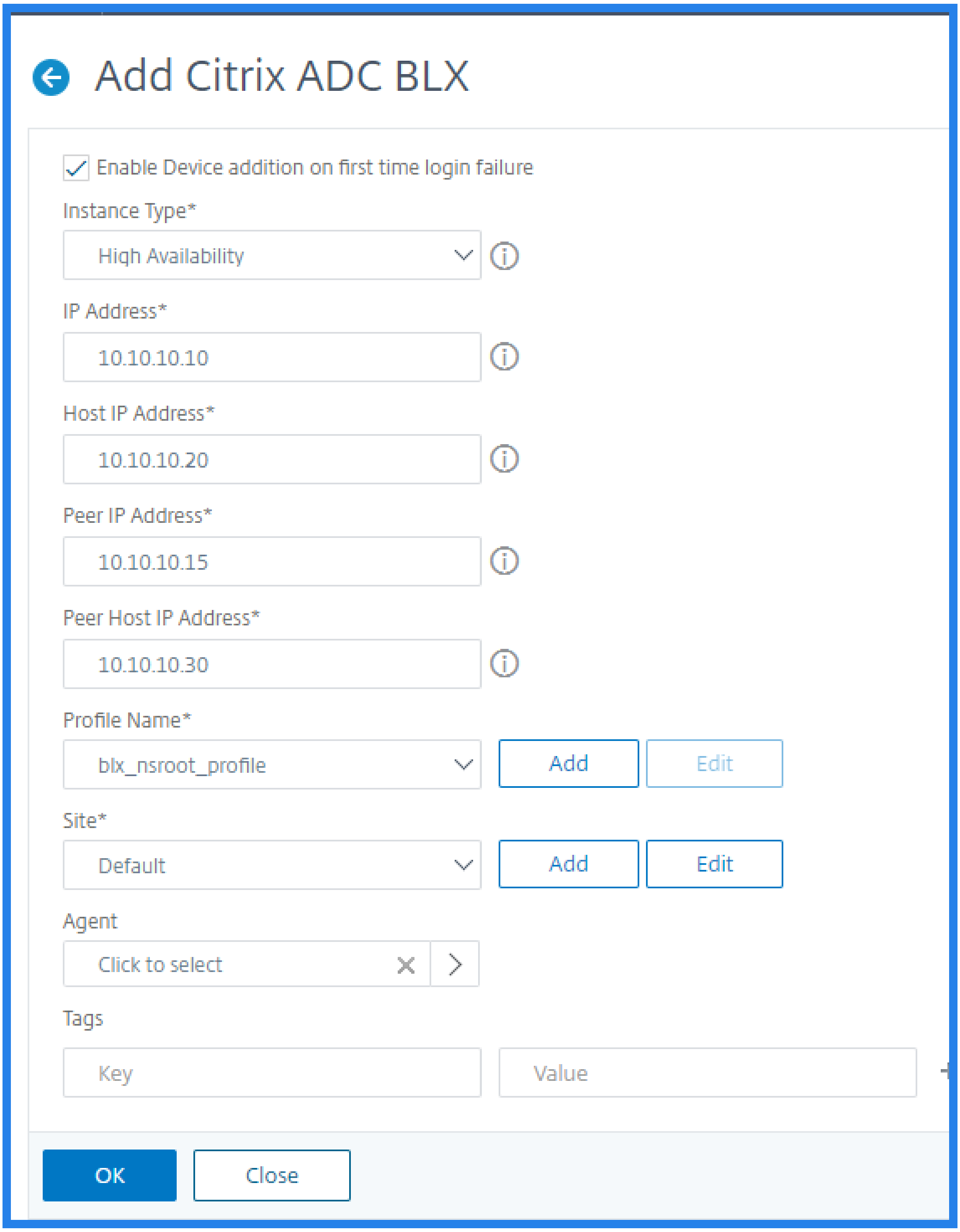
9. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.

10. In the **Agent** list, select the Citrix Application Delivery and Management agent to which you want to associate the instance.

    If there is only one agent configured on your Citrix Application Delivery and Management, that agent is selected by default.

11. Click **OK**.



Add Citrix ADC BLX

☑ Enable Device addition on first time login failure

Instance Type*: High Availability

IP Address*: 10.10.10.10

Host IP Address*: 10.10.10.20

Peer IP Address*: 10.10.10.15

Peer Host IP Address*: 10.10.10.30

Profile Name*: blx_nsroot_profile

Site*: Default

Agent: Click to select

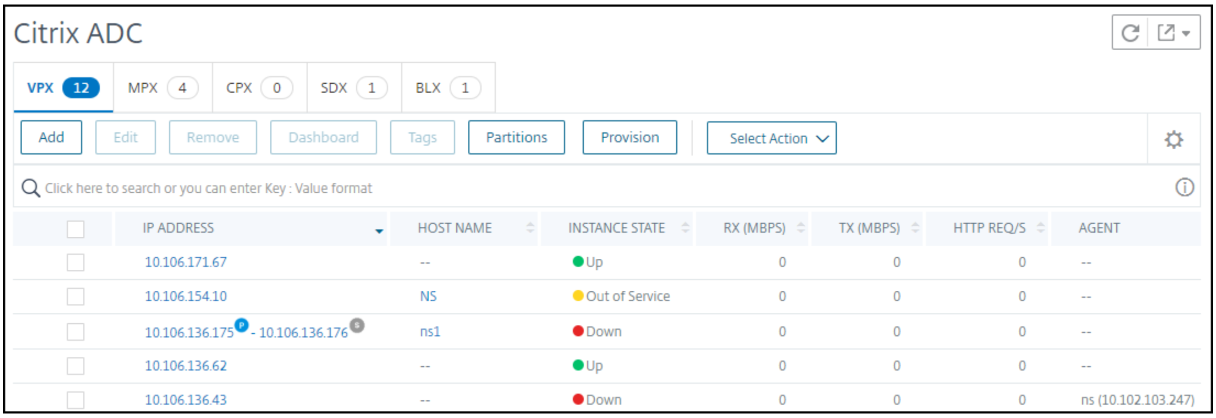
Tags: Key Value

To access an instance GUI from the Citrix Application Delivery and Management

1. Navigate to **Infrastructure > Instances** > **Citrix ADC**.

2. Select the type of instance you want to access (for example, VPX, MPX, CPX, SDX, or BLX).

3. Click the required Citrix ADC IP address or host name.



□	IP ADDRESS	HOST NAME	INSTANCE STATE	RX (MBPS)	TX (MBPS)	HTTP REQ/S	AGENT
□	10.106.171.67	--	● Up	0	0	0	--
□	10.106.154.10	NS	● Out of Service	0	0	0	--
□	10.106.136.175 P - 10.106.136.176 S	ns1	● Down	0	0	0	--
□	10.106.136.62	--	● Up	0	0	0	--
□	10.106.136.43	--	● Down	0	0	0	ns (10.102.103.247)

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

Resolve instance warnings

A warning sign appears on the instance for the following reasons:

- **Login failed** - When you add an instance without valid credentials, it appears in DOWN state, with a Login failed warning. Specify the correct credentials to manage the instance in Citrix Application Delivery and Management.

  If the instance is unlicensed, the **License** option appears when you select the instance. Click **License** to apply the license to an instance from the license pool.

- **Unlicensed instance with HTTPS profile** - If an unlicensed instance uses only HTTPS connection, apply license to an instance from the ADC GUI.

Adding HAProxy instances

September 25, 2021

You can add an HAProxy instance provisioned on a host by providing the details of the host while setting up the Citrix Application Delivery and Management for the first time or later.

Citrix Application Delivery and Management supports HAProxy version 1.6.3 or later and you can add HAProxy instances provisioned on the following hosts to Citrix Application Delivery and Management:

- Ubuntu 14.0 or later
- Red Hat Enterprise Linux (RHEL) 6.0 or later
- SUSE 11.0 or later
- CentOS 6.0 or later
- Amazon Linux AMI

> **Note**
>
> Ensure that the host is not configured with a customized prompt string for the shell. The shell must have either **$** or **#** as the prompt string.

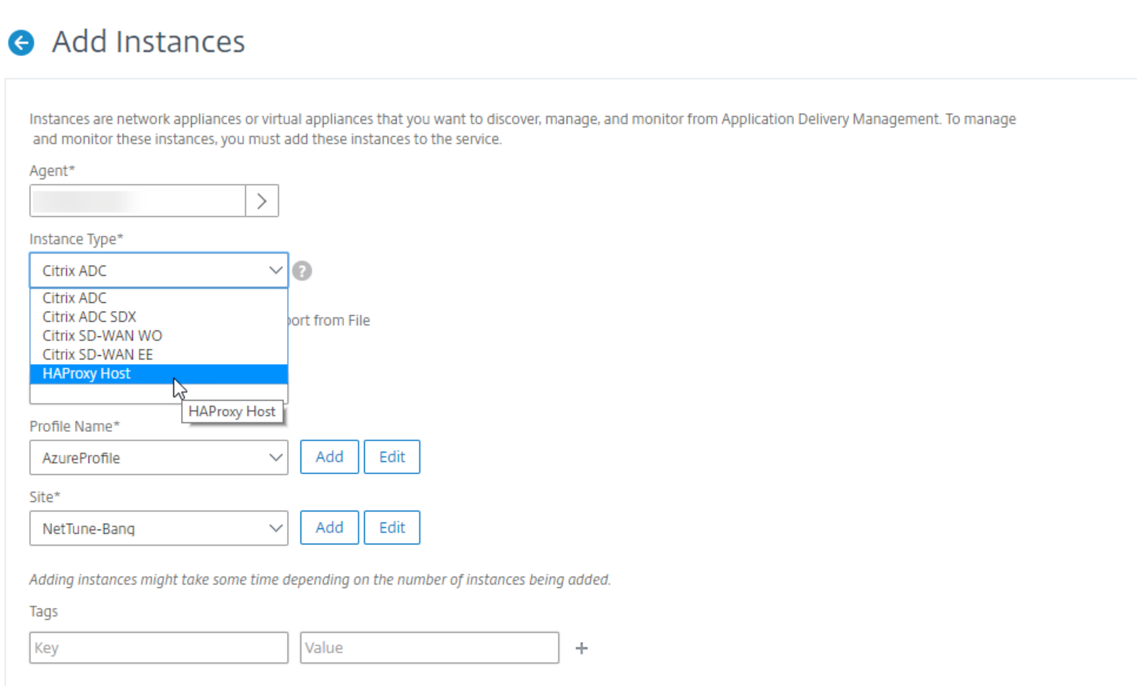
To add HAProxy instances, you must specify the IP address of the host on which you have provisioned the HAProxy instances. You must then specify an HAProxy profile that Citrix Application Delivery and Management can use to access the host. This HAProxy profile contains the user name and password of the host that you want to add to the service.

> **Note**
>
> Ensure that the user account associated with the user name has:
>
> - Privileges to run the ps command to list all the HAProxy instances on the host.
> - Permission to restart the HAProxy instance on the host.

After you add the host on which you have provisioned the HAProxy instances to Citrix Application Delivery and Management, Citrix Application Delivery and Management accesses the host using SSH protocol. It automatically discovers the HAProxy instances provisioned on the host and adds them to Citrix Application Delivery and Management inventory. It also discovers all the front ends, back ends, and servers configured on the HAProxy instances, and treats the front ends as discovered applications.

To add HAProxy instances to Citrix Application Delivery and Management:

1. Navigate to **Infrastructure > Instances** and click Total Instances. On the Instances section, click **Add** at the top right corner of the page. On the Add Instances page, from the **Instance Type** drop-down list, select **HAProxy Host**.



Add Instances

Instances are network appliances or virtual appliances that you want to discover, manage, and monitor from Application Delivery Management. To manage and monitor these instances, you must add these instances to the service.

Agent*

Instance Type*

Citrix ADC

Profile Name*

AzureProfile

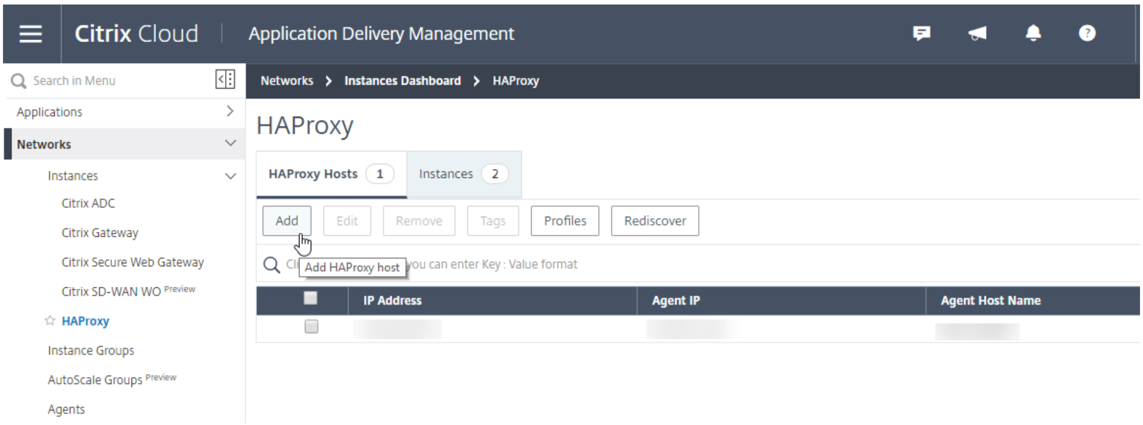
Site*

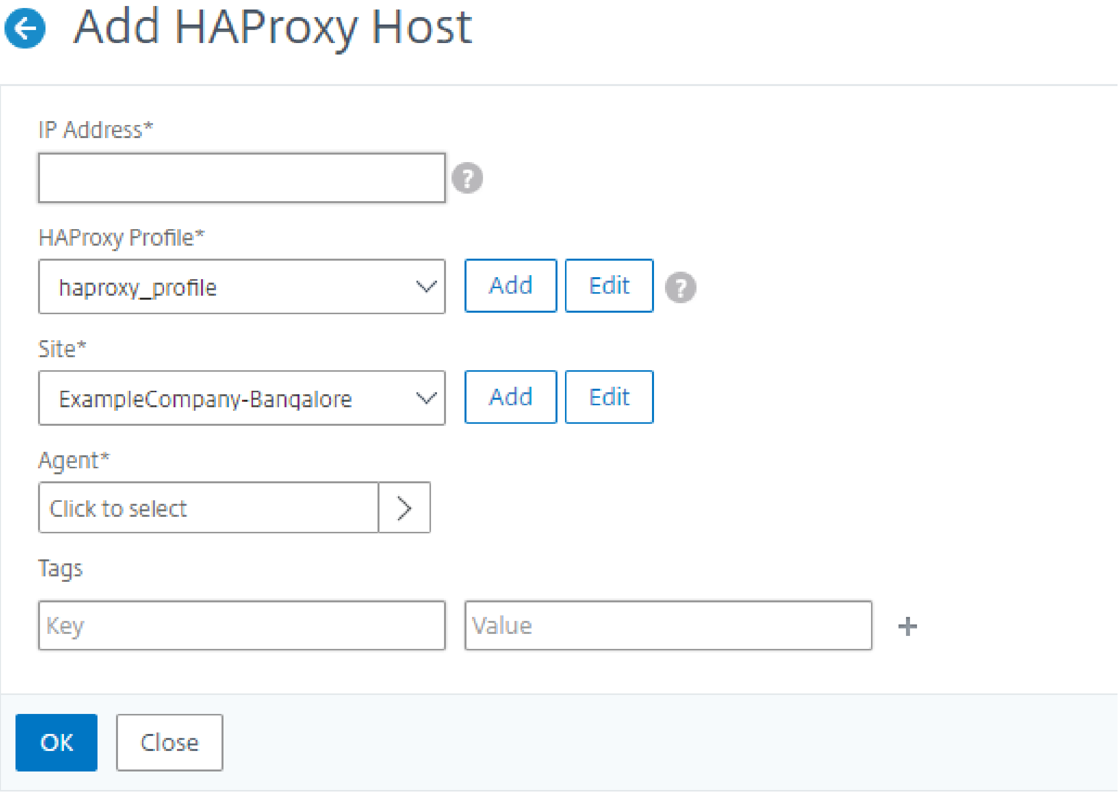
NetTune-Banq

Adding instances might take some time depending on the number of instances being added.

Tags

Alternatively, navigate to **Infrastructure > Instances**. Under Instances, select **HAProxy** and click **Add**.





Add HAProxy Host

IP Address*

HAProxy Profile*: haproxy_profile

Site*: ExampleCompany-Bangalore

Agent*: Click to select

Tags: Key / Value

2. In the **IP Address** field, enter the IP address of the host on which you have provisioned the HAProxy instances.

3. In the **HAProxy Profile** drop-down list, select an existing HAProxy profile or create and select a new HAProxy profile. To create an HAProxy profile, click the **+** icon.

4. In the **Add HAProxy Profile** dialog box, do the following:

a) In the **Profile Name** field, enter a unique name for the HAProxy profile.

b) In the **User Name** field, enter the user name that is used to access the host using the SSH protocol.

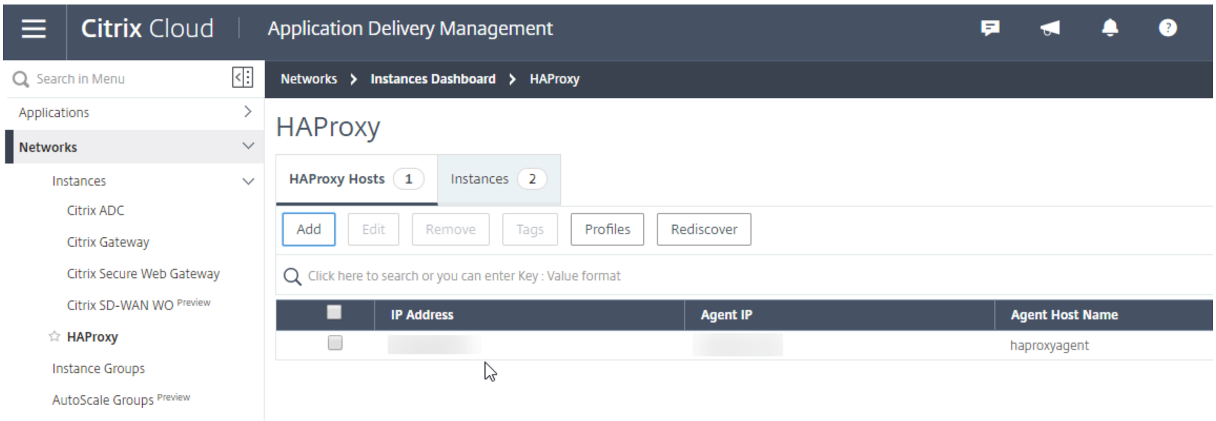
> **Note**
>
> Ensure that the user account associated with the user name has:
>
> - Privileges to run the ps command to list all the HAProxy instances on the host.
> - Permission to restart the HAProxy instance on the host.

c) In the **Password** field, enter the password of the host.

d) Click **Create**.

5. Specify a Site for the instance.
6. In the **Agent** drop-down list, select the agent with which you want to associate the instances.
7. In the Tags field, specify a key and associated values for the HAProxy instance. Tags help you to classify and identify the instances. For example, specify Location as the key and Bangalore as the Value. You can also add multiple values for a key. Separate the multiple values with commas.
8. Select **OK**.

Citrix Application Delivery and Management discovers the HAProxy instances provisioned on the host, and you can view all the HAProxy instances on the **Instances** tab in the **Infrastructure > Instances > HAProxy** page.



□	IP Address	Agent IP	Agent Host Name
□	[redacted]	[redacted]	haproxyagent

Configuring syslog on instances

September 24, 2021

The syslog protocol provides a transport to allow the Citrix ADC instances to send event notification messages to Citrix Application Delivery and Management, which is configured as a collector or the syslog server for these messages.

You can monitor the syslog events generated on your Citrix ADC instances if you have configured your device to redirect all syslog messages to Citrix Application Delivery and Management. To monitor syslog events, you need to first configure Citrix Application Delivery and Management as the syslog server for your Citrix ADC instance. After the instance is configured, all the syslog messages are redirected to Citrix Application Delivery and Management, so that these logs can be displayed to the user in a structured manner.

Syslog uses the User Datagram Protocol (UDP), port 514, for communication, and because UDP is a connectionless protocol it does not provide any acknowledgment back to the instances. The syslog packet size is limited to 1024 bytes and carries the following information:

- Facility
- Severity
- Host name
- Timestamp
- Message

In Citrix Application Delivery and Management, you must configure facility and log severity levels on the instances.

- **Facility** - Syslog messages are broadly categorized on the basis of the sources that generate them. These sources can be the operating system, the process, or an application. These categories are called facilities and are represented by integers. For example, 0 is used by kernel messages, 1 is used by user-level messages, 2 is used by the mail system, and so on. The local use facilities (from local0 to local7) are not reserved and are available for general use. Hence, the processes and applications that do not have pre-assigned facility values can be directed to any of the eight local use facilities.

- **Severity** - The source or facility that generates the syslog message also specifies the severity of the message using a single-digit integer, as shown below:

  ```
  1 - Emergency: System is unusable.

  2 - Alert: Action must be taken immediately.

  3 - Critical: Critical conditions.

  4 - Error: Error conditions.

  5 - Warning: Warning conditions.

  ```

```
6 - Notice: Normal but significant condition.

7 - Informational: Informational messages.

8 - Debug: Debug-level messages.
```

To configure syslog on Citrix ADC instances:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances**.
2. Select the Citrix ADC instance from which you want the syslog messages to be collected and displayed in Citrix Application Delivery and Management.
3. In the **Action** drop-down 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**.

This configures all the syslog commands in the Citrix ADC instance, and Citrix Application Delivery and Management starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**.

Logstream overview

September 24, 2021

Citrix ADC instances generate AppFlow records and are a central point of control for all application traffic in the data center. **IPFIX** and **Logstream** are the protocols that transport these AppFlow records from Citrix ADC instances to Citrix Application Delivery and Management. For more information, see AppFlow.

- **IPFIX** is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. **IPFIX** uses UDP protocol which is unreliable transport protocol used for data flow in one direction. Since IPFIX uses UDP protocol, adhering to IPFIX standard results in processing more resources in Citrix Application Delivery and Management.

- **Logstream** is a Citrix-owned protocol that is used as one of the transport modes to efficiently transfer the analytics log data from Citrix ADC instances to Citrix Application Delivery and Management. **Logstream** uses reliable TCP protocol and requires lesser resources in processing the data.

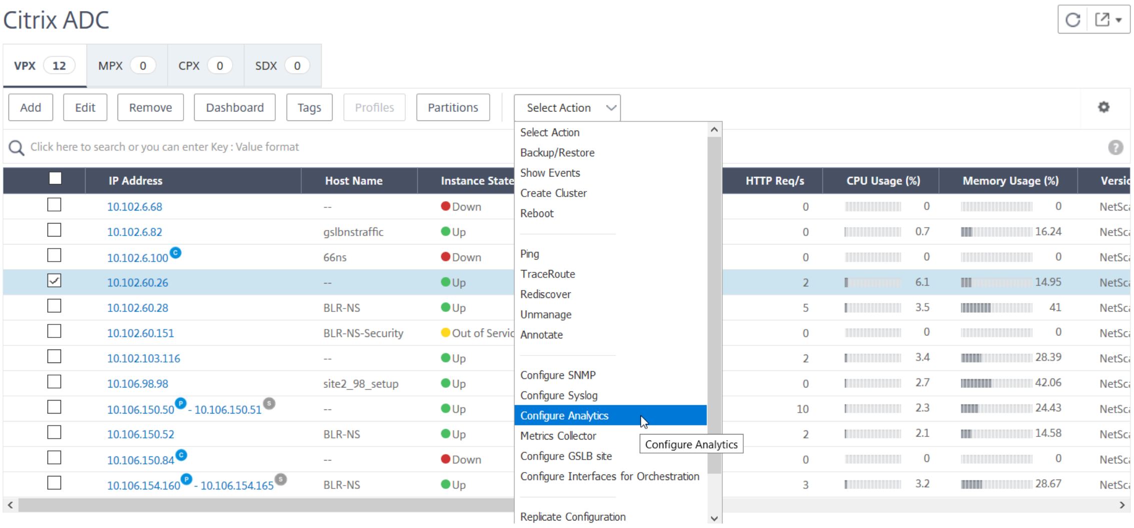
For Citrix ADC between **11.1 Build 47.14 and 11.1 Build 62.8**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights.

For Citrix ADC version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

> **Note**
>
> The Citrix Application Delivery and Management version and build must be **equal to or higher** than your Citrix ADC version and build. For example, if you have installed Citrix ADC 12.1 Build 50.28/50.31, then ensure you have installed Citrix Application Delivery and Management 12.1 Build 50.39 or later.

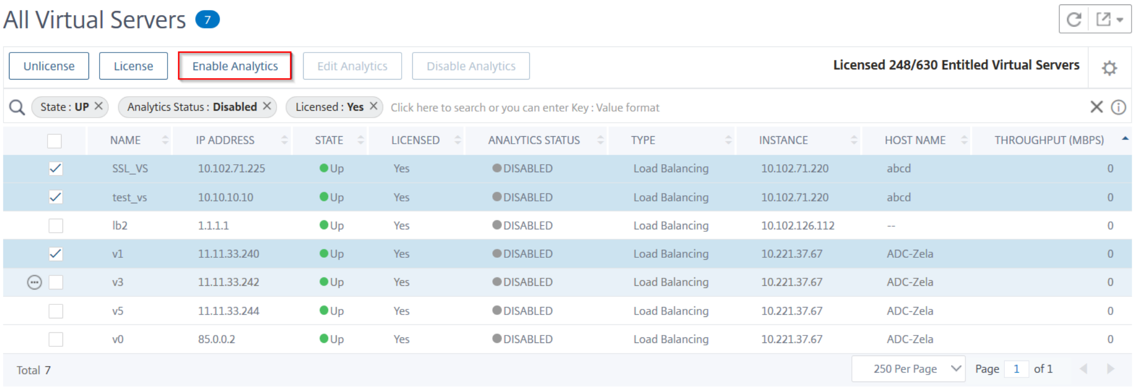
Enable Logstream as Transport Mode

1. Navigate to **Infrastructure > Instances**, and select the ADC instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.



☐	IP Address	Host Name	Instance State	HTTP Req/s	CPU Usage (%)	Memory Usage (%)	Versi
☐	10.102.6.68	--	● Down	0	0	0	NetSc
☐	10.102.6.82	gslbnstraffic	● Up	0	0.7	16.24	NetSc
☐	10.102.6.100 C	66ns	● Down	0	0	0	NetSc
☑	10.102.60.26	--	● Up	2	6.1	14.95	NetSc
☐	10.102.60.28	BLR-NS	● Up	5	3.5	41	NetSc
☐	10.102.60.151	BLR-NS-Security	● Out of Servic	0	0	0	NetSc
☐	10.102.103.116	--	● Up	2	3.4	28.39	NetSc
☐	10.106.98.98	site2_98_setup	● Up	0	2.7	42.06	NetSc
☐	10.106.150.50 P - 10.106.150.51 S	--	● Up	10	2.3	24.43	NetSc
☐	10.106.150.52	BLR-NS	● Up	2	2.1	14.58	NetSc
☐	10.106.150.84 C	--	● Down	0	0	0	NetSc
☐	10.106.154.160 P - 10.106.154.165 S	BLR-NS	● Up	3	3.2	28.67	NetSc

3. Select the virtual servers and then click **Enable Analytics**.



Licensed 248/630 Entitled Virtual Servers

State : **UP** ✕ Analytics Status : **Disabled** ✕ Licensed : **Yes** ✕ Click here to search or you can enter Key : Value format

☐	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE	HOST NAME	THROUGHPUT (MBPS)
☑	SSL_VS	10.102.71.225	● Up	Yes	● DISABLED	Load Balancing	10.102.71.220	abcd	0
☑	test_vs	10.10.10.10	● Up	Yes	● DISABLED	Load Balancing	10.102.71.220	abcd	0
☐	lb2	1.1.1.1	● Up	Yes	● DISABLED	Load Balancing	10.102.126.112	--	0
☑	v1	11.11.33.240	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
☐	v3	11.11.33.242	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
☐	v5	11.11.33.244	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
☐	v0	85.0.0.2	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0

Total 7 250 Per Page Page 1 of 1

4. On the **Enable Analytics** window:

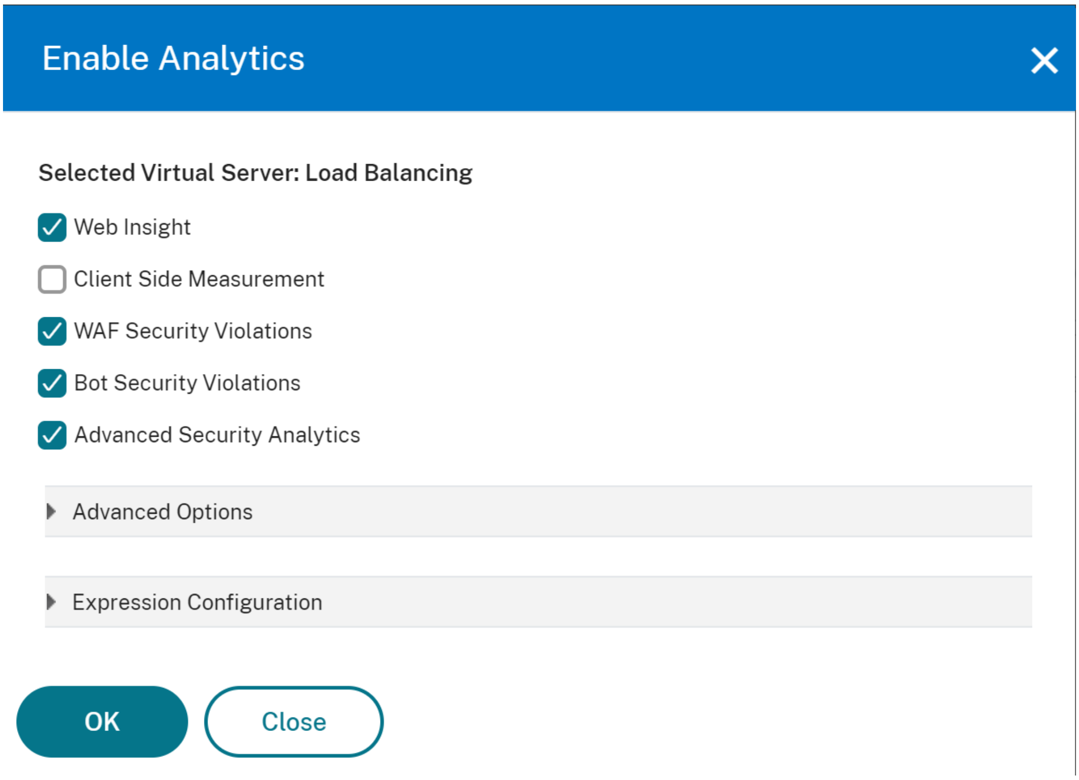
   a) Select the insight types (Web Insight or WAF Security Violations or Bot Security Violations)

b) Select **Logstream** as Transport Mode

> **Note**
>
> For Citrix ADC between **11.1 Build 47.14 and 11.1 Build 62.8**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights. For Citrix ADC version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

c) The Expression is true by default

d) Click **OK**



Enable Analytics

Selected Virtual Server: Load Balancing

☑ Web Insight

□ Client Side Measurement

☑ WAF Security Violations

☑ Bot Security Violations

☑ Advanced Security Analytics

> **Note**
>
> - If you select virtual servers that are not licensed, then Citrix Application Delivery and Management 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.

The following table describes the features of Citrix Application Delivery and Management that supports **Logstream** as the transport mode:

Feature	**IPFIX**	**Logstream**
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

How to assign more permissions to delegated admin users

September 25, 2021

When the first user of your organization signs up and logs on to Citrix Application Delivery and Management, this user is assigned the super admin privileges. Every subsequent user that logs on is assigned a delegated admin role by default. A delegated admin does not have the permission to view and perform any tasks related to user administration or RBAC settings.

However, you can assign super admin privileges or specific non-super admin roles to a delegated admin so that the admin is able to perform tasks related to user administration.

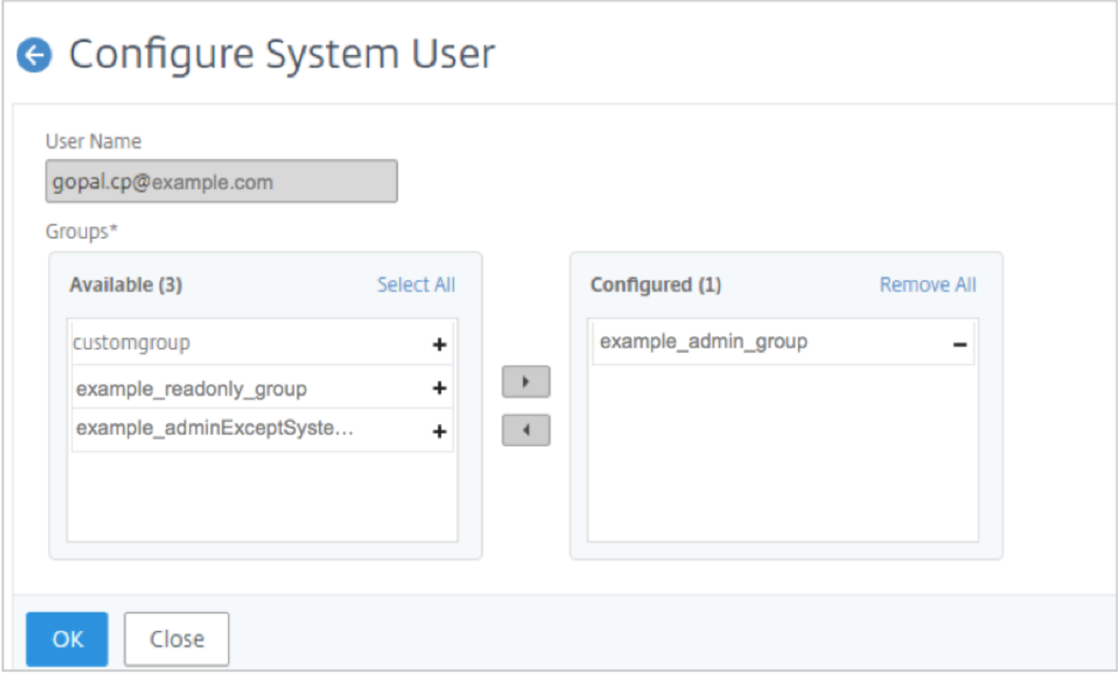
For detailed information about role-based access control see Configuring Role-Based Access Control.

Assigning Super Admin Permissions to a Delegated Admin

To assign super admin permissions to a delegated admin, a super admin has to assign the default admin group to a delegated admin user. Perform the following tasks:

1. Log on to Citrix Application Delivery and Management as the super admin.
2. Navigate to **Account** > **User Administration** > **Users**.
3. Select the user name of the delegated admin and click **Edit**.

4. Assign the group ***<tenant_name>*_admin_group** to the delegated admin and click **OK**. For example, in the following image, "example_admin_group" is assigned to a delegated admin user.



Configure System User

User Name: gopal.cp@example.com

Groups*

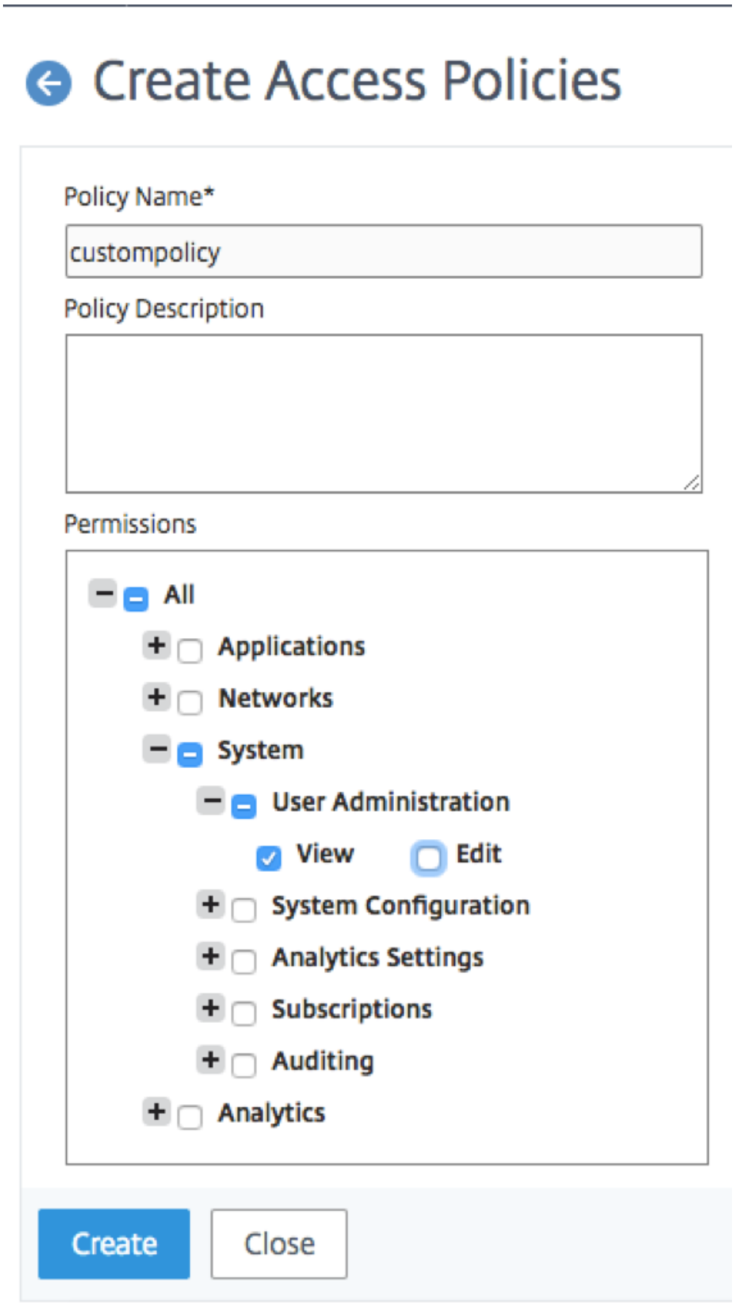
Available (3): customgroup, example_readonly_group, example_adminExceptSyste...

Configured (1): example_admin_group

Assigning Custom Role to a Delegated Admin

To assign any custom role to a delegated admin, the super admin has to create a group, role, and policy and assign to the delegated admin user. This ensures that the delegated admin has only the required permissions. Perform the following tasks:

1. Log on to Citrix Application Delivery and Management as the super admin.
2. Navigate to **Account** > **User Administration** > **Access Policies**. Select **Add** to create an access policy with the required permissions for the delegated admin. In this example, an access policy `custompolicy` is created that allows view access to User Administration settings.



Create Access Policies

Policy Name*

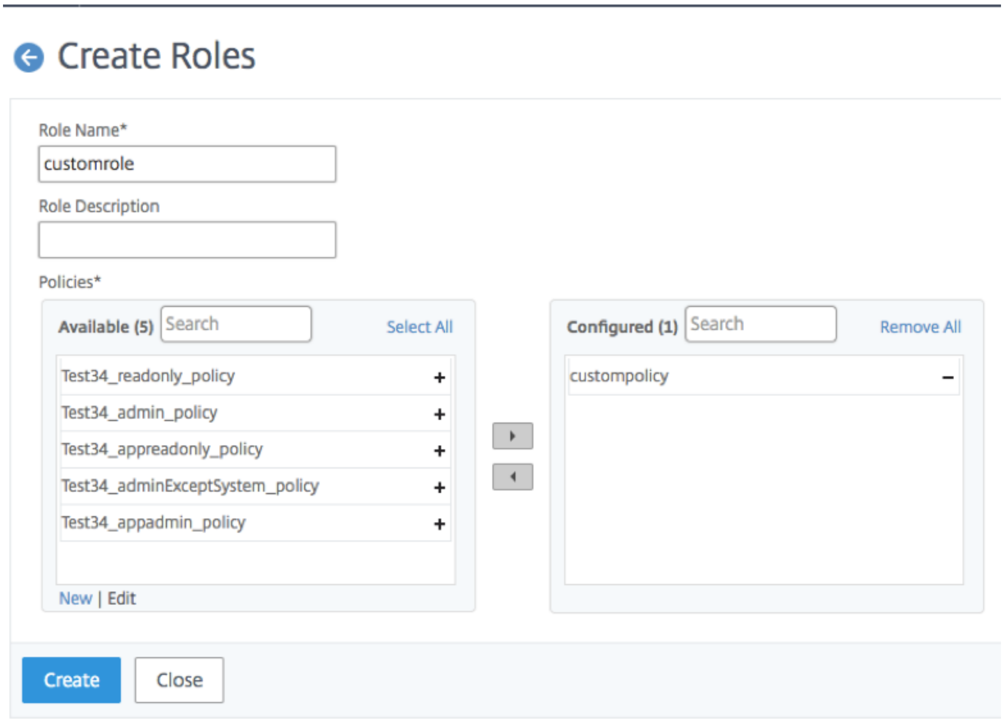
custompolicy

Policy Description

Permissions

- ▣ All
  - □ Applications
  - □ Networks
  - ▣ System
    - ▣ User Administration
      - ☑ View □ Edit
    - □ System Configuration
    - □ Analytics Settings
    - □ Subscriptions
    - □ Auditing
  - □ Analytics

3. Navigate to **Account** > **User Administration** > **Roles**. Select **Add** to create a role and bind this role to the access policy that you created in the previous step. In this example, a role `customrole` is created and bound to the `custompolicy` access policy.



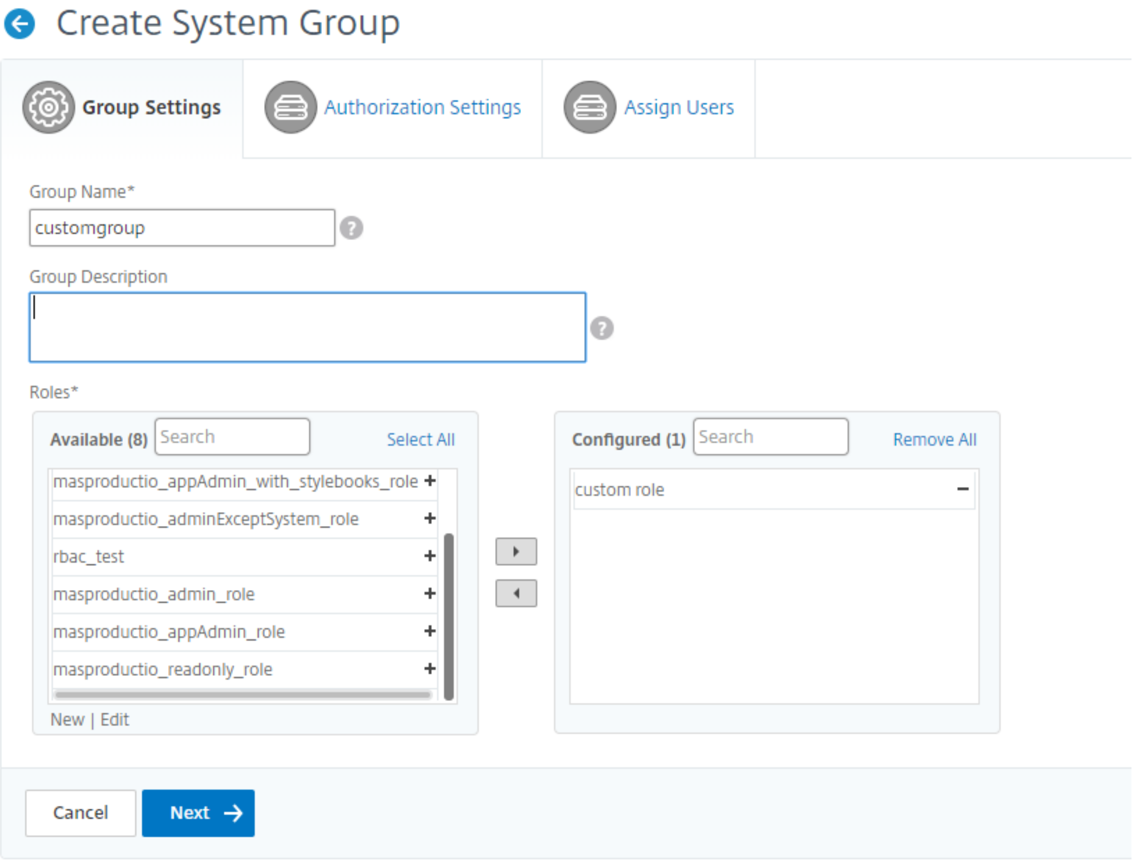
Create Roles

Role Name*: customrole

Role Description:

Policies*

4. Navigate to **Account** > **User Administration** > **Groups**. Select **Add** to create a group and bind this group to the role you created in the previous step. In this example, the group "custom group" is created and bound to the role "custom role."



Group Name*
customgroup

Group Description

Roles*

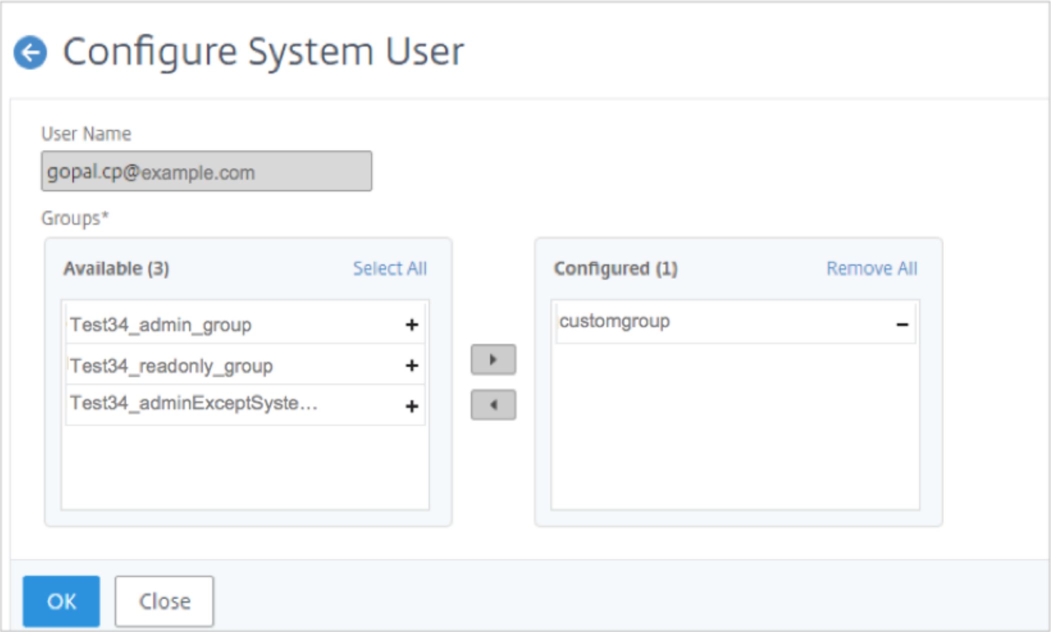
Available (8)

masproductio_appAdmin_with_stylebooks_role
masproductio_adminExceptSystem_role
rbac_test
masproductio_admin_role
masproductio_appAdmin_role
masproductio_readonly_role

Configured (1)

custom role

5. Navigate to **Account** > **User Administration** > **Users**
6. Select the user name of the delegated admin and click **Edit**.
7. Assign the group you created in the previous step to the delegated admin user. In this example, the delegated admin user is assigned the group `customgroup`.



Configure System User

User Name: gopal.cp@example.com

Groups*

Integration with the ServiceNow instance

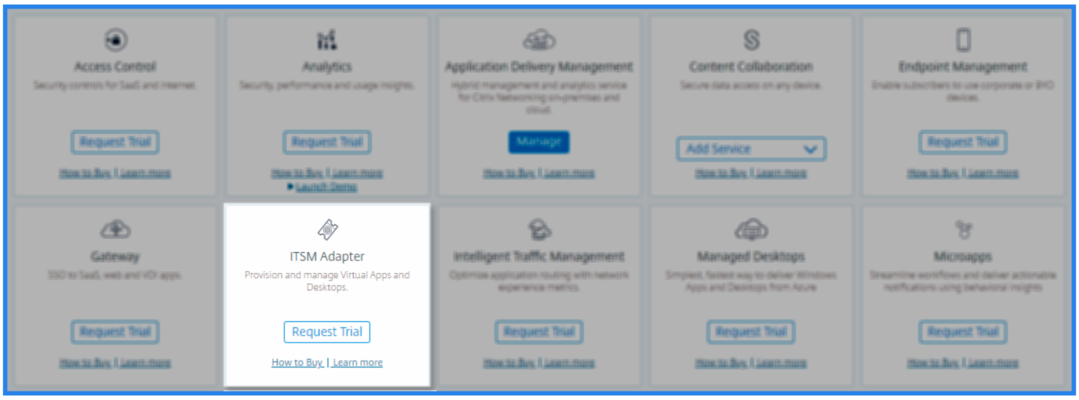
October 20, 2021

When you want to enable ServiceNow notifications for Citrix ADC events and Citrix Application Delivery and Management events, you must integrate Citrix Application Delivery and Management with the ServiceNow instance. To integrate Citrix Application Delivery and Management with the ServiceNow instance, use Citrix ITSM connector. The ITSM connector establishes the communication between Citrix Application Delivery and Management and the ServiceNow instance. For more information, see How ITSM Adapter works.

Perform the following steps to integrate Citrix Application Delivery and Management with ServiceNow using ITSM connector:

1. Subscribe to **ITSM Adapter** service in Citrix Cloud

    a) On the **ITSM Adapter** tile, click **Request Trial**.



b) Navigate to **Identity Access and Management** > **API Access** and note the **Client ID** and **Client Secret** information.

2. Log in to your ServiceNow instance with an administrator credential and perform the following steps:

    a) Go to ServiceNow store. Download and install the **Citrix ITSM connector**.

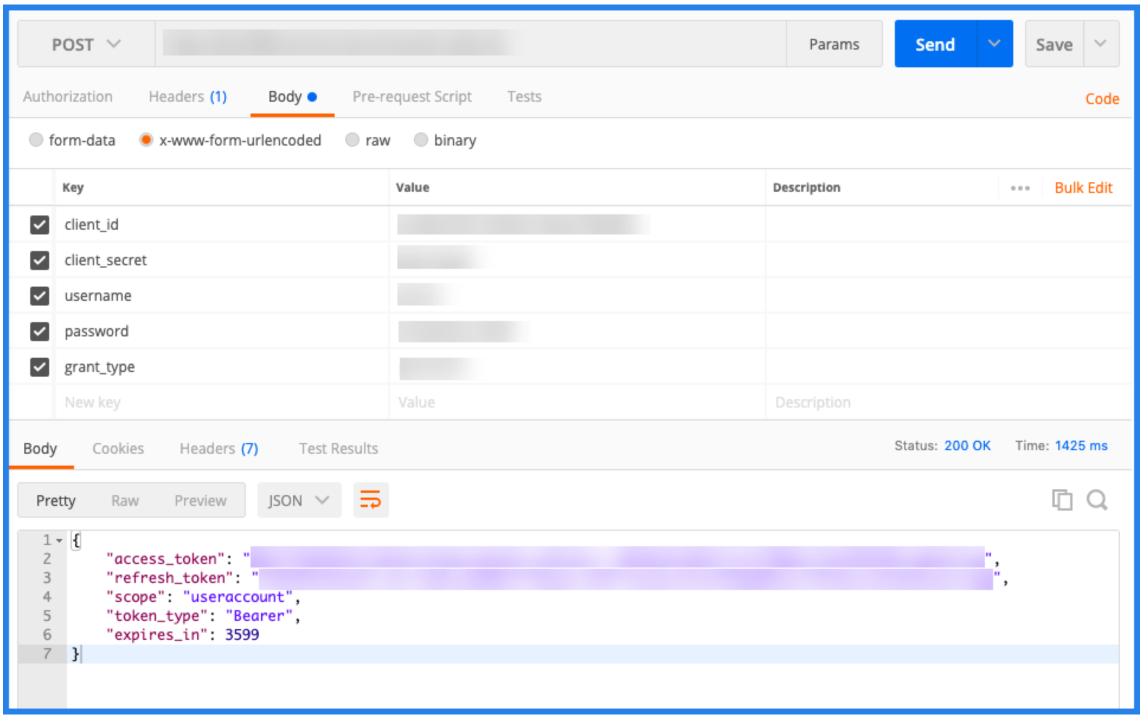
    b) On the **Citrix ITSM Connector** pane, select **Home** and then click **Authenticate**. Type the Client ID and Secret that you have noted from Citrix Cloud.

    c) Test the connection.

    d) Save the configuration. An acknowledgment from ServiceNow appears indicating that the connection is active.

3. Create an endpoint to access a ServiceNow instance. See Create an endpoint for clients to access the instance.

4. Obtain the Access and Refresh tokens using the Client ID and Client Secret. See OAuth tokens.



POST [redacted]

	Key	Value	Description
☑	client_id	[redacted]	
☑	client_secret	[redacted]	
☑	username	[redacted]	
☑	password	[redacted]	
☑	grant_type	[redacted]	
	New key	Value	Description

Status: 200 OK Time: 1425 ms

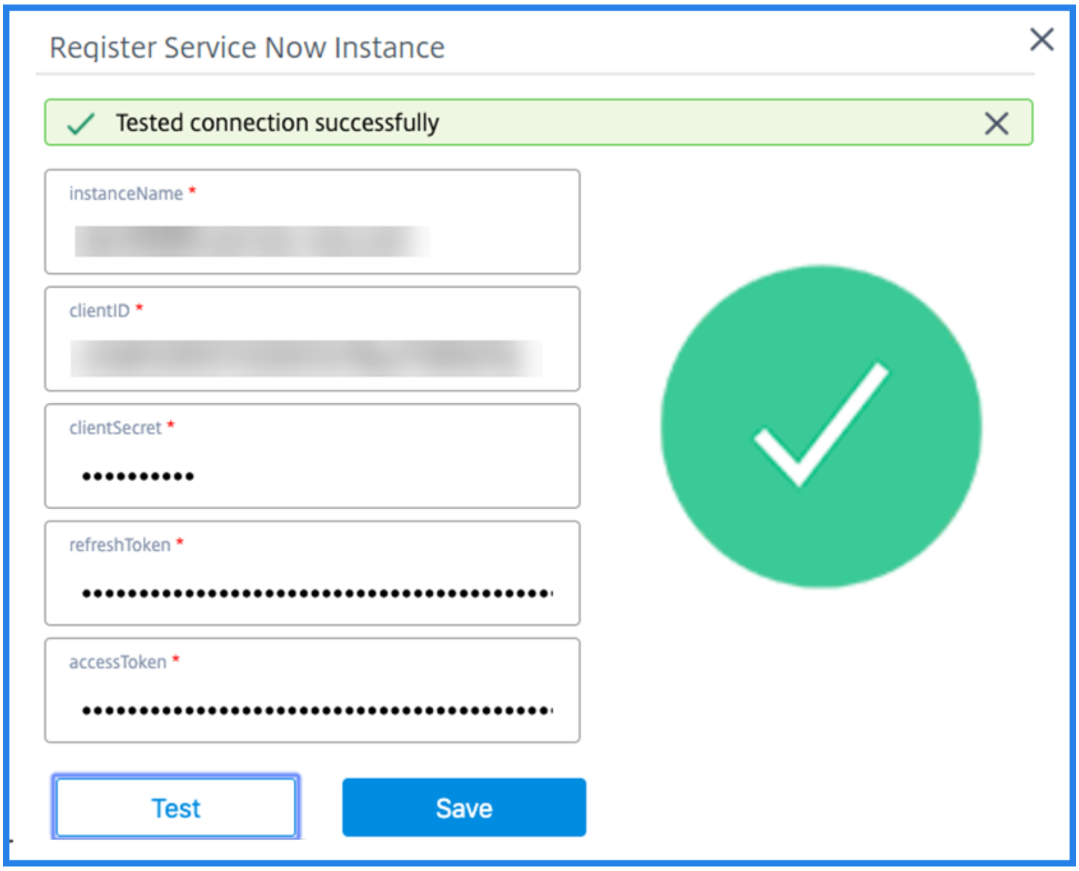
```
{
    "access_token": "[redacted]",
    "refresh_token": "[redacted]",
    "scope": "useraccount",
    "token_type": "Bearer",
    "expires_in": 3599
}
```

5. In ITSM adapter, add a ServiceNow instance:

    a) In the **Manage** tab, select Add ServiceNow Instance.

    b) Specify the **Instance Name**, **Client ID**, **Client Secret**, **Refresh Token**, and **Access Token**.

    c) Click **Test**.



The ServiceNow instance is now connected to the ITSM Adapter service.

   d) After testing the connection successfully, click **Save** to add a ServiceNow instance.

6. Test auto-generation of ServiceNow tickets in Citrix Application Delivery and Management.

   a) Log in to Citrix Application Delivery and Management.

   b) Navigate to **Settings > Notifications** and select **ServiceNow**.

   c) Select the ServiceNow profile from the list.

   d) Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

      If you want to view ServiceNow tickets in the Citrix Application Delivery and Management GUI, select **ServiceNow Tickets**.

After ServiceNow instance is registered on the ITSM adapter, you can set up ServiceNow notifications for the following events in the Citrix Application Delivery and Management GUI:

> **Important**
>
> This feature is supported on ServiceNow Cloud.

- **Citrix ADC events**: Citrix Application Delivery and Management can generate the ServiceNow incidents for selected set of Citrix ADC events from selected managed Citrix ADC instances.

To send ServiceNow notifications for Citrix ADC 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 Citrix Application Delivery and Management by navigating to **Infrastructure > Events > Rules**. For more information, see Send ServiceNow notifications.

- **The SSL certificate and Citrix Application Delivery and Management license events**: Citrix Application Delivery and Management can generate the ServiceNow incidents for the SSL certificate expiry and Citrix Application Delivery and Management license expiry events.

  To send ServiceNow notifications for an SSL certificate expiry, see The SSL certificate expiry.

  To send ServiceNow notifications for an Citrix Application Delivery and Management license expiry, see The Citrix Application Delivery and Management license expiry.

Applications

September 25, 2021

The application analytics and management feature of Citrix Application Delivery and Management 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 (Citrix ADC).

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 Citrix ADC instances in Citrix Application Delivery and Management
- Ensure you have valid license for your Citrix ADC 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, Citrix Application Delivery and Management 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, Citrix provides an Ingress Controller for Citrix ADC MPX (hardware), Citrix ADC VPX (virtualized), and Citrix ADC CPX (containerized). For more information, see Citrix Ingress Controller.

The discrete applications that are configured using the Citrix ADC CPX instances are referred to as microservices applications.

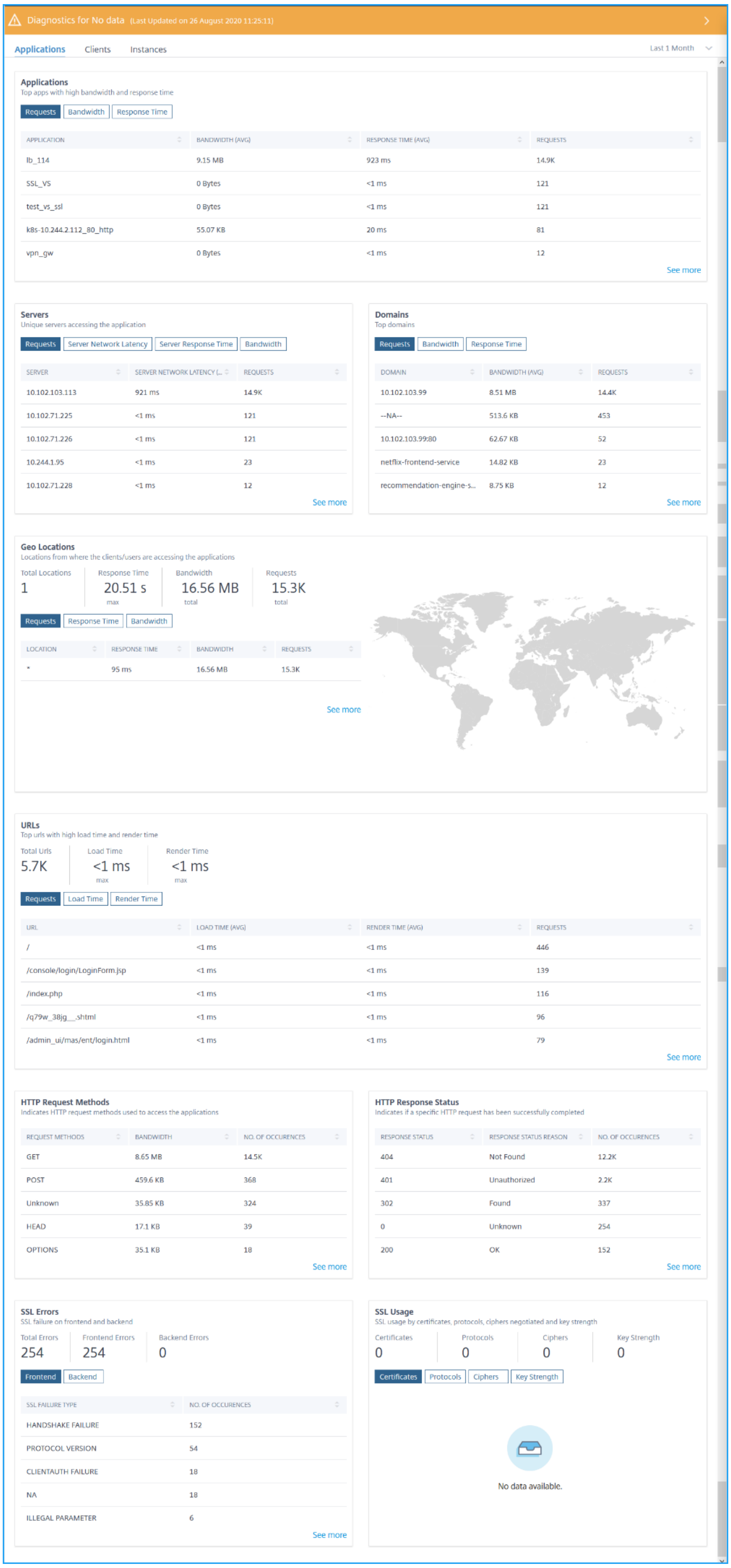
Web Insight dashboard

September 25, 2021

The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and Citrix ADC 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
Application with Response Time Anomalies	Clients	Instance Metrics
Applications	Geo Locations	Applications
Servers	HTTP Request Methods	Domains
Domains	HTTP Response Status	URLs
Geo Locations	URLs	HTTP Request Methods
URLs	Operating System	HTTP Response Status
HTTP Request Methods	Browsers	Clients
HTTP Response Status	SSL Errors	Servers
SSL Errors	SSL Usage	Operating System
SSL Usage		Browsers



Applications
Top apps with high bandwidth and response time

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
lb_114	9.15 MB	923 ms	14.9K
SSL_VS	0 Bytes	<1 ms	121
test_vs_ssl	0 Bytes	<1 ms	121
k8s-10.244.2.112_80_http	55.07 KB	20 ms	81
vpn_gw	0 Bytes	<1 ms	12

Servers
Unique servers accessing the application

SERVER	SERVER NETWORK LATENCY (...	REQUESTS
10.102.103.113	921 ms	14.9K
10.102.71.225	<1 ms	121
10.102.71.226	<1 ms	121
10.244.1.95	<1 ms	23
10.102.71.228	<1 ms	12

Domains
Top domains

DOMAIN	BANDWIDTH (AVG)	REQUESTS
10.102.103.99	8.51 MB	14.4K
--NA--	513.6 KB	453
10.102.103.99:80	62.67 KB	52
netflix-frontend-service	14.82 KB	23
recommendation-engine-s...	8.75 KB	12

Geo Locations
Locations from where the clients/users are accessing the applications

Total Locations	Response Time	Bandwidth	Requests
1	20.51 s max	16.56 MB total	15.3K total

LOCATION	RESPONSE TIME	BANDWIDTH	REQUESTS
*	95 ms	16.56 MB	15.3K

URLs
Top urls with high load time and render time

Total Urls	Load Time	Render Time
5.7K	<1 ms max	<1 ms max

URL	LOAD TIME (AVG)	RENDER TIME (AVG)	REQUESTS
/	<1 ms	<1 ms	446
/console/login/LoginForm.jsp	<1 ms	<1 ms	139
/index.php	<1 ms	<1 ms	116
/q79w_38jg__.shtml	<1 ms	<1 ms	96
/admin_ui/mas/ent/login.html	<1 ms	<1 ms	79

HTTP Request Methods
Indicates HTTP request methods used to access the applications

REQUEST METHODS	BANDWIDTH	NO. OF OCCURENCES
GET	8.65 MB	14.5K
POST	459.6 KB	368
Unknown	35.85 KB	324
HEAD	17.1 KB	39
OPTIONS	35.1 KB	18

HTTP Response Status
Indicates if a specific HTTP request has been successfully completed

RESPONSE STATUS	RESPONSE STATUS REASON	NO. OF OCCURENCES
404	Not Found	12.2K
401	Unauthorized	2.2K
302	Found	337
0	Unknown	254
200	OK	152

SSL Errors
SSL failure on frontend and backend

Total Errors	Frontend Errors	Backend Errors
254	254	0

SSL FAILURE TYPE	NO. OF OCCURENCES
HANDSHAKE FAILURE	152
PROTOCOL VERSION	54
CLIENTAUTH FAILURE	18
NA	18
ILLEGAL PARAMETER	6

SSL Usage
SSL usage by certificates, protocols, ciphers negotiated and key strength

Certificates	Protocols	Ciphers	Key Strength
0	0	0	0

No data available.

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.

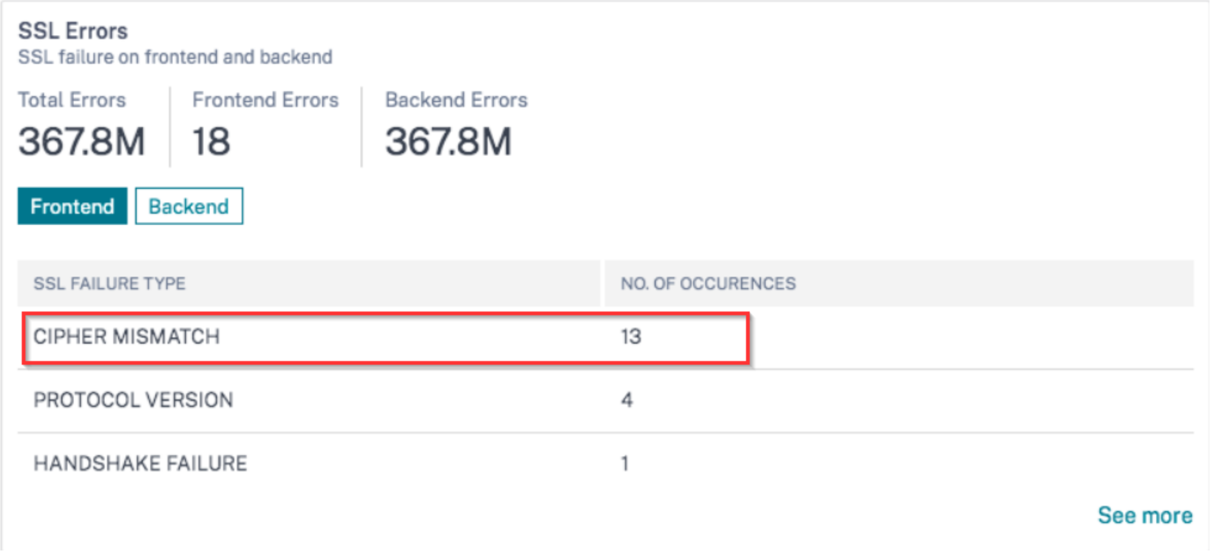
> Note
>
> In some scenarios, Citrix ADC might not be able to calculate the RTT values for some transactions. For such transactions, Citrix Application Delivery and Management displays the RTT values as
>
> - **NA** – Displays when the ADC instance cannot calculate the RTT.
> - **< 1ms** – Displays when the ADC instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

View details for cipher related issues

Under **SSL Errors**, you can view details for the following SSL parameters:

- Cipher mismatch
- Unsupported Ciphers

Under **SSL errors**, click an SSL parameter (Cipher Mismatch or Unsupported Ciphers) to view details such as the SSL cipher name, the recommended actions, and the details of the affected applications and clients.



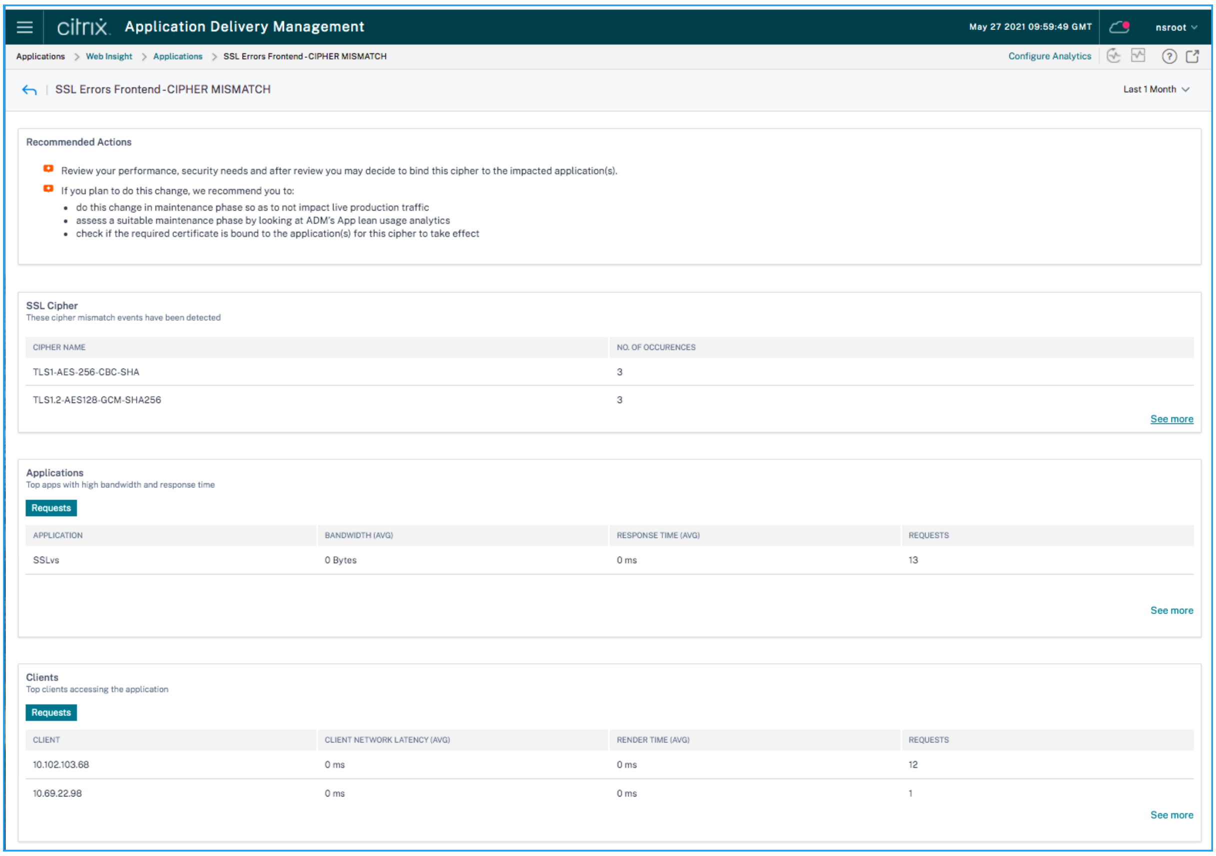
SSL Errors
SSL failure on frontend and backend

Total Errors 367.8M | Frontend Errors 18 | Backend Errors 367.8M

SSL FAILURE TYPE	NO. OF OCCURENCES
CIPHER MISMATCH	13
PROTOCOL VERSION	4
HANDSHAKE FAILURE	1

The details page appears for the selected SSL parameter. You can:

- Review the suggestions provided in the **Recommended Actions**
- View the cipher names and number of occurrences under **SSL Cipher**
- View the total applications and clients affected


citrix Application Delivery Management
May 27 2021 09:59:49 GMT
nsroot
Applications > Web Insight > Applications > SSL Errors Frontend - CIPHER MISMATCH
Configure Analytics
Last 1 Month

SSL Errors Frontend - CIPHER MISMATCH

Recommended Actions

- Review your performance, security needs and after review you may decide to bind this cipher to the impacted application(s).
- If you plan to do this change, we recommend you to:
  - do this change in maintenance phase so as to not impact live production traffic
  - assess a suitable maintenance phase by looking at ADM's App lean usage analytics
  - check if the required certificate is bound to the application(s) for this cipher to take effect

SSL Cipher

These cipher mismatch events have been detected

CIPHER NAME	NO. OF OCCURENCES
TLS1-AES-256-CBC-SHA	3
TLS1.2-AES128-GCM-SHA256	3

See more

Applications

Top apps with high bandwidth and response time

Requests

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
SSLvs	0 Bytes	0 ms	13

See more

Clients

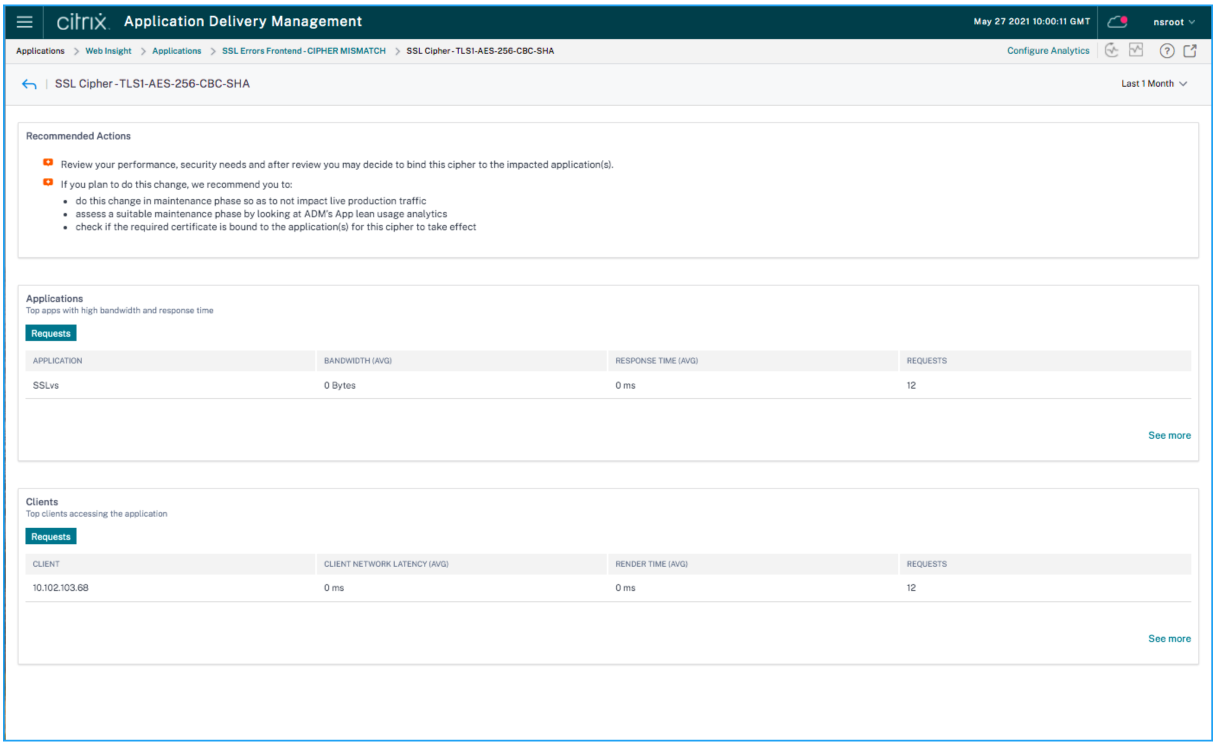
Top clients accessing the application

Requests

CLIENT	CLIENT NETWORK LATENCY (AVG)	RENDER TIME (AVG)	REQUESTS
10.102.103.68	0 ms	0 ms	12
10.69.22.98	0 ms	0 ms	1

See more

Click the **SSL Cipher name** to see the application and client details.


citrix Application Delivery Management
May 27 2021 10:00:11 GMT
nsroot
Applications > Web Insight > Applications > SSL Errors Frontend - CIPHER MISMATCH > SSL Cipher - TLS1-AES-256-CBC-SHA
Configure Analytics
Last 1 Month

SSL Cipher - TLS1-AES-256-CBC-SHA

Recommended Actions

- Review your performance, security needs and after review you may decide to bind this cipher to the impacted application(s).
- If you plan to do this change, we recommend you to:
  - do this change in maintenance phase so as to not impact live production traffic
  - assess a suitable maintenance phase by looking at ADM's App lean usage analytics
  - check if the required certificate is bound to the application(s) for this cipher to take effect

Applications

Top apps with high bandwidth and response time

Requests

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
SSLvs	0 Bytes	0 ms	12

See more

Clients

Top clients accessing the application

Requests

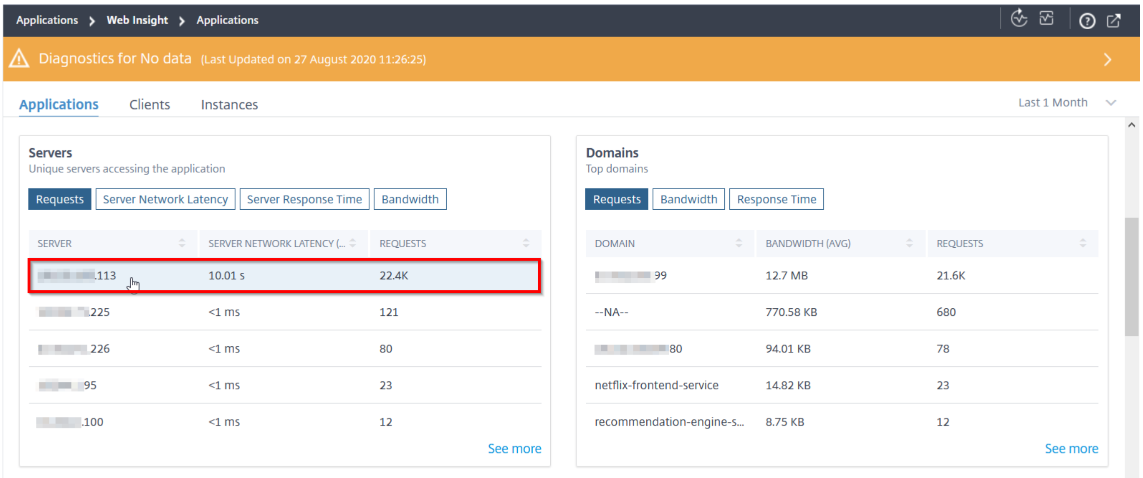
CLIENT	CLIENT NETWORK LATENCY (AVG)	RENDER TIME (AVG)	REQUESTS
10.102.103.68	0 ms	0 ms	12

See more

Other use case

Consider that you want to analyze the server network latency for 1-month time duration and take a 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.



Applications > Web Insight > Applications

⚠ Diagnostics for No data (Last Updated on 27 August 2020 11:26:25)

Applications | Clients | Instances | Last 1 Month

Servers
Unique servers accessing the application

Requests | Server Network Latency | Server Response Time | Bandwidth

SERVER	SERVER NETWORK LATENCY (...	REQUESTS
[redacted].113	10.01 s	22.4K
[redacted].225	<1 ms	121
[redacted].226	<1 ms	80
[redacted].95	<1 ms	23
[redacted].100	<1 ms	12

See more

Domains
Top domains

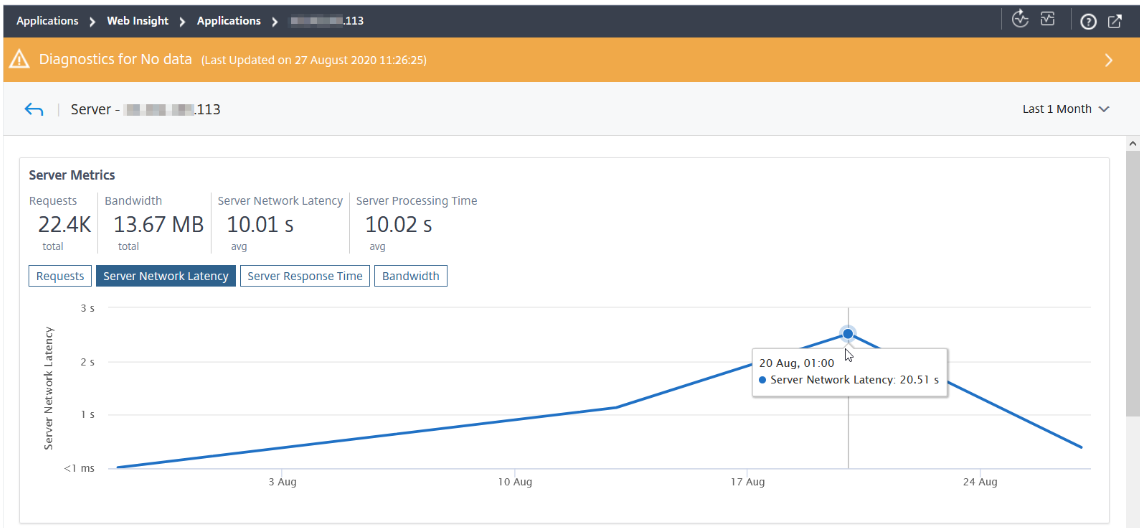
Requests | Bandwidth | Response Time

DOMAIN	BANDWIDTH (AVG)	REQUESTS
[redacted]99	12.7 MB	21.6K
--NA--	770.58 KB	680
[redacted]80	94.01 KB	78
netflix-frontend-service	14.82 KB	23
recommendation-engine-s...	8.75 KB	12

See more

The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.



Applications > Web Insight > Applications > [redacted].113

⚠ Diagnostics for No data (Last Updated on 27 August 2020 11:26:25)

Server - [redacted].113 | Last 1 Month

Server Metrics

Requests	Bandwidth	Server Network Latency	Server Processing Time
22.4K	13.67 MB	10.01 s	10.02 s
total	total	avg	avg

Requests | Server Network Latency | Server Response Time | Bandwidth

The average latency indicates 10.01s 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 a decision to scale up the production environment.

Analyze the root cause for application slowness

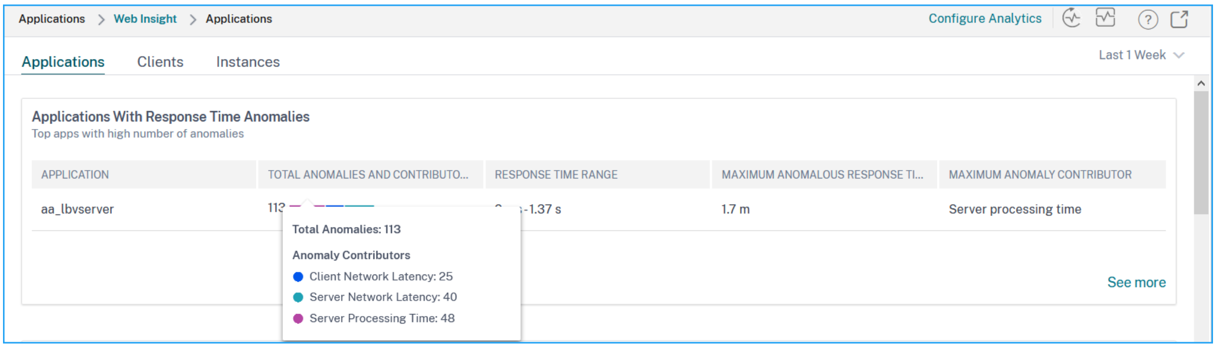
October 26, 2021

Application slowness is a major concern for any organization because it results in business impact or productivity. As an administrator, you must ensure that all applications perform optimally to avoid any business impact. When your users experience a slowness in accessing the application, you must ensure if the issue is with:

- Client network latency
- Server network latency
- Server processing time

Citrix Application Delivery and Management performs anomaly checks every hour and reports anomalies for past 1 hour traffic, based on certain prerequisites. For example, to avoid false positive results, if the response time is < 1 ms, the anomaly checks for those results are skipped.

The **Applications > Web Insight** page enables you to view the applications with response time anomalies for the selected duration. The **Applications with Response Time Anomalies** metric displays the top five applications based on the total anomalies. Click **See more** to view all applications.



Applications With Response Time Anomalies

Top apps with high number of anomalies

APPLICATION	TOTAL ANOMALIES AND CONTRIBUTO...	RESPONSE TIME RANGE	MAXIMUM ANOMALOUS RESPONSE TI...	MAXIMUM ANOMALY CONTRIBUTOR
aa_lbvserver	113	[illegible]-1.37 s	1.7 m	Server processing time

Total Anomalies: 113

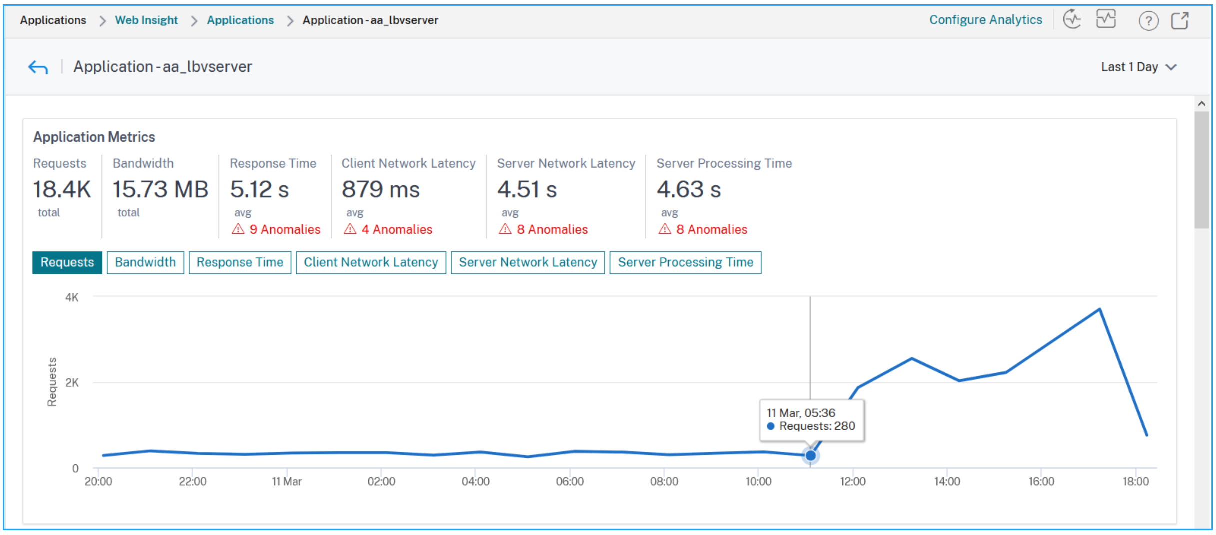
Anomaly Contributors

- ● Client Network Latency: 25
- ● Server Network Latency: 40
- ● Server Processing Time: 48

- **Application** – Denotes the application name.
- **Total Anomalies and Contributors** – Denotes the total anomalies from the application. When you hover the mouse pointer, you can view the total anomalies that are from the client network latency, server network latency, and server processing time respectively.
- **Response Time Range** – Denotes the expected response time range from the application.
- **Maximum Anomalous Response Time** – Denotes the highest response time from the application.
- **Maximum Anomaly Contributor** – Denotes if the maximum number of anomalies for the application are from client network latency, server network latency, or server processing time.

Application drill-down

Click an application to view the **Application Metrics** details for the selected duration.



Application Metrics

Requests 18.4K total | Bandwidth 15.73 MB total | Response Time 5.12 s avg ⚠ 9 Anomalies | Client Network Latency 879 ms avg ⚠ 4 Anomalies | Server Network Latency 4.51 s avg ⚠ 8 Anomalies | Server Processing Time 4.63 s avg ⚠ 8 Anomalies

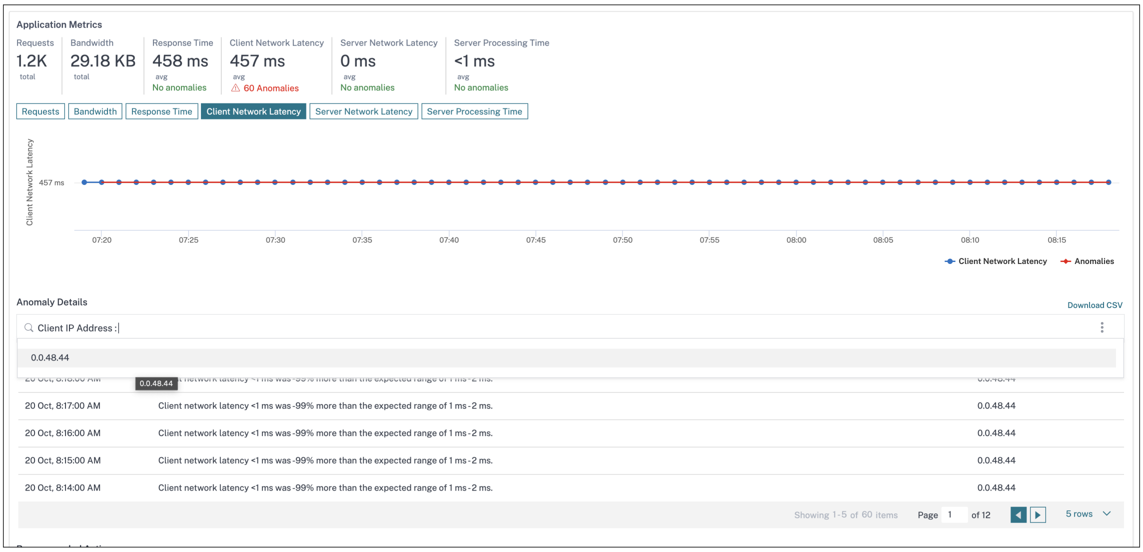
The **Application Metrics** enable you to view:

- **Requests** – The total requests received by the application
- **Bandwidth** – The total bandwidth processed by the application
- **Response Time** – The average response time from the application
- **Client Network Latency** – The average client network latency (from client to ADC)
- **Server Network Latency** – The average server network latency (from ADC to server)
- **Server Processing Time** – The average server processing time (from server to ADC)

If the application has anomalies, you can view if the anomalies are from client network latency, server network latency, or server processing time. Click each tab to view details.

In the **Client Network Latency** and **Server Network Latency** tabs, you can view:

- **A search bar** - Click the search bar to view the IP address of all clients (in Client Network Latency) and servers (in Server Network Latency). You can select the IP address to filter results.
- **An export option** - Click **Download CSV** to export the details in CSV format.



Application Metrics

Requests	Bandwidth	Response Time	Client Network Latency	Server Network Latency	Server Processing Time
1.2K total	29.18 KB total	458 ms avg No anomalies	457 ms avg ⚠ 60 Anomalies	0 ms avg No anomalies	<1 ms avg No anomalies

Anomaly Details

Download CSV

Client IP Address :

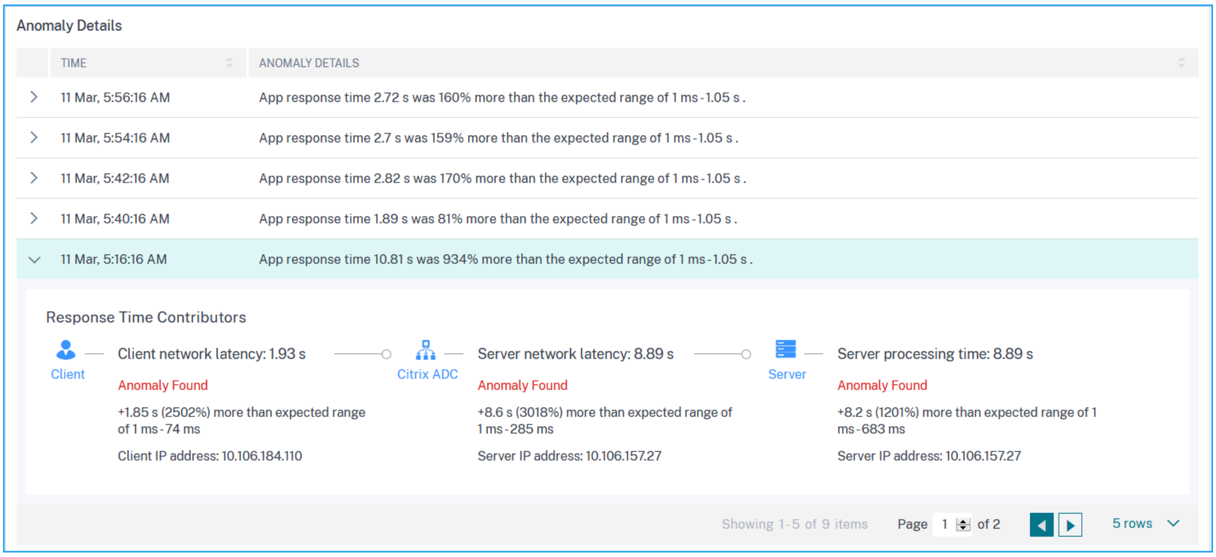
0.0.48.44

20 Oct, 8:17:00 AM	Client network latency <1 ms was -99% more than the expected range of 1 ms - 2 ms.	0.0.48.44
20 Oct, 8:16:00 AM	Client network latency <1 ms was -99% more than the expected range of 1 ms - 2 ms.	0.0.48.44
20 Oct, 8:15:00 AM	Client network latency <1 ms was -99% more than the expected range of 1 ms - 2 ms.	0.0.48.44
20 Oct, 8:14:00 AM	Client network latency <1 ms was -99% more than the expected range of 1 ms - 2 ms.	0.0.48.44

Showing 1 - 5 of 60 items Page 1 of 12 5 rows

Response Time

Under **Anomaly Details**, click to view details for the response time contributors (from client to server). The following example has an anomaly for client network latency, server network latency, and server processing time. You can also view the expected ranges and the breach that has happened beyond the expected range.



Anomaly Details

TIME	ANOMALY DETAILS
11 Mar, 5:56:16 AM	App response time 2.72 s was 160% more than the expected range of 1 ms - 1.05 s .
11 Mar, 5:54:16 AM	App response time 2.7 s was 159% more than the expected range of 1 ms - 1.05 s .
11 Mar, 5:42:16 AM	App response time 2.82 s was 170% more than the expected range of 1 ms - 1.05 s .
11 Mar, 5:40:16 AM	App response time 1.89 s was 81% more than the expected range of 1 ms - 1.05 s .
11 Mar, 5:16:16 AM	App response time 10.81 s was 934% more than the expected range of 1 ms - 1.05 s .

Response Time Contributors

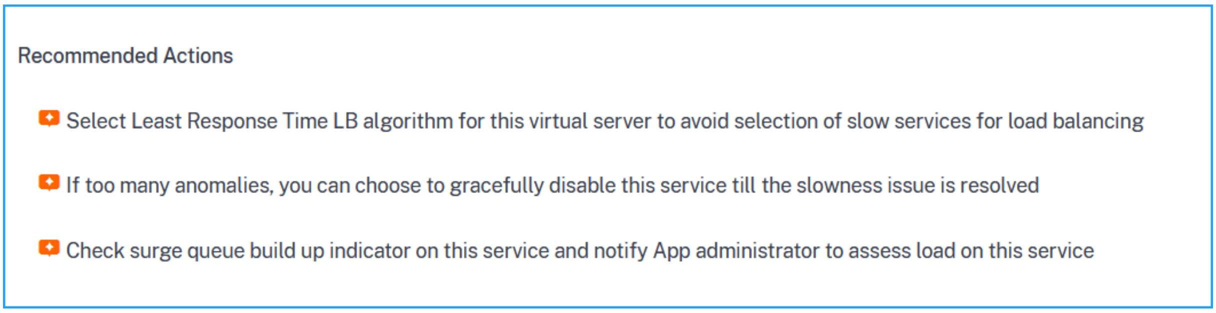
Client network latency: 1.93 s
Anomaly Found
+1.85 s (2502%) more than expected range of 1 ms - 74 ms
Client IP address: 10.106.184.110

Server network latency: 8.89 s
Anomaly Found
+8.6 s (3018%) more than expected range of 1 ms - 285 ms
Server IP address: 10.106.157.27

Server processing time: 8.89 s
Anomaly Found
+8.2 s (1201%) more than expected range of 1 ms - 683 ms
Server IP address: 10.106.157.27

Showing 1 - 5 of 9 items Page 1 of 2 5 rows

The **Recommended Actions** suggest you the possible resolutions for the anomalies.



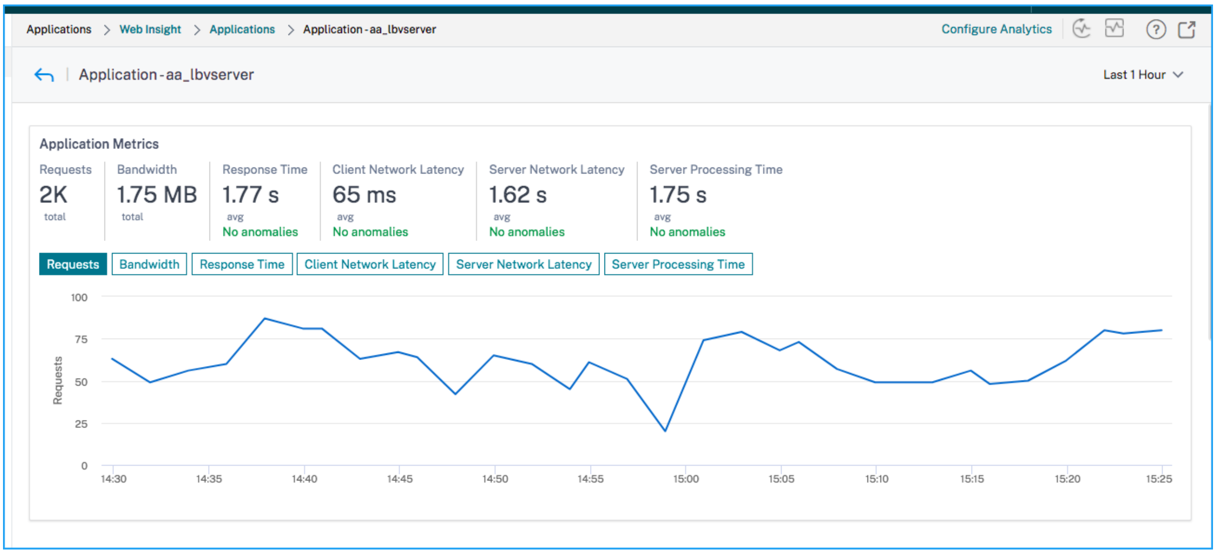
Recommended Actions

- Select Least Response Time LB algorithm for this virtual server to avoid selection of slow services for load balancing
- If too many anomalies, you can choose to gracefully disable this service till the slowness issue is resolved
- Check surge queue build up indicator on this service and notify App administrator to assess load on this service

Similarly, you can click the **Client Network Latency**, **Server Network Latency**, and **Server Processing Time** tabs to view:

- Anomaly that has breached the expected range.
- Recommended Actions that suggest you the possible resolutions.

If the application is performing well, you can view application metrics as no anomalies.



Applications > Web Insight > Applications > Application - aa_lbvserver

Application - aa_lbvserver

Application Metrics

Requests	Bandwidth	Response Time	Client Network Latency	Server Network Latency	Server Processing Time
2K total	1.75 MB total	1.77 s avg No anomalies	65 ms avg No anomalies	1.62 s avg No anomalies	1.75 s avg No anomalies

Service Graph

September 25, 2021

The service graph feature in Citrix Application Delivery and Management 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. Navigate to **Applications > Service Graph** to view service graph for:

- Applications configured across all Citrix ADC instances
- Kubernetes applications

- 3-tier Web applications

Service graph for applications across all Citrix ADC 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 (Citrix ADC 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 Citrix ADC 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 Citrix ADC metrics information
- All Citrix ADC 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
- View client metrics and client transaction summary details

By visualizing these metrics in Citrix Application Delivery and Management, 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 Citrix ADC 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**. Citrix Application Delivery and Management 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**. Citrix Application Delivery and Management 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**. Citrix Application Delivery and Management 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

September 25, 2021

StyleBooks simplify the task of managing complex Citrix ADC configurations for your applications. A StyleBook is a template that you can use to create and manage Citrix ADC configurations. You can create a StyleBook for configuring a specific feature of Citrix ADC, 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 ADC instance. Citrix Application Delivery and Management computes the diff between existing state on an ADC 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 Citrix Application Delivery and Management 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 Citrix ADC 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 ADC configuration. Configurations that are created from StyleBooks are not tied to the infrastructure. A single configuration can thus be deployed on one or multiple ADC instances, and can also be moved among instances.
- **Auto-Generated UI**: Citrix Application Delivery and Management auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the Citrix Application Delivery and Management 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 Citrix Application Delivery and Management 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 run it on a Citrix ADC instance. This configuration is saved as a config pack. You can use the same StyleBook to create another configuration with different values and run it on the same or a different instance. A new config pack is created for this configuration. A config pack is saved both on Citrix Application Delivery and Management and on the ADC instance on which the configuration is run.

You can either use default StyleBooks, shipped with Citrix Application Delivery and Management, to create configurations for your deployment, or design your own StyleBooks and import them to Citrix Application Delivery and Management. You can use the StyleBooks to create configurations either by using the Citrix Application Delivery and Management 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

September 25, 2021

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.

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 Citrix Application Delivery and Management only when a violation or attack occurs. Many breaches and vulnerabilities lead to a high threat index value.

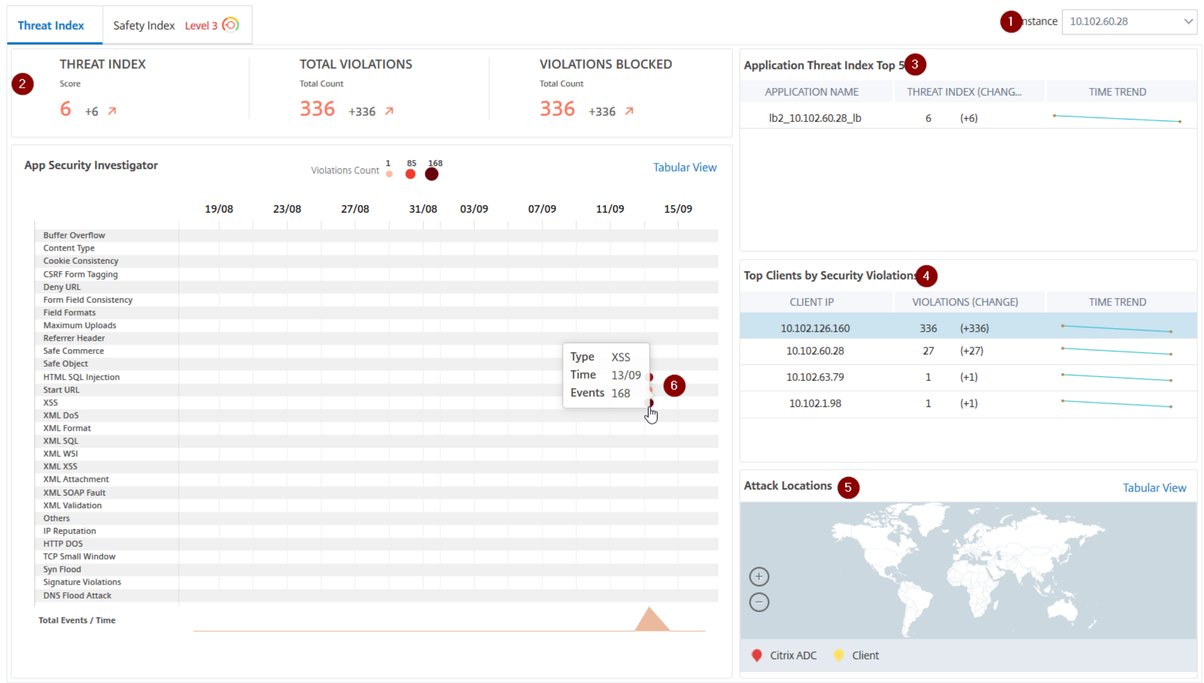
   - **Safety index**. A single-digit rating system that indicates how securely you have configured the Citrix ADC instances to protect applications from external threats and vulnerabilities.

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 Citrix ADC 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 Citrix ADC 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 discrepancies reported on the **App Security Investigator**.

Threat index details



Application Threat Index Top 5

APPLICATION NAME	THREAT INDEX (CHANG...	TIME TREND
lb2_10.102.60.28_lb	6 (+6)	

Top Clients by Security Violations

CLIENT IP	VIOLATIONS (CHANGE)	TIME TREND
10.102.126.160	336 (+336)	
10.102.60.28	27 (+27)	
10.102.63.79	1 (+1)	
10.102.1.98	1 (+1)	

1 - Displays the Citrix ADC 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 results.

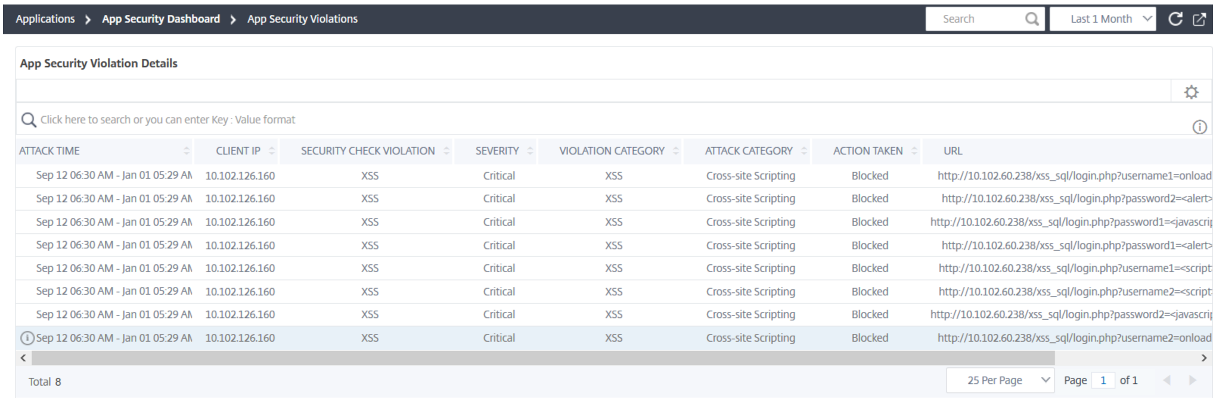
5 - Displays the violations in map view and tabular view.

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 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.


Applications > App Security Dashboard > App Security Violations
Search
Last 1 Month

App Security Violation Details

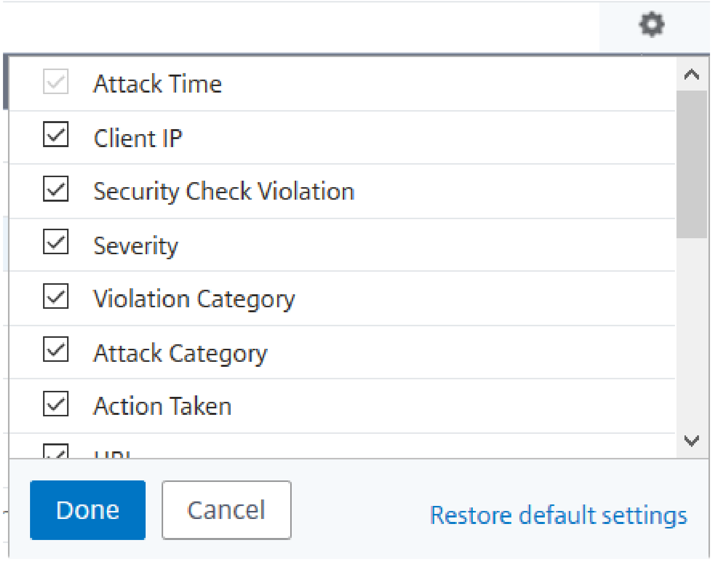
Click here to search or you can enter Key : Value format

ATTACK TIME	CLIENT IP	SECURITY CHECK VIOLATION	SEVERITY	VIOLATION CATEGORY	ATTACK CATEGORY	ACTION TAKEN	URL
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?username1=onload
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?password2=<alert>
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?password1=<javascrip
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?password1=<alert>
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?username1=<script
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?username2=<script
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?password2=<javascrip
Sep 12 06:30 AM - Jan 01 05:29 AM	10.102.126.160	XSS	Critical	XSS	Cross-site Scripting	Blocked	http://10.102.60.238/xss_sql/login.php?username2=onload

Total 8

25 Per Page Page 1 of 1

You can also click the **Settings** option to select the options that you want to get it displayed.



☑ Attack Time
☑ Client IP
☑ Security Check Violation
☑ Severity
☑ Violation Category
☑ Attack Category
☑ Action Taken
☑ URL

Safety index details

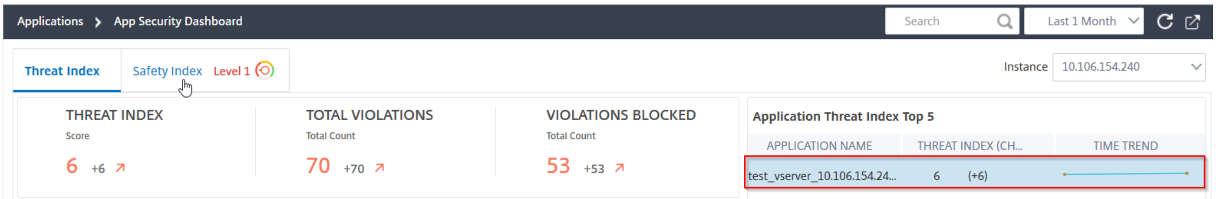
After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application safety index summary.

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.

- **Citrix Application Delivery and Management 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.

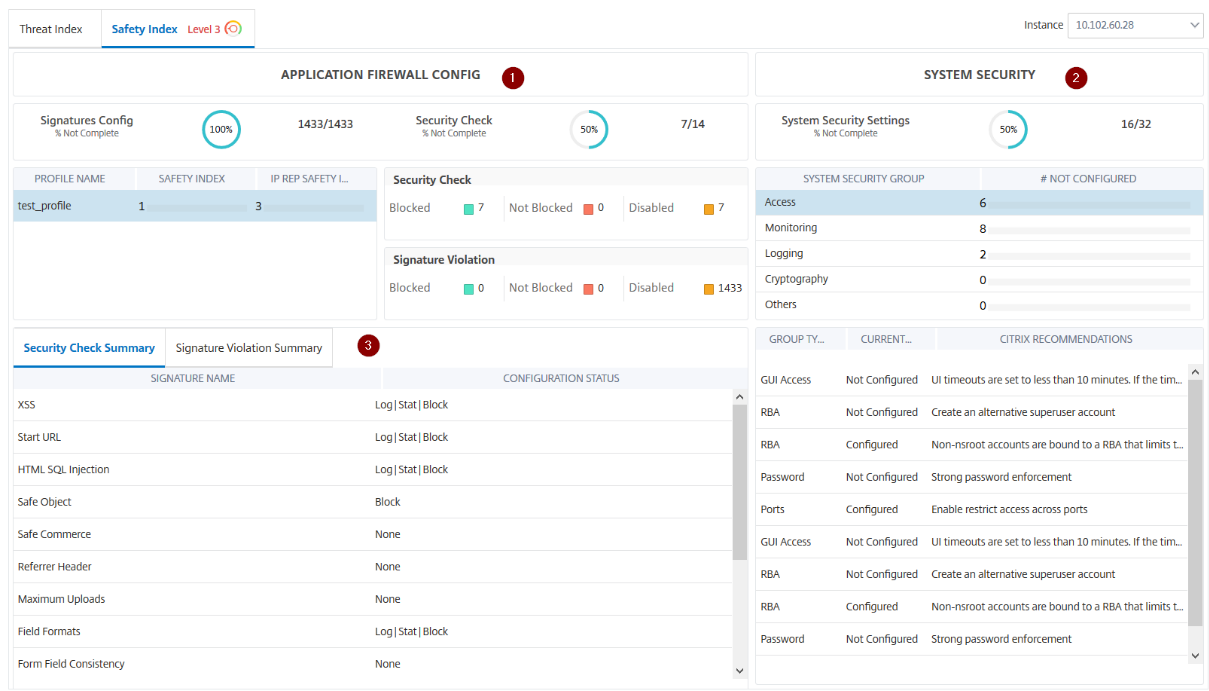


THREAT INDEX Score	TOTAL VIOLATIONS Total Count	VIOLATIONS BLOCKED Total Count
6 +6 ↗	70 +70 ↗	53 +53 ↗

Application Threat Index Top 5

APPLICATION NAME	THREAT INDEX (CH...	TIME TREND
test_vserver_10.106.154.24...	6 (+6)	

The details are displayed.



Signatures Config (% Not Complete) 100% 1433/1433

Security Check (% Not Complete) 50% 7/14

System Security Settings (% Not Complete) 50% 16/32

PROFILE NAME	SAFETY INDEX	IP REP SAFETY I...
test_profile	1	3

Security Check

Blocked	🟩 7	Not Blocked	🟥 0	Disabled	🟧 7

Signature Violation

Blocked	🟩 0	Not Blocked	🟥 0	Disabled	🟧 1433

SYSTEM SECURITY GROUP	# NOT CONFIGURED
Access	6
Monitoring	8
Logging	2
Cryptography	0
Others	0

SIGNATURE NAME	CONFIGURATION STATUS
XSS	Log | Stat | Block
Start URL	Log | Stat | Block
HTML SQL Injection	Log | Stat | Block
Safe Object	Block
Safe Commerce	None
Referrer Header	None
Maximum Uploads	None
Field Formats	Log | Stat | Block
Form Field Consistency	None

GROUP TY...	CURRENT...	CITRIX RECOMMENDATIONS
GUI Access	Not Configured	UI timeouts are set to less than 10 minutes. If the tim...
RBA	Not Configured	Create an alternative superuser account
RBA	Configured	Non-nsroot accounts are bound to a RBA that limits t...
Password	Not Configured	Strong password enforcement
Ports	Configured	Enable restrict access across ports
GUI Access	Not Configured	UI timeouts are set to less than 10 minutes. If the tim...
RBA	Not Configured	Create an alternative superuser account
RBA	Configured	Non-nsroot accounts are bound to a RBA that limits t...
Password	Not Configured	Strong password enforcement

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 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 security insight for virtual servers and then navigating to **Security > Security violations**. For more information on safety index use case, see security insight.

View application security violation details

September 25, 2021

Web applications that are exposed to the internet have become vulnerable to attacks drastically. Citrix Application Delivery and Management 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 security insight and bot insight
- 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.

Setting up

You must enable **Advanced Security Analytics** and select **Web Transaction Settings** to **All** to view the following violations in Citrix Application Delivery and Management:

- Unusually High Upload Transactions (WAF)
- Unusually High Download Transactions (WAF)
- Excessive Unique IPs (WAF)
- Account Takeover (BOT)
- Website Scanners (BOT)
- Content Scrapers (BOT)

For other violations, ensure if **Metrics Collector** is enabled. By default, **Metrics Collector** is enabled on the Citrix ADC instance. For more information, see Configure Intelligent App Analytics.

Enable Advanced Security Analytics

1. Navigate to **Infrastructure > Instances > Citrix ADC**, and select the instance type. For example, MPX.
2. Select the Citrix ADC instance and from the **Select Action** list, select **Configure Analytics**.
3. Select the virtual server and click **Enable Analytics**.

4. On the **Enable Analytics** window:

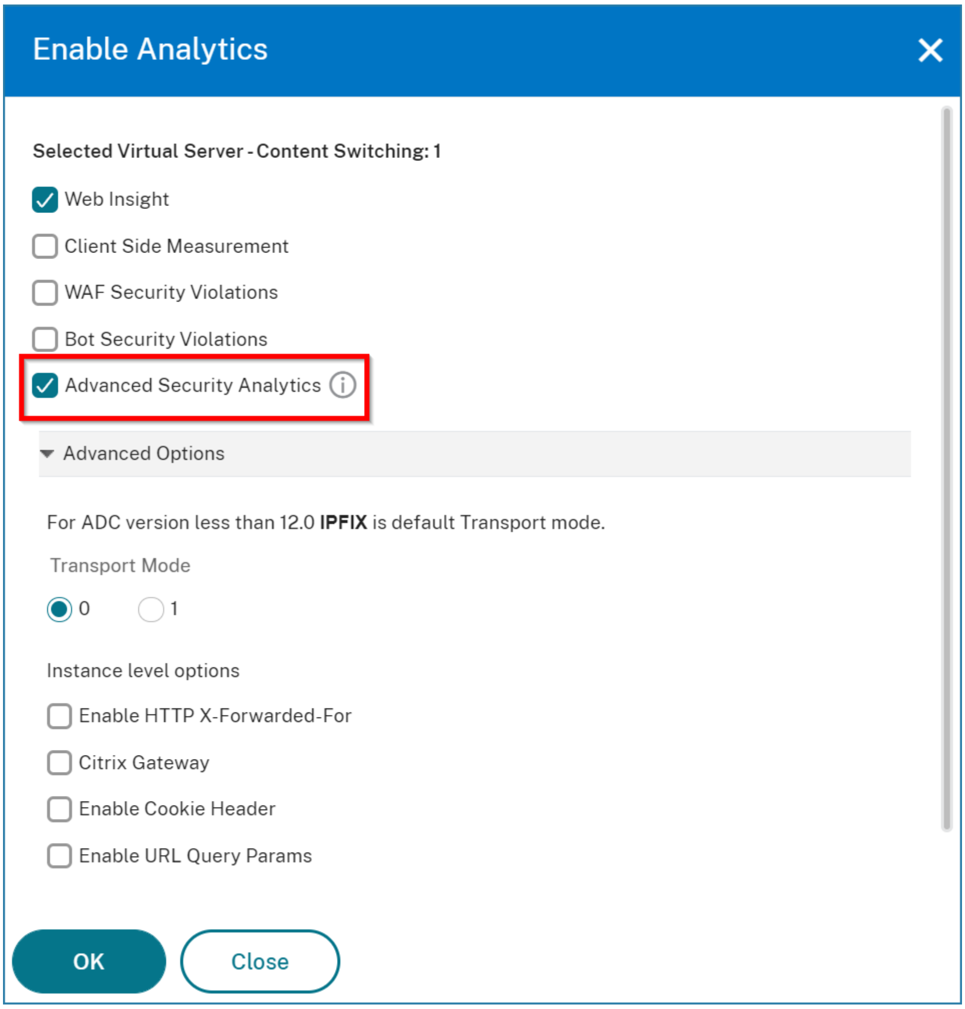
   a) Select **Web Insight**. After you select Web Insight, the read-only **Advanced Security Analytics** option is enabled automatically.

   > **Note**
   >
   > The **Advanced Security Analytics** option is displayed only for premium licensed ADC instances.

   b) Select **Logstream** as Transport Mode

   c) The Expression is true by default

   d) Click **OK**



Enable Analytics

Selected Virtual Server - Content Switching: 1

☑ Web Insight

□ Client Side Measurement

□ WAF Security Violations

□ Bot Security Violations

☑ Advanced Security Analytics

Advanced Options

For ADC version less than 12.0 **IPFIX** is default Transport mode.

Transport Mode

● 0 ○ 1

Instance level options

□ Enable HTTP X-Forwarded-For

□ Citrix Gateway

□ Enable Cookie Header

□ Enable URL Query Params

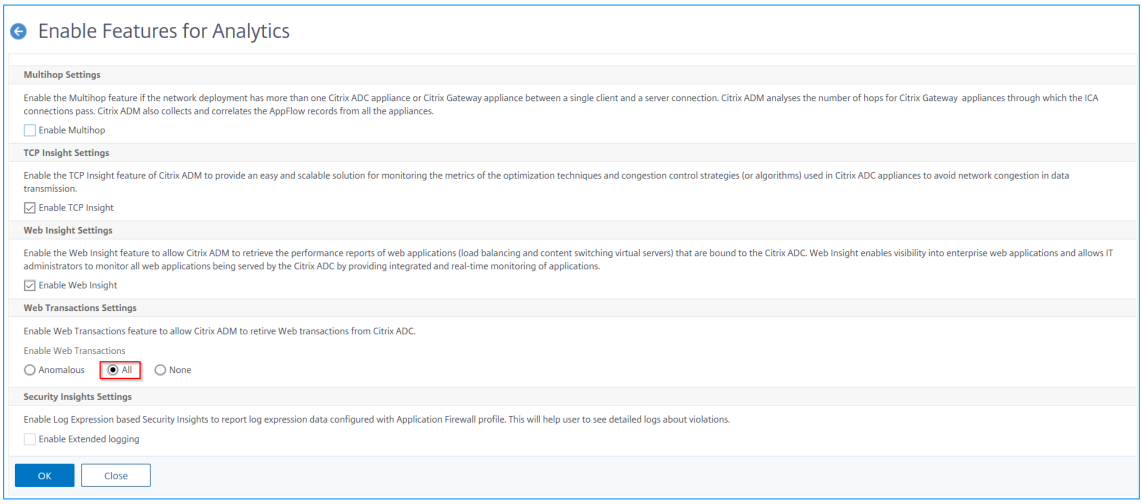
Enable Web Transaction settings

1. Navigate to **Settings > Analytics Settings**.

   The **Analytics Settings** page is displayed.

2. Click **Enable Features for Analytics**.

3. Under **Web Transaction Settings**, select **All**.



Enable Features for Analytics

Multihop Settings

Enable the Multihop feature if the network deployment has more than one Citrix ADC appliance or Citrix Gateway appliance between a single client and a server connection. Citrix ADM analyses the number of hops for Citrix Gateway appliances through which the ICA connections pass. Citrix ADM also collects and correlates the AppFlow records from all the appliances.

□ Enable Multihop

TCP Insight Settings

Enable the TCP Insight feature of Citrix ADM to provide an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in Citrix ADC appliances to avoid network congestion in data transmission.

☑ Enable TCP Insight

Web Insight Settings

Enable the Web Insight feature to allow Citrix ADM to retrieve the performance reports of web applications (load balancing and content switching virtual servers) that are bound to the Citrix ADC. Web Insight enables visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the Citrix ADC by providing integrated and real-time monitoring of applications.

☑ Enable Web Insight

Web Transactions Settings

Enable Web Transactions feature to allow Citrix ADM to retirve Web transactions from Citrix ADC.

Enable Web Transactions

○ Anomalous ● All ○ None

Security Insights Settings

Enable Log Expression based Security Insights to report log expression data configured with Application Firewall profile. This will help user to see detailed logs about violations.

□ Enable Extended logging

4. Click **Ok**.

Configure behavior check profiles

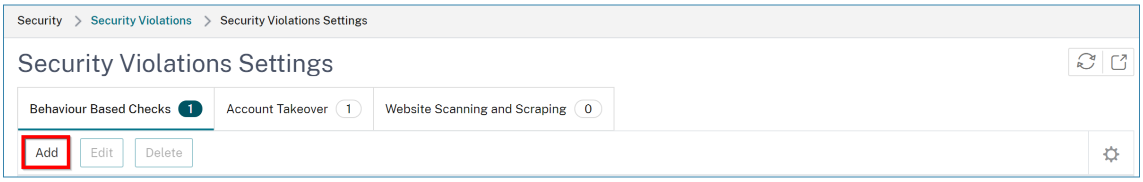
Citrix Application Delivery and Management enables you to select the behavior based violations. For **Excessive Client Connections**, **Website Scanning**, **Unusually high upload transactions**, and **Unusually high download transactions** violations, you can choose the sensitivity level as **Low**, **Medium**, and **High**. By creating a profile, you can decide how you want Citrix Application Delivery and Management to report the total number of anomalies for these violations.

To configure this setting:

1. Navigate to **Security > Security Violations**.

2. Click the settings icon that is available next to the time duration list.

3. Under **Behavior Based Checks**, click **Add**.



Security > Security Violations > Security Violations Settings
Security Violations Settings
Behaviour Based Checks 1
Account Takeover 1
Website Scanning and Scraping 0
Add
Edit
Delete

4. Specify the following parameters:

    a) **Behavior Based Check Profile Name** – Specify a profile name of your choice.

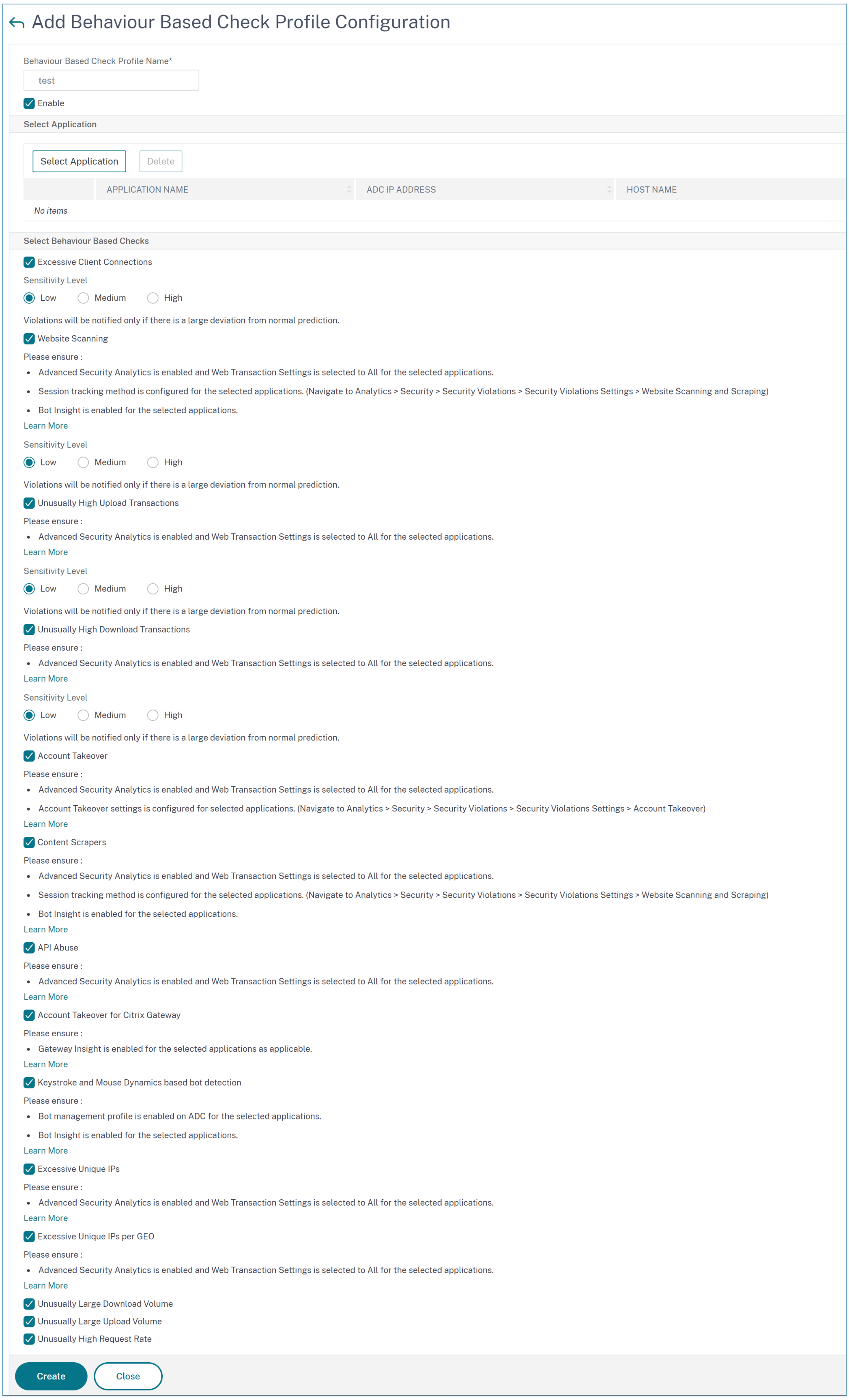
    b) Select the **Enable** option. By default, this option is selected.

    c) Under **Select Application**, select the applications for which you want to apply the profile.

d) Under **Select Behavior Based Checks**, select **Low**, **Medium**, or **High** to define the sensitivity level for those mentioned violations.

> **Note**
>
> By default, all other behavior-based violations are also enabled. If you disable any violation, Citrix Application Delivery and Management detects anomalies for these violations only based on a normal prediction.

e) Click **Create**.



Add Behaviour Based Check Profile Configuration

Behaviour Based Check Profile Name*

test

☑ Enable

Select Application

APPLICATION NAME	ADC IP ADDRESS	HOST NAME

No items

Select Behaviour Based Checks

☑ Excessive Client Connections

Sensitivity Level

● Low ○ Medium ○ High

Violations will be notified only if there is a large deviation from normal prediction.

☑ Website Scanning

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.
- Session tracking method is configured for the selected applications. (Navigate to Analytics > Security > Security Violations > Security Violations Settings > Website Scanning and Scraping)
- Bot Insight is enabled for the selected applications.

Learn More

Sensitivity Level

● Low ○ Medium ○ High

Violations will be notified only if there is a large deviation from normal prediction.

☑ Unusually High Upload Transactions

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.

Learn More

Sensitivity Level

● Low ○ Medium ○ High

Violations will be notified only if there is a large deviation from normal prediction.

☑ Unusually High Download Transactions

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.

Learn More

Sensitivity Level

● Low ○ Medium ○ High

Violations will be notified only if there is a large deviation from normal prediction.

☑ Account Takeover

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.
- Account Takeover settings is configured for selected applications. (Navigate to Analytics > Security > Security Violations > Security Violations Settings > Account Takeover)

Learn More

☑ Content Scrapers

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.
- Session tracking method is configured for the selected applications. (Navigate to Analytics > Security > Security Violations > Security Violations Settings > Website Scanning and Scraping)
- Bot Insight is enabled for the selected applications.

Learn More

☑ API Abuse

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.

Learn More

☑ Account Takeover for Citrix Gateway

Please ensure :

- Gateway Insight is enabled for the selected applications as applicable.

Learn More

☑ Keystroke and Mouse Dynamics based bot detection

Please ensure :

- Bot management profile is enabled on ADC for the selected applications.
- Bot Insight is enabled for the selected applications.

Learn More

☑ Excessive Unique IPs

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.

Learn More

☑ Excessive Unique IPs per GEO

Please ensure :

- Advanced Security Analytics is enabled and Web Transaction Settings is selected to All for the selected applications.

Learn More

☑ Unusually Large Download Volume

☑ Unusually Large Upload Volume

☑ Unusually High Request Rate

API gateway

September 25, 2021

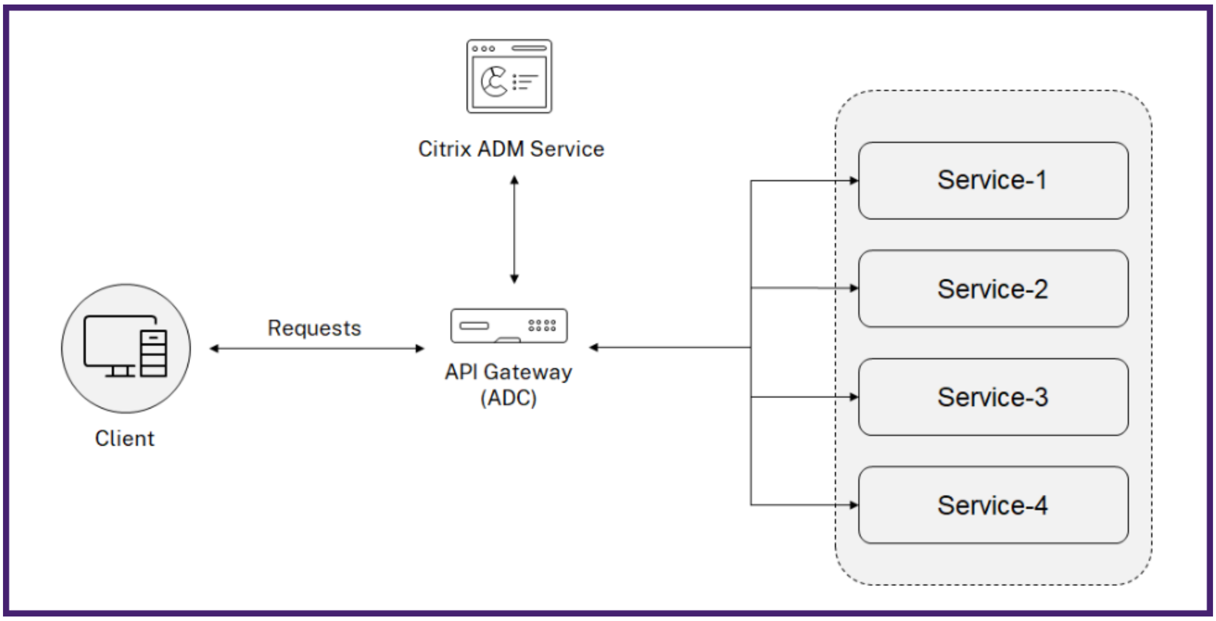
An API gateway acts as the entry point for all requests to your API endpoints. And, ensures secure and reliable access to all API endpoints and microservices in your system.

An API gateway proxies all requests and responses between your API clients/applications and back-end API services. It helps you configure, manage, and secure API endpoints. You can also create and manage API definitions in one of the following ways:

- Upload Swagger OAS specification file
- Create your own API definition

For more information, see Create or upload an API definition.

The following image describes how the API gateway receives the client request and sends the response from the back-end API services:



> **Note**
>
> In Citrix Application Delivery and Management, this feature is available for the users who have Premium or Advanced licenses.

Benefits of API gateway

The API gateway provides you the following benefits:

- **Secures your API endpoints**: The API gateway adds a security layer and it protects your API endpoints and back-end API servers from the attacks such as:

  - Buffer Overflow
  - SQL injection
  - Cross-site scripting
  - Denial of Service (Dos)

- **Monitors and improves the API performance**: The API gateway provides services such as SSL offloading, Authentication, Authorization, Rate limiting, and more. These services increase the API performance and its availability.

  The API analytics provide you the visibility to your API performance metrics and threats to your API endpoints. For more information, see View API analytics.

- **Manages the API traffic**: The API gateway abstracts the complexity of your back-end API infrastructure.

- **Discovers API endpoints**: The API gateway discovers the API endpoints that are in your organization and adds to the **API Discovery** page.

Manage API gateway

As an administrator, you can create API definitions and deploy the API instances on an API gateway (ADC) in Citrix Application Delivery and Management. For more information, see:

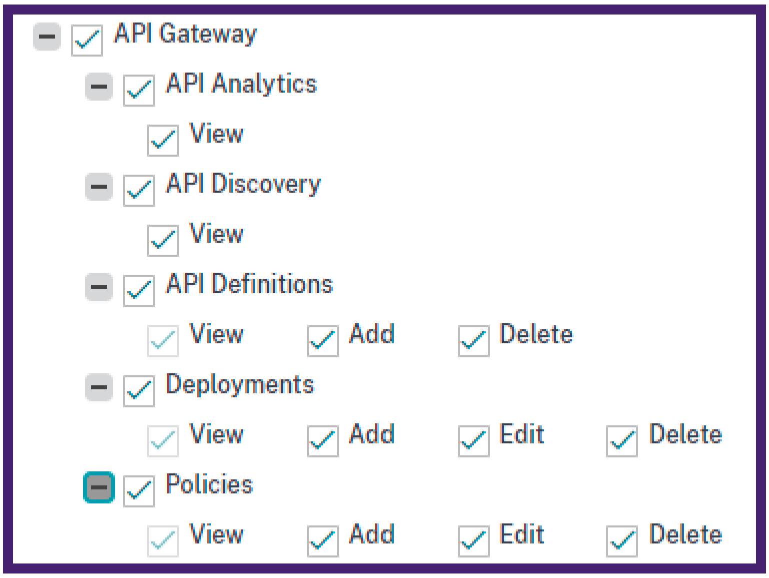
- Add an API definition
- Deploy an API instance

In an API gateway, you can apply security policies. To know how to create an API policy, see Add policies to an API deployment.

Grant API gateway configuration and management permissions

As an administrator, you can create an access policy to grant user permissions for API gateway configuration and management. The user permissions can be view, add, edit, and delete. Do the following to grant permissions:

1. Navigate to **Settings > User & Roles > Access policies**.
2. Click **Add**.
3. In **Create Access Policies**, specify a policy Name and the description.
4. In the **Permissions** field, expand **Applications** and then **API Gateway**.
5. Select the required **API Gateway** pages. Then, select the permissions that you want to grant.



- ☑ API Gateway
  - ☑ API Analytics
    - ☑ View
  - ☑ API Discovery
    - ☑ View
  - ☑ API Definitions
    - ☑ View ☑ Add ☑ Delete
  - ☑ Deployments
    - ☑ View ☑ Add ☑ Edit ☑ Delete
  - ☑ Policies
    - ☑ View ☑ Add ☑ Edit ☑ Delete

> **Important**
>
> Ensure to grant permissions for the features that are necessary to use an API gateway. For example, if you grant user access to the **Deployments** page, the following features also require user access:
>
> - StyleBooks
> - IPAM
> - Load Balancing (Under **Network Functions**)
> - Content Switching (Under **Network Functions**)
> - Device API Proxy (Under **API**)

For more information about access policies, see Configure access policies on Citrix Application Delivery and Management.

Integration with Splunk

October 20, 2021

You can now integrate Citrix Application Delivery and Management with Splunk to view analytics for WAF and Bot violations in your Splunk dashboard. Splunk add-on enables you to:

- Combine all other external data sources
- Provide greater visibility of analytics in a centralized place

Citrix Application Delivery and Management collects Bot and WAF 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 WAF and Bot violations in the Splunk dashboard.

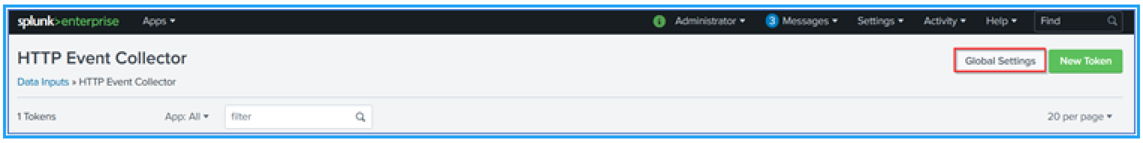
Prerequisites

For Splunk integration, you must:

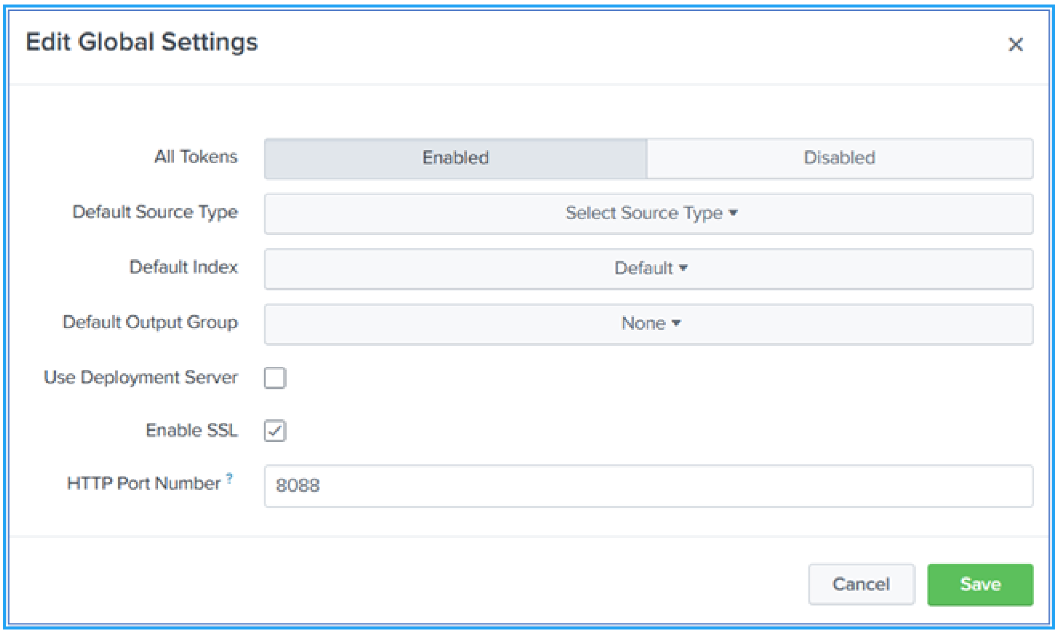
- Set up the global setting
- Set up the HTTP Event Collector endpoint in Splunk
- Install the Splunk Common Information Model (CIM) add-on
- Install the Citrix CIM normalizer
- Add the Splunk HTTP collector and token details

Set up the global setting

1. Log on to Splunk
2. Navigate to **Settings > Data Inputs > HTTP event collector**
   The **HTTP event collector** page is displayed
3. Click **Global Settings**



4. Specify the following parameters and click **Save**



Edit Global Settings

All Tokens: Enabled

Default Source Type: Select Source Type

Default Index: Default

Default Output Group: None

Use Deployment Server: □

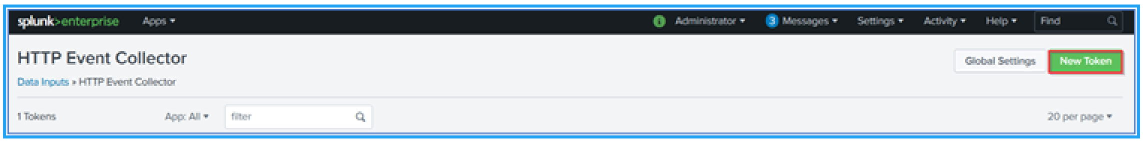
Enable SSL: ☑

HTTP Port Number: 8088

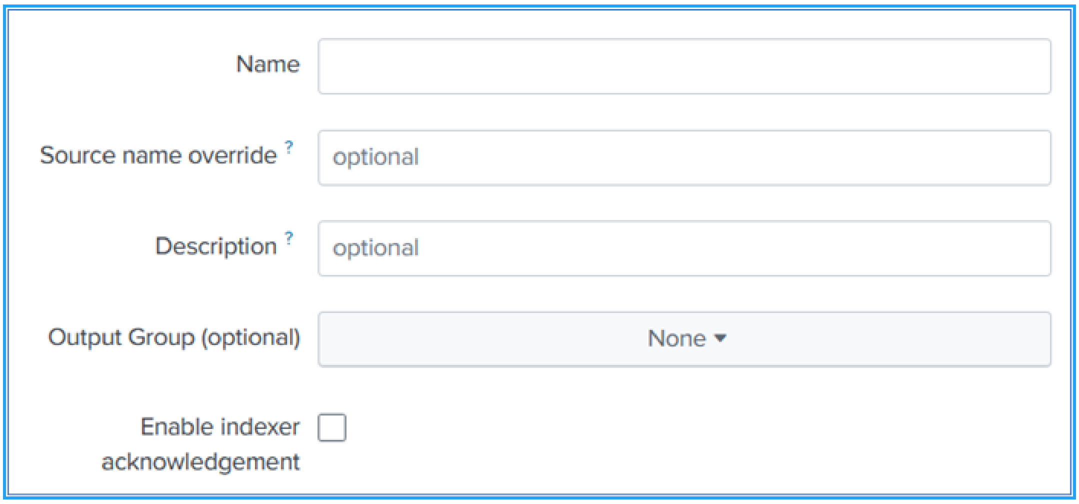
> Note
>
> By default, the HTTP Port Number indicates the default port. If you have any other preferred port number, you can specify the required port number.

Set up the HTTP Event Collector endpoint in Splunk

1. Log on to Splunk
2. Navigate to **Settings > Data Inputs > HTTP event collector**
   The **HTTP event collector** page is displayed
3. Click **New Token**



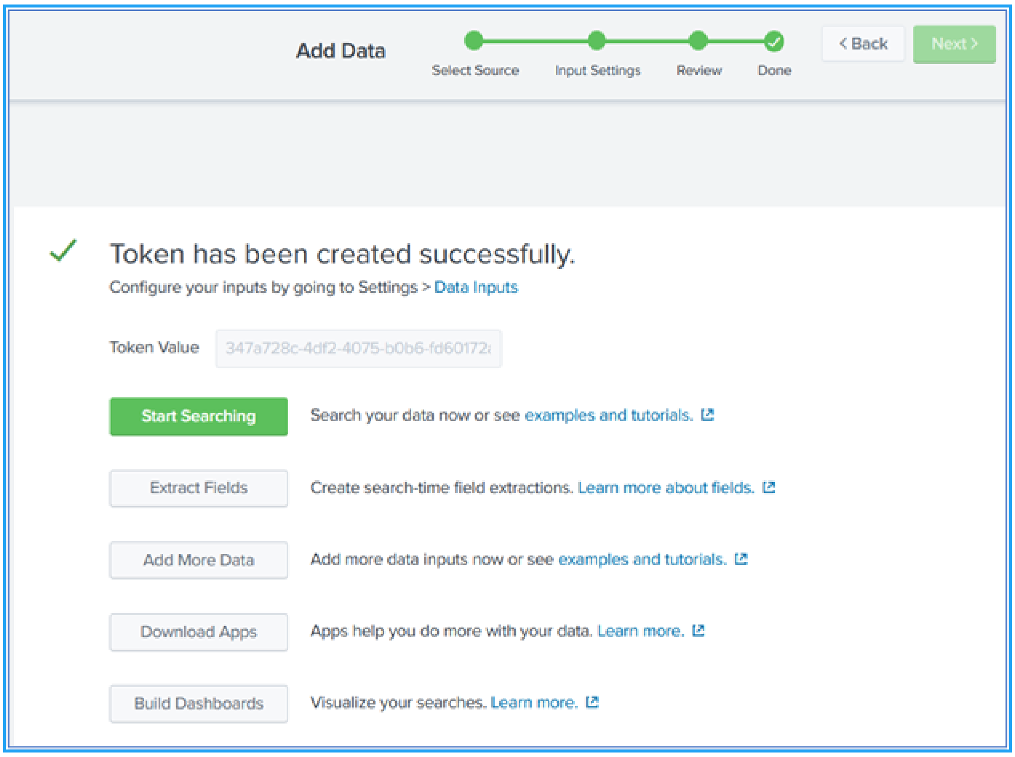
4. Specify the following:
   a) **Name**: Specify a name of your choice
   b) **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector
   c) **Description (optional)**: Specify a description
   d) **Output Group (optional)**: By default, this option is selected as None
   e) **Enable indexer acknowledgement**: By default, this option is not selected



Name	
Source name override ?	optional
Description ?	optional
Output Group (optional)	None ▾
Enable indexer acknowledgement	□

   f) Click **Next**
   g) In the **Input Settings** page, specify the **Source Type**, **App context**, **Index**, and then click **Review**

h) Review if everything you have specified is correct and then click Submit
A token gets generated. You must use this token when you add details in Citrix Application Delivery and Management



Token has been created successfully.
Configure your inputs by going to Settings > Data Inputs

Token Value 347a728c-4df2-4075-b0b6-fd60172

Search your data now or see examples and tutorials.

Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

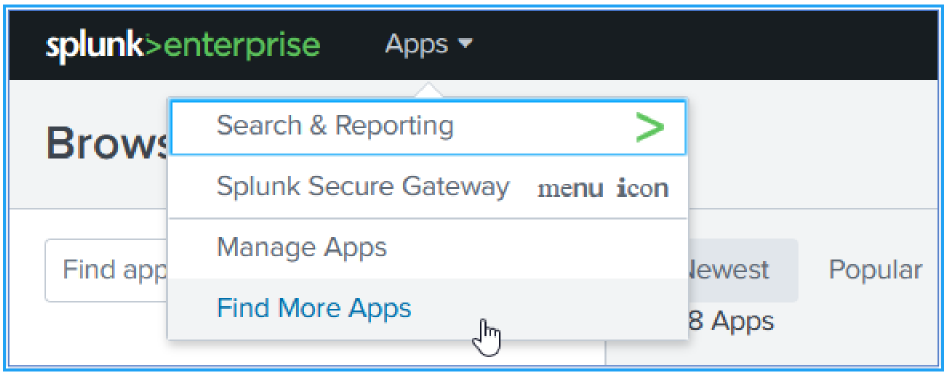
Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

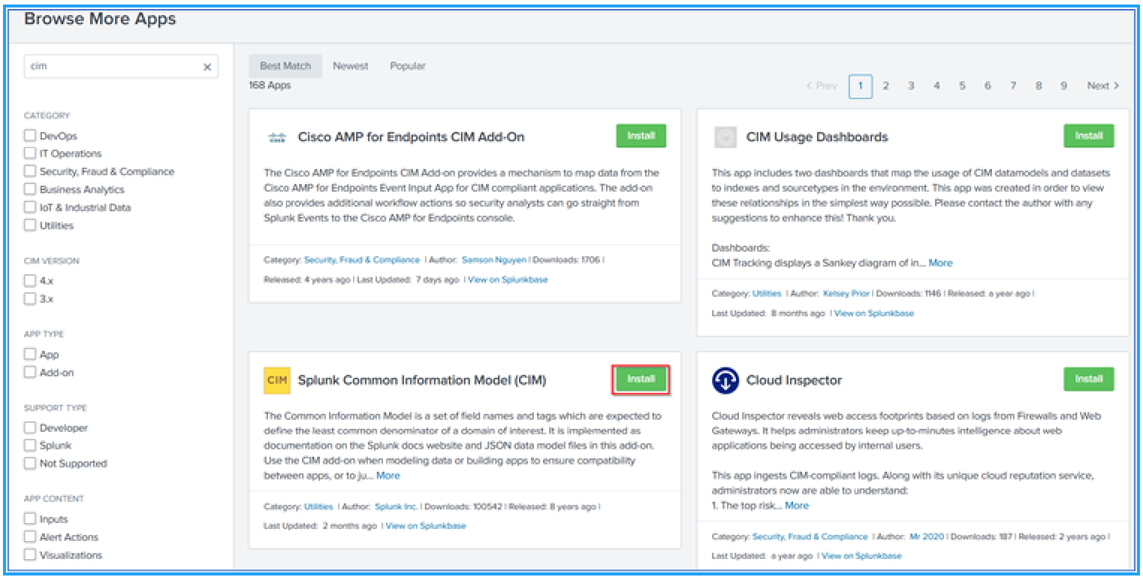
Install the Splunk Common Information Model

In Splunk, you must install the Splunk CIM to ensure that the data are populated in the dashboard.

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**



Cisco AMP for Endpoints CIM Add-On

The Cisco AMP for Endpoints CIM Add-on provides a mechanism to map data from the Cisco AMP for Endpoints Event Input App for CIM compliant applications. The add-on also provides additional workflow actions so security analysts can go straight from Splunk Events to the Cisco AMP for Endpoints console.

Category: Security, Fraud & Compliance | Author: Samson Nguyen | Downloads: 1706 | Released: 4 years ago | Last Updated: 7 days ago | View on Splunkbase

CIM Usage Dashboards

This app includes two dashboards that map the usage of CIM datamodels and datasets to indexes and sourcetypes in the environment. This app was created in order to view these relationships in the simplest way possible. Please contact the author with any suggestions to enhance this! Thank you.

Dashboards:
CIM Tracking displays a Sankey diagram of in... More

Category: Utilities | Author: Kelsey Prior | Downloads: 1146 | Released: a year ago | Last Updated: 8 months ago | View on Splunkbase

Splunk Common Information Model (CIM)

The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when modeling data or building apps to ensure compatibility between apps, or to ju... More

Category: Utilities | Author: Splunk Inc. | Downloads: 100542 | Released: 8 years ago | Last Updated: 2 months ago | View on Splunkbase

Cloud Inspector

Cloud Inspector reveals web access footprints based on logs from Firewalls and Web Gateways. It helps administrators keep up-to-minutes intelligence about web applications being accessed by internal users.

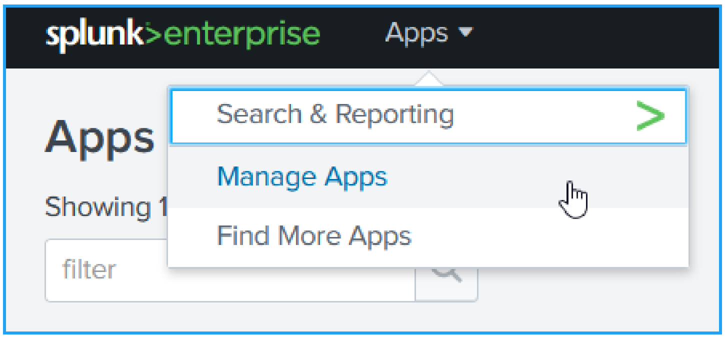
This app ingests CIM-compliant logs. Along with its unique cloud reputation service, administrators now are able to understand:
1. The top risk... More

Category: Security, Fraud & Compliance | Author: Mr 2020 | Downloads: 187 | Released: 2 years ago | Last Updated: a year ago | View on Splunkbase

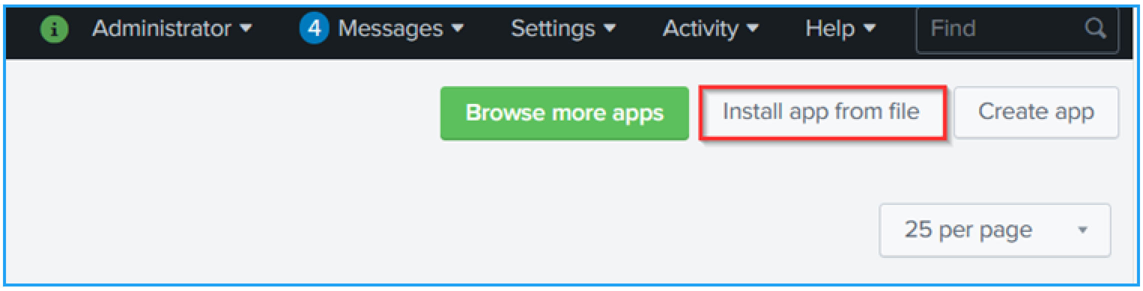
Install the Citrix CIM normalizer

After you install the Splunk CIM, you must install the Citrix CIM normalizer to transform the events into the Splunk CIM.

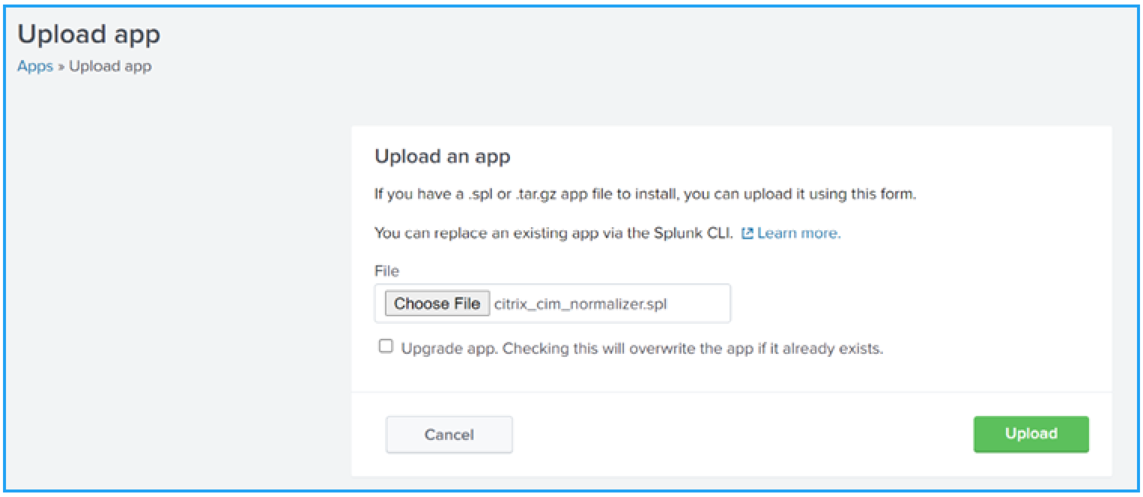
1. Log on to Citrix downloads page and download the Citrix CIM add-on for Splunk
2. In the Splunk portal, navigate to **Apps > Manage Apps**



3. Click **Install App from file**



4. Upload the **.spl** or **.tgz** file and click **Upload**



If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: citrix_cim_normalizer.spl

□ Upgrade app. Checking this will overwrite the app if it already exists.

You receive a notification message on the **Apps** page that the add-on is installed

Add the Splunk HTTP collector and token details

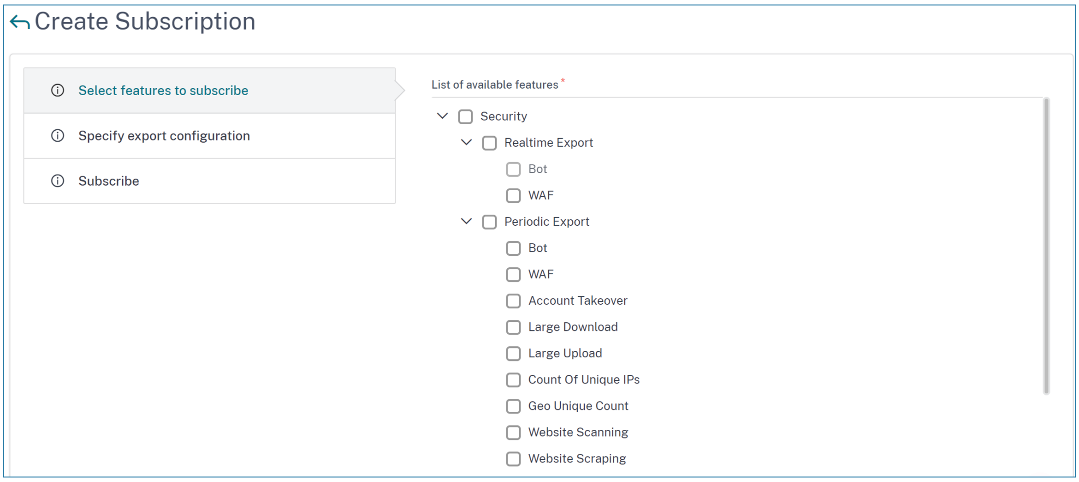
After you generate a token, you must add details in Citrix Application Delivery and Management to integrate with Splunk.

1. Log on to Citrix Application Delivery and Management
2. Navigate to **Settings > Ecosystem Integration**

   The **Create Subscription** page is displayed

3. In the **Select features to subscribe** tab enables you to select the features that you want to export and click **Next**

   - **Realtime Export** - Enables you to export to Splunk for realtime
   - **Periodic Export** - Enables you to export to Splunk based on the duration you select



4. In the **Specify export configuration** tab:

a) **End Point Type** – Select **Splunk** from the list

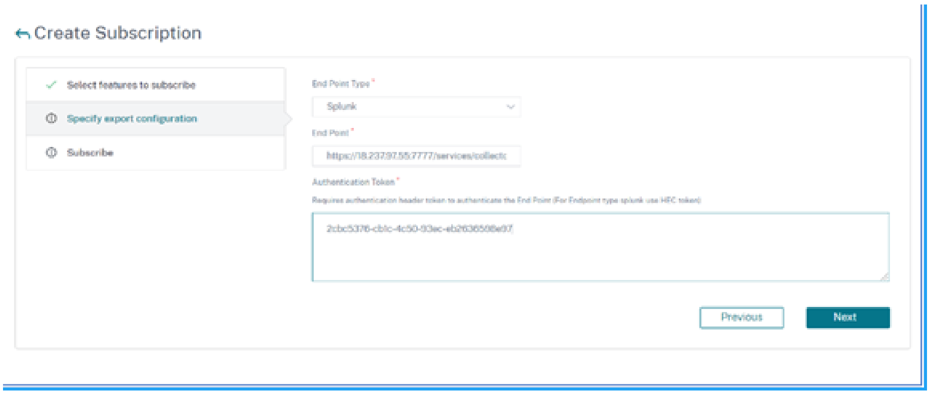
b) **End Point** – Specify the Splunk end point details. The end point must be in the https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event format.

> 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**



Create Subscription

✓ Select features to subscribe

Specify export configuration

Subscribe

End Point Type *: Splunk

End Point *: https://18.237.97.55:7777/services/collectc

Authentication Token *

Requires authentication header token to authenticate the End Point (For Endpoint type splunk use HEC token)

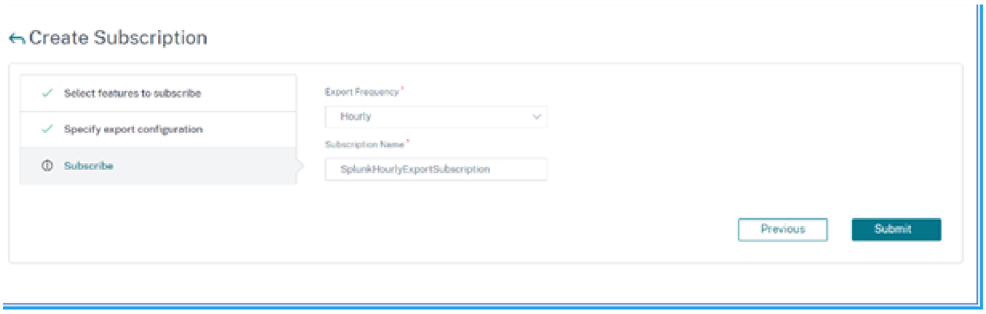
2cbc5376-cb1c-4c50-93ec-eb2636508e97

5. In the **Subscribe** page:

a) **Export Frequency** – Select Daily or Hourly from the list. Based on the selection, Citrix Application Delivery and Management exports the details to Splunk

b) **Subscription Name** – Specify a name of your choice

c) Click **Submit**



Create Subscription

✓ Select features to subscribe

✓ Specify export configuration

Subscribe

Export Frequency *: Hourly

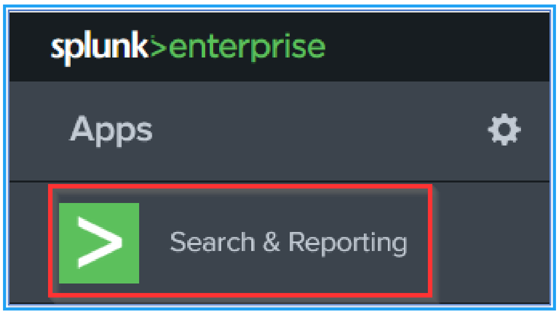
Subscription Name *: SplunkHourlyExportSubscription

> Note
>
> When you configure it 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).

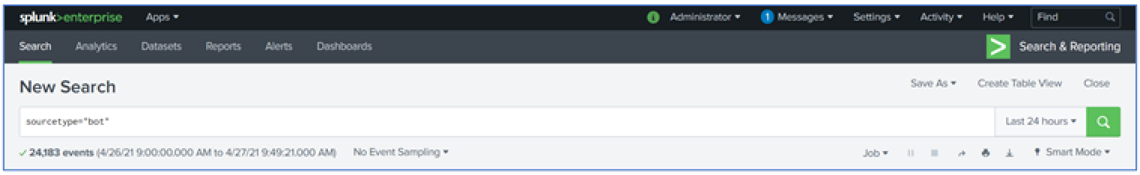
Verify details in Splunk

After you add details in Citrix Application Delivery and Management, you can verify if Splunk receives the events.

1. From the Splunk home page, click **Search & Reporting**

2. In the search bar, type the details in the search bar, select the duration from the list, and click the search icon or press Enter. For example, you can type `sourcetype=” bot”` or `sourcetype =” waf”` to check the details

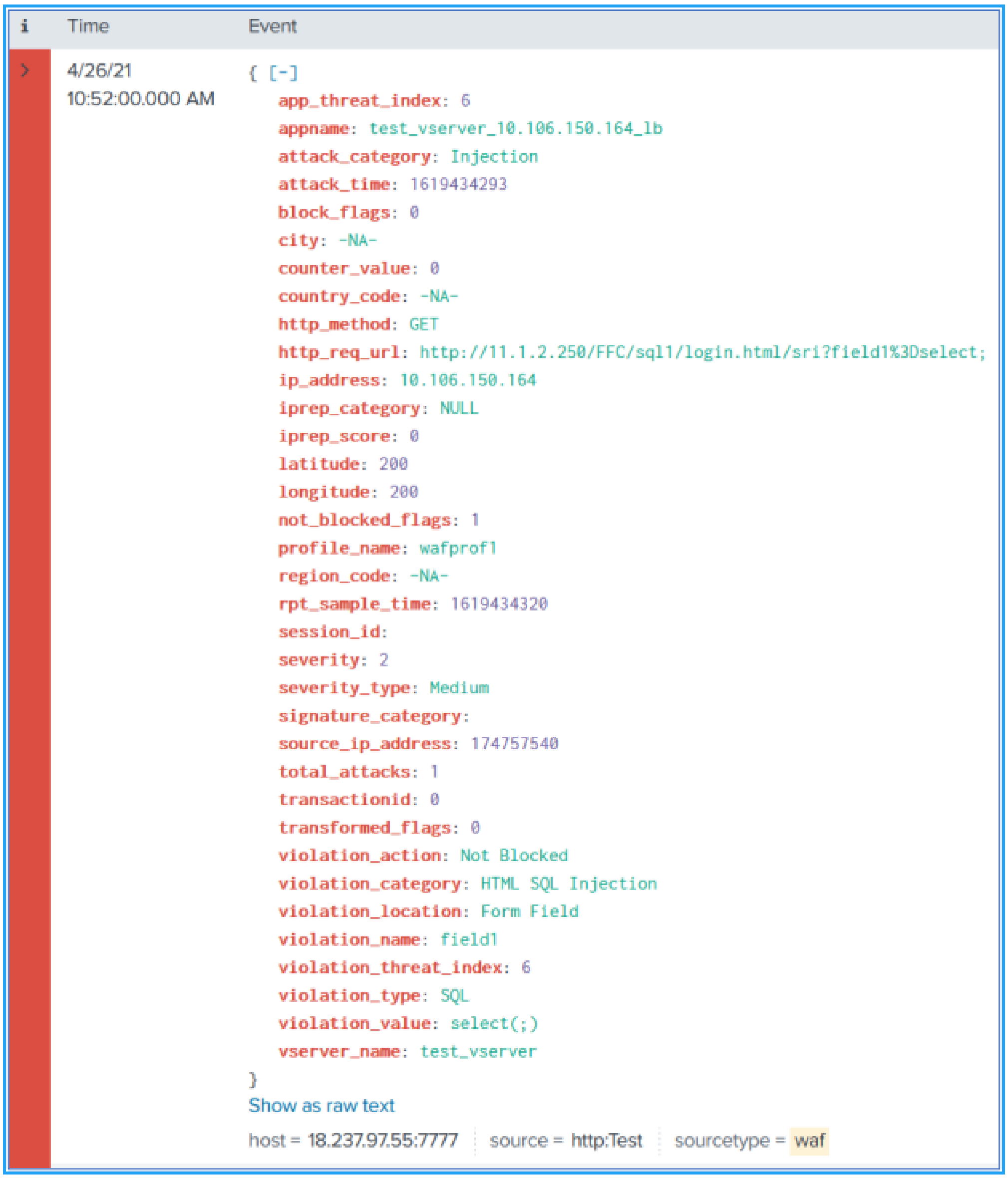
   

   sourcetype="bot"

   Last 24 hours ▾

   ✓ 24,183 events (4/26/21 9:00:00.000 AM to 4/27/21 9:49:21.000 AM) No Event Sampling ▾

   The following search result is an example for a WAF violation:

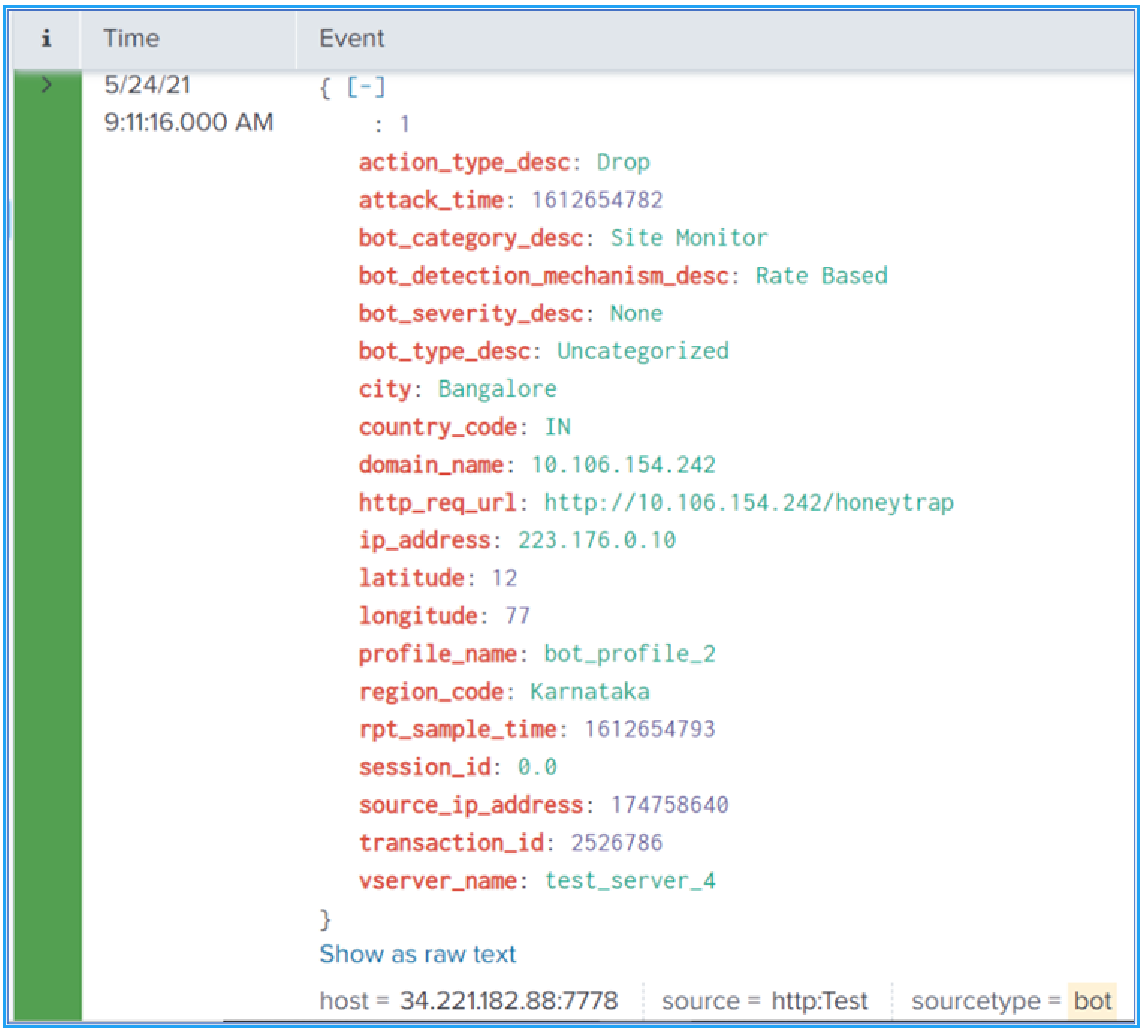


4/26/21
10:52:00.000 AM

```
{ [-]
   app_threat_index: 6
   appname: test_vserver_10.106.150.164_lb
   attack_category: Injection
   attack_time: 1619434293
   block_flags: 0
   city: -NA-
   counter_value: 0
   country_code: -NA-
   http_method: GET
   http_req_url: http://11.1.2.250/FFC/sql1/login.html/sri?field1%3Dselect;
   ip_address: 10.106.150.164
   iprep_category: NULL
   iprep_score: 0
   latitude: 200
   longitude: 200
   not_blocked_flags: 1
   profile_name: wafprof1
   region_code: -NA-
   rpt_sample_time: 1619434320
   session_id:
   severity: 2
   severity_type: Medium
   signature_category:
   source_ip_address: 174757540
   total_attacks: 1
   transactionid: 0
   transformed_flags: 0
   violation_action: Not Blocked
   violation_category: HTML SQL Injection
   violation_location: Form Field
   violation_name: field1
   violation_threat_index: 6
   violation_type: SQL
   violation_value: select(;)
   vserver_name: test_vserver
}
```

host = 18.237.97.55:7777 | source = http:Test | sourcetype = waf

The following search result is for a Bot violation:



5/24/21
9:11:16.000 AM

```
{ [-]
    : 1
   action_type_desc: Drop
   attack_time: 1612654782
   bot_category_desc: Site Monitor
   bot_detection_mechanism_desc: Rate Based
   bot_severity_desc: None
   bot_type_desc: Uncategorized
   city: Bangalore
   country_code: IN
   domain_name: 10.106.154.242
   http_req_url: http://10.106.154.242/honeytrap
   ip_address: 223.176.0.10
   latitude: 12
   longitude: 77
   profile_name: bot_profile_2
   region_code: Karnataka
   rpt_sample_time: 1612654793
   session_id: 0.0
   source_ip_address: 174758640
   transaction_id: 2526786
   vserver_name: test_server_4
}
```

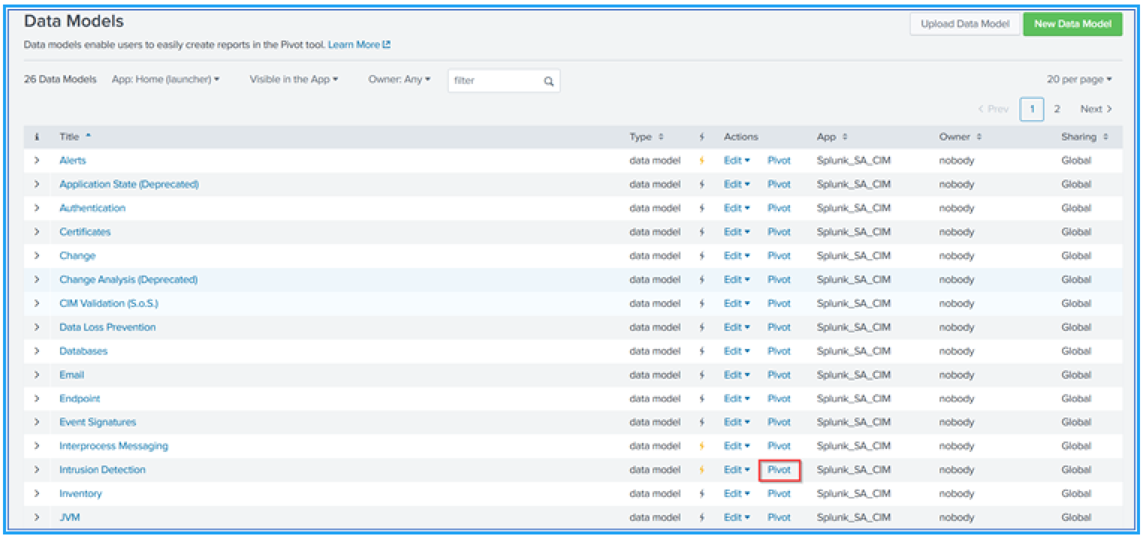
host = 34.221.182.88:7778 | source = http:Test | sourcetype = bot

Access Pivot details

You must identify the Data Model type to see the pivot details. For example, the Splunk add-on converts the WAF and Bot events in CIM format, with the closest data model type such as Alert and Intrusion Detection.

To access the events in Splunk:

1. Navigate to **Settings > Data Models**
2. Identify the **Intrusion Detection** data model and click **Pivot**

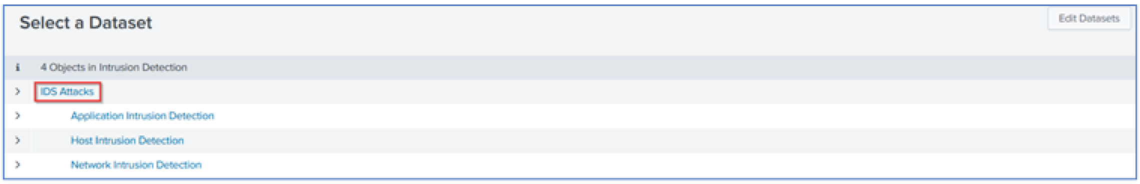


Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

i	Title	Type	⚡	Actions		App	Owner	Sharing
›	Alerts	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Application State (Deprecated)	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Authentication	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Certificates	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Change	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Change Analysis (Deprecated)	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	CIM Validation (S.o.S.)	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Data Loss Prevention	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Databases	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Email	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Endpoint	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Event Signatures	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Interprocess Messaging	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Intrusion Detection	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Inventory	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	JVM	data model	⚡	Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global

3. Select a Dataset. In the following example, the IDS Attacks option is selected

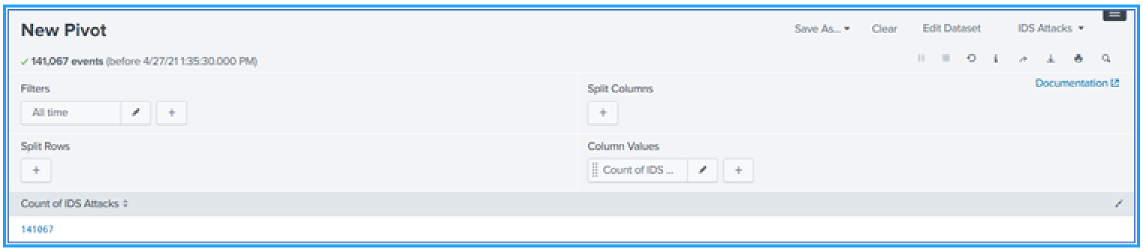


Select a Dataset

i 4 Objects in Intrusion Detection

- › IDS Attacks
  - › Application Intrusion Detection
  - › Host Intrusion Detection
  - › Network Intrusion Detection

The total count of IDS Attacks is displayed.



New Pivot

✓ 141,067 events (before 4/27/21 1:35:30.000 PM)

Filters: All time

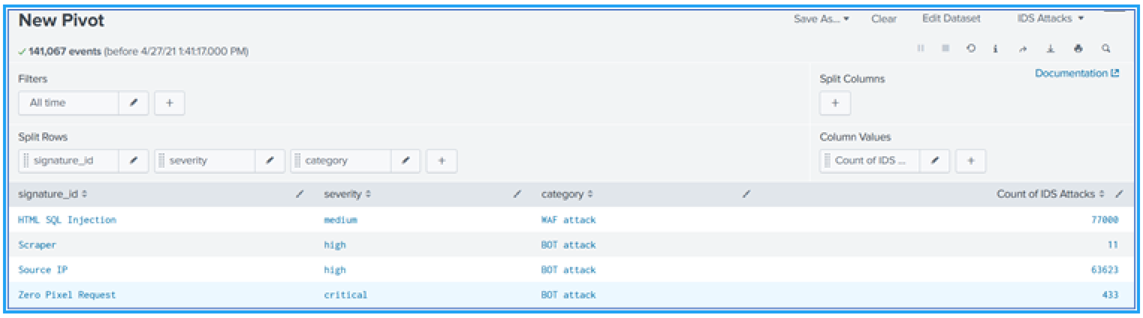
Split Columns: +

Split Rows: +

Column Values: Count of IDS ...

Count of IDS Attacks
141067

You can also click the **+** button to add more details to the table. The following example displays the details based on severity, category, and signature ID:



New Pivot

✓ 141,067 events (before 4/27/21 1:41:17.000 PM)

Filters: All time

Split Columns: +

Split Rows: signature_id, severity, category

Column Values: Count of IDS ...

signature_id	severity	category	Count of IDS Attacks
HTML SQL Injection	medium	WAF attack	77000
Scraper	high	BOT attack	11
Source IP	high	BOT attack	63623
Zero Pixel Request	critical	BOT attack	433

Splunk dashboard

Using a dashboard, you can view details of WAF and Bot violation analytics with panels such as charts, tables, lists, and so on. You can configure a:

- Dashboard with applications that use the CIM compatible data.
- Custom dashboard that pulls data from the CIM data models.

Depending upon your choice, you can create the dashboard. For more information, see the About dashboard section in Splunk documentation.

WAF learning engine

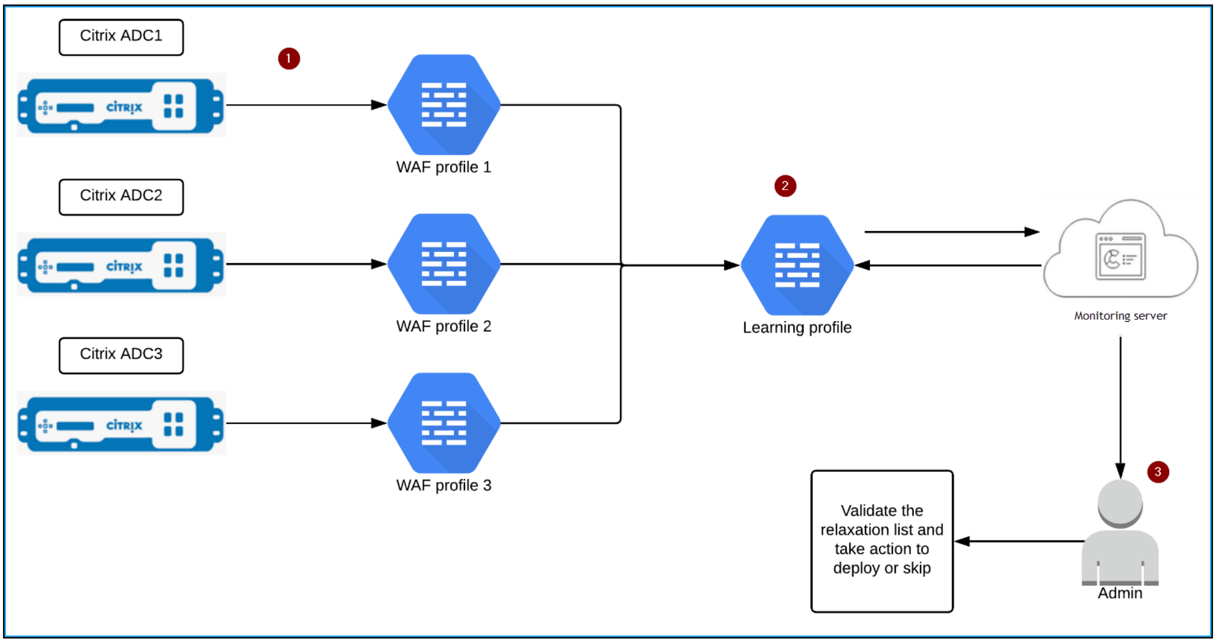
October 20, 2021

Citrix Web App Firewall (WAF) protects your web applications from malicious attacks such as SQL injection and cross-site scripting. To prevent data breaches and provide the right security protection, you must monitor your traffic for threats and real-time actionable data on attacks. Sometimes, the attacks reported might be false-positive and those need to be provided as an exception.

The Learning engine on Citrix Application Delivery and Management is a repetitive pattern filter that enables WAF to learn the behavior (the normal activities) of your web applications. Based on monitoring, the engine generates a list of suggested rules or exceptions for each security check applied on the HTTP traffic.

It is much easier to deploy relaxation rules using the Learning engine than manually deploy it as necessary relaxations.

The following image explains the high-level information on how the WAF learning in Citrix Application Delivery and Management works:



1 – Citrix ADC instances with its WAF profiles

2 – Configure a learning profile in Citrix Application Delivery and Management, add the WAF profiles, and select to auto deploy or manually deploy the relaxation rules

3 – Administrator can validate the relaxation rules in Citrix Application Delivery and Management and decide to deploy or skip

Get started

To deploy the learning feature, you must:

- Enable the centralized learning in the ADC instance. Run the following command in the ADC instance:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Ensure that the ADC instance version is **13.0-76.6** or later.
- Configure a Web App Firewall profile (set of security settings) on your Citrix ADC appliance. For more information, see Creating Web App Firewall profiles.

After you enable the centralized learning and configure the WAF profile, Citrix Application Delivery and Management generates a list of exceptions (relaxations) for the configured security check. As an administrator, you can review the list of exceptions in Citrix Application Delivery and Management and decide to deploy or skip.

Using the WAF learning feature in Citrix Application Delivery and Management, you can:

- Configure a learning profile with the following security checks:

  - Start URL
  - Cookie Consistency
  - Credit Card

    > **Note**
    >
    > For the credit card security check, you must configure the `doSecureCreditCardLogging` in Citrix ADC instance and ensure the setting is **OFF**.

  - Content Type
  - Form Field Consistency
  - Field Formats
  - CSRF Form Tagging
  - HTML Cross-Site Scripting
  - HTML SQL Injection

    > **Note**
    >
    > For the HTML SQL Injection check, you must configure `set -sqlinjectionTransformSpecialCh` `ON` and `set -sqlinjectiontype sqlspclcharorkeywords`in Citrix ADC instance.

  - HTML Command Injection

    > **Note**
    >
    > Supported only in ADC instance 13.0-72.12 or later.

- Check the relaxation rules in Citrix Application Delivery and Management and decide to take necessary action (deploy or skip)
- Get the notifications through email, slack, and ServiceNow
- Use the **Action Summary** page to view relaxation details

To use the WAF learning in Citrix Application Delivery and Management:

1. Configure the learning profile
2. See the relaxation rules
3. Use the WAF learning Action Summary page

WAF recommendations

September 24, 2021

Citrix Web App Firewall (WAF) and WAF Signatures protect your web applications from malicious attacks. WAF signatures provide specific, configurable rules to simplify the task of protecting your websites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, web server, website, XML-based web service, or other resource. To protect your application using signatures, you must review the rules, enable, and configure the ones that you want to apply.

Similarly, to prevent data breaches and provide the right security protection in the application, you must create a WAF profile with security checks. When you create a WAF profile in the ADC instance, the traffic might:

- Get generated with the mentioned security checks
- Not get generated with the mentioned security checks

The instance might be receiving other attacks, but you might not have enabled that security check in the WAF profiles.

As an administrator, you must understand to enable the right signatures and create the right WAF profiles to protect the web application. Identifying the right signatures and the WAF profiles might be a difficult task at some scenarios.

Citrix Application Delivery and Management WAF recommendation scans the application for vulnerabilities and generates the following recommendations:

- WAF Profile
- WAF Signature

For more information, see WAF profile and WAF Signatures.

WAF recommendation database is updated on a frequent duration to include any new vulnerabilities. You can scan and then select to enable the required recommendations. You can enable all signatures and security checks, but it might result in false positives and affect the ADC instance performance. Hence, it is recommended to select only the required security checks and signatures. WAF recommendation engine also automatically detects which signatures and security checks must be enabled for the application.

Gateway Insight

September 25, 2021

In a Citrix Gateway deployment, visibility into a user access detail is essential for troubleshooting access failure issues. As the network administrator, you want to know when a user is not able to log on to Citrix Gateway, and you want to know the user activity and the reasons for logon failure, but that 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 Citrix 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, 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.

You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with an ADC 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 Citrix Application Delivery and Management 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 Citrix Application Delivery and Management release and build must be same or later than that of the Citrix Gateway appliance.
- One hour of Gateway Insight reports can be viewed for ADC instances with Advanced license. A Premium license is required to view Gateway Insight reports beyond one hour.

Limitations:

- Citrix Gateway does not support Gateway Insight when the authentication method is configured as certificate-based authentication.
- 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 ADC Gateway appliance in the second DMZ is not available.
- Remote Desktop Protocol (RDP) desktop access issues are not reported.
- The Gateway Insight records for the SAML authentication 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

Enable Gateway Insight

To enable Gateway Insight for your Citrix Gateway appliance, you must first add the ADC Gateway appliance to Citrix Application Delivery and Management. You must then enable AppFlow for the virtual server representing the VPN application. For information about adding device to Citrix Application Delivery and Management, see Adding Instances.

> **Note**
>
> To view end-point analysis (EPA) failures in Citrix Application Delivery and Management, you must enable AppFlow authentication, authorization, and access control user name logging on the ADC Gateway appliance.

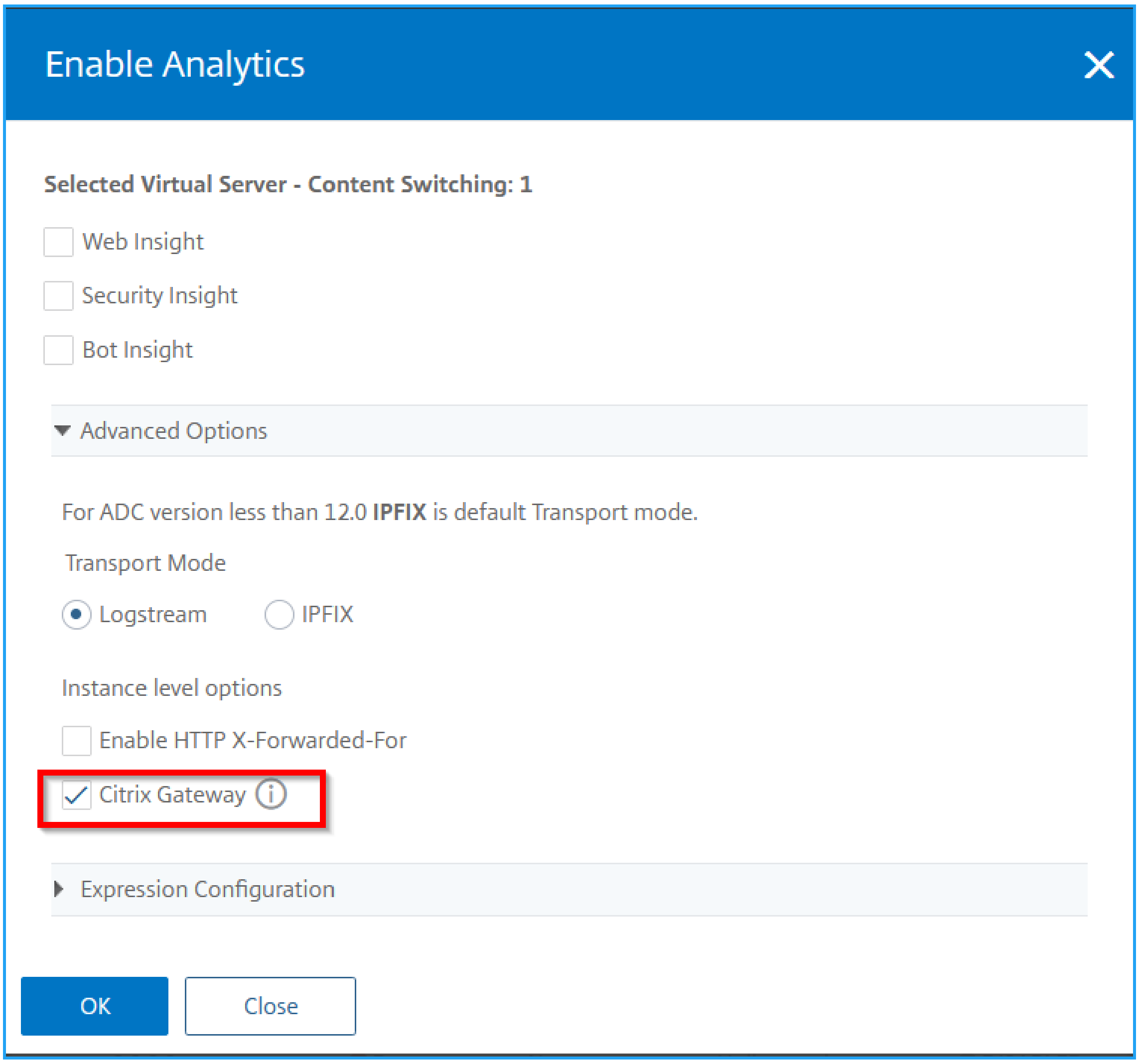
Enable AppFlow for a virtual server in Citrix Application Delivery and Management

1. Navigate to **Infrastructure > Instances > Citrix ADC**, and select the instance for which you want to enable AppFlow.

2. From the **Select Action** list, select **Configure Analytics**.

3. Select the virtual server and then click **Enable Analytics**.

4. Under **Advanced Options**, select **Citrix Gateway**.



Enable Analytics

Selected Virtual Server - Content Switching: 1

□ Web Insight

□ Security Insight

□ Bot Insight

▾ Advanced Options

For ADC version less than 12.0 **IPFIX** is default Transport mode.

Transport Mode

● Logstream ○ IPFIX

Instance level options

□ Enable HTTP X-Forwarded-For

☑ Citrix Gateway ⓘ

▸ Expression Configuration

5. Click OK.

Enable AppFlow user name logging on an ADC 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**.

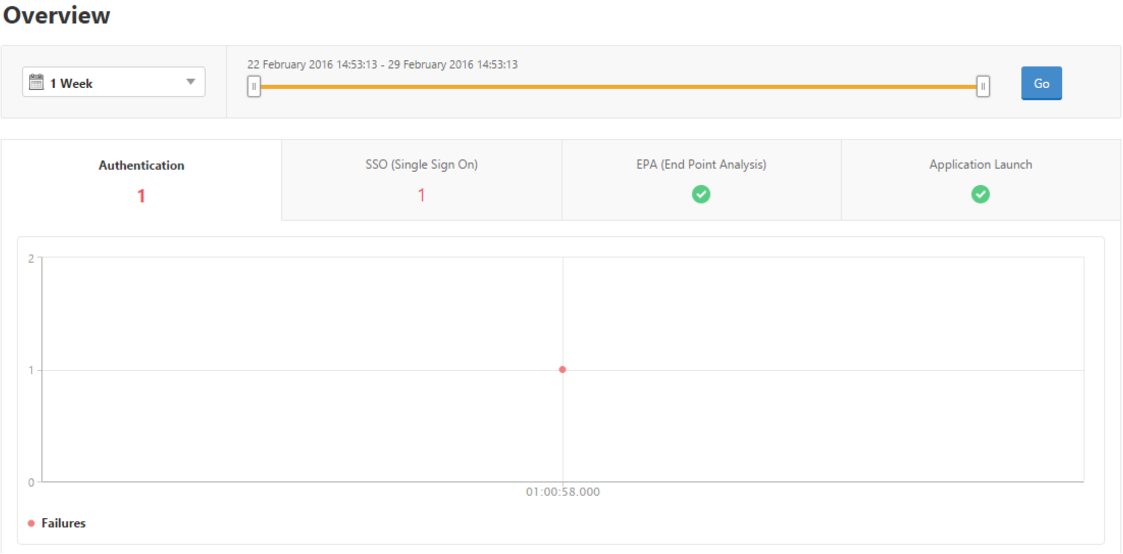
View Gateway Insight reports

In Citrix Application Delivery and Management, you can view reports for all users, applications, and gateways associated with the ADC 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. Citrix Application Delivery and Management 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 on Citrix Application Delivery and Management.

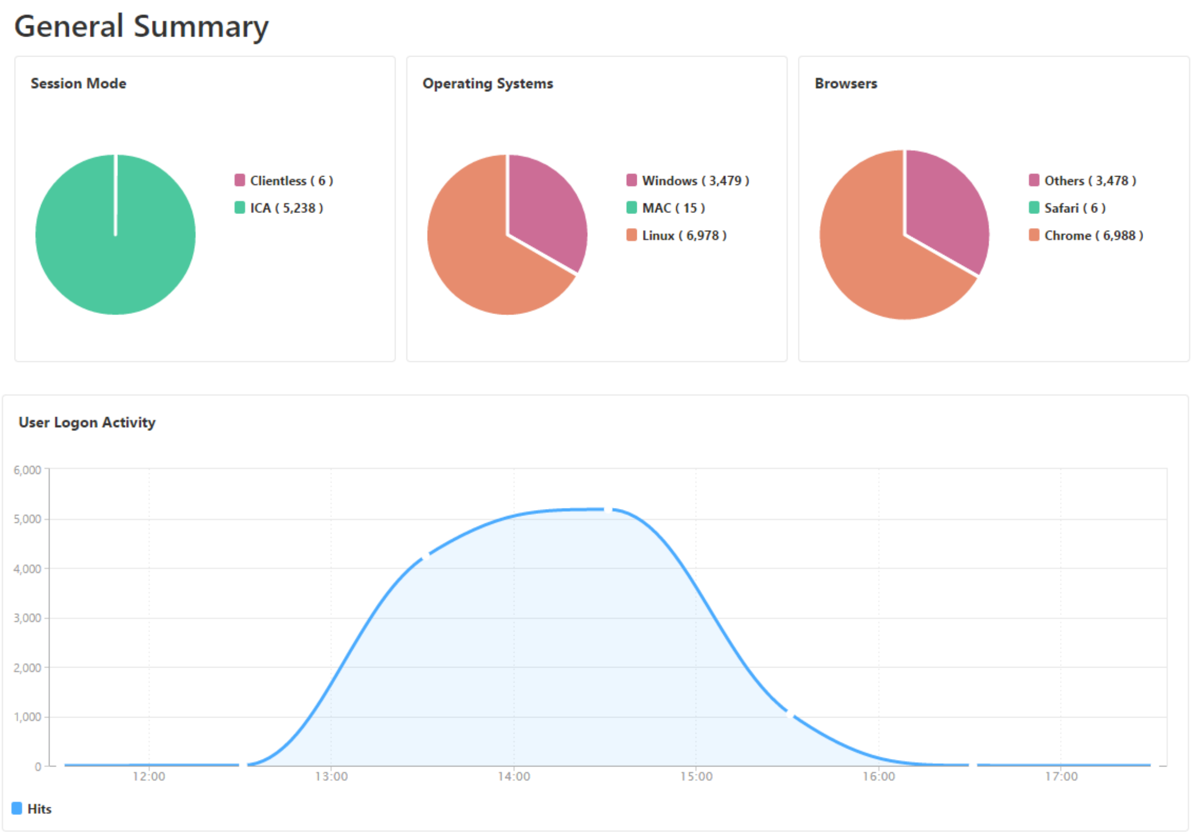
View EPA, SSO, authentication, authorization, and application launch failures

1. In Citrix Application Delivery and Management, 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.



View summary of session modes, clients, and the number of users

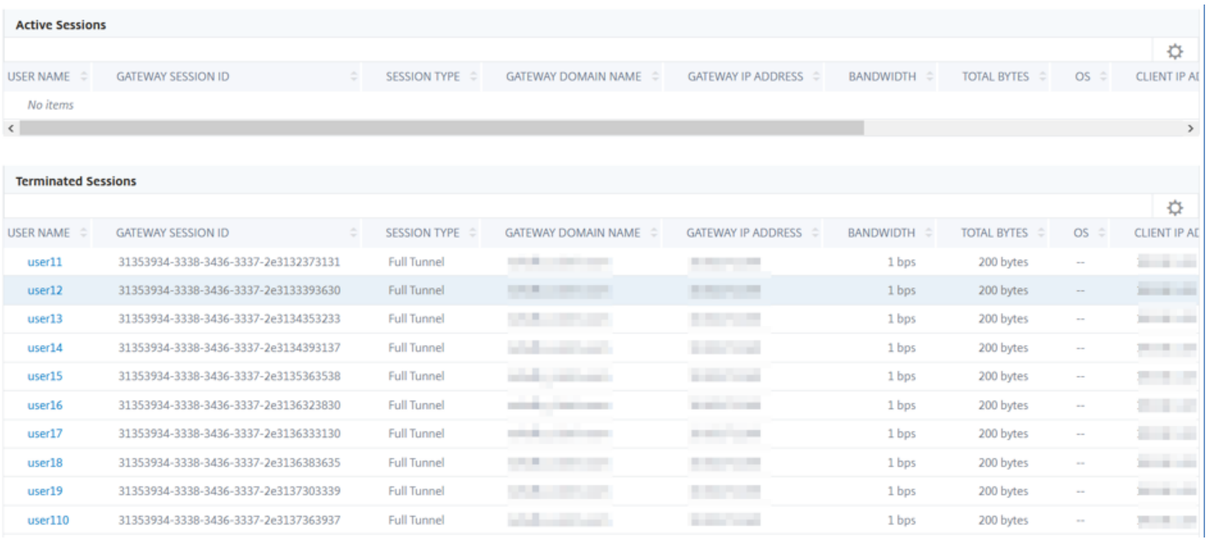
In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight**, scroll down to view the reports.



Users

You can view a complete report for the users associated with the ADC Gateway appliances. You can view the EPA, authentication, SSO, application launch failures, and so on for a user.

You can also visualize a consolidated view of all users active and terminated sessions.



Active Sessions

USER NAME	GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP AI
No items								

Terminated Sessions

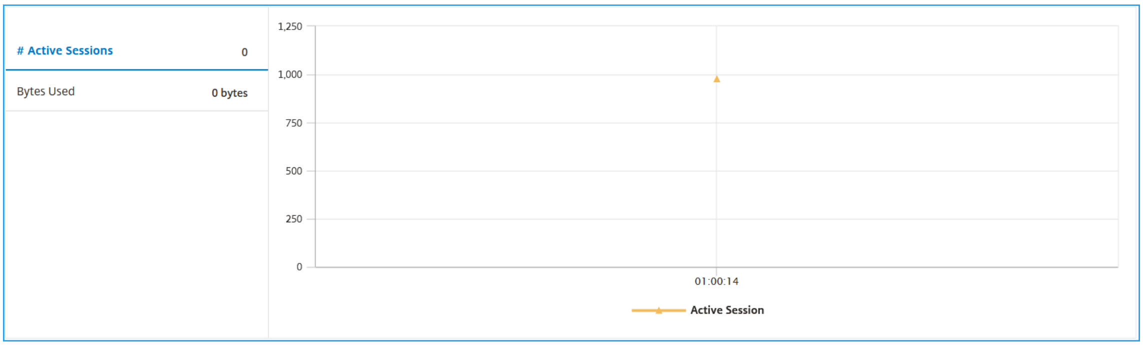
USER NAME	GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP AI
user11	31353934-3338-3436-3337-2e3132373131	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user12	31353934-3338-3436-3337-2e3133393630	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user13	31353934-3338-3436-3337-2e3134353233	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user14	31353934-3338-3436-3337-2e3134393137	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user15	31353934-3338-3436-3337-2e3135363538	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user16	31353934-3338-3436-3337-2e3136323830	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user17	31353934-3338-3436-3337-2e3136333130	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user18	31353934-3338-3436-3337-2e3136383635	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user19	31353934-3338-3436-3337-2e3137303339	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]
user110	31353934-3338-3436-3337-2e3137363937	Full Tunnel	[redacted]	[redacted]	1 bps	200 bytes	--	[redacted]

As an administrator, this view enables you to:

- View all users details in a single-pane visualization
- Eliminate the complexity in selecting each user and seeing the active and terminated sessions

View user details

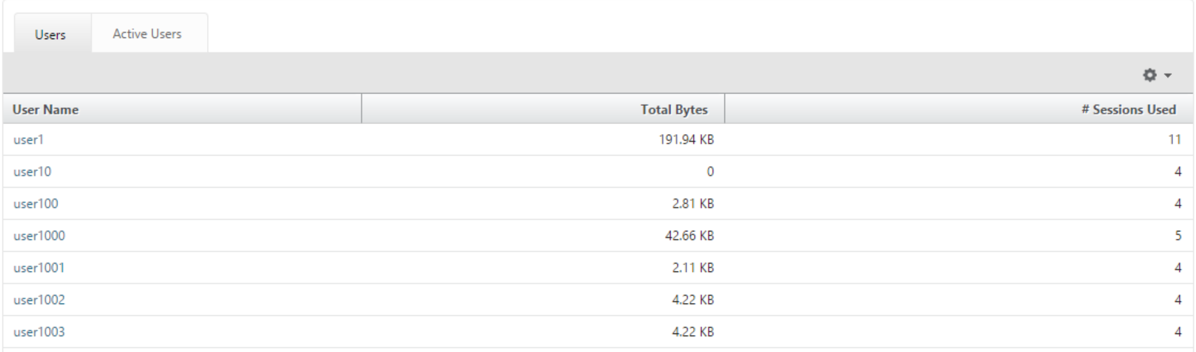
1. In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight > Users**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. You can view the number of active users, number of active sessions, and bytes by all users during the time period.



Active Sessions 0

Bytes Used 0 bytes

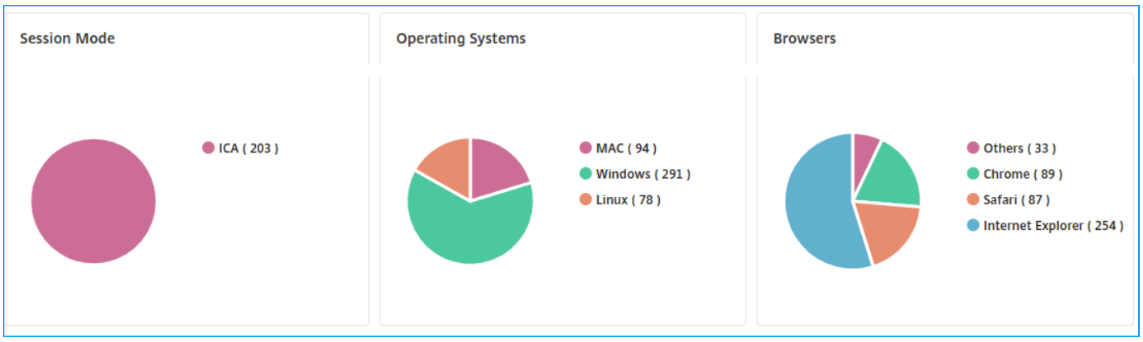
Scroll down to view a list of available users and active users.



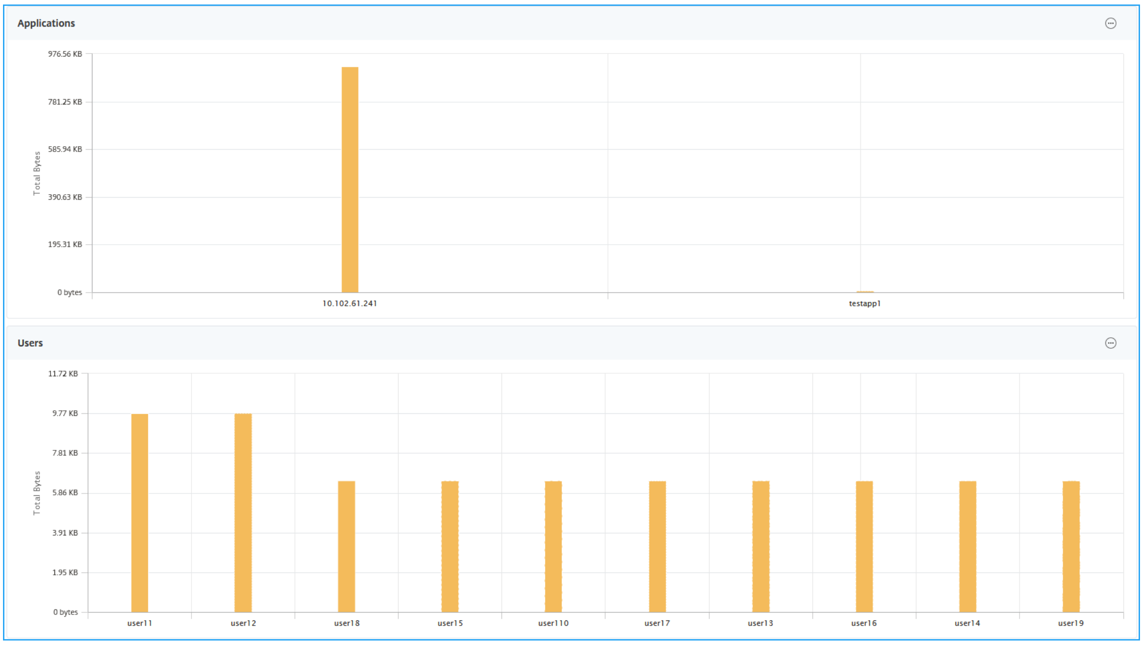
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

On the **Users** or **Active Users** tab, click a user to view the following user details:

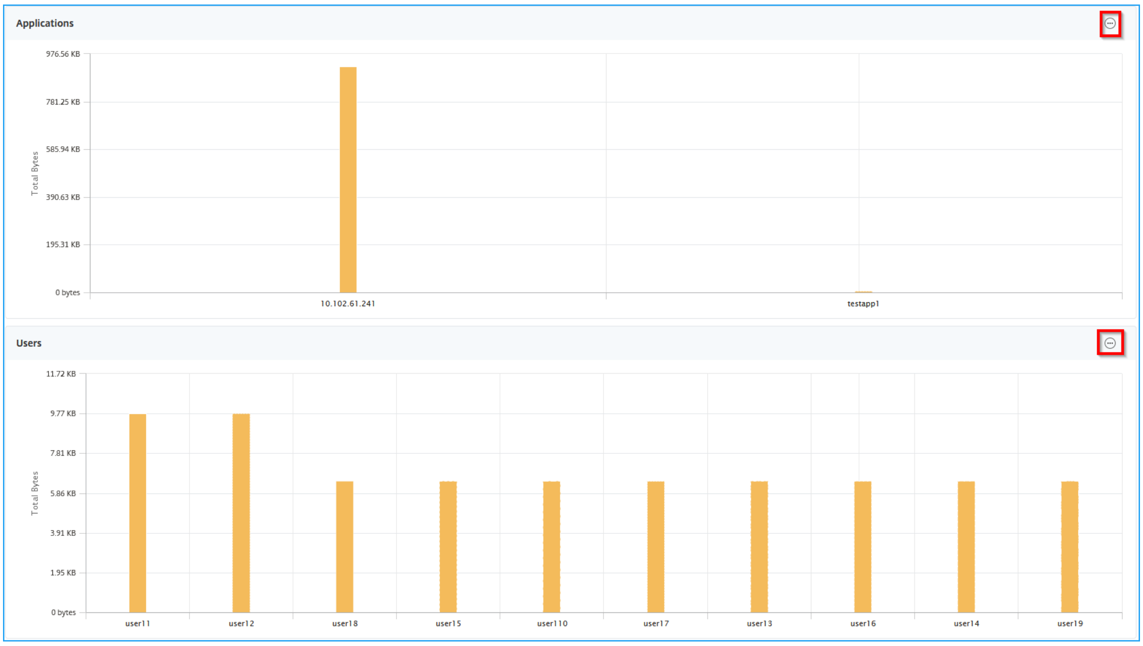
- **User details** - You can view insights for each user associated with the ADC Gateway appliances. Navigate to **Gateway** > **Gateway Insight** > **Users** and click a user to view insights for the selected user such as Session Mode, Operating System, and Browsers.



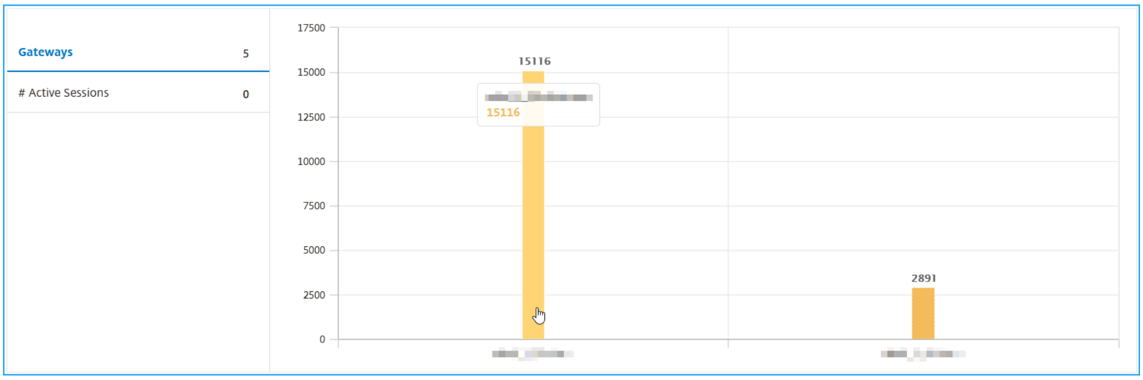
- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.



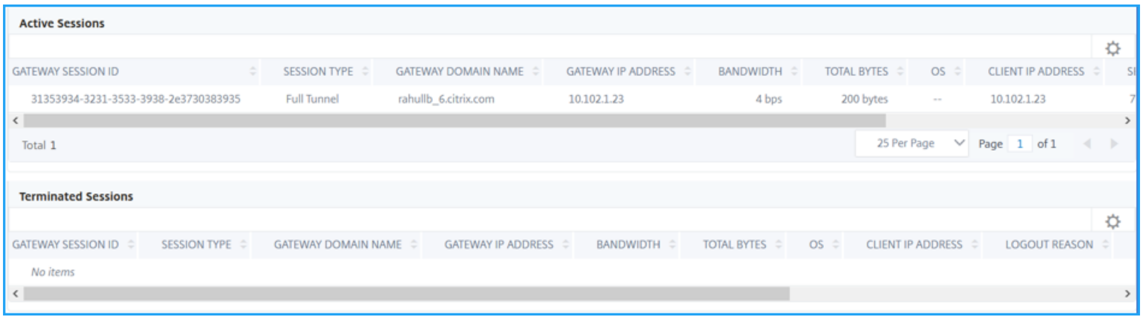
- **View more option for applications and users** – For more than 10 applications and users, you can click the more icon in Applications and Users to view all users and applications details that are associated with the selected gateway.



- **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**.



Active Sessions

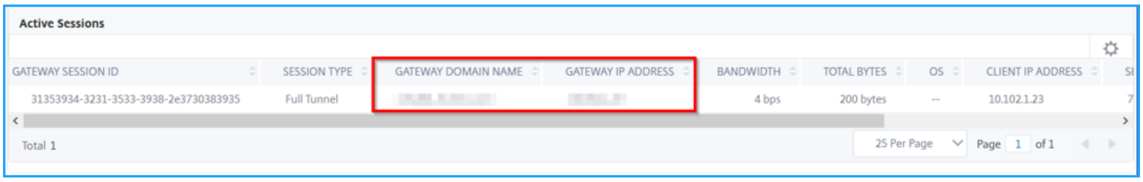
GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	SI
31353934-3231-3533-3938-2e3730383935	Full Tunnel	rahullb_6.citrix.com	10.102.1.23	4 bps	200 bytes	--	10.102.1.23	7

Total 1 25 Per Page Page 1 of 1

Terminated Sessions

GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	LOGOUT REASON
No items								

- The gateway domain name and gateway IP address in **Active Sessions**.

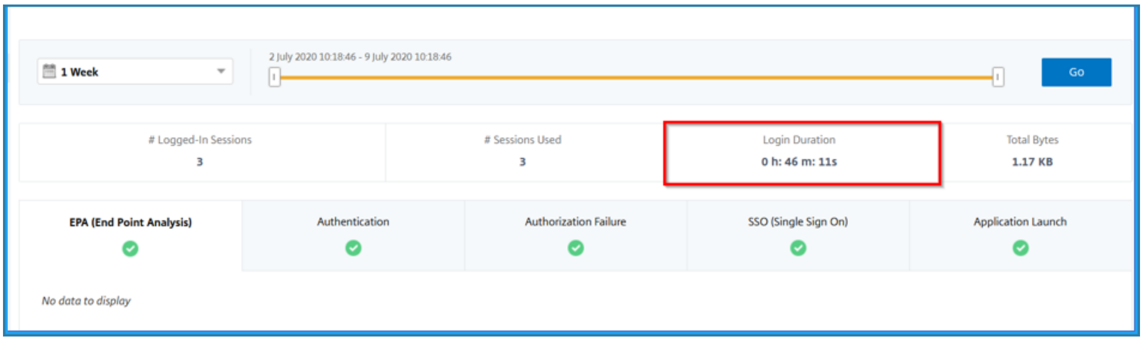


Active Sessions

GATEWAY SESSION ID	SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	SI
31353934-3231-3533-3938-2e3730383935	Full Tunnel	[redacted]	[redacted]	4 bps	200 bytes	--	10.102.1.23	7

Total 1 · 25 Per Page · Page 1 of 1

- The user login duration.

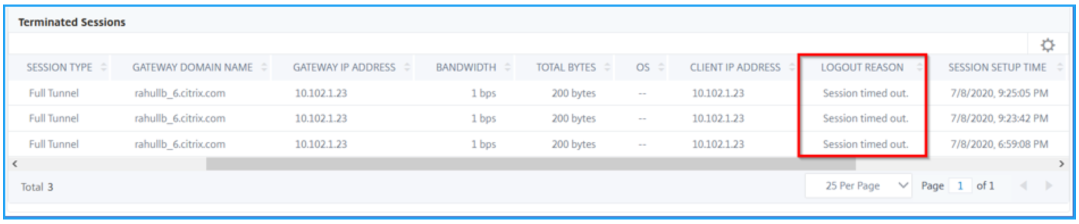


# Logged-In Sessions	# Sessions Used	Login Duration	Total Bytes
3	3	0 h: 46 m: 11s	1.17 KB

EPA (End Point Analysis)	Authentication	Authorization Failure	SSO (Single Sign On)	Application Launch
✓	✓	✓	✓	✓

No data to display

- 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



Terminated Sessions

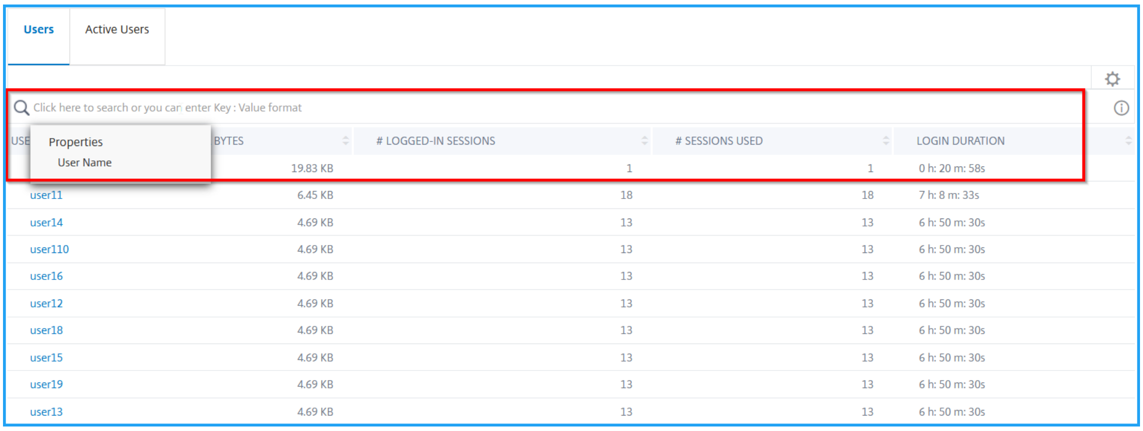
SESSION TYPE	GATEWAY DOMAIN NAME	GATEWAY IP ADDRESS	BANDWIDTH	TOTAL BYTES	OS	CLIENT IP ADDRESS	LOGOUT REASON	SESSION SETUP TIME
Full Tunnel	rahullb_6.citrix.com	10.102.1.23	1 bps	200 bytes	--	10.102.1.23	Session timed out.	7/8/2020, 9:25:05 PM
Full Tunnel	rahullb_6.citrix.com	10.102.1.23	1 bps	200 bytes	--	10.102.1.23	Session timed out.	7/8/2020, 9:23:42 PM
Full Tunnel	rahullb_6.citrix.com	10.102.1.23	1 bps	200 bytes	--	10.102.1.23	Session timed out.	7/8/2020, 6:59:08 PM

Total 3 · 25 Per Page · Page 1 of 1

Search bar and Geo map view

You can view:

- A search bar that enables you to filter results based on the user name. Navigate to **Gateway > Gateway Insight > Users** to view the search bar for **Users** and **Active Users**. Place the mouse pointer on the search bar, select **User Name**, and type a user name to filter results.



USE	BYTES	# LOGGED-IN SESSIONS	# SESSIONS USED	LOGIN DURATION
	19.83 KB	1	1	0 h: 20 m: 58s
user11	6.45 KB	18	18	7 h: 8 m: 33s
user14	4.69 KB	13	13	6 h: 50 m: 30s
user110	4.69 KB	13	13	6 h: 50 m: 30s
user16	4.69 KB	13	13	6 h: 50 m: 30s
user12	4.69 KB	13	13	6 h: 50 m: 30s
user18	4.69 KB	13	13	6 h: 50 m: 30s
user15	4.69 KB	13	13	6 h: 50 m: 30s
user19	4.69 KB	13	13	6 h: 50 m: 30s
user13	4.69 KB	13	13	6 h: 50 m: 30s

- A geo map that displays the users information based on the users geographical location. As an administrator, this geo map enables you to view the summary of total users, total apps, and total sessions for a specific location.

  1. Navigate to **Gateway > Gateway Insight** to view the geo map
  2. Click a country. For example, United States

     The geo map displays the details such as users list, active sessions, terminated sessions, applications for the selected country.

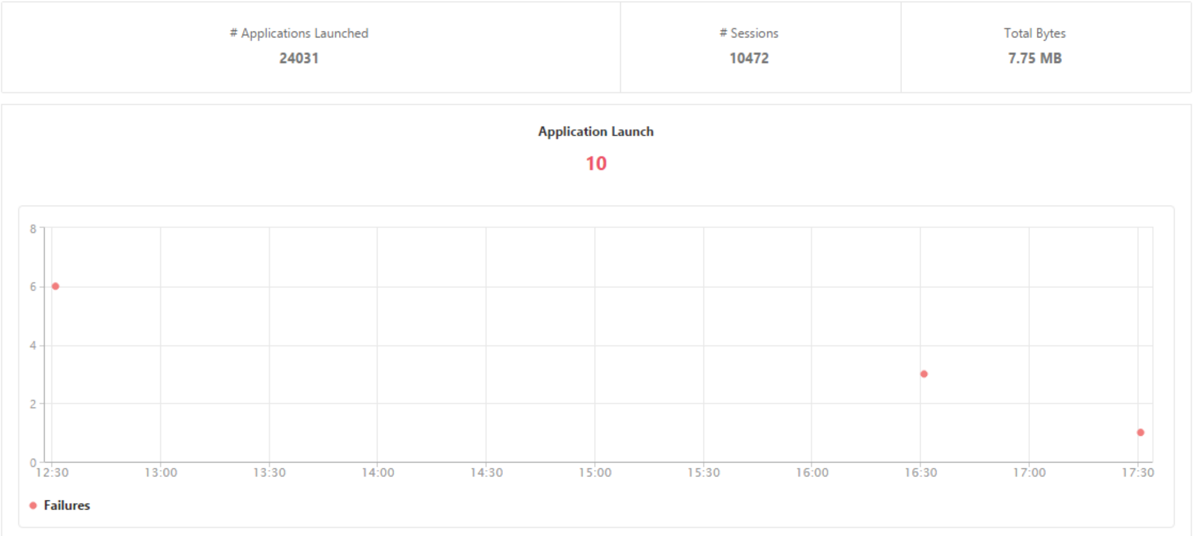
Applications

You can view the number of applications launched, 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.

View application details

1. In Citrix Application Delivery and Management, 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, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.

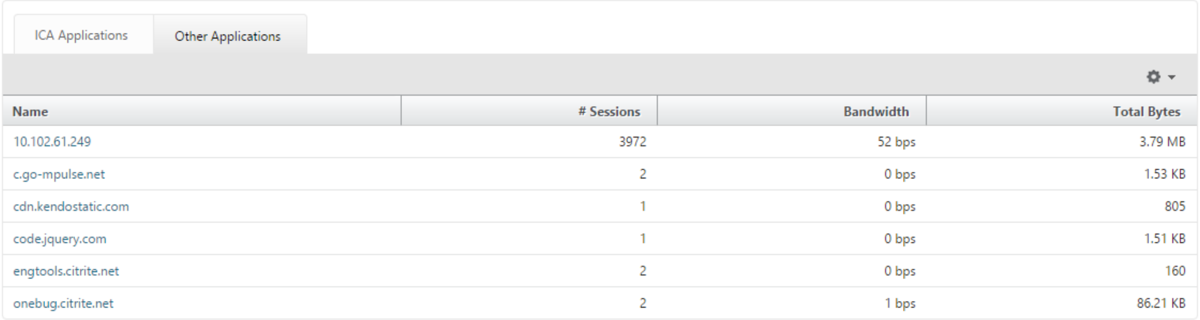


# Applications Launched	# Sessions	Total Bytes
24031	10472	7.75 MB

Application Launch

10

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.

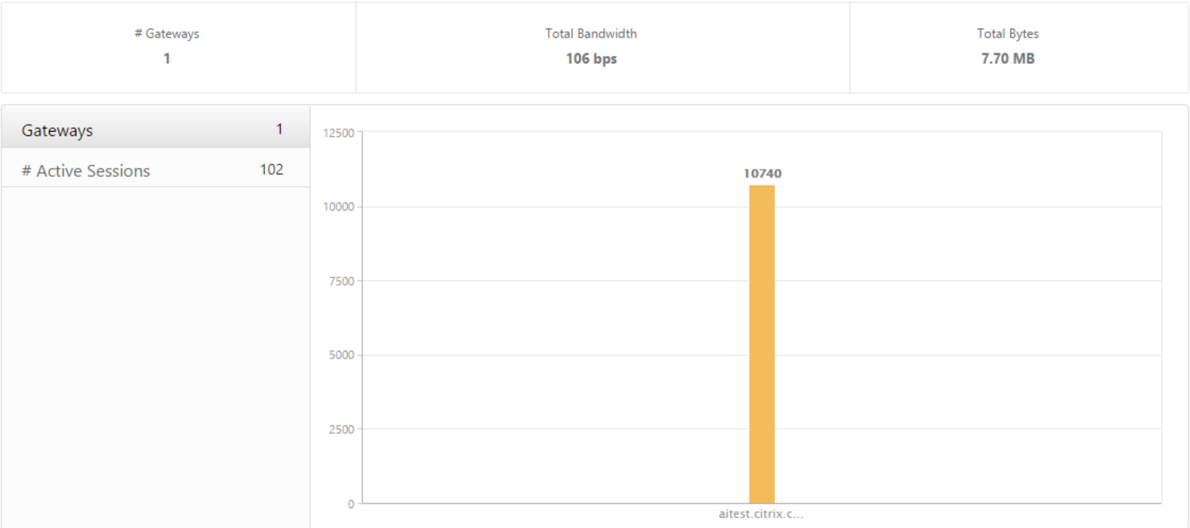
Gateways

You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with an ADC 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.

View gateway details

1. In Citrix Application Delivery and Management, 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**.

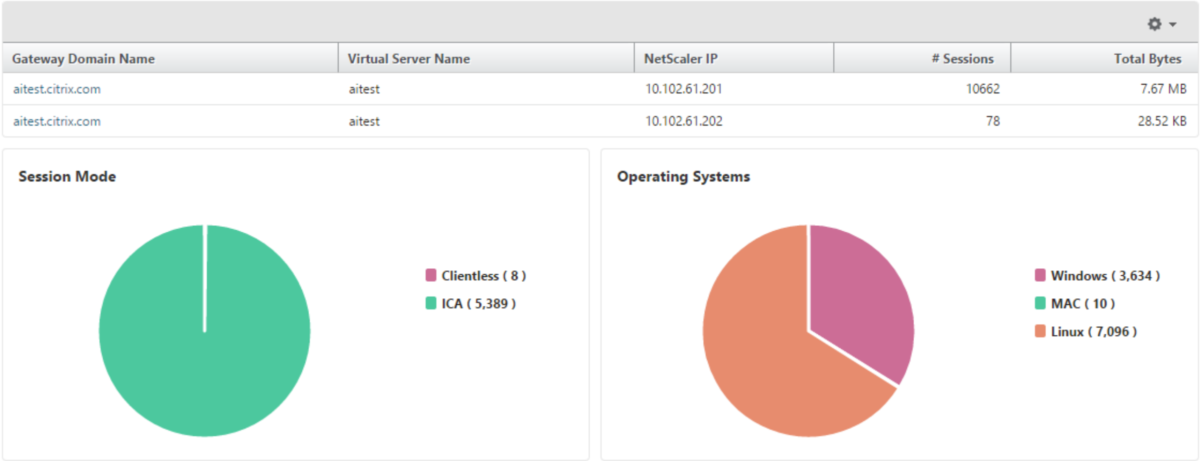
You can now view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with an ADC Gateway appliance at any given time.



# Gateways	Total Bandwidth	Total Bytes
1	106 bps	7.70 MB

Gateways	1
# Active Sessions	102

Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, ADC IP address, session modes, and Total Bytes.



Gateway Domain Name	Virtual Server Name	NetScaler IP	# Sessions	Total Bytes
aitest.citrix.com	aitest	10.102.61.201	10662	7.67 MB
aitest.citrix.com	aitest	10.102.61.202	78	28.52 KB

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.

You can also view a geo map for gateways that enables you to filter users based on a particular location.

1. Navigate to **Gateway > Gateway Insight > Gateways**
2. Select a gateway domain name to view the geo map
3. Click a country. For example, United States

   The geo map displays the details such as users list, active sessions, terminated sessions, applications for the selected country.

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 Citrix Application Delivery and Management has internet connectivity.

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 edit the export schedule:

1. On the Configuration tab, navigate to **Configuration** > **NetScaler Insight Center** > **Export Schedules**.
2. Select a report from the available list, and then click **Edit**.
3. After editing, click **Save**.

> **Note**
>
> Configure the email server settings before scheduling the report by navigating to **System** > **Notifications** > **Email** and by clicking **Add**.

To add an email server or an email distribution list:

1. On the **Configuration** tab, navigate to **System** > **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 ADC Gateway appliances.

1. User is not able to log on to the ADC Gateway appliance or to the internal web servers

You are an ADC Gateway administrator monitoring ADC Gateway appliances through Citrix Application Delivery and Management, 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.

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, you can search for a particular user and then view all the details for that user.

To search for a user:

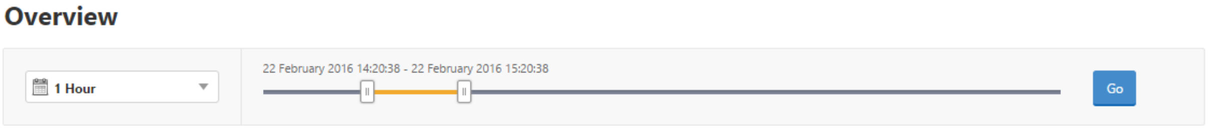
In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

Authentication Failures

You can view authentication errors such as incorrect credentials or no response from the authentication server. If you have set up two-stage authentication, you can see whether the primary, secondary, or both stages of the authentication have failed.

View the authentication failure details

1. In Citrix Application Delivery and Management, 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**.

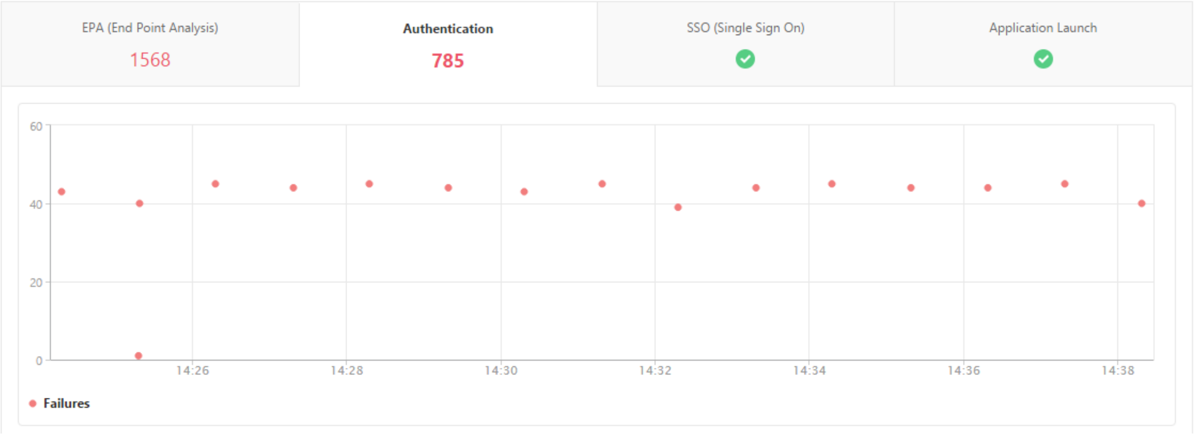


Overview

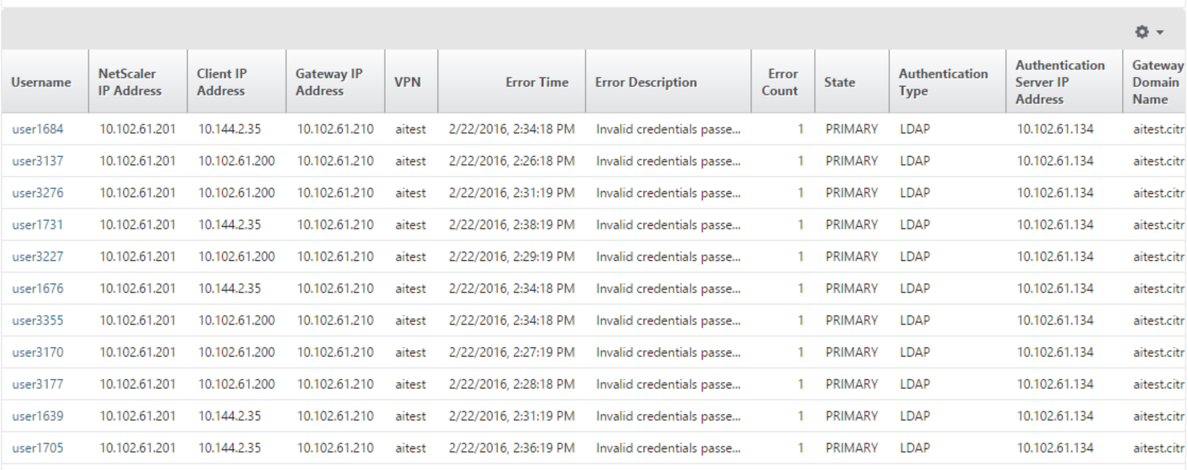
1 Hour

22 February 2016 14:20:38 - 22 February 2016 15:20:38

1. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.



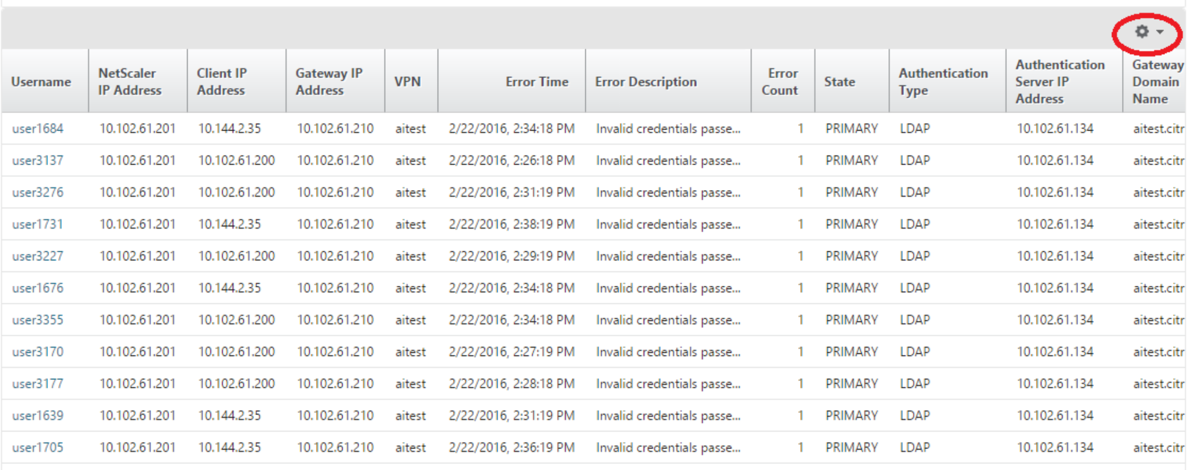
Scroll down to view details of each authentication error such as **Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address**, and more from the table on the same tab. The **Error Description** column in the table displays the reason for the logon failure, and the **State** column displays at what stage of a two-stage authentication the failure occurred.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

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 list arrow as indicated in the following image.



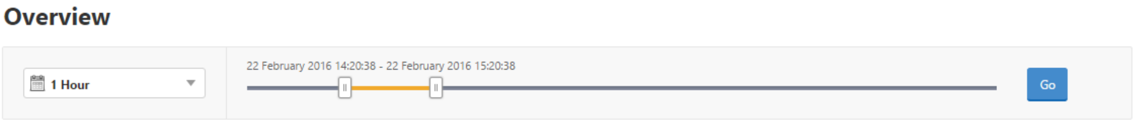
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

EPA Failures

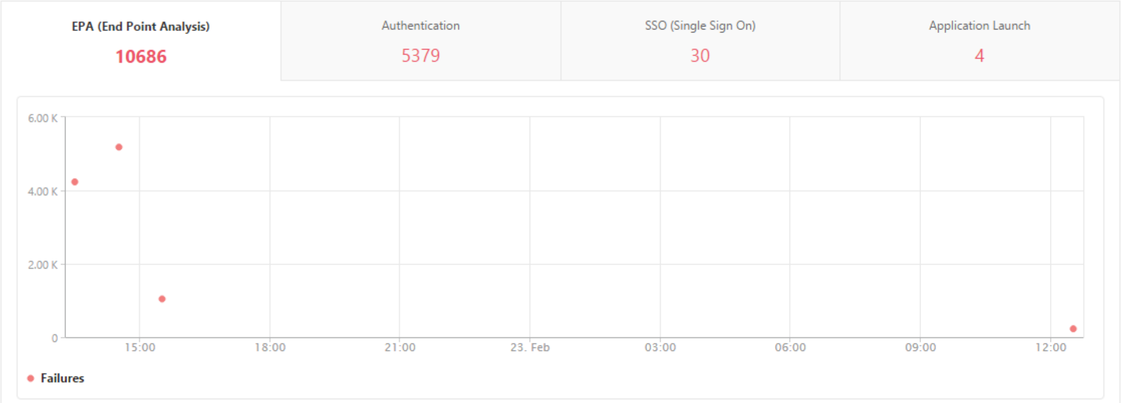
You can view EPA failures at pre- or post-authentication stage.

View EPA failure details

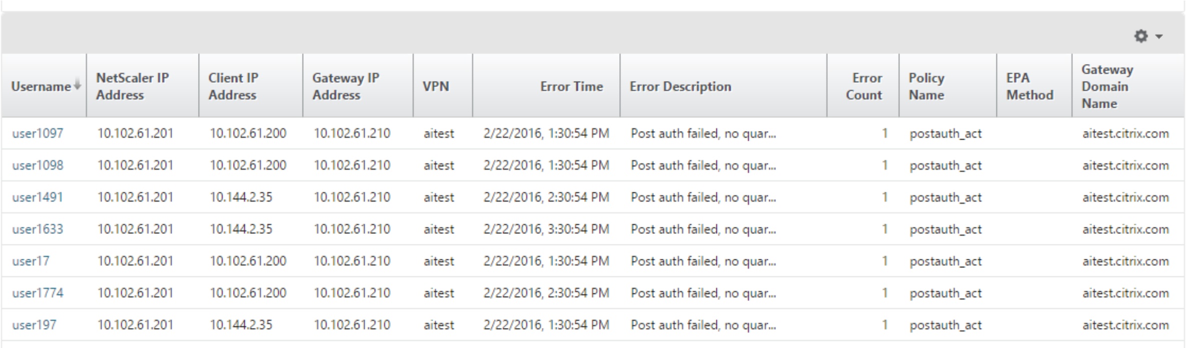
1. In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click **Go**.

3. Click the **EPA (End Point Analysis)** tab. You can view the number of EPA errors at any given time in the **Failures** graph.

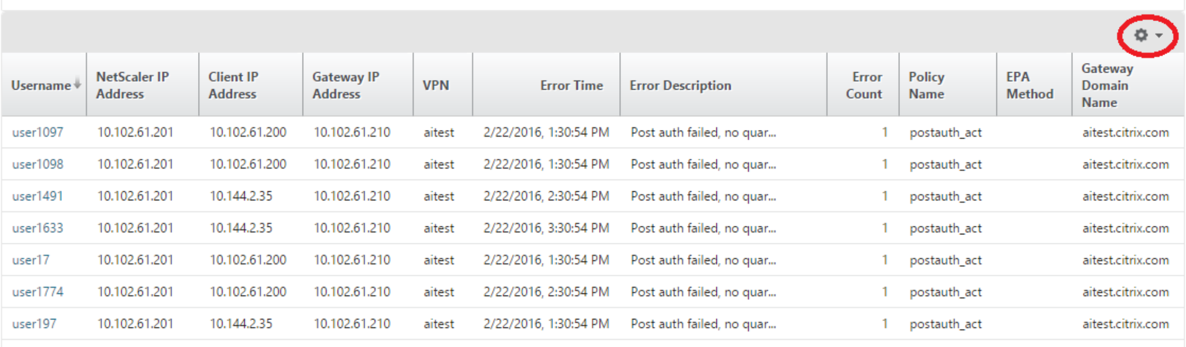
Scroll down to view details of each EPA error such as **Username, ADC IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name** and more from the table on the same tab. The **Error Description** column in the table displays the reason for the EPA failure, and the **Policy Name** 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 list arrow as indicated in the following image.



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

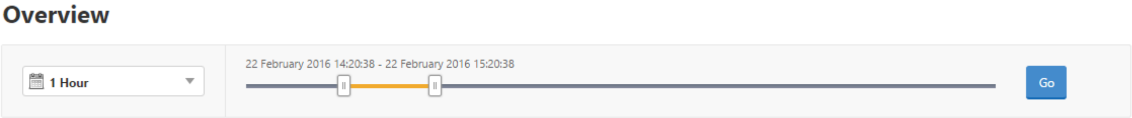
> **Note**
>
> ADC Gateway doesn't report the EPA failures when the "clientSecurity" expression is configured as a VPN session policy rule.

SSO Failures

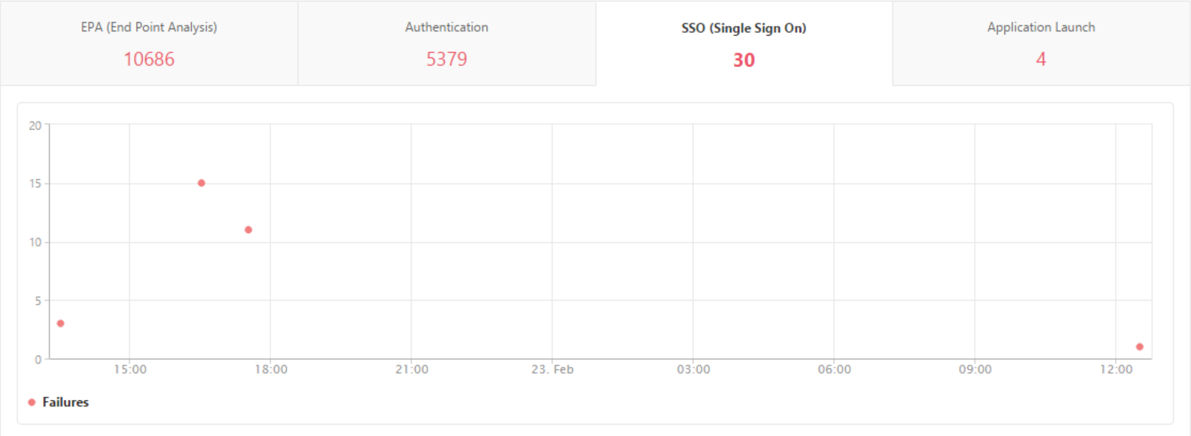
You can view the all the SSO failures at any stage for a user accessing any applications through the ADC Gateway appliance.

View SSO failure details

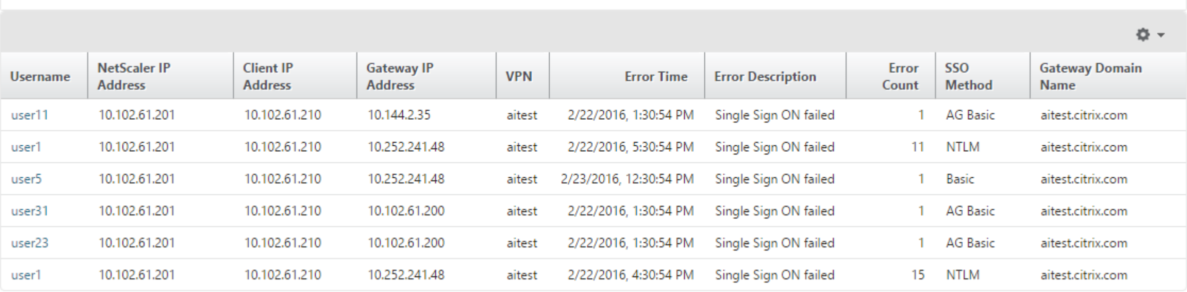
1. In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.



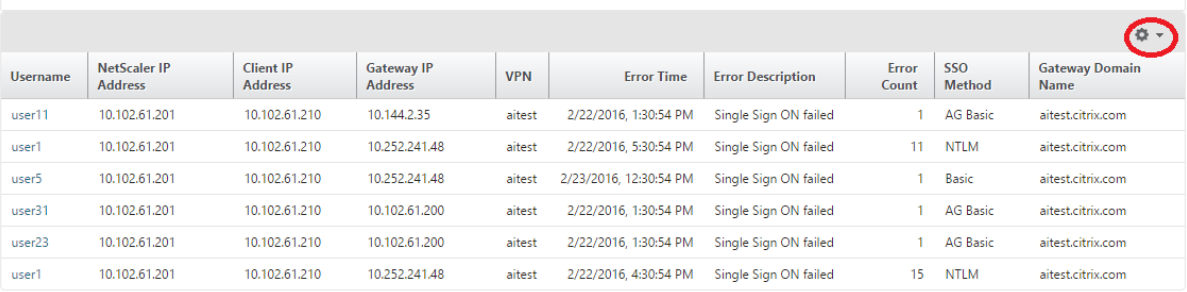
Scroll down to view details of each SSO error such as **Username, ADC IP Address, Error Time, Error Description, Resource Name** and more from the table on the same tab.



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 list arrow as indicated in the following image.



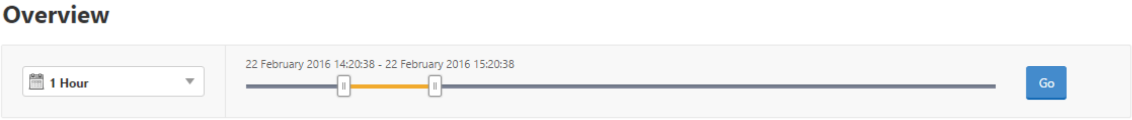
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	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

2. After successfully logging on to ADC Gateway, a user is not able to launch any virtual application

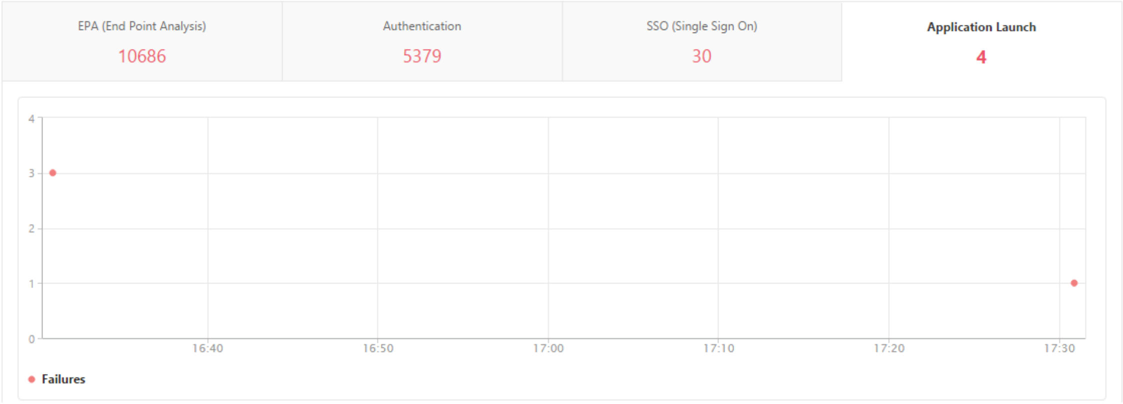
For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or Citrix Virtual App server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

View application launch failure details

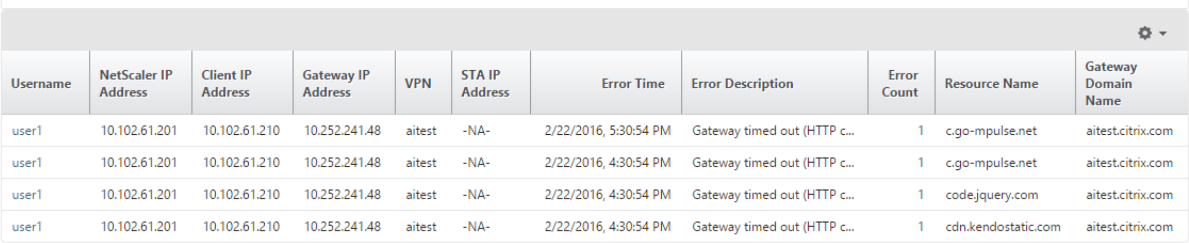
1. In Citrix Application Delivery and Management, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **Application Launch** tab. You can view the number of application launch failures at any given time in the **Failures** graph.



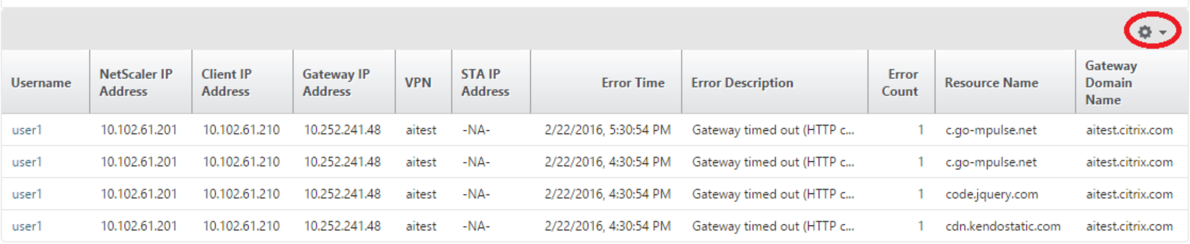
Scroll down to view details of each application launch error, such as **ADC IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, and more, from the table on the same tab. The **Error Description** column in the table displays the IP address of the STA server and the **Resource Name** column displays the details of the resource for which the STA validation has failed.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

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 list arrow as indicated in the following image.



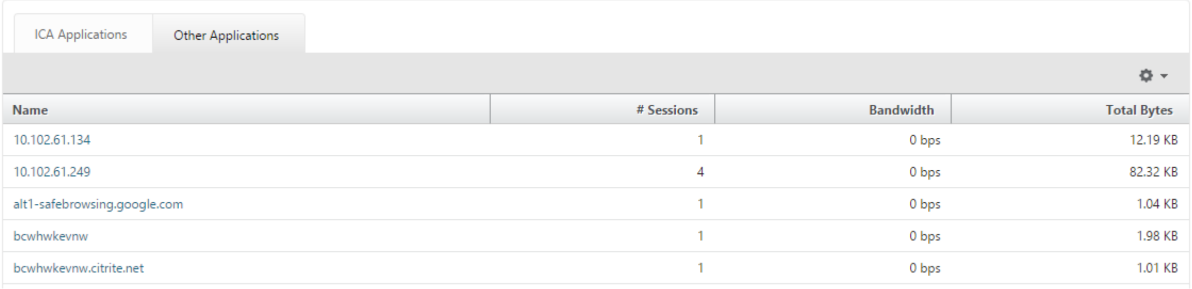
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

3. 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 Citrix Application Delivery and Management, you can view the total bytes and bandwidth consumed by that application.

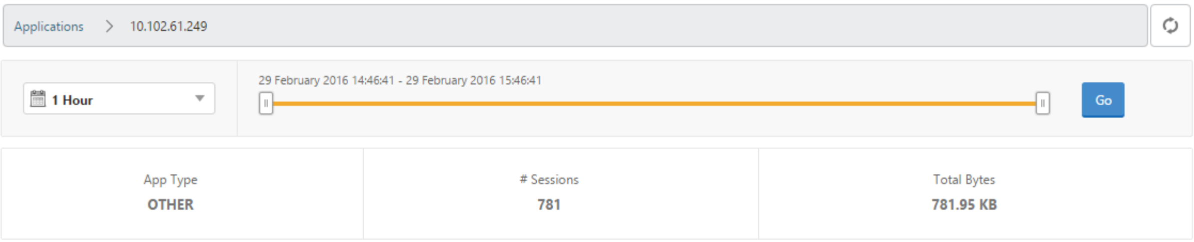
View total bytes and bandwidth consumed by an application

In Citrix Application Delivery and Management, 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.

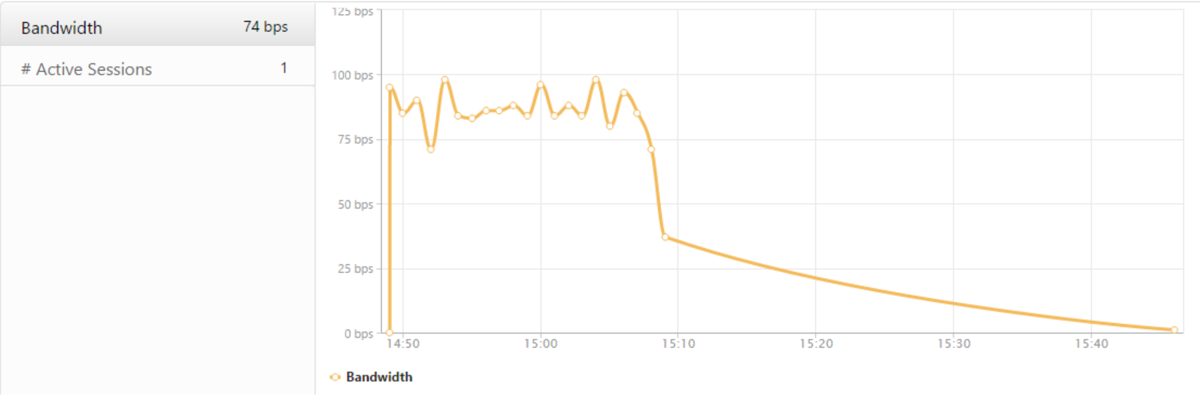


1 Hour

29 February 2016 14:46:41 - 29 February 2016 15:46:41

App Type	# Sessions	Total Bytes
OTHER	781	781.95 KB

You can also view the bandwidth consumed by that application.



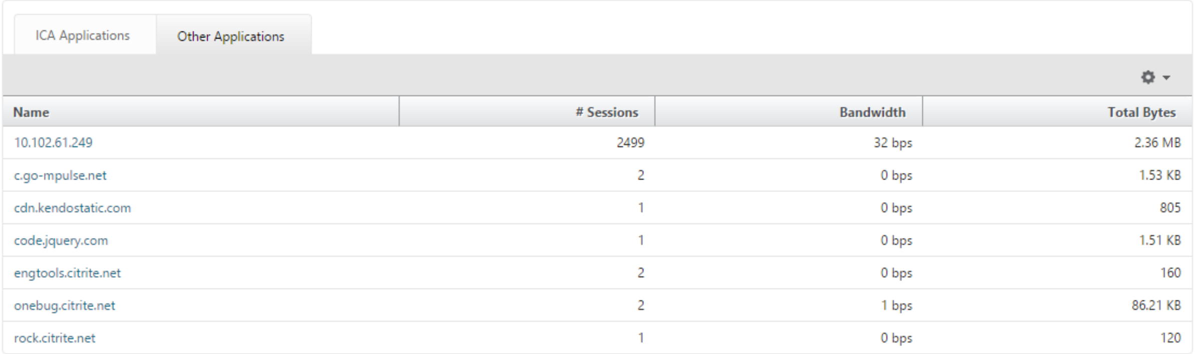
Bandwidth	74 bps
# Active Sessions	1

4. A user has logged on to ADC 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.

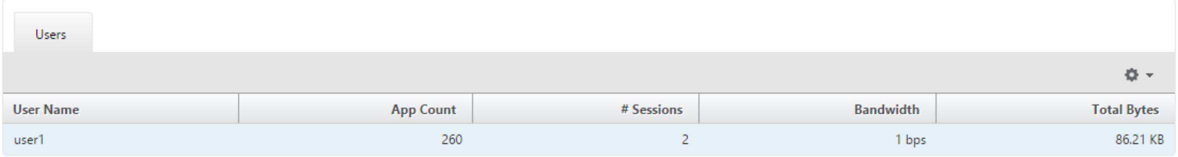
View user access for resources

1. In Citrix Application Delivery and Management, 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 to.



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

On the screen that appears, scroll down, and in the **Users** table, all the users that have access to that application are displayed.



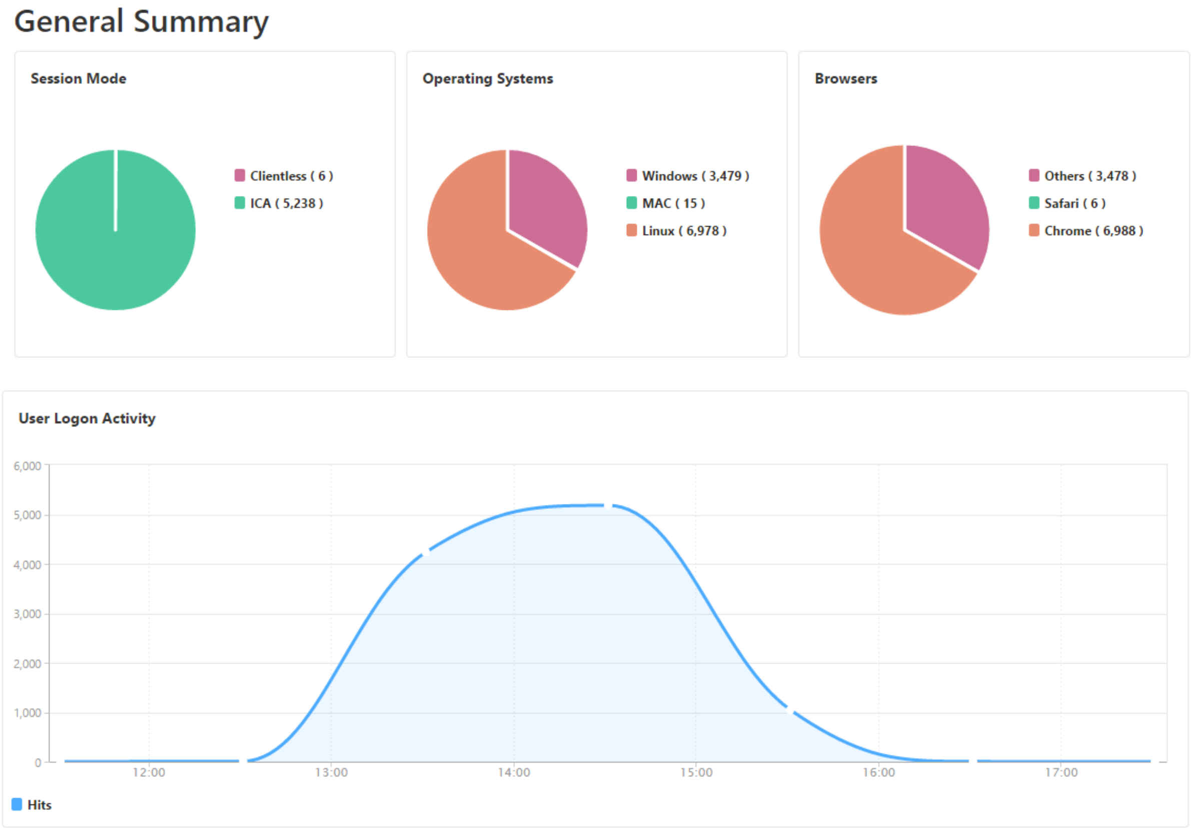
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. Different users might be using different ADC Gateway deployments or might log on to ADC 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 ADC Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

View summary of session modes, type of clients, and number of users logged on

1. In Citrix Application Delivery and Management, 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.



HDX Insight

September 25, 2021

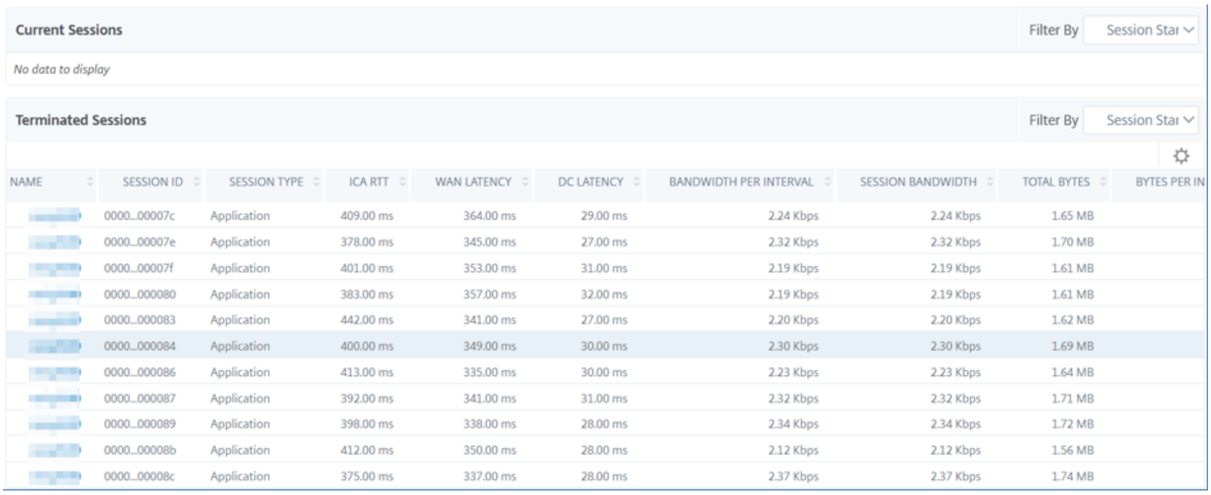
HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktops passing through Citrix ADC. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables Citrix Application Delivery and Management to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your ADC 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.

You can also visualize a consolidated view of all users active and terminated sessions.



Current Sessions

No data to display

Terminated Sessions

NAME	SESSION ID	SESSION TYPE	ICA RTT	WAN LATENCY	DC LATENCY	BANDWIDTH PER INTERVAL	SESSION BANDWIDTH	TOTAL BYTES	BYTES PER IN
[redacted]	0000...00007c	Application	409.00 ms	364.00 ms	29.00 ms	2.24 Kbps	2.24 Kbps	1.65 MB	
[redacted]	0000...00007e	Application	378.00 ms	345.00 ms	27.00 ms	2.32 Kbps	2.32 Kbps	1.70 MB	
[redacted]	0000...00007f	Application	401.00 ms	353.00 ms	31.00 ms	2.19 Kbps	2.19 Kbps	1.61 MB	
[redacted]	0000...000080	Application	383.00 ms	357.00 ms	32.00 ms	2.19 Kbps	2.19 Kbps	1.61 MB	
[redacted]	0000...000083	Application	442.00 ms	341.00 ms	27.00 ms	2.20 Kbps	2.20 Kbps	1.62 MB	
[redacted]	0000...000084	Application	400.00 ms	349.00 ms	30.00 ms	2.30 Kbps	2.30 Kbps	1.69 MB	
[redacted]	0000...000086	Application	413.00 ms	335.00 ms	30.00 ms	2.23 Kbps	2.23 Kbps	1.64 MB	
[redacted]	0000...000087	Application	392.00 ms	341.00 ms	31.00 ms	2.32 Kbps	2.32 Kbps	1.71 MB	
[redacted]	0000...000089	Application	398.00 ms	338.00 ms	28.00 ms	2.34 Kbps	2.34 Kbps	1.72 MB	
[redacted]	0000...00008b	Application	412.00 ms	350.00 ms	28.00 ms	2.12 Kbps	2.12 Kbps	1.56 MB	
[redacted]	0000...00008c	Application	375.00 ms	337.00 ms	28.00 ms	2.37 Kbps	2.37 Kbps	1.74 MB	

As an administrator, this view enables you to:

- View all users details in a single-pane visualization
- Eliminate the complexity in selecting each user and seeing the active and terminated sessions

> **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. Citrix Application Delivery and Management 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 Configuring Groups on Citrix Application Delivery and Management.

You can also navigate to **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 **HDX Insight > Users**.

> **Note**
>
> HDX insight supports Admin Partitions configured in ADC 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.

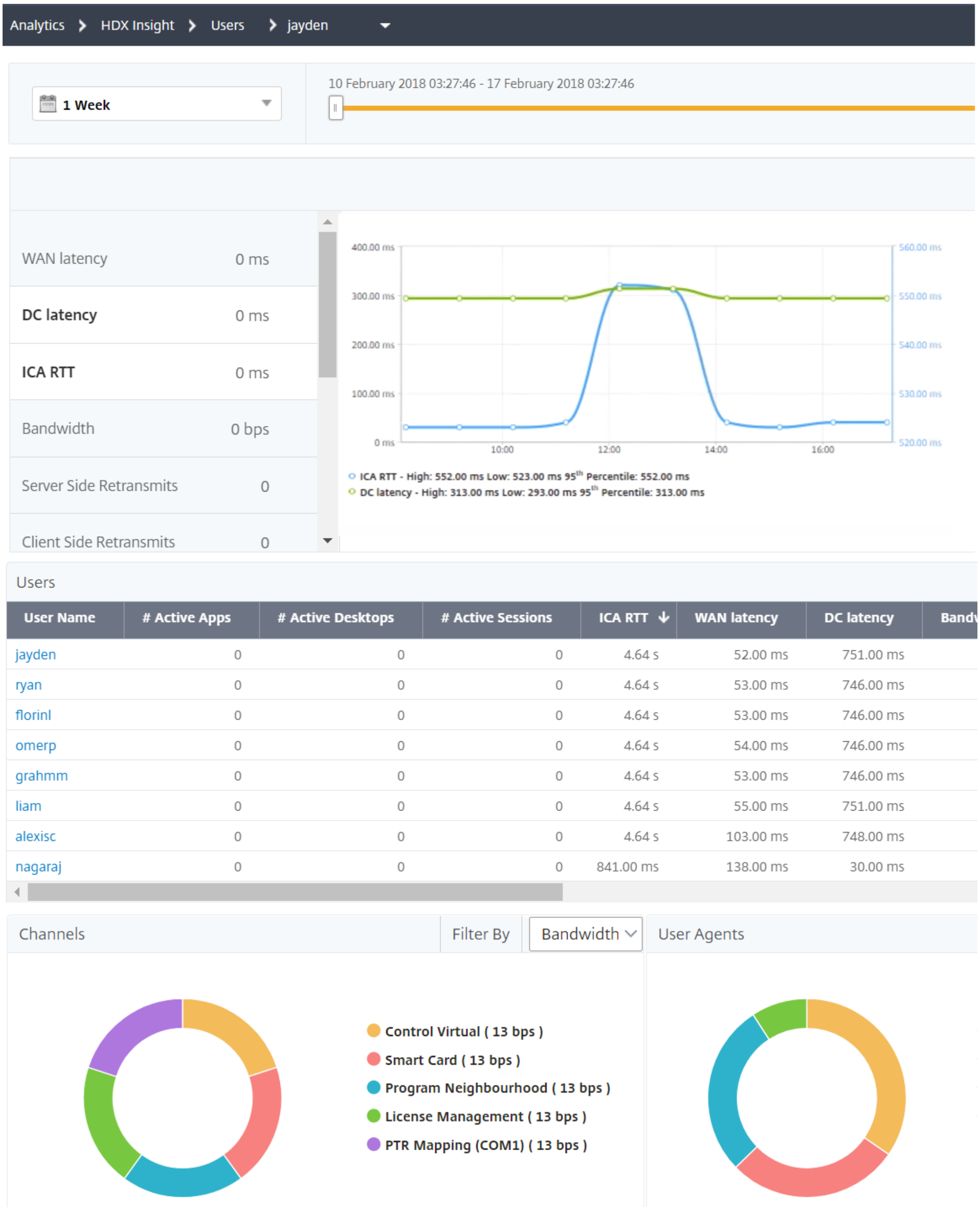
To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

1. On the **Analytics** tab, navigate to **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.



Analytics > HDX Insight > Users > jayden

1 Week

10 February 2018 03:27:46 - 17 February 2018 03:27:46

WAN latency	0 ms
DC latency	0 ms
ICA RTT	0 ms
Bandwidth	0 bps
Server Side Retransmits	0
Client Side Retransmits	0

ICA RTT - High: 552.00 ms Low: 523.00 ms 95th Percentile: 552.00 ms

DC latency - High: 313.00 ms Low: 293.00 ms 95th Percentile: 313.00 ms

Users

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT ↓	WAN latency	DC latency	Bandw
jayden	0	0	0	4.64 s	52.00 ms	751.00 ms	
ryan	0	0	0	4.64 s	53.00 ms	746.00 ms	
florinl	0	0	0	4.64 s	53.00 ms	746.00 ms	
omerp	0	0	0	4.64 s	54.00 ms	746.00 ms	
grahmm	0	0	0	4.64 s	53.00 ms	746.00 ms	
liam	0	0	0	4.64 s	55.00 ms	751.00 ms	
alexisc	0	0	0	4.64 s	103.00 ms	748.00 ms	
nagaraj	0	0	0	841.00 ms	138.00 ms	30.00 ms	

Channels

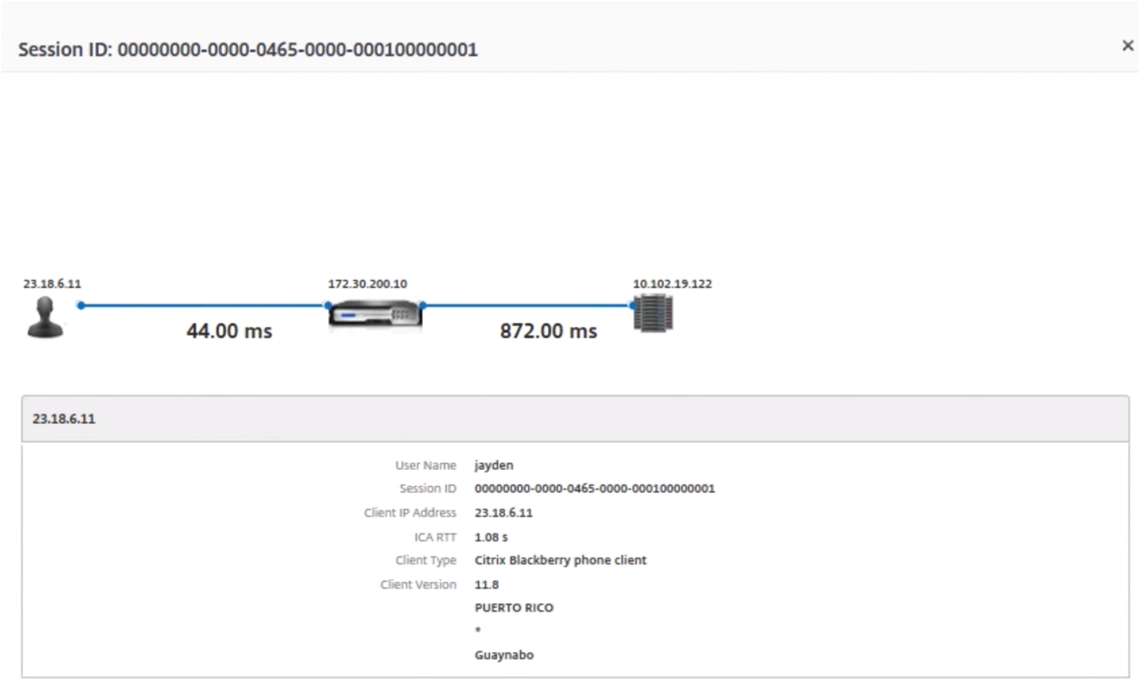
Filter By: Bandwidth

User Agents

- Control Virtual (13 bps)
- Smart Card (13 bps)
- Program Neighbourhood (13 bps)
- License Management (13 bps)
- PTR Mapping (COM1) (13 bps)

4. On the **Current Application Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.

5. On the **Current Application Sessions** table, click the hop diagram symbol to display information about the connection between the client and the server, including latency values.



Session ID: 00000000-0000-0465-0000-000100000001

23.18.6.11

User Name	jayden
Session ID	00000000-0000-0465-0000-000100000001
Client IP Address	23.18.6.11
ICA RTT	1.08 s
Client Type	Citrix Blackberry phone client
Client Version	11.8
	PUERTO RICO
	*
	Guaynabo

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 Apps or Desktops

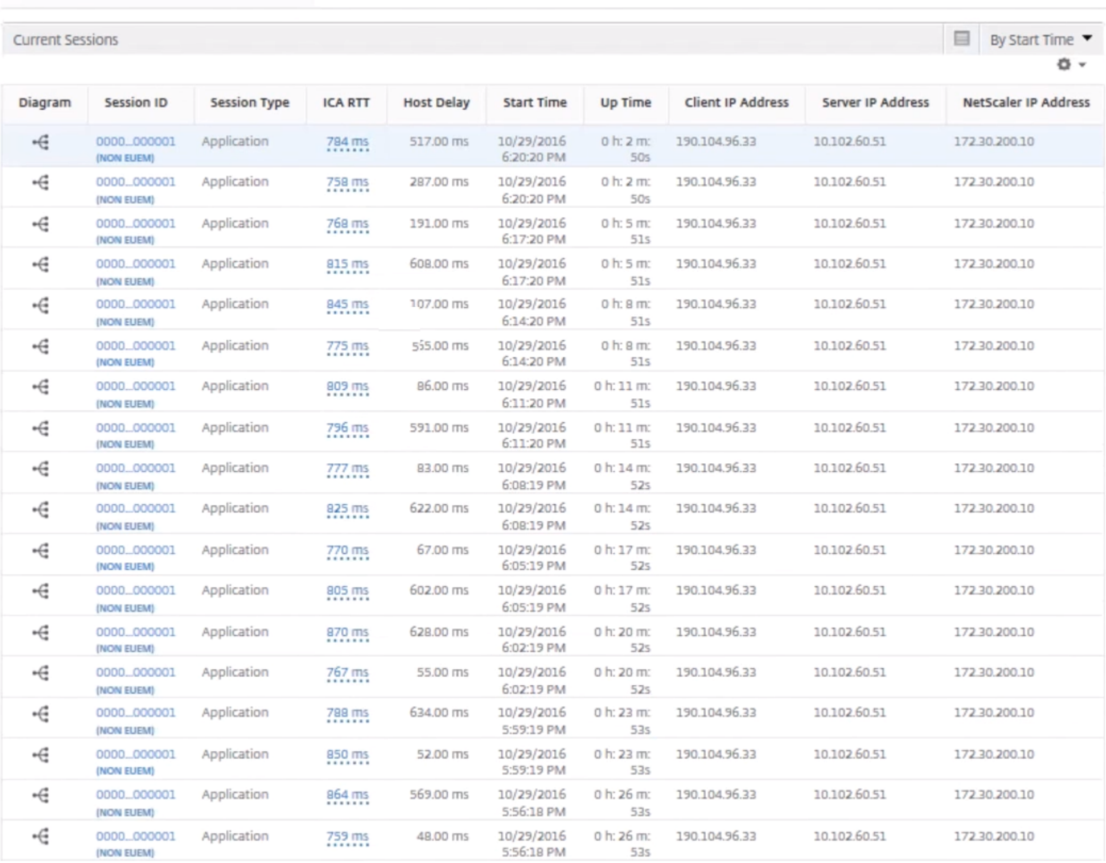
The delay might be due to latency on the server network, ICA-traffic delays caused by the server network, latency on the client network, or time taken to launch an application.

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 Application Sessions** table, note that the host delay is high.



Current Sessions

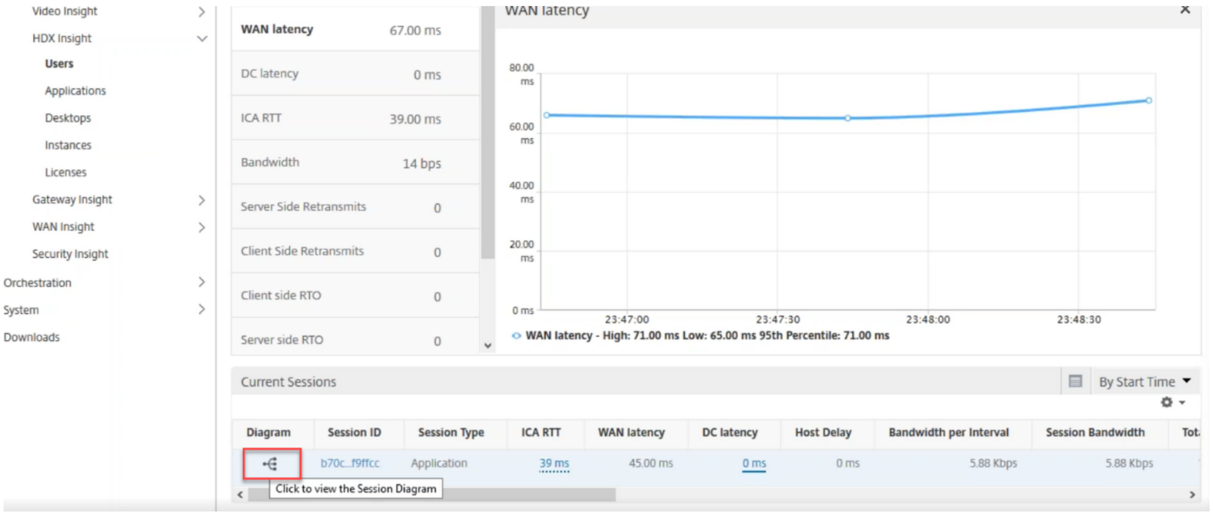
By Start Time ▾

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 Citrix Application Delivery and Management 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.



WAN latency	67.00 ms
DC latency	0 ms
ICA RTT	39.00 ms
Bandwidth	14 bps
Server Side Retransmits	0
Client Side Retransmits	0
Client side RTO	0
Server side RTO	0

Current Sessions

Diagram	Session ID	Session Type	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Tot
	b70c...f9ffcc	Application	39 ms	45.00 ms	0 ms	0 ms	5.88 Kbps	5.88 Kbps	

Geo map for HDX Insight

Geo map feature in Citrix Application Delivery and Management displays the usage of web applications across different geographical locations on a map. As an administrator, you can use this information to understand the trends in application usage and for capacity planning.

Geo map provides information about the following metrics specific to a country, state, and city:

- Total Hits: Total number of times an application is accessed.
- Bandwidth: Total bandwidth consumed while serving client requests
- Response Time: Average time taken to send responses to client requests.

Geo map provides information which can be used to address several use cases such as the following:

- Region that has the maximum number of clients accessing an application
- Region that has the highest response time
- Region that consumes the most bandwidth

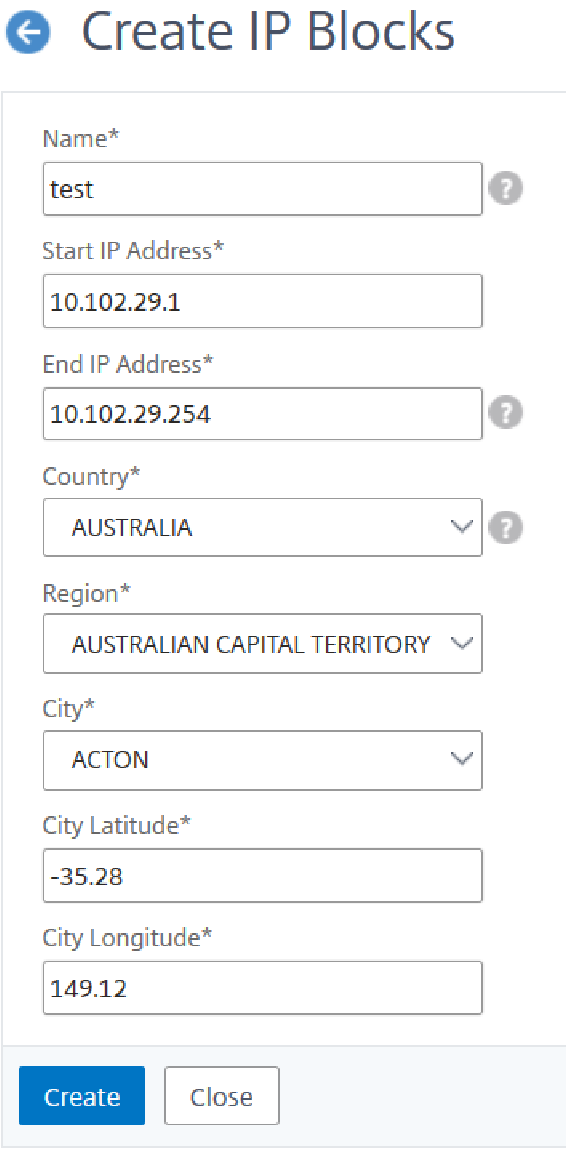
Citrix Application Delivery and Management **automatically enables** geomaps for private IP addresses or public IP addresses, when you enable **Web insight**.

Create a private IP block

Citrix Application Delivery and Management can recognize the location of a client when the client private IP address is added to the Citrix Application Delivery and Management server. For example, if the IP address of a client falls within the range of a private IP address block associated with City A, Citrix Application Delivery and Management recognizes that the traffic is originating from City A for this client.

To create an IP block:

1. In Citrix Application Delivery and Management, navigate to **Settings > Analytics Settings > IP Blocks**, and then click **Add**.
2. In **Create IP Blocks** page, specify the following parameters:
   - **Name**. Specify a name for the private IP block
   - **Start IP address**. Specify the lowest IP address range for the IP block.
   - **End IP address**. Specify the highest IP address range for the IP block.
   - **Country**. Select the country from the list.
   - **Region**. Based on the country, the region is auto-populated, but you can select your region.
   - **City**. Based on the region, the city is auto-populated, but you can select your city.
   - **City Latitude** and **City Longitude**. Based on the city you select, the latitude and longitude are auto-populated.
3. Click **Create** to finish.



Create IP Blocks

Name*: test

Start IP Address*: 10.102.29.1

End IP Address*: 10.102.29.254

Country*: AUSTRALIA

Region*: AUSTRALIAN CAPITAL TERRITORY

City*: ACTON

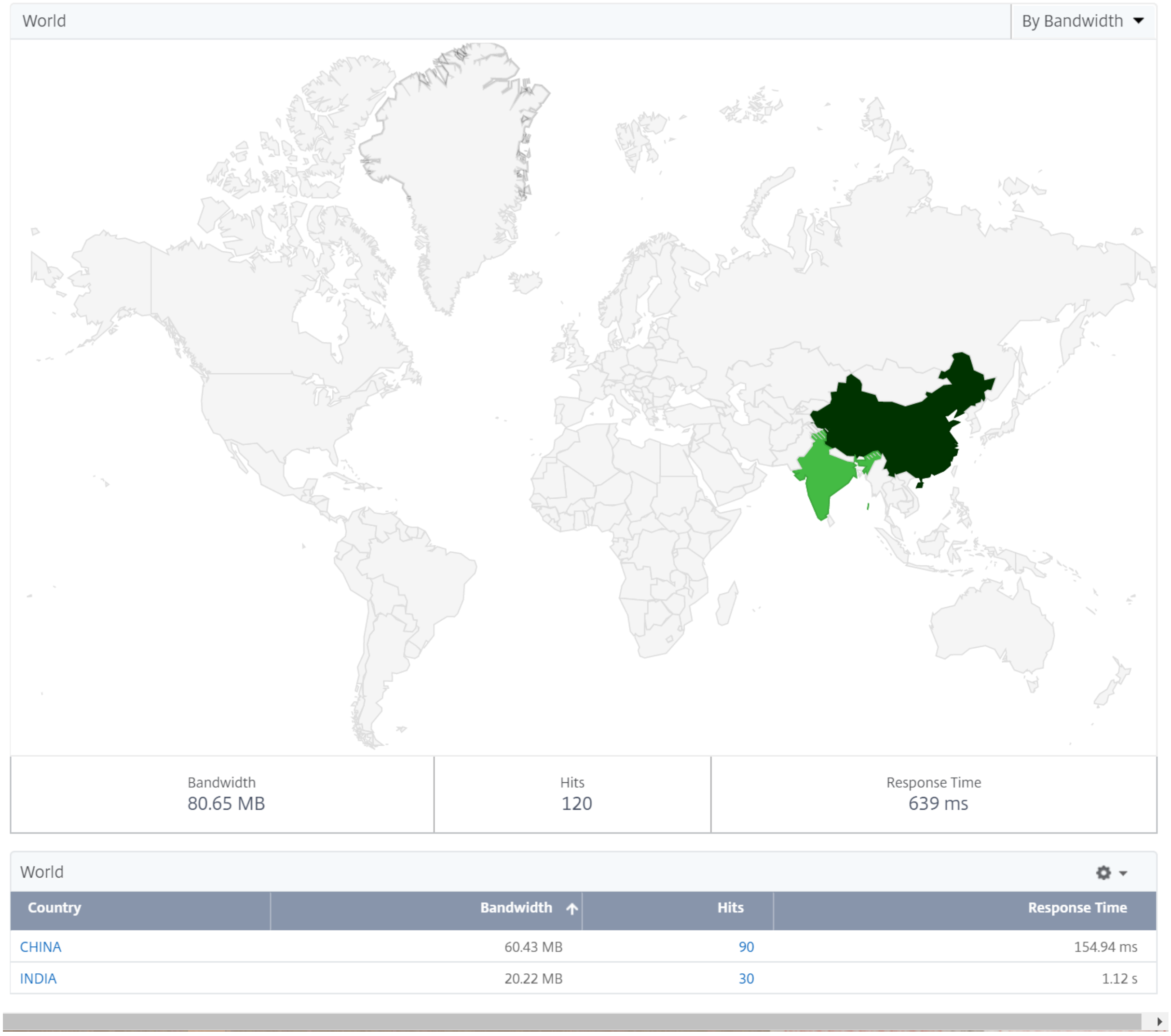
City Latitude*: -35.28

City Longitude*: 149.12

Public IP blocks

Citrix Application Delivery and Management can also recognize the client location if the client uses public IP address. Citrix Application Delivery and Management has its built-in location CSV file that matches the location based on the client IP address range. For using public IP block, the only requirement is that you have to enable the **Enable geo data** collection from the Configure Insight page.

> Note
>
> Citrix Application Delivery and Management requires an internet connection to display the geomaps for a particular geographical location. Internet connection is also required to export the GeoMap in .pdf, .png, or .jpg formats.



Bandwidth 80.65 MB | Hits 120 | Response Time 639 ms

World

Country	Bandwidth	Hits	Response Time
CHINA	60.43 MB	90	154.94 ms
INDIA	20.22 MB	30	1.12 s

To export the report of this dashboard:

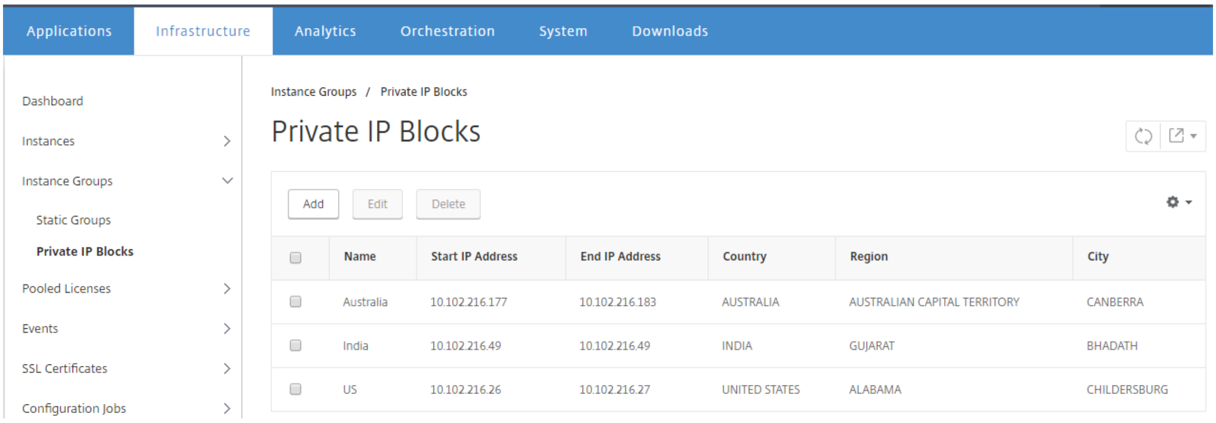
To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over email or slack message.

> **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.

To configure a geomap for data centers:

On the **Infrastructure** tab, navigate to **Sites** > **Private IP Blocks** to configure geomaps for a particular location.



□	Name	Start IP Address	End IP Address	Country	Region	City
□	Australia	10.102.216.177	10.102.216.183	AUSTRALIA	AUSTRALIAN CAPITAL TERRITORY	CANBERRA
□	India	10.102.216.49	10.102.216.49	INDIA	GUJARAT	BHADATH
□	US	10.102.216.26	10.102.216.27	UNITED STATES	ALABAMA	CHILDERSBURG

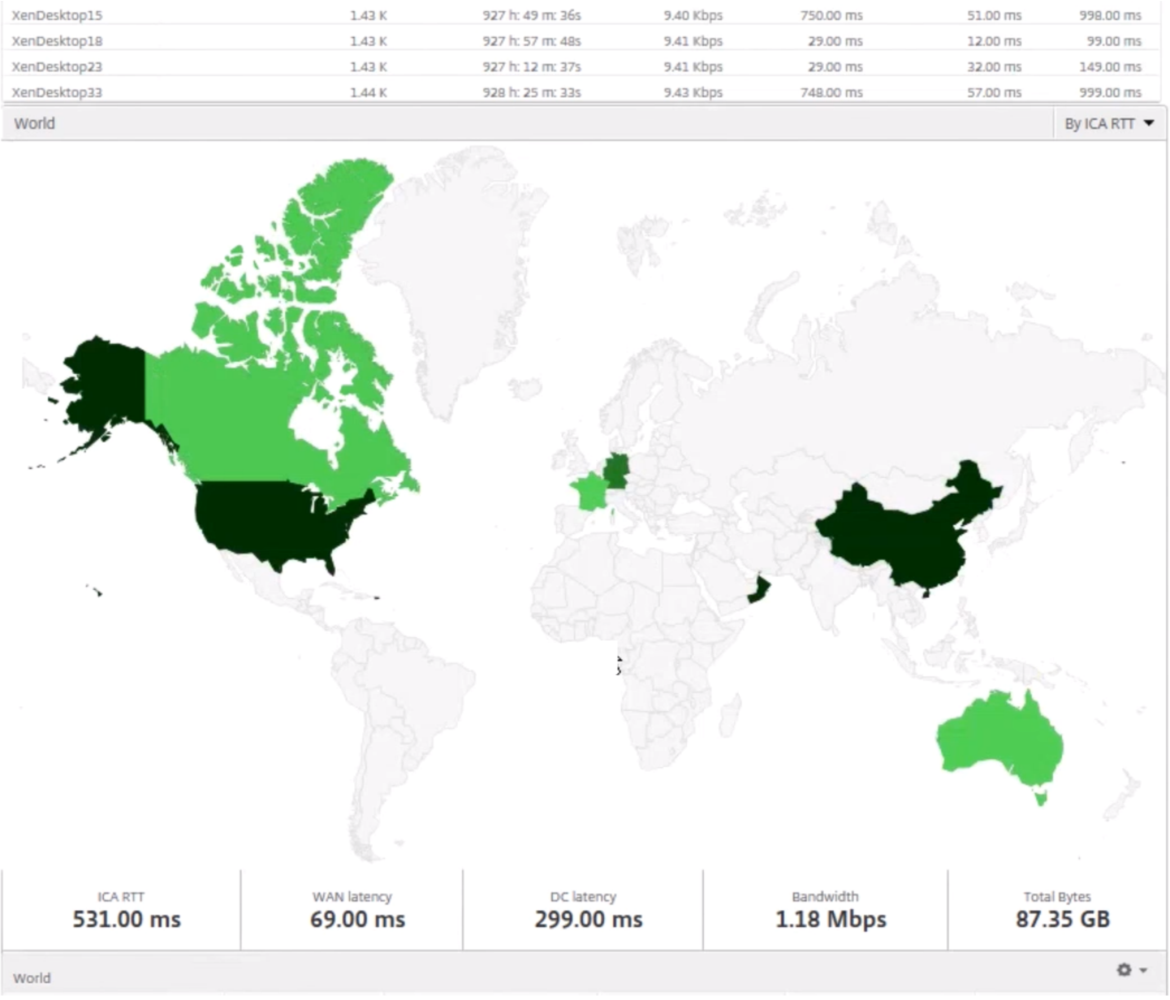
Use Case

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 ADC Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the ADC 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 ADC Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

An ADC 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 ADC Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another ADC Gateway, so that users have two local ADC Gateway appliances through which to access the VPN.



XenDesktop15	1.43 K	927 h: 49 m: 36s	9.40 Kbps	750.00 ms	51.00 ms	998.00 ms
XenDesktop18	1.43 K	927 h: 57 m: 48s	9.41 Kbps	29.00 ms	12.00 ms	99.00 ms
XenDesktop23	1.43 K	927 h: 12 m: 37s	9.41 Kbps	29.00 ms	32.00 ms	149.00 ms
XenDesktop33	1.44 K	928 h: 25 m: 33s	9.43 Kbps	748.00 ms	57.00 ms	999.00 ms

ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
531.00 ms	69.00 ms	299.00 ms	1.18 Mbps	87.35 GB

Limitations

If ADC instances have Advanced license, thresholds set on Citrix Application Delivery and Management for HDX Insight will not be triggered since analytical data is collected for only 1 hour.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over email or slack message.

> **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.

Enable HDX Insight data collection

September 28, 2021

HDX Insight enables the administrator to deliver an exceptional user experience by providing end-to-end visibility into the ICA traffic that passes through the Citrix ADC appliance.

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 ADC instances differs with the position of the appliance in the deployment topology. This topic includes the following details:

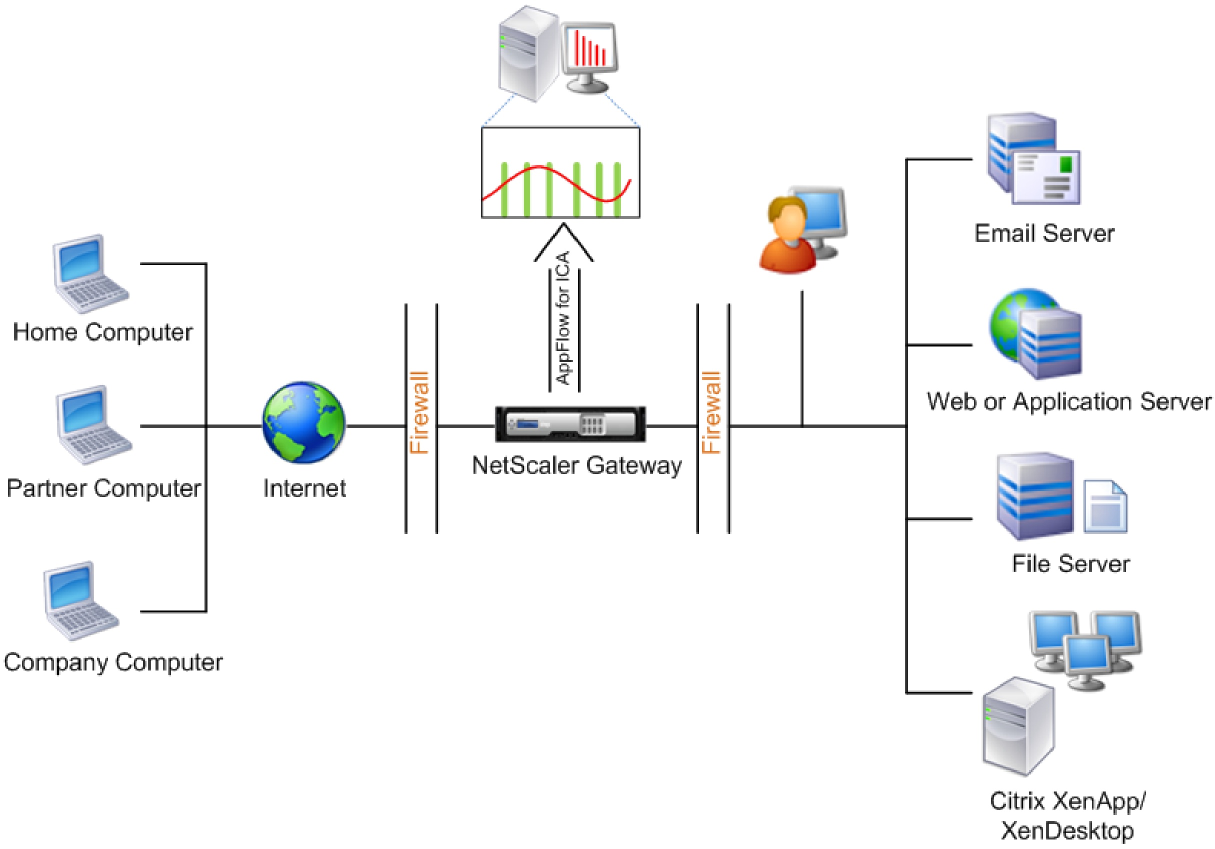
- Enabling data collection for monitoring Citrix ADCs deployed in transparent mode
- Enabling data collection for Citrix ADC Gateway appliances deployed in single-hop mode
- Enabling data collection for Citrix ADC Gateway appliances deployed in double-hop mode
- Enabling data collection for monitoring Citrix ADCs deployed in LAN user mode

Enable data collection for Citrix ADC Gateway appliances deployed in single-hop mode

September 24, 2021

When Citrix ADC Gateway is deployed in single-hop mode, the ADC Gateway is at the edge of the network and proxies ICA connections to the desktop delivery infrastructure. This deployment is the simplest and most common deployment. This mode provides security if an external user tries to access the internal network in an organization. In single-hop mode, users access the ADC appliances through a virtual private network (VPN).

To start collecting the reports, you must add the ADC Gateway appliance to the Citrix Application Delivery and Management inventory and enable AppFlow on Citrix Application Delivery and Management. The following image illustrates a Citrix Application Delivery and Management deployed in single-hop mode



Enable the AppFlow feature from Citrix Application Delivery and Management

1. Navigate to **Infrastructure** > **Instances**, and select the ADC instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the VPN virtual servers, and click **Enable Analytics**.
4. Select **Web Insight**.
5. Click **OK**.

> **Note**
>
> The following commands start to run in the background when you enable AppFlow in single-hop mode. 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`

Enable data collection to monitor Citrix ADCs deployed in transparent mode

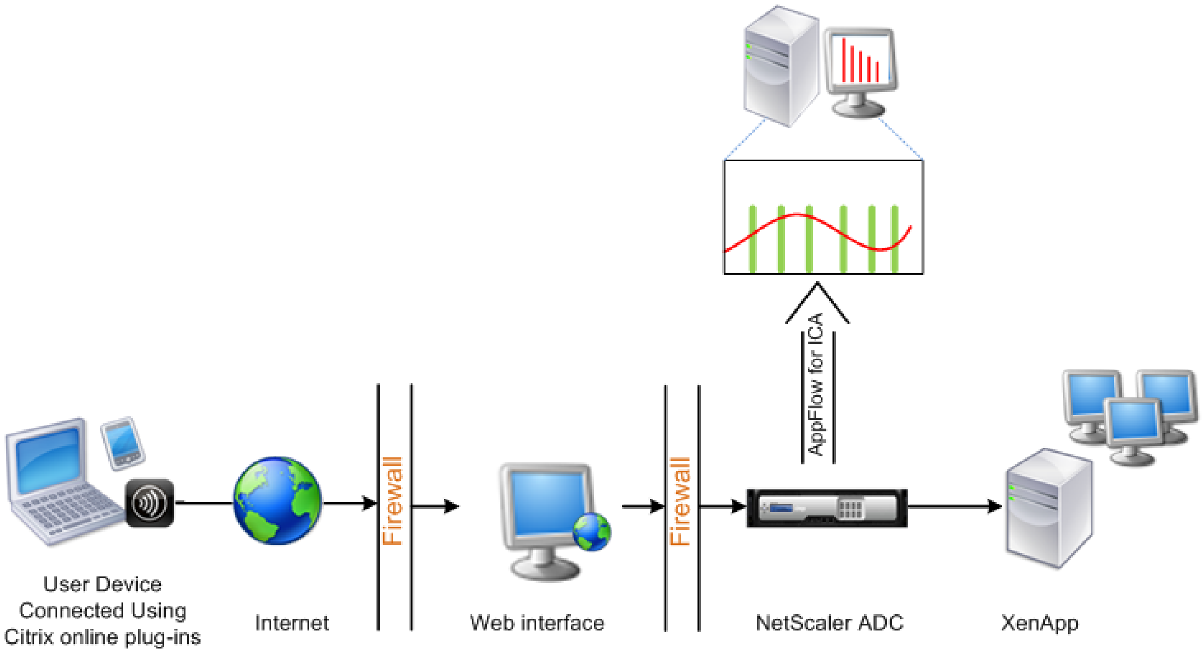
September 24, 2021

When a Citrix ADC is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a Citrix ADC appliance 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 Citrix ADC to the Citrix Application Delivery and Management 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 Citrix Application Delivery and Management as an AppFlow collector on each Citrix ADC 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 Citrix ADC deployed in transparent mode by using the Citrix Application Delivery and Management 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 image shows the network deployment of a Citrix Application Delivery and Management when a Citrix ADC is deployed in a transparent mode:



To configure data collection on a Citrix ADC 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 Citrix ADC 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 Citrix ADC 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 Citrix ADC 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
<!--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 Citrix ADC Gateway appliances deployed in double-hop mode

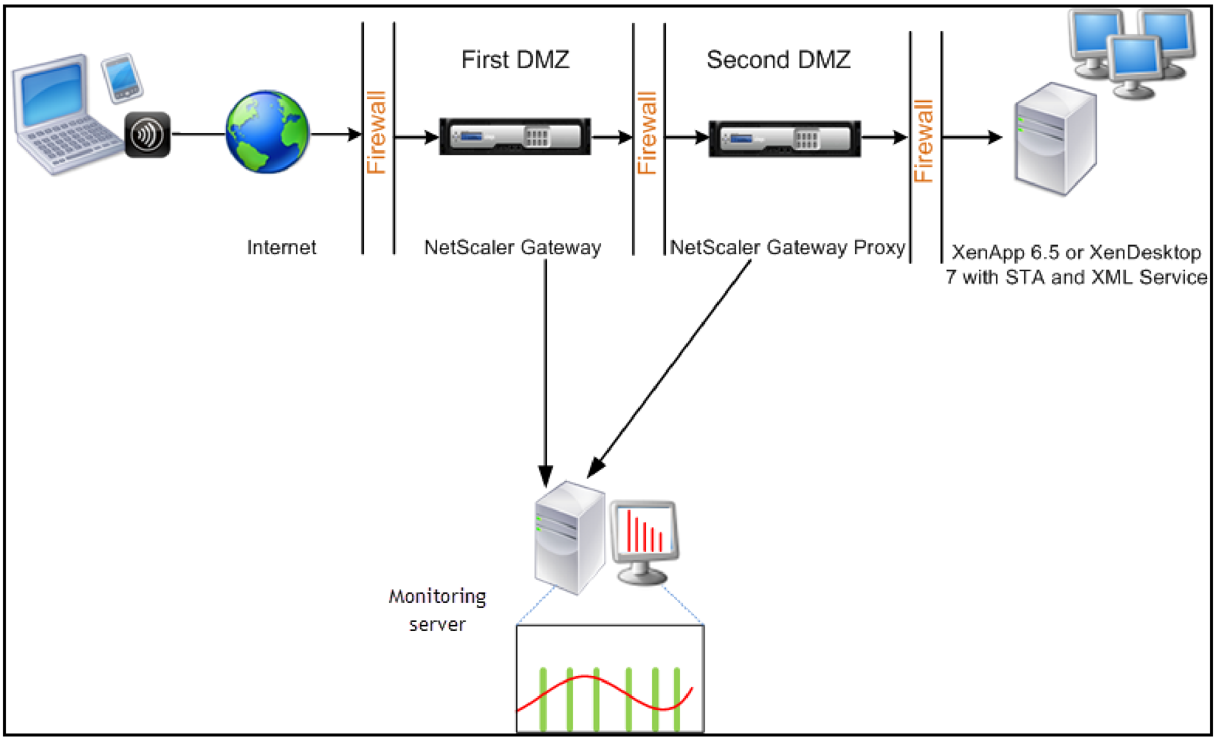
September 24, 2021

The Citrix ADC Gateway double-hop mode provides extra protection to an organization internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network.

As an administrator, using Citrix Application Delivery and Management, you can analyze:

- The number of hops (Citrix ADC Gateway appliances) through which the ICA connections pass
- The details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client

The following image indicates that the Citrix Application Delivery and Management and Citrix ADC Gateway in the first DMZ are deployed in the same subnet.



The Citrix ADC Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This Citrix ADC Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The Citrix ADC Gateway in the second DMZ serves as a Citrix ADC Gateway proxy device. This Citrix ADC Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The Citrix Application Delivery and Management can be deployed either in the subnet belonging to the Citrix ADC Gateway appliance in the first DMZ or the subnet belonging to the Citrix ADC Gateway appliance second DMZ.

In a double-hop mode, Citrix Application Delivery and Management collects TCP records from one appliance and ICA records from the other appliance. After you add the Citrix ADC Gateway appliances to the Citrix Application Delivery and Management inventory and enable data collection, each appliance export the reports by keeping track of the hop count and connection chain ID.

For Citrix Application Delivery and Management 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 Citrix ADC 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.

Citrix Application Delivery and Management uses the hop count and connection chain ID to co-relate the data from both the Citrix ADC Gateway appliances and generates the reports.

To monitor Citrix ADC Gateway appliances deployed in this mode, you must first add the Citrix ADC Gateway to Citrix Application Delivery and Management inventory, enable AppFlow on Citrix Application Delivery and Management, and then view the reports on the Citrix Application Delivery and Management dashboard.

Enabling data collection on Citrix Application Delivery and Management

If you enable Citrix Application Delivery and Management to start collecting the ICA details from both the appliances, the details collected are redundant. To overcome this situation, you must enable AppFlow for ICA on the first Citrix ADC Gateway appliance, 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 Citrix Application Delivery and Management:

1. Navigate to **Infrastructure** > **Instances**, and select the Citrix ADC instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the virtual servers, and click **Enable Analytics**.
4. Select Web **Insight**
5. Click **OK**.

Configure Citrix ADC Gateway appliances to export data

After you install the Citrix ADC Gateway appliances, you must configure the following settings on the Citrix ADC gateway appliances to export the reports to Citrix Application Delivery and Management:

- Configure virtual servers of the Citrix ADC Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the Citrix ADC Gateway virtual server in the second DMZ to the Citrix ADC Gateway virtual server in the first DMZ.
- Enable double hop on the Citrix ADC Gateway in the second DMZ.
- Disable authentication on the Citrix ADC Gateway virtual server in the second DMZ.
- Enable one of the Citrix ADC Gateway appliances to export ICA records
- Enable the other Citrix ADC Gateway appliance to export TCP records:
- Enable connection chaining on both the Citrix ADC Gateway appliances.

Configure Citrix ADC Gateway using the command line interface:

1. Configure the Citrix ADC Gateway virtual server in the first DMZ to communicate with the Citrix ADC Gateway virtual server in the second DMZ.

add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure** (ON	OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443  - secure ON
<!--NeedCopy-->
```

2. Bind the Citrix ADC Gateway virtual server in the second DMZ to the Citrix ADC Gateway virtual server in the first DMZ. Run the following command on the Citrix ADC 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 Citrix ADC Gateway in the second DMZ.

set vpn vserver <name> [-**doubleHop** (ENABLED	DISABLED)] [**- appflowLog** (ENABLED	DISABLED)]

```
set vpn vserver vpnhop2  - doubleHop ENABLED  - appFlowLog ENABLED
```

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

4. Disable authentication on the Citrix ADC Gateway virtual server in the second DMZ.

set vpn vserver<name> [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Enable one of the Citrix ADC 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 Citrix ADC 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 Citrix ADC Gateway appliances:

set appFlow param [**-connectionChaining** DISABLED)]
(ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configuring Citrix ADC Gateway using configuration utility:

1. Configure the Citrix ADC Gateway in the first DMZ to communicate with the Citrix ADC Gateway in the second DMZ and bind the Citrix ADC Gateway in the second DMZ to the Citrix ADC Gateway in the first DMZ.

   a) On the **Configuration** tab expand **Citrix ADC 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 Citrix ADC Gateway appliance.

2. Enable double hop on the Citrix ADC Gateway in the second DMZ.

   a) On the **Configuration** tab expand **Citrix ADC 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 Citrix ADC Gateway in the second DMZ.

   a) On the **Configuration** tab expand **Citrix ADC 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 Citrix ADC Gateway appliances to export TCP records.

   a) On the **Configuration** tab expand **Citrix ADC 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 Citrix ADC Gateway appliance to export ICA records:

   a) On the **Configuration** tab expand **Citrix ADC 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**.

6. Enable connection chaining on both the Citrix ADC Gateway appliances.

a) On the **Configuration** tab, navigate to **System** > **Appflow**.

b) In the right Pane, in the **Settings** group, click **Change Appflow Settings**.

c) Select **Connection Chaining** and Click **OK**.

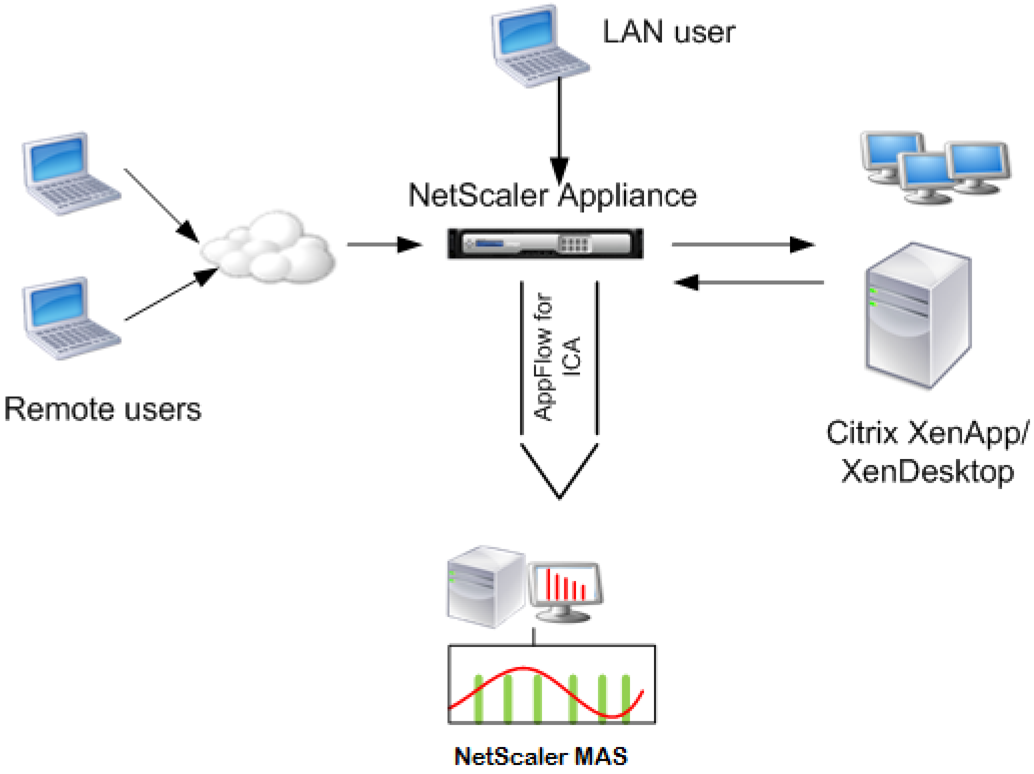
Enable data collection to monitor Citrix ADCs deployed in LAN user mode

September 24, 2021

External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the Citrix ADC Gateway. Internal users, however, might not require to be redirected to the ADC Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the Citrix ADC appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual App and Desktop applications, you can deploy the ADC appliance in a LAN user mode by configuring a cache redirection virtual server. The cache redirection virtual server acts as a SOCKS proxy on the ADC Gateway appliance.

The following image illustrates Citrix Application Delivery and Management deployed in **LAN User Mode**.



> **Note**
>
> Citrix ADC Gateway appliance must be able to reach the Citrix Application Delivery and Management agent.

To monitor Citrix ADC appliances deployed in this mode, first add the Citrix ADC appliance to the Citrix ADC Insight inventory, enable AppFlow, and then view the reports on the dashboard.

After you add the Citrix ADC appliance to the Citrix Application Delivery and Management inventory, you must enable AppFlow for data collection.

> **Note**
>
> - You cannot enable data collection on a Citrix ADC deployed in LAN User mode by using the Citrix Application Delivery and Management 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 Citrix ADC appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to Citrix ADC 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 Citrix ADC Gateway appliance, add an action to apply 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 Citrix Application Delivery and Management as an AppFlow collector on the Citrix ADC 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

September 24, 2021

HDX Insight on Citrix Application Delivery and Management allows you to monitor the HDX traffic passing through the Citrix ADC instances. Citrix Application Delivery and Management allows you to set thresholds on various counters used to monitor the Insight traffic. You can also configure rules and create alerts in Citrix Application Delivery and Management.

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 several 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 Citrix Application Delivery and Management 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 users entity, the threshold group can be associated with a geolocation as well.

An alert is generated on Citrix Application Delivery and Management 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, Citrix Application Delivery and Management 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 Citrix Application Delivery and Management or receive the alert as an email or both, or as an SMS on your mobile device. For the last two actions, you must configure the email server or the SMS server on Citrix Application Delivery and Management.

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 the Citrix ADC Gateway and 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.

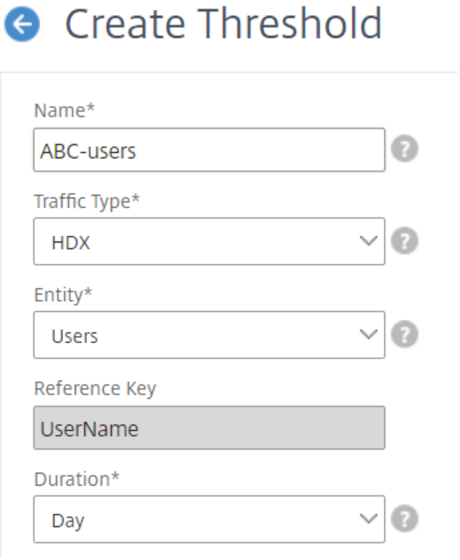
Create a threshold rule group and configure alerts for HDX Insight using Citrix Application Delivery and Management

1. In Citrix Application Delivery and Management, navigate to **Gateway** > **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 Citrix Application Delivery and Management generates an alert.
   b) **Traffic Type**. From the drop-down list box, select HDX.

c) **Entity**. From the drop-down 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 drop-down 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.



Create Threshold

Name*: ABC-users

Traffic Type*: HDX

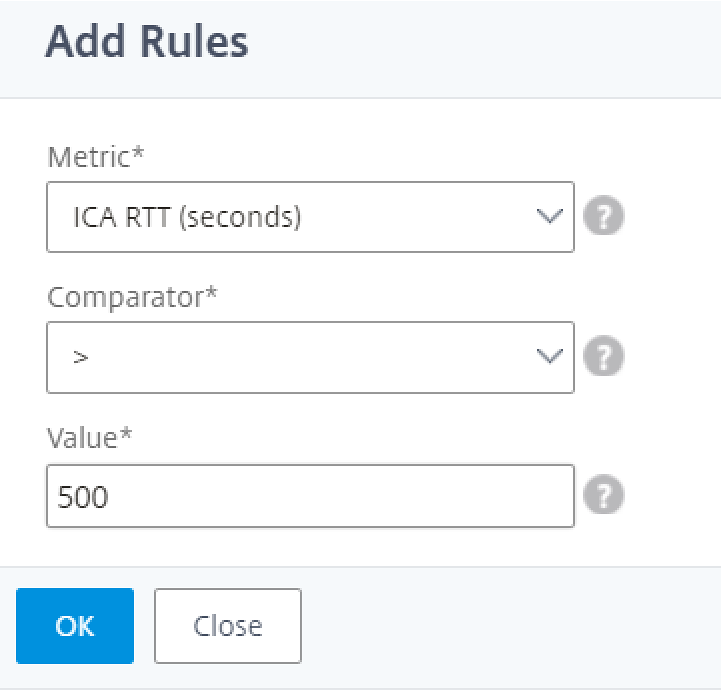
Entity*: Users

Reference Key: UserName

Duration*: Day

3. **Creating threshold rules group for all entities:**

   For HDX traffic, you must create a rule by clicking **Add Rule**. Enter the values in the **Add Rules** pop-up window that opens.



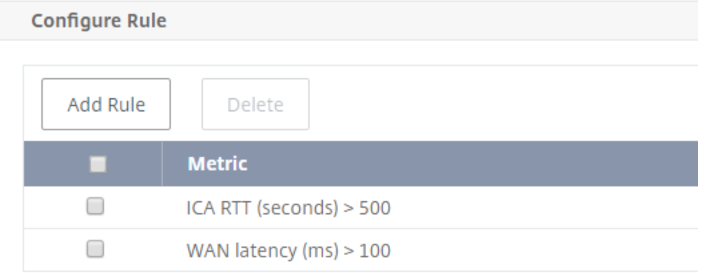
Add Rules

Metric*: ICA RTT (seconds)

Comparator*: >

Value*: 500

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.

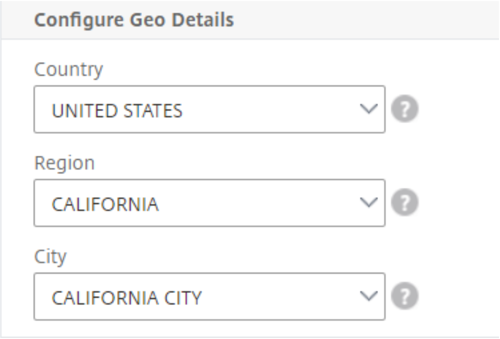


Configure Rule

□	Metric
□	ICA RTT (seconds) > 500
□	WAN latency (ms) > 100

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.



Configure Geo Details

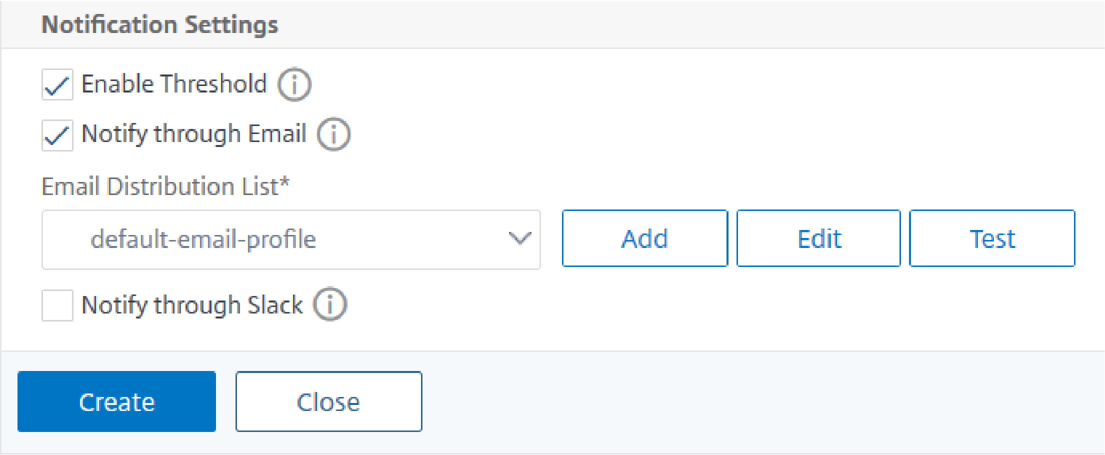
Country: UNITED STATES

Region: CALIFORNIA

City: CALIFORNIA CITY

5. Click **Enable Thresholds** to allow Citrix Application Delivery and Management to start monitoring the entities.

6. Optionally, configure actions such as email and Slack notifications.



Notification Settings

☑ Enable Threshold

☑ Notify through Email

Email Distribution List*: default-email-profile

□ Notify through Slack

7. Click **Create** to create a threshold rule group.

View HDX Insight reports and metrics

September 28, 2021

HDX insight provides complete visibility of the reports and metrics pertaining to HDX traffic on your Citrix ADC 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 Apps and Desktops 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 ADC 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.

This document includes the following:

- User View Reports and Metrics
- Application View Reports and Metrics
- Desktop View Reports and Metrics
- Instance View Reports and Metrics
- License View Reports and Metrics

Troubleshoot HDX Insight issues

September 28, 2021

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 Citrix ADC and Citrix Application Delivery and Management.
- Record generation for HDX/ICA traffic in Citrix ADC.
- Population of records in Citrix Application Delivery and Management.

HDX Insight configuration checklist

- Ensure that the AppFlow feature is enabled in Citrix ADC. For details, see Enabling AppFlow.
- Check HDX Insight configuration in the Citrix ADC 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 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 Citrix 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 Citrix ADC. For details see, Configuring Citrix Gateway appliances to export data.
- After HA Failover if the HDX Insight details are Skip parsed, check ICA param "enableSRonHAFailover" is enabled. For details, see Session Reliability on Citrix ADC High Availability Pair.

Connectivity between Citrix ADC and Citrix Application Delivery and Management checklist

- Check AppFlow collector status in Citrix ADC. For details, see How to check the status of connectivity between Citrix ADC 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 **System > 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 Citrix ADC 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 app

  Solution: Upgrade Citrix Workspace app 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 Citrix ADC.

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_C	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_B	Insufficient bytes to assign a coder to a channel
105	NS_ICA_ERR_INVALID_CHANNEL	Invalid ICA channel number
106	NS_ICA_ERR_INVALID_DECODE	Invalid decoder specified for a channel
107	NS_ICA_ERR_INVALID_TW_PARAM	Invalid parameter count specified on Thinwire channel

Skip Code	Error message	Cause of error
108	NS_ICA_ERR_INVALID_TW_DEC	Invalid decoder for Thinwire channel
109	NS_ICA_ERR_REDUC_NO_DECODER	No decoder defined for channel
110	NS_ICA_ERR_REDUC_V3_EXPAN	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Expander error: Bytes consumed more than bytes available
112	NS_ICA_ERR_REDUC_BYTES_O	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
116	NS_ICA_ERR_MEM_REDUC_CTX	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_SUPPOR	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_CH	Insufficient bytes over channel

Skip Code	Error message	Cause of error
123	NS_ICA_ERR_CHANNEL_DATA	Incorrect data on EUEM, CONTROL, or SEAMLESS channel
124	NS_ICA_ERR_INVALID_PURE_C	Invalid command received while processing pure ICA channel data
125	NS_ICA_ERR_INVALID_PURE_LEN	Invalid length encountered while processing pure ICA channel data
126	NS_ICA_ERR_INVALID_PURE_LI	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_REC	Retrieval of reconnected session failed
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Error disabling SR
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 receivers
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

Skip Code	Error message	Cause of error
138	NS_ICA_ERR_ICAFRAME_TOO_L	ICA frame is too large, exceeds 1,460 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_F	Skipped ICA parsing for this receiver (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_RECONN	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_	Invalid receiver 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_CORRUP	Invalid channel length post expansion
149	NS_ICA_ERR_SPECIAL_THINWIRE	Decompression error
150	NS_ICA_ERR_SEAMLESS_INSUF	Encountered insufficient bytes for seamless command
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Encountered insufficient bytes for EUEM command
152	NS_ICA_ERR_SEAMLESS_INVAL	Invalid event for seamless channel parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Invalid event for CTRL channel parsing

Skip Code	Error message	Cause of error
154	NS_ICA_ERR_EUEM_INVALID_E	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_E	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_EV	Invalid event for ICA data parsing
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Invalid event for CGP data parsing
160	NS_ICA_ERR_BASICCRYPT_INV	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_INVAL	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_RE	VDA does not support Reducer Version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Receiver does not support Reducer Version 3
168	NS_ICA_ERR_ICAP_INSUFFBYT	Unexpected number of bytes in ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Higher CGP resumption sequence number from peer post reconnects

Skip Code	Error message	Cause of error
170	NS_ICA_ERR_DESCSRINFO_ABS	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_E	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_CLIEN	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 fetching service reconnects ticket in service node
180	NS_ICA_ERR_SN_HIGHER_RECO	Error when receiving higher reconnect sequence number in service node
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NON_NSAP	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 [0x8820220228], 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 [0x8820220008], 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 counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_tot_udt_conn	Indicates total number of UDP ICA connections detected by NS	Stats
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 du valid 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 Citrix ADC error	Stats/Diagnostics

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_host_rejected_ns_rec	Total number of hosts rejected reconnects requests by client	Stats/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, HDX Insight skips this connection.	Error
hdx_err_skip_old_server	Old unsupported server version	Error
hdx_err_clnt_not_whitelist	Client receiver not in allow list, HDX Insight skips this connection	Error
hdx_sm_ica_cam_channel_disa	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_disa	Total number of NS_ICA_CLIP_CHANNEL disabled via SmartAccess policy	Diagnostics

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_sm_ica_ccm_channel_disabled	Total number of NS_ICA_CCM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cdm_channel_disa	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_di	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_disa	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 counter name	Purpose	Category(Stats/Error/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_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 Citrix ADC.

Population of records in Citrix Application Delivery and Management checklist

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`and check logs to confirm Citrix Application Delivery and Management is receiving AppFlow records.
- Confirm Citrix ADC instance is added to Citrix Application Delivery and Management.
- Validate Citrix Gateway/VPN virtual server is licensed in Citrix Application Delivery and Management.
- Make sure multi-hop parameter setting is enabled for double-hop.
- Make sure Citrix 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.
- Citrix ADC and Citrix Application Delivery and Management versions.
- Citrix Virtual Apps and Desktops server versions.
- Client Receiver versions.
- Number of Active ICA sessions when the issue occurred.
- Tech support bundle captured by running the `show techsupport` command at the Citrix ADC command prompt.
- Tech support bundle captured for Citrix Application Delivery and Management.
- Packet traces captured on all Citrix ADC.
  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 Citrix ADC release notes for known issues on HDX Insight.

Metrics information for thresholds

September 25, 2021

You can create thresholds and get it notified whenever the threshold value breaches. In a typical deployment, you can set thresholds to:

- Track various application metrics
- Facilitate planning
- Get notified whenever the applications metric value exceeds the set threshold

To configure threshold:

1. Navigate to **Settings > Analytics Settings > Thresholds**.
2. On the **Thresholds** page, click **Add**.

Web

Metrics	Entity	Description
Applications	Hits	Total number of hits received by a virtual server (application)
	Bandwidth (MB)	Total bandwidth consumed by the virtual server (application)
	Response Time (ms)	The time taken for the virtual server to respond
Clients	Requests	The total request received by a client
	Render Time (ms)	The time taken to render server response by the client
	Client Network Latency	The time taken for requests from the client network
Devices	Hits	Total number of hits received by a device. For example: laptop, mobile phone
	Bandwidth (MB)	Total bandwidth consumed by a device
Domains	Hits	Total number of hits received by a network domain
	Bandwidth (MB)	Total bandwidth consumed by a network domain
	Response Time (ms)	The time taken to respond requests by a network domain
Operating System	Hits	Total number of hits received by an operating system
	Bandwidth (MB)	Total bandwidth consumed by an operating system
	Render Time (ms)	The time taken to render server response by an operating system

Metrics	Entity	Description
Request Methods	Hits	Total number of requests received by a Request Method. For example: GET, POST
	Bandwidth (MB)	Total bandwidth consumed by a Request Method
Response Status	Hits	Total number of hits received with response codes
	Bandwidth (MB)	Total bandwidth consumed by response code
Servers	Hits	Total number of requests/hits received by a server
	Bandwidth (MB)	Total bandwidth consumed by a server
	Server Network Latency (ms)	The time taken for requests from the server network
	Server Processing Time (ms)	The time taken by a server to respond to requests
URLs	Hits	Total number of hits received by a URL. For example: www.Citrix.com
	Load Time (ms)	The time taken for a URL to load from the server
	Render Time (ms)	The time taken by the URL to render and display
User Agents	Hits	Total number of requests received by a user agent. For example: Chrome web browser
	Bandwidth (MB)	Total bandwidth consumed by the user agent
	Render Time (ms)	The time taken to render the server response by the user agent

Security

Metric	Entity	Description
Applications	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.
	Safety Index	A single-digit rating system that indicates how securely you have configured the Citrix ADC 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.

APPANALYTICS

Metric	Entity	Description
Applications	AppScore	App Score defines how well an application is performing and shows whether the application is performing well in terms of responsiveness. The values range from 0 to 80.

HDX

For information on HDX thresholds, see Create thresholds and configure alerts for HDX Insight

Infrastructure Analytics

September 25, 2021

A key goal for network administrators is to monitor Citrix ADC 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. Administrators must also be able to remediate any probable issues in configuration, setup, connectivity, certificates, and other impacts in application usage or performance. For example, a sudden change in 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 to a measurable score that defines the health of an instance. With this feature, administrators get a single touch point to understand the problem, the origin of the problem, and probable remediations that they can perform.

Infrastructure Analytics in Citrix Application Delivery and Management

The Infrastructure Analytics feature collates all the data gathered from the Citrix ADC instances and quantifies it into an **Instance Score** that defines the health of the instances. The instance score is summarized over 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 explained

- System resources indicators

  The following are the critical system resource issues that might occur on Citrix ADC instances and monitored by Citrix Application Delivery and Management.

  - **High CPU usage**. The CPU usage has crossed the higher threshold value in the Citrix ADC instance.
  - **High memory usage**. The memory usage has crossed the higher threshold value in the Citrix ADC instance.
  - **High disk usage**. The disk usage has crossed the higher threshold value in the Citrix ADC 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 Citrix ADC instance.
  - **NIC discards**. The packets discarded by the NIC card have crossed the higher threshold value in the Citrix ADC instance.

For more information on these system resources errors, see Instance dashboard.

- Critical events indicators

  The following critical events are identified by the events under event management feature of Citrix Application Delivery and Management 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 Citrix ADC instances.

  For more information on events in Citrix Application Delivery and Management, see Events.

- SSL configuration indicators
  - **Not recommended key strength**. The key strength of the SSL certificates is not as per Citrix 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 Citrix 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.

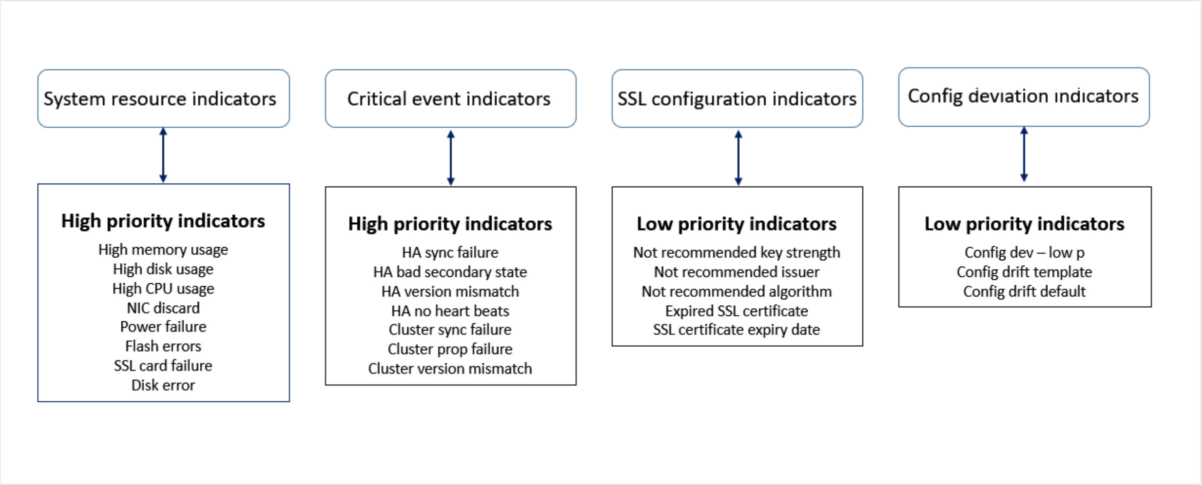
For more information on configuration deviations and how to run audit reports to check configuration deviation, see View audit reports..

View ADC Capacity issues

When an ADC instance has consumed most its available capacity, packet-drop might occur while processing the client traffic. By understanding such ADC capacity issues, you can proactively allocate additional licenses to steady the ADC performance. For more information, see View the capacity issuess in an ADC instance.

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.

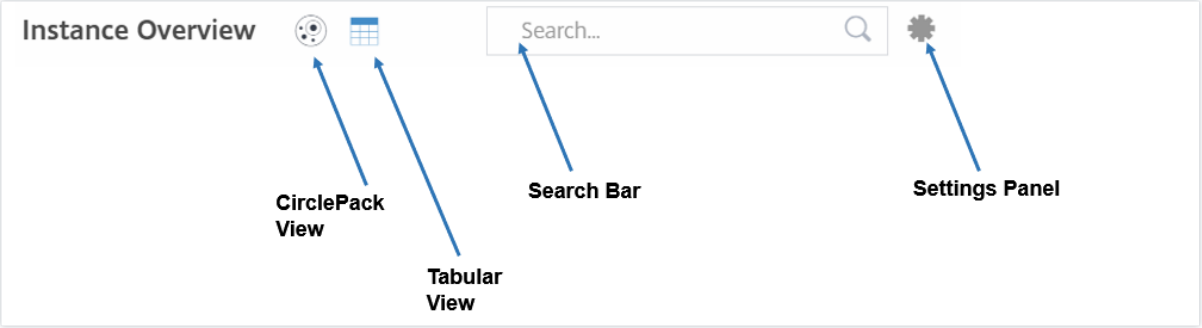
3. **Based on the low and high threshold value breach**. Here, an indicator can be triggered in two ways:
    - When the value of the indicator is between low and high thresholds, in which case a partial penalty is levied on the instance score.
    - When the value crosses the high threshold, in which 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**.

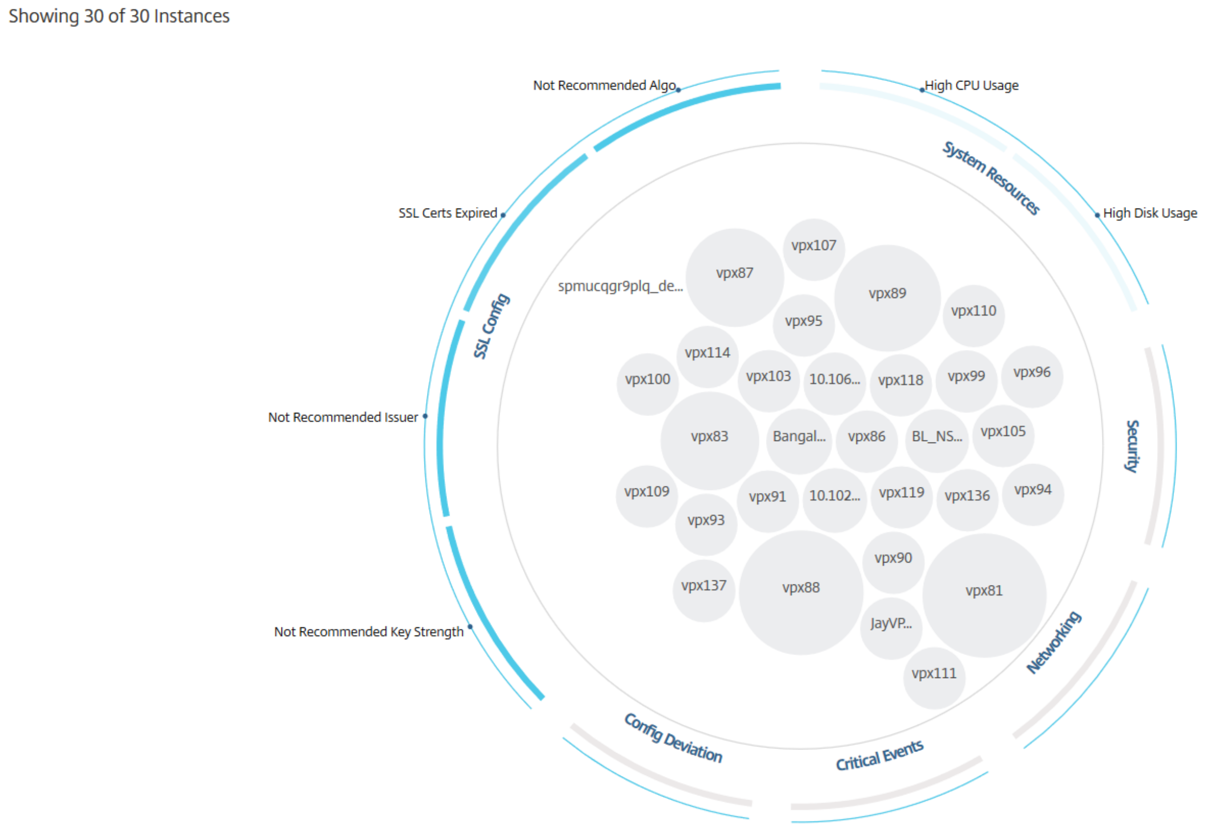
The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.



- 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

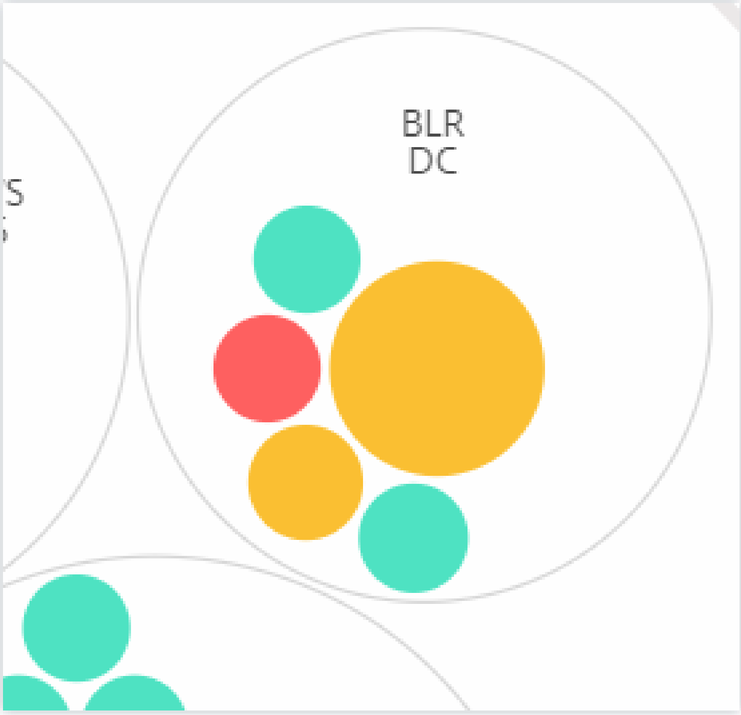
Circle packing diagrams show instance groups as tightly organized circles. They often show hierarchies where smaller instance groups are either colored similarly to others in the same category, or nested within larger groups. Circle packs represent hierarchical data sets and shows different levels in the hierarchy and how they interact with each other.



Instance circles

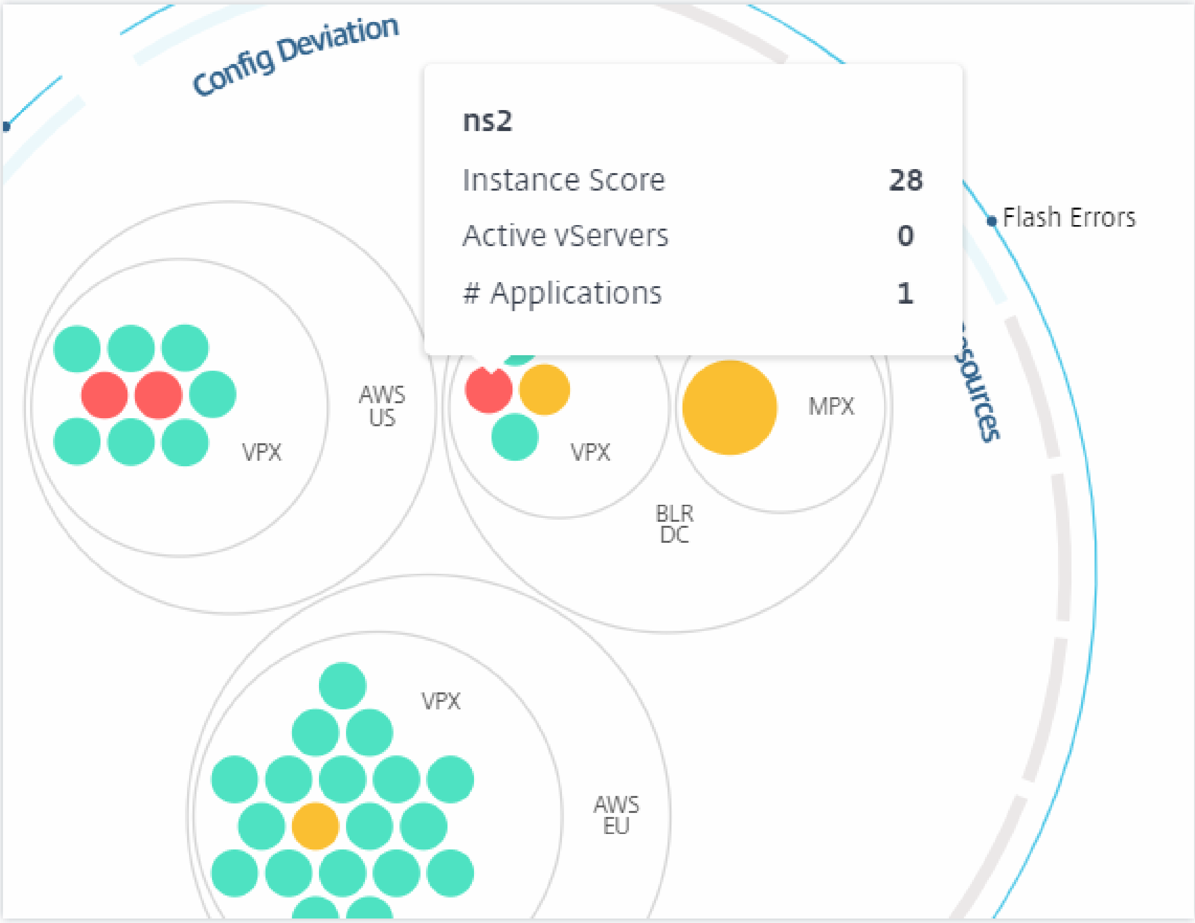
Color. Each instance is represented in Circle Pack as a colored circle. The color of the circle indicates the health of that instance.

- **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.



ns2

Instance Score 28

Active vServers 0

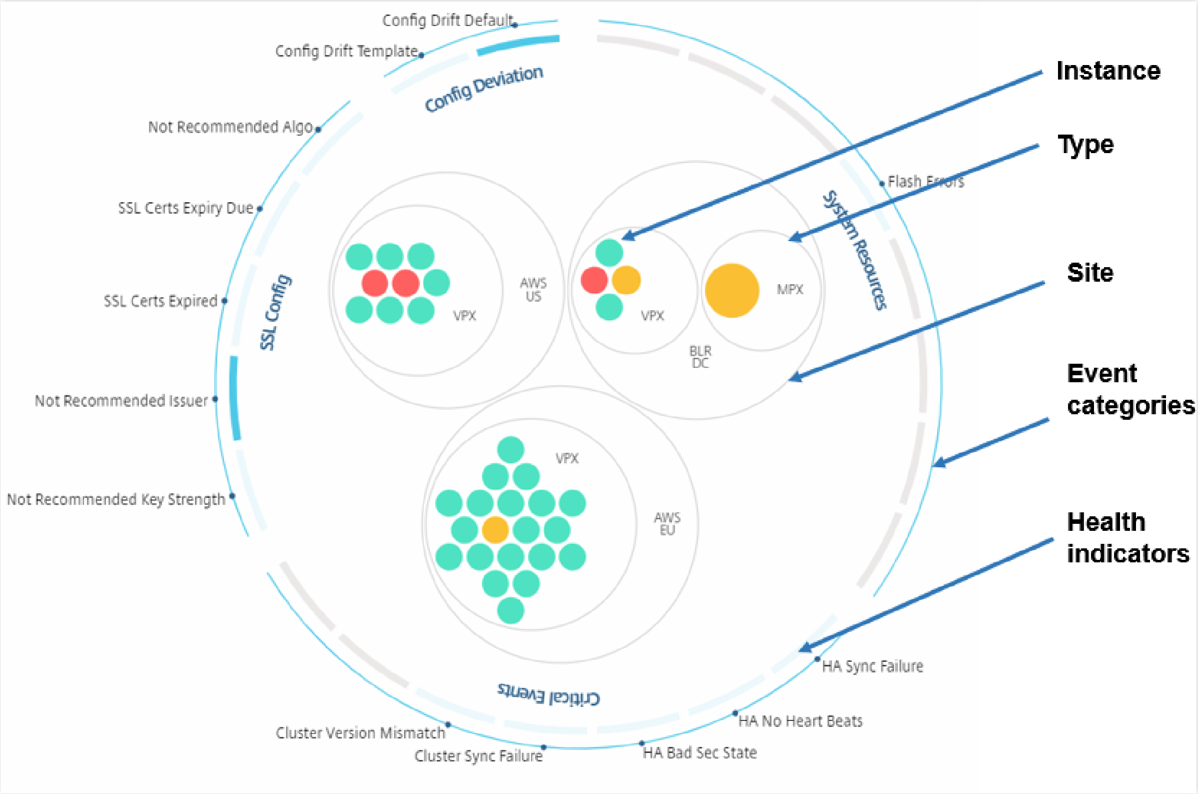
Applications 1

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.

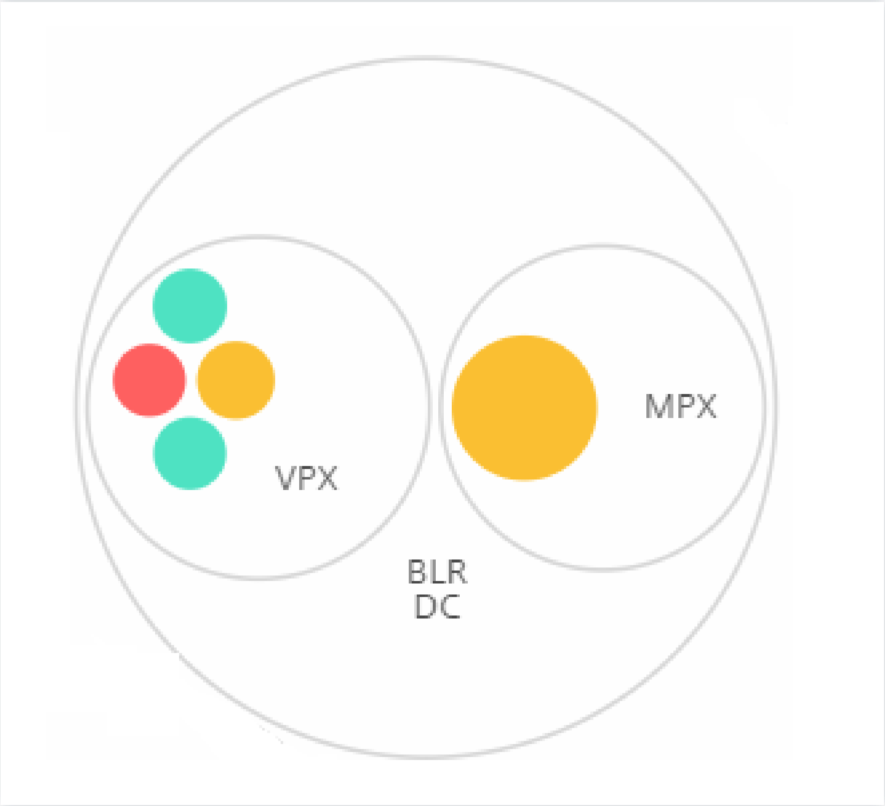


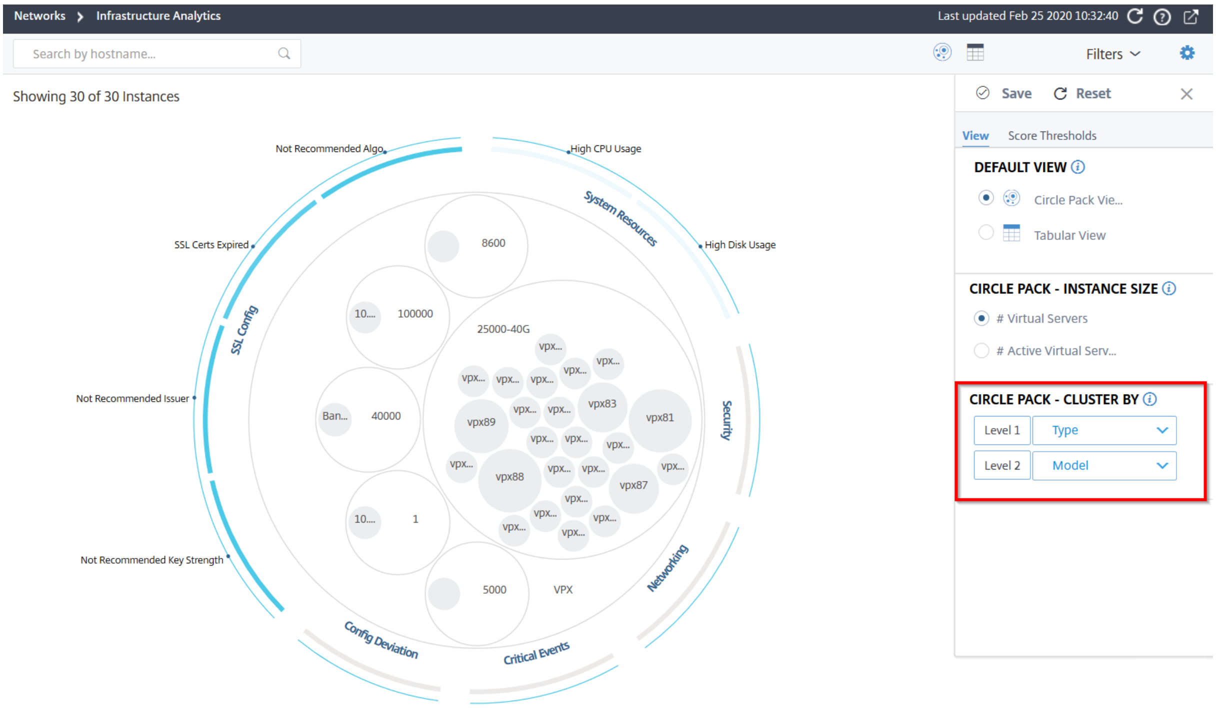
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the Citrix Application Delivery and Management (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

Clustered instance circles

Citrix Application Delivery and Management 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.





Last updated Feb 25 2020 10:32:40

Search by hostname...

Showing 30 of 30 Instances

Save Reset

View Score Thresholds

DEFAULT VIEW

● Circle Pack Vie...

○ Tabular View

CIRCLE PACK - INSTANCE SIZE

● # Virtual Servers

○ # Active Virtual Serv...

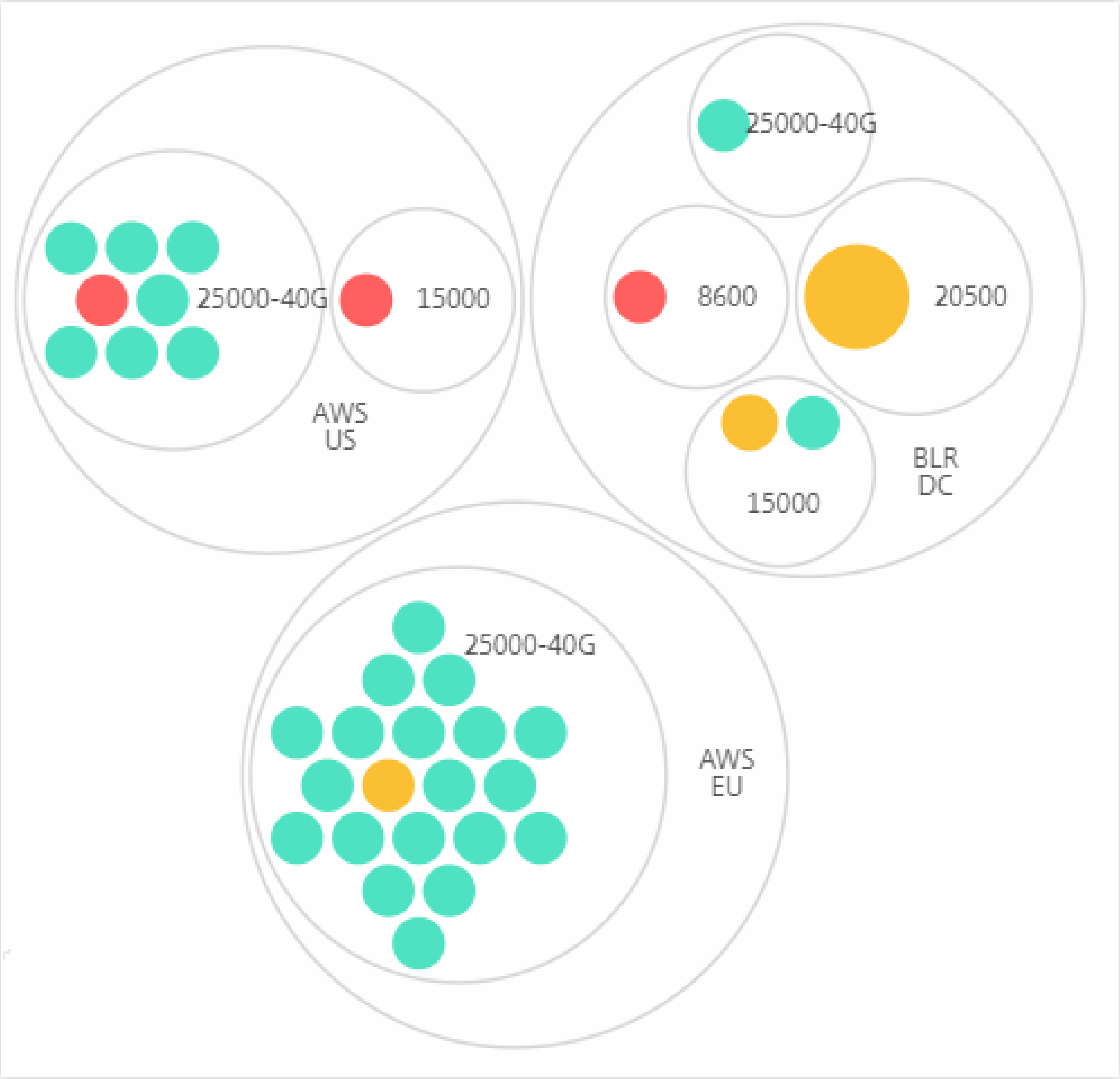
CIRCLE PACK - CLUSTER BY

Level 1: Type

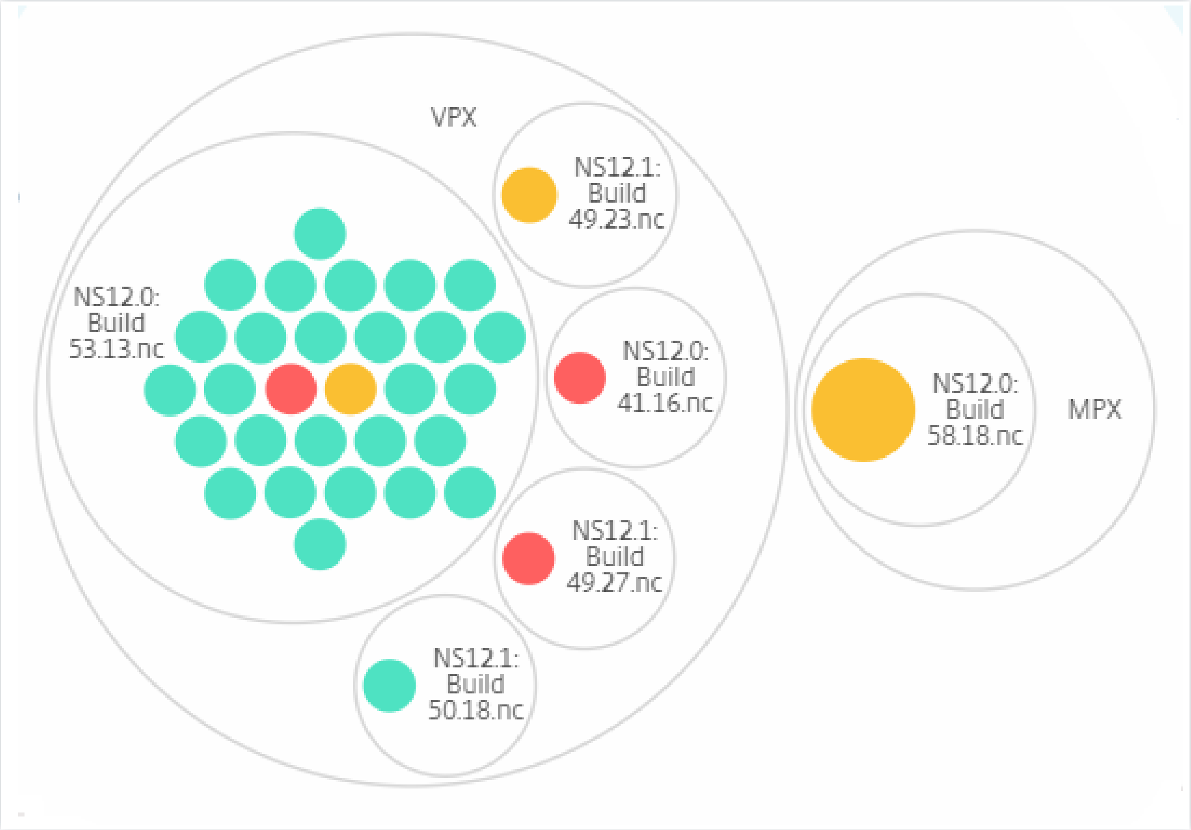
Level 2: Model

A few more examples of two-level clustering are as follows:

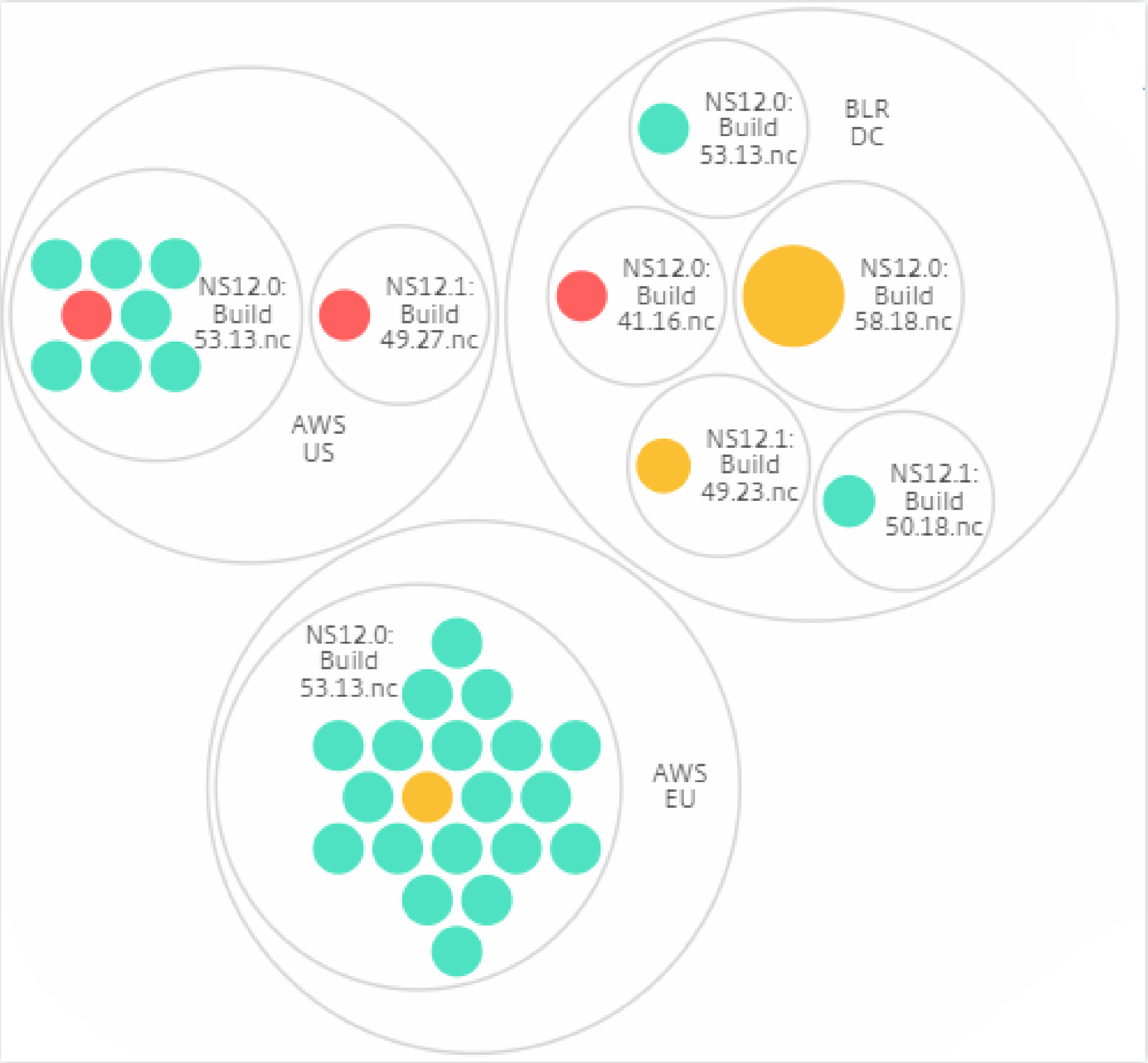
Site and model:



Type and version:

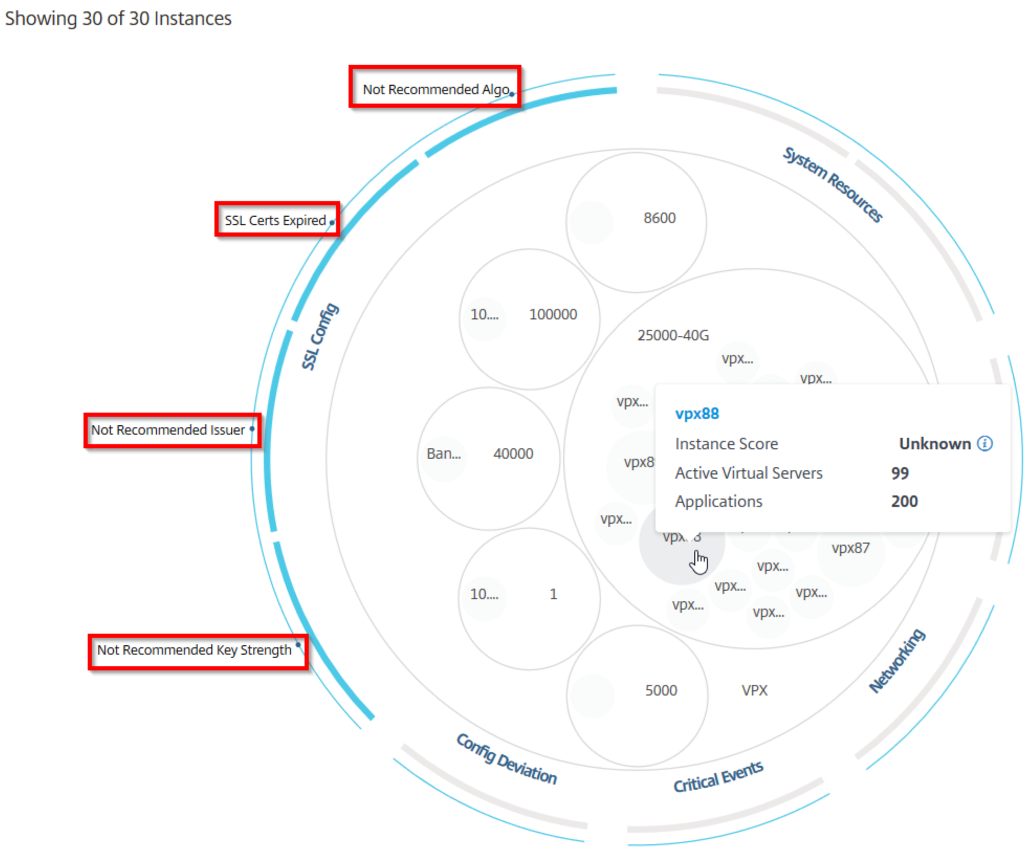


Site and version:



How to use Circle Pack

Click each of the colored circle to highlight that instance.

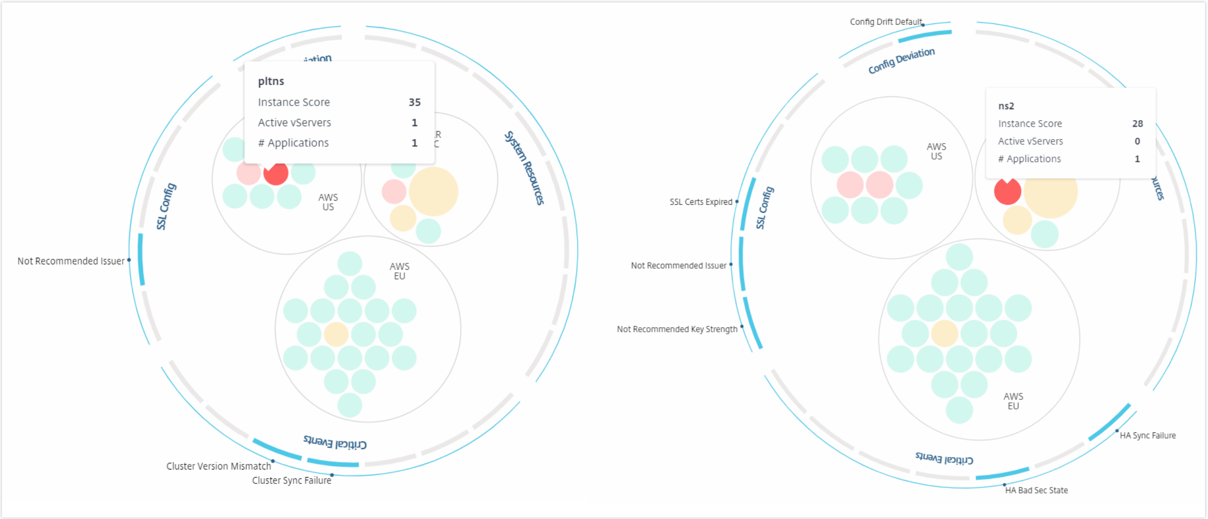


Showing 30 of 30 Instances

vpx88

Instance Score	Unknown
Active Virtual Servers	99
Applications	200

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.



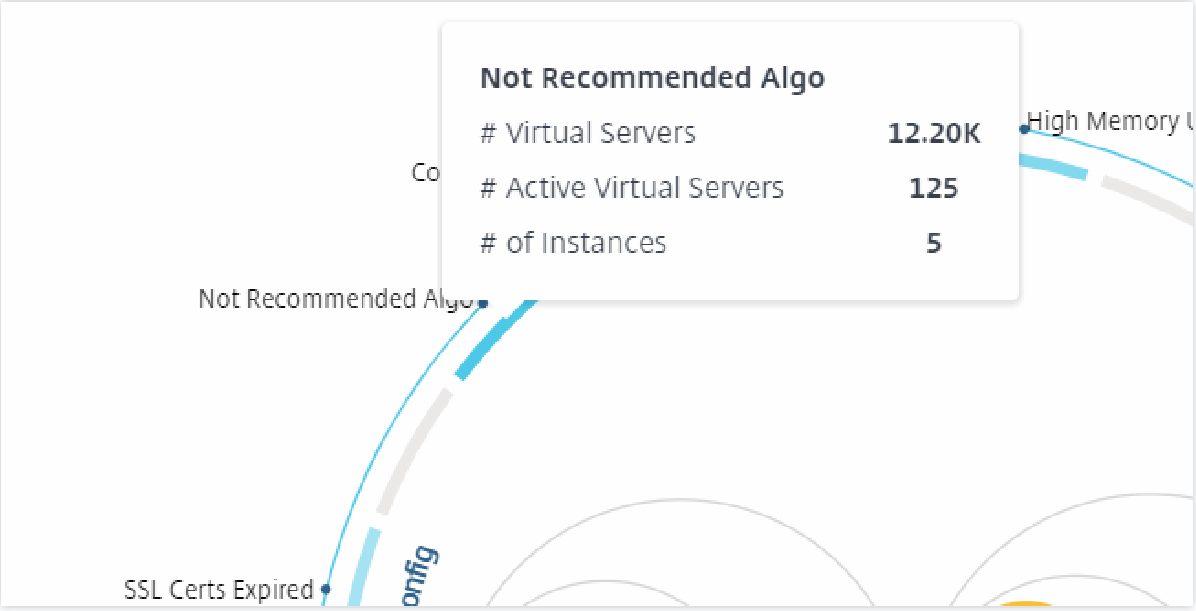
pltns

Instance Score	35
Active vServers	1
# Applications	1

ns2

Instance Score	28
Active vServers	0
# Applications	1

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.



Not Recommended Algo

# Virtual Servers	12.20K
# Active Virtual Servers	125
# of Instances	5

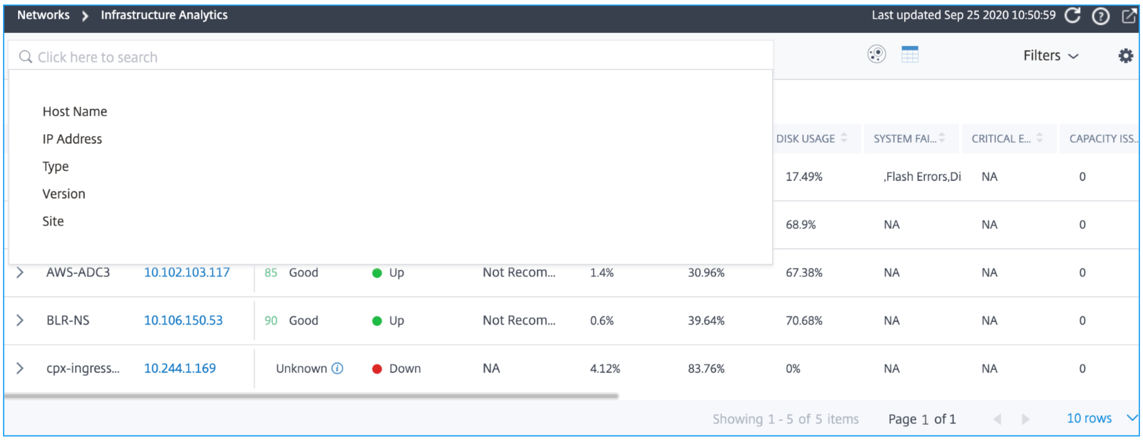
Tabular view

The tabular view displays the instances and the details of those instances in a tabular format. For more information, see Instance details

Search bar

Place the mouse cursor on the search bar and select the following search attributes to filter the results:

- Host name
- IP address
- Type
- Version
- Site



Last updated Sep 25 2020 10:50:59

							DISK USAGE	SYSTEM FAI...	CRITICAL E...	CAPACITY ISS...
							17.49%	,Flash Errors,Di	NA	0
							68.9%	NA	NA	0
AWS-ADC3	10.102.103.117	85 Good	● Up	Not Recom...	1.4%	30.96%	67.38%	NA	NA	0
BLR-NS	10.106.150.53	90 Good	● Up	Not Recom...	0.6%	39.64%	70.68%	NA	NA	0
cpx-ingress...	10.244.1.169	Unknown ⓘ	● Down	NA	4.12%	83.76%	0%	NA	NA	0

Showing 1 - 5 of 5 items Page 1 of 1 10 rows

The search results work for both circle view and table view.

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

For more information on these indicators, see *Health indicators in Citrix ADC instances*.

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.

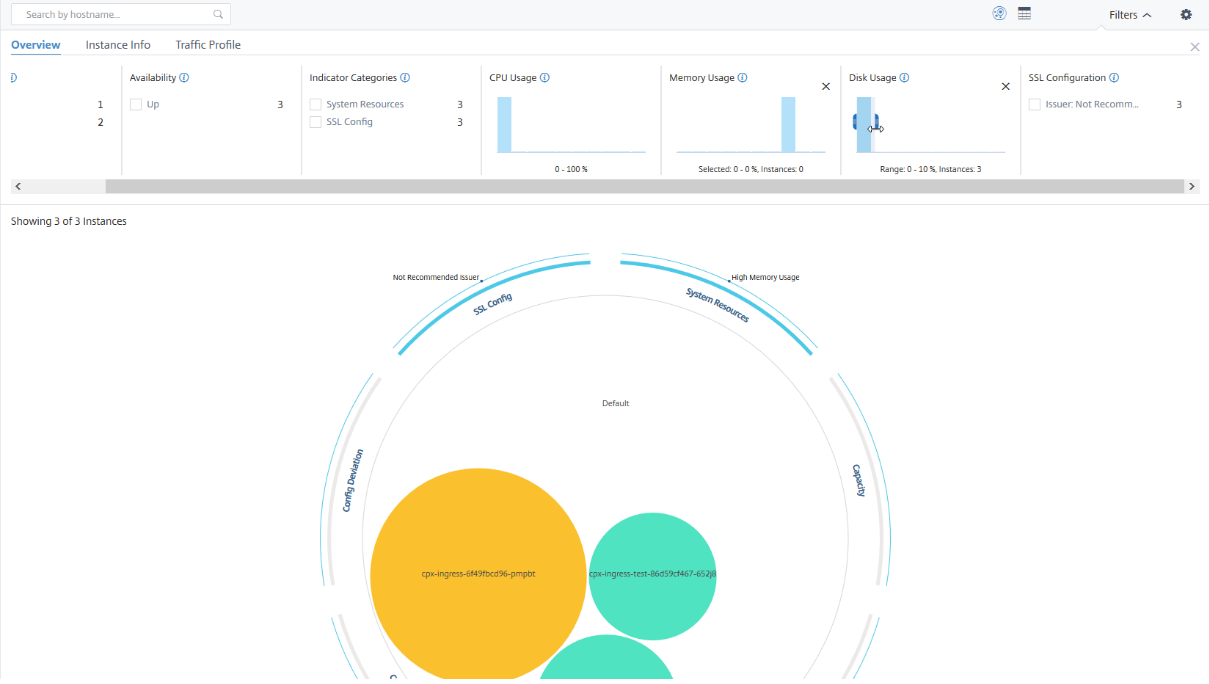
Example 2: View instances that are consuming between 10% and 20% of the allocated memory:

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 disk space in multiple ranges:

To view instances that have consumed memory between 0% and 10% disk space, drag the mouse pointer over the two ranges as shown in the following image.

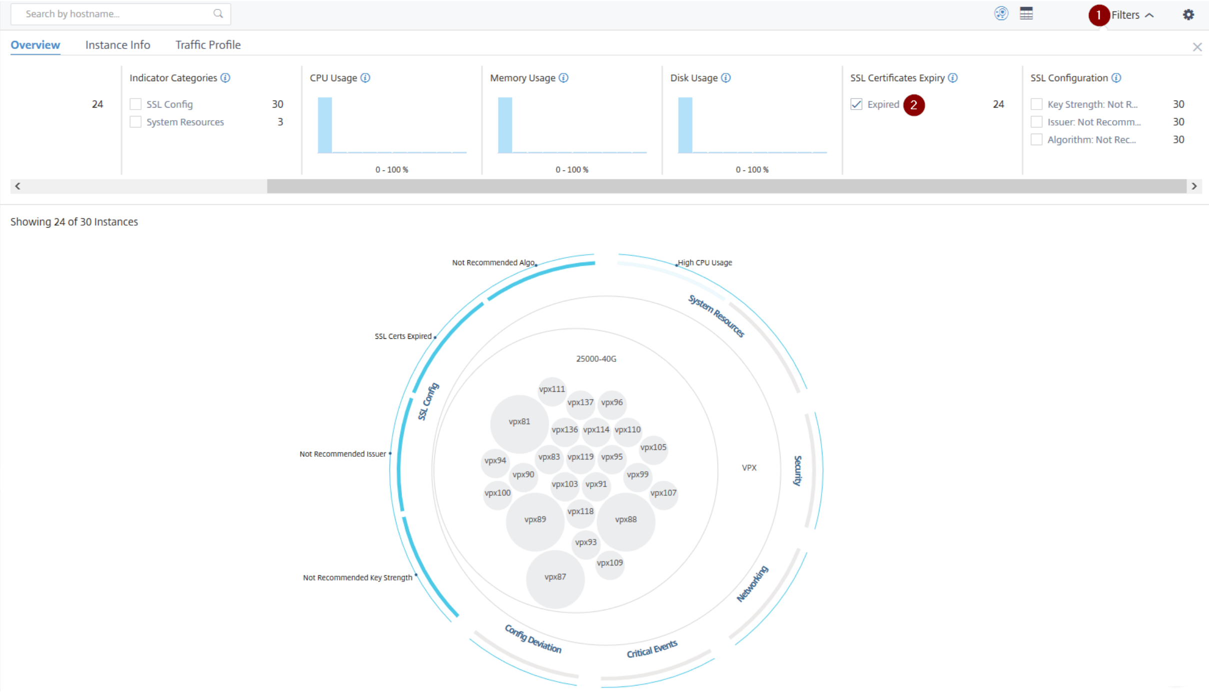


> **Note**
>
> Click "X" to remove the selection. You can also click **Reset** to remove multiple selections.

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:

In the **SSL certificates expiry** section, select **Expired** check box to view the three instances.



1 - Click the **Filter** list.

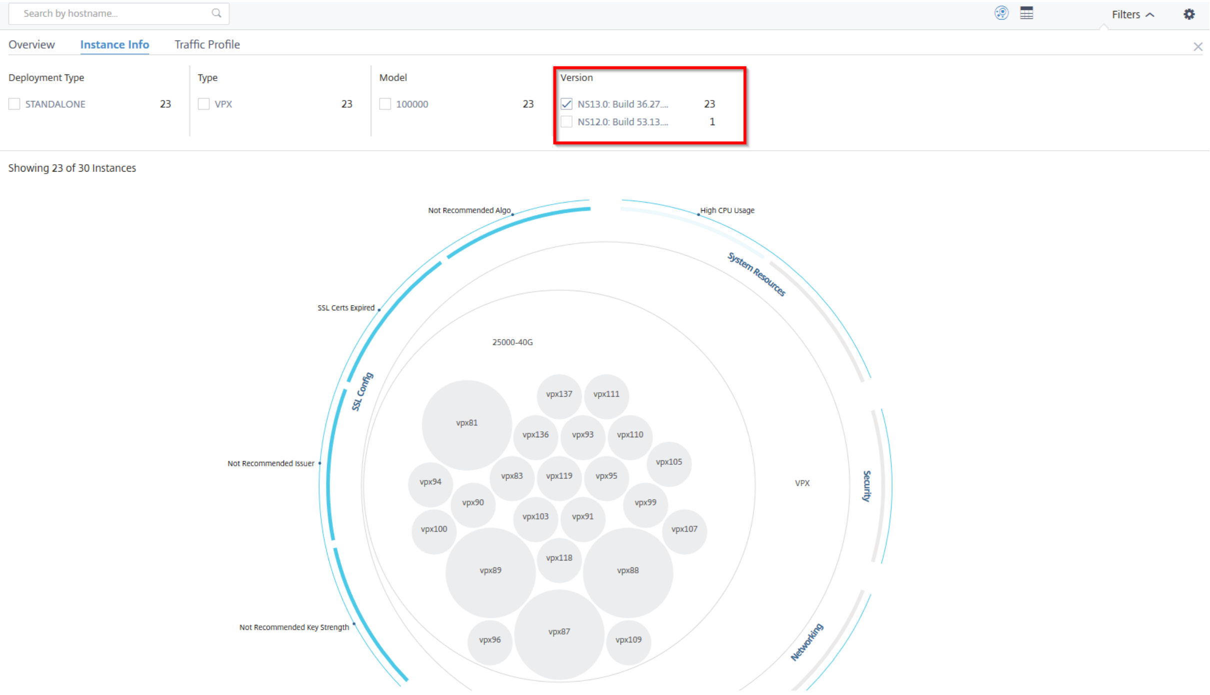
2 - In the **SSL certificates expiry** section, select **Expired** check box to view the instances.

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 ADC VPX instances with specific build number:

Select the version that you want to view.



Search by hostname...

Overview | Instance Info | Traffic Profile

Deployment Type
□ STANDALONE 23

Type
□ VPX 23

Model
□ 100000 23

Version
☑ NS13.0: Build 36.27... 23
□ NS12.0: Build 53.13... 1

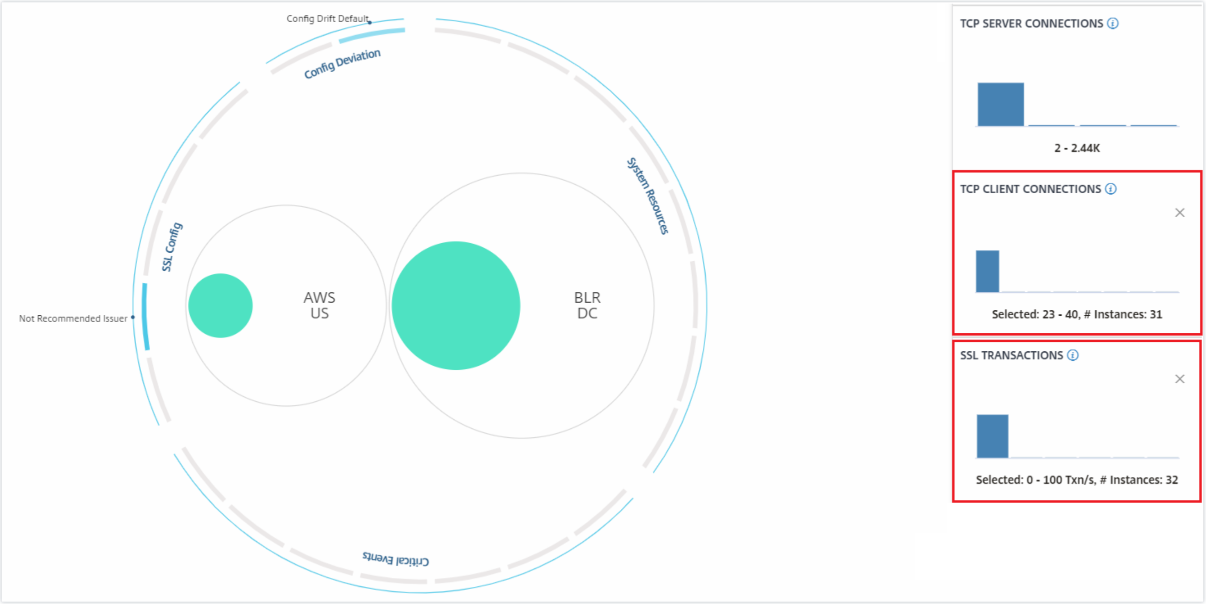
Showing 23 of 30 Instances

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 between 23 and 40, and also processing up to 100 SSL transactions per second.

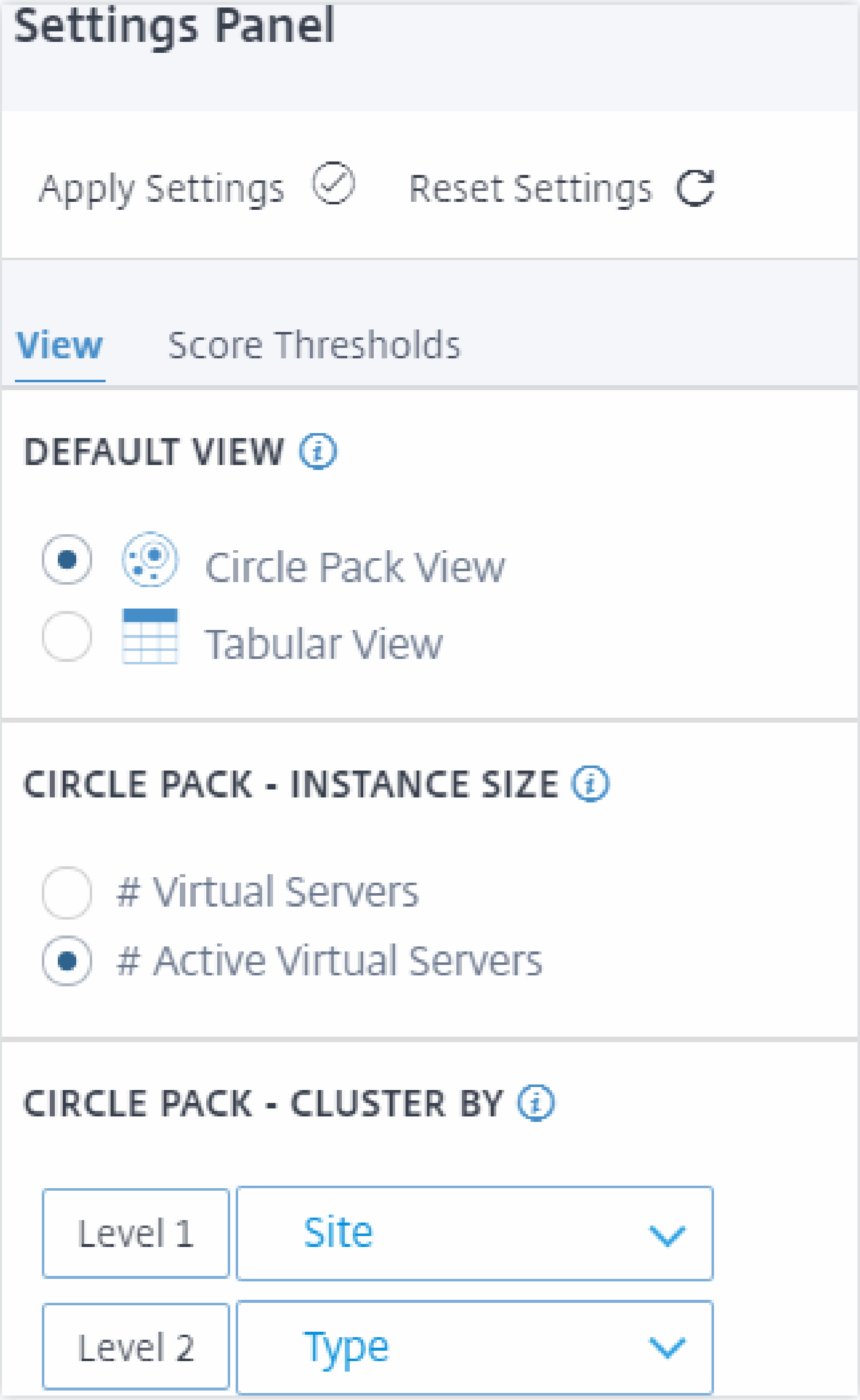


How to use the settings panel

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 Citrix Application Delivery and Management.
- **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.



Settings Panel

Apply Settings ✓ Reset Settings

View Score Thresholds

DEFAULT VIEW

● Circle Pack View
○ Tabular View

CIRCLE PACK - INSTANCE SIZE

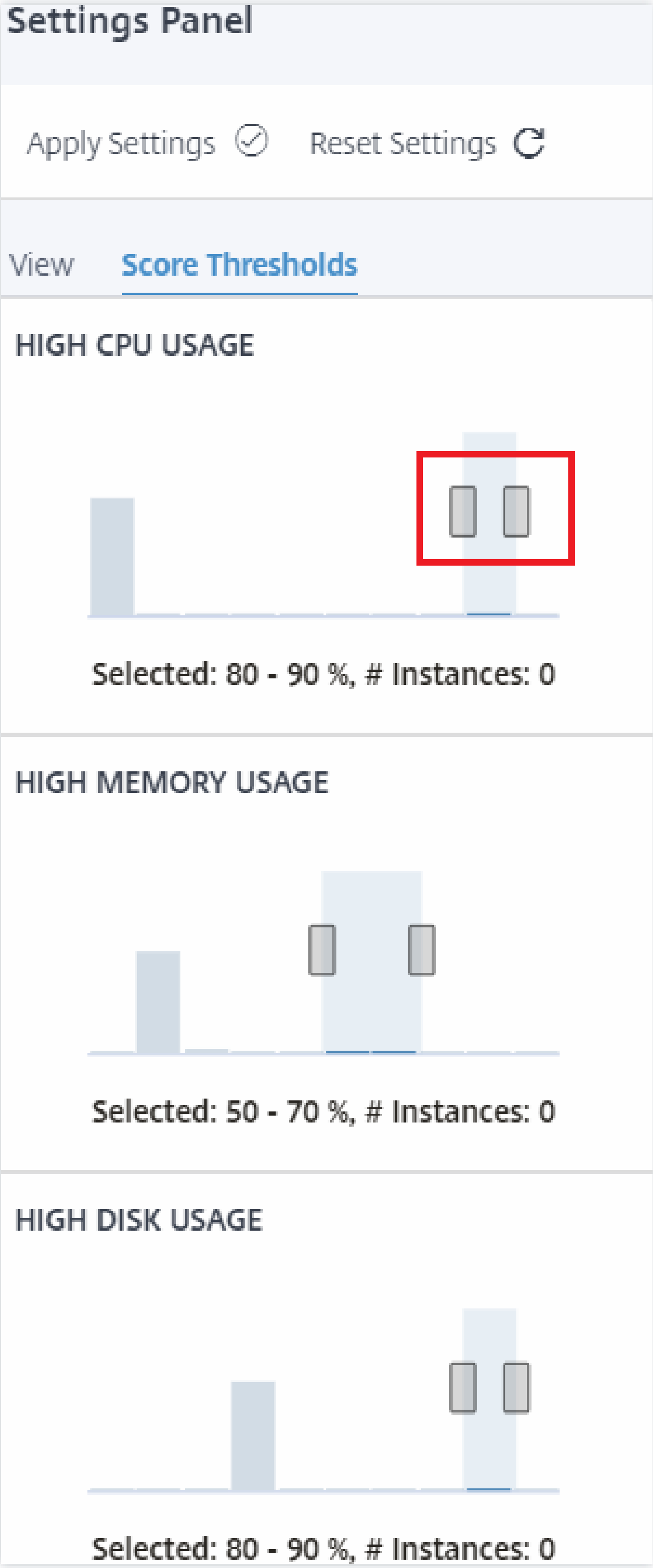
○ # Virtual Servers
● # Active Virtual Servers

CIRCLE PACK - CLUSTER BY

Level 1: Site
Level 2: Type

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.



Settings Panel

HIGH CPU USAGE

Selected: 80 - 90 %, # Instances: 0

HIGH MEMORY USAGE

Selected: 50 - 70 %, # Instances: 0

HIGH DISK USAGE

Selected: 80 - 90 %, # Instances: 0

> **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 this in more detail, let us consider the case of Chris, a network admin of ExampleCompany.

Chris maintains many Citrix ADC instances in his organization. A few of the instances process high traffic, and he needs to monitor them closely. He notices that a few high-traffic instances are no longer processing the full traffic passing through them. To analyze this reduction, earlier, he 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. He 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. He clicks the instance to see what the issue is. The instance summary displays that there is an SSL card failure on that instance and therefore that 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.

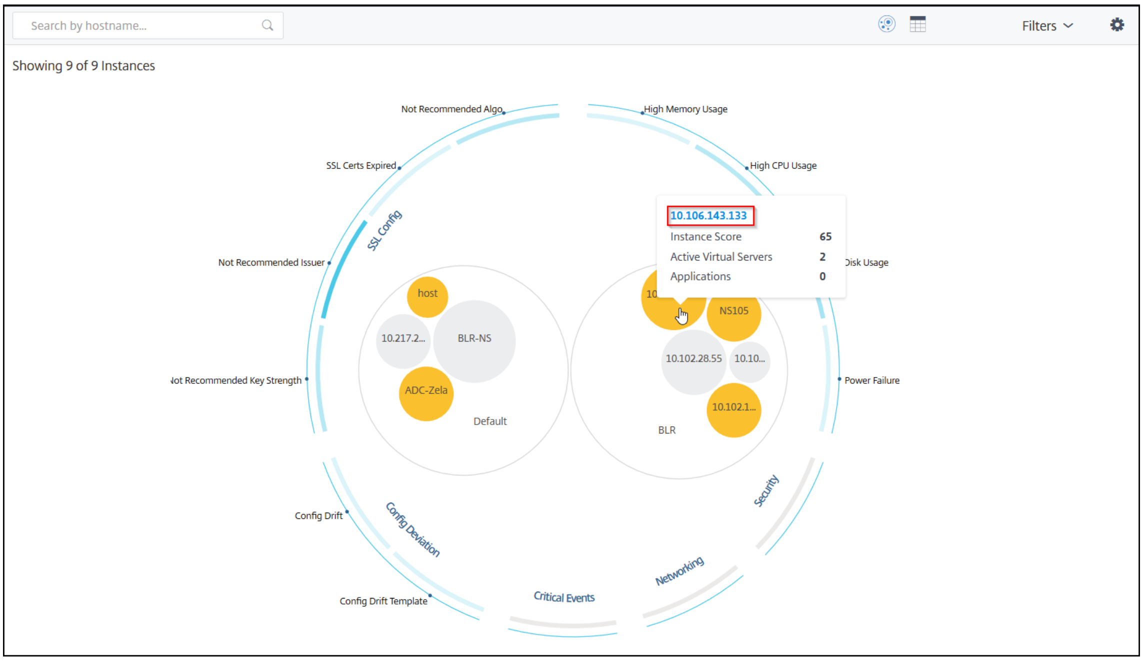
Example 2 - To monitor configuration changes:

Chris also notices that another instance is in "Review" state and that there has been a config deviation recently. When he clicks the config deviation risk indicator, he 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. He also notices that the SSL transaction traffic profile for this instance has gone down. He exports this report and sends it to the admin to inquire further.

View instance details in Infrastructure Analytics

September 25, 2021

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Click the circle pack view and select the IP address.



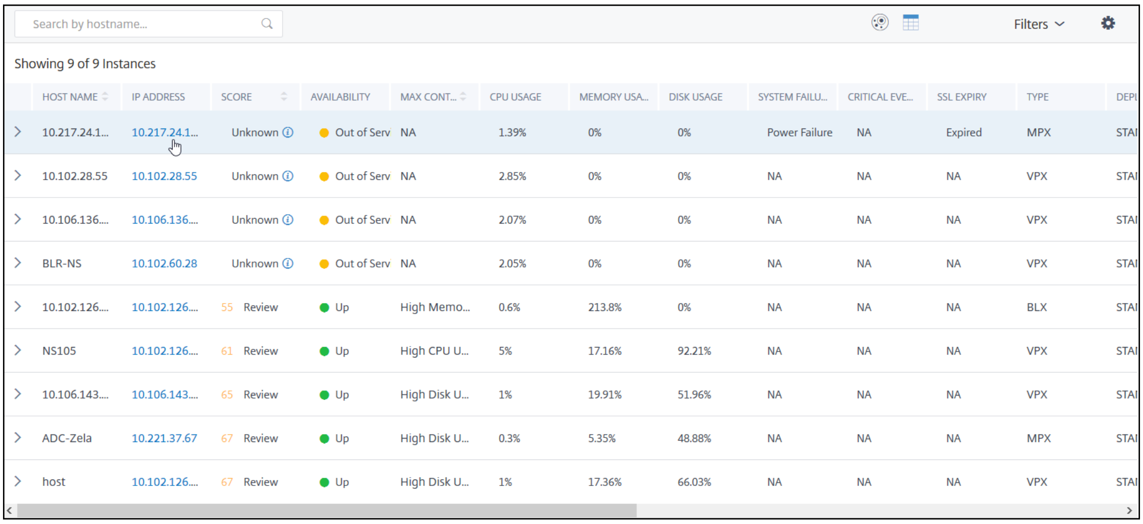
10.106.143.133

Instance Score 65

Active Virtual Servers 2

Applications 0

You can also click an IP address from the table view.



Showing 9 of 9 Instances

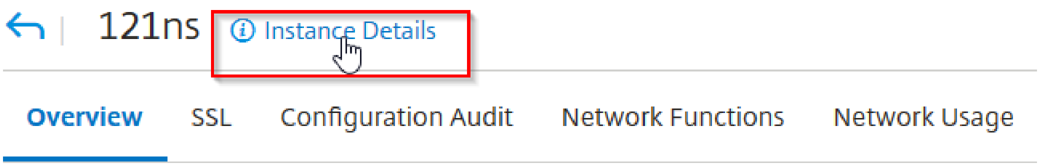
	HOST NAME	IP ADDRESS	SCORE	AVAILABILITY	MAX CONT...	CPU USAGE	MEMORY USA...	DISK USAGE	SYSTEM FAILU...	CRITICAL EVE...	SSL EXPIRY	TYPE	DEPL
>	10.217.24.1...	10.217.24.1...	Unknown ⓘ	● Out of Serv	NA	1.39%	0%	0%	Power Failure	NA	Expired	MPX	STAI
>	10.102.28.55	10.102.28.55	Unknown ⓘ	● Out of Serv	NA	2.85%	0%	0%	NA	NA	NA	VPX	STAI
>	10.106.136....	10.106.136....	Unknown ⓘ	● Out of Serv	NA	2.07%	0%	0%	NA	NA	NA	VPX	STAI
>	BLR-NS	10.102.60.28	Unknown ⓘ	● Out of Serv	NA	2.05%	0%	0%	NA	NA	NA	VPX	STAI
>	10.102.126....	10.102.126....	55 Review	● Up	High Memo...	0.6%	213.8%	0%	NA	NA	NA	BLX	STAI
>	NS105	10.102.126....	61 Review	● Up	High CPU U...	5%	17.16%	92.21%	NA	NA	NA	VPX	STAI
>	10.106.143....	10.106.143....	65 Review	● Up	High Disk U...	1%	19.91%	51.96%	NA	NA	NA	VPX	STAI
>	ADC-Zela	10.221.37.67	67 Review	● Up	High Disk U...	0.3%	5.35%	48.88%	NA	NA	NA	MPX	STAI
>	host	10.102.126....	67 Review	● Up	High Disk U...	1%	17.36%	66.03%	NA	NA	NA	VPX	STAI

- **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 current 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 Citrix ADC instance has the maximum events
- **SSL expiry** – Denotes the current 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.

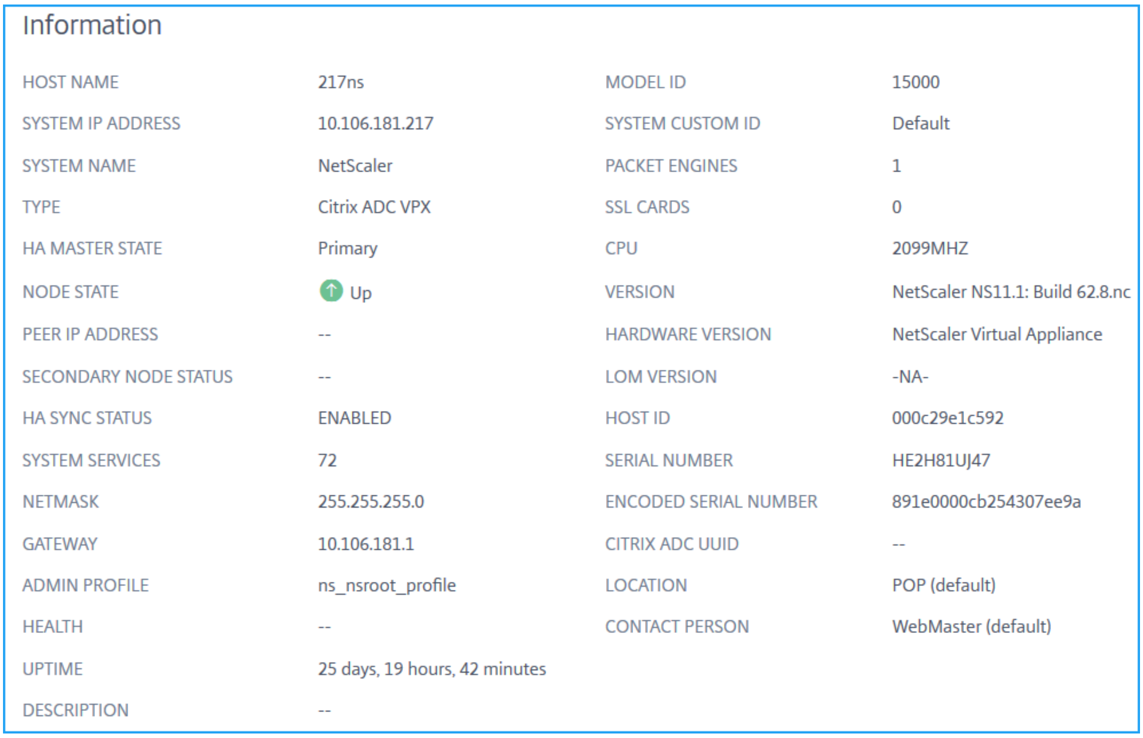
> **Note**
>
> For every 5 minutes, the current values for CPU usage, memory usage, disk usage, throughput, and so on are updated.

Click **Instance Details** to view the details.



The following details are displayed:

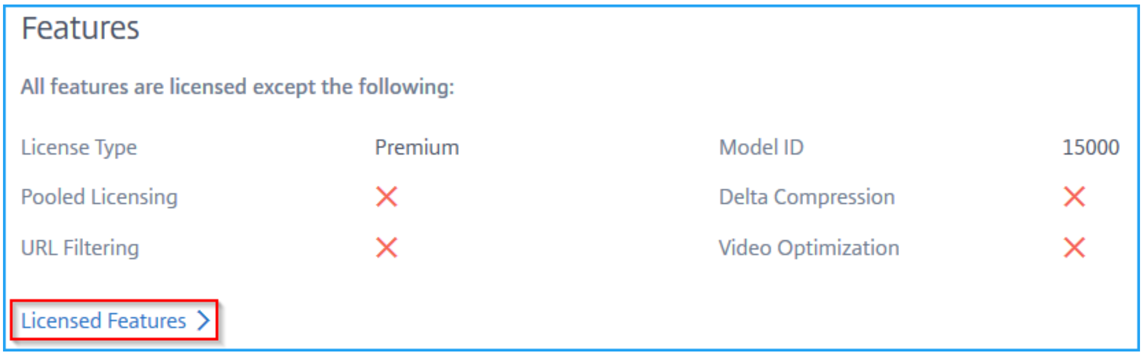
- **Information** - Instance details such as instance type, deployment type, version, model, and so on.



Information

HOST NAME	217ns	MODEL ID	15000
SYSTEM IP ADDRESS	10.106.181.217	SYSTEM CUSTOM ID	Default
SYSTEM NAME	NetScaler	PACKET ENGINES	1
TYPE	Citrix ADC VPX	SSL CARDS	0
HA MASTER STATE	Primary	CPU	2099MHZ
NODE STATE	● Up	VERSION	NetScaler NS11.1: Build 62.8.nc
PEER IP ADDRESS	--	HARDWARE VERSION	NetScaler Virtual Appliance
SECONDARY NODE STATUS	--	LOM VERSION	-NA-
HA SYNC STATUS	ENABLED	HOST ID	000c29e1c592
SYSTEM SERVICES	72	SERIAL NUMBER	HE2H81UJ47
NETMASK	255.255.255.0	ENCODED SERIAL NUMBER	891e0000cb254307ee9a
GATEWAY	10.106.181.1	CITRIX ADC UUID	--
ADMIN PROFILE	ns_nsroot_profile	LOCATION	POP (default)
HEALTH	--	CONTACT PERSON	WebMaster (default)
UPTIME	25 days, 19 hours, 42 minutes		
DESCRIPTION	--		

- **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.

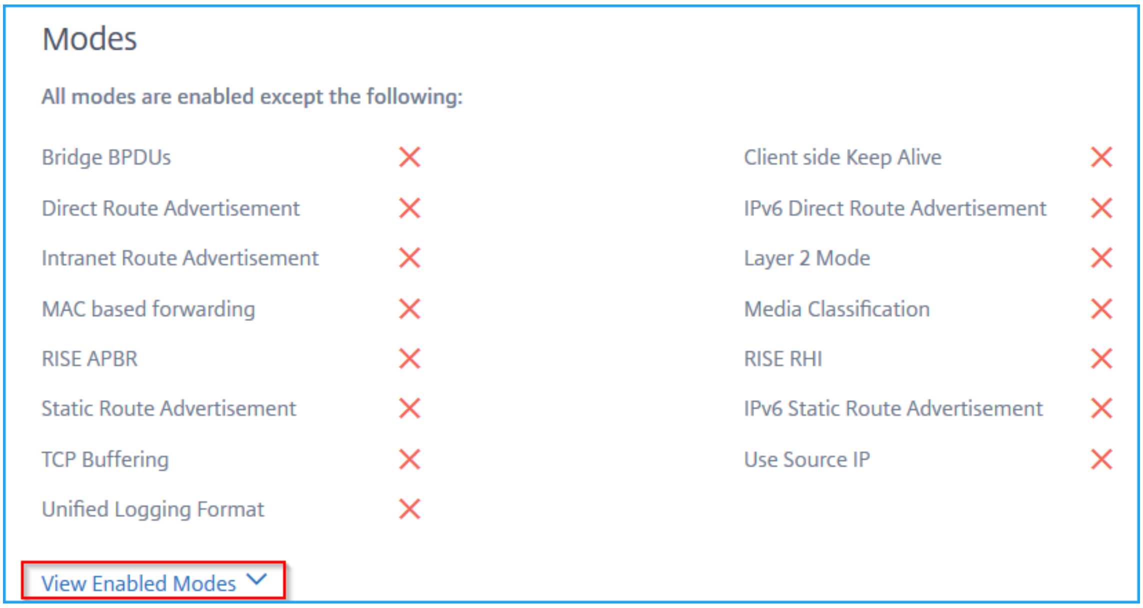


Features

All features are licensed except the following:

License Type	Premium	Model ID	15000
Pooled Licensing	✗	Delta Compression	✗
URL Filtering	✗	Video Optimization	✗

- **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.



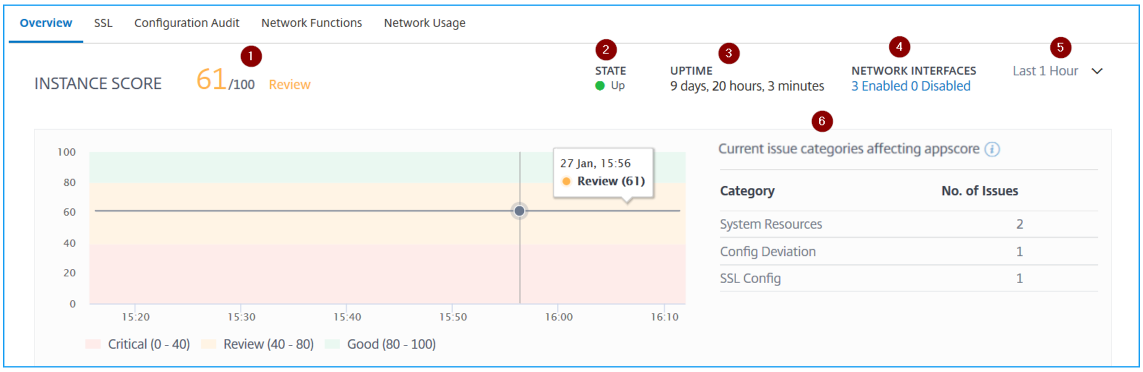
Modes

All modes are enabled except the following:

Bridge BPDUs	✗	Client side Keep Alive	✗
Direct Route Advertisement	✗	IPv6 Direct Route Advertisement	✗
Intranet Route Advertisement	✗	Layer 2 Mode	✗
MAC based forwarding	✗	Media Classification	✗
RISE APBR	✗	RISE RHI	✗
Static Route Advertisement	✗	IPv6 Static Route Advertisement	✗
TCP Buffering	✗	Use Source IP	✗
Unified Logging Format	✗		

The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**



INSTANCE SCORE 61/100 Review

STATE ● Up

UPTIME 9 days, 20 hours, 3 minutes

NETWORK INTERFACES 3 Enabled 0 Disabled

Critical (0 - 40) Review (40 - 80) Good (80 - 100)

Current issue categories affecting appscore

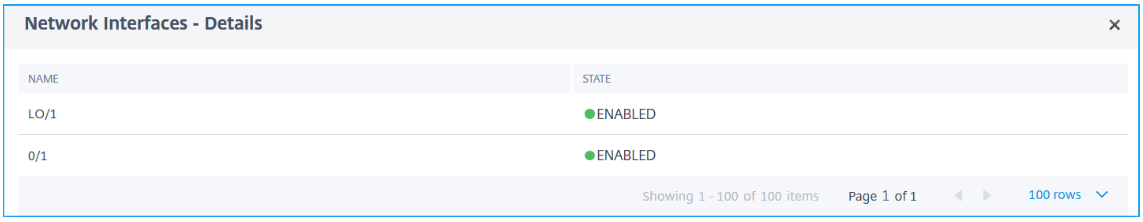
Category	No. of Issues
System Resources	2
Config Deviation	1
SSL Config	1

1 – Indicates the current Citrix ADC 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 current status of the Citrix ADC instance, such as **Up**, **Down**, and **Out of Service**.

3 – Indicates the duration that the Citrix ADC 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).



Network Interfaces - Details

NAME	STATE
LO/1	●ENABLED
0/1	●ENABLED

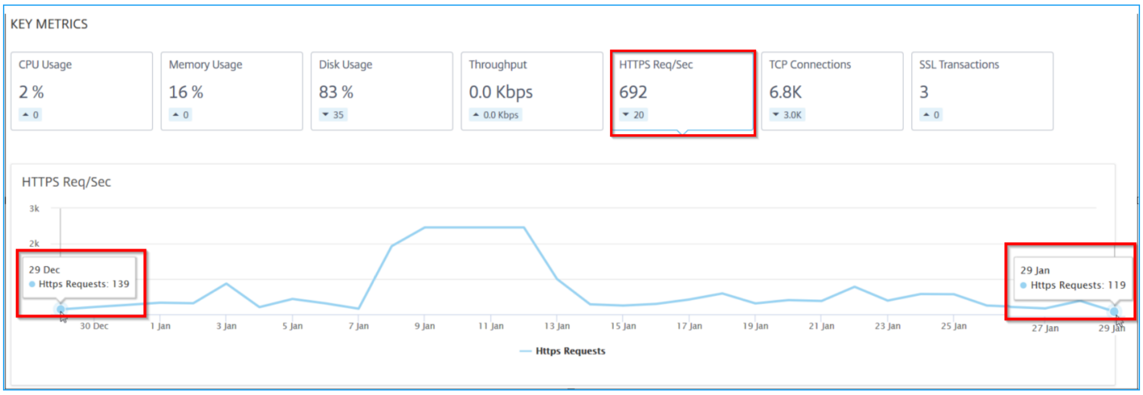
5 – Select the time duration from the list to view the instance details.

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.

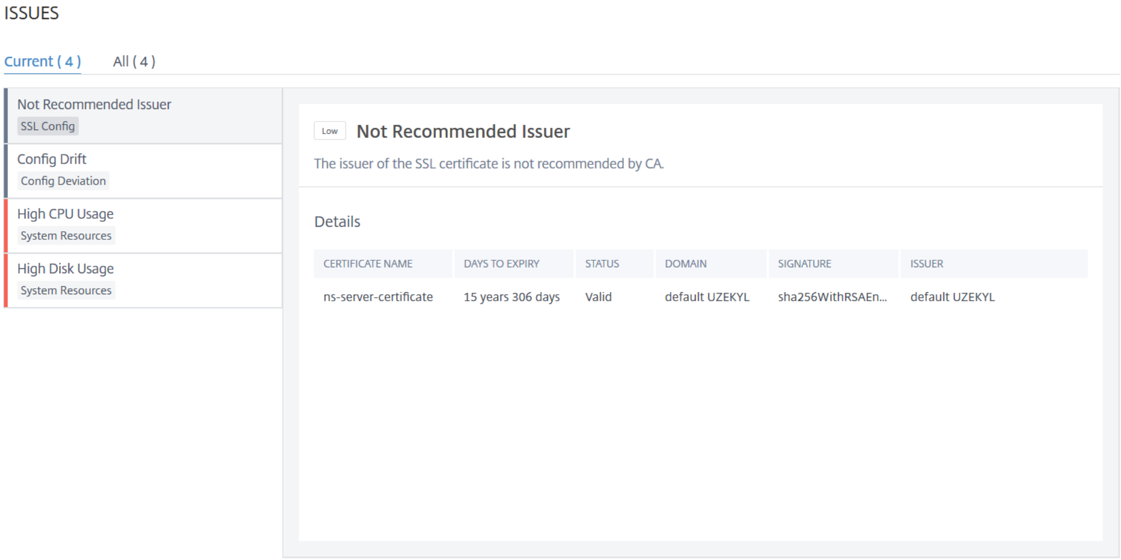
- **Issues**

  You can view the following issues that occur in Citrix ADC instance:

Issue Category	Description	Issues
System Resources	Displays all issues related to the Citrix ADC system resource such as CPU, Memory, disk usage, and so on.	- 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 Citrix ADC instance.	- SSL Certs Expired
		- Not Recommended Issuer
		- Not Recommended Algo
		- Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in Citrix ADC instance.	- Config Drift
		- Running vs Template
Critical events	Displays all critical events related to Citrix ADC instances configured in HA pair and in Cluster.	- Cluster Prop Failure
		- Cluster Sync Failure
		- Cluster versions Mismatch
		- HA Bad Sec State
		- HA No Heat Beats
		- HA Sync Failure

Issue Category	Description	Issues
		- HA Version Mismatch
Capacity issues	Displays ADC capacity issues. The Citrix Application Delivery and Management 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
		- PE CPU Limit Reached
		- PPS Limit Reached
		- SSL Throughput Rate Limit
		- SSL TPS Rate Limit
Networking	Displays the operational issues that occur in the instances.	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:



ISSUES

Current (4) All (4)

- Not Recommended Issuer — SSL Config
- Config Drift — Config Deviation
- High CPU Usage — System Resources
- High Disk Usage — System Resources

Low

Not Recommended Issuer

The issuer of the SSL certificate is not recommended by CA.

Details

CERTIFICATE NAME	DAYS TO EXPIRY	STATUS	DOMAIN	SIGNATURE	ISSUER
ns-server-certificate	15 years 306 days	Valid	default UZEKYL	sha256WithRSAEn...	default UZEKYL

- 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

September 24, 2021

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.

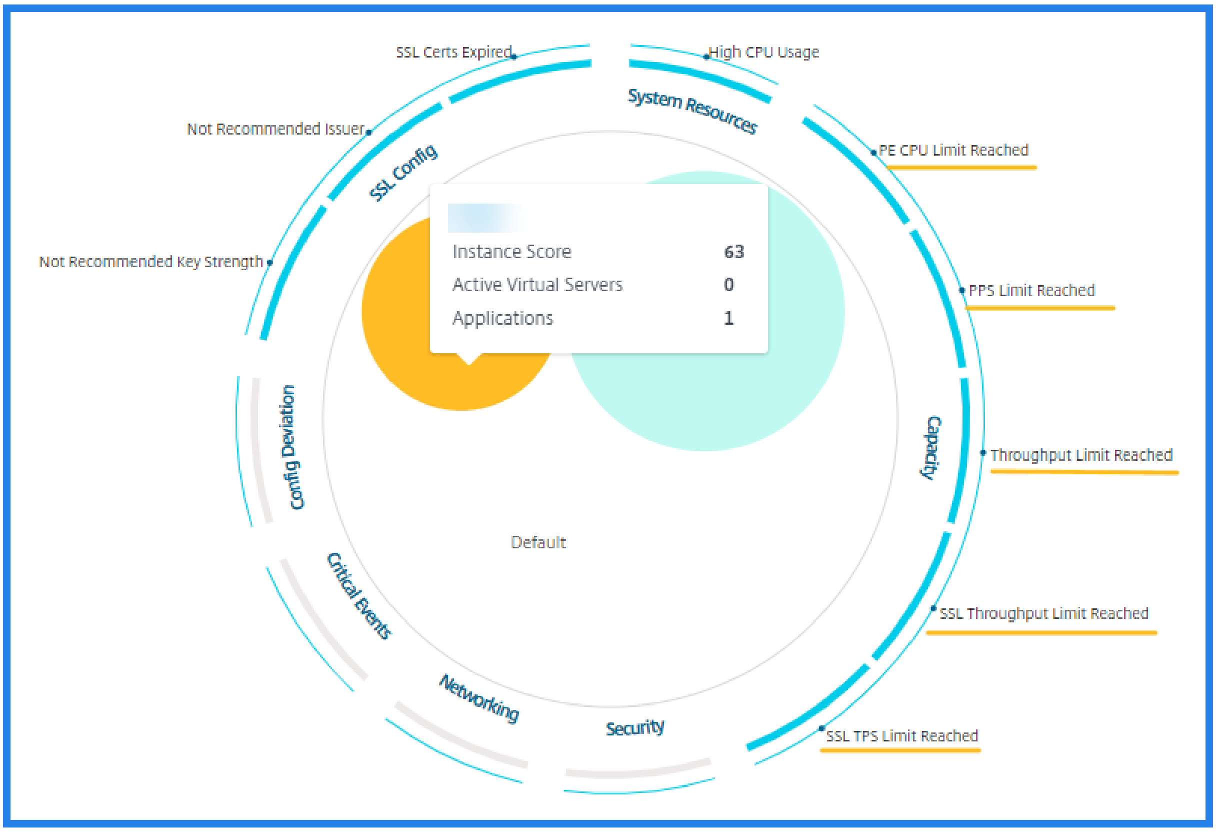
In the **Circle Pack View**, you can view the ADC instance capacity issues if exists.

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:



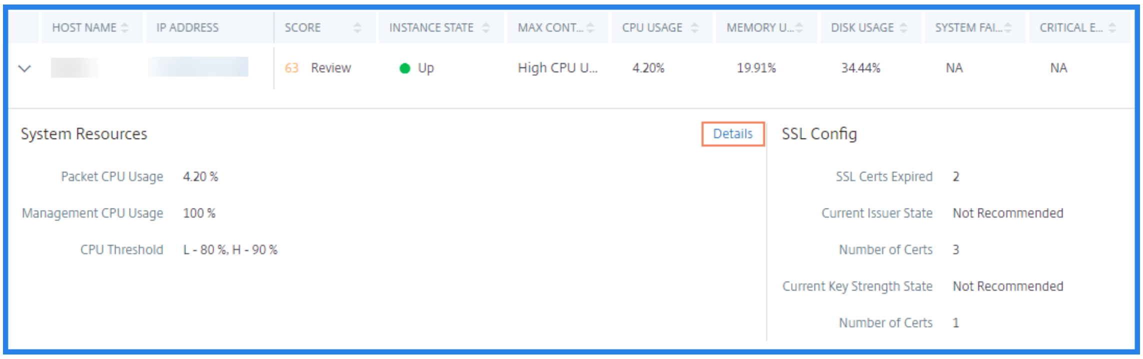
The issues are categorized on the following capacity parameters:

- **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 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 Citrix Application Delivery and Management 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**.



	HOST NAME	IP ADDRESS	SCORE	INSTANCE STATE	MAX CONT...	CPU USAGE	MEMORY U...	DISK USAGE	SYSTEM FAI...	CRITICAL E...
⌄	[redacted]	[redacted]	63 Review	● Up	High CPU U...	4.20%	19.91%	34.44%	NA	NA

System Resources

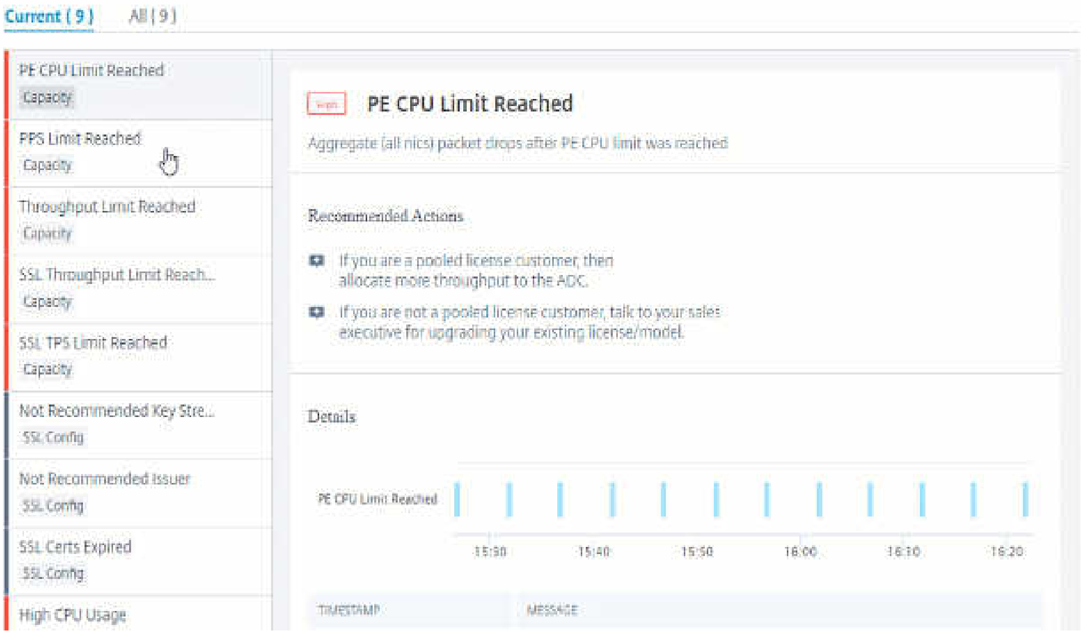
Details

Packet CPU Usage	4.20 %
Management CPU Usage	100 %
CPU Threshold	L - 80 %, H - 90 %

SSL Config

SSL Certs Expired	2
Current Issuer State	Not Recommended
Number of Certs	3
Current Key Strength State	Not Recommended
Number of Certs	1

3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.



PE CPU Limit Reached

Aggregate (all nics) packet drops after PE CPU limit was reached

Recommended Actions

- If you are a pooled license customer, then allocate more throughput to the ADC.
- If you are not a pooled license customer, talk to your sales executive for upgrading your existing license/model.

Details

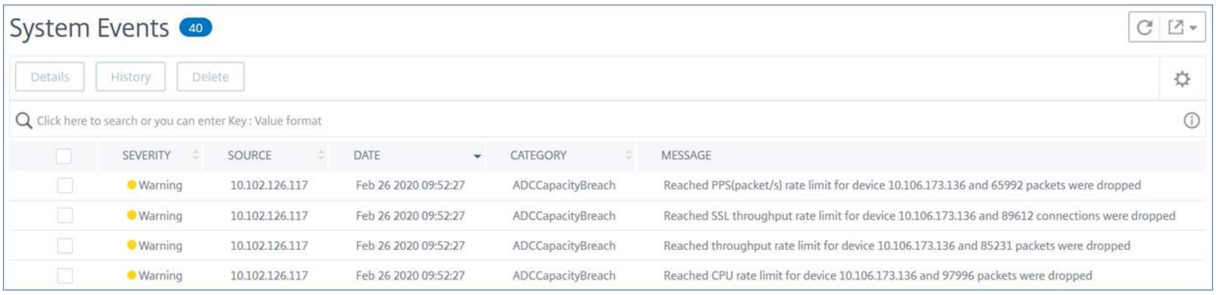
The Citrix Application Delivery and Management polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists.

The Citrix Application Delivery and Management 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 **Settings > Citrix Application Delivery and Management System Events**.



	SEVERITY	SOURCE	DATE	CATEGORY	MESSAGE
□	● Warning	10.102.126.117	Feb 26 2020 09:52:27	ADCCapacityBreach	Reached PPS(packet/s) rate limit for device 10.106.173.136 and 65992 packets were dropped
□	● Warning	10.102.126.117	Feb 26 2020 09:52:27	ADCCapacityBreach	Reached SSL throughput rate limit for device 10.106.173.136 and 89612 connections were dropped
□	● Warning	10.102.126.117	Feb 26 2020 09:52:27	ADCCapacityBreach	Reached throughput rate limit for device 10.106.173.136 and 85231 packets were dropped
□	● Warning	10.102.126.117	Feb 26 2020 09:52:27	ADCCapacityBreach	Reached CPU rate limit for device 10.106.173.136 and 97996 packets were dropped

Enhanced Infrastructure Analytics with new indicators

September 24, 2021

Using the Citrix Application Delivery and Management **Infrastructure Analytics**, you can:

- View a new set of operational issues that occur in Citrix ADC instances.
- View error messages and check recommendations to troubleshoot the issues.

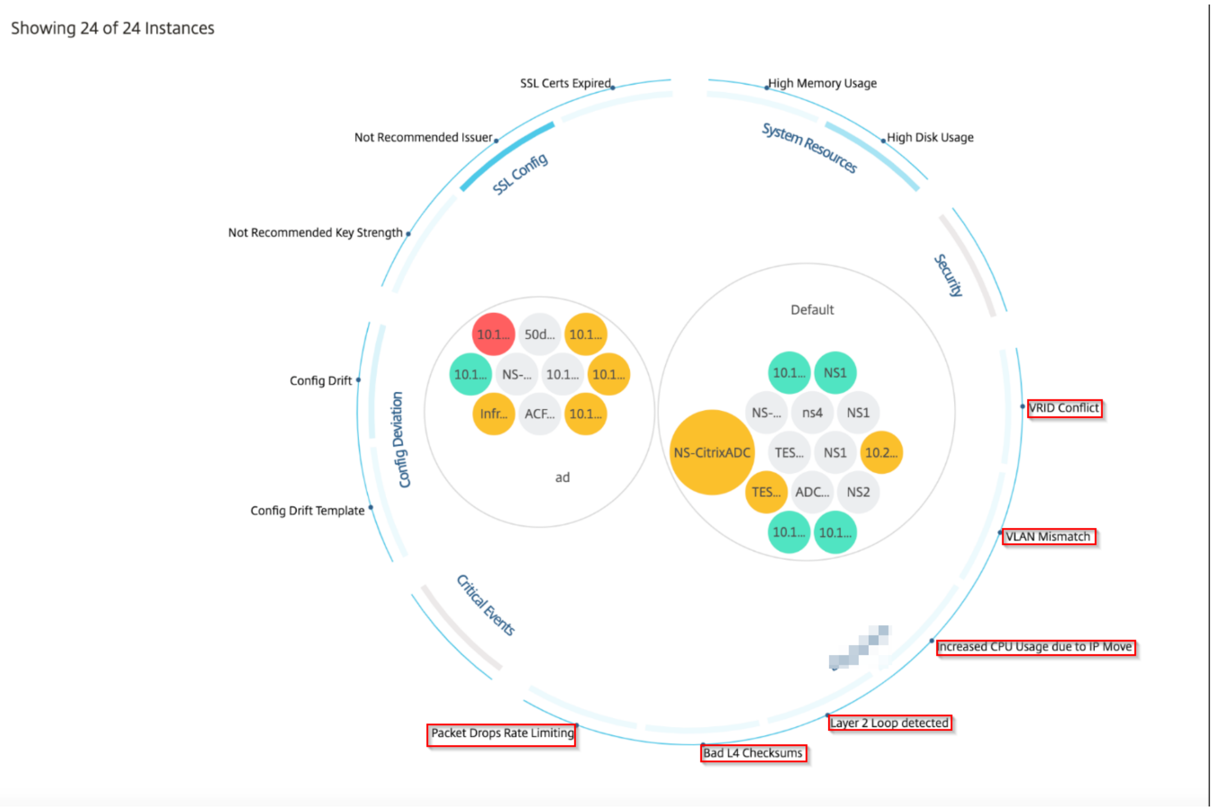
As an administrator, you can quickly identify the root cause analysis of issues.

> **Note**
>
> Rule indicators are not supported for:
>
> - Citrix ADC instances configured in a cluster mode.
> - Citrix ADC instances configured with admin partitions.

In Citrix Application Delivery and Management, navigate to **Infrastructure > Infrastructure Analytics** to view indicators for:

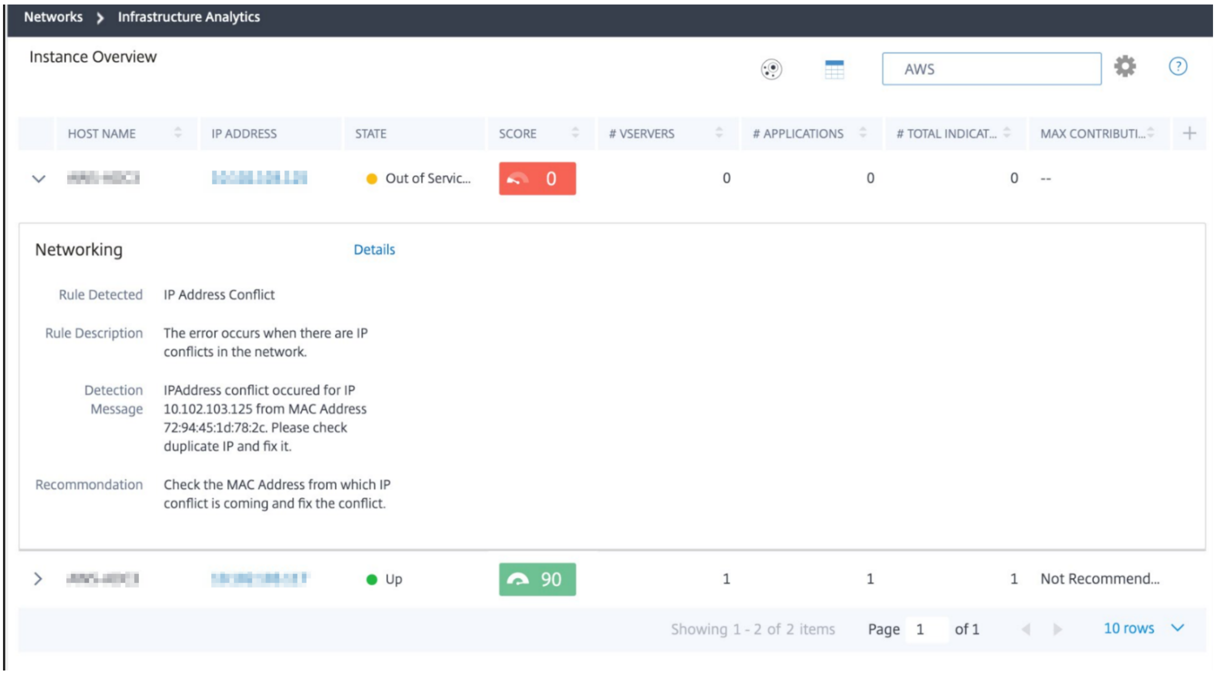
Indicator name in Infrastructure Analytics	Description
Port allocation failure	Detects when Citrix ADC uses SNIP to communicate with a new server connection and total ports available on that SNIP are exhausted. The recommended action is to add another SNIP in the same subnet.
Session Buildup	Detects when Citrix ADC memory is held up by SSL sessions.
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.

Indicator name in Infrastructure Analytics	Description
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.
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 Citrix ADC 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.



Networks > Infrastructure Analytics

Instance Overview

AWS

	HOST NAME	IP ADDRESS	STATE	SCORE	# VSERVERS	# APPLICATIONS	# TOTAL INDICAT...	MAX CONTRIBUTI...
⌄	[redacted]	[redacted]	● Out of Servic...	0	0	0	0	--

Networking

Details

Rule Detected: IP Address Conflict

Rule Description: The error occurs when there are IP conflicts in the network.

Detection Message: IPAddress conflict occured for IP 10.102.103.125 from MAC Address 72:94:45:1d:78:2c. Please check duplicate IP and fix it.

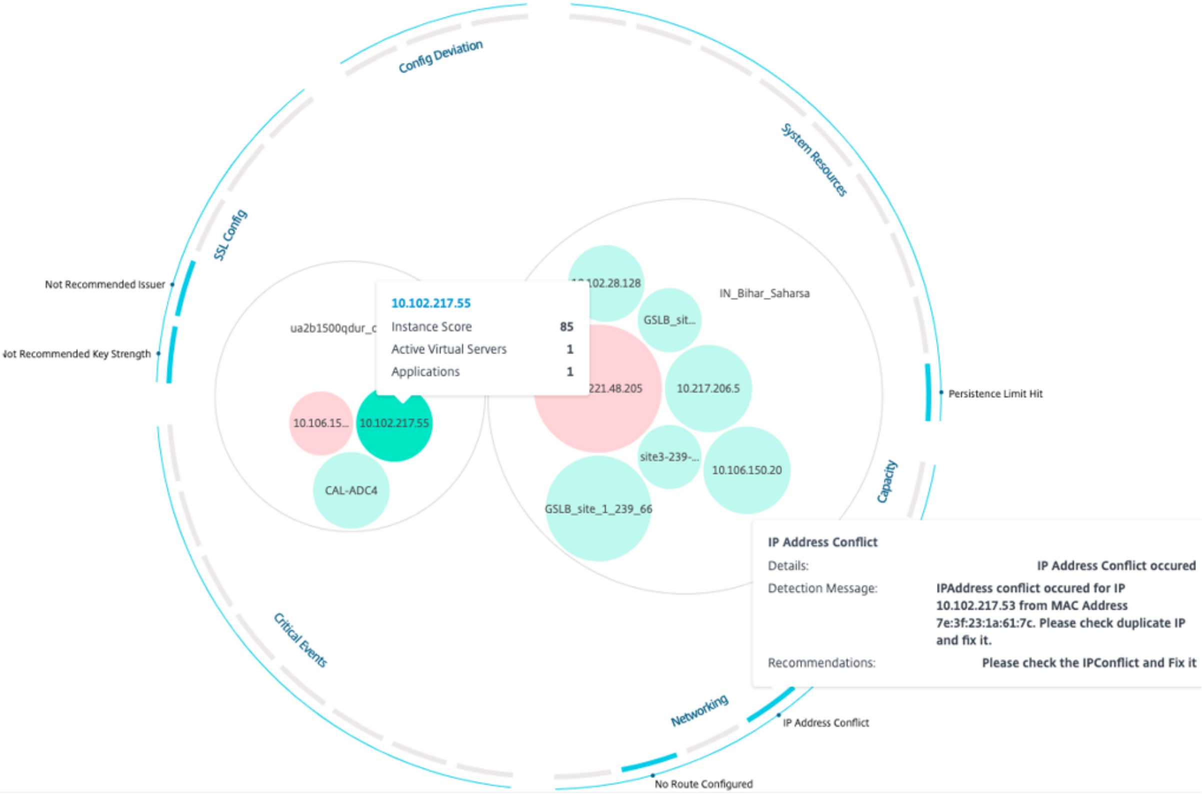
Recommondation: Check the MAC Address from which IP conflict is coming and fix the conflict.

	HOST NAME	IP ADDRESS	STATE	SCORE	# VSERVERS	# APPLICATIONS	# TOTAL INDICAT...	MAX CONTRIBUTI...
>	[redacted]	[redacted]	● Up	90	1	1	1	Not Recommend...

Showing 1 - 2 of 2 items Page 1 of 1 10 rows

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.



10.102.217.55

Instance Score	85
Active Virtual Servers	1
Applications	1

IP Address Conflict

Details: IP Address Conflict occured

Detection Message: IPAddress conflict occured for IP 10.102.217.53 from MAC Address 7e:3f:23:1a:61:7c. Please check duplicate IP and fix it.

Recommendations: Please check the IPConflict and Fix it

- **Details** - Indicates what anomaly is detected
- **Detection Message** - Indicates the MAC address for which the IP address has the conflict
- **Recommendations** - Indicates the troubleshooting procedure to resolve this IP address conflict

Instance management

September 25, 2021

Instances are Citrix Application Delivery Controller (ADC) appliances that you can manage, monitor, and troubleshoot using Citrix Application Delivery and Management. Add instances to Citrix Application Delivery and Management to monitor them. Instances can be added when you set up Citrix Application Delivery and Management or later as well. After you add instances to Citrix Application Delivery and Management, 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 others. A private IP-block groups your instances based on their geographical locations.

Add an instance

You can add instances either while setting up the Citrix Application Delivery and Management server for the first time or later. To add instances, you must specify either the host name or IP address of each Citrix ADC instance, or a range of IP addresses.

To learn how to add an instance to Citrix Application Delivery and Management, see Add Instances to Citrix Application Delivery and Management.

When you add an instance to the Citrix Application Delivery and Management server, the server implicitly adds itself as a trap destination for the instance and collects an inventory of the instance. To learn more, see How Citrix Application Delivery and Management discovers instances.

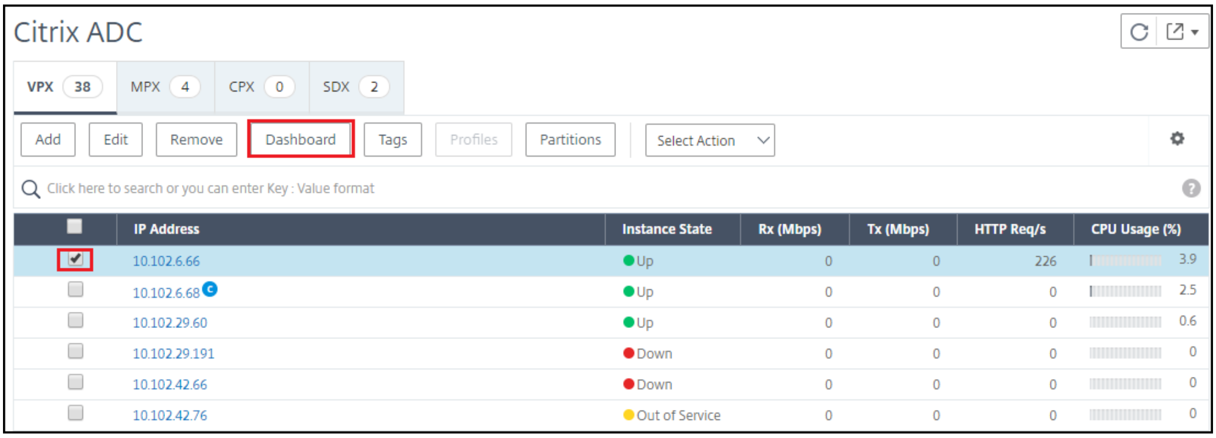
After you've added an instance, you can delete it by navigating to **Infrastructure > Instances** and select the instance category. Then, select the instance you want to delete and click **Remove**.

How to use the instance dashboard

The per-instance dashboard in Citrix Application Delivery and Management 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.

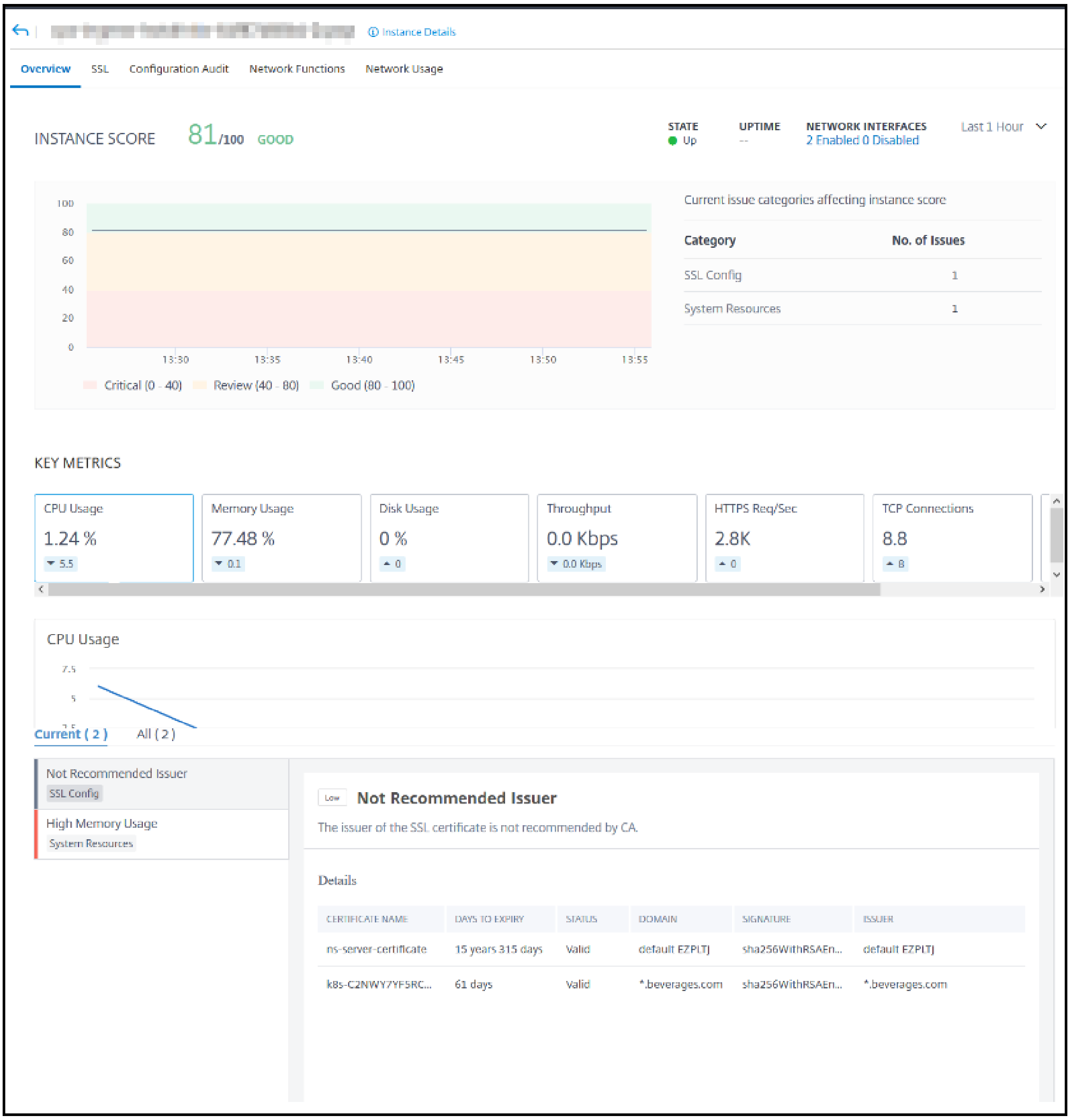
By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.

To view a specific instance's dashboard, navigate to **Infrastructure > Instances > Citrix ADC**. On the Citrix ADC page, choose the instance type and then, select the instance you want to view and click **Dashboard**.



□	IP Address	Instance State	Rx (Mbps)	Tx (Mbps)	HTTP Req/s	CPU Usage (%)
☑	10.102.6.66	● Up	0	0	226	3.9
□	10.102.6.68	● Up	0	0	0	2.5
□	10.102.29.60	● Up	0	0	0	0.6
□	10.102.29.191	● Down	0	0	0	0
□	10.102.42.66	● Down	0	0	0	0
□	10.102.42.76	● Out of Service	0	0	0	0

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:



INSTANCE SCORE 81/100 GOOD

STATE: Up
UPTIME: --
NETWORK INTERFACES: 2 Enabled 0 Disabled

Current issue categories affecting instance score

Category	No. of Issues
SSL Config	1
System Resources	1

KEY METRICS

CPU Usage	Memory Usage	Disk Usage	Throughput	HTTPS Req/Sec	TCP Connections
1.24 %	77.48 %	0 %	0.0 Kbps	2.8K	8.8
▼ 5.5	▼ 0.1	▲ 0	▼ 0.0 Kbps	▲ 0	▲ 8

Not Recommended Issuer
SSL Config

High Memory Usage
System Resources

Low **Not Recommended Issuer**

The issuer of the SSL certificate is not recommended by CA.

Details

CERTIFICATE NAME	DAYS TO EXPIRY	STATUS	DOMAIN	SIGNATURE	ISSUER
ns-server-certificate	15 years 315 days	Valid	default EZPLTJ	sha256WithRSAEn...	default EZPLTJ
k8s-C2NWY7YF5RC...	61 days	Valid	*.beverages.com	sha256WithRSAEn...	*.beverages.com

- **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 others are 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 **Citrix ADC config saved status** and **Citrix ADC 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 Citrix ADC 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 another performance report.

How to monitor globally distributed sites

September 25, 2021

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 Citrix Application Delivery and Management 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 sections explain how you can monitor data centers in Citrix Application Delivery and Management.

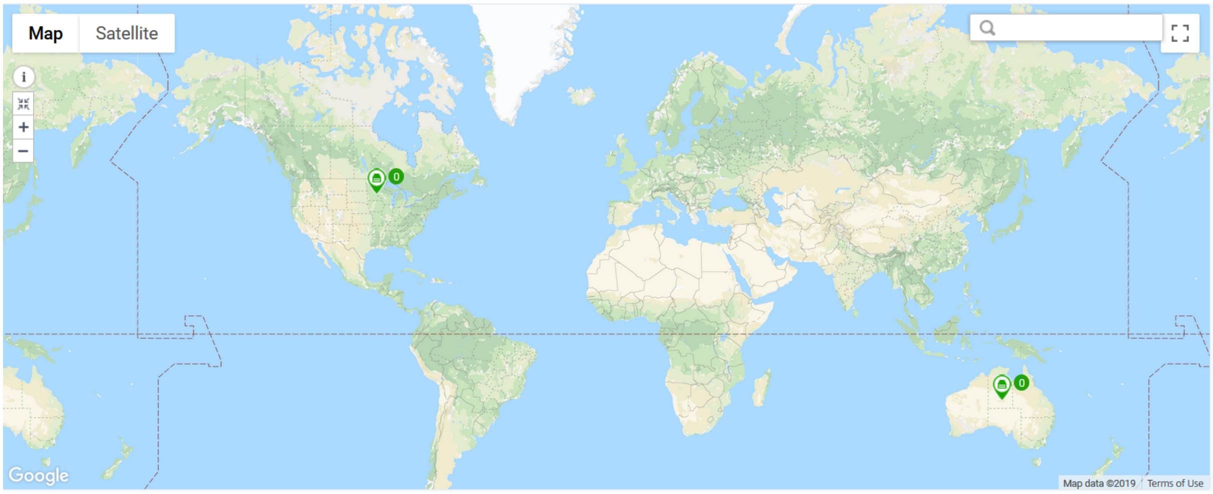
Monitoring globally distributed sites in Citrix Application Delivery and Management

Citrix Application Delivery and Management site is a logical grouping of Citrix Application Delivery Controller (Citrix 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. Citrix Application Delivery and Management manages and monitors all Citrix ADC instances connected to all sites. You can use Citrix Application Delivery and Management to monitor and collect syslog, AppFlow, SNMP, and any such data originating from the managed instances.

Geomaps in Citrix Application Delivery and Management 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 click **Infrastructure** on the menu and this displays the **Instances Dashboard** for a visual representation of the sites created on the world map.

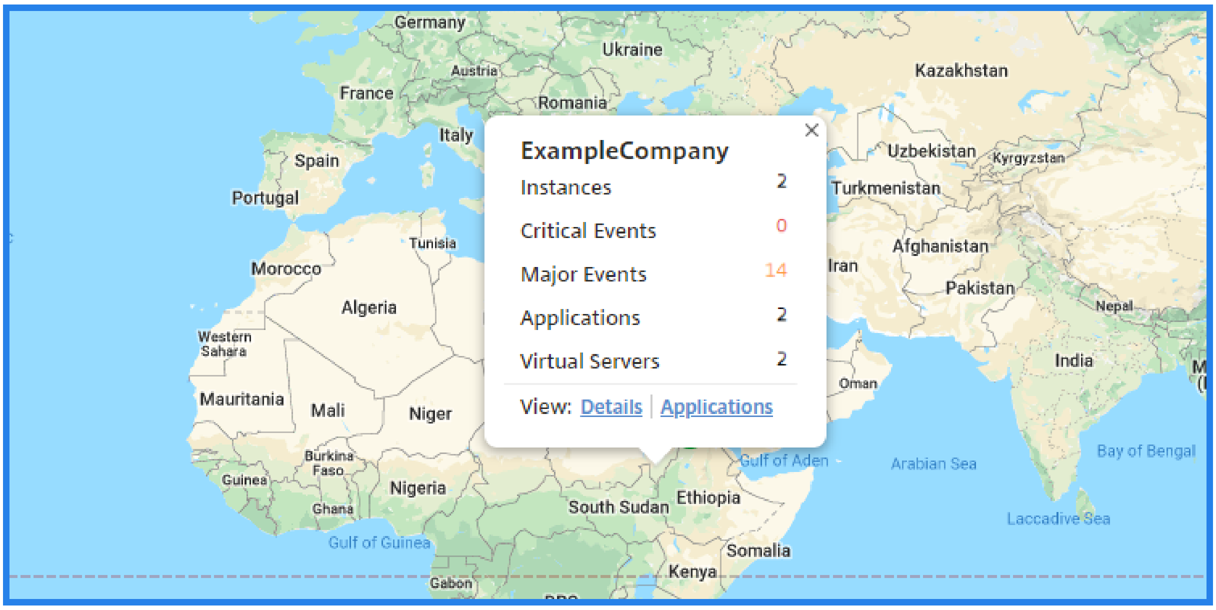
Use case

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 the count of the following components on the site:

- **Instances**: Indicates the number of instances available.
- **Applications**: Indicates the number of applications hosted.
- **Virtual Servers**: Indicates the number of virtual servers available.
- **Critical Events**: Indicates the count of critical events occurred on the instances.
- **Major Events**: Indicates the count of major events occurred on the instances.



ExampleCompany

Instances 2

Critical Events 0

Major Events 14

Applications 2

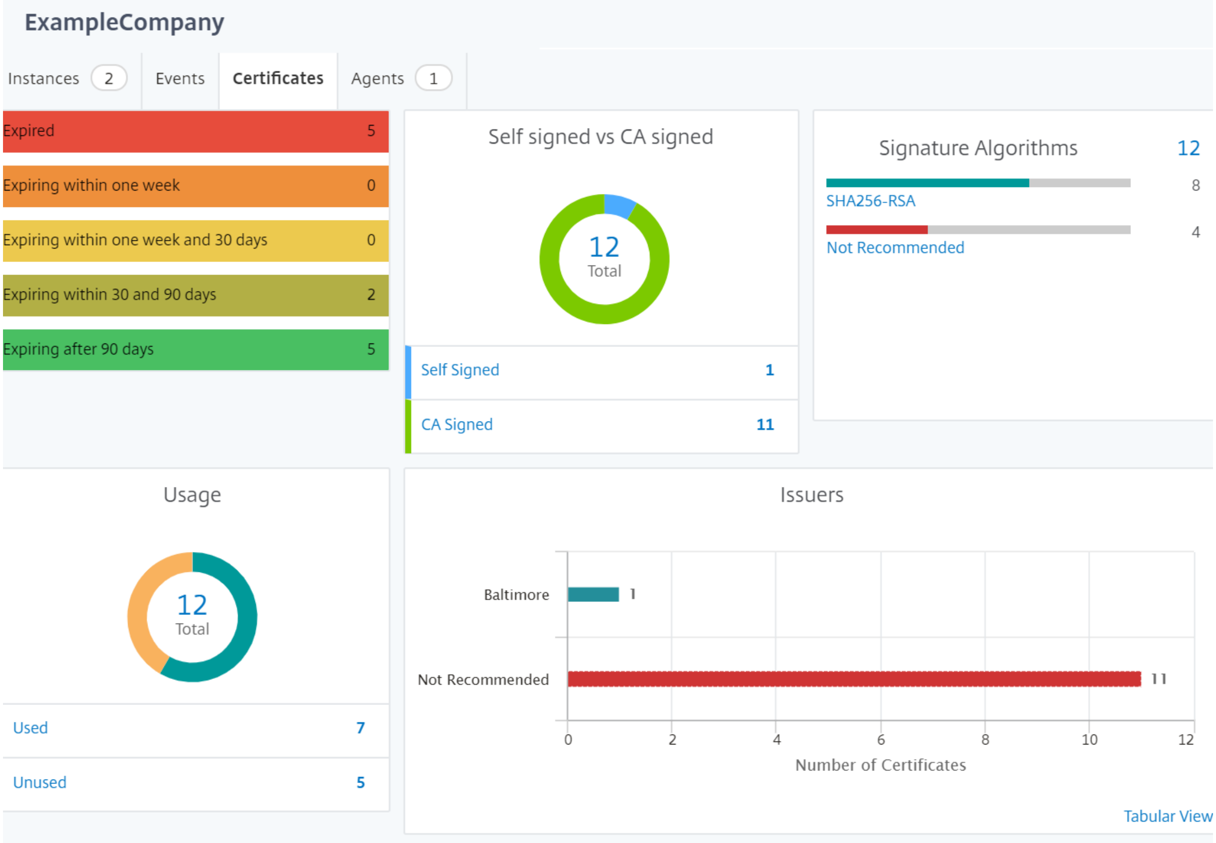
Virtual Servers 2

View: Details | Applications

Click **Applications** to see all custom applications created in each site.

Click **Details** to see a list of Citrix ADC instances added in 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 Citrix ADC instance
  - Number of critical events
  - Significant events and all events raised on a Citrix ADC 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.



ExampleCompany

Instances 2 | Events | Certificates | Agents 1

Expired 5
Expiring within one week 0
Expiring within one week and 30 days 0
Expiring within 30 and 90 days 2
Expiring after 90 days 5

Self signed vs CA signed

12 Total

Self Signed 1
CA Signed 11

Signature Algorithms 12

SHA256-RSA 8
Not Recommended 4

Usage

12 Total

Used 7
Unused 5

Issuers

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 Citrix ADC instances in Citrix Application Delivery and Management. You must also add the instance to the site, add an agent, and bind the agent to the site. Citrix Application Delivery and Management then recognizes the site that the Citrix ADC instance and the agent belong.

For more information on adding Citrix ADC instances, see Adding Instances.

To create sites:

Create sites before you add instances in Citrix Application Delivery and Management. Providing location information allows you to locate the site precisely.

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Sites** , and click **Add**.
2. On the **Create Site** page, update the following information, and click **Create**.
    a) **Site Type**. Select **Data Center**.

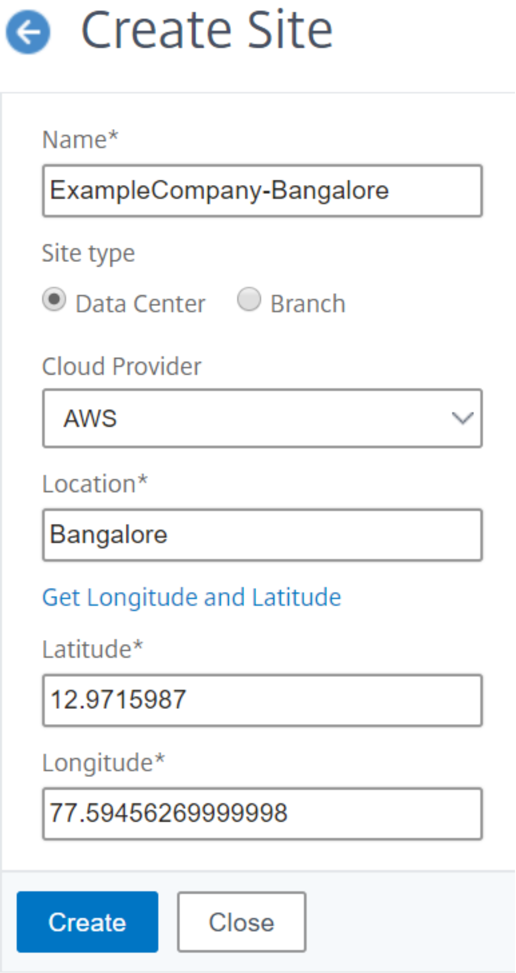
> **Note**
>
> The site can function as the primary data center or as a branch. Choose accordingly.

a) **Type**. Select AWS as the cloud provider from the list.

> **Note**
>
> Check the **Use existing VPC as a site** box accordingly.

b) **Site Name**. Type the name of the site.

c) **Search Location**. Type the name of the city. Click **Get Location** to place the site precisely at the location.
The City, Zip code, Region, Country, Latitude, and Longitude fields are filled in automatically.



Create Site

Name*: ExampleCompany-Bangalore

Site type: ● Data Center ○ Branch

Cloud Provider: AWS

Location*: Bangalore

Latitude*: 12.9715987

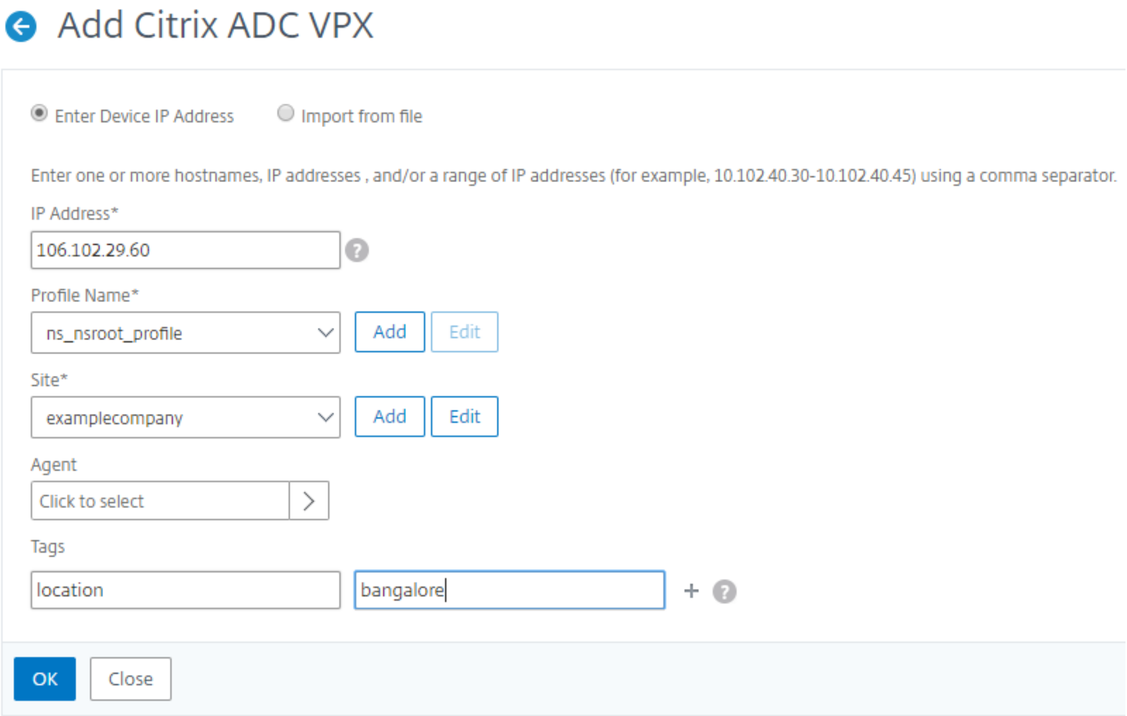
Longitude*: 77.59456269999998

d) Click **Create** to create a site in Bangalore.

To add instances and select sites:

After creating sites, you must add instances in Citrix Application Delivery and Management. You can select the previously created site, or you can also create a site and associate the instance.

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Citrix ADC**.
2. Select the **VPX**, and click **Add**.
3. On the **Add Citrix ADC VPX** page, type the IP address and select the profile from the list.
4. Select the site from the list. You can click the **Add** button next to **Site** field to create a site or click the **Edit** button to change the details of the default site.
5. Click the right arrow and select the agent from the list that displays.



Add Citrix ADC VPX

● Enter Device IP Address ○ Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

IP Address*: 106.102.29.60

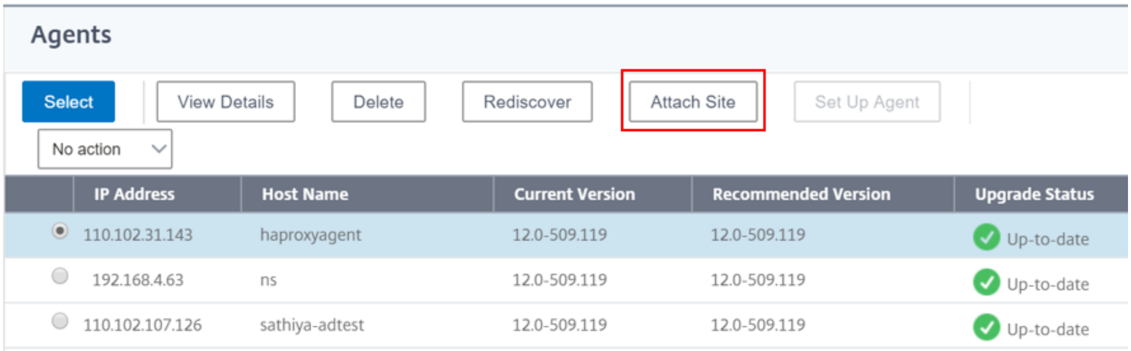
Profile Name*: ns_nsroot_profile

Site*: examplecompany

Agent: Click to select

Tags: location bangalore

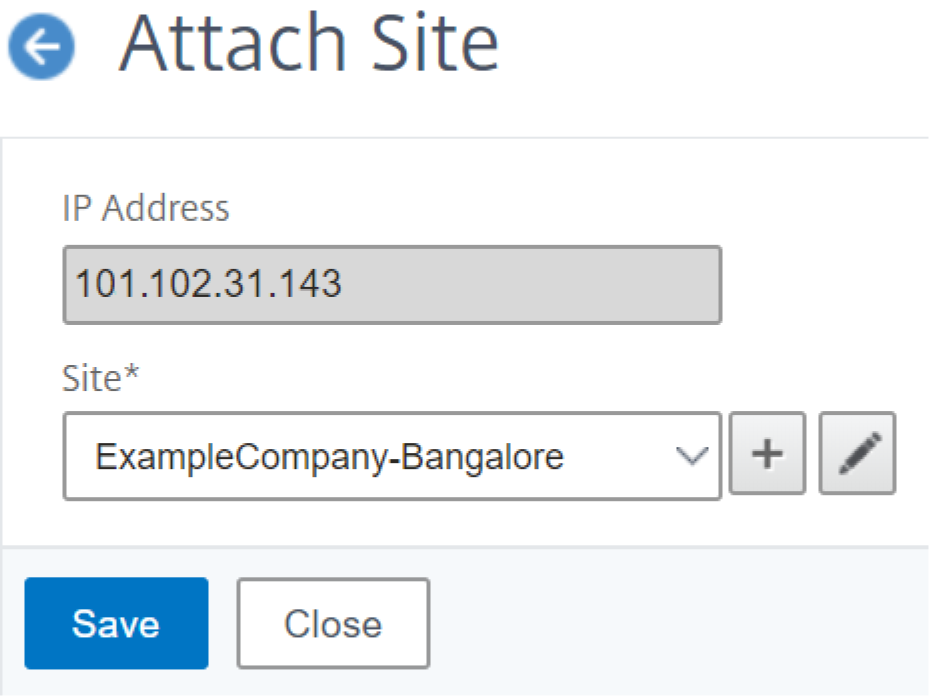
6. After choosing the agent, you must associate the agent with the site. This step allows the agent to be bound to the site. Select the agent and click **Attach Site**.



Agents

	IP Address	Host Name	Current Version	Recommended Version	Upgrade Status
●	110.102.31.143	haproxyagent	12.0-509.119	12.0-509.119	✓ Up-to-date
○	192.168.4.63	ns	12.0-509.119	12.0-509.119	✓ Up-to-date
○	110.102.107.126	sathiya-adtest	12.0-509.119	12.0-509.119	✓ Up-to-date

a) Select the site from the list and click **Save**.



Attach Site

IP Address

101.102.31.143

Site*

ExampleCompany-Bangalore

7. Optionally, you can enter key and value fields for **Tags**.
8. Click **OK**.

You can also attach an agent to a site by navigating to **Infrastructure > Instances > Agents**.

To associate a Citrix Application Delivery and Management agent with the site:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent, and click **Attach Site**.
3. You can associate the site and click **Save**.

Citrix Application Delivery and Management starts monitoring the Citrix ADC instances added in the Bangalore site along with the instances at the other two sites as well.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon in the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

How to create tags and assign to instances

September 25, 2021

Citrix Application Delivery and Management now allows you to associate your Citrix 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 will help you to better monitor them.

- **Use case 1**: You can create a tag to identify all instances that are located 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 that are located 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 a 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 Citrix ADC instances that are located in the 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 Citrix ADC VPX instance:

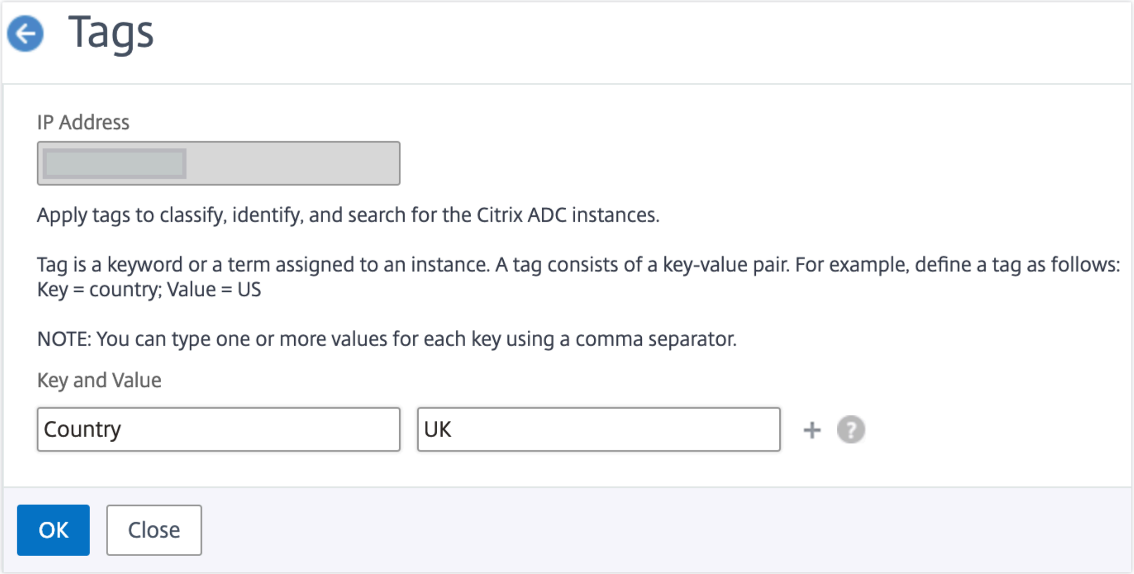
1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Citrix ADC**.

2. Select the **VPX** tab.

3. Select the required VPX instance.

4. Click **Tags**. 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.



Tags

IP Address

[redacted]

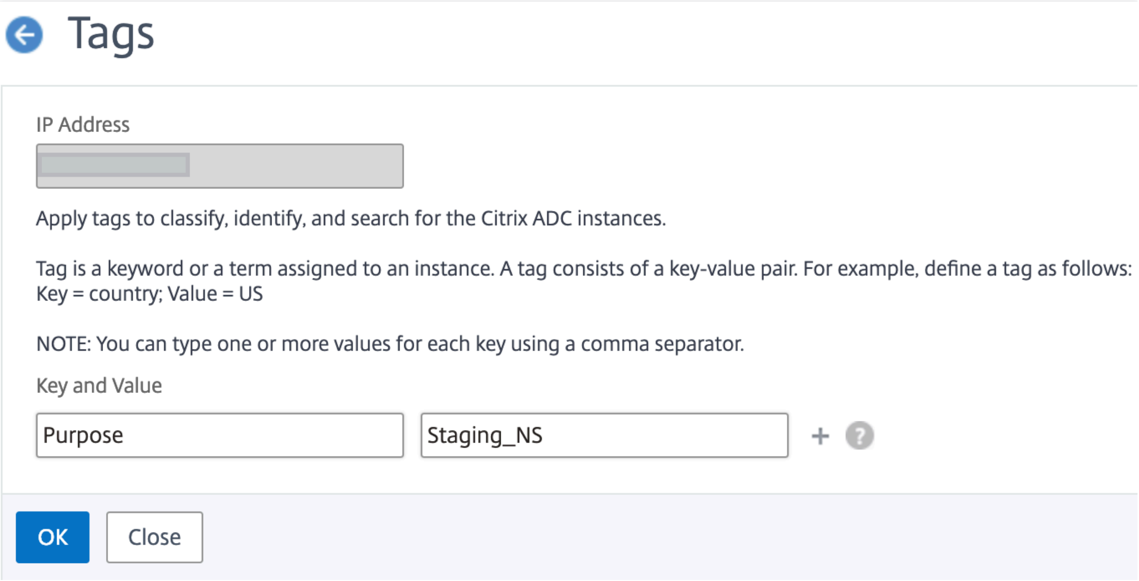
Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows: Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country | UK



Tags

IP Address

[redacted]

Apply tags to classify, identify, and search for the Citrix ADC instances.

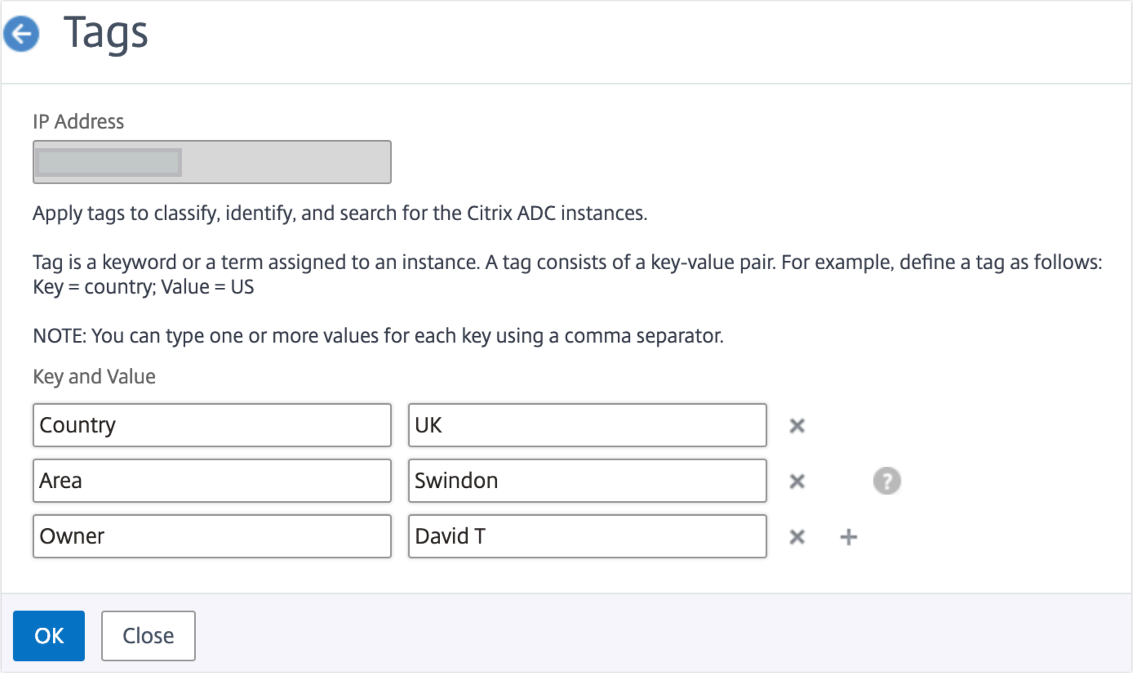
Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows: Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Purpose | Staging_NS

You can also add multiple tags by clicking "+". Adding multiple and meaningful tags allows you to efficiently search for the instances.



Tags

IP Address

[redacted]

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows: Key = country; Value = US

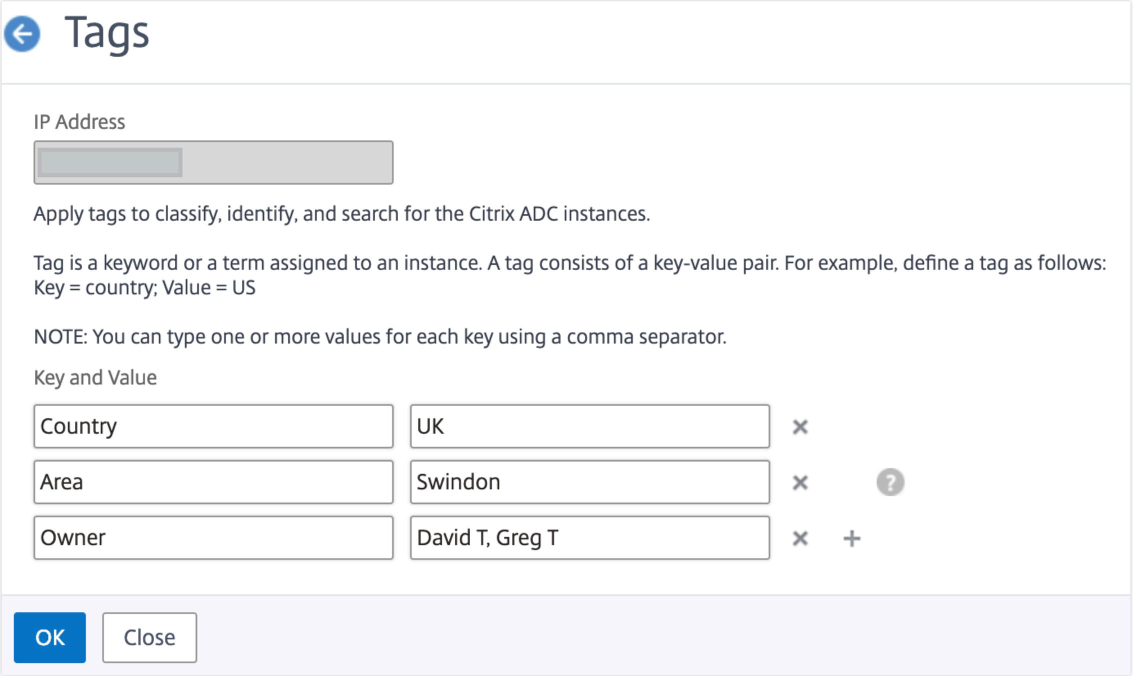
NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country	UK
Area	Swindon
Owner	David T

You can add multiple values to a keyword by separating them with commas.

For example, you are assigning the 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. Citrix Application Delivery and Management recognizes the comma separated values into two different values.



Tags

IP Address

[redacted]

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows: Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country	UK
Area	Swindon
Owner	David T, Greg T

To know more about how to search for instances based on tags, see How to search instances using values of tags and properties.

5. Click **OK**.

> **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

September 25, 2021

There might be a situation where Citrix Application Delivery and Management is managing many Citrix ADC instances. As an admin, you might want the flexibility to search on the instance inventory based on certain parameters. Citrix Application Delivery and Management now offers improved search capability to search a subset of Citrix ADC 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 can be assigned by you to a Citrix ADC instance to add some additional description about the Citrix ADC instance. You can now associate your Citrix ADC instances with tags. These tags can be used to better identify and search on the Citrix ADC instances.
- **Properties**. Each Citrix ADC instance added in Citrix Application Delivery and Management 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 Citrix ADC 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.

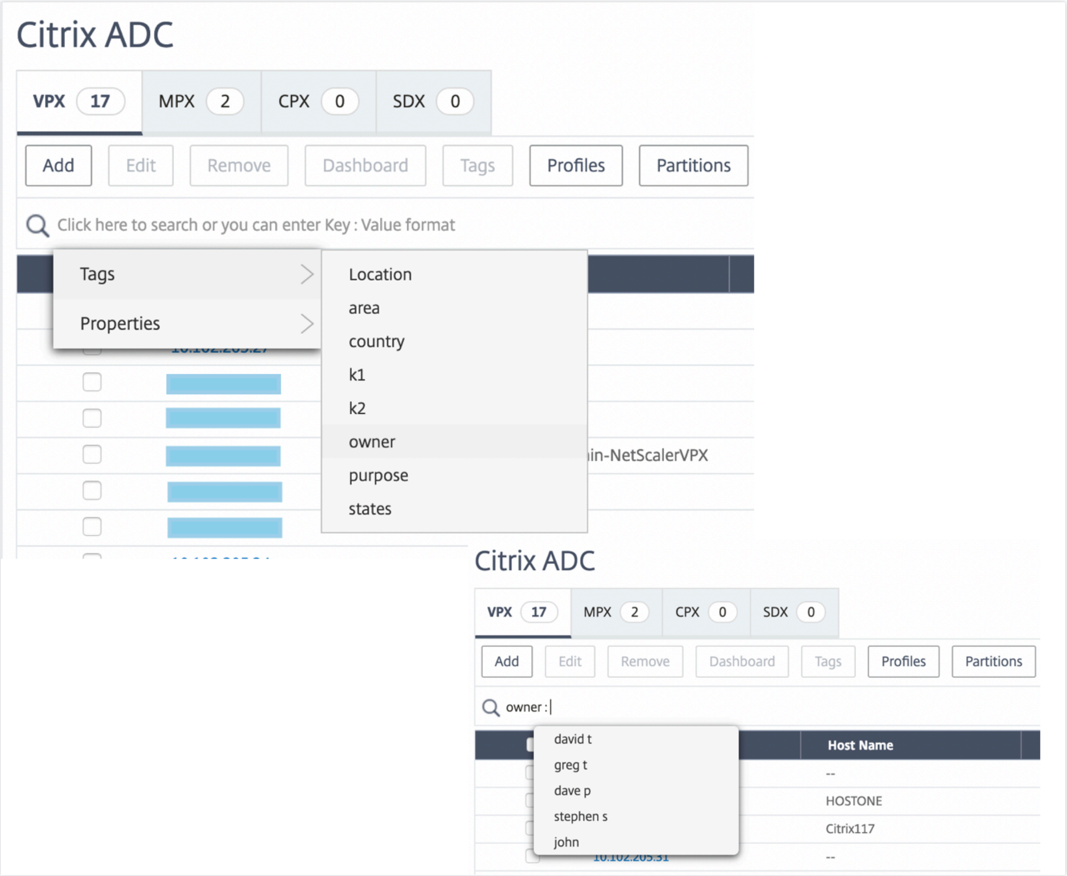
To search for Citrix ADC VPX instances

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Citrix ADC**.
2. Select the **VPX** tab.

3. Click the search field. You can create a search expression by using Tags or Properties or by combining both.

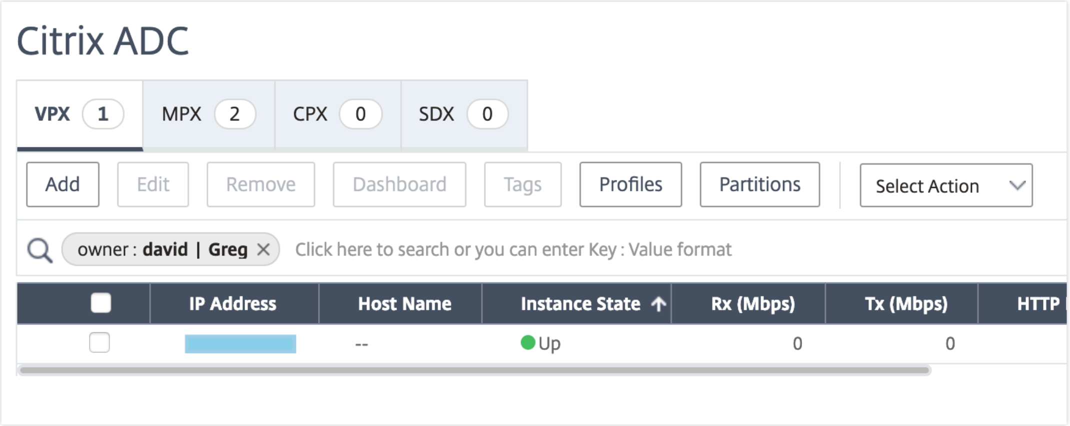
   The following examples show how you can use the search expression efficiently to search for the instance.

   a) Select **Tags** option and select **Owner**. Select "David T".



   Citrix Application Delivery and Management supports regular expressions and wildcard characters in the search expressions.

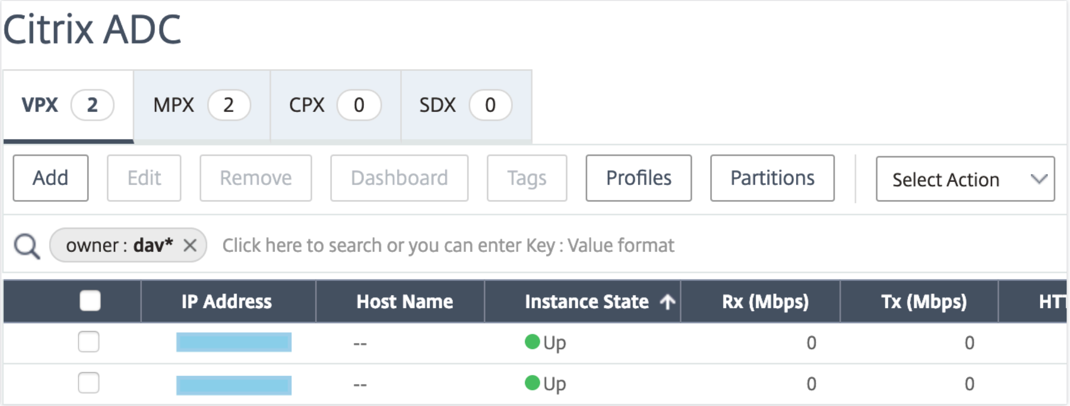
   a) You can use regular expressions to further expand the search criteria. For example, you want to search instances owned by either David or Stephen. In such a case, you can type the values by separating the values with a "|" expression.



owner : **david | Greg** × Click here to search or you can enter Key : Value format

□	IP Address	Host Name	Instance State	Rx (Mbps)	Tx (Mbps)	HTTP
□	[redacted]	--	● Up	0	0	

b) 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" and "Dave P".



owner : **dav*** × Click here to search or you can enter Key : Value format

□	IP Address	Host Name	Instance State	Rx (Mbps)	Tx (Mbps)	HT
□	[redacted]	--	● Up	0	0	
□	[redacted]	--	● Up	0	0	

> **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 Citrix ADC instances

October 20, 2021

You can configure admin partitions on your Citrix Application Delivery Controller (Citrix ADC) instances so that different groups in your organization are assigned different partitions on the same Citrix ADC instance. You can assign a network administrator to manage multiple partitions on multiple Citrix ADC instances.

Citrix Application Delivery and Management 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. For more information about creating a group or user, see Create a user and Create a group.

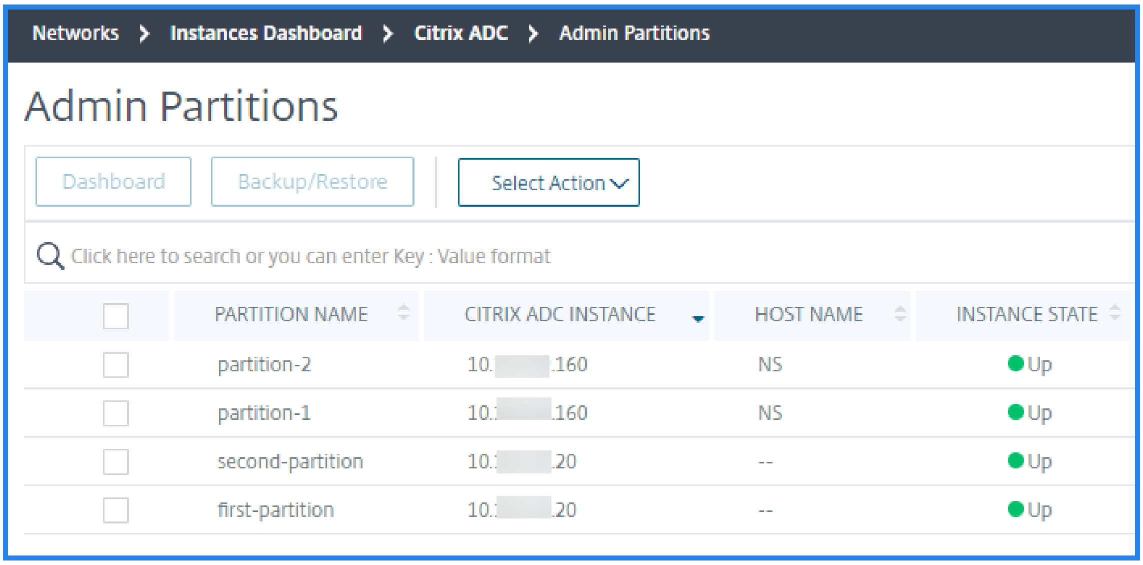
A user can view and manage only the partitions in the group to which the user belongs. When you discover a Citrix ADC instance, the admin partitions configured on that Citrix ADC instance get added to the system automatically. Each admin partition is considered as an instance in Citrix Application Delivery and Management.

View admin partitions

Consider that you have two Citrix ADC VPX instances and two admin partitions are configured on each instance. For example, Citrix ADC instance 10.xx.xx.160 has partition-1 and partition-2 and the 10.xx.xx.20 instance has first-partition and second-partition.

Perform the following steps to view admin partitions:

1. Navigate to **Infrastructure > Instances > Citrix ADC**.
2. In the **VPX** tab, click **Partitions**.

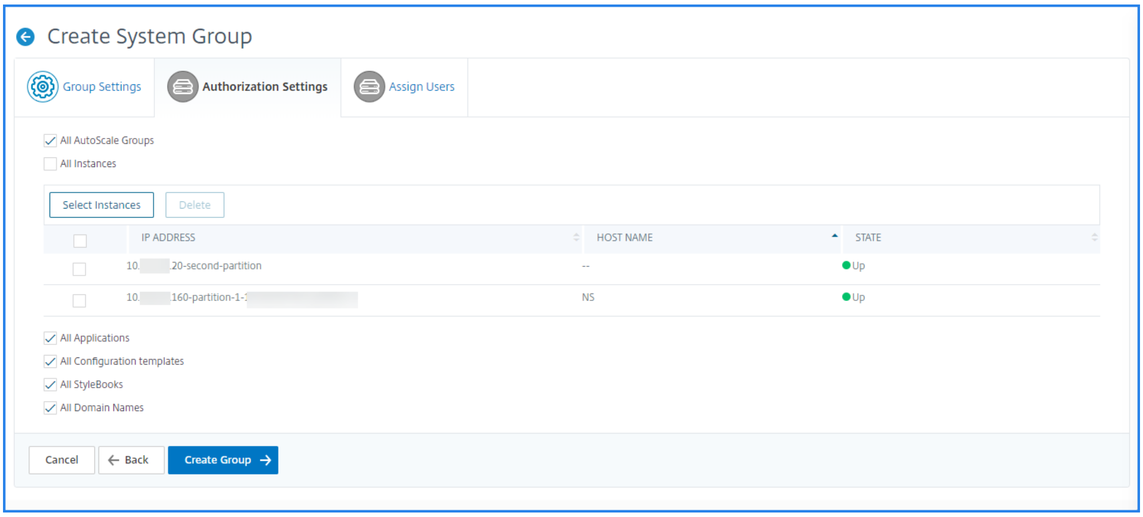


Networks > Instances Dashboard > Citrix ADC > Admin Partitions
Admin Partitions
Dashboard
Backup/Restore
Select Action
Click here to search or you can enter Key : Value format

□	PARTITION NAME	CITRIX ADC INSTANCE	HOST NAME	INSTANCE STATE
□	partition-2	10.[redacted].160	NS	● Up
□	partition-1	10.[redacted].160	NS	● Up
□	second-partition	10.[redacted].20	--	● Up
□	first-partition	10.[redacted].20	--	● Up

For example, when you create a group with the following conditions:

- In the **Authorization Settings** tab, the "10.xx.xx.20-second-partition" and "10.xx.xx.160-partition-1" instances are selected.



Create System Group

☑ All AutoScale Groups

□ All Instances

□	IP ADDRESS	HOST NAME	STATE
□	10.[redacted].20-second-partition	--	● Up
□	10.[redacted].160-partition-1-[redacted]	NS	● Up

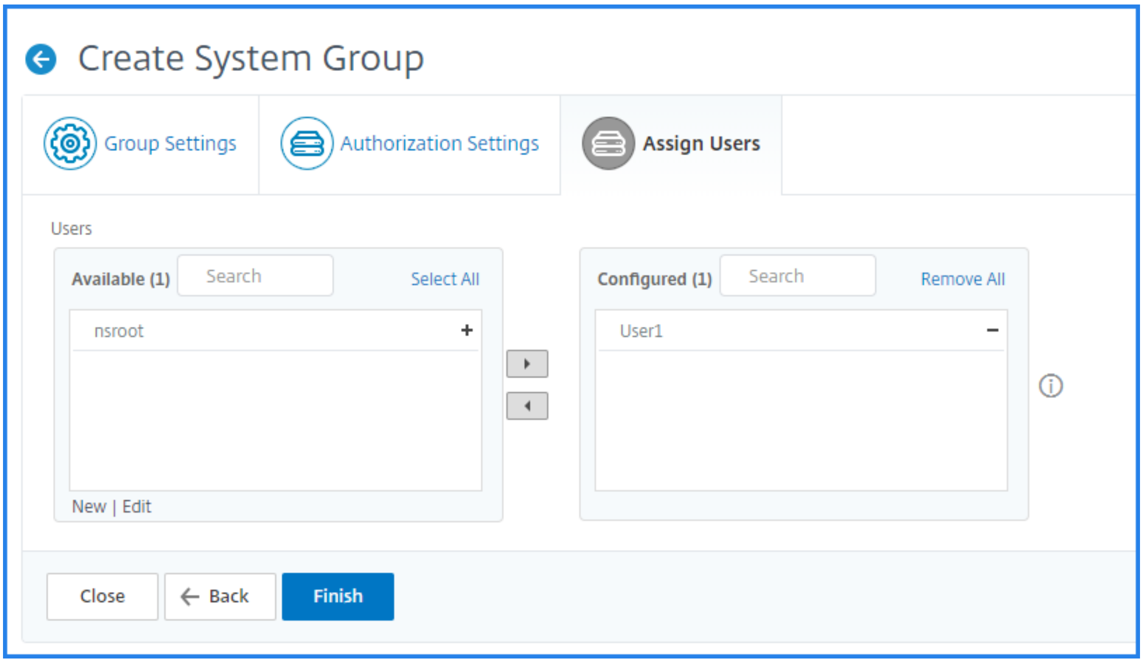
☑ All Applications

☑ All Configuration templates

☑ All StyleBooks

☑ All Domain Names

- "User1" is assigned to the group.



Create System Group

User1 can view and manage only those partitions that are added to the group. However, the partitions that are not added to the group are restricted to the user even though they belong to the same instances.

In this example, 10.xx.xx.20-first-partition and 10.xx.xx.160-partition-2 are restricted. Because the instances are not added to the group where the user is assigned.

If you want a different user to manage the admin partitions 10.xx.xx.20-first-partition and 10.xx.xx.160-partition-2, create a group with the following conditions:

- In the **Authorization Settings** tab, select the 10.xx.xx.20-first-partition and 10.xx.xx.160-partition-2 instances.

- Assign the required user to the group.

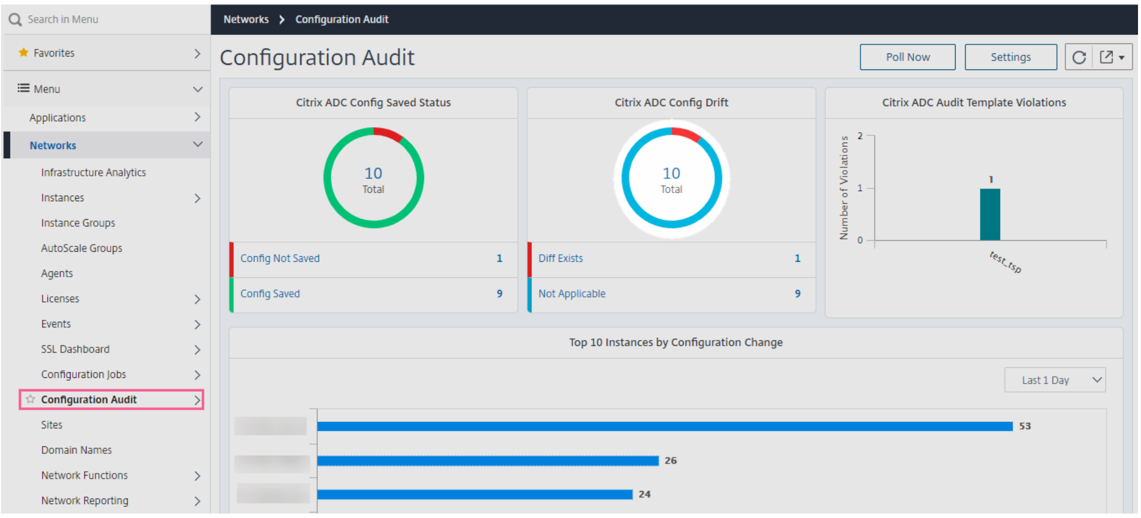
This group enables the assigned user to view and manage the selected admin partitions.

View the revision history difference

Revision history difference for an admin partition allows you to view the difference between the five latest configuration files for a partitioned Citrix ADC instance. You can compare the configuration 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.

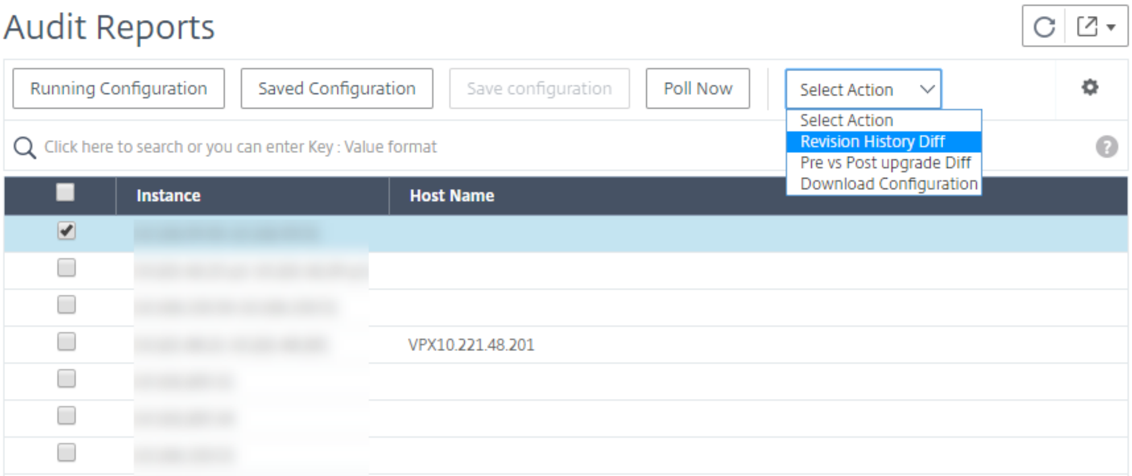
To view the revision history difference:

1. Navigate to **Infrastructure > Configuration Audit**. The Configuration Audit dashboard displays various reports. Click the number displayed in the center of the donut chart.



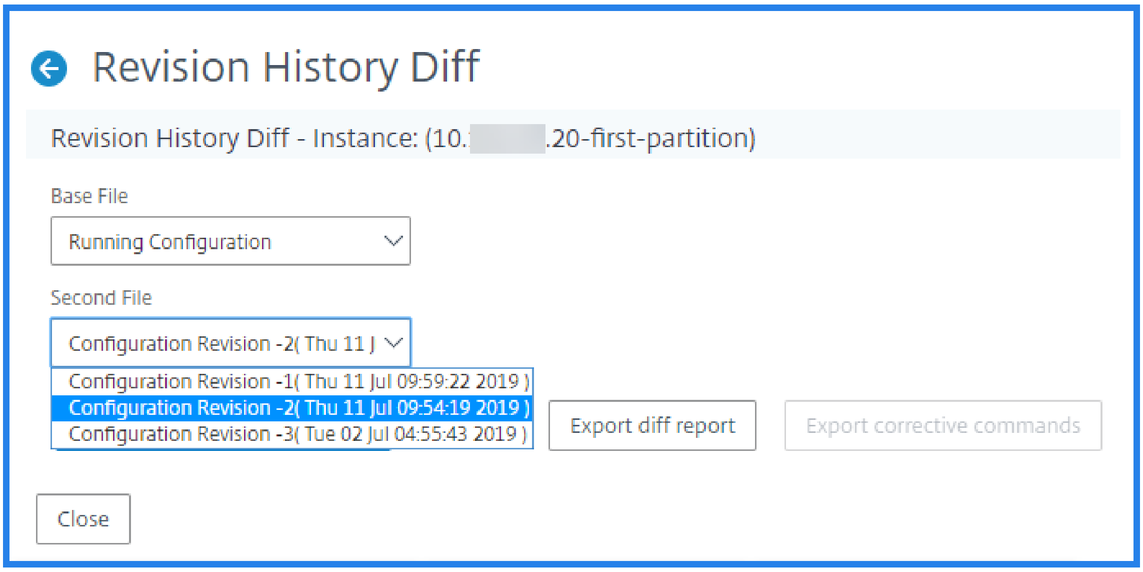
2. Select the partitioned Citrix ADC instance.

3. From the Action box, click **Revision History Diff.**

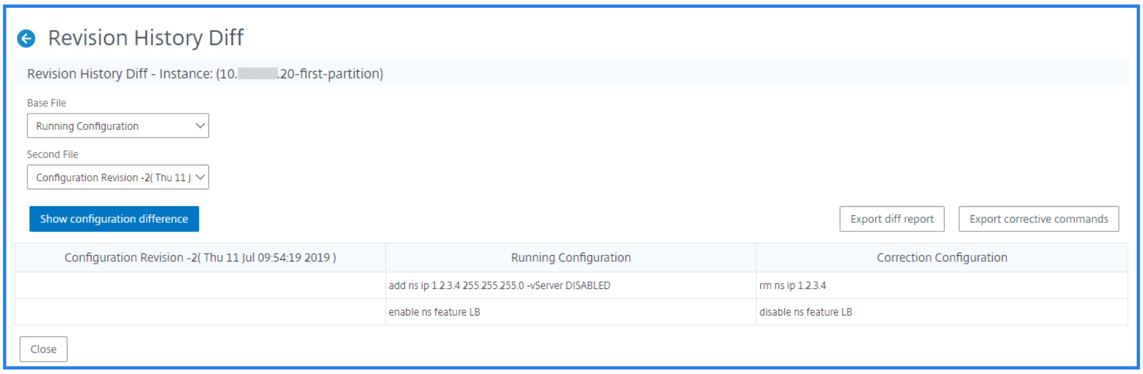


4. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision-2 and then, click **Show configuration difference**.

   You can then view the differences between the five latest configuration files for the selected partitioned Citrix ADC instance. The following is an example admin partition that has three saved configurations:

   
   Revision History Diff
Revision History Diff - Instance: (10. .20-first-partition)
Base File
Running Configuration
Second File
Configuration Revision -2(Thu 11 J
Configuration Revision -1(Thu 11 Jul 09:59:22 2019)
Configuration Revision -2(Thu 11 Jul 09:54:19 2019)
Configuration Revision -3(Tue 02 Jul 04:55:43 2019)
Export diff report
Export corrective commands
Close

   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 to get the configuration to the desired state (configuration file that is being used for comparison).



Revision History Diff

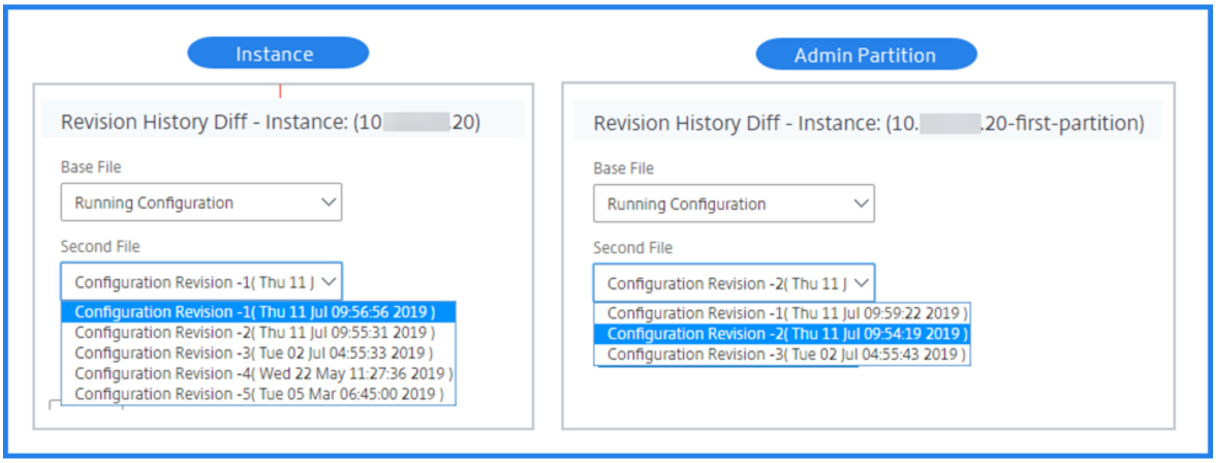
Revision History Diff - Instance: (10.[redacted].20-first-partition)

Base File: Running Configuration

Second File: Configuration Revision -2(Thu 11 J

Configuration Revision -2(Thu 11 Jul 09:54:19 2019)	Running Configuration	Correction Configuration
	add ns ip 1.2.3.4 255.255.255.0 -vServer DISABLED	rm ns ip 1.2.3.4
	enable ns feature LB	disable ns feature LB

The saved configurations on an admin partition and the instance are different. In the following example, the 10.xx.xx.20 instance has five saved configurations where the admin partition of this instance has three different saved configurations:



Revision History Diff - Instance: (10[redacted]20)

Base File: Running Configuration

Second File: Configuration Revision -1(Thu 11 J

- Configuration Revision -1(Thu 11 Jul 09:56:56 2019)
- Configuration Revision -2(Thu 11 Jul 09:55:31 2019)
- Configuration Revision -3(Tue 02 Jul 04:55:33 2019)
- Configuration Revision -4(Wed 22 May 11:27:36 2019)
- Configuration Revision -5(Tue 05 Mar 06:45:00 2019)

Revision History Diff - Instance: (10.[redacted].20-first-partition)

Base File: Running Configuration

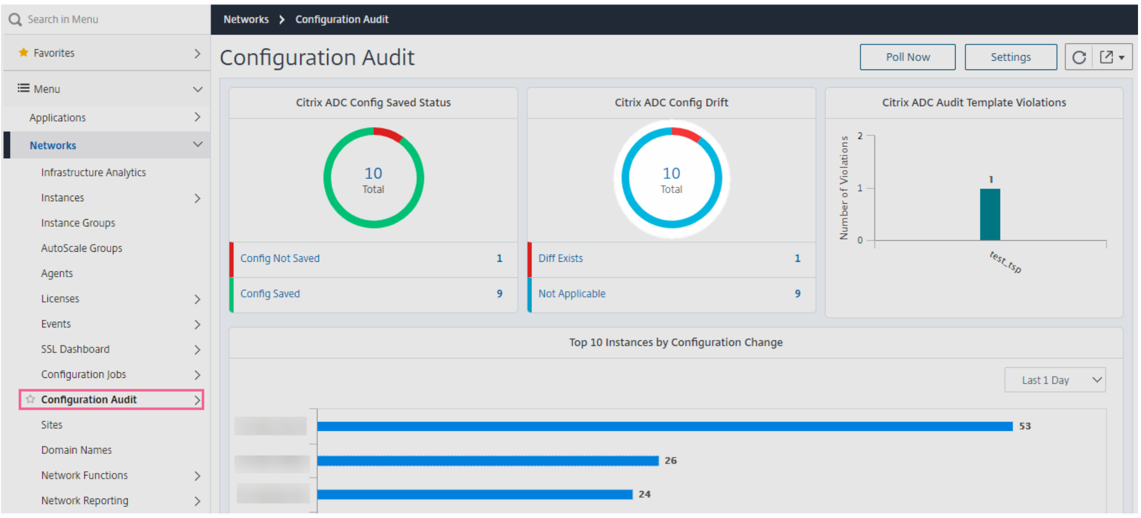
Second File: Configuration Revision -2(Thu 11 J

- Configuration Revision -1(Thu 11 Jul 09:59:22 2019)
- Configuration Revision -2(Thu 11 Jul 09:54:19 2019)
- Configuration Revision -3(Tue 02 Jul 04:55:43 2019)

View the template vs running difference

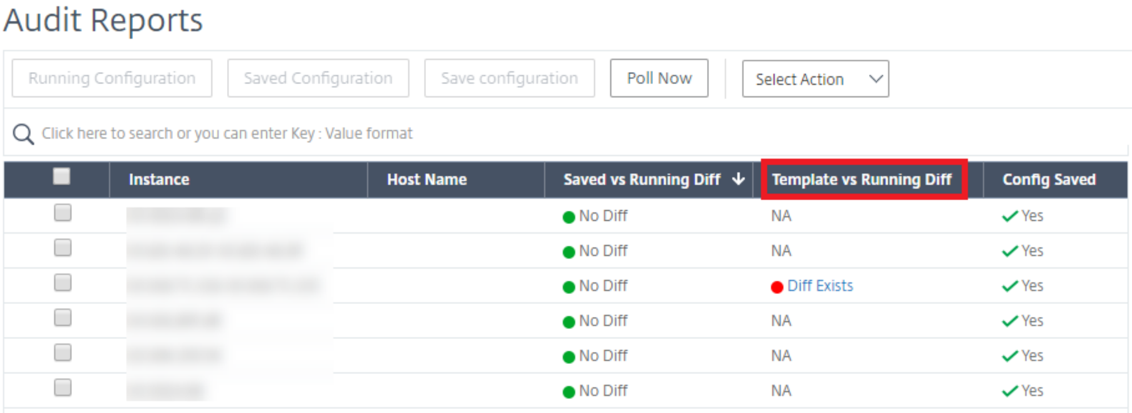
Audit templates for partition allow you to create a custom configuration template and associate it with a partition instance. Any variation in the running configuration of the instance with the audit template is shown in the "**Template vs Running diff**" column of the **Audit Reports** page. Along with 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.

1. Navigate to **Infrastructure > Configuration Audit**. The Configuration Audit dashboard displays various reports. Click the number displayed in the center of the donut chart.



2. In the **Audit Reports** page, click the **Diff Exists** hyperlink under the Template vs Running Diff column.

   If there is any difference between the audit template and the running configuration, 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.



□	Instance	Host Name	Saved vs Running Diff ↓	Template vs Running Diff	Config Saved
□	[redacted]		● No Diff	NA	✓ Yes
□	[redacted]		● No Diff	NA	✓ Yes
□	[redacted]		● No Diff	● Diff Exists	✓ Yes
□	[redacted]		● No Diff	NA	✓ Yes
□	[redacted]		● No Diff	NA	✓ Yes
□	[redacted]		● No Diff	NA	✓ Yes

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Back up and restore Citrix ADC instances

September 28, 2021

You can back up the current state of a Citrix Application Delivery Controller (Citrix ADC) instance and later use the backed-up files to restore the Citrix ADC instance to the same state. You must 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 Citrix ADC instance. You can manually backup and restore Citrix ADC configurations using the GUI, CLI, or you can use Citrix Application Delivery and Management to perform automatic backups and manual restores. Citrix Application Delivery and Management backs up the current state of your managed Citrix ADC instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

Citrix Application Delivery and Management creates a complete backup and restores the following Citrix ADC instance types:

- Citrix ADC SDX
- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

For more information, see Backup and restore an ADC instance.

> **Note**
>
> - From Citrix Application Delivery and Management, you cannot perform the backup and restore operation on a Citrix ADC 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/tenants/<specify-the-tenant-name>/device_backup/

<!--NeedCopy-->
```

To avoid issues due to non-availability of disk space, you can save a maximum of three backup files in this directory.

To back up and restore Citrix ADC instances, you must first configure the backup settings on Citrix Application Delivery and Management. After configuring the settings, you can select a single Citrix ADC instance or multiple instances and create a backup of the configuration files in these instances. If necessary you can also restore the Citrix ADC instances by using these backed-up files.

Create a backup for a selected Citrix ADC instance by using Citrix Application Delivery and Management

Perform this task if you want to back up a selected Citrix ADC instance or multiple instances:

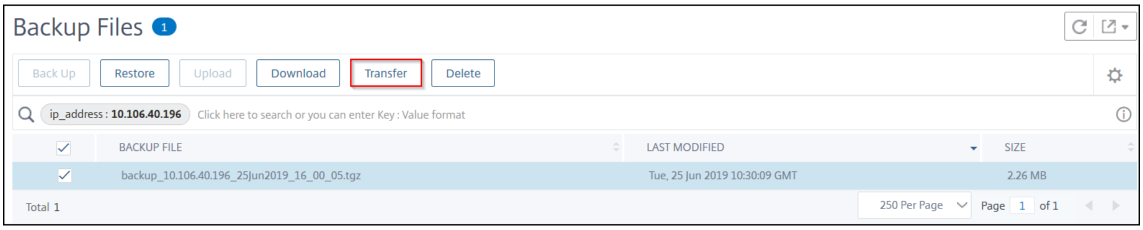
1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instances (for example, VPX) to display on the screen.
2. Select the instance that you want to back up.
    - For MPX, VPX, and BLX instance, select **Backup/Restore** from the **Select Action** list.
    - For an SDX instance, click **Backup/Restore**.
3. On the **Backup Files** page, click **Back Up**.
4. 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**.

Transfer a backup file to an external system

You can transfer a copy of your backup file to another system as a precautionary measure. When you want to restore the configuration, you have to first upload the backup file to the Citrix Application Delivery and Management server and then perform the restore operation.

To transfer a Citrix Application Delivery and Management backup file:

1. Navigate to **Infrastructure > Instances > Citrix ADC** and then select the instance type. For example, VPX.
2. Select the instance and from the **Select Action** list, select **Backup/Restore**.
3. Select the backup file and then click **Transfer**.



Backup Files 1

ip_address : 10.106.40.196 Click here to search or you can enter Key : Value format

☑	BACKUP FILE	LAST MODIFIED	SIZE
☑	backup_10.106.40.196_25Jun2019_16_00_05.tgz	Tue, 25 Jun 2019 10:30:09 GMT	2.26 MB

Total 1   250 Per Page   Page 1 of 1

The **Transfer Backup File** page is displayed. Specify the following parameters:

a) **Server** - IP address of the system where you want to transfer the back-up file.

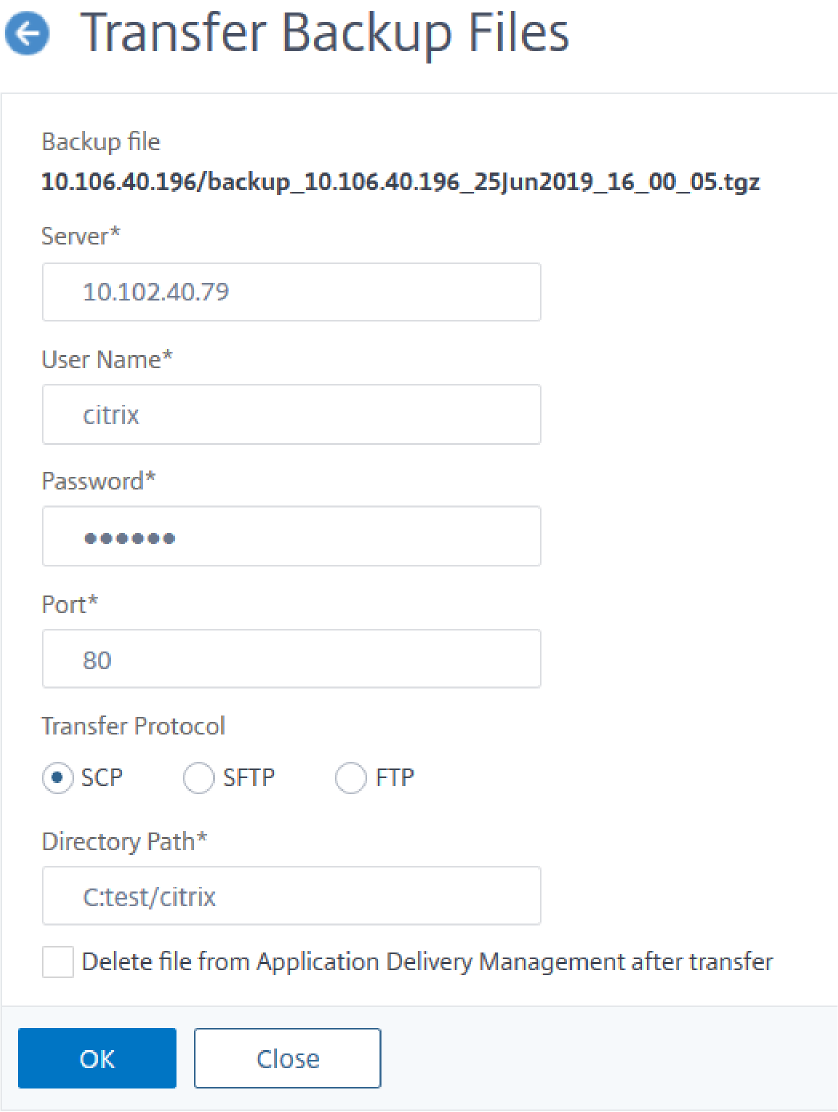
b) **User name** and **password** – User credentials of the new system, where the backed-up files are being copied.

c) **Port** – Port number of the system the files are being transferred to.

d) **Transfer protocol** – Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the back-up file.

e) **Directory path** – The location where the backed-up file is being transferred to on the new system.

f) Click **OK**.



Transfer Backup Files

Backup file
10.106.40.196/backup_10.106.40.196_25Jun2019_16_00_05.tgz

Server*
10.102.40.79

User Name*
citrix

Password*
●●●●●●

Port*
80

Transfer Protocol
● SCP ○ SFTP ○ FTP

Directory Path*
C:test/citrix

□ Delete file from Application Delivery Management after transfer

Restore a Citrix ADC instance by using Citrix Application Delivery and Management

> Note:
>
> If you have Citrix ADC 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 Citrix ADC instance by using the backup file that you had 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 Citrix ADC SDX appliance using Citrix Application Delivery and Management

In Citrix Application Delivery and Management, the backup of a Citrix ADC SDX appliance includes the following:

- Citrix ADC 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
- Citrix ADC config files of devices present on SDX
- Citrix ADC build images
- Citrix ADC 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)

You must restore your Citrix ADC SDX appliance to the configuration available in the backup file. During appliance restore, the entire current configuration is deleted.

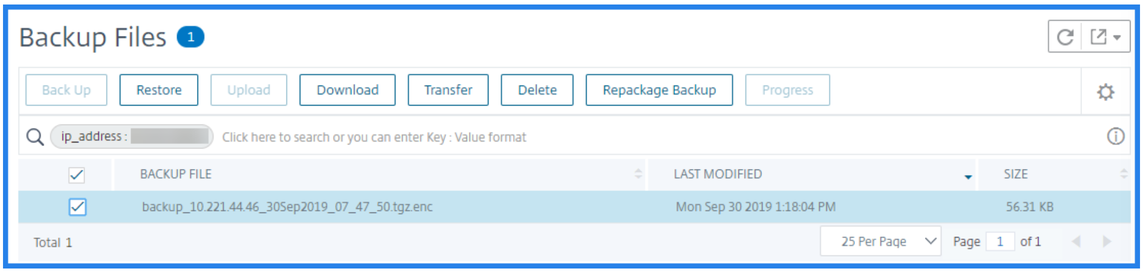
If you are restoring the Citrix ADC SDX appliance by using a backup of a different Citrix ADC SDX appliance, make sure that you add the licenses and configure the appliance's Management Service network settings to match those in the backup file before you start the restore process.

Ensure that the Citrix ADC SDX platform variant that was backed up was taken is the same as the one on which you are trying to restore. You cannot restore from a different platform variant.

> **Note**
>
> Before you restore the SDX RMA appliance, ensure 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 Citrix Application Delivery and Management GUI, navigate to **Infrastructure > Instances > Citrix ADC**.
2. Click **Backup/Restore**.
3. Select the backup file of the same instance that you want to restore.
4. Click **Repackage Backup**.



☑	BACKUP FILE	LAST MODIFIED	SIZE
☑	backup_10.221.44.46_30Sep2019_07_47_50.tgz.enc	Mon Sep 30 2019 1:18:04 PM	56.31 KB

Total 1 | 25 Per Page | Page 1 of 1

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**.

Export the report of this dashboard

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Force a failover to the secondary Citrix ADC instance

September 24, 2021

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix Application Delivery Controller (Citrix 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 Citrix ADC 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.

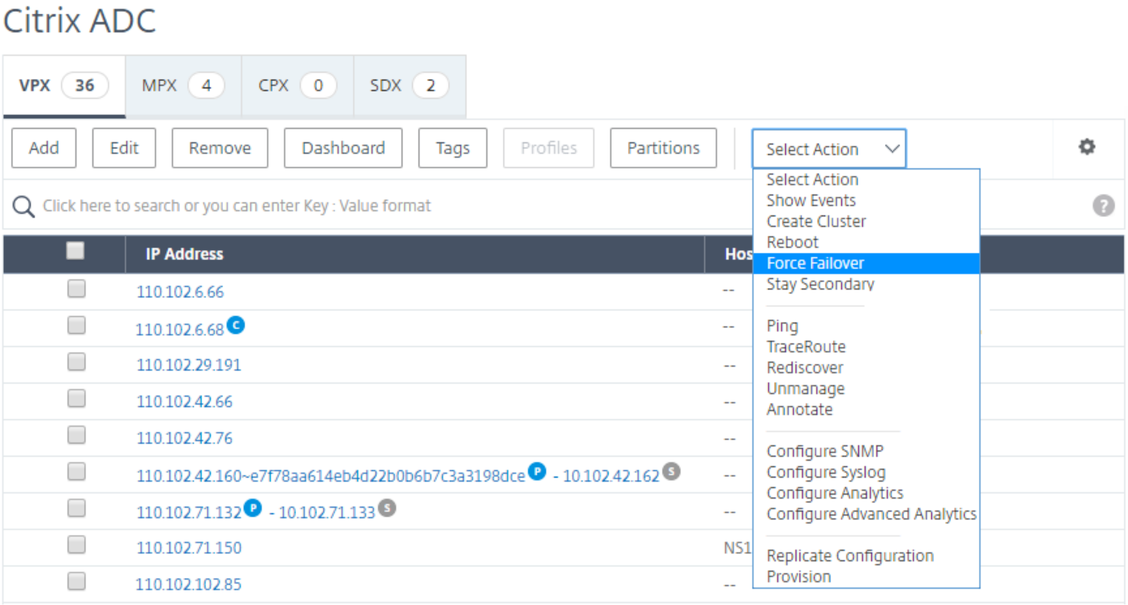
To force a failover to the secondary Citrix ADC instance using Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances**. Go to **VPX** tab and select an instance.

2. Select instances in an HA setup from the instances listed under the selected instance type.

3. From the **Action** box, select **Force Failover.**

4. Click **Yes** to confirm the force failover action.



☐	IP Address	Hos
☐	110.102.6.66	--
☐	110.102.6.68 C	--
☐	110.102.29.191	--
☐	110.102.42.66	--
☐	110.102.42.76	--
☐	110.102.42.160~e7f78aa614eb4d22b0b6b7c3a3198dce P - 10.102.42.162 S	--
☐	110.102.71.132 P - 10.102.71.133 S	--
☐	110.102.71.150	NS1
☐	110.102.102.85	--

Force a secondary Citrix ADC instance to stay secondary

September 24, 2021

In a High Availability (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, and 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.

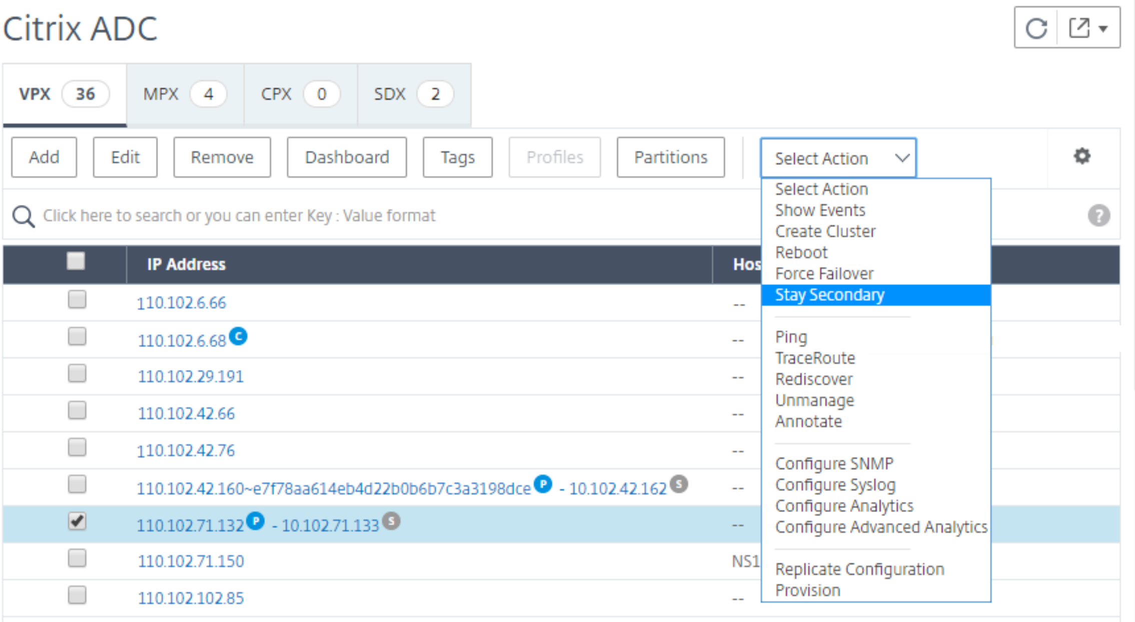
To configure a secondary Citrix ADC instance to stay secondary by using Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances**, and then select an instance under an instance type (VPX).

2. Select instances in an HA setup from the instances listed under the selected instance type.

3. From the **Action** box, select **Stay Secondary**.

4. Click **Yes** to confirm the execution of the “Stay Secondary” action.



☐	IP Address	Hos
☐	110.102.6.66	--
☐	110.102.6.68 C	--
☐	110.102.29.191	--
☐	110.102.42.66	--
☐	110.102.42.76	--
☐	110.102.42.160~e7f78aa614eb4d22b0b6b7c3a3198dce P - 10.102.42.162 S	--
☑	110.102.71.132 P - 10.102.71.133 S	--
☐	110.102.71.150	NS1
☐	110.102.102.85	--

Create instance groups

September 24, 2021

To create an instance group, you must first add all your Citrix ADC instances to Citrix Application Delivery and Management. 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 Citrix Application Delivery and Management

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Instance Groups**, and then click **Add**.

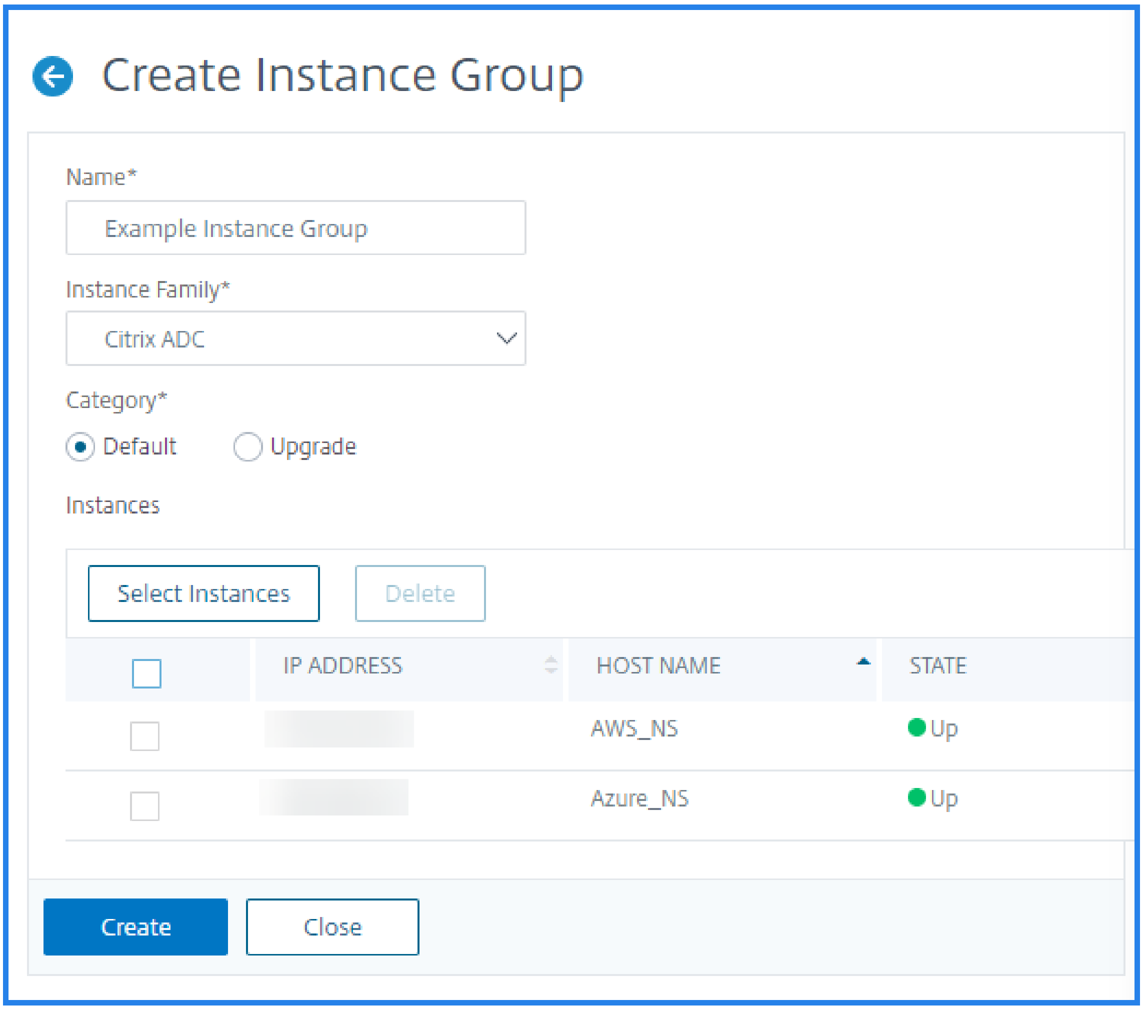
2. Specify a name to your instance group and select **Citrix ADC** from the **Instance Family** list.

3. In **Category**, select the **Default** option.

4. 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**.

5. Click **Create**.



Create Instance Group

Name*: Example Instance Group

Instance Family*: Citrix ADC

Category*: ● Default ○ Upgrade

Instances

□	IP ADDRESS	HOST NAME	STATE
□	[redacted]	AWS_NS	● Up
□	[redacted]	Azure_NS	● Up

Provision ADC VPX instances on SDX

October 20, 2021

You can provision one or more ADC VPX instances on the SDX appliance by using Citrix Application Delivery and Management. 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 Citrix Application Delivery and Management does not allow you to provision more Citrix ADC instances.

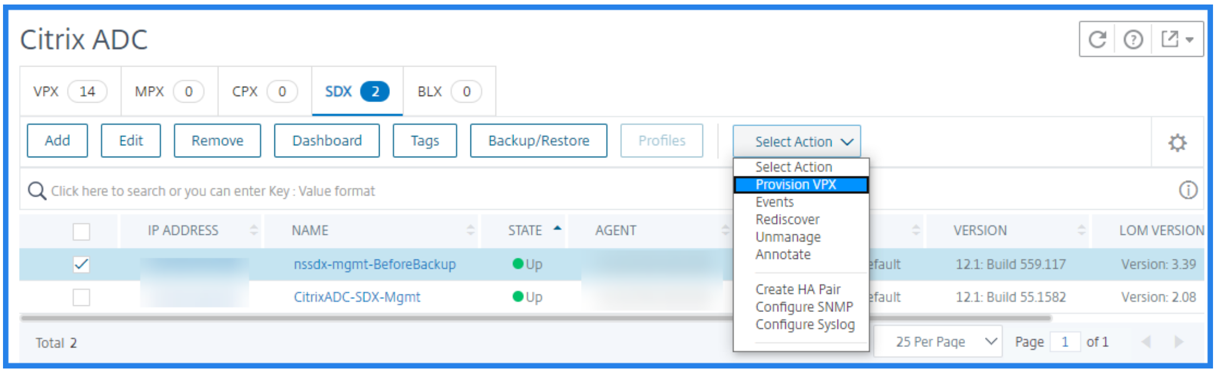
Before you begin, ensure to add an SDX instance in Citrix Application Delivery and Management where you want to provision VPX instances.

To provision a VPX instance, do the following:

1. Navigate to **Infrastructure > Instances > Citrix ADC**.

2. In the **SDX** tab, select an SDX instance where you want to provision a VPX instance.

3. In **Select Action**, select **Provision VPX**.



☐	IP ADDRESS	NAME	STATE	AGENT		VERSION	LOM VERSION
☑	[redacted]	nssdx-mgmt-BeforeBackup	● Up	[redacted]	efault	12.1: Build 559.117	Version: 3.39
☐	[redacted]	CitrixADC-SDX-Mgmt	● Up	[redacted]	efault	12.1: Build 55.1582	Version: 2.08

Step 1 - Add a VPX instance

The Citrix Application Delivery and Management 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 Citrix Application Delivery and Management and a VPX instance.

  - **IP address** - You can select an **IPv4** or **IPv6** address or both to manage the Citrix VPX instance. A VPX instance can have only one management IP (also called Citrix ADC IP). You cannot remove the Citrix ADC IP address.

    For the selected option, assign a netmask, default gateway, and next hop to the Citrix Application Delivery and Management for the IP address.

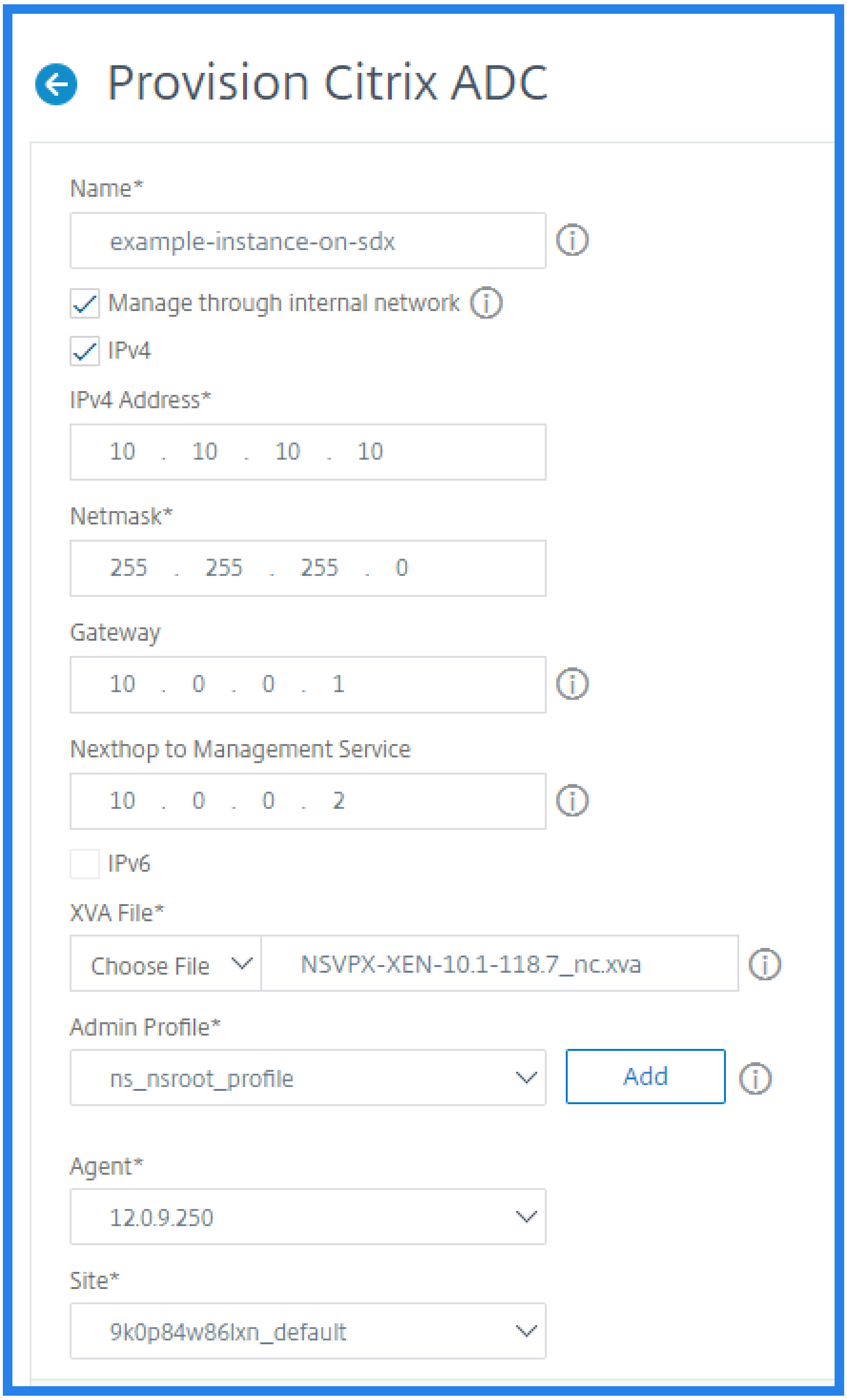
- **XVA File** - Select the XVA file from which you want to provision a VPX instance. Use one of the following options to select the XVA file.

  - **Local** - Select the XVA file from your local machine.

  - **Appliance** - Select the XVA file from an Citrix Application Delivery and Management file browser.

- **Admin Profile** - This profile provides access to provision VPX instances. With this profile, Citrix Application Delivery and Management 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.



Provision Citrix ADC

Name*: example-instance-on-sdx

☑ Manage through internal network

☑ IPv4

IPv4 Address*: 10 . 10 . 10 . 10

Netmask*: 255 . 255 . 255 . 0

Gateway: 10 . 0 . 0 . 1

Nexthop to Management Service: 10 . 0 . 0 . 2

□ IPv6

XVA File*: Choose File NSVPX-XEN-10.1-118.7_nc.xva

Admin Profile*: ns_nsroot_profile

Agent*: 12.0.9.250

Site*: 9k0p84w86lxn_default

Step 2 - Allocate licenses

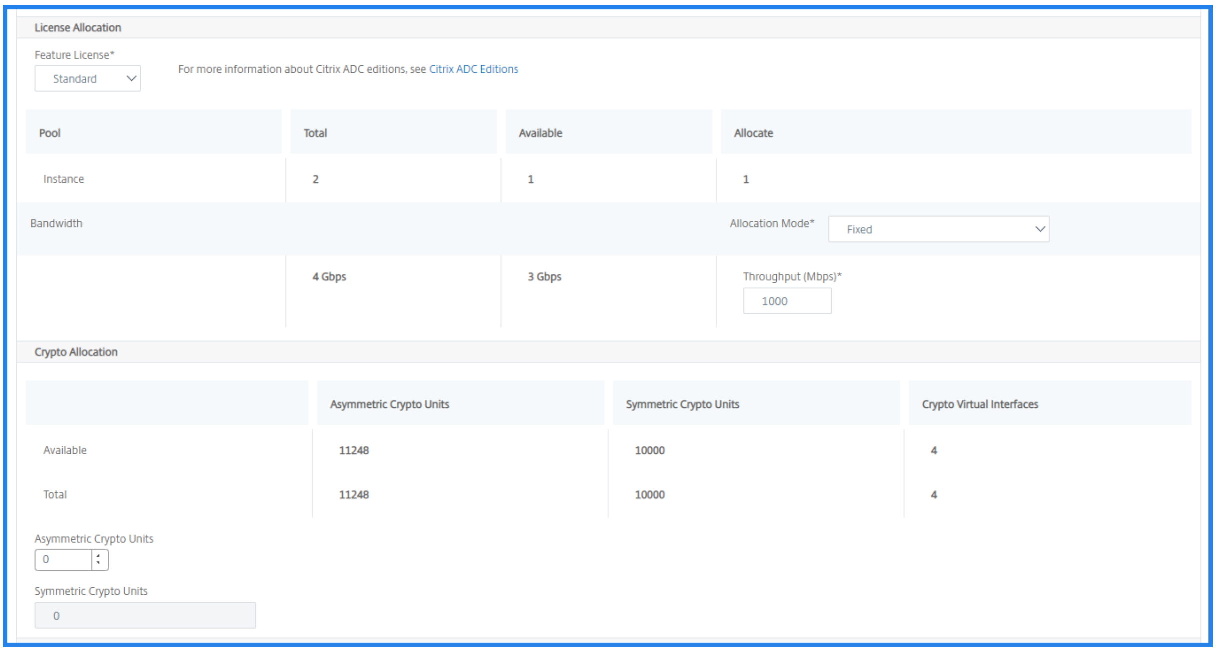
In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **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.



License Allocation

Feature License*: Standard

For more information about Citrix ADC editions, see Citrix ADC Editions

Pool	Total	Available	Allocate
Instance	2	1	1

Bandwidth

Allocation Mode*: Fixed

	Total	Available	Allocate
	4 Gbps	3 Gbps	Throughput (Mbps)*: 1000

Crypto Allocation

	Asymmetric Crypto Units	Symmetric Crypto Units	Crypto Virtual Interfaces
Available	11248	10000	4
Total	11248	10000	4

Asymmetric Crypto Units: 0

Symmetric Crypto Units: 0

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.

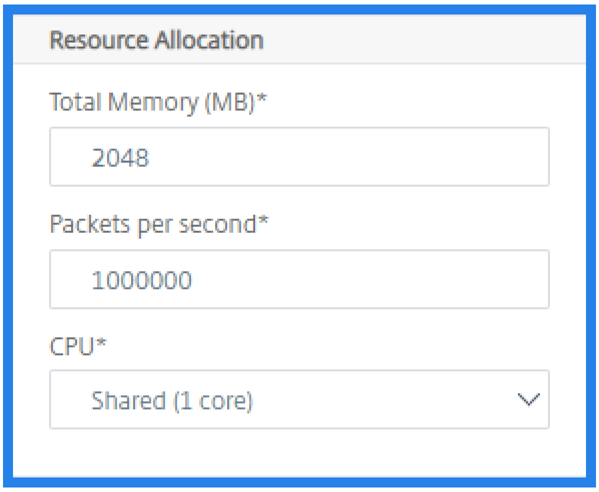
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  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.



Resource Allocation

Total Memory (MB)*

2048

Packets per second*

1000000

CPU*

Shared (1 core)

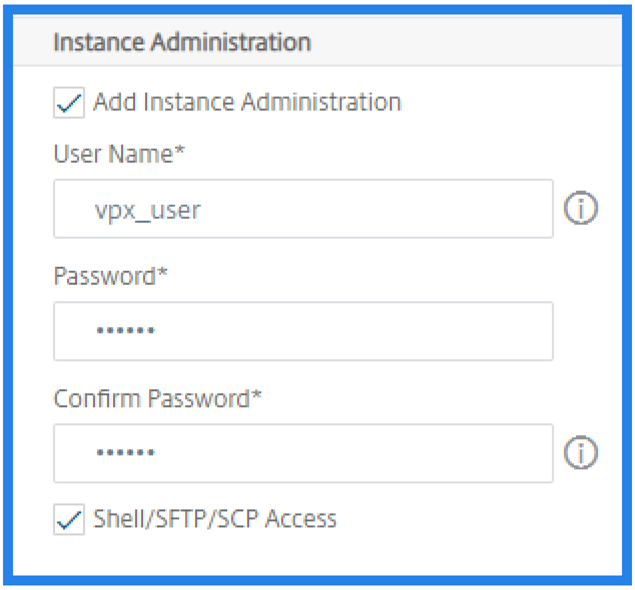
See the table in Provision Citrix ADC instances that lists the supported VPX, single bundle image version, and the number of cores you can assign to an instance.

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 Citrix ADC 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 Citrix ADC instance administrator. This option is selected by default.



Instance Administration

☑ Add Instance Administration

User Name*: vpx_user

Password*: ••••••

Confirm Password*: ••••••

☑ Shell/SFTP/SCP Access

Step 5 - Specify network settings

Select the required network settings to an instance:

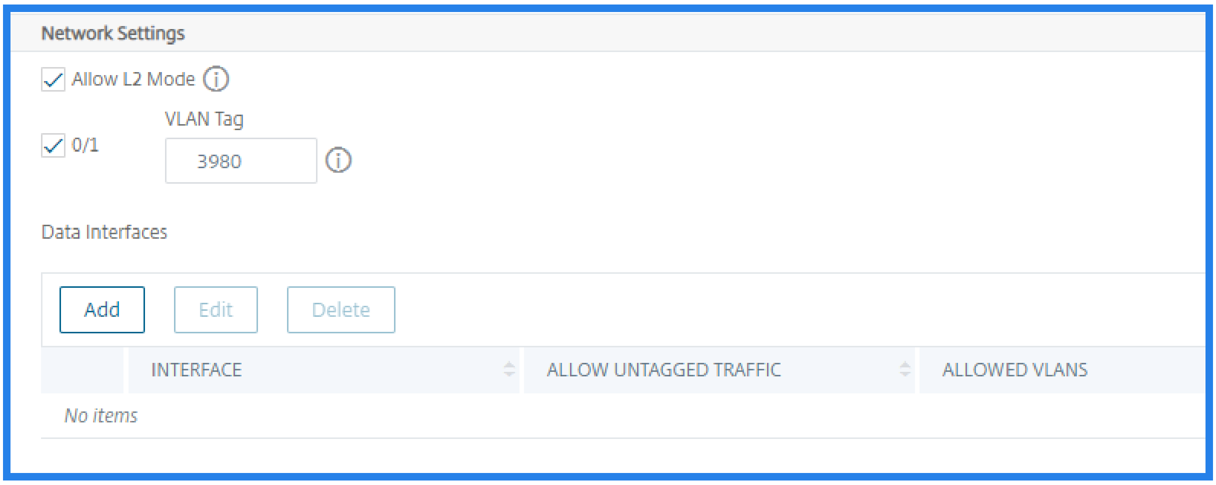
- **Allow L2 Mode under network settings** - You can allow L2 mode on the Citrix ADC instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode. For more information, see Allowing L2 Mode on a Citrix ADC instance.

  > **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 Citrix ADC 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.



Network Settings

☑ Allow L2 Mode

☑ 0/1 VLAN Tag: 3980

Data Interfaces

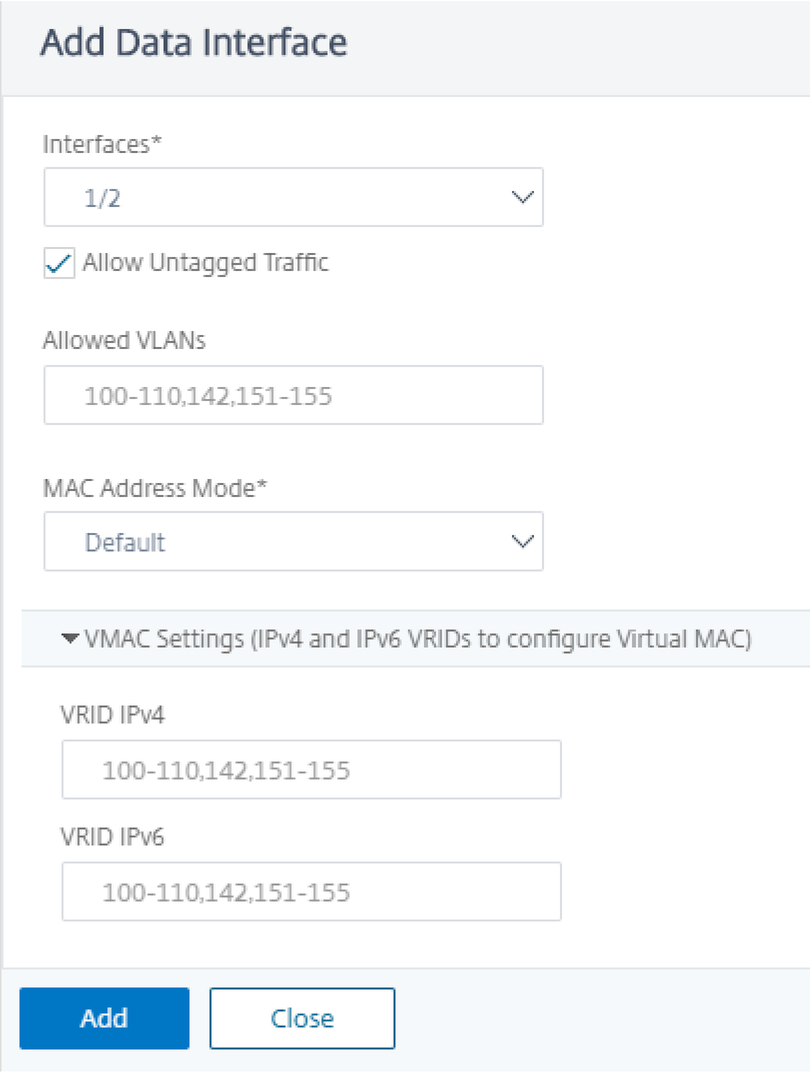
INTERFACE	ALLOW UNTAGGED TRAFFIC	ALLOWED VLANS
No items		

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 Citrix ADC 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.



Add Data Interface

Interfaces*

1/2

☑ Allow Untagged Traffic

Allowed VLANs

100-110,142,151-155

MAC Address Mode*

Default

▾ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

100-110,142,151-155

VRID IPv6

100-110,142,151-155

Click **Add**.

Step 6 - Specify Management VLAN settings

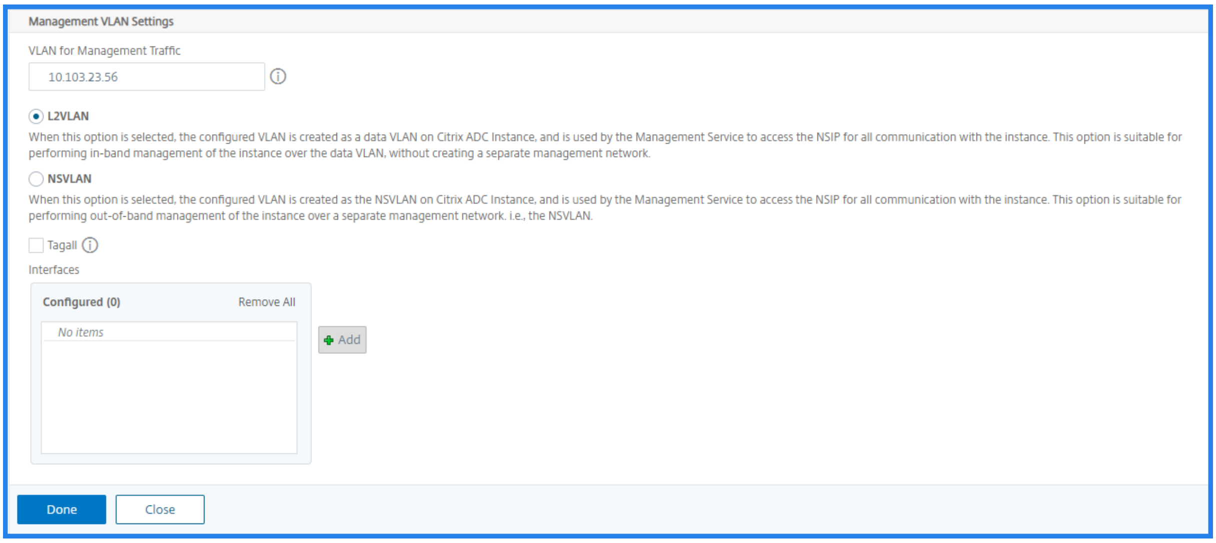
The Management Service and the management address (NSIP) of the VPX instance are in the same subnetwork, and communication is over a management interface.

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.



Management VLAN Settings

VLAN for Management Traffic

10.103.23.56

● L2VLAN

When this option is selected, the configured VLAN is created as a data VLAN on Citrix ADC Instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing in-band management of the instance over the data VLAN, without creating a separate management network.

○ NSVLAN

When this option is selected, the configured VLAN is created as the NSVLAN on Citrix ADC Instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing out-of-band management of the instance over a separate management network. i.e., the NSVLAN.

□ Tagall

Interfaces

Configured (0) Remove All

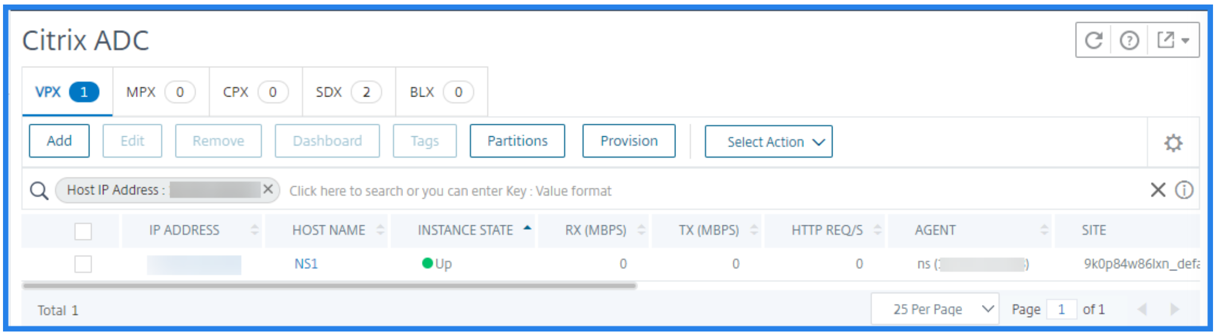
No items

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 > Citrix ADC**.
2. In the **VPX** tab, search an instance by the **Host IP address** property and specify SDX instance IP to it.



Citrix ADC

Host IP Address : [redacted]

Click here to search or you can enter Key : Value format

□	IP ADDRESS	HOST NAME	INSTANCE STATE	RX (MBPS)	TX (MBPS)	HTTP REQ/S	AGENT	SITE
□	[redacted]	NS1	● Up	0	0	0	ns ([redacted])	9k0p84w86lxn_defa

Total 1

25 Per Page Page 1 of 1

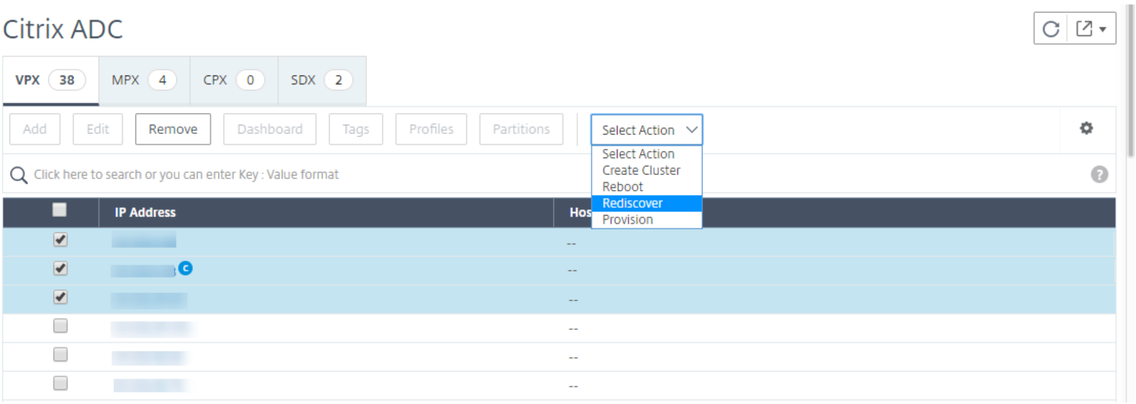
Rediscover multiple Citrix ADC instances

September 24, 2021

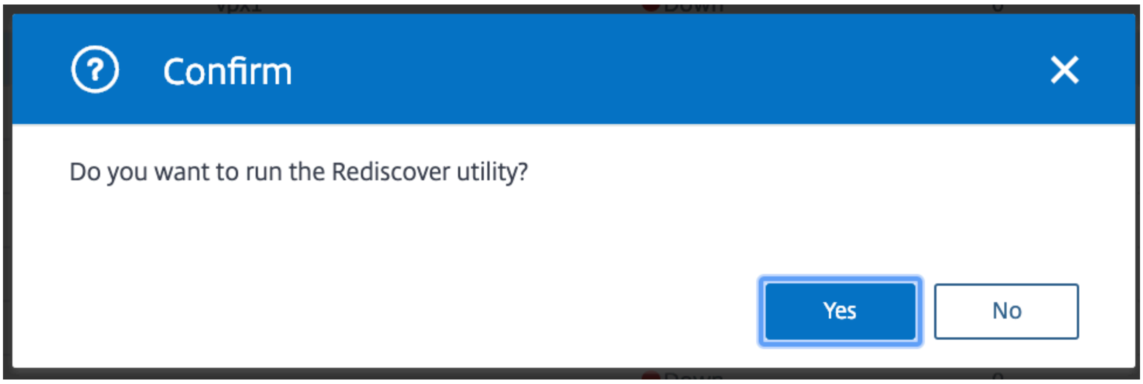
You can rediscover multiple Citrix Application Delivery Controller (Citrix ADC) instances (VPX, MPX, SDX, BLX, and CPX) in your Citrix Application Delivery and Management setup. After you rediscover the instances, you can view the latest states and configurations of those instances. The Citrix Application Delivery and Management server rediscovers all ADC instances and checks whether the instances are reachable.

To rediscover multiple Citrix ADC VPX instances:

1. Navigate to **Infrastructure > Instances > Citrix ADC**. Select the instance tab (VPX, MPX, SDX, BLX, and CPX) and select the instances you want to rediscover.
2. In the **Action** box, click **Rediscover**. The following screen captures show how to rediscover multiple VPX instances.

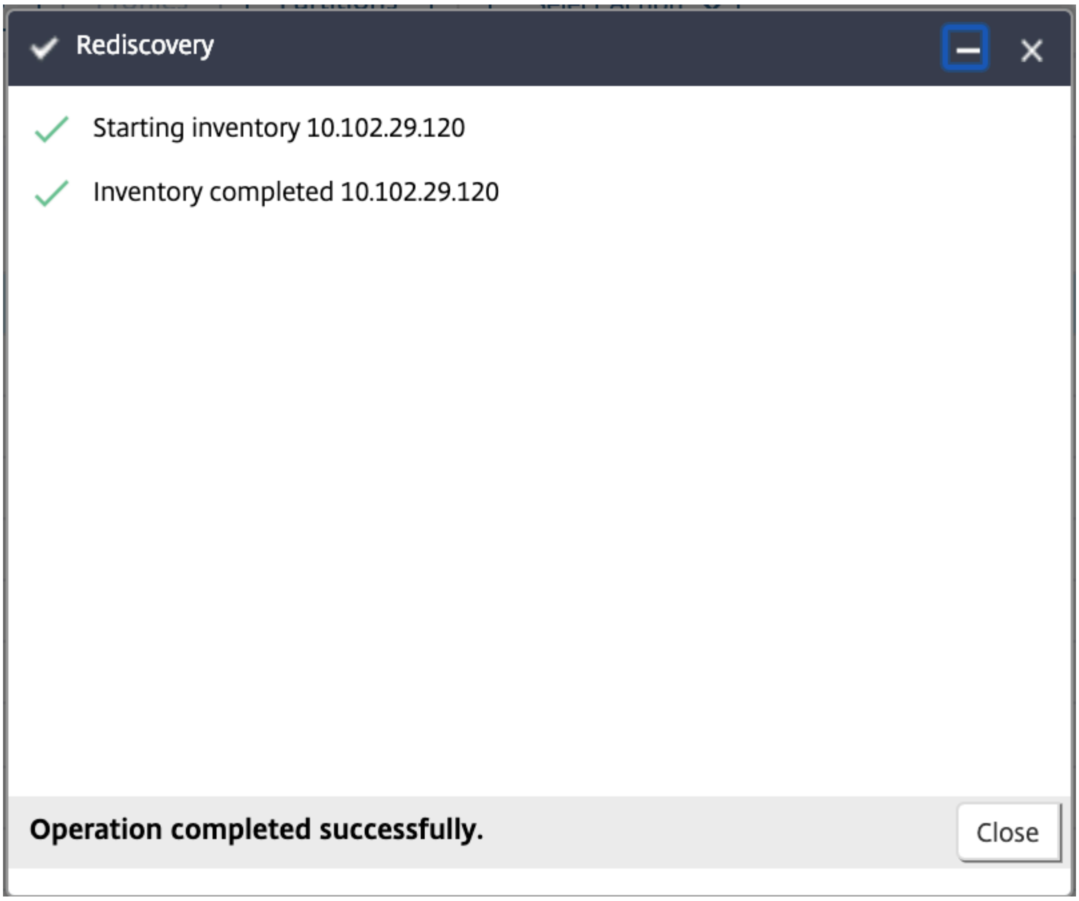


3. When the confirmation message for running the Rediscover utility appears, Click **Yes**.



Do you want to run the Rediscover utility?

The screen reports the progress of rediscovery of each of the ADC instances.



✓ Starting inventory 10.102.29.120

✓ Inventory completed 10.102.29.120

Operation completed successfully.

Polling overview

September 25, 2021

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

- Instance polling
- Inventory polling
- Performance data collection
- Instance backup polling

- Configuration audit polling
- SSL certificate polling
- Entity polling

Citrix Application Delivery and Management uses protocols such as NITRO call, Secure Shell (SSH), and Secure Copy (SCP) to poll information from Citrix ADC instances.

How Citrix Application Delivery and Management polls managed instances and entities

Citrix Application Delivery and Management automatically polls at regular intervals by default. Citrix Application Delivery and Management 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 5 minutes (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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Instance backup polling	Every 12 hours (by default)	The backup file of the current state of the managed ADC instances	NITRO calls, SSH, and SCP.	Yes. Navigate to **Infrastructure > Instances > Citrix ADC**. Select the instance and from the **Select Action** list, click **Backup/Restore**.
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 > Configuration Audit**. On the Configuration Audit page, click **Settings** and configure the polling interval for Configuration Audit Polling.

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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
				You can poll SSL certificates manually and add all certificates of the instances immediately to Citrix Application Delivery and Management. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page lets you 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 Citrix Application Delivery and Management 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.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
				You can poll entities manually and add all entities of the instances immediately to Citrix Application Delivery and Management. To do so, navigate to **Infrastructure > Network Functions** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network

> **Note**
>
> In addition to polling, events generated by managed ADC instances are received by Citrix Application Delivery and Management 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 Citrix Application Delivery and Management. During a configuration audit, ns.conf files are downloaded and stored in the file system. All information collected from managed Citrix ADC instances are stored internally within the database.

Different ways of polling instances

The following are the different ways of polling that Citrix Application Delivery and Management performs on the managed instances:

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

Global polling of instances

Citrix Application Delivery and Management automatically polls all the managed instances in the network depending on the interval configured by you. Though the default polling interval is 60 minutes, you can set the interval depending on your requirements by navigating to **Infrastructure > Network Functions > Settings**.

Manual polling of instances

When Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, there is a minimum polling interval period when automatic polling does not happen. If you add a new Citrix ADC instance, or if an entity is updated, Citrix Application Delivery and Management 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 Citrix ADC network to be polled, which creates a heavy load on the network. Instead of polling the entire network, Citrix Application Delivery and Management now allows you to poll only selected instances and entities at any given time.

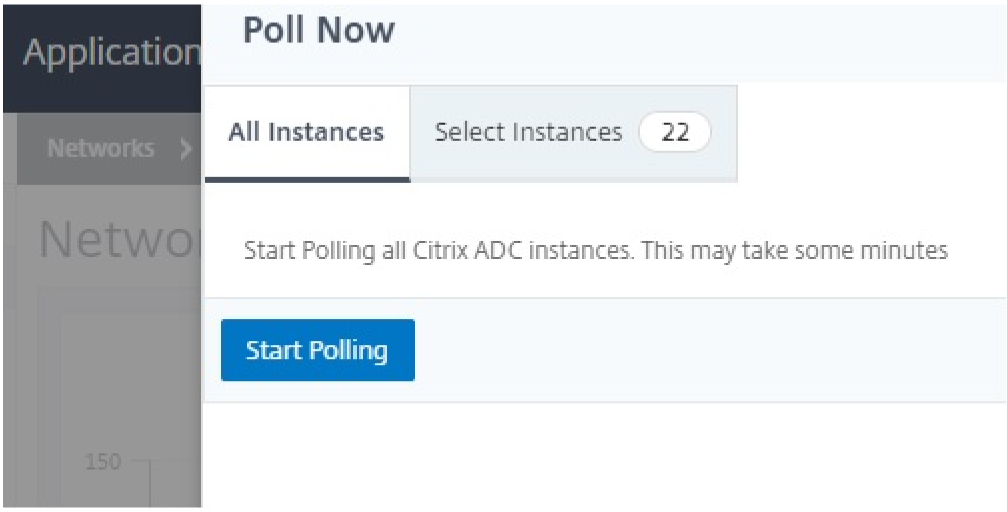
Citrix Application Delivery and Management automatically polls managed instances to collect information at set times in a day. Selected polling reduces the refresh time that Citrix Application Delivery and Management requires to display the most recent status of the entities bound to these selected instances.

To poll specific instances in Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, 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 Citrix ADC instances in the network or poll the selected instances.
    a) **All Instances** tab - click **Start Polling** to poll all the instances.

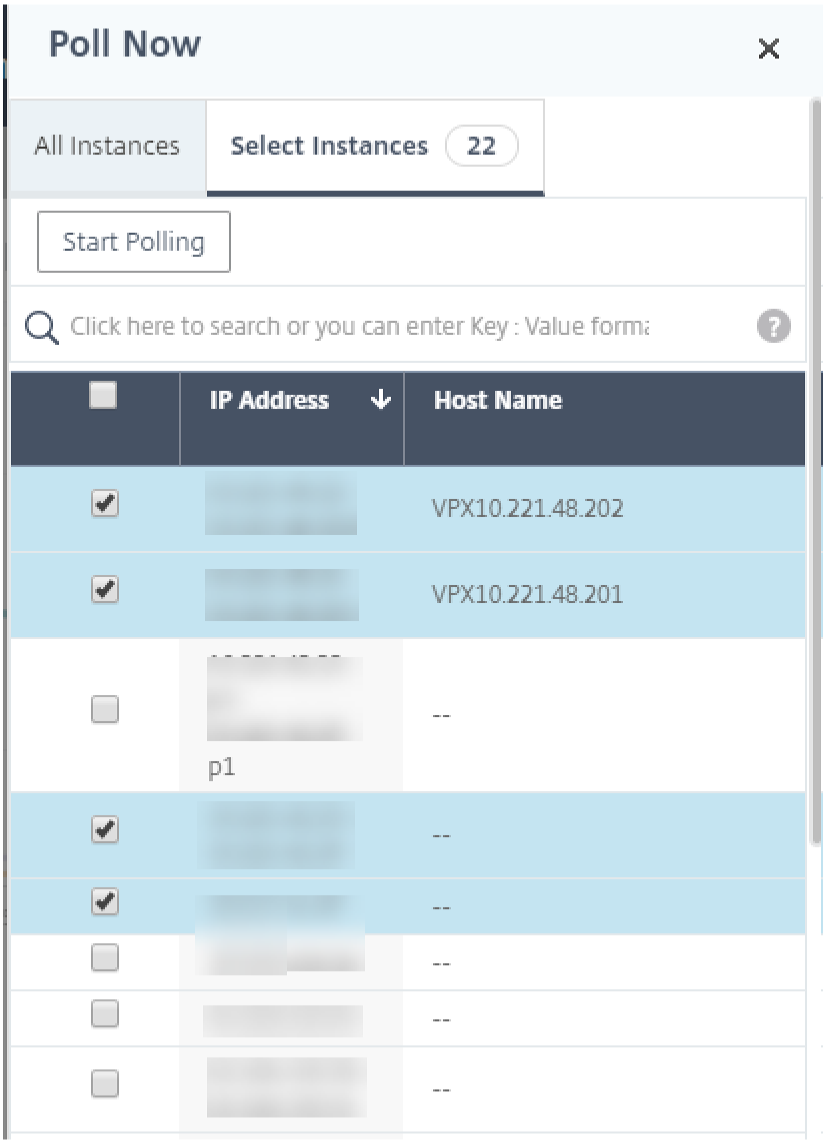
   b) **Select Instances** tab - select the instances from the list

4. Click **Start Polling**.



Poll Now

Start Polling all Citrix ADC instances. This may take some minutes



Poll Now ×

□	IP Address ↓	Host Name
☑	[redacted]	VPX10.221.48.202
☑	[redacted]	VPX10.221.48.201
□	[redacted] p1	--
☑	[redacted]	--
☑	[redacted]	--
□	[redacted]	--
□	[redacted]	--
□	[redacted]	--

Citrix Application Delivery and Management initiates manual polling and adds all the entities.

Manual polling of entities

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

Consider an example of a virtual server being **DOWN**. The status 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 status is displayed on the GUI immediately.

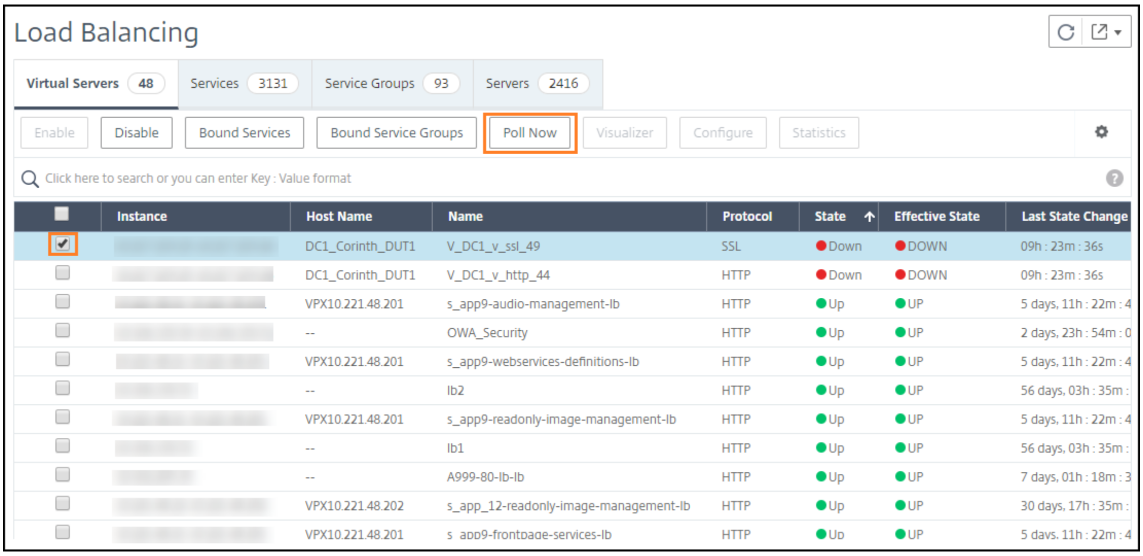
You can now poll the following entities for any update in their status, services, service groups, load balancing virtual servers, cache reduction virtual servers, content switching virtual servers, authentication virtual servers, VPN virtual servers, GSLB virtual servers, and application servers.

> **Note**
>
> If you poll a virtual server, only that virtual server is polled. The associated entities such as services, 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 Citrix Application Delivery and Management:

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

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Network Functions > Load Balancing > Virtual Servers**.
2. Select the virtual server that shows the status as **DOWN**, and then click **Poll Now**. The status of the virtual server now changes to **UP**.



□	Instance	Host Name	Name	Protocol	State	Effective State	Last State Change
☑	[redacted]	DC1_Corinth_DUT1	V_DC1_v_ssl_49	SSL	● Down	● DOWN	09h : 23m : 36s
□	[redacted]	DC1_Corinth_DUT1	V_DC1_v_http_44	HTTP	● Down	● DOWN	09h : 23m : 36s
□	[redacted]	VPX10.221.48.201	s_app9-audio-management-lb	HTTP	● Up	● UP	5 days, 11h : 22m : 4
□	[redacted]	--	OWA_Security	HTTP	● Up	● UP	2 days, 23h : 54m : 0
□	[redacted]	VPX10.221.48.201	s_app9-webservices-definitions-lb	HTTP	● Up	● UP	5 days, 11h : 22m : 4
□	[redacted]	--	lb2	HTTP	● Up	● UP	56 days, 03h : 35m :
□	[redacted]	VPX10.221.48.201	s_app9-readonly-image-management-lb	HTTP	● Up	● UP	5 days, 11h : 22m : 4
□	[redacted]	--	lb1	HTTP	● Up	● UP	56 days, 03h : 35m :
□	[redacted]	--	A999-80-lb-lb	HTTP	● Up	● UP	7 days, 01h : 18m : 3
□	[redacted]	VPX10.221.48.202	s_app_12-readonly-image-management-lb	HTTP	● Up	● UP	30 days, 17h : 35m :
□	[redacted]	VPX10.221.48.201	s_app9-frontpage-services-lb	HTTP	● Up	● UP	5 days, 11h : 22m : 4

Unmanage an instance

September 24, 2021

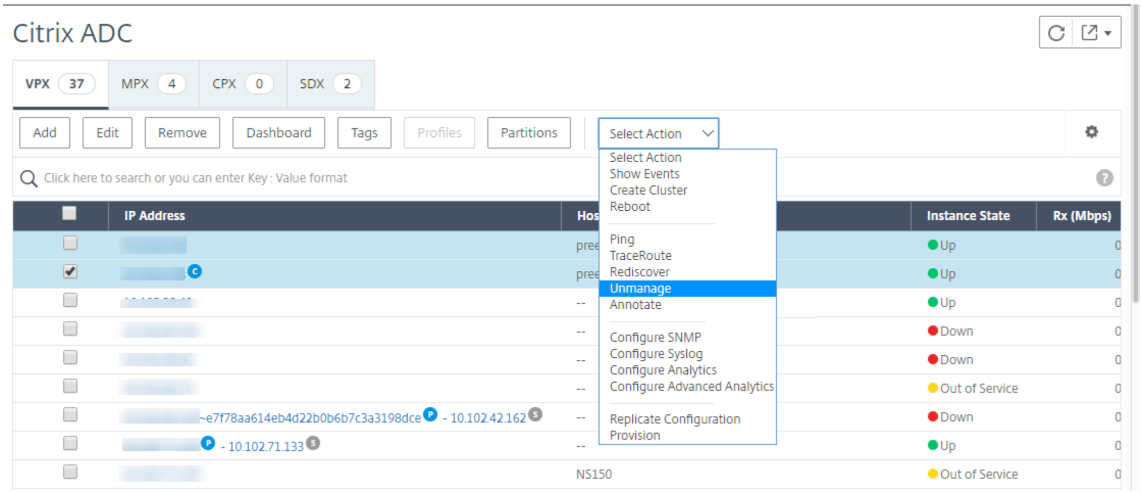
If you want to stop the exchange of information between Citrix Application Delivery and Management and the instances in your network, you can unmanage the instances.

To unmanage an instance:

1. Navigate to **Infrastructure > Instances > Citrix ADC**.

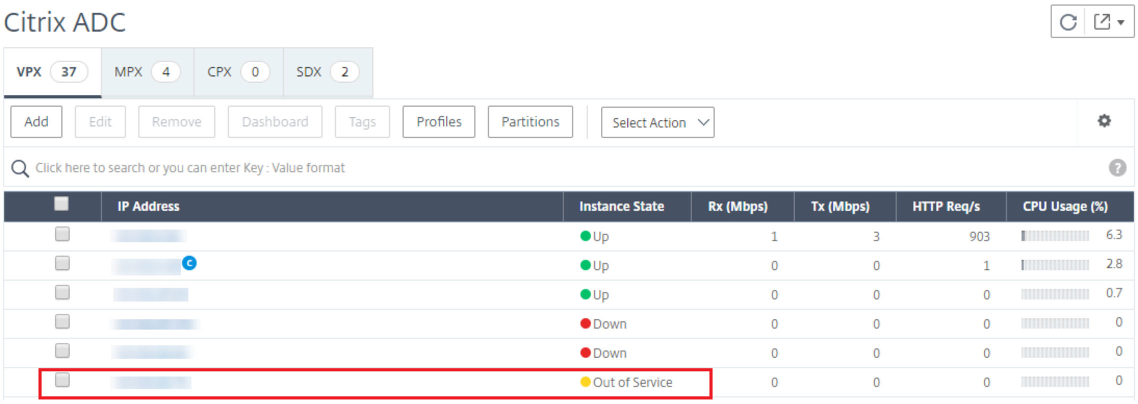
2. Select the ADC instance tab (for example, VPX).

3. In the list of instances, either right-click an instance and then select **Unmanage**, or select instance and from the **Action** list, select **Unmanage**.



□	IP Address	Hos	Instance State	Rx (Mbps)
□	[redacted]	pree	● Up	0
☑	[redacted] C	pree	● Up	0
□	[redacted]	--	● Up	0
□	[redacted]	--	● Down	0
□	[redacted]	--	● Down	0
□	[redacted]	--	● Out of Service	0
□	[redacted]~e7f78aa614eb4d22b0b6b7c3a3198dce P - 10.102.42.162 S	--	● Down	0
□	[redacted] P - 10.102.71.133 S	--	● Up	0
□	[redacted]	NS150	● Out of Service	0

The status of the selected instance changes to **Out of Service**.



□	IP Address	Instance State	Rx (Mbps)	Tx (Mbps)	HTTP Req/s	CPU Usage (%)
□	[redacted]	● Up	1	3	903	6.3
□	[redacted] C	● Up	0	0	1	2.8
□	[redacted]	● Up	0	0	0	0.7
□	[redacted]	● Down	0	0	0	0
□	[redacted]	● Down	0	0	0	0
□	[redacted]	● Out of Service	0	0	0	0

The instance is no longer managed by Citrix Application Delivery and Management, and it no longer exchanges data with Citrix Application Delivery and Management.

Trace the route to an instance

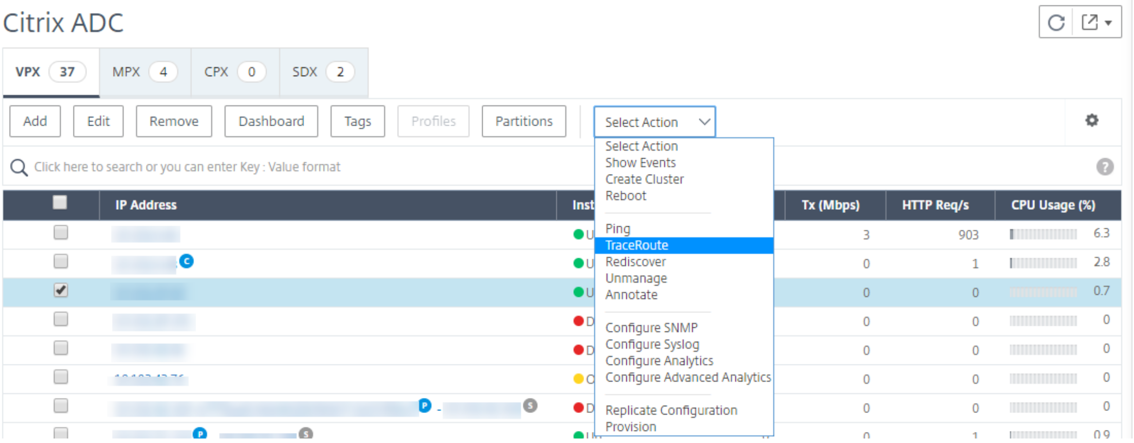
September 24, 2021

By tracing the route of a packet from the Citrix Application Delivery and Management to an instance, you can find information such as the number of hops necessary to reach the instance. The 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.

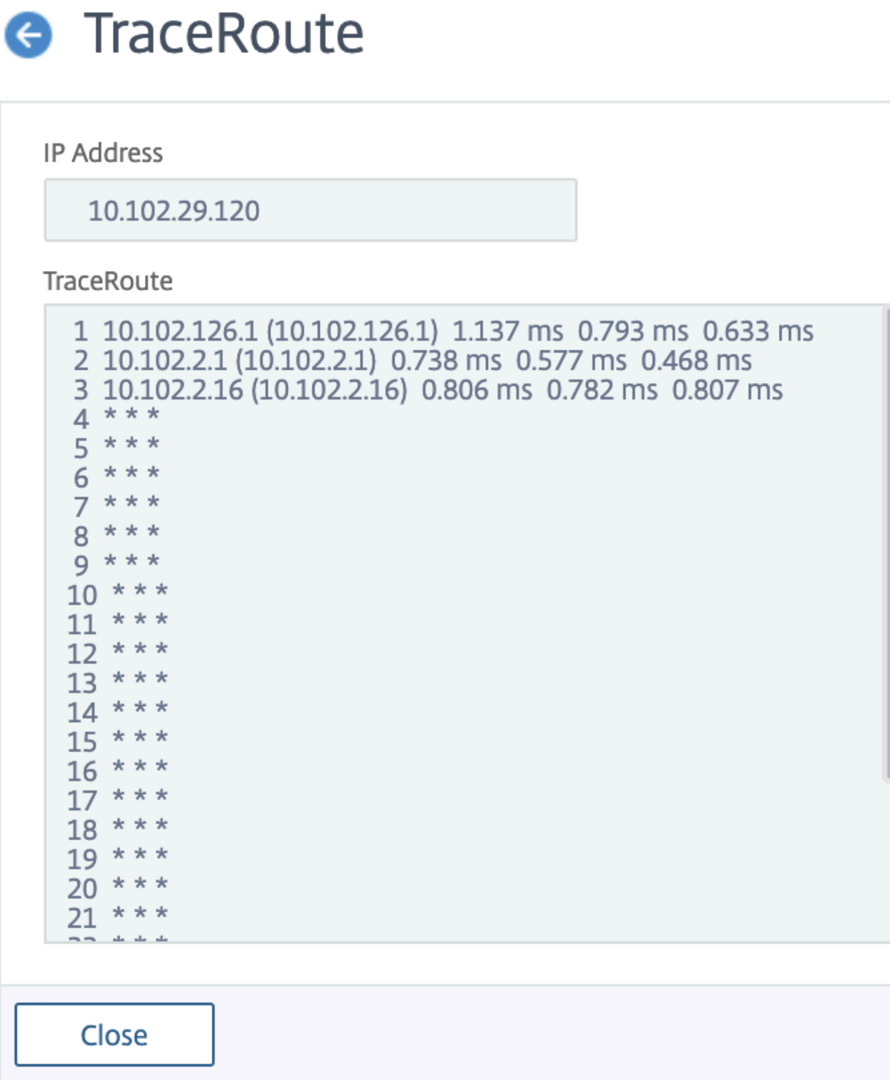
Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, the traceroute shows where the problem exists.

To trace the route of an instance:

1. Navigate to **Infrastructure > Instances > Citrix ADC**.
2. Select the ADC instance tab (for example, VPX).
3. In the list of instances, either right-click an instance and then select **TraceRoute**, or select the instance and, from the **Action** list, click **TraceRoute**.



The TraceRoute message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.



IP Address

10.102.29.120

TraceRoute

```
1  10.102.126.1 (10.102.126.1)  1.137 ms  0.793 ms  0.633 ms
2  10.102.2.1 (10.102.2.1)  0.738 ms  0.577 ms  0.468 ms
3  10.102.2.16 (10.102.2.16)  0.806 ms  0.782 ms  0.807 ms
4  * * *
5  * * *
6  * * *
7  * * *
8  * * *
9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
```

Events

September 24, 2021

When the IP address of a Citrix Application Delivery Controller (Citrix ADC) instance is added to Citrix Application Delivery and Management, Citrix Application Delivery and Management 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 Citrix ADC instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on the Citrix Application Delivery and Management server. Events received in Citrix Application Delivery and Management are displayed on the Events Summary page (**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**).

Citrix Application Delivery and Management also checks on the events generated on instances to form alarms of different severity levels and displays them as messages, some of which might require immediate attention. For example, system failure can be categorized as a "Critical" event severity and can be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor various events generated across your Citrix ADC 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 ADC instances, category, failure objects, configuration commands, and messages.

You can also ensure that multiple notifications are triggered for a specific time interval for an event until the event is cleared. As an extra measure, you might want to customize your email with a specific subject line, user message, and upload an attachment.

Use events dashboard

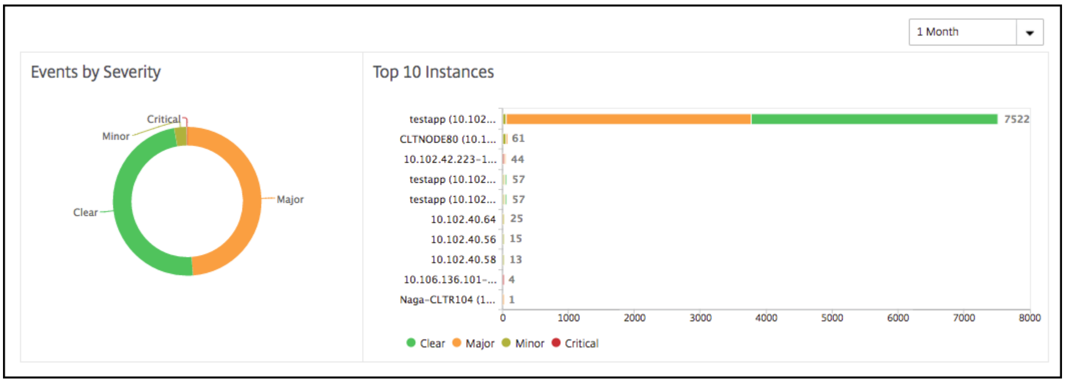
September 28, 2021

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 (Citrix ADC) instances, along with events and their severity on specific instances. You can use the events dashboard of Citrix Application Delivery and Management to view reports generated for critical event severity details on all your Citrix ADC instances.

To view the details on the events dashboard:

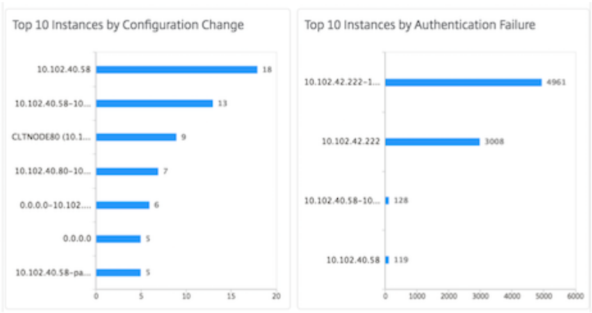
Navigate to **Infrastructure > Events > Reports**.

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.

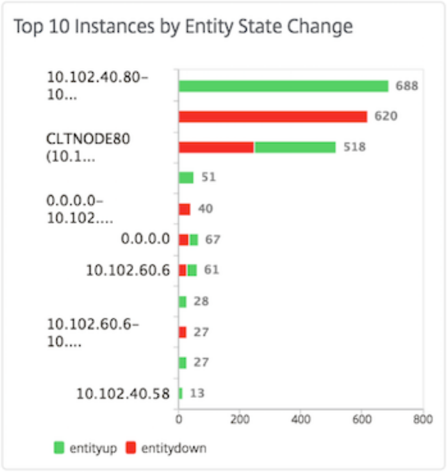


You can view more details by navigating to the Citrix ADC instance type (**Infrastructure > Events > Reports** > **Citrix ADC/ Citrix ADC SDX/ Citrix ADC**) to view the following:

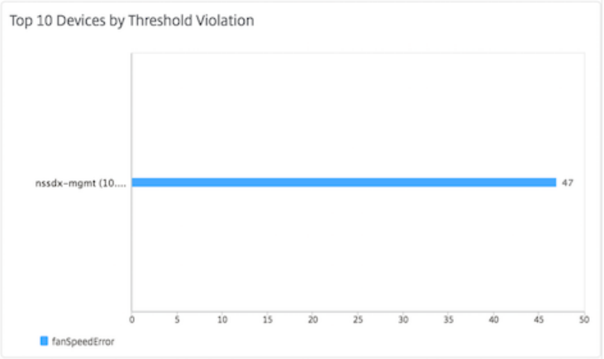
- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure



- Top 10 devices by entity state changes



- Top 10 devices by threshold violation



To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Set event age for events

September 24, 2021

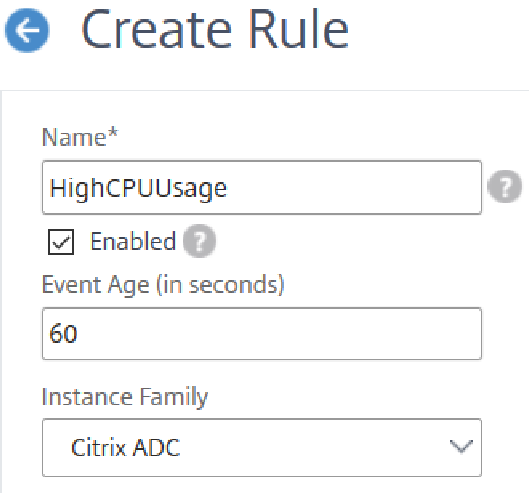
You can set the event age option to specify the time interval (in seconds). Citrix Application Delivery and Management monitors the appliances until the set duration and generates an event only if the event age exceeds the set duration.

> 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 Citrix Application Delivery and Management:

1. In the Citrix Application Delivery and Management, 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.



Create Rule

Name*

HighCPUUsage

☑ Enabled

Event Age (in seconds)

60

Instance Family

Citrix ADC

Schedule an event filter

September 24, 2021

After creating a filter for your rule, if you do not want the Citrix Application Delivery and Management 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.

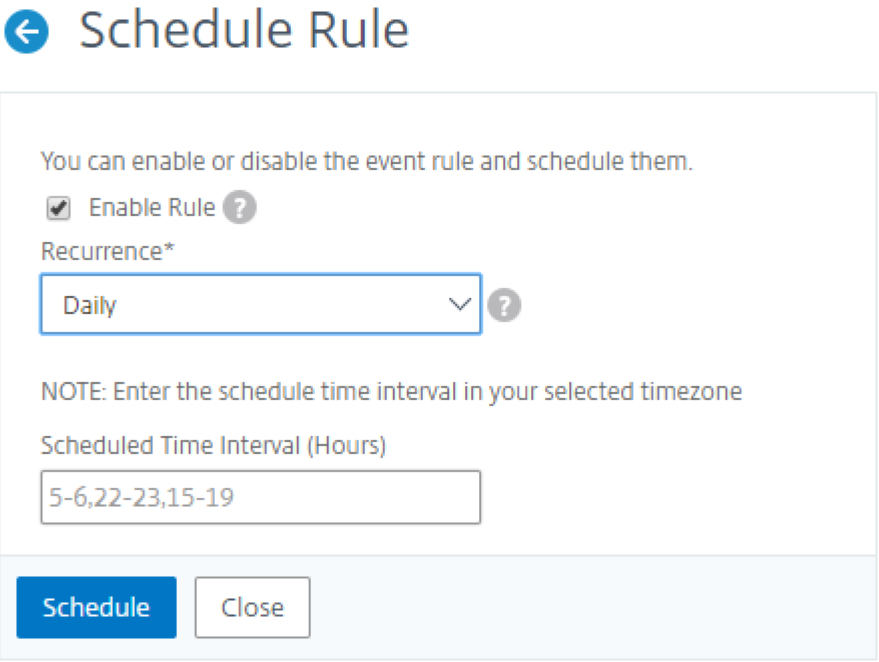
For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends many email notifications when Citrix Application Delivery and Management 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 Citrix Application Delivery and Management:

1. In the Citrix Application Delivery and Management, 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.
   - **Scheduled Time Interval (Hours)** – Hours, at which to schedule the rule (use the 24 hour format).

4. Click **Schedule**.



Schedule Rule

You can enable or disable the event rule and schedule them.

☑ Enable Rule

Recurrence*: Daily

NOTE: Enter the schedule time interval in your selected timezone

Scheduled Time Interval (Hours): 5-6,22-23,15-19

Set repeated email notifications for events

September 24, 2021

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.

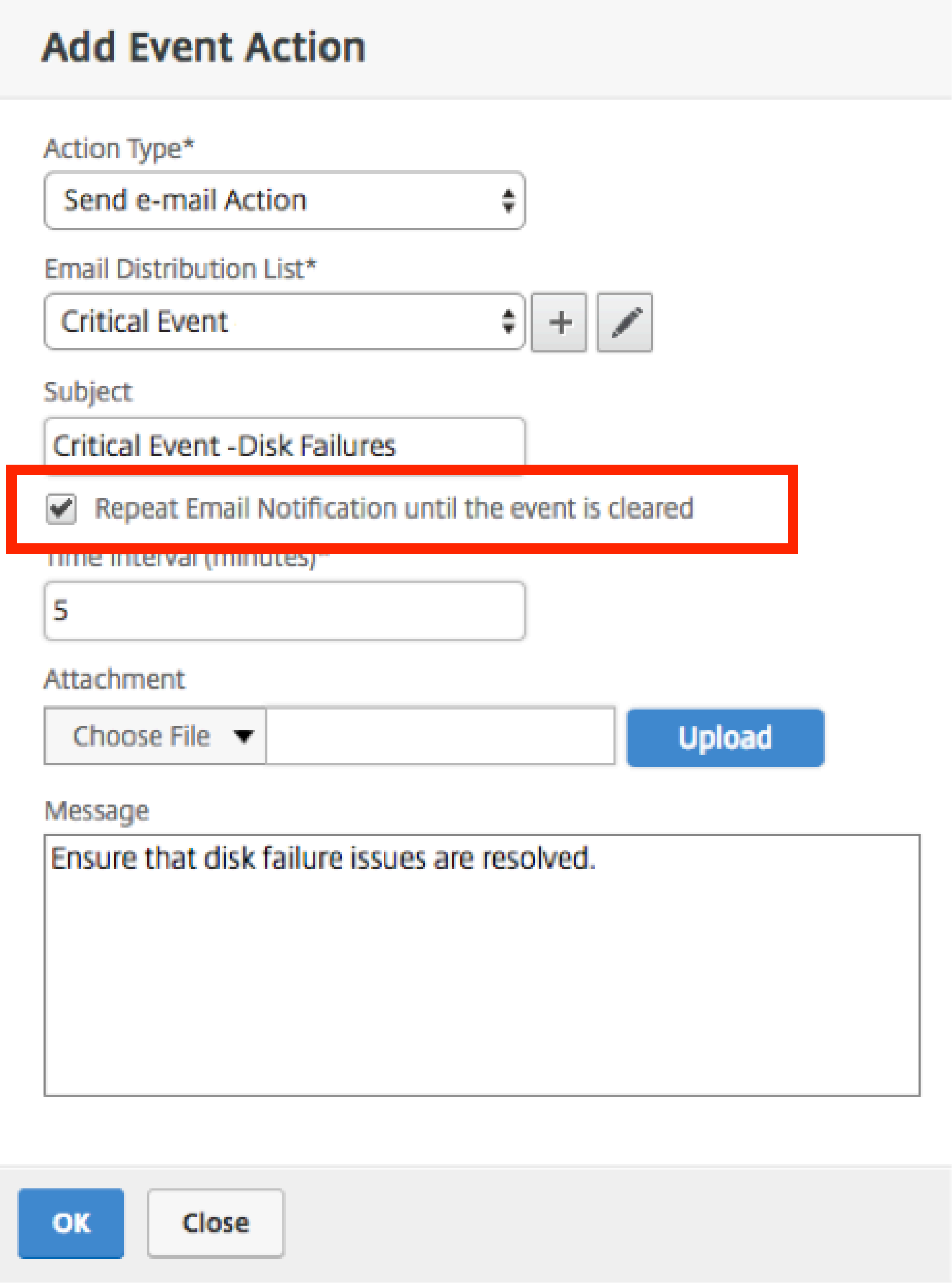
These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

> **Note**
>
> Events can only be cleared automatically if there is an equivalent "clear" trap set and sent from your Citrix ADC instance.
>
> To clear an event manually, you can do the following:
>
> - Navigate to **Infrastructure > Events > Event Summary**, select **Category**, and then 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 following grid and click **Clear**.

To set repeated email notifications from Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, 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.



Add Event Action

Action Type*: Send e-mail Action

Email Distribution List*: Critical Event

Subject: Critical Event -Disk Failures

☑ Repeat Email Notification until the event is cleared

Time Interval (minutes)*: 5

Attachment

Message: Ensure that disk failure issues are resolved.

Suppress events

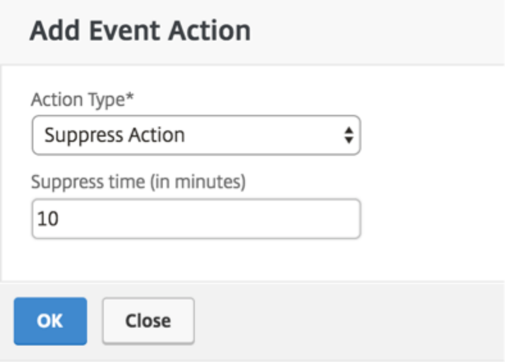
September 24, 2021

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 Citrix Application Delivery and Management considers the suppress time as zero and it never expires.

To suppress events by using Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Events > Rules**.
2. Go to **Create Rule** or **Configure Rule** page. 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 menu and specify the time period, in minutes, for which an event must be suppressed.
5. Click **OK**.



Add Event Action

Action Type*: Suppress Action

Suppress time (in minutes): 10

Create event rules

September 28, 2021

You can configure rules to monitor specific events. Rules make it easier to filter the events generated across your infrastructure.

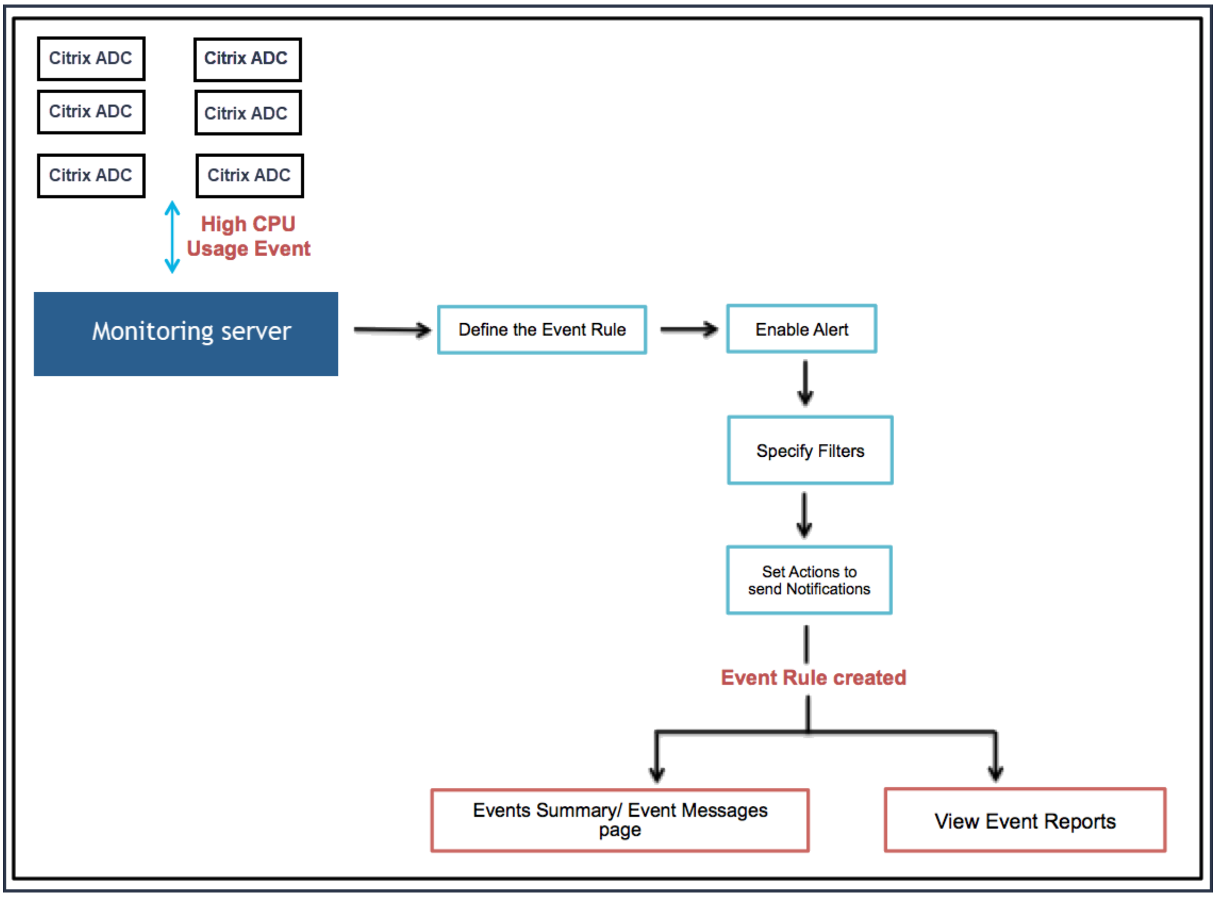
You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, Citrix Application Delivery Controller (Citrix ADC) 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 on ADC instances which might lead to an outage. You can perform any of the following actions to receive notifications:

- Create a rule to monitor instances. And, add an action to the rule to receive notifications when such events occur.
- Schedule a rule to monitor instances at a specific interval. So, you receive notifications when such events occur within that interval.

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 Citrix ADC 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

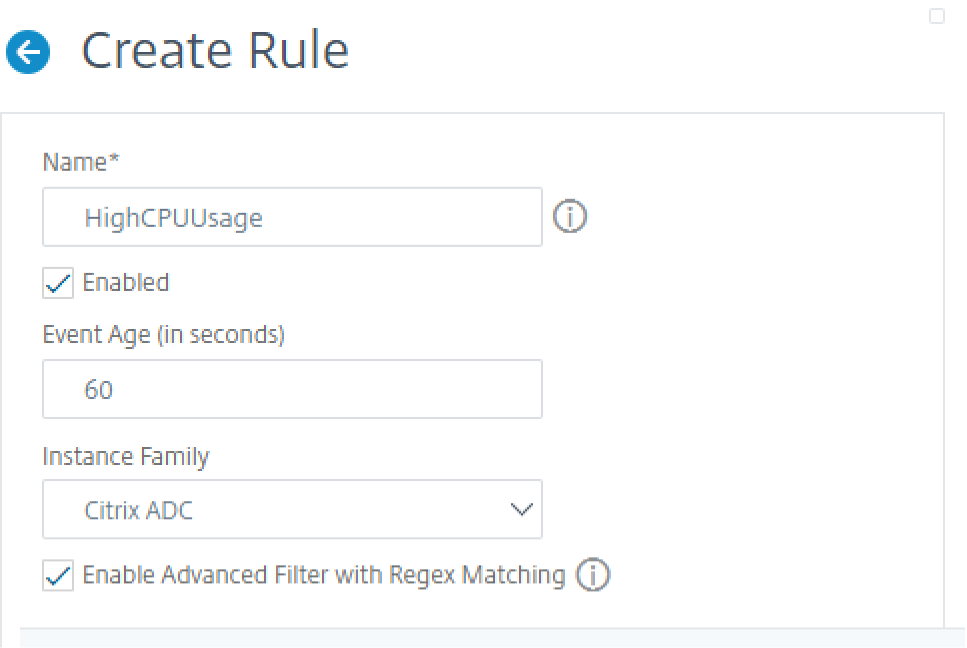
Step 1 - Define an event rule

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 Citrix Application Delivery and Management 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 Citrix ADC 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 Citrix ADC instance has a "high CPU usage" event for 60 seconds or more, you receive an email notification with details of the event.



Create Rule

Name*: HighCPUUsage

☑ Enabled

Event Age (in seconds): 60

Instance Family: Citrix ADC

☑ Enable Advanced Filter with Regex Matching

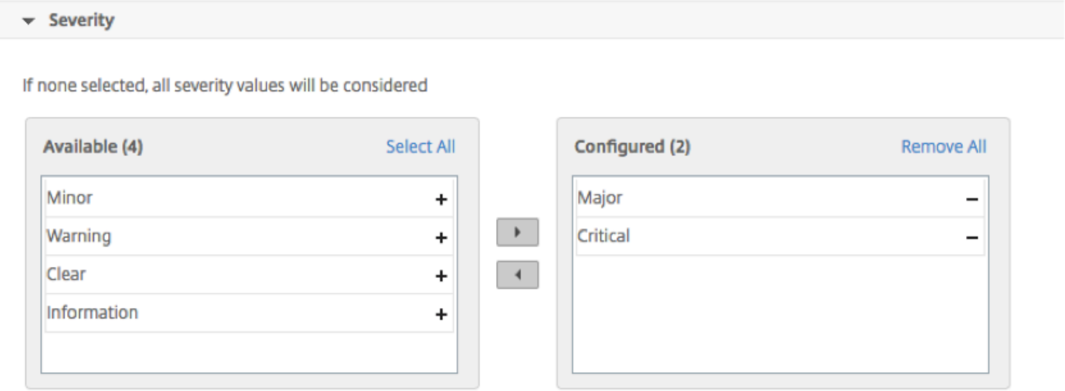
You can also filter event rules by **Instance Family** to track the Citrix ADC instance from which Citrix Application Delivery and Management receives an event.

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 which you want to add the event rule.

You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.

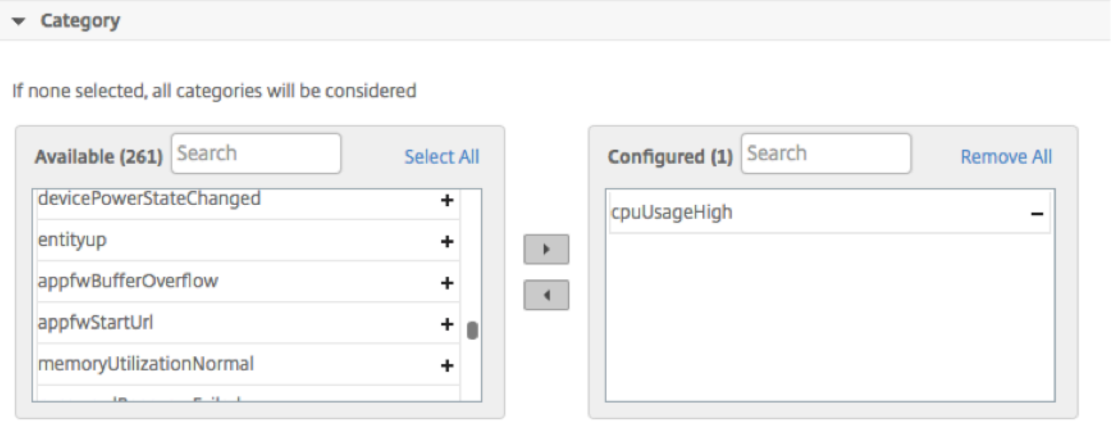


> **Note**
>
> You can configure severity for both generic and Advanced-specific events. To modify event severity for Citrix ADC instances managed on Citrix Application Delivery and Management, navigate to **Infrastructure > Events > Event Settings**. Choose the **Category** for which you want to configure event severity and click **Configure Severity**. Assign a new severity level and click **OK**.

Step 3 - Specify the event category

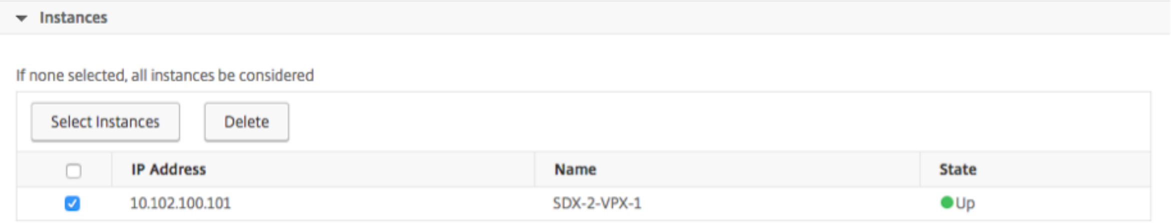
You can specify the category or categories of the events generated by your Citrix ADC instances. All categories are created on Citrix ADC instances. These categories are then mapped with the Citrix Application Delivery and Management that can be used to define event rules. Select the category you want 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 Citrix ADC instances

Select the IP addresses of the Citrix ADC 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**.



If none selected, all instances be considered

□	IP Address	Name	State
☑	10.102.100.101	SDX-2-VPX-1	● Up

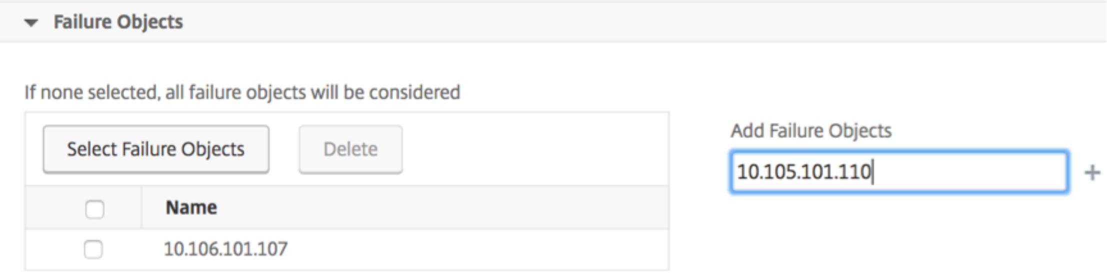
Step 5 - Select failure objects

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 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.



If none selected, all failure objects will be considered

□	Name
□	10.106.101.107

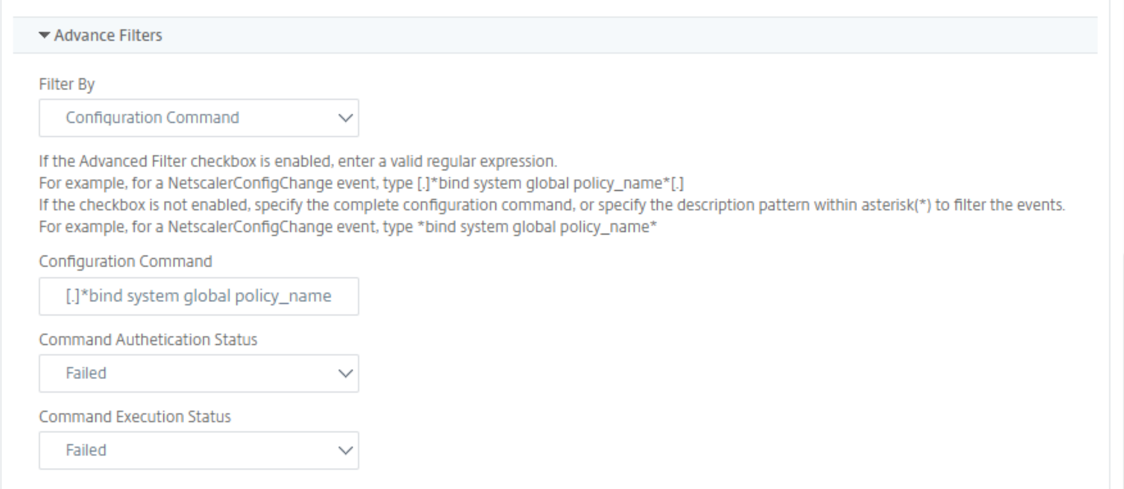
Add Failure Objects: 10.105.101.110

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[.]*`.



Filter By: Configuration Command

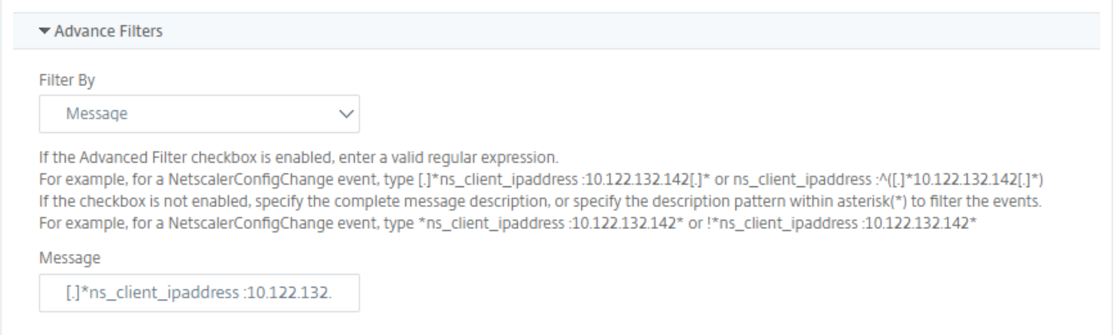
If the Advanced Filter checkbox is enabled, enter a valid regular expression.
For example, for a NetscalerConfigChange event, type [.]*bind system global policy_name*[.]
If the checkbox is not enabled, specify the complete configuration command, or specify the description pattern within asterisk(*) to filter the events.
For example, for a NetscalerConfigChange event, type *bind system global policy_name*

Configuration Command: [.]*bind system global policy_name

Command Authetication Status: Failed

Command Execution Status: Failed

- **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[.]*)`.



Filter By: Message

If the Advanced Filter checkbox is enabled, enter a valid regular expression.
For example, for a NetscalerConfigChange event, type [.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)
If the checkbox is not enabled, specify the complete message description, or specify the description pattern within asterisk(*) 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*

Message: [.]*ns_client_ipaddress :10.122.132.

> **Important**
>
> To filter configuration commands and messages using regular expression other than asterisk (*) pattern matching, select **Enable Advanced Filter with Regex Matching** in Step 1.

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

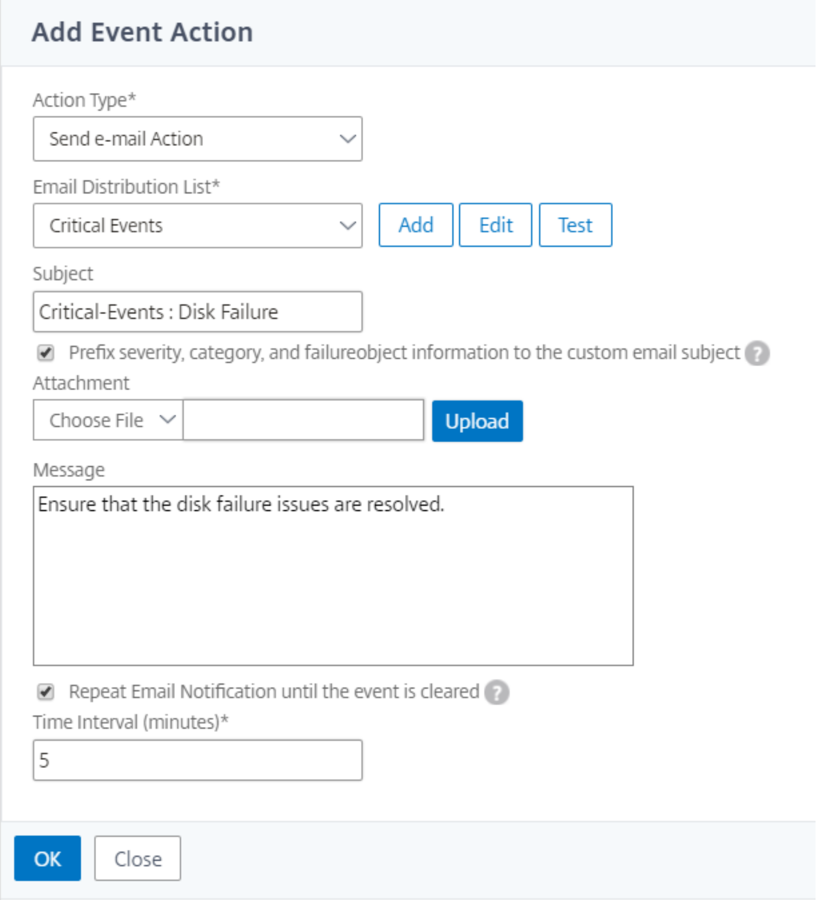
When you choose **Send e-mail Action**, an email is triggered when the events meet the defined filter criteria. You must either create an email distribution list by providing mail server or mail profile details or you can select an email distribution list that you've previously created.

Due to a high number of virtual servers being configured in Citrix Application Delivery and Management, 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, that is the 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.



Add Event Action

Action Type*: Send e-mail Action

Email Distribution List*: Critical Events

Subject: Critical-Events : Disk Failure

☑ Prefix severity, category, and failureobject information to the custom email subject

Attachment

Message: Ensure that the disk failure issues are resolved.

☑ Repeat Email Notification until the event is cleared

Time Interval (minutes)*: 5

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 a specific trap listener 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 Citrix Application Delivery and Management 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 the 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 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 Citrix Application Delivery and Management, 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 the Citrix Application Delivery and Management agent. For example, `/var`.
- Provide the .sh file location in Citrix Application Delivery and Management 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

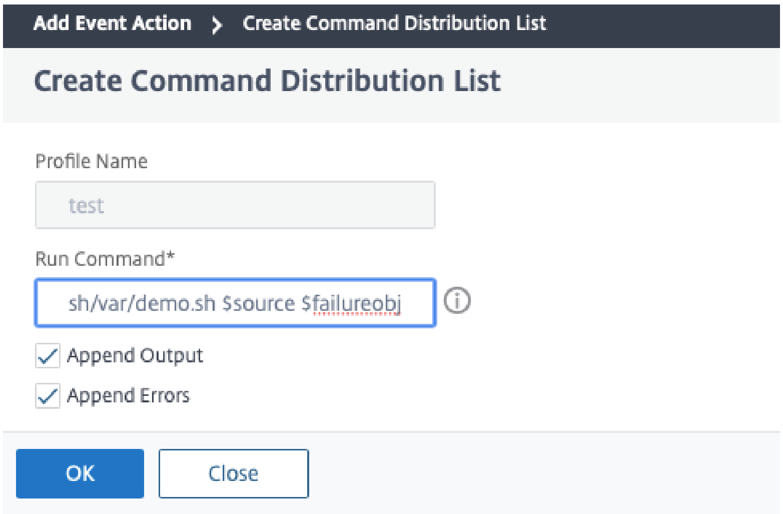
   b) In **Run Command**, specify the Citrix Application Delivery and Management agent location, where the script has to run. For example: `/sh/var/demo.sh $source $failureobj`.

   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 Citrix Application Delivery and Management server log files. If you do not enable these options, Citrix Application Delivery and Management discards all outputs and errors generated while running the command script.

   d) Click **Create**.

8. In the **Add Event Action** page, click **OK**.



Add Event Action > Create Command Distribution List
Create Command Distribution List
Profile Name
Run Command*
OK
Close

Profile Name: test

Run Command*: sh/var/demo.sh $source $failureobj

☑ Append Output

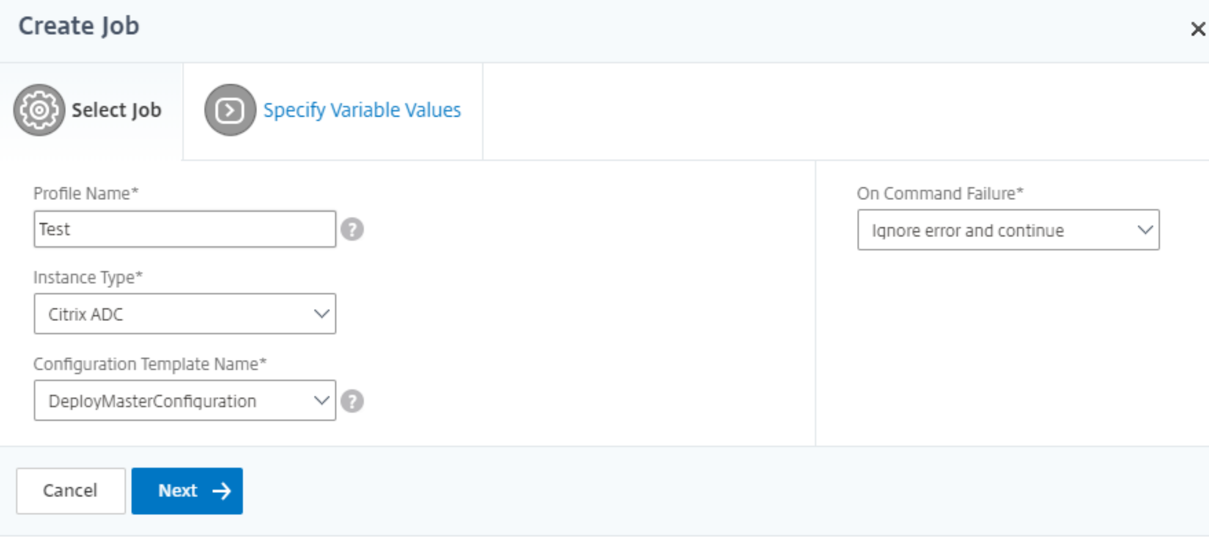
☑ Append Errors

> **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 Citrix Application Delivery and Management server log files. If you do not enable these options, Citrix Application Delivery and Management 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 Citrix ADC, and Citrix ADC 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** list.
2. Create a profile with a job 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.



Profile Name*: Test

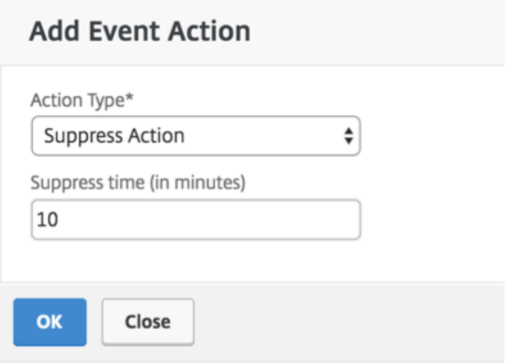
Instance Type*: Citrix ADC

Configuration Template Name*: DeployMasterConfiguration

On Command Failure*: Ignore error and continue

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.



Action Type*: Suppress Action

Suppress time (in minutes): 10

To set Slack notifications from Citrix Application Delivery and Management

Configure the required Slack channel by providing the profile name and the webhook URL in the Citrix Application Delivery and Management GUI. The event notifications are then sent to this channel. You can configure multiple Slack channels to receive these notifications

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > 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 you want to monitor.
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 Citrix Application Delivery and Management

    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 **Account** > **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 Citrix Application Delivery and Management

You can add a PagerDuty profile as an option in Citrix Application Delivery and Management 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 a registered number.

Before you add a PagerDuty profile in Citrix Application Delivery and Management, ensure you have completed the required configurations in PagerDuty. For more information, see PagerDuty documentation.

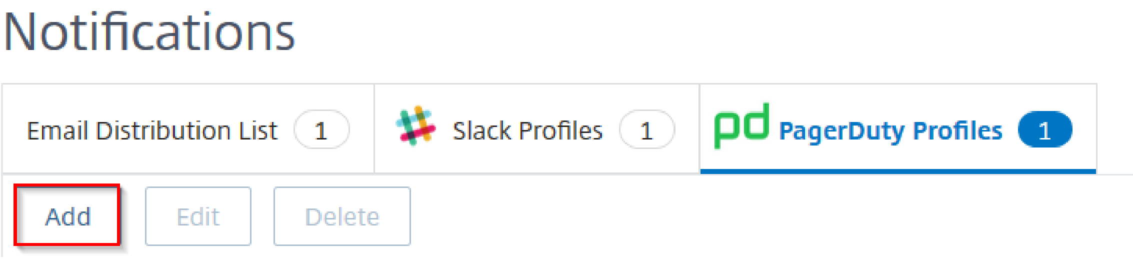
You can select your PagerDuty profile as one of the options to get notifications for the following features:

- **Events** – List of events that are generated for Citrix ADC 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 Citrix ADC instances.

To add a PagerDuty profile in Citrix Application Delivery and Management:

1. Log on to Citrix Application Delivery and Management using administrator credentials.
2. Navigate to **Account** > **Notifications** > **PagerDuty Profiles**.

3. Click **Add** to create a profile.



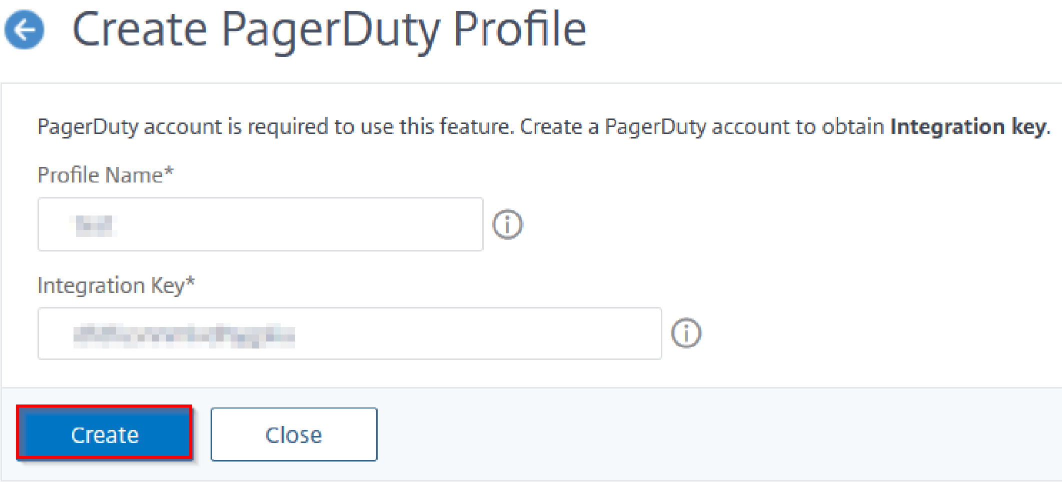
4. In the Create PagerDuty Profile page:

   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**.



PagerDuty account is required to use this feature. Create a PagerDuty account to obtain **Integration key**.

Profile Name*

Integration Key*

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 Citrix ADC events.

To configure:

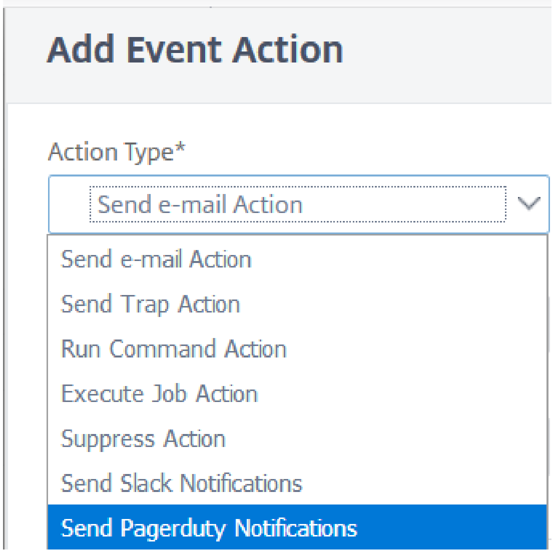
a) Navigate to **Events** > **Rules**

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.

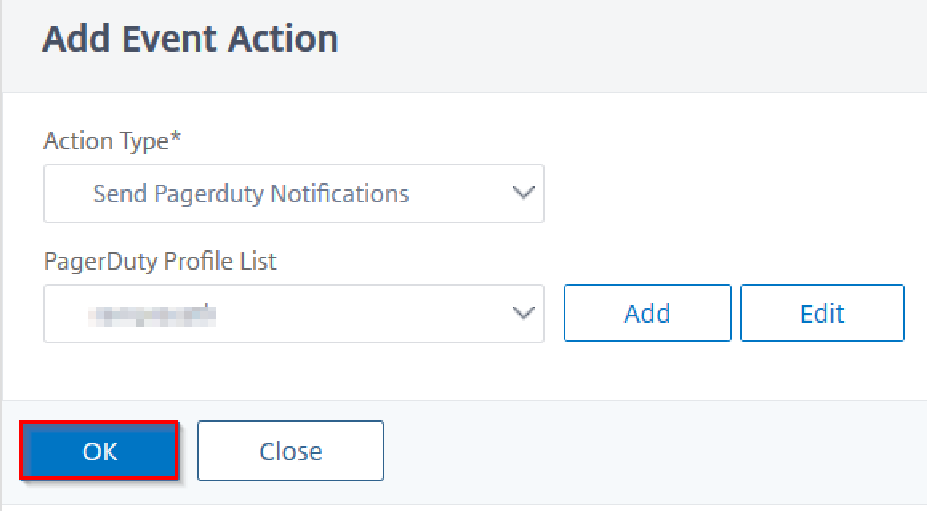
i. Under **Action Type**, select **Send PagerDuty Notifications**.



Add Event Action

Action Type*: Send e-mail Action

ii. Select your PagerDuty profile and click **OK**.



Add Event Action

Action Type*: Send Pagerduty Notifications

PagerDuty Profile List: [redacted]

After the configuration is complete, whenever a new event is generated for the Citrix ADC 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 Citrix Application Delivery and Management

You can auto-generate ServiceNow incidents for Citrix Application Delivery and Management events by selecting the ServiceNow profile on the Citrix Application Delivery and Management GUI. You must choose the **ServiceNow** profile in Citrix Application Delivery and Management to configure an event rule.

Before you configure an event rule to auto-generate ServiceNow incidents, integrate the Citrix Application Delivery and Management with the ServiceNow instance. For more information, see Configure ITSM adapter for ServiceNow.

To configure an event rule, navigate to **Events** > **Rules**.

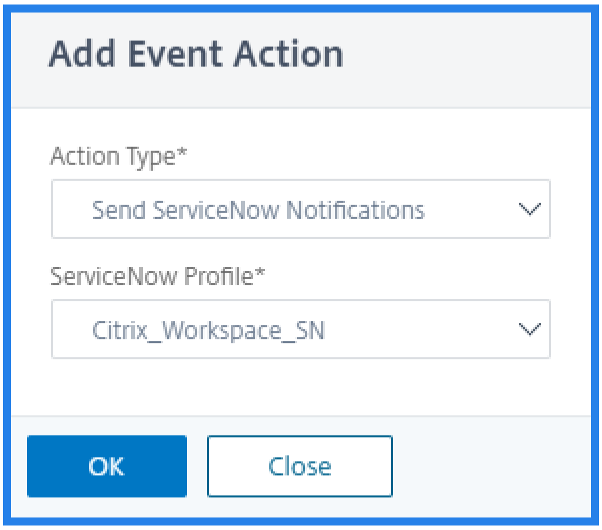
1. On the **Create Rule** page, configure all other parameters to create a rule.
2. Under **Create Rule Actions**, click **Add Action**.

   The **Add Event Action** page is displayed.

   a) In **Action Type**, select **Send ServicNow Notifications**.

   b) In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.

   c) Click **OK**.



Add Event Action

Action Type*: Send ServiceNow Notifications

ServiceNow Profile*: Citrix_Workspace_SN

Modify the reported severity of events that occur on Citrix ADC instances

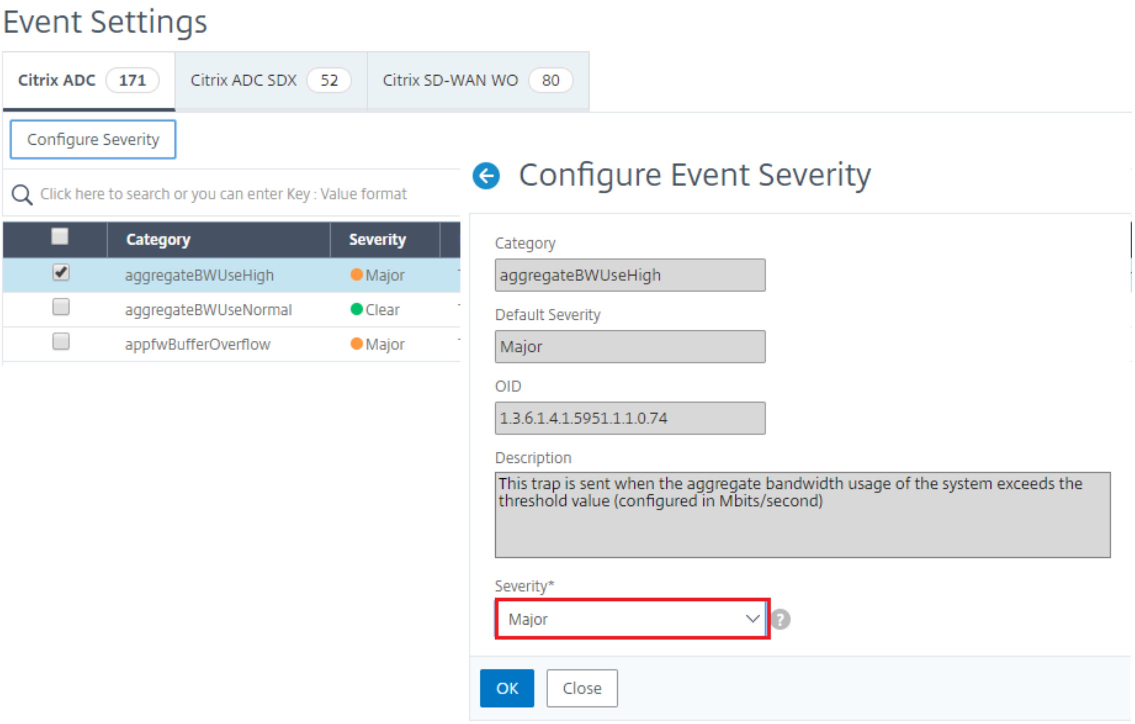
September 23, 2021

You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on an instance and view reports based on event severity. Also, 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 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**.



Event Settings

	Category	Severity
☑	aggregateBWUseHigh	● Major
□	aggregateBWUseNormal	● Clear
□	appfwBufferOverflow	● Major

Configure Event Severity

Category: aggregateBWUseHigh

Default Severity: Major

OID: 1.3.6.1.4.1.5951.1.1.0.74

Description: This trap is sent when the aggregate bandwidth usage of the system exceeds the threshold value (configured in Mbits/second)

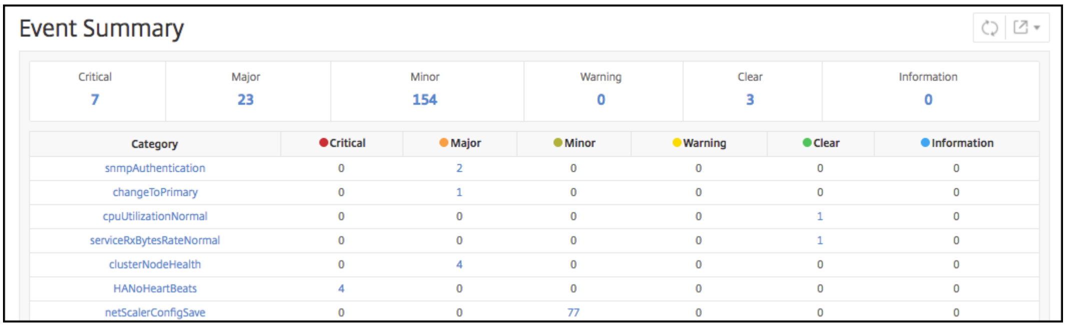
Severity*: Major

View events summary

September 25, 2021

You can now view an Events Summary page to monitor the events and traps received on your Citrix Application Delivery and Management. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by Citrix Application Delivery and Management**. 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 (Citrix ADC) instance goes down and stops sending information to the Citrix Application Delivery and Management. During the event, a notification is sent to an administrator, explaining the reason for 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 the summary and access the details of the event.



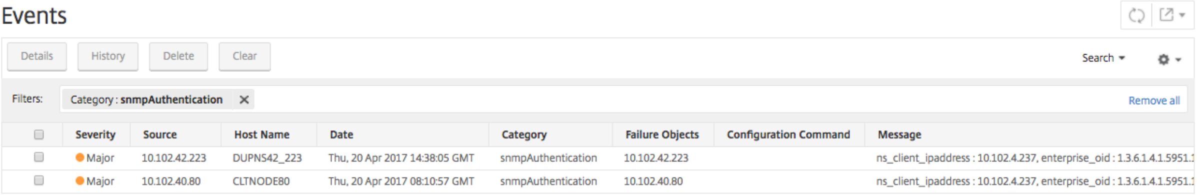
Event Summary

Critical	Major	Minor	Warning	Clear	Information
7	23	154	0	3	0

Category	● Critical	● Major	● Minor	● Warning	● Clear	● Information
snmpAuthentication	0	2	0	0	0	0
changeToPrimary	0	1	0	0	0	0
cpuUtilizationNormal	0	0	0	0	1	0
serviceRxBytesRateNormal	0	0	0	0	1	0
clusterNodeHealth	0	4	0	0	0	0
HANoHeartBeats	4	0	0	0	0	0
netScalerConfigSave	0	0	77	0	0	0

- **Number of traps received for each category**. The number of traps received, categorized by severity. By default, each trap sent from Citrix ADC instances to Citrix Application Delivery and Management has an assigned severity, but as the network administrator, you can specify its severity in the Citrix Application Delivery and Management 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 IP address and host name of a Citrix ADC instance, date on which the trap was received, category, failure objects, configuration command run, and the message notification.



Events

Filters: Category : snmpAuthentication

□	Severity	Source	Host Name	Date	Category	Failure Objects	Configuration Command	Message
□	● Major	10.102.42.223	DUPNS42_223	Thu, 20 Apr 2017 14:38:05 GMT	snmpAuthentication	10.102.42.223		ns_client_ipaddress : 10.102.4.237, enterprise_oid : 1.3.6.1.4.1.5951.1
□	● Major	10.102.40.80	CLTNODE80	Thu, 20 Apr 2017 08:10:57 GMT	snmpAuthentication	10.102.40.80		ns_client_ipaddress : 10.102.4.237, enterprise_oid : 1.3.6.1.4.1.5951.1

You can configure the number of days between 1 and 40, for which you want to view the events in Citrix Application Delivery and Management. For example, if you select 30 days, Citrix Application Delivery and Management displays the events for 30 days and after 30 days, the events are cleared. To configure this event setting, navigate to **Settings > Global Settings > Data Rentention Policy**. For more information, see Data retention policy.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Display event severities and SNMP trap details

September 24, 2021

When you create an event and its settings in Citrix Application Delivery and Management, 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 (Citrix ADC) instances added to your Citrix Application Delivery and Management 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 Citrix ADC 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 Citrix ADC 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 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 others. You can also select the instance and see the instance dashboard for more details.

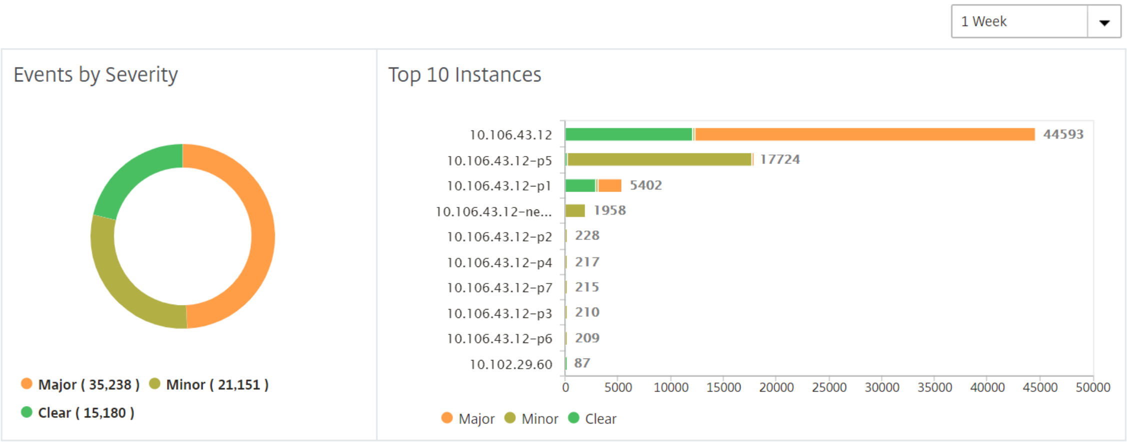
To select specific events by severity in Citrix Application Delivery and Management:

1. Log on to Citrix Application Delivery and Management, using your administrator credentials.
2. Navigate to **Infrastructure > Instances**.

   Or,

Navigate to **Infrastructure > Events > Reports**.

3. From the drop-down list in the upper-right corner of the page, select the duration for which you want to see events by severity.

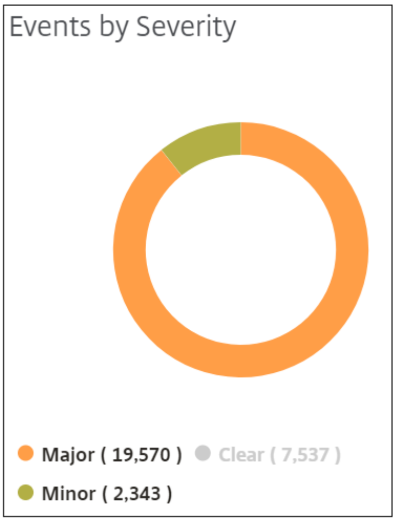


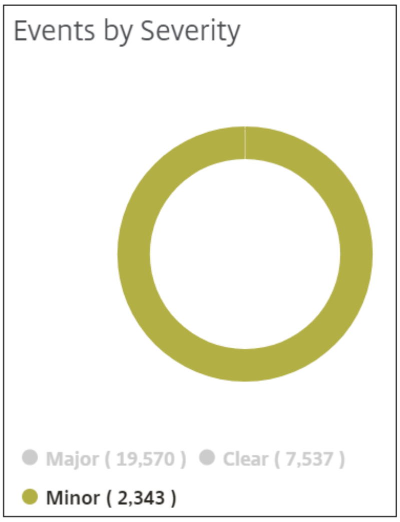
4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.

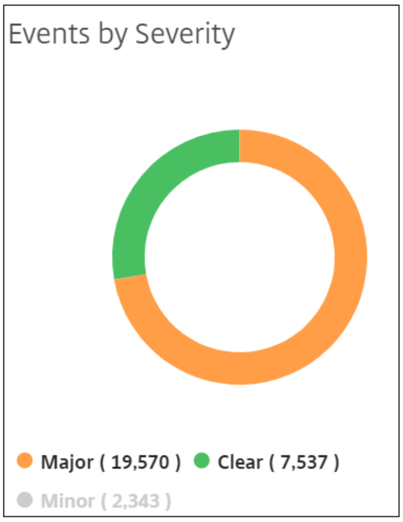
5. You can click each section on the donut chart to display the corresponding **Severity based events** page, which shows the following details for the selected severity for the selected duration:

   - Instance Source
   - Data of the event
   - Category of events generated by the Citrix ADC 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 view and monitor your chosen severity more easily.





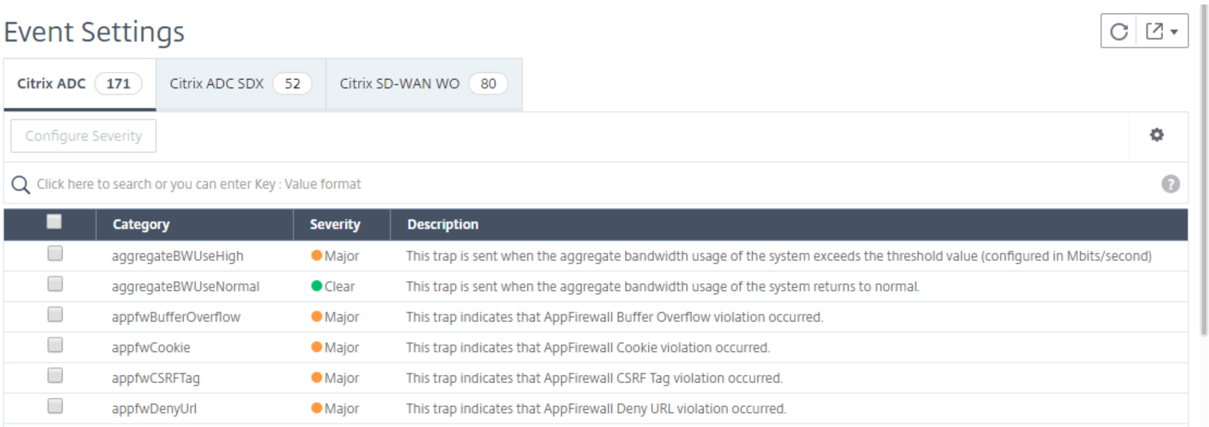


To view Citrix ADC SNMP trap details on Citrix Application Delivery and Management:

You can now view the details of each SNMP trap received from its managed Citrix ADC instances on the Citrix Application Delivery and Management 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."



□	Category	Severity	Description
□	aggregateBWUseHigh	● Major	This trap is sent when the aggregate bandwidth usage of the system exceeds the threshold value (configured in Mbits/second)
□	aggregateBWUseNormal	● Clear	This trap is sent when the aggregate bandwidth usage of the system returns to normal.
□	appfwBufferOverflow	● Major	This trap indicates that AppFirewall Buffer Overflow violation occurred.
□	appfwCookie	● Major	This trap indicates that AppFirewall Cookie violation occurred.
□	appfwCSRFTag	● Major	This trap indicates that AppFirewall CSRF Tag violation occurred.
□	appfwDenyUrl	● Major	This trap indicates that AppFirewall Deny URL violation occurred.

View and Export syslog messages

September 28, 2021

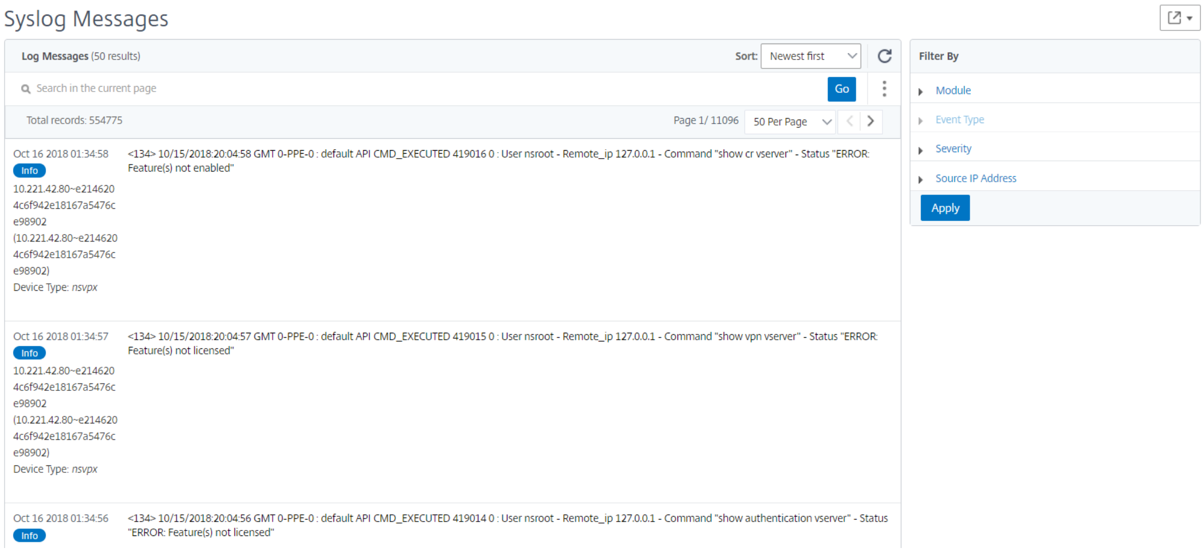
You can view syslog messages without logging into Citrix Application Delivery and Management, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your Citrix Application Delivery Controller (Citrix ADC) instances in PDF, CSV, PNG, and JPEG formats. Also, you can schedule the export of these reports to specified email addresses at various intervals.

View syslog messages

You can view all your syslog messages generated on your managed Citrix ADC instances. To view the messages you must configure the instances to redirect the syslog messages to the Citrix Application Delivery and Management server. The syslog messages are stored in the database centrally and are available on the Syslog Viewer for auditing purposes. You can combine this logging information and derive reports for analytics from the collected data.

You can also configure syslog to log different types of events.

To view the Syslog Viewer, navigate to **Infrastructure > Events > Syslog Messages**. Choose the appropriate filters, to view your System Log messages.

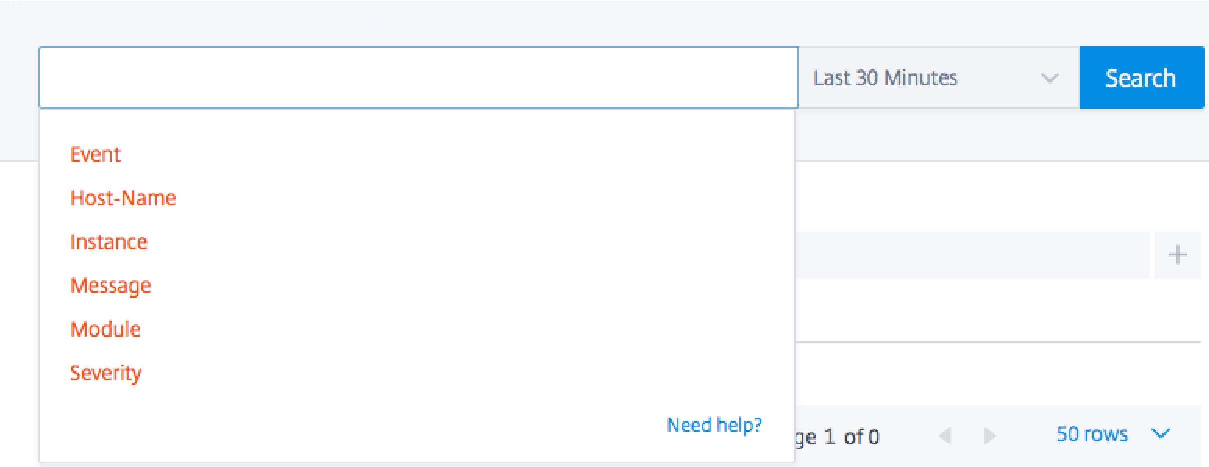


```
Oct 16 2018 01:34:58
Info
10.221.42.80~e214620
4c6f942e18167a5476c
e98902
(10.221.42.80~e214620
4c6f942e18167a5476c
e98902)
Device Type: nsvpx
<134> 10/15/2018:20:04:58 GMT 0-PPE-0 : default API CMD_EXECUTED 419016 0 : User nsroot - Remote_ip 127.0.0.1 - Command "show cr vserver" - Status "ERROR: Feature(s) not enabled"

Oct 16 2018 01:34:57
Info
10.221.42.80~e214620
4c6f942e18167a5476c
e98902
(10.221.42.80~e214620
4c6f942e18167a5476c
e98902)
Device Type: nsvpx
<134> 10/15/2018:20:04:57 GMT 0-PPE-0 : default API CMD_EXECUTED 419015 0 : User nsroot - Remote_ip 127.0.0.1 - Command "show vpn vserver" - Status "ERROR: Feature(s) not licensed"

Oct 16 2018 01:34:56
Info
<134> 10/15/2018:20:04:56 GMT 0-PPE-0 : default API CMD_EXECUTED 419014 0 : User nsroot - Remote_ip 127.0.0.1 - Command "show authentication vserver" - Status "ERROR: Feature(s) not licensed"
```

Search syslog messages

You can use filters to search syslog messages and audit log messages to narrow down your results and find exactly what you are looking for and in real time.

To search syslog messages for all ADC instances present in the Citrix Application Delivery and Management software, from the Citrix Application Delivery and Management GUI, navigate to **Infrastructure > Events > Syslog Messages**. The new filter categories are instance, module, event, severity, and message.



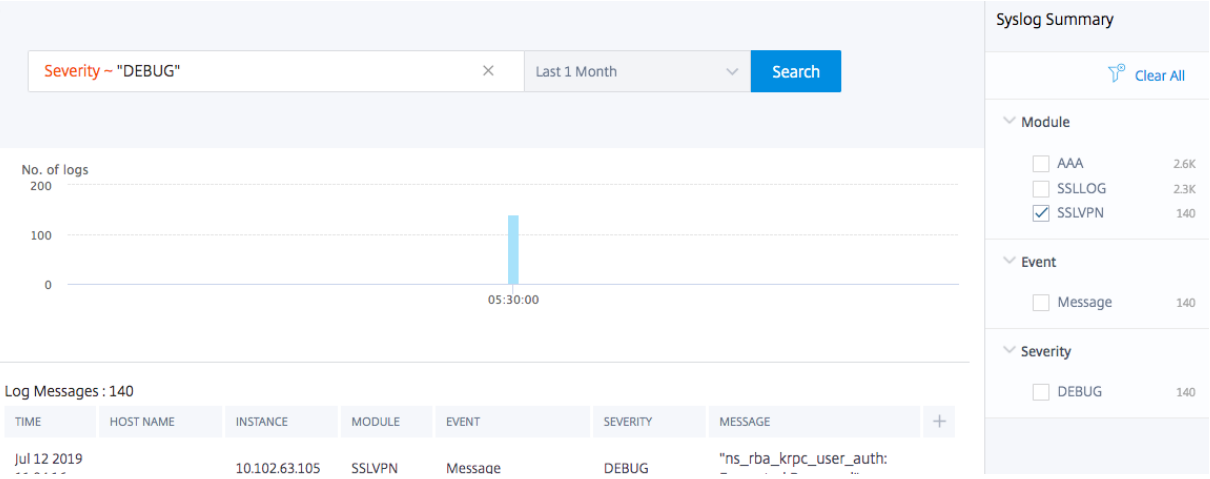
To search all Citrix Application Delivery and Management system audit log messages present in the Citrix Application Delivery and Management software, from the Citrix Application Delivery and Management GUI, navigate to **Settings > Audit Log Messages**. The new filter categories are instance, module, event, severity, and message.

To search audit log messages for all applications present in the Citrix Application Delivery and Management, from the Citrix Application Delivery and Management GUI, navigate to **Infrastructure > Network Functions > Auditing**.

To search the audit log messages for a specific application on the Citrix Application Delivery and Management, from the Citrix Application Delivery and Management GUI, navigate to **Application > Dashboard** and select the virtual server for which you want search the audit log messages. Next, click the **Audit Log** tab.

After you select a filter category, specify if it equals to or contains the search term.

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** or **Audit Log Summary** pane.



Severity ~ "DEBUG" | Last 1 Month

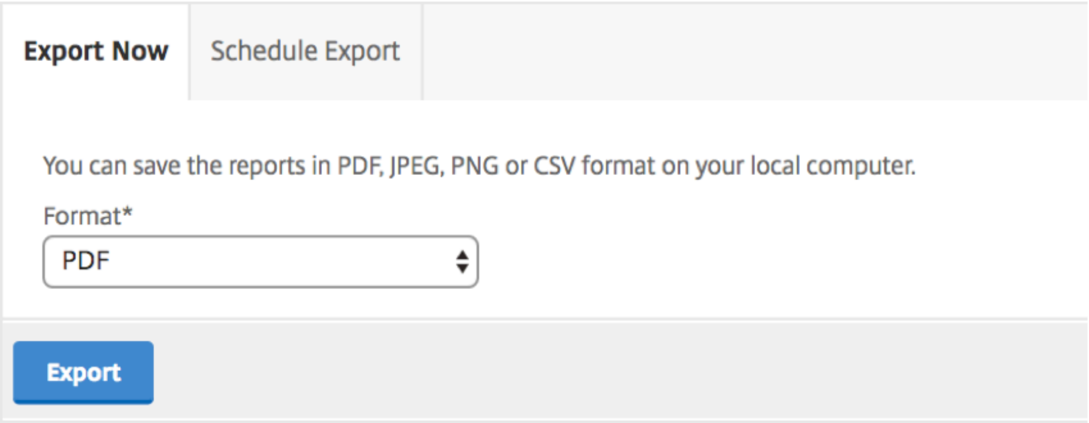
Log Messages : 140

TIME	HOST NAME	INSTANCE	MODULE	EVENT	SEVERITY	MESSAGE
Jul 12 2019		10.102.63.105	SSLVPN	Message	DEBUG	"ns_rba_krpc_user_auth:

Export syslog messages

To export a syslog messages report by using Citrix Application Delivery and Management:

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. In the right pane, click the export button at the top right corner of the Syslog Messages page.
3. Under **Export Now**, select the required format, and then click **Export**.



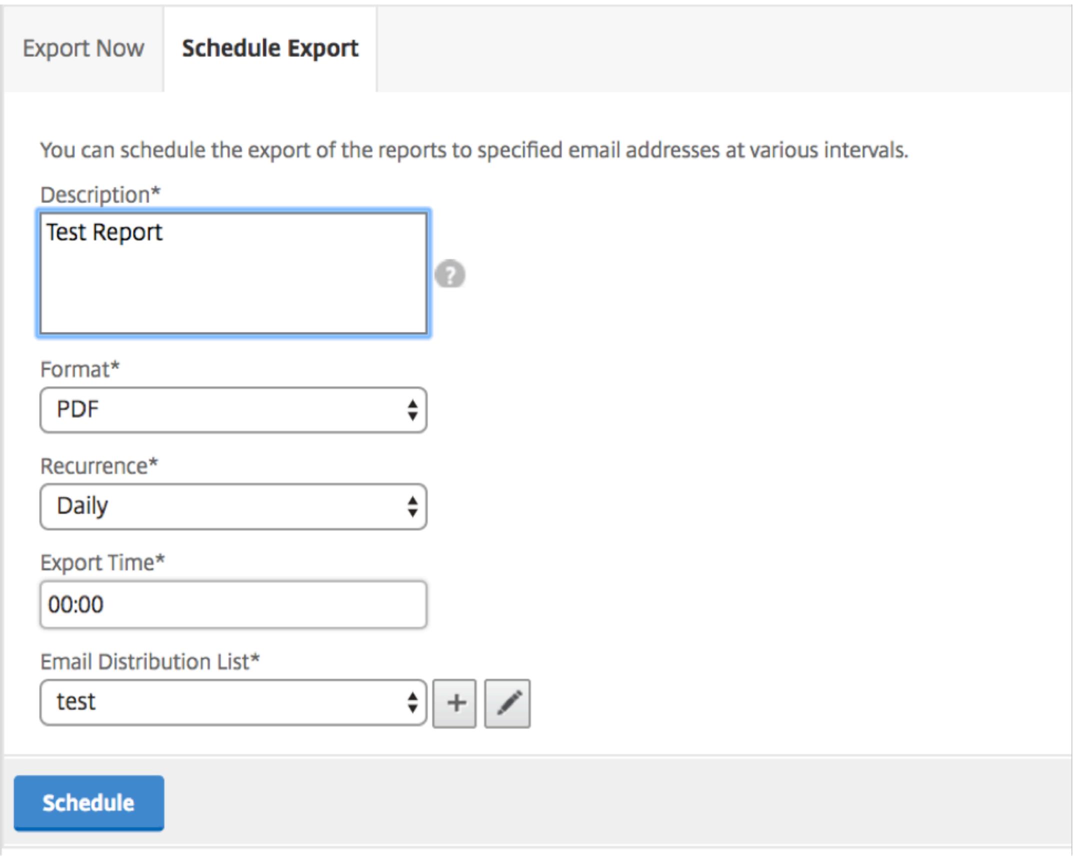
You can save the reports in PDF, JPEG, PNG or CSV format on your local computer.

Format*: PDF

To schedule the export of syslog messages report by using Citrix Application Delivery and Management:

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. On the **Syslog Messages** page, in the right pane, click **Export**.
3. Under the **Schedule Report** tab, set the following parameters:
   - **Description**: Message describing the reason for exporting the report.
   - **Format**: Format in which to export the report.

- **Recurrence**: Interval at which to export the report.
- **Export Time**: Time at which to export the report. Enter the time in a 24 hour format, for your local time zone.
- **Email Distribution List**: List of recipients to receive the report by email. Choose an email distribution list from the list provided. An email is triggered when the report is generated and meets the scheduled time criteria. If you want to create an email distribution list, click **+** and provide mail server and mail profile details.



You can schedule the export of the reports to specified email addresses at various intervals.

Description*: Test Report

Format*: PDF

Recurrence*: Daily

Export Time*: 00:00

Email Distribution List*: test

Suppress syslog messages

September 24, 2021

When configured as a syslog server, Citrix Application Delivery and Management receives all syslog messages from the configured Citrix Application Delivery Controller (Citrix ADC) instances. There might be many messages that you might not want to see. For example, you might not be interested in seeing all the 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 Citrix Application Delivery and Management by setting up some filters. Citrix Application Delivery and Management drops all messages that match with the criteria. These dropped messages do not appear on the Citrix Application Delivery and Management GUI and these messages are also not stored in the customer's Citrix Application Delivery and Management database.

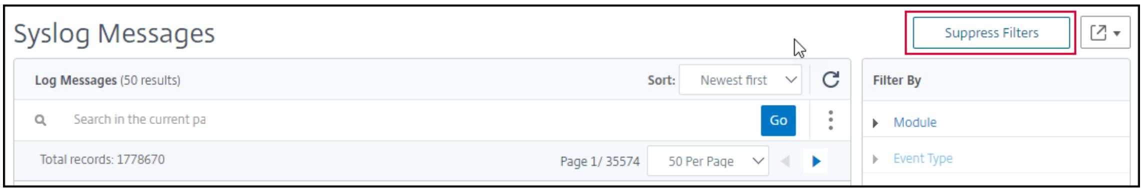
You can suppress some of the logged syslog messages coming into Citrix Application Delivery and Management by setting up some filters. The two filters that can be used for suppressing syslog messages are severity and facility. You can also suppress messages coming from a particular Citrix ADC instance or multiple instances. You can also provide a text pattern for Citrix Application Delivery and Management to search and suppress messages. Citrix Application Delivery and Management drops all messages that match with the criteria. These dropped messages do not appear on the Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, navigate to **Infrastructure > Events > Syslog Messages**.
2. Click **Suppress Filters**.



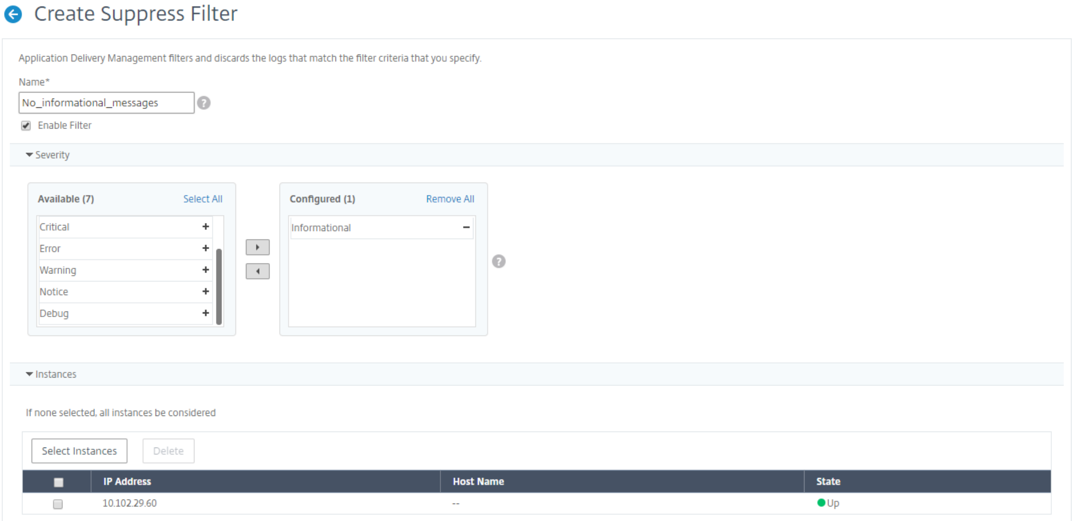
3. On the **Suppress Filters** page, click **Add**.
4. On **Create Suppress Filter** page, update the following information:

   a) **Name** - type a name for the filter.

   > **Note**
   >
   > If different users have different access to multiple Citrix ADC 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 Citrix ADC instances on which the syslog messages have been configured.



Create Suppress Filter

Application Delivery Management filters and discards the logs that match the filter criteria that you specify.

Name*: No_informational_messages

☑ Enable Filter

Severity

Available (7)	Configured (1)
Critical	Informational
Error	
Warning	
Notice	
Debug	

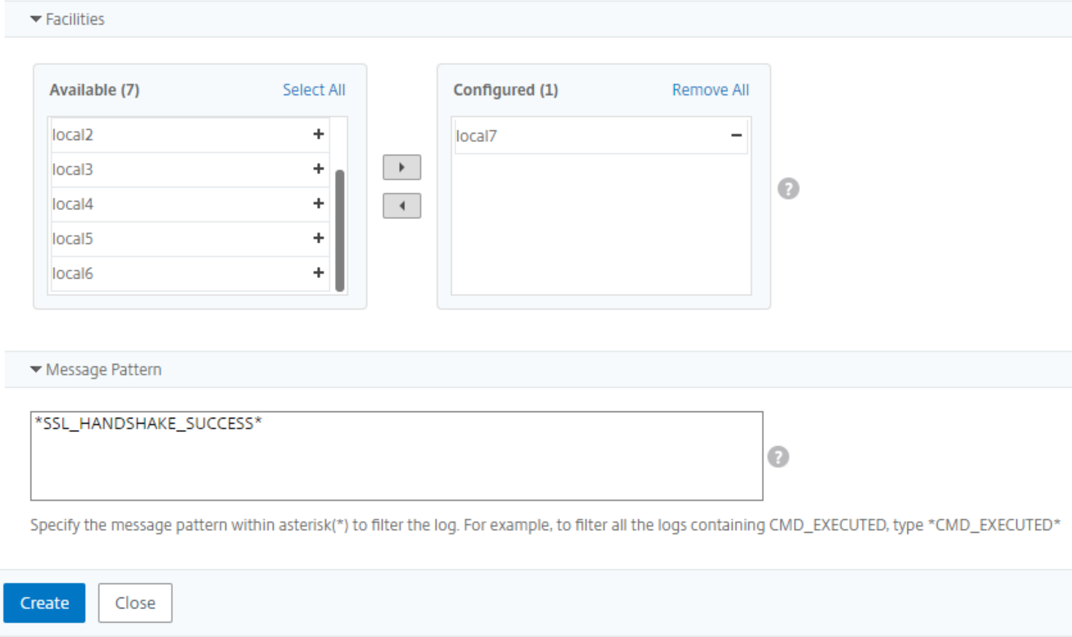
Instances

If none selected, all instances be considered

□	IP Address	Host Name	State
□	10.102.29.60	--	● Up

d) **Facilities** - Select the facility to suppress messages based on the source that generates them.

e) **Message Pattern** - You can also type a text pattern surrounded by asterisks (*) to suppress the messages. The messages are searched for the text pattern string and those messages that contain this pattern are suppressed.



Facilities

Available (7)	Configured (1)
local2	local7
local3	
local4	
local5	
local6	

Message Pattern

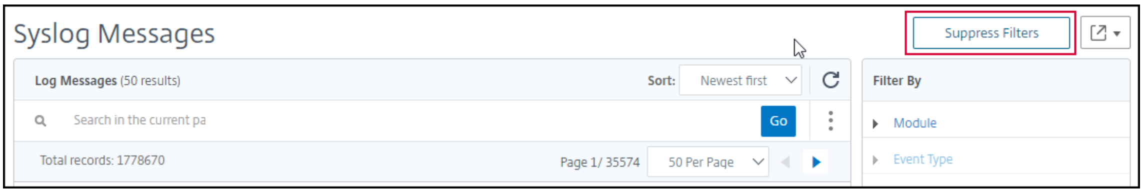
SSL_HANDSHAKE_SUCCESS

Specify the message pattern within asterisk(*) to filter the log. For example, to filter all the logs containing CMD_EXECUTED, type *CMD_EXECUTED*

Disabling the filter

To allow the messages to be viewed on Citrix Application Delivery and Management, you must disable the filter.

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. Click **Suppress Filters**.



3. On the **Suppress Filters** page, select the filter and click **Edit**.
4. On the **Configure Suppress Filter** page, clear the **Enable Filter** check box to disable the filter.

SSL dashboard

September 25, 2021

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management's SSL dashboard and its functionalities, you must understand what an SSL certificate is and how you can use Citrix Application Delivery and Management to track your SSL certificates.

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 ADC appliance, is used to complete asymmetric key (or public key) encryption and decryption.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA)
- By generating a new SSL certificate and key on the Citrix ADC appliance

Citrix Application Delivery and Management provides a centralized view of SSL certificates installed across all managed Citrix ADC instances. On the SSL Dashboard, you can view graphs that help you track certificate issuers, key strengths, signature algorithms, expired or unused certificates and so on. You can also see the distribution of SSL protocols that are running on your virtual servers and the keys that are enabled on them.

You can also set up notifications to inform you when certificates are about to expire and include information about which Citrix ADC instances use those certificates.

You can link a Citrix ADC instance certificate to a CA certificate. However, make sure the certificates you link to the same CA certificate have the same source and the same issuer. After you have linked one or more certificates to a CA certificate, you can unlink them.

> **Note**
>
> You can also use a Venafi Trust Protection Platform server with Citrix Application Delivery and Management to automate the management of the entire lifecycle of SSL certificates. For more information, see Automate SSL certificate management.

Use the SSL dashboard

September 24, 2021

You can use the SSL certificate dashboard in Citrix Application Delivery and Management to view graphs that help you keep track of certificate issuers, key strengths, and signature algorithms. The SSL certificate dashboard also displays graphs that indicate the following:

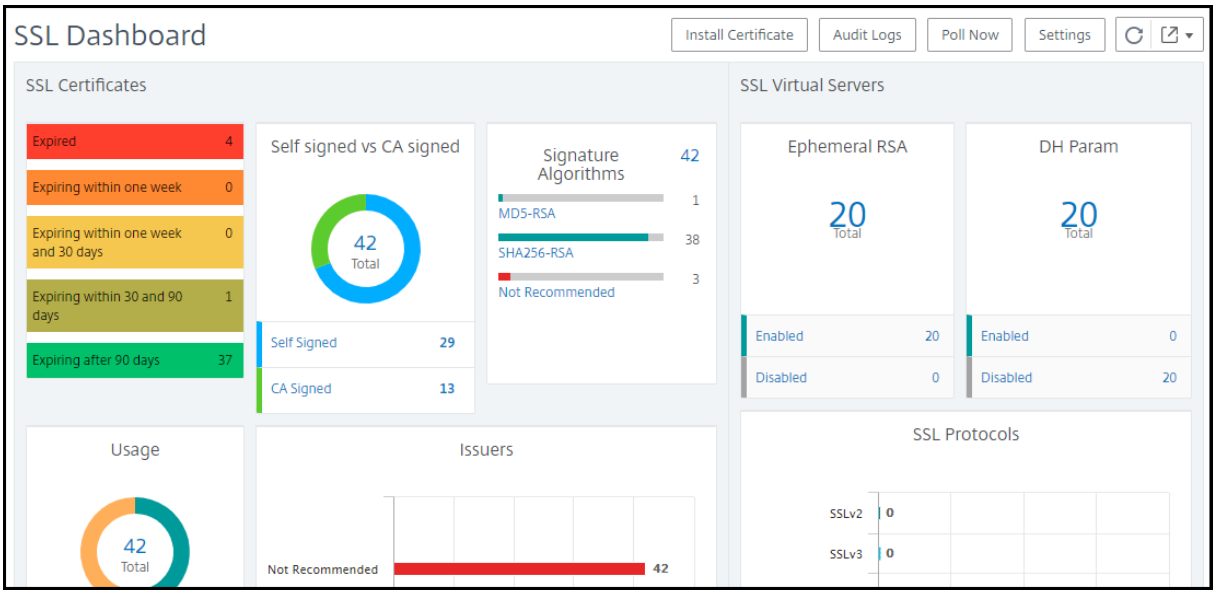
- Number of days after which certificates expire
- Number of used and unused certificates
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

Monitor SSL certificates

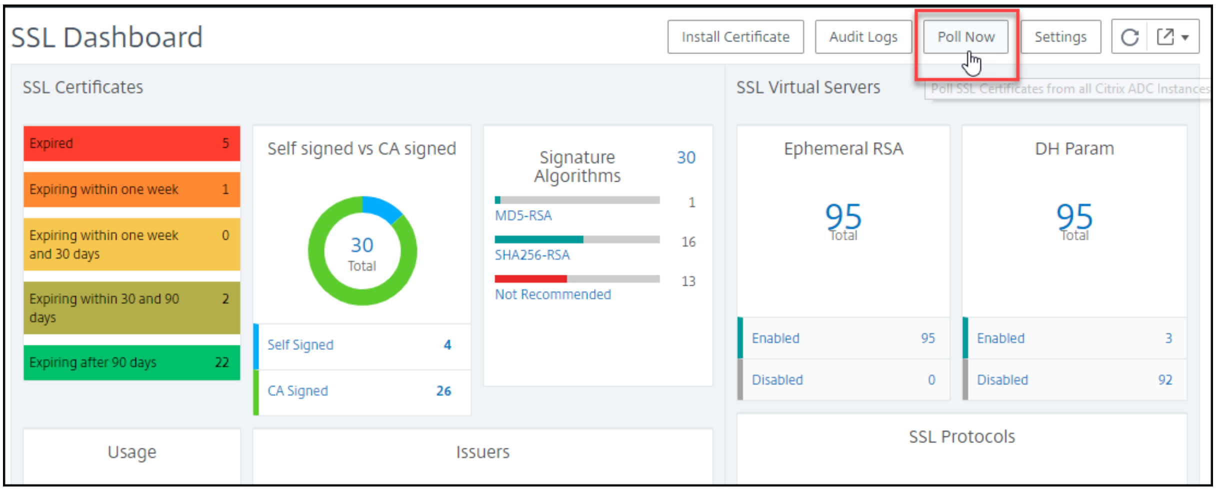
You may use the SSL dashboard on Citrix Application Delivery and Management to monitor your certificates if your company has an SSL Policy where you have defined certain SSL certificate requirements such as all certificates must have minimum key strengths of 2048 bits and a trusted CA authority must authorize it.

In another example, you may 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.

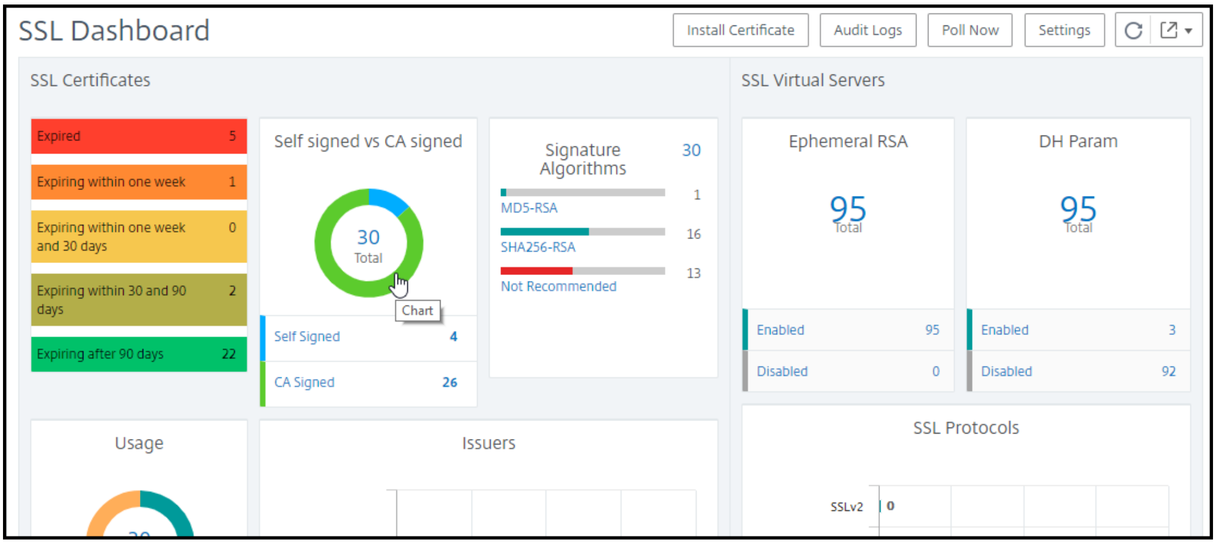
To monitor SSL certificates in Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**.



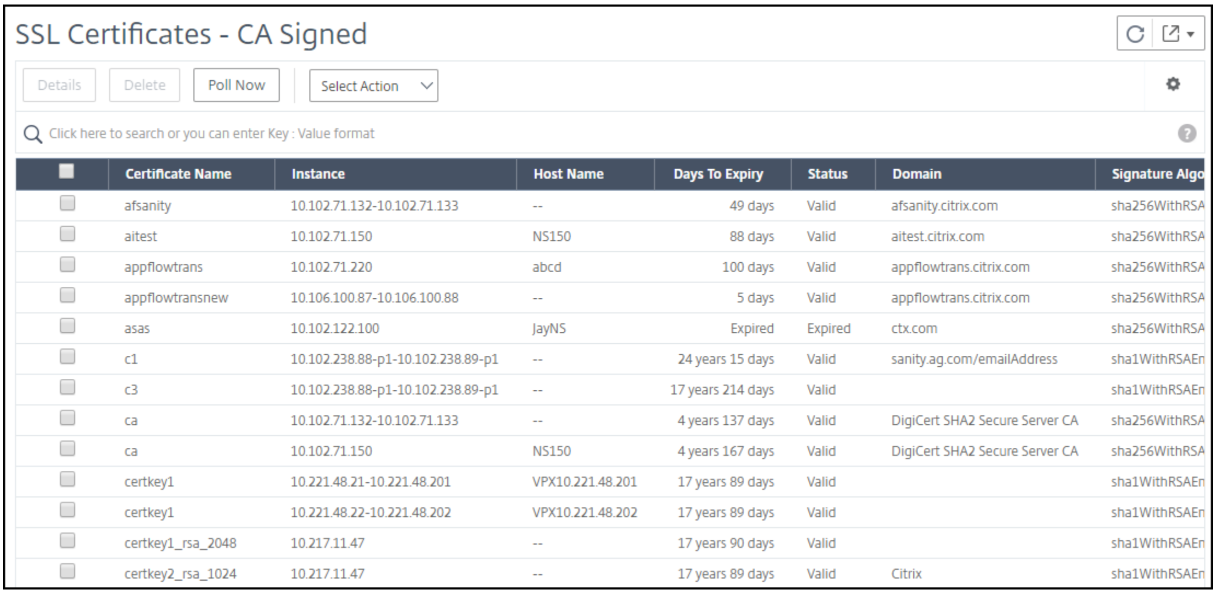
Citrix Application Delivery and Management allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to Citrix Application Delivery and Management. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page pops up, presenting the option to poll all Citrix ADC instances in the network or poll selected instances.



You can use the Citrix Application Delivery and Management SSL dashboard to view or monitor the details of SSL certificates, SSL Virtual Servers, and SSL protocols. "Total" numbers are hyperlinks, which you can click to display details related to SSL certificates, SSL Virtual Servers, or SSL protocols.



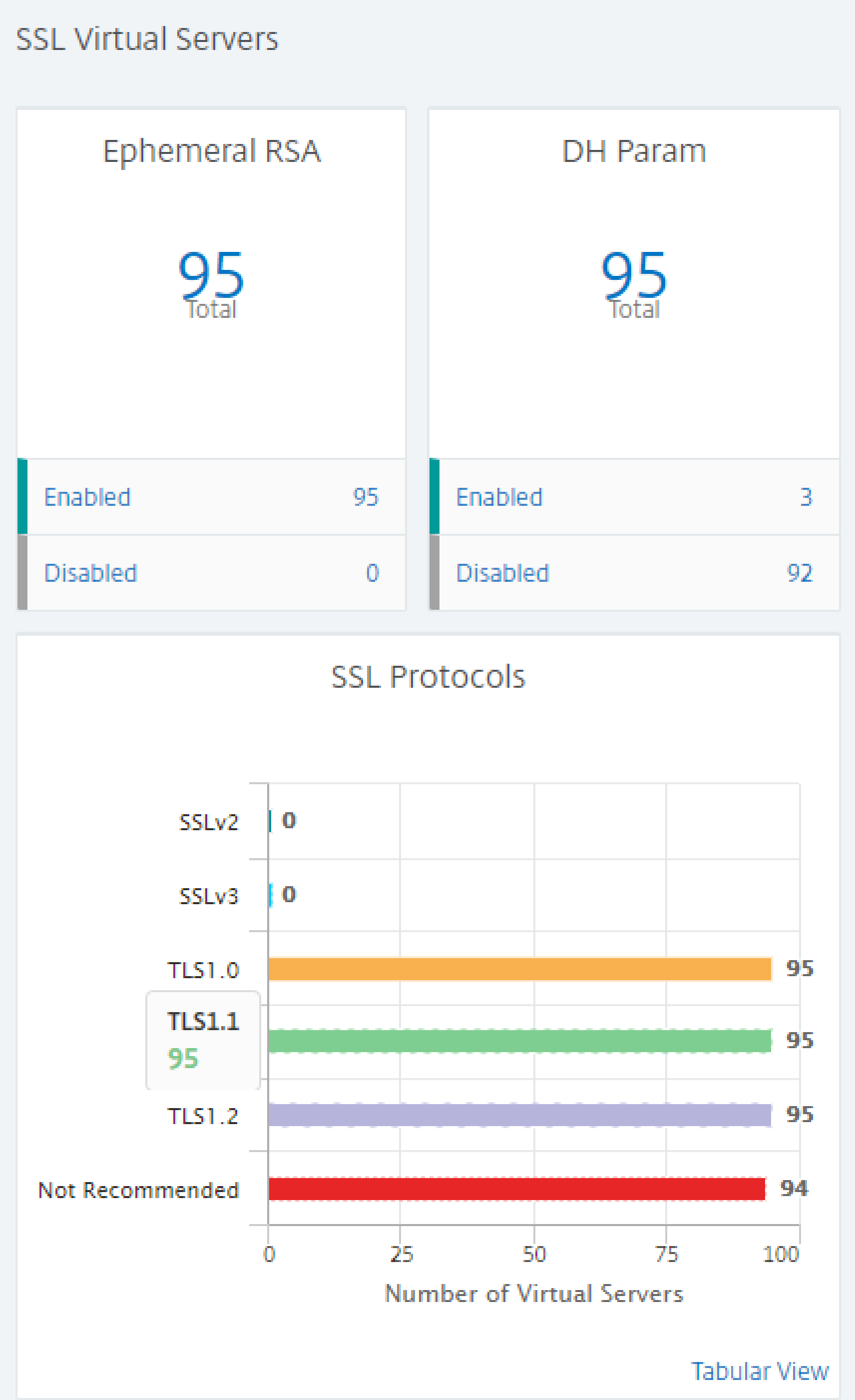
For example, when a user clicks the number 30 under "Self-signed vs. CA signed" in the above figure, a new window appears, showing details of the 30 SSL certificates on the Citrix ADC instances.


SSL Certificates - CA Signed
Details
Delete
Poll Now
Select Action
Click here to search or you can enter Key : Value format

□	Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
□	afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
□	aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
□	appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
□	appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
□	asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
□	c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
□	c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
□	ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
□	ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
□	certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
□	certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
□	certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
□	certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

The Citrix Application Delivery and Management 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, TLS1.0, TLS1.1, and TLS1.2. 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.



SSL Virtual Servers

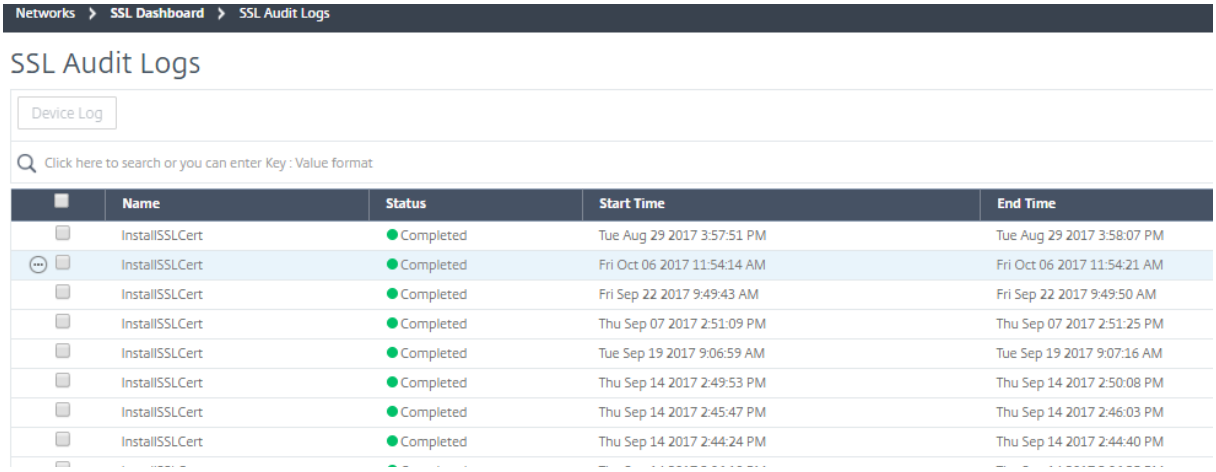
Ephemeral RSA	
Total	95
Enabled	95
Disabled	0

DH Param	
Total	95
Enabled	3
Disabled	92

View audit logs for SSL certificates

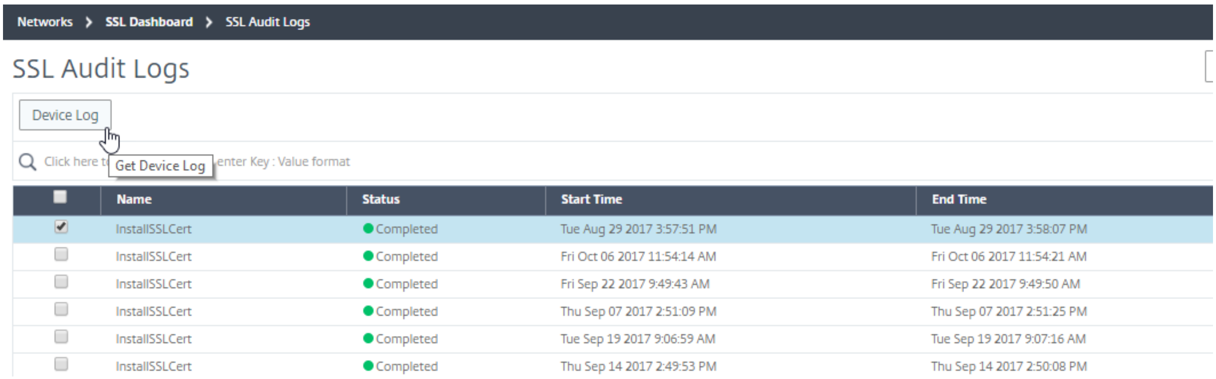
You can now view log details of SSL certificates on Citrix Application Delivery and Management. The log details display operations performed using SSL certificates on Citrix Application Delivery and Management such as: installing SSL certificates, linking and unlinking SSL certificates, updating SSL certificates, and deleting SSL certificates. Audit log 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 Citrix Application Delivery and Management using SSL certificates, navigate to **Infrastructure > SSL Dashboard** and select **Audit Logs**.

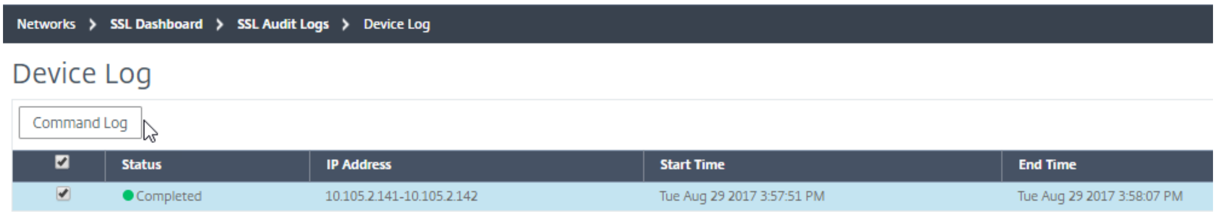

Networks > SSL Dashboard > SSL Audit Logs
SSL Audit Logs
Device Log
Click here to search or you can enter Key : Value format

□	Name	Status	Start Time	End Time
□	InstallSSLCert	● Completed	Tue Aug 29 2017 3:57:51 PM	Tue Aug 29 2017 3:58:07 PM
□	InstallSSLCert	● Completed	Fri Oct 06 2017 11:54:14 AM	Fri Oct 06 2017 11:54:21 AM
□	InstallSSLCert	● Completed	Fri Sep 22 2017 9:49:43 AM	Fri Sep 22 2017 9:49:50 AM
□	InstallSSLCert	● Completed	Thu Sep 07 2017 2:51:09 PM	Thu Sep 07 2017 2:51:25 PM
□	InstallSSLCert	● Completed	Tue Sep 19 2017 9:06:59 AM	Tue Sep 19 2017 9:07:16 AM
□	InstallSSLCert	● Completed	Thu Sep 14 2017 2:49:53 PM	Thu Sep 14 2017 2:50:08 PM
□	InstallSSLCert	● Completed	Thu Sep 14 2017 2:45:47 PM	Thu Sep 14 2017 2:46:03 PM
□	InstallSSLCert	● Completed	Thu Sep 14 2017 2:44:24 PM	Thu Sep 14 2017 2:44:40 PM

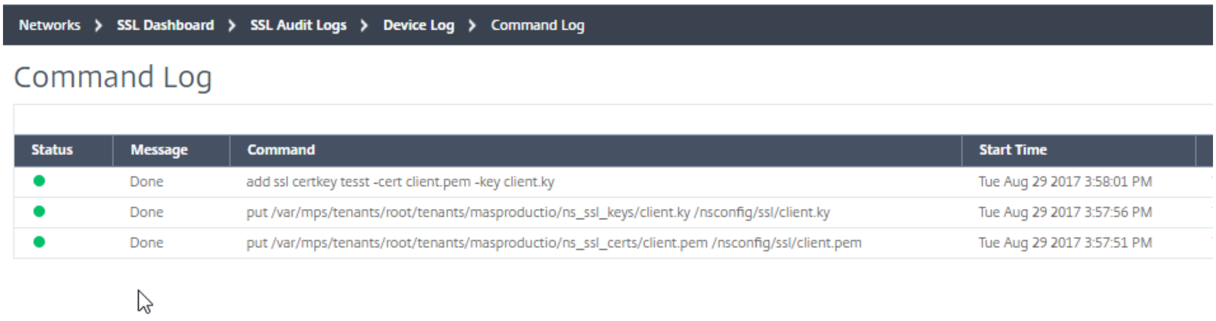
For a particular operation performed using the SSL certificate you can view its status, start time, and end time. Furthermore, you can view the instance on which the operation was performed and the commands run on that instance.


Networks > SSL Dashboard > SSL Audit Logs
SSL Audit Logs
Device Log
Get Device Log
Click here t enter Key : Value format

□	Name	Status	Start Time	End Time
☑	InstallSSLCert	● Completed	Tue Aug 29 2017 3:57:51 PM	Tue Aug 29 2017 3:58:07 PM
□	InstallSSLCert	● Completed	Fri Oct 06 2017 11:54:14 AM	Fri Oct 06 2017 11:54:21 AM
□	InstallSSLCert	● Completed	Fri Sep 22 2017 9:49:43 AM	Fri Sep 22 2017 9:49:50 AM
□	InstallSSLCert	● Completed	Thu Sep 07 2017 2:51:09 PM	Thu Sep 07 2017 2:51:25 PM
□	InstallSSLCert	● Completed	Tue Sep 19 2017 9:06:59 AM	Tue Sep 19 2017 9:07:16 AM
□	InstallSSLCert	● Completed	Thu Sep 14 2017 2:49:53 PM	Thu Sep 14 2017 2:50:08 PM



☑	Status	IP Address	Start Time	End Time
☑	● Completed	10.105.2.141-10.105.2.142	Tue Aug 29 2017 3:57:51 PM	Tue Aug 29 2017 3:58:07 PM



Networks > SSL Dashboard > SSL Audit Logs > Device Log > Command Log

Command Log

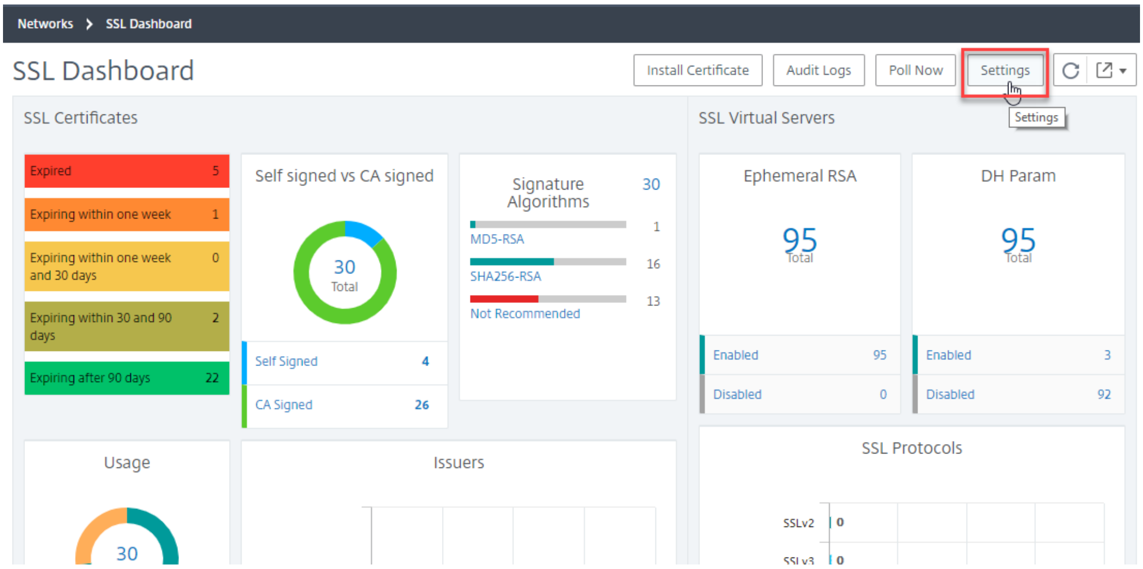
Status	Message	Command	Start Time
●	Done	add ssl certkey tesst -cert client.pem -key client.ky	Tue Aug 29 2017 3:58:01 PM
●	Done	put /var/mps/tenants/root/tenants/masproductio/ns_ssl_keys/client.ky /nsconfig/ssl/client.ky	Tue Aug 29 2017 3:57:56 PM
●	Done	put /var/mps/tenants/root/tenants/masproductio/ns_ssl_certs/client.pem /nsconfig/ssl/client.pem	Tue Aug 29 2017 3:57:51 PM

Exclude default Citrix ADC certificates on the SSL Dashboard

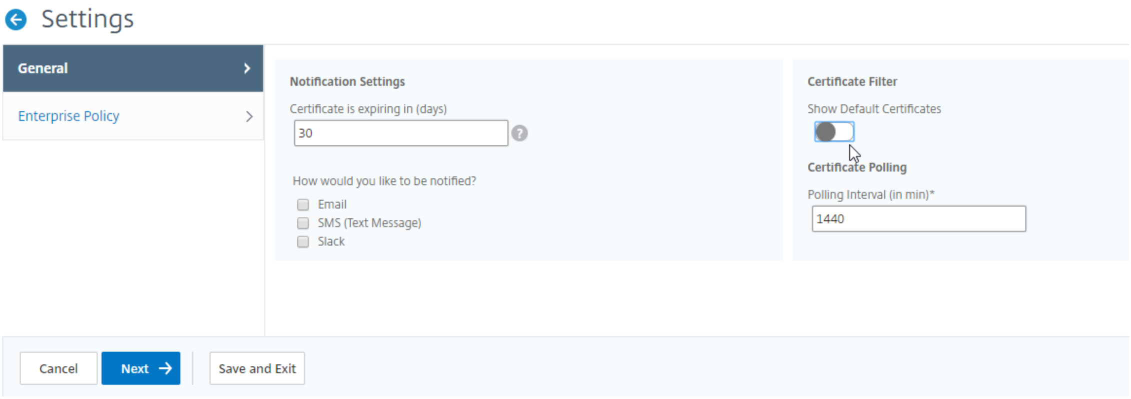
Citrix Application Delivery and Management allows you to show or hide default certificates showing up on the SSL Dashboard charts based on your preferences. By default, all certificates are displayed on the SSL dashboard including default certificates.

To show or hide default certificates on the SSL dashboard:

1. Navigate to **Infrastructure > SSL Dashboard** in the Citrix Application Delivery and Management GUI.
2. On **SSL Dashboard** page, click **Settings**.



3. On the **Settings** page, select **General**.
4. In **Certificate Filter** section, disable the **Show Default Certificates** and select **Save and Exit**.



Notification Settings

Certificate is expiring in (days): 30

How would you like to be notified?

- □ Email
- □ SMS (Text Message)
- □ Slack

Certificate Filter

Show Default Certificates

Certificate Polling

Polling Interval (in min)*: 1440

Download SSL certificates

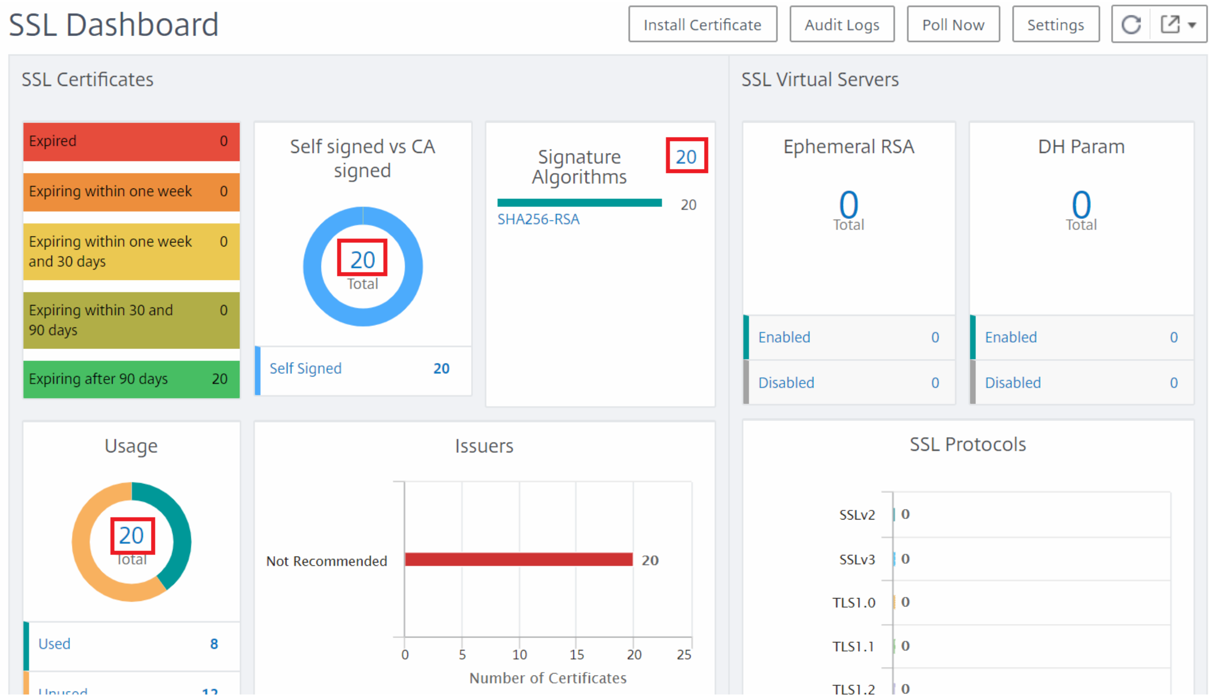
SSL certificates have to be individually managed per instance. Citrix Application Delivery and Management provides visibility into all certificates deployed across multiple instances.

- You can select which certificates are expiring and automate certificate renewals.
- Policies can be set and enforced around the types of certificates and signing authorities that are permitted.
- You can also download the SSL certificates for renewal and upload them later.

To download SSL certificates:

1. Navigate to **Infrastructure > SSL Dashboard** in the Citrix Application Delivery and Management GUI.

2. On **SSL Dashboard** page, click the total number of SSL certificates in any of the graphs.



1. On the **SSL Certificates** page, click the certificate that you wan to download. For example you want to download the one that is expiring in the next one week.
2. From the **Select Action** list box, select **Download**.
3. The certificate downloads to your system.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Set up notifications for SSL certificate expiry

As a security administrator, you can configure notifications when the certificates are about to expire and to include information about which Citrix ADC instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

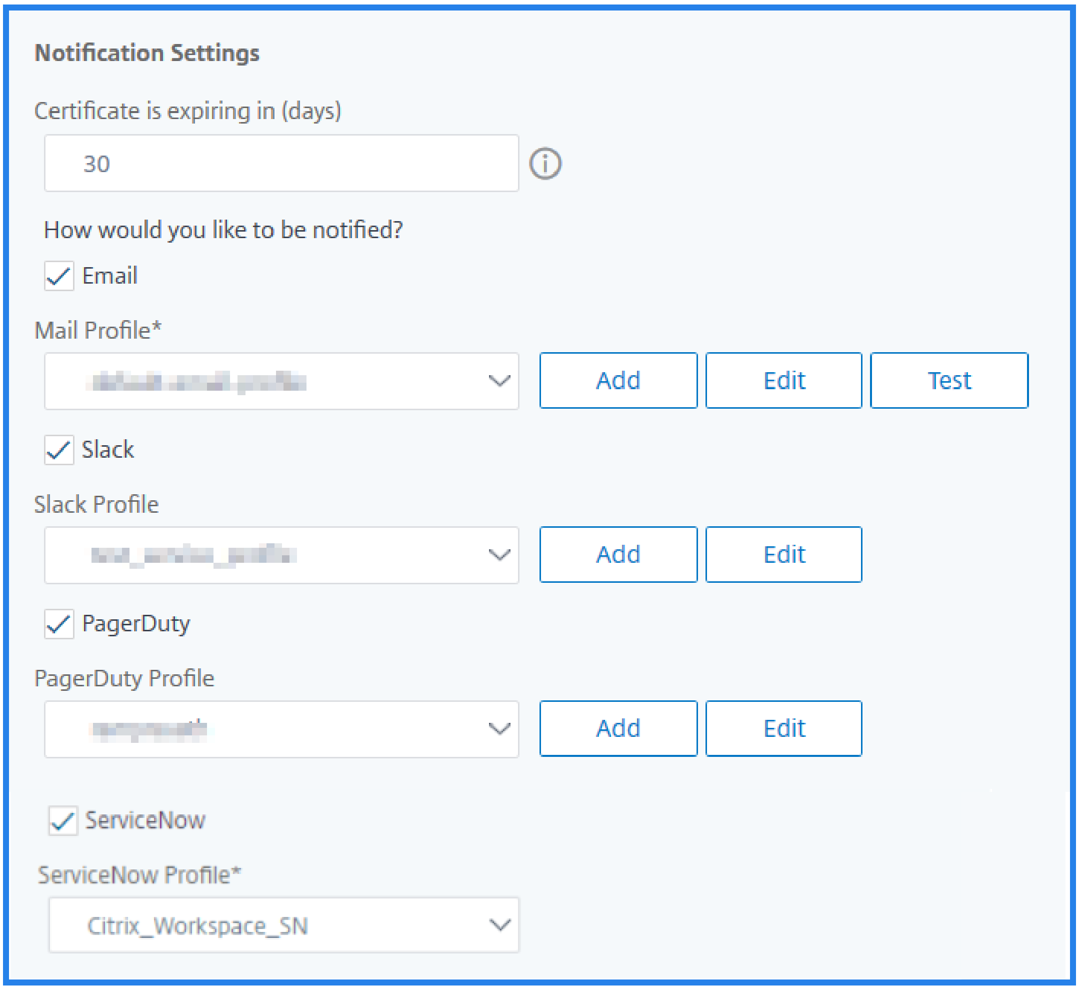
For example, you can set an email notification to be sent an email distribution list 30 days before your certificate is due to expire.

To set up notifications from Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**.
2. On the **SSL Dashboard** page, click **Settings**.
3. On the **Settings** page, click the **General**.
4. In the **Notification Settings** section, specify when 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 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.
   - **Slack** - Specify a slack profile. A notification is sent when your certificates are about to expire.
   - **PagerDuty** - 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 Citrix Application Delivery and Management. For more information, see Integrate Citrix Application Delivery and Management with ServiceNow instance.



Notification Settings

Certificate is expiring in (days)

30

How would you like to be notified?

☑ Email

Mail Profile*

[redacted]

☑ Slack

Slack Profile

[redacted]

☑ PagerDuty

PagerDuty Profile

[redacted]

☑ ServiceNow

ServiceNow Profile*

Citrix_Workspace_SN

6. Click **Save and Exit**.

Update an installed certificate

September 24, 2021

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from Citrix Application Delivery and Management without needing to log on to individual Citrix ADC instances.

To update an SSL certificate, key, or both from Citrix Application Delivery and Management:

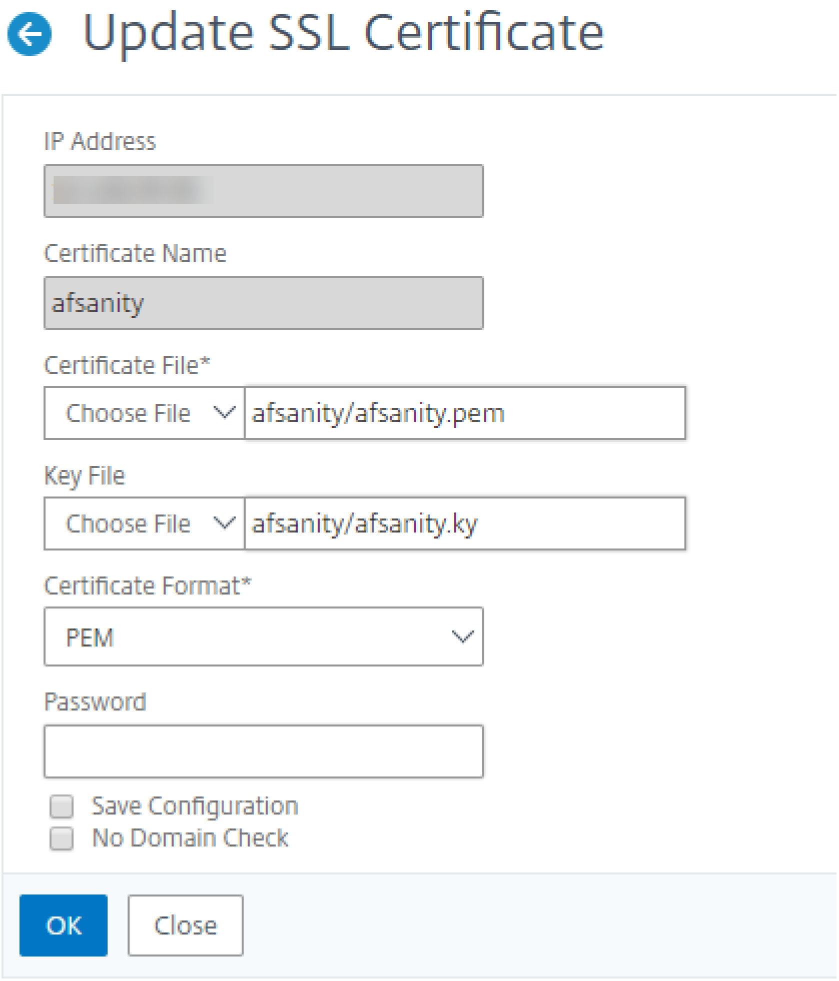
1. In Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**.

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**.



Update SSL Certificate

IP Address: [redacted]

Certificate Name: afsanity

Certificate File*: Choose File afsanity/afsanity.pem

Key File: Choose File afsanity/afsanity.ky

Certificate Format*: PEM

Password:

□ Save Configuration

□ No Domain Check

Install SSL certificates on a Citrix ADC instance

September 24, 2021

Before installing SSL certificates on Citrix ADC instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2,048 bits or higher and that the keys are signed with secure signature algorithms.

To install an SSL certificate from another Citrix ADC instance:

You can also import a certificate from a chosen Citrix ADC instance and apply it to other targeted Citrix

ADC instances from the Citrix Application Delivery and Management GUI.

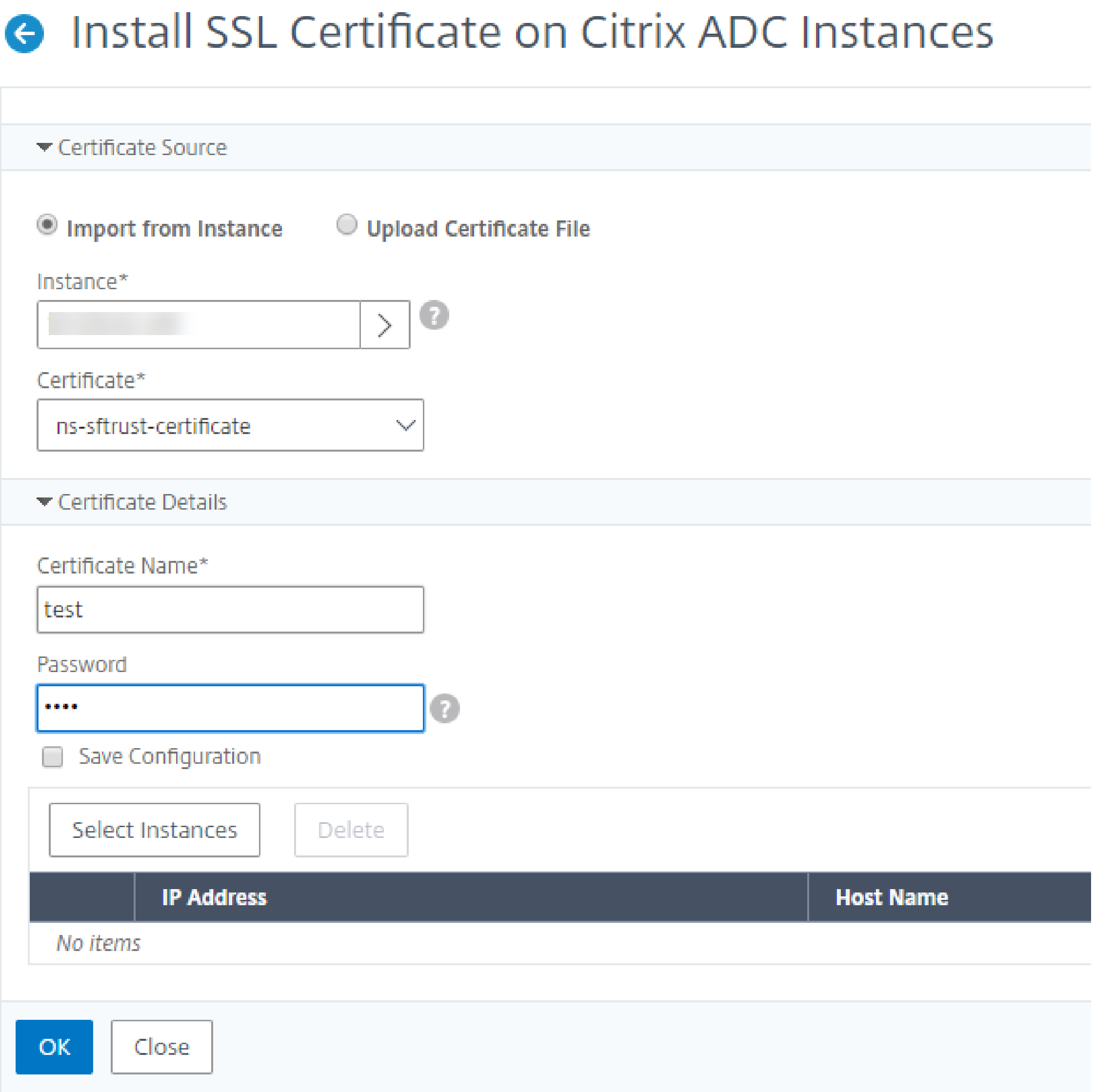
1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the SSL dashboard, click **Install Certificate**.
3. On the **Install SSL Certificate on Citrix ADC Instances** page, specify the following parameters:
   a) Certificate Source

      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 Citrix ADC instances on which you want to install your certificates.
5. Click **OK**.



Install SSL Certificate on Citrix ADC Instances

Certificate Source

● Import from Instance ○ Upload Certificate File

Instance*: [redacted]

Certificate*: ns-sftrust-certificate

Certificate Details

Certificate Name*: test

Password: ••••

□ Save Configuration

	IP Address	Host Name
	No items	

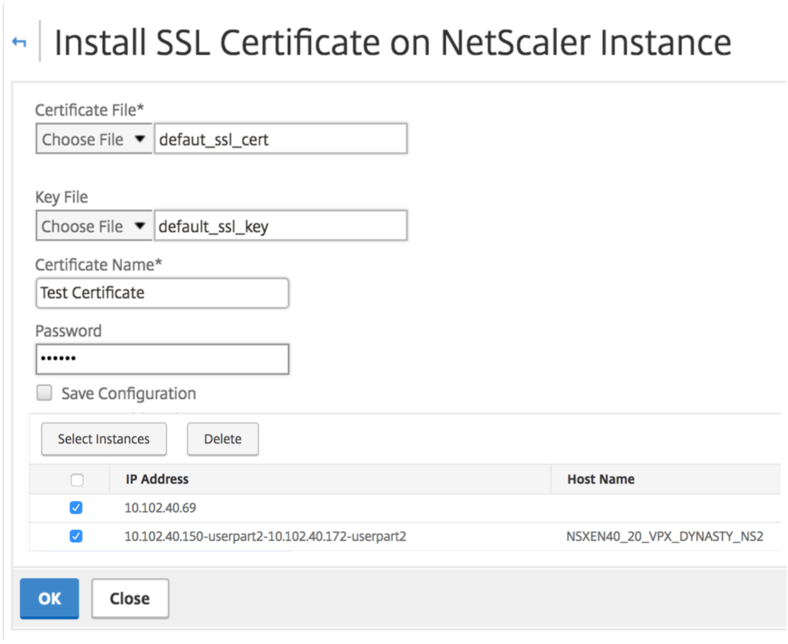
To install an SSL certificate from Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the dashboard, click **Install Certificate**.
3. On the **Install SSL Certificate on Citrix ADC Instance** page, 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 Citrix Application Delivery and Management 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 en-

crypted private keys.

- **Select Instances** - Select the Citrix ADC 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**.



Install SSL Certificate on NetScaler Instance

Certificate File*
Choose File ▾ defaut_ssl_cert

Key File
Choose File ▾ defaut_ssl_key

Certificate Name*
Test Certificate

Password
••••••

□ Save Configuration

□	IP Address	Host Name
☑	10.102.40.69	
☑	10.102.40.150-userpart2-10.102.40.172-userpart2	NSXEN40_20_VPX_DYNASTY_NS2

Create a Certificate Signing Request (CSR)

September 24, 2021

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 is included in the certificate such as the name of your organization, common name (domain name), locality, and country.

To create a CSR using Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, 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** drop-down 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 Citrix Application Delivery and Management 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 must provide a PEM Passphrase.
PEM Passphrase	If you’ve chosen the PEM Encoding Algorithm, enter a passphrase.
Confirm PEM Passphrase	Confirm your PEM passphrase.

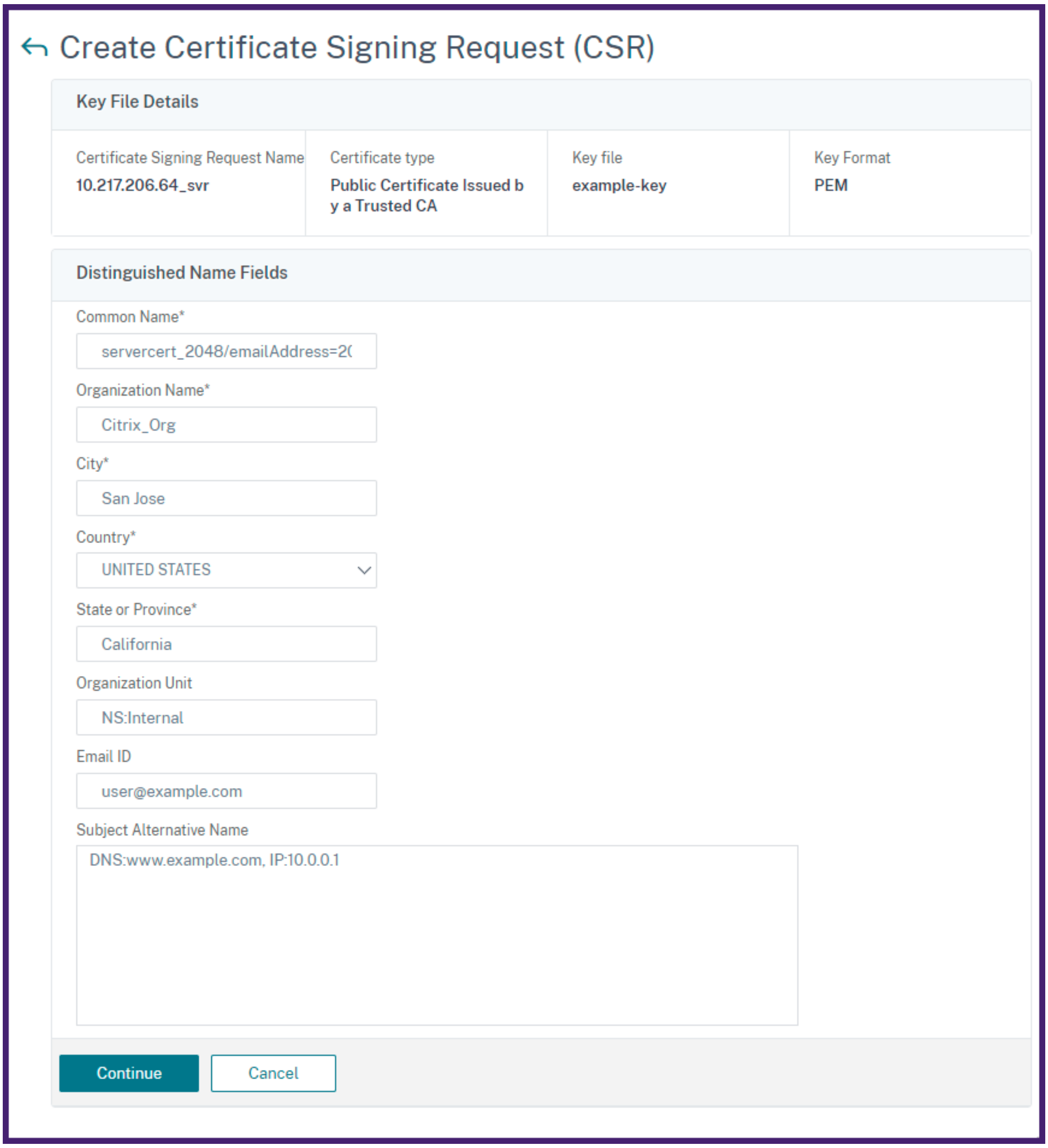
5. Click **Continue**.
6. On the following page, provide more details.

   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-->
```



Create Certificate Signing Request (CSR)

Key File Details

Certificate Signing Request Name	Certificate type	Key file	Key Format
10.217.206.64_svr	Public Certificate Issued b y a Trusted CA	example-key	PEM

Distinguished Name Fields

Common Name*: servercert_2048/emailAddress=2(

Organization Name*: Citrix_Org

City*: San Jose

Country*: UNITED STATES

State or Province*: California

Organization Unit: NS:Internal

Email ID: user@example.com

Subject Alternative Name: DNS:www.example.com, IP:10.0.0.1

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

September 24, 2021

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 Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, 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 **Select 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 Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, 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 **Select 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

September 24, 2021

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 Citrix Application Delivery and Management. If any of the certificates installed on your Citrix 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 Citrix Application Delivery and Management:

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**, and then click **Settings**.
2. On the **Settings** page, click the **Enterprise Policy** icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys.
    - **Recommended key strengths** - Denotes the algorithm security and the number of bits in a key.
    - **Recommended Signature Algorithms** - Denotes the signed tokens issues for the applications.
    - **Recommended Trusted CA** - Denotes the trusted entity that issues the digital certificates. Click the **+** icon to add more entities.
    - **Recommended SSL protocols** - Denotes the TLS/SSL versions.
3. Click **Finish** or **Save and Exit** to save your enterprise policy.

Poll SSL certificates from Citrix ADC instances

September 24, 2021

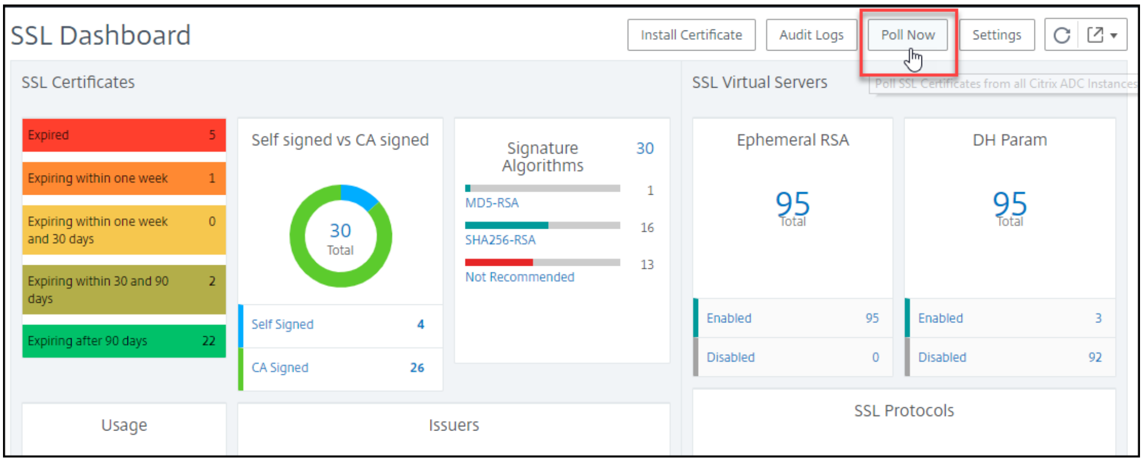
Citrix Application Delivery and Management automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix ADC instances. Polling all the Citrix ADC instances SSL certificates places a heavy load on the network.

Instead of polling all the Citrix ADC instances SSL certificates, you can manually poll only the SSL certificates of a selected instance or instances.

To poll SSL certificates on Citrix ADC instances:

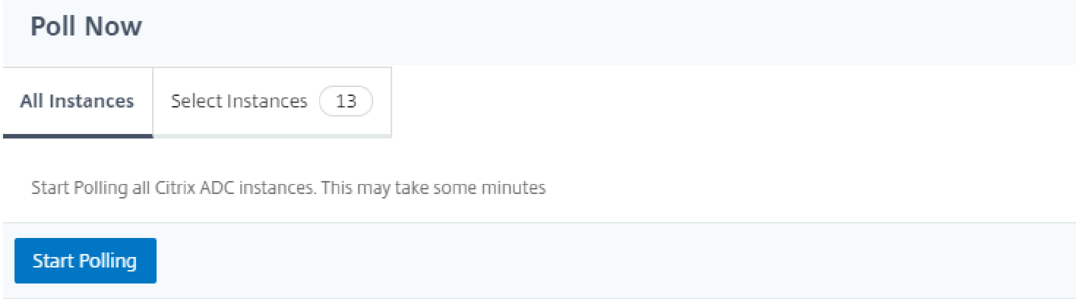
1. In Citrix Application Delivery and Management, navigate to **Infrastructure > SSL Dashboard**.

2. On **SSL Dashboard** page, in the top right-hand corner, click **Poll Now**.



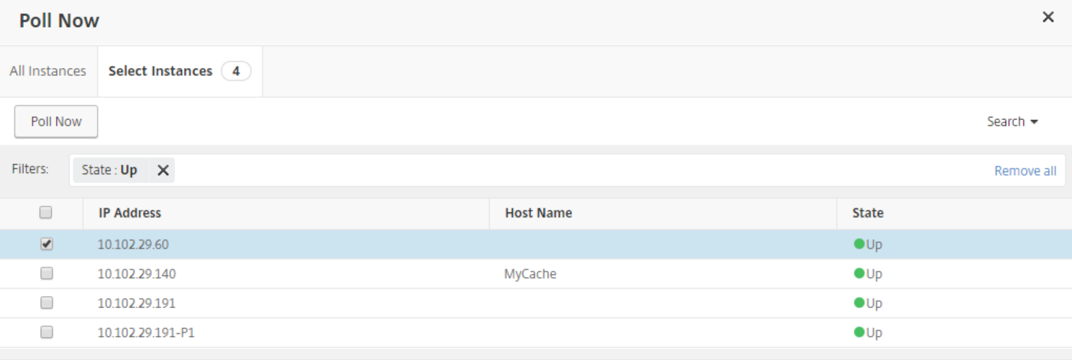
3. The **Poll Now** page pops up, giving you the option to poll all Citrix ADC instances in the network or poll selected instances.

   - To poll the SLL certificates of all the Citrix ADC instances, select the **All Instances** tab and click **Start Polling**.



Start Polling all Citrix ADC instances. This may take some minutes

   - To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.



	IP Address	Host Name	State
☑	10.102.29.60		● Up
□	10.102.29.140	MyCache	● Up
□	10.102.29.191		● Up
□	10.102.29.191-P1		● Up

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Configuration jobs

September 25, 2021

Citrix Application Delivery and Management configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple Citrix ADC instances in the network.

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management. 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 Citrix Application Delivery and Management. 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 Citrix ADC SDX instances running Citrix ADC release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in Citrix Application Delivery and Management. You can also upgrade a Citrix ADC instance by extracting the running configuration or a saved configuration and running the commands on another Citrix ADC instance of the same type. This upgrade 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 Citrix ADC session. When you run the job, changes in the ns.conf on the selected instance are recorded and copied to Citrix Application Delivery and Management.

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 Citrix Application Delivery and Management

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

> **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.

Create a configuration job

September 25, 2021

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. You can replicate configurations on multiple instances on your network and
record and play configuration tasks using the Citrix Application Delivery and Management GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of Citrix Application Delivery and Management to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on Citrix Application Delivery and Management:

1. Navigate to the **Infrastructure > Configuration > 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 Citrix ADC 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.

    b) Click **Add Instances** and select the instances from the list. Click **OK**.

    c) Click **Next**.

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 Citrix Application Delivery and Management server.

    b) Enter common values for the variables that you have defined for all instances

    c) Click **Next**.

7. Evaluate and verify the commands to be run on each instance on the **Job Preview** tab. This tab also display the rollback commands if specified on the **Select Configuration** tab.

8. In the **Execute** tab, choose to either run your job now, or schedule to run the job later.

    Also, select one of the following actions from the **On Command Failure** list that Citrix Application Delivery and Management must perform if the command fails:

    - **Ignore error and continue**: Citrix Application Delivery and Management ignores the failed command and runs the remaining commands for the selected instance.

        > **Note**
        >
        > This action does not allow you to abort a configuration job that is in progress.

    - **Stop further execution**: Citrix Application Delivery and Management stops the remaining commands if any command fails during execution.

    - **Rollback successful commands**: Citrix Application Delivery and Management restores the successfully run commands if any command fails during execution.

        If the custom rollback is enabled, the Citrix Application Delivery and Management runs the corresponding rollback commands for the failed commands.

9. 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 > Configuration Jobs**.

2. Select the job that you want to enable email and Slack notification and click **Edit**.

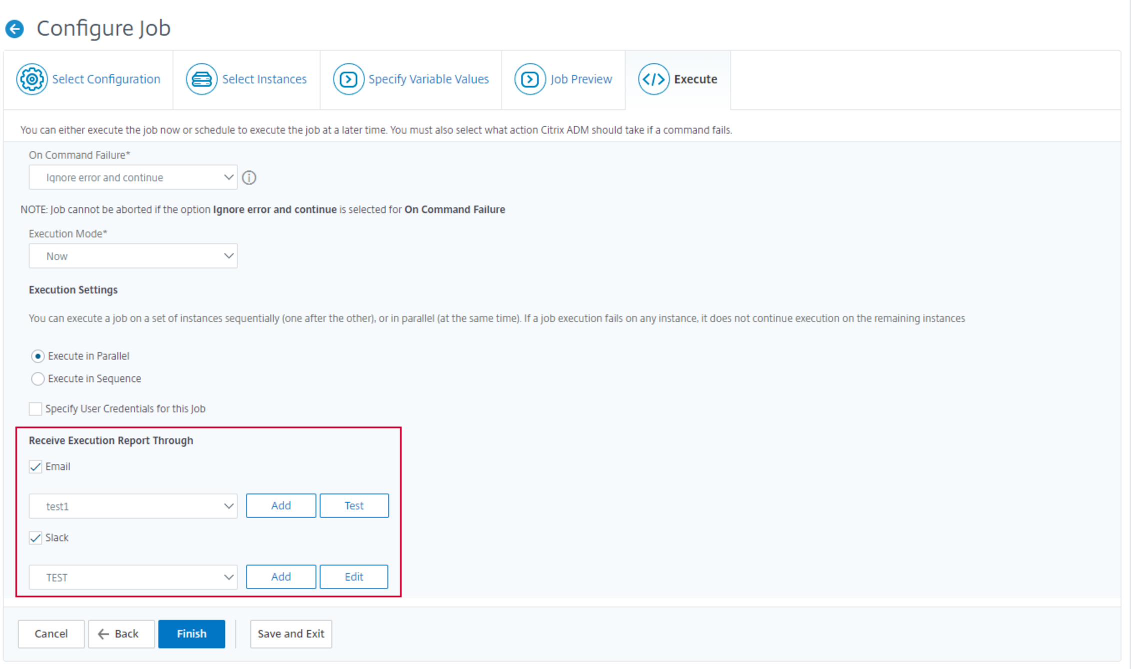
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:

- 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.



Configure Job

You can either execute the job now or schedule to execute the job at a later time. You must also select what action Citrix ADM should take if a command fails.

On Command Failure*: Ignore error and continue

NOTE: Job cannot be aborted if the option **Ignore error and continue** is selected for **On Command Failure**

Execution Mode*: Now

Execution Settings

You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances

● Execute in Parallel
○ Execute in Sequence

□ Specify User Credentials for this Job

Receive Execution Report Through

☑ Email

test1

☑ Slack

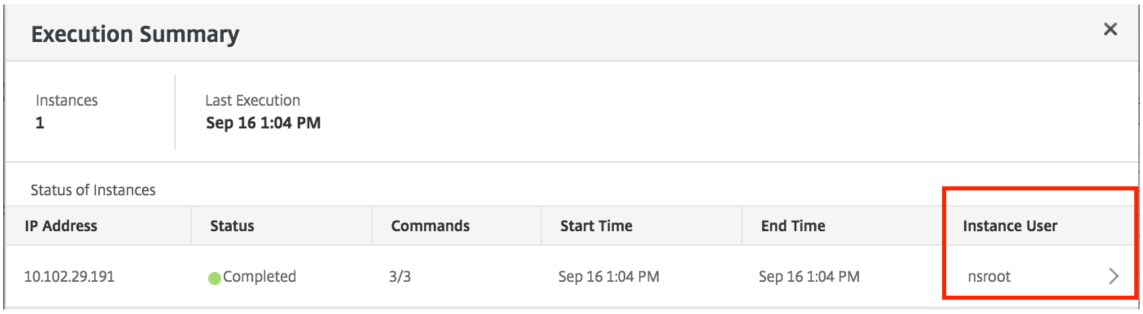
TEST

4. Click **Finish**.

To view execution summary details:

1. Navigate to **Infrastructure > Configuration > 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 the job that was run
   - The commands run on the job
   - The start and end time of the job, and
   - The instance user’s name



Instances
1

Last Execution
Sep 16 1:04 PM

Status of Instances

IP Address	Status	Commands	Start Time	End Time	Instance User
10.102.29.191	● Completed	3/3	Sep 16 1:04 PM	Sep 16 1:04 PM	nsroot

Configuration audit

September 25, 2021

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 Citrix Application Delivery and Management instances
- Generate configuration audit diff for ConfigChange SNMP traps

Maintenance jobs

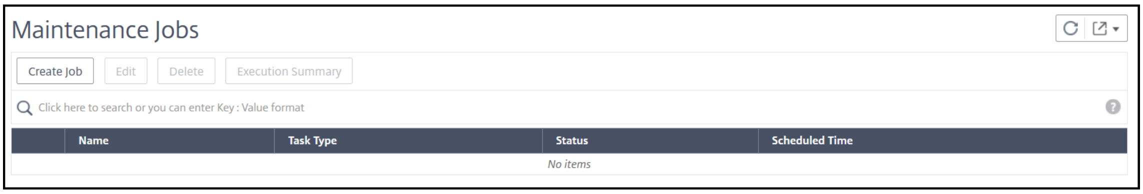
September 28, 2021

You can create the following maintenance tasks using Citrix Application Delivery and Management. You can then schedule the maintenance tasks at a specific date and time.

- Upgrade Citrix ADC instances
- Upgrade Citrix ADC SDX instances
- Upgrade Citrix ADC instances in the Autoscale Group
- Configure HA pair of Citrix ADC instances
- Convert HA pair of instances to Cluster

Schedule upgrading of Citrix ADC instances

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Configuration > Configuration Jobs**. Click the **Create Job** button.



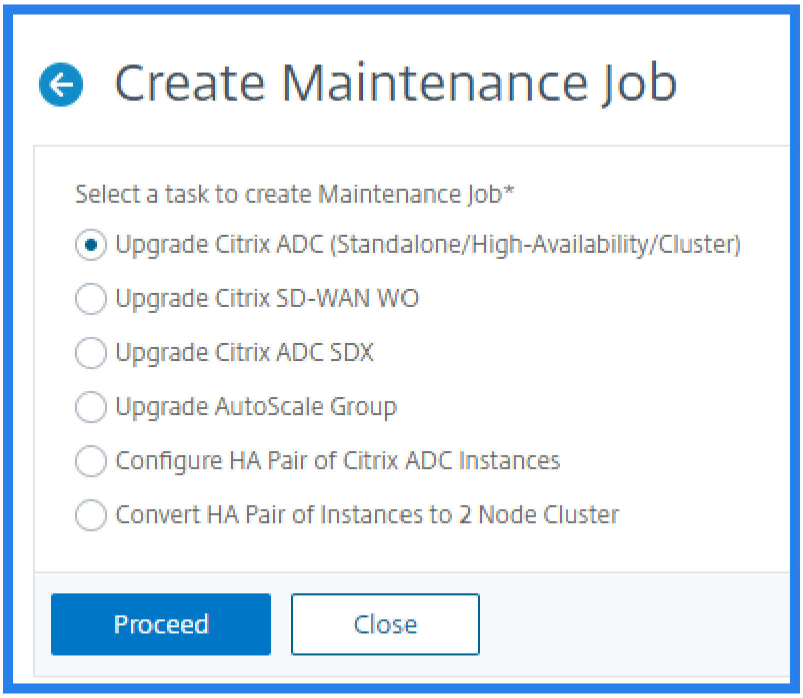
Maintenance Jobs

Create Job | Edit | Delete | Execution Summary

Click here to search or you can enter Key : Value format

Name	Task Type	Status	Scheduled Time
No items			

2. In **Create Maintenance Jobs**, select **Upgrade Citrix ADC (Standalone/High-Availability/Cluster)** and click **Proceed**.



Create Maintenance Job

Select a task to create Maintenance Job*

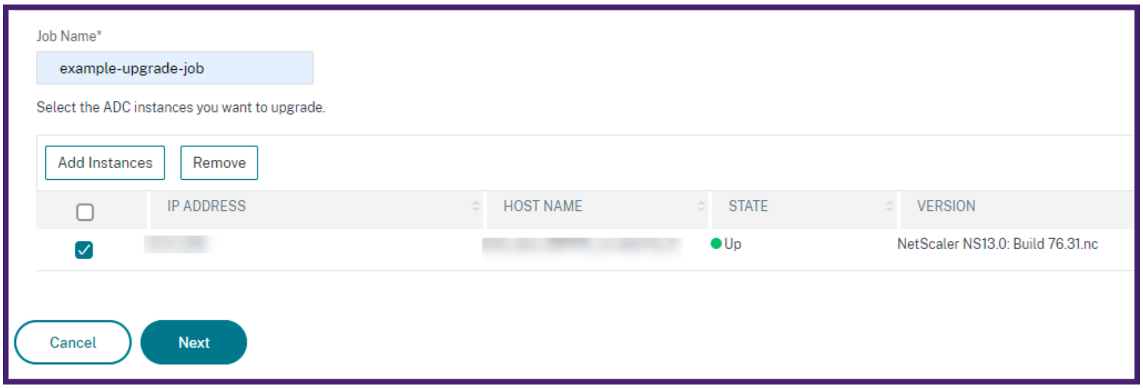
- ● Upgrade Citrix ADC (Standalone/High-Availability/Cluster)
- ○ Upgrade Citrix SD-WAN WO
- ○ Upgrade Citrix ADC SDX
- ○ Upgrade AutoScale Group
- ○ Configure HA Pair of Citrix ADC Instances
- ○ Convert HA Pair of Instances to 2 Node Cluster

Proceed | Close

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.



Job Name*

example-upgrade-job

Select the ADC instances you want to upgrade.

Add Instances | Remove

□	IP ADDRESS	HOST NAME	STATE	VERSION
☑	[redacted]	[redacted]	● Up	NetScaler NS13.0: Build 76.31.nc

Cancel | Next

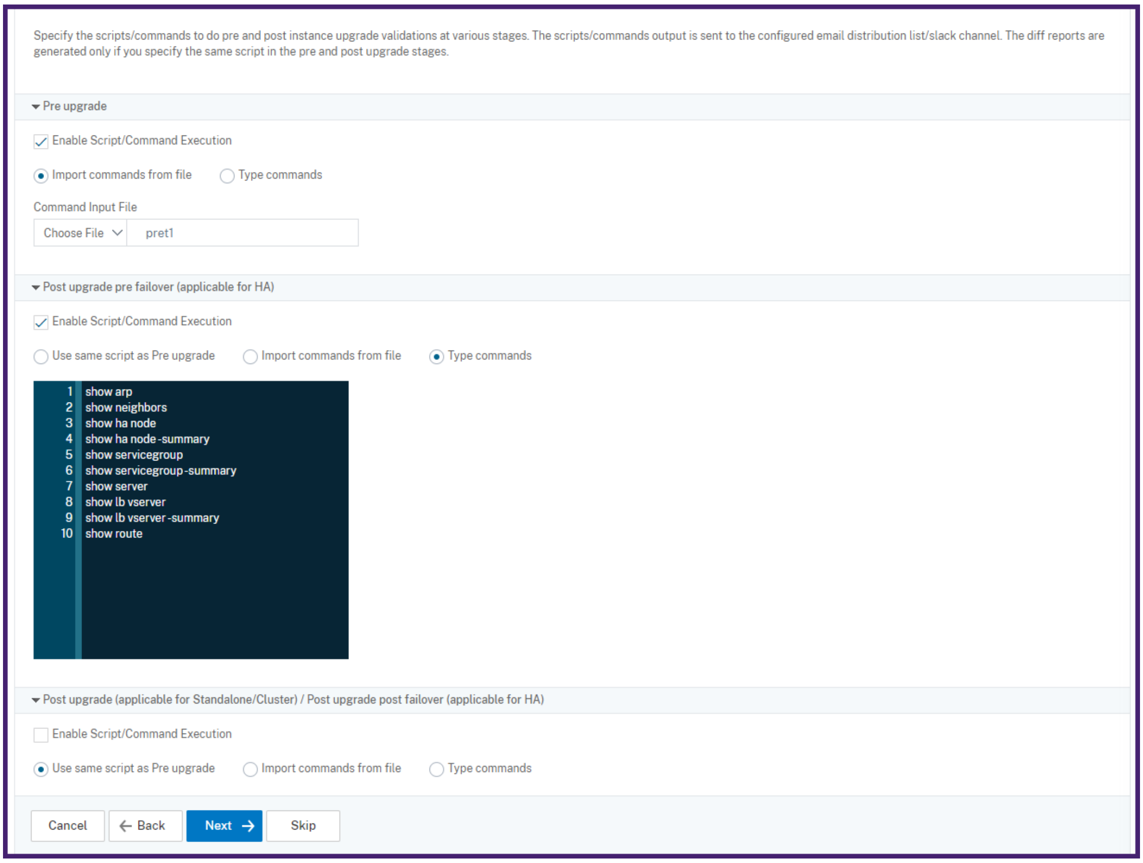
5. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **Important**
   >
   > If you specify cluster IP address, the Citrix Application Delivery and Management does pre-upgrade validation only on the specified instance not on the other cluster nodes.

6. 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.



Specify the scripts/commands to do pre and post instance upgrade validations at various stages. The scripts/commands output is sent to the configured email distribution list/slack channel. The diff reports are generated only if you specify the same script in the pre and post upgrade stages.

▾ Pre upgrade

☑ Enable Script/Command Execution

● Import commands from file ○ Type commands

Command Input File: pret1

▾ Post upgrade pre failover (applicable for HA)

☑ Enable Script/Command Execution

○ Use same script as Pre upgrade ○ Import commands from file ● Type commands

```
show arp
show neighbors
show ha node
show ha node -summary
show servicegroup
show servicegroup -summary
show server
show lb vserver
show lb vserver -summary
show route
```

▾ Post upgrade (applicable for Standalone/Cluster) / Post upgrade post failover (applicable for HA)

□ Enable Script/Command Execution

● Use same script as Pre upgrade ○ Import commands from file ○ Type commands

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.

7. 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.

8. In **Create Job**, specify the following details:

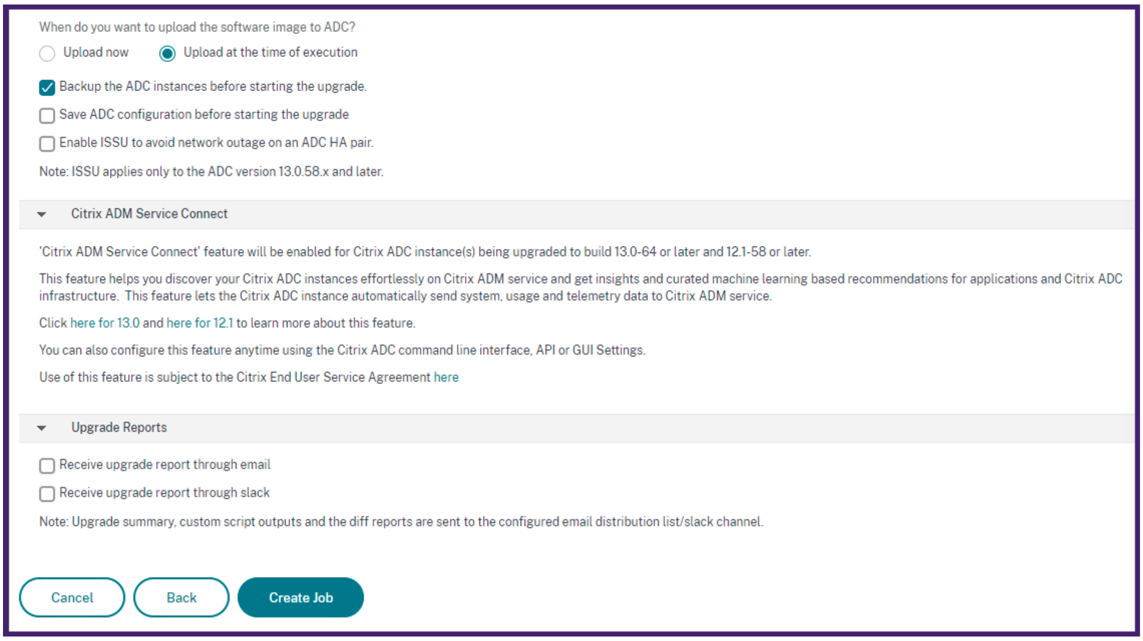
   a) Select one of the following options from the **Software Image** list:

      - **Local** - Select the instance upgrade file from your local machine.
      - **Appliance** - Select the instance upgrade file from an Citrix Application Delivery and Management file browser. The Citrix Application Delivery and Management GUI displays the instance files that are present at `/var/mps/mps_images`.

   b) 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.

   - **Clean software image from Citrix ADC on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.
   - **Backup the ADC instances before starting the upgrade.** - Creates a backup of the selected ADC instances.
   - **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.
   - **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.



When do you want to upload the software image to ADC?

○ Upload now ● Upload at the time of execution

☑ Backup the ADC instances before starting the upgrade.

□ Save ADC configuration before starting the upgrade

□ Enable ISSU to avoid network outage on an ADC HA pair.

Note: ISSU applies only to the ADC version 13.0.58.x and later.

Citrix ADM Service Connect

'Citrix ADM Service Connect' feature will be enabled for Citrix ADC instance(s) being upgraded to build 13.0-64 or later and 12.1-58 or later.

This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to Citrix ADM service.

Click here for 13.0 and here for 12.1 to learn more about this feature.

You can also configure this feature anytime using the Citrix ADC command line interface, API or GUI Settings.

Use of this feature is subject to the Citrix End User Service Agreement here

Upgrade Reports

□ Receive upgrade report through email

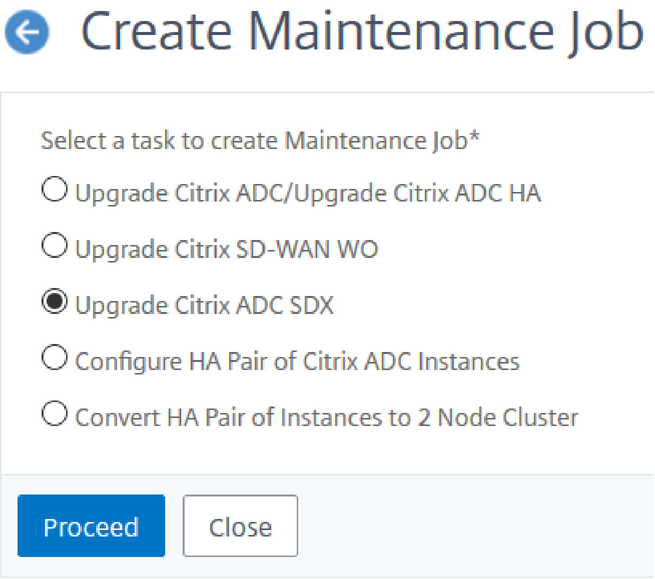
□ Receive upgrade report through slack

Note: Upgrade summary, custom script outputs and the diff reports are sent to the configured email distribution list/slack channel.

9. Click **Create Job**.

Schedule upgrading of Citrix ADC SDX instances

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**. Click the **Create Job** button.
2. Select **Upgrade Citrix ADC SDX** and click **Proceed**.



Create Maintenance Job

Select a task to create Maintenance Job*

○ Upgrade Citrix ADC/Upgrade Citrix ADC HA

○ Upgrade Citrix SD-WAN WO

● Upgrade Citrix ADC SDX

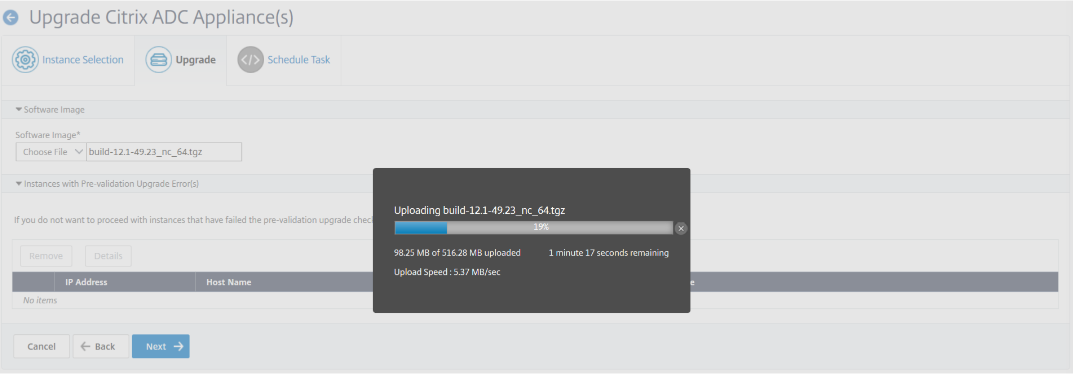
○ Configure HA Pair of Citrix ADC Instances

○ Convert HA Pair of Instances to 2 Node Cluster

3. On the **Upgrade Citrix ADC SDX** page, in the **Instance Selection** tab:
   a) Add a **Task Name**.

b) From the Software Image drop-down menu, select either Local (your local machine) or Appliance (the build file must be present on the Citrix Application Delivery and Management virtual appliance).

The upload process begins.



Upgrade Citrix ADC Appliance(s)

Software Image

Software Image*: Choose File | build-12.1-49.23_nc_64.tgz

Instances with Pre-validation Upgrade Error(s)

If you do not want to proceed with instances that have failed the pre-validation upgrade chec

	IP Address	Host Name
No items		

Uploading build-12.1-49.23_nc_64.tgz

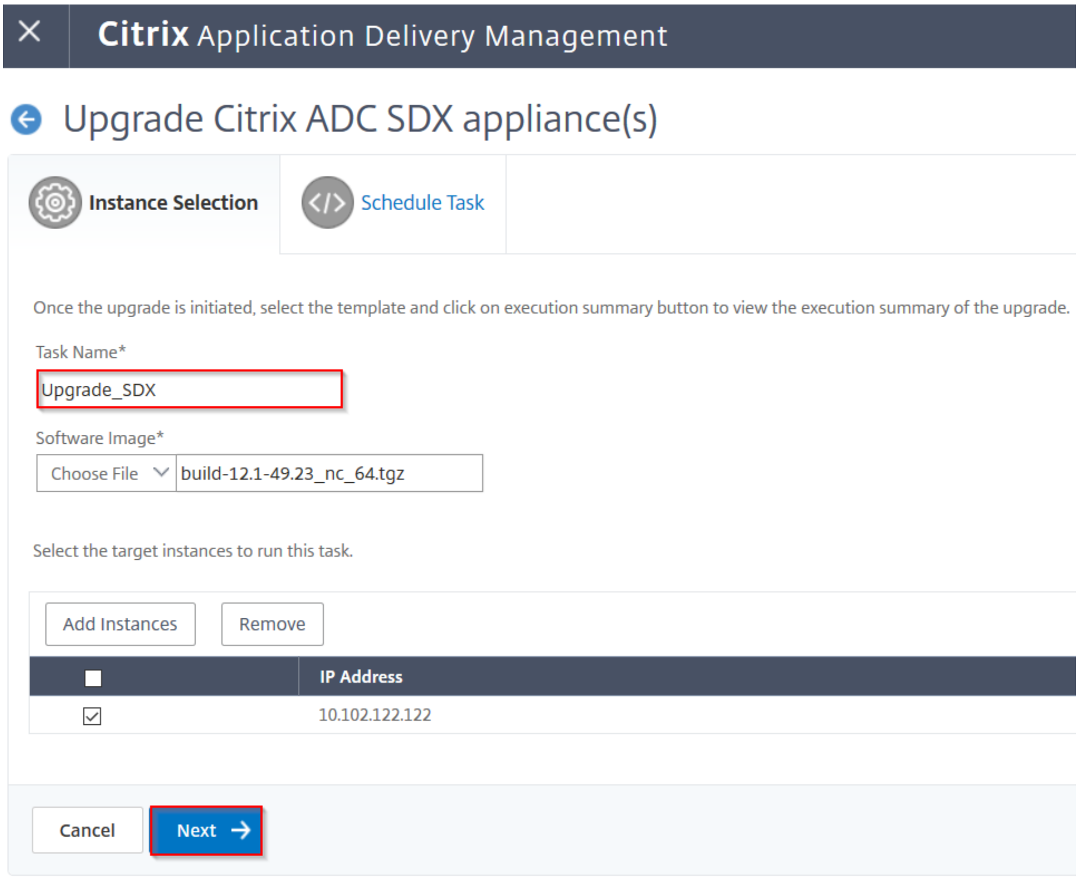
19%

98.25 MB of 516.28 MB uploaded 1 minute 17 seconds remaining

Upload Speed : 5.37 MB/sec

c) Add the Citrix ADC SDX instances on which you want to run the upgrade process.

d) Click **Next**.



Citrix Application Delivery Management

Upgrade Citrix ADC SDX appliance(s)

Once the upgrade is initiated, select the template and click on execution summary button to view the execution summary of the upgrade.

Task Name*: Upgrade_SDX

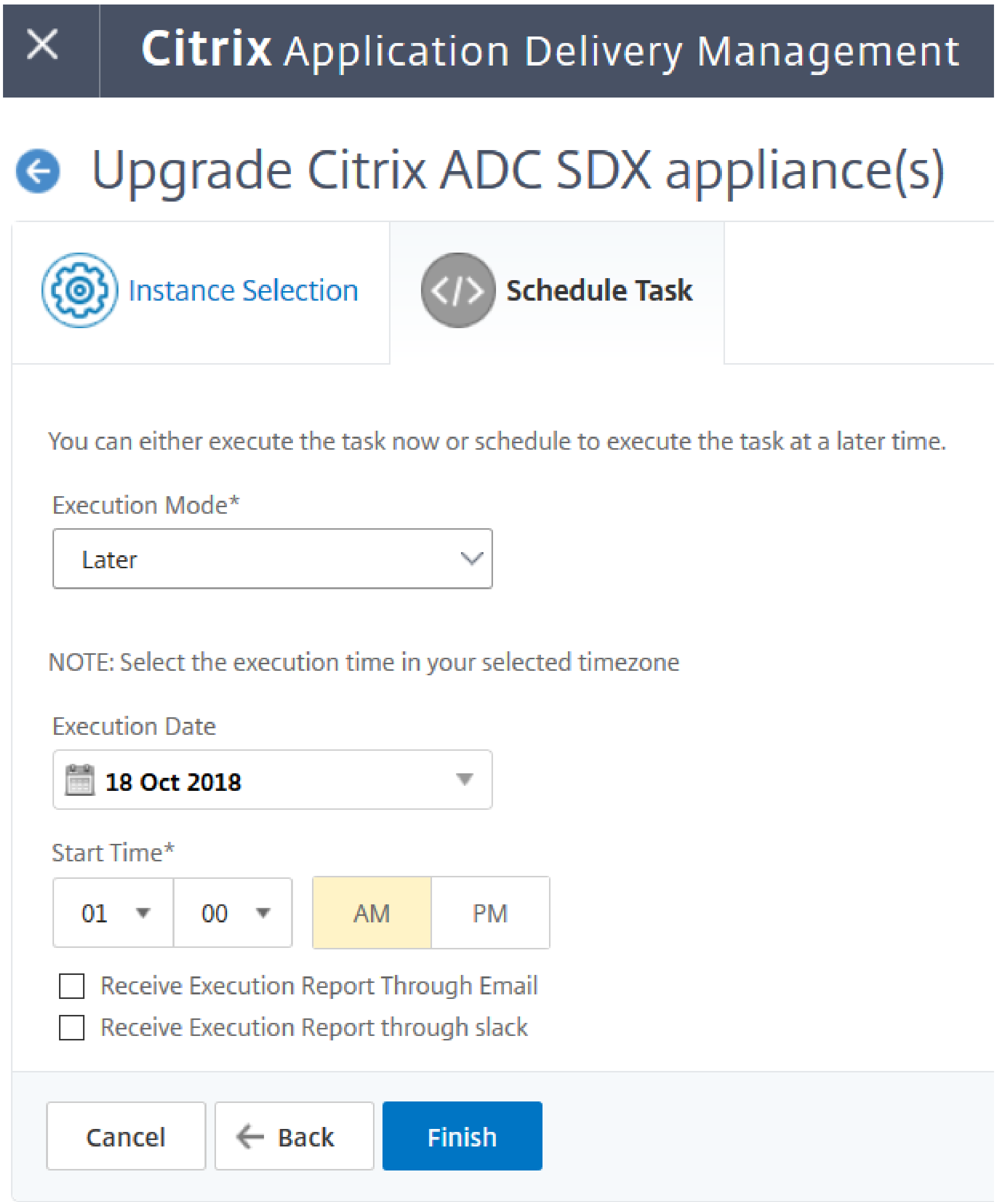
Software Image*: Choose File | build-12.1-49.23_nc_64.tgz

Select the target instances to run this task.

□	IP Address
☑	10.102.122.122

4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a Citrix SDX instance now, and click **Finish**.

5. To upgrade a Citrix ADC SDX instance later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the Citrix ADC instance, and click **Finish**


Citrix Application Delivery Management
Upgrade Citrix ADC SDX appliance(s)
Instance Selection
Schedule Task

You can either execute the task now or schedule to execute the task at a later time.

Execution Mode*: Later

NOTE: Select the execution time in your selected timezone

Execution Date: 18 Oct 2018

Start Time*: 01 00 AM PM

☐ Receive Execution Report Through Email
☐ Receive Execution Report through slack

6. You can also enable email and slack notifications to receive the execution report of the upgrading Citrix ADC 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 Citrix ADC instances

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. In Citrix Application Delivery and Management, navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**. Click the **Create Job** button.
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 Citrix ADC version. This image is the existing version of Citrix ADC instances in the Autoscale group.
   c) In **Citrix ADC Image**, browse the Citrix ADC 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 Citrix ADC instances upgrade immediately.
      - **Later:** To start the Citrix ADC instances upgrade at later time.

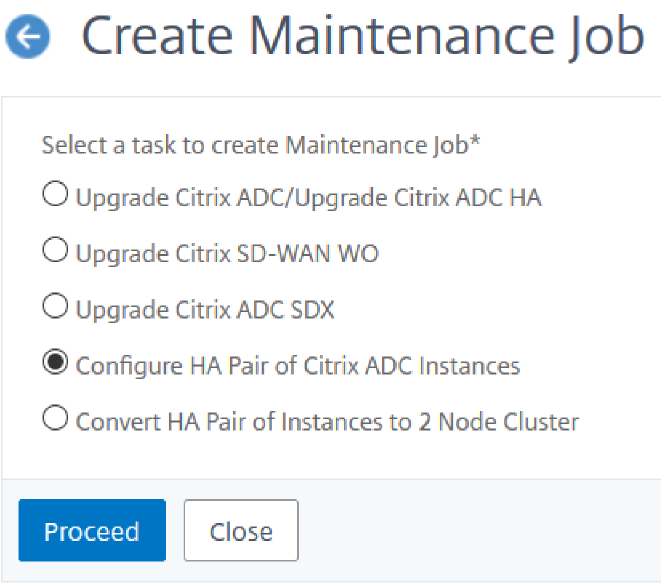
   b) If you select the **Later** option, select the Execution Date and Start Time when you want to start the upgrade task.

   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 Citrix ADC instances

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**. Click the **Create Job** button.
2. Select **Configure HA Pair of Citrix ADC Instances** and click **Proceed**.



Create Maintenance Job

Select a task to create Maintenance Job*

○ Upgrade Citrix ADC/Upgrade Citrix ADC HA

○ Upgrade Citrix SD-WAN WO

○ Upgrade Citrix ADC SDX

● Configure HA Pair of Citrix ADC Instances

○ Convert HA Pair of Instances to 2 Node Cluster

3. On the **Citrix ADC HA Pair** page, in the **Instance Selection** tab:

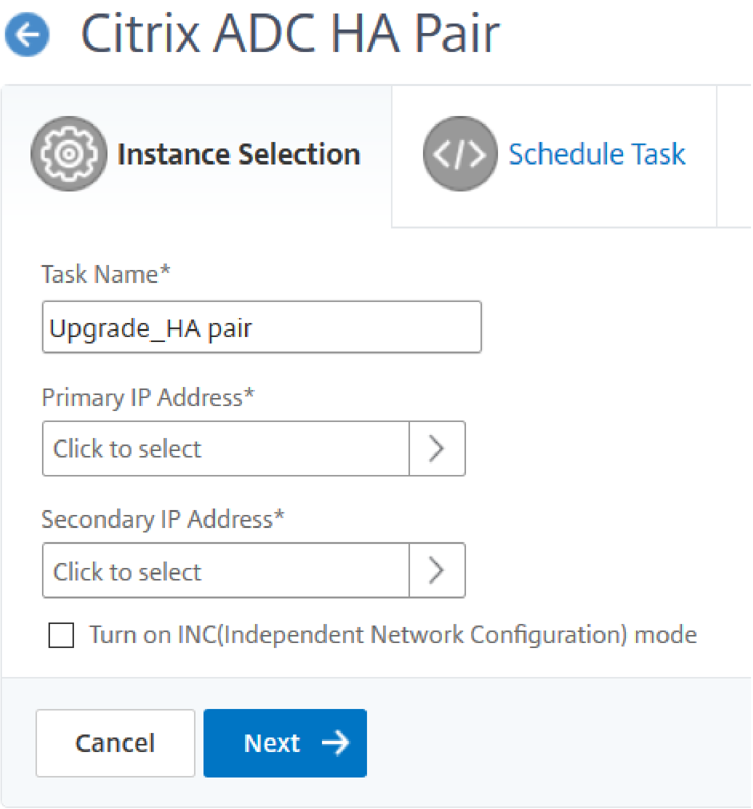
   a) Add a **Task Name**.

   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.



Citrix ADC HA Pair

Task Name*

Upgrade_HA pair

Primary IP Address*

Click to select

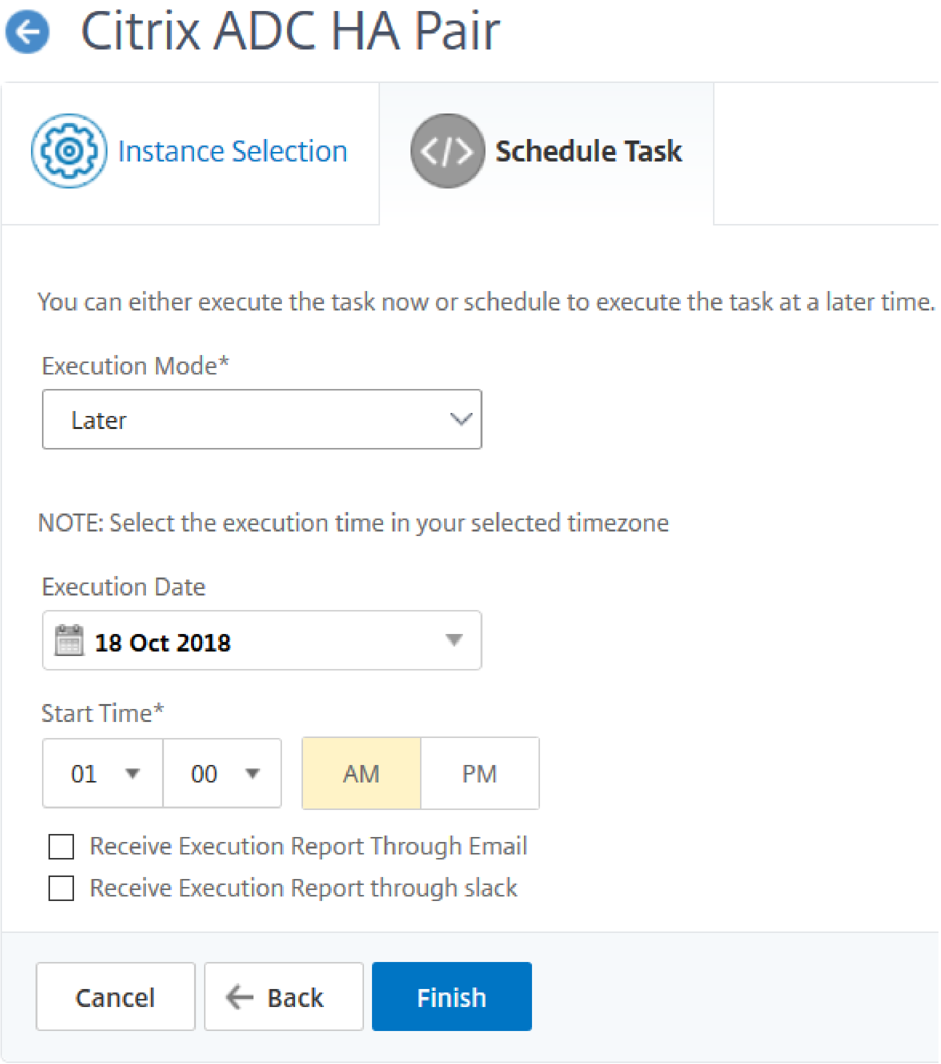
Secondary IP Address*

Click to select

□ Turn on INC(Independent Network Configuration) mode

4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a Citrix ADC instance now, and click **Finish**.

5. To upgrade a Citrix ADC HA pair later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the Citrix ADC instance, and click **Finish**.



Citrix ADC HA Pair

You can either execute the task now or schedule to execute the task at a later time.

Execution Mode*: Later

NOTE: Select the execution time in your selected timezone

Execution Date: 18 Oct 2018

Start Time*: 01 : 00 AM

□ Receive Execution Report Through Email

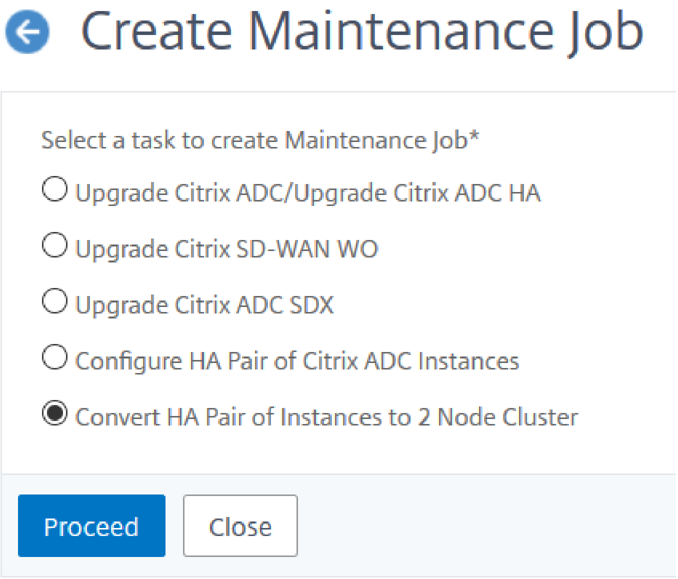
□ Receive Execution Report through slack

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 Citrix ADC instances

Schedule converting HA pair of instances to cluster

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**. Click the **Create Job** button.
2. Select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.



Create Maintenance Job

Select a task to create Maintenance Job*

○ Upgrade Citrix ADC/Upgrade Citrix ADC HA

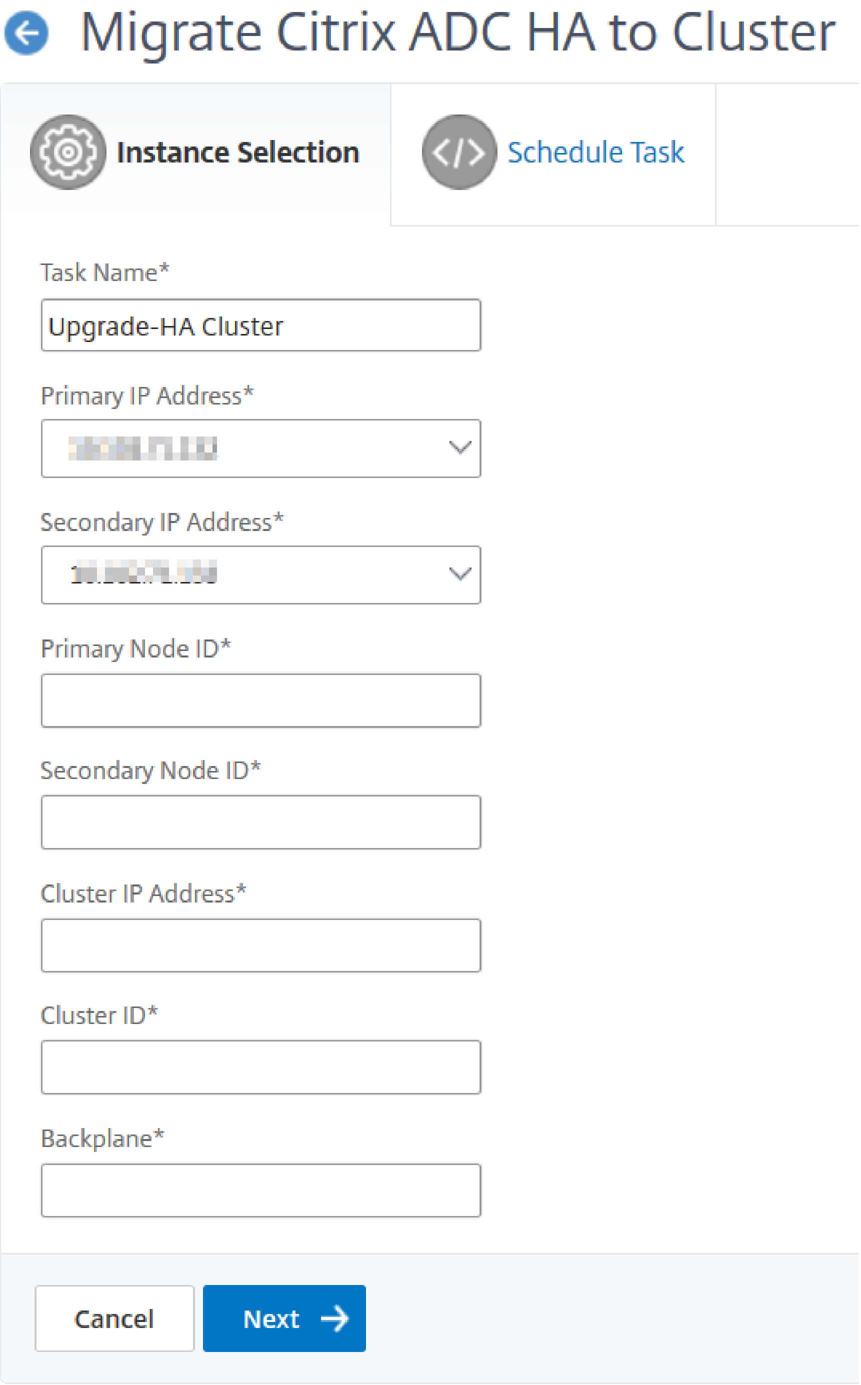
○ Upgrade Citrix SD-WAN WO

○ Upgrade Citrix ADC SDX

○ Configure HA Pair of Citrix ADC Instances

● Convert HA Pair of Instances to 2 Node Cluster

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**.



Migrate Citrix ADC HA to Cluster

Task Name*: Upgrade-HA Cluster

Primary IP Address*: [redacted]

Secondary IP Address*: [redacted]

Primary Node ID*:

Secondary Node ID*:

Cluster IP Address*:

Cluster ID*:

Backplane*:

4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a Citrix ADC 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 Citrix ADC HA pair instance, and click **Finish**.
6. You can also enable email and slack notifications to receive the execution report of upgrading a Citrix ADC 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 Citrix ADC instances

Use jobs to upgrade Citrix ADC instances

September 29, 2021

In Citrix Application Delivery and Management, you can upgrade one or more Citrix ADC instances. You must know the licensing framework and types of licenses before you upgrade an instance.

Prerequisites

Before you upgrade an ADC instance, do the pre-validation check on the instance that you want to upgrade.

1. **Check for disk space** - Clean up disk space to have a sufficient disk capacity for an instance upgrade. Resolve disk issues if any.
2. **Check for disk hardware issues** - Resolve the hardware issues if any.
3. **Check for customizations** - Back up your customizations and delete them from the instances. You can reapply the backed-up customizations after the instance upgrade.
4. **Policy issues** - ADC does not support classic policies from `13.1` version. Before upgrading an instance to this version, migrate classic policies to advanced policies.

   For more information, see Classic and advanced policies.

ADC high-availability pair

When you upgrade an ADC high-availability pair, note the following:

- The secondary node is upgraded first.
- Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.
- After the successful high-availability pair upgrade, an error message appears in the execution history. This message appears if your nodes in the high-availability pair are on different builds or versions. It indicates that synchronization between primary and secondary node is disabled.

You can upgrade an ADC high-availability pair in two stages:

1. Create an upgrade job and run on one of the nodes immediately or schedule later.

2. Schedule the upgrade job to run on the remaining node later. Ensure to schedule this job after the initial node's upgrade.

ADC clusters

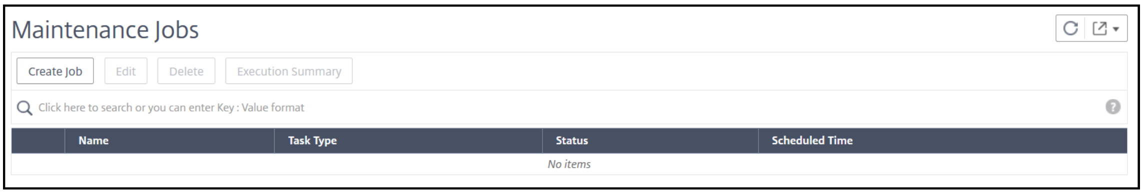
When you upgrade an ADC cluster, in the pre-upgrade validation stage, the Citrix Application Delivery and Management only validates the specified instance. So, check and resolve the following issues on the cluster nodes:

- Customization
- Disk usage
- hardware issues

Create an ADC upgrade job

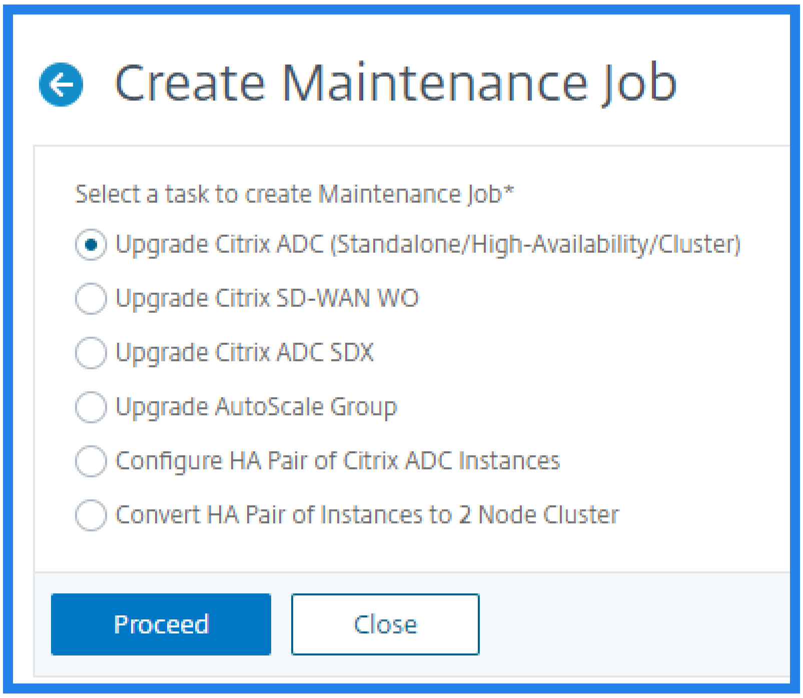
To create an ADC upgrade job, do the following:

1. Navigate to **Infrastructure > Configuration job > Maintenance Jobs**.



Name	Task Type	Status	Scheduled Time
		No items	

2. In **Create Maintenance Jobs**, select **Upgrade Citrix ADC (Standalone/High-Availability/Cluster)** and click **Proceed**.



Select a task to create Maintenance Job*

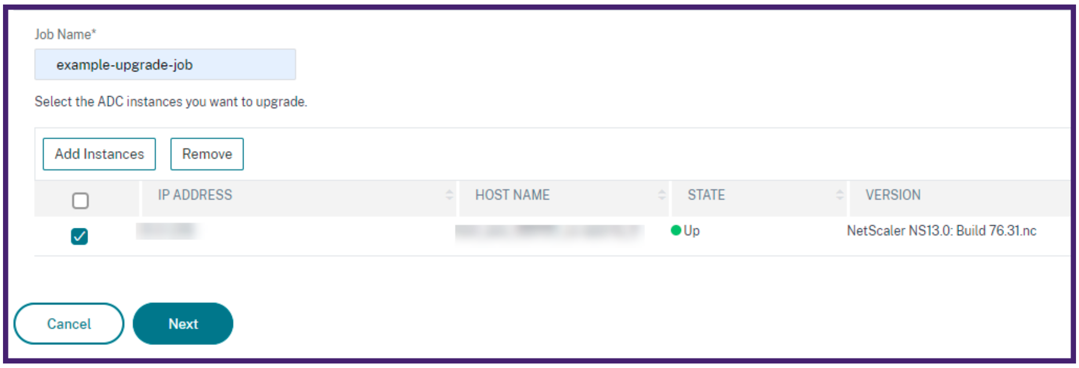
- ● Upgrade Citrix ADC (Standalone/High-Availability/Cluster)
- ○ Upgrade Citrix SD-WAN WO
- ○ Upgrade Citrix ADC SDX
- ○ Upgrade AutoScale Group
- ○ Configure HA Pair of Citrix ADC Instances
- ○ Convert HA Pair of Instances to 2 Node Cluster

3. In the **Select Instance** tab,

   a) Specify a name of your choice for **Job Name**.

   b) Click **Add Instances** to add ADC instances that you want to upgrade.

      - To upgrade an ADC high-availability pair, specify the IP address of either the primary or secondary node.
      - To upgrade a cluster, specify the cluster IP address.



Job Name*

example-upgrade-job

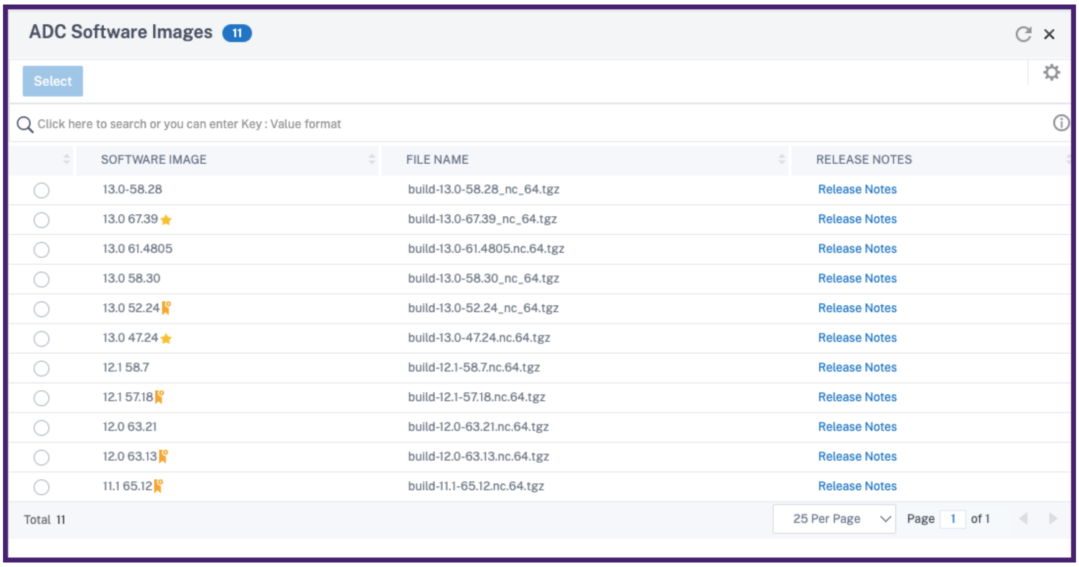
Select the ADC instances you want to upgrade.

□	IP ADDRESS	HOST NAME	STATE	VERSION
☑	[redacted]	[redacted]	● Up	NetScaler NS13.0: Build 76.31.nc

   c) Click **Next**.

4. In the **Select Image** tab, select an ADC image from the image library or local or appliance.

   - **Select from Image Library**: Select an ADC image from the list. This option lists all ADC images that are available in the Citrix Downloads website.



ADC Software Images 11

Click here to search or you can enter Key : Value format

	SOFTWARE IMAGE	FILE NAME	RELEASE NOTES
○	13.0-58.28	build-13.0-58.28_nc_64.tgz	Release Notes
○	13.0 67.39 ★	build-13.0-67.39_nc_64.tgz	Release Notes
○	13.0 61.4805	build-13.0-61.4805.nc.64.tgz	Release Notes
○	13.0 58.30	build-13.0-58.30_nc_64.tgz	Release Notes
○	13.0 52.24 🔖	build-13.0-52.24_nc_64.tgz	Release Notes
○	13.0 47.24 ★	build-13.0-47.24.nc.64.tgz	Release Notes
○	12.1 58.7	build-12.1-58.7.nc.64.tgz	Release Notes
○	12.1 57.18 🔖	build-12.1-57.18.nc.64.tgz	Release Notes
○	12.0 63.21	build-12.0-63.21.nc.64.tgz	Release Notes
○	12.0 63.13 🔖	build-12.0-63.13.nc.64.tgz	Release Notes
○	11.1 65.12 🔖	build-11.1-65.12.nc.64.tgz	Release Notes

Total 11

The ADC software images display the preferred builds with the star icon. And, most downloaded builds with the bookmark icon.

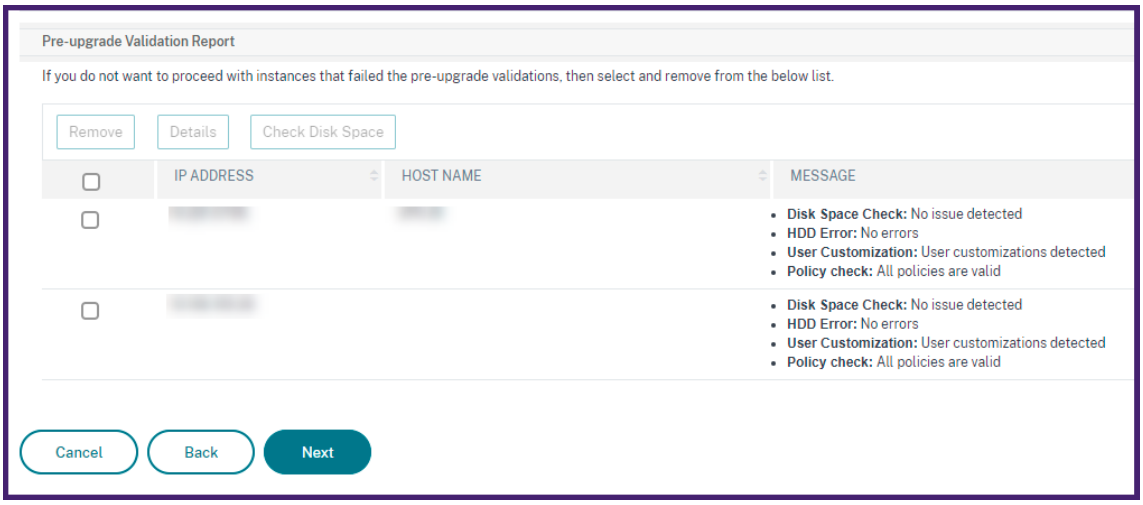
   - **Select from local or appliance**: You can upload the image from your local computer or the ADC appliance. When you select ADC appliance, the Citrix Application Delivery and

Management GUI displays the instance files that are present in `/var/mps/ns_images`. Select the image from the Citrix Application Delivery and Management GUI.

- **Skip image uploading to ADC if the selected image is already available** - This option checks whether the selected image is available in ADC. Upgrade job skips uploading a new image and uses the image available in ADC.
- **Clean software image from Citrix ADC on successful upgrade** - This option clears the uploaded image in the ADC instance after the instance upgrade.

Click **Next** to start the pre-upgrade validation on the selected instances.

5. The **Pre-upgrade validation** tab displays the failed instances. you can remove the failed instances and click **Next**.



Pre-upgrade Validation Report

If you do not want to proceed with instances that failed the pre-upgrade validations, then select and remove from the below list.

□	IP ADDRESS	HOST NAME	MESSAGE
□	[redacted]	[redacted]	**Disk Space Check:** No issue detected **HDD Error:** No errors **User Customization:** User customizations detected **Policy check:** All policies are valid
□	[redacted]		**Disk Space Check:** No issue detected **HDD Error:** No errors **User Customization:** User customizations detected **Policy check:** All policies are valid

- **Disk Space Check**: If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up ADC disk space.
- **Policy Check**: If Citrix Application Delivery and Management finds unsupported classic policies, you can remove such policies to create an upgrade job.

> **Important**
>
> If you specify cluster IP address, the Citrix Application Delivery and Management does pre-upgrade validation only on the specified instance not on the other cluster nodes.

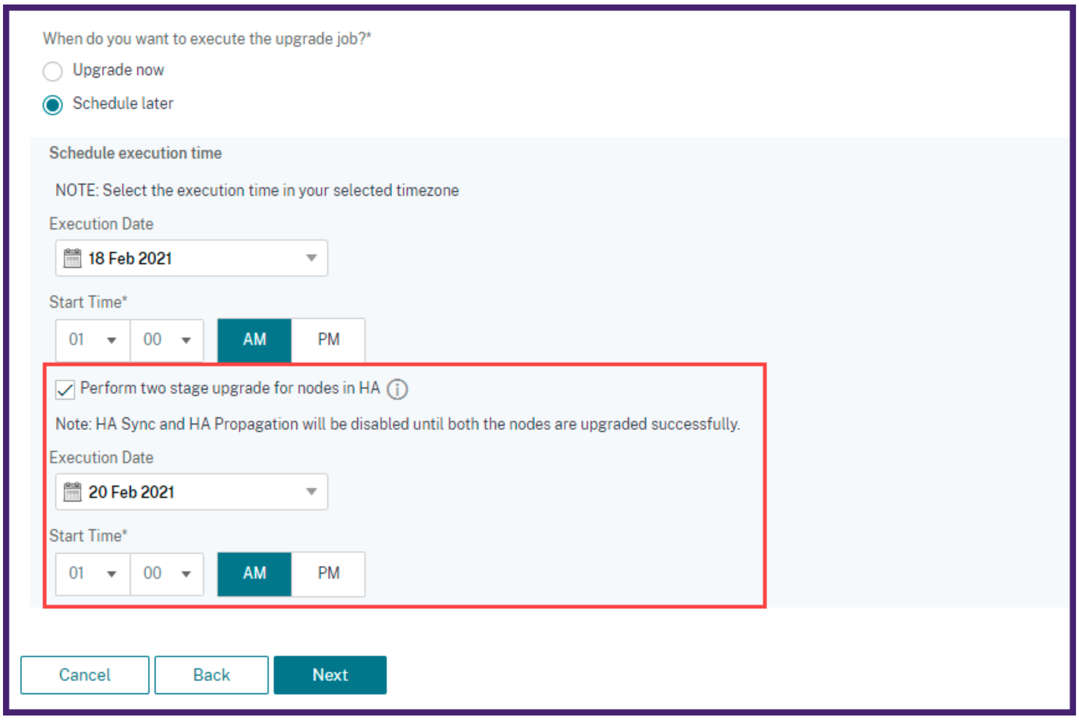
6. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. For more information, see Use custom scripts.

7. 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 high-availability pair in two stages, select **Perform two stage upgrade for nodes in high-availability**.

Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the high-availability pair.


When do you want to execute the upgrade job?*

○ Upgrade now

● Schedule later

Schedule execution time

NOTE: Select the execution time in your selected timezone

Execution Date: 18 Feb 2021

Start Time*: 01 : 00 AM

☑ Perform two stage upgrade for nodes in HA

Note: HA Sync and HA Propagation will be disabled until both the nodes are upgraded successfully.

Execution Date: 20 Feb 2021

Start Time*: 01 : 00 AM

For more information, see ADC high-availability pair.

8. In **Create Job**, specify the following details:

   If you schedule the upgrade job, you can 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.

   For more information on other upgrade options, see ADC upgrade options.

9. Click **Create Job**.

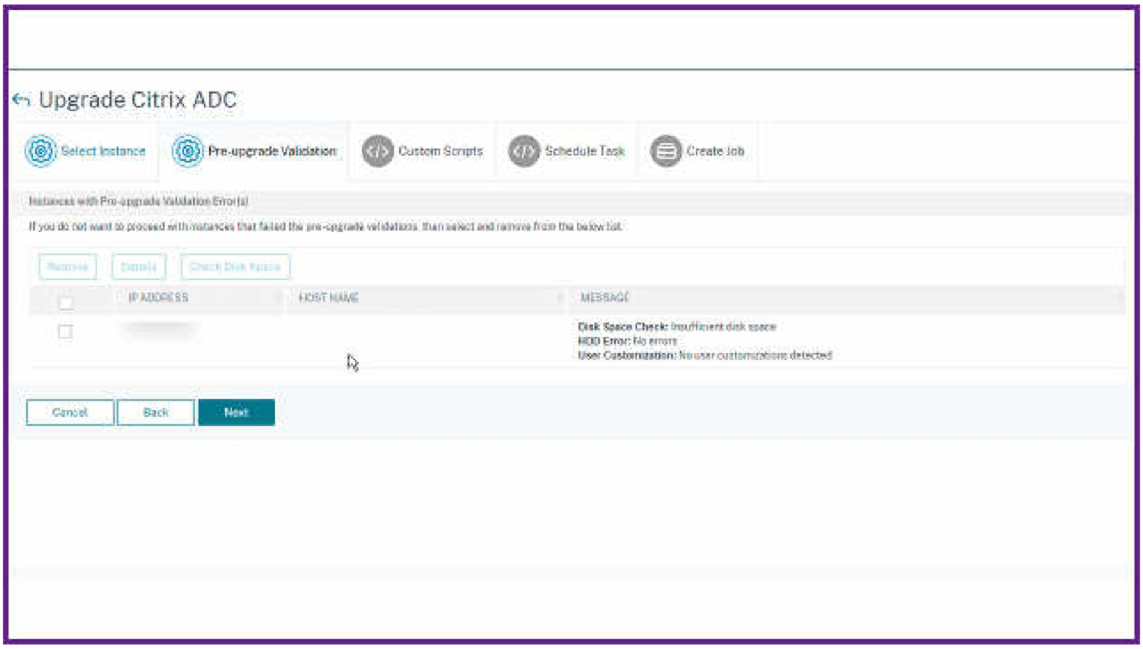
The upgrade job appears in the **Infrastructure > Configuration job > Maintenance Jobs**. When you edit an existing job, you can switch to any tabs if the required fields are already filled. For example, if you are in the **Select Configuration** tab, you can switch to the **Job Preview** tab.

Clean up the ADC disk space

If you face the insufficient disk space issue while upgrading an ADC instance, clean up the disk space from the Citrix Application Delivery and Management GUI itself.

1. In the **Pre-upgrade validation** tab, select the instance that has the disk space issue.
2. Select **Check Disk Space**.

   This pane displays the instance's disk that has low space. It also displays how much memory is used and available on the disk.
3. In the **Check Disk Space** pane, select the instance that requires cleanup.
4. Click **Disk Cleanup**.

   Instances with Pre-upgrade Validation Error(s)

   If you do not want to proceed with instances that failed the pre-upgrade validations, then select and remove from the below list.

□	IP ADDRESS	HOST NAME	MESSAGE
□	[redacted]		**Disk Space Check:** Insufficient disk space **HDD Error:** No errors **User Customization:** No user customizations detected

5. Select the files that you want to erase.
6. Click **Delete**

Use custom scripts

You can specify custom scripts while you create an ADC upgrade job. The custom scripts are used to check the changes before and after an ADC 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.

Specify the custom scripts to run in the following stages:

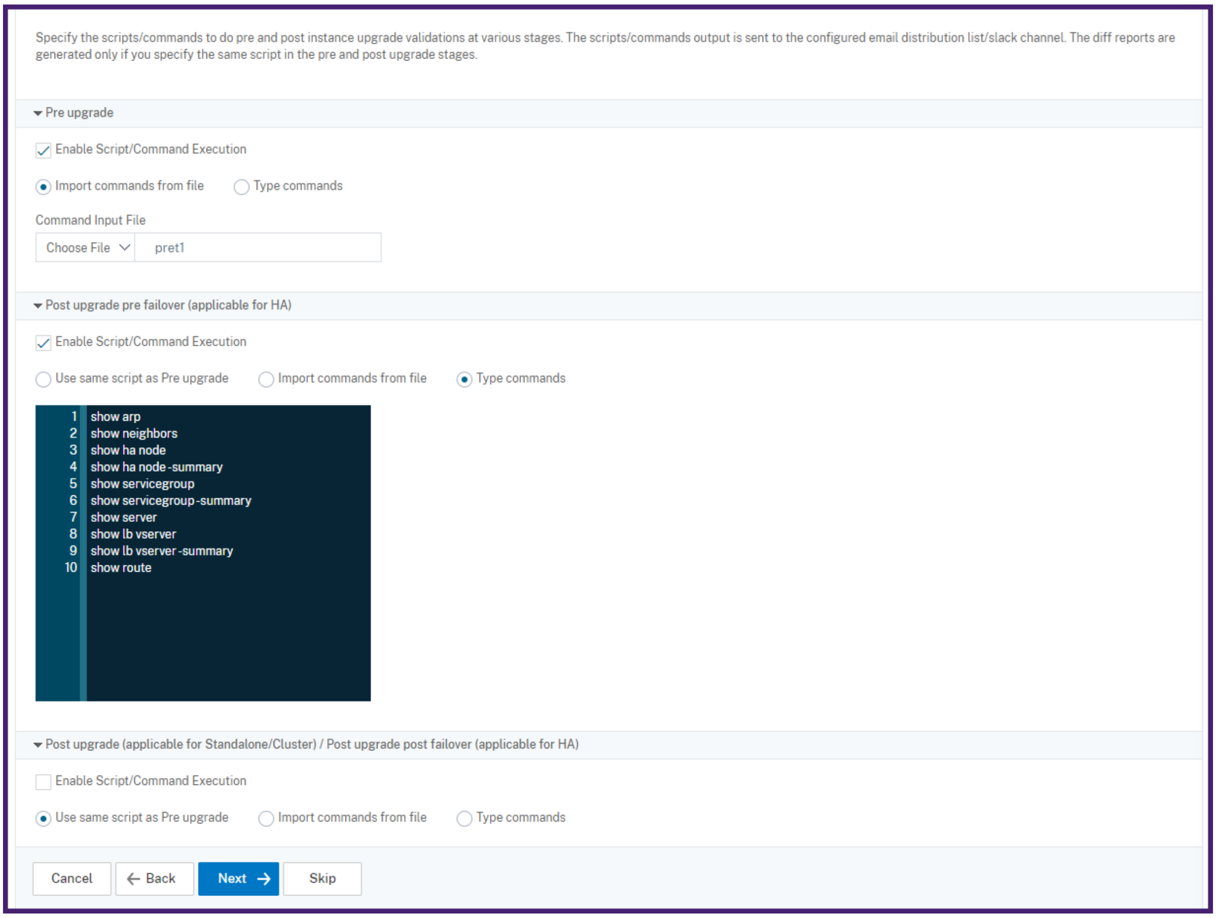
- **Pre upgrade**: The specified script runs before upgrading an instance.
- **Post upgrade pre failover (applicable for HA)**: This stage only applies to the high-availability deployment. The specified script runs after upgrading the nodes, but before their failover.
- **Post upgrade (applicable for standalone) / Post upgrade post failover (applicable for HA)**: The specified script runs after upgrading an instance in the standalone deployment. In the high-availability deployment, the script runs after upgrading the nodes and their failover.

> **Note**
>
> - Ensure to enable script or commands execution at the required stages. Otherwise, the specified scripts do not run.
> - The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages. So, ensure to select **Use same script as Pre-upgrade** in the post-upgrade stages. See, Download a consolidated diff report of an ADC upgrade job.

You can import a script file or type commands directly in the Citrix Application Delivery and Management GUI.

- **Import commands from file**: Select the command input file from your local computer.
- **Type commands**: Enter commands directly on the GUI.

In the post upgrade stages, you can use the same script specified in the pre-upgrade stage.



Specify the scripts/commands to do pre and post instance upgrade validations at various stages. The scripts/commands output is sent to the configured email distribution list/slack channel. The diff reports are generated only if you specify the same script in the pre and post upgrade stages.

▾ Pre upgrade

☑ Enable Script/Command Execution

● Import commands from file ○ Type commands

Command Input File

Choose File: pret1

▾ Post upgrade pre failover (applicable for HA)

☑ Enable Script/Command Execution

○ Use same script as Pre upgrade ○ Import commands from file ● Type commands

```
show arp
show neighbors
show ha node
show ha node -summary
show servicegroup
show servicegroup -summary
show server
show lb vserver
show lb vserver -summary
show route
```

▾ Post upgrade (applicable for Standalone/Cluster) / Post upgrade post failover (applicable for HA)

☐ Enable Script/Command Execution

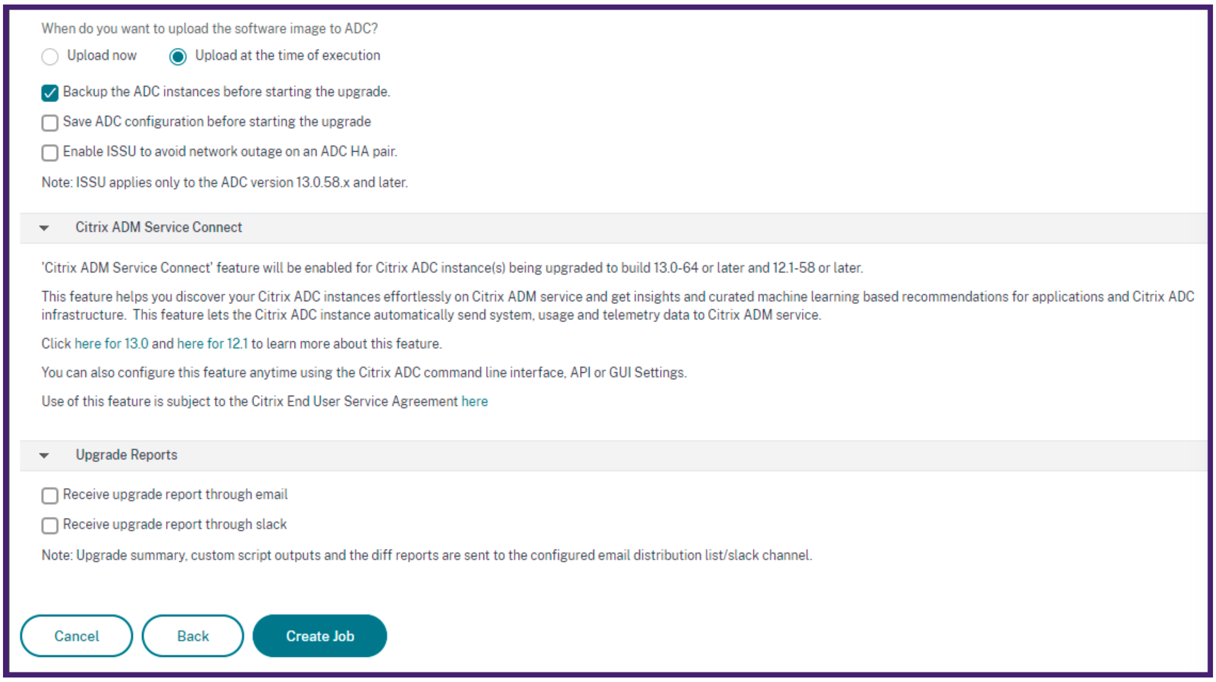
● Use same script as Pre upgrade ○ Import commands from file ○ Type commands

ADC upgrade options

While you create an ADC upgrade job, you can select the following options in the **Create Job** tab:

- **Backup the ADC instances before starting the upgrade.**: Creates a backup of the selected ADC instances.
- **Maintain the primary and secondary status of high-availability nodes after upgrade**: Select this option if you want the upgrade job to start a failover after each node's upgrade. In this way, the upgrade job maintains the primary and secondary status of the nodes.
- **Save ADC configuration before starting the upgrade** - Saves the running ADC configuration before upgrading the ADC instances.
- **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 high-availability pair without downtime. Specify the ISSU migration timeout in minutes.
- **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.



When do you want to upload the software image to ADC?

○ Upload now ● Upload at the time of execution

☑ Backup the ADC instances before starting the upgrade.

□ Save ADC configuration before starting the upgrade

□ Enable ISSU to avoid network outage on an ADC HA pair.

Note: ISSU applies only to the ADC version 13.0.58.x and later.

Citrix ADM Service Connect

'Citrix ADM Service Connect' feature will be enabled for Citrix ADC instance(s) being upgraded to build 13.0-64 or later and 12.1-58 or later.

This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to Citrix ADM service.

Click here for 13.0 and here for 12.1 to learn more about this feature.

You can also configure this feature anytime using the Citrix ADC command line interface, API or GUI Settings.

Use of this feature is subject to the Citrix End User Service Agreement here

Upgrade Reports

□ Receive upgrade report through email

□ Receive upgrade report through slack

Note: Upgrade summary, custom script outputs and the diff reports are sent to the configured email distribution list/slack channel.

Download a consolidated diff report of an ADC upgrade job

In Citrix Application Delivery and Management, you can download a diff report of an ADC upgrade job. To do so, the upgrade job must have custom scripts. A diff report contains the differences between the outputs of the pre-upgrade and post-upgrade script. With this report, you can determine what changes occurred on the ADC instance post upgrade.

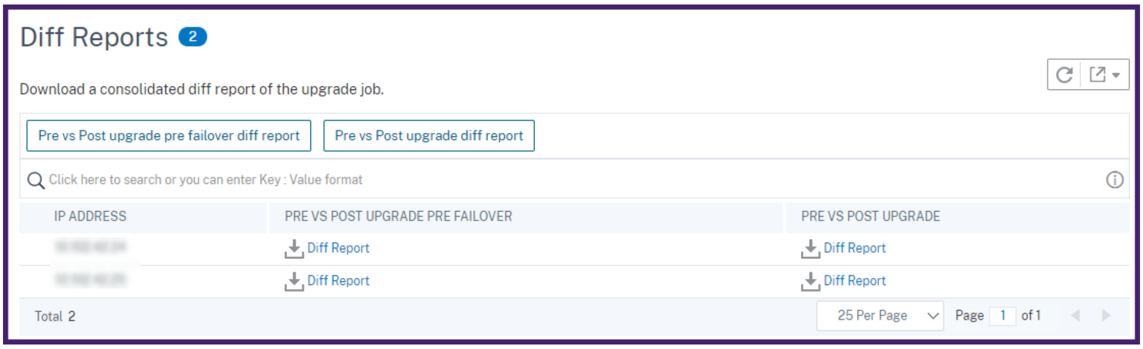
> **Note**
>
> The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages.

To download a diff report of an upgrade job, do the following:

1. Navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**.
2. Select the upgrade job for which you want to download a diff report.
3. Click **Diff Reports**.
4. In **Diff Reports**, download a consolidated diff report of the selected upgrade job.

   In this page, you can download any of the following diff reports type:

   - **Pre vs Post upgrade pre failover diff report**
   - **Pre vs Post upgrade diff report**



Diff Reports 2

Download a consolidated diff report of the upgrade job.

Pre vs Post upgrade pre failover diff report
Pre vs Post upgrade diff report
Click here to search or you can enter Key : Value format

IP ADDRESS	PRE VS POST UPGRADE PRE FAILOVER	PRE VS POST UPGRADE
[redacted]	Diff Report	Diff Report
[redacted]	Diff Report	Diff Report

Total 2

Network functions

September 28, 2021

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix Application Delivery Controller (Citrix 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
- Load Balancing Method
- Load Balancing Persistence

Generate reports for load balancing entities

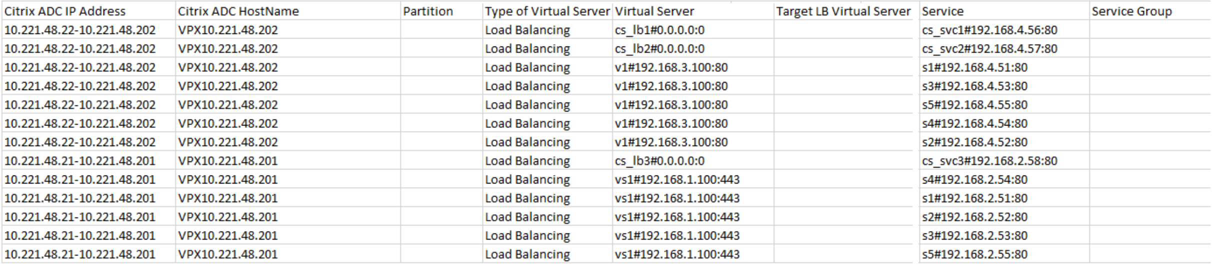
September 24, 2021

Citrix Application Delivery and Management allows you to view the reports of Citrix Application Delivery Controller (Citrix ADC) instance entities at all levels. There are two types of reports that you can download in **Citrix Application Delivery and Management > 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 Citrix ADC instances.

This report allows you to have a high-level view of the mapping between the Citrix ADC 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
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb1#0.0.0.0:0		cs_svc1#192.168.4.56:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb2#0.0.0.0:0		cs_svc2#192.168.4.57:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s1#192.168.4.51:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s3#192.168.4.53:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s5#192.168.4.55:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s4#192.168.4.54:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s2#192.168.4.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	cs_lb3#0.0.0.0:0		cs_svc3#192.168.2.58:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s4#192.168.2.54:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s1#192.168.2.51:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s2#192.168.2.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s3#192.168.2.53:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s5#192.168.2.55:80	

The consolidated report is in a CSV format. The entries in each column are described as follows:

- **Citrix ADC IP Address**: IP address of the Citrix ADC instance is displayed in the report
- **Citrix ADC 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

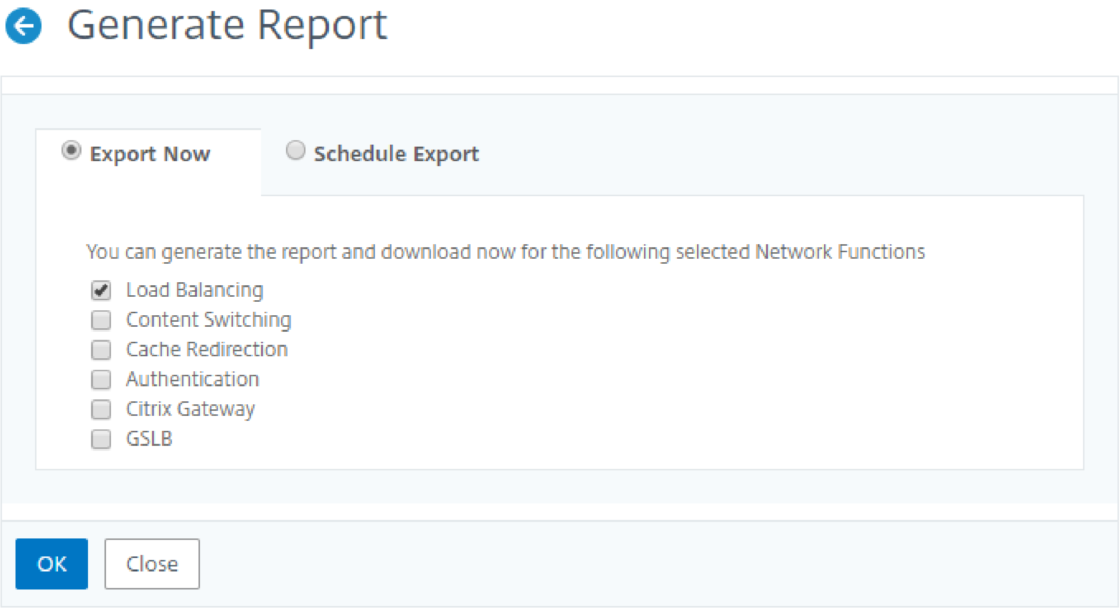
> **Note**
>
> - If there is no host name available, the corresponding IP address is displayed.
> - Blank columns indicate that the respective entities are not configured for that Citrix ADC instance.

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.

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, navigate to **Infrastructure > Network Functions**.
2. Click **Generate Report**.



Generate Report

● Export Now ○ Schedule Export

You can generate the report and download now for the following selected Network Functions

☑ Load Balancing
□ Content Switching
□ Cache Redirection
□ Authentication
□ Citrix Gateway
□ GSLB

3. On the **Generate Report** page that opens, you have two options to view the report:
    a) On the **Export Now** tab, select **Load Balancing** and click **OK**.

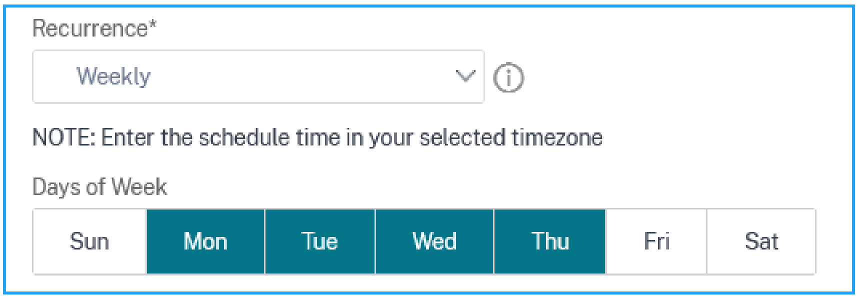
       The consolidated report downloads to your system.

    b) Select **Schedule Report** to create a schedule for generating and exporting reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

       i. Select **Enable Schedule**.

       ii. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the list.

> **Note**
>
> If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.



Recurrence*

Weekly

NOTE: Enter the schedule time in your selected timezone

Days of Week

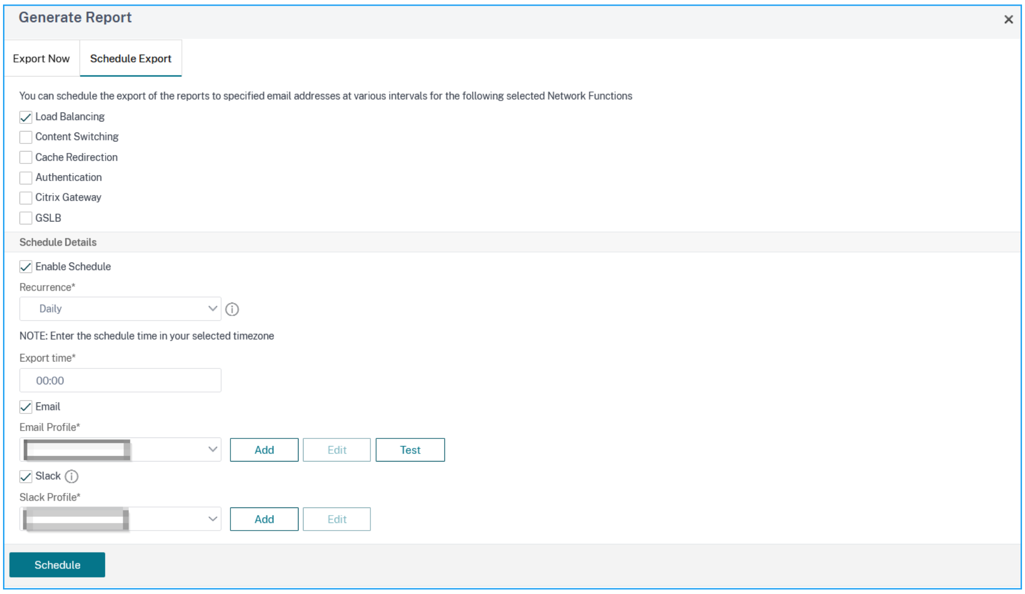
> **Note**
>
> If you select **Monthly** recurrence, ensure that you enter days of month, with the values between 1 and 31.

iii. **Export time** - Enter the time in the Hour: Minute in 24-hour format.

iv. **Email** - check the check-box and then select a profile from the list, or click **Add** to create an email profile.

v. **Slack** - Select the Slack check box and then select a profile from the list box, or click **Add** to create a slack profile.

vi. Click **Schedule** to complete the process.



Generate Report

You can schedule the export of the reports to specified email addresses at various intervals for the following selected Network Functions

☑ Load Balancing

□ Content Switching

□ Cache Redirection

□ Authentication

□ Citrix Gateway

□ GSLB

Schedule Details

☑ Enable Schedule

Recurrence*

Daily

NOTE: Enter the schedule time in your selected timezone

Export time*

00:00

☑ Email

Email Profile*

[redacted]

☑ Slack

Slack Profile*

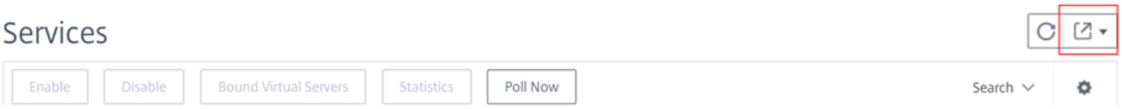
[redacted]

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 Citrix Application Delivery and Management, navigate to **Infrastructure > Network Functions > Load Balancing > Services**.

2. On **Services** page, click the **Export** button at the top right-hand corner.



Select **Export Now** tab if you want to generate and view the report at this instant.

> **Note**
>
> You can only download the reports or export the reports as mail attachments. You cannot view the reports on the Citrix Application Delivery and Management GUI.

Export or schedule export of network functions reports

September 28, 2021

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 Citrix Gateway in Citrix Application Delivery and Management. This report allows you to have a high-level view of the mapping between the 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:

- Citrix ADC 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.

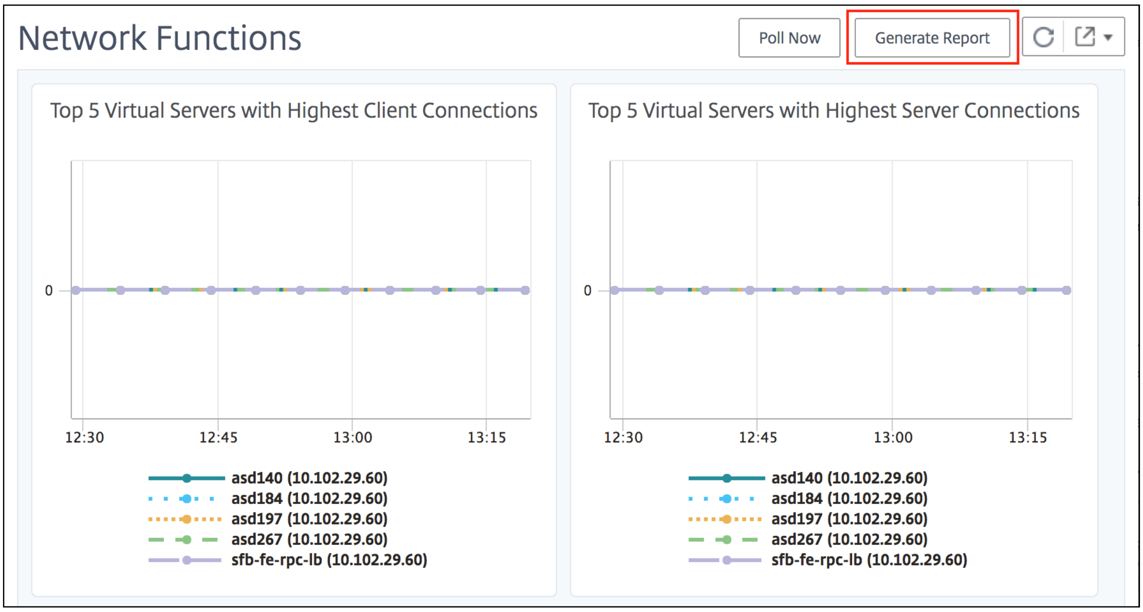
- Service name
- Service group name

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 Citrix Application Delivery and Management.
> - When a new report is generated, the older reports are automatically purged from your account.

To export and schedule network functions reports:

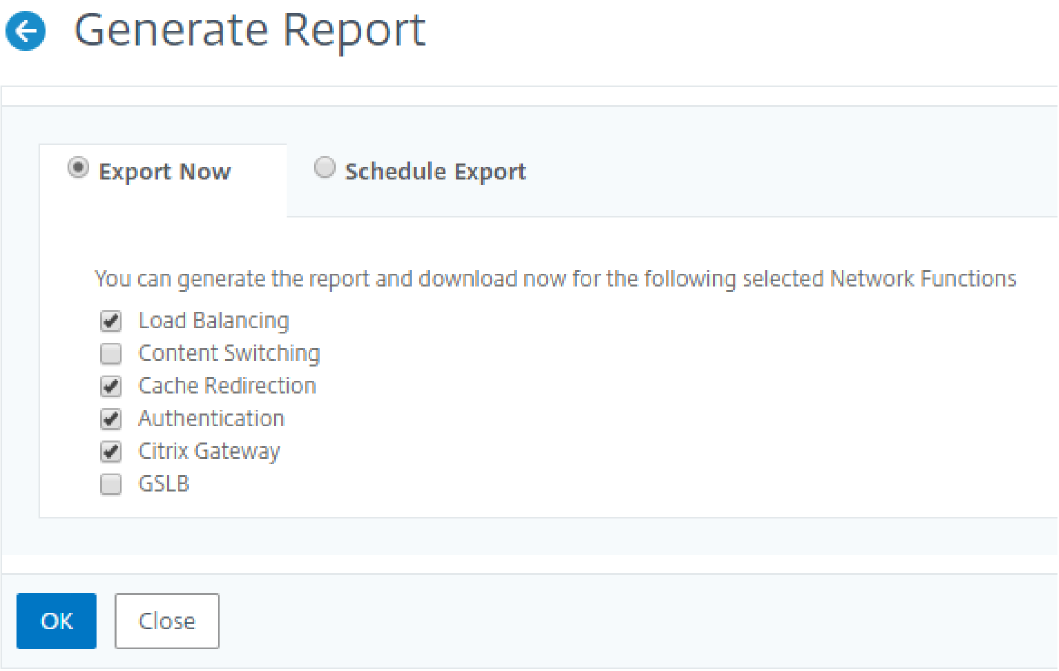
1. Navigate to **Infrastructure > Network Functions**.
2. On the **Network Functions** page, in the right pane, click **Generate Report** at the top right corner of the page.



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.



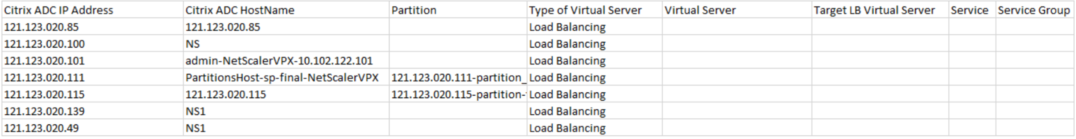
Generate Report

● Export Now ○ Schedule Export

You can generate the report and download now for the following selected Network Functions

☑ Load Balancing
□ Content Switching
☑ Cache Redirection
☑ Authentication
☑ Citrix Gateway
□ GSLB

The following image shows an example of a network functions report.



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
121.123.020.85	121.123.020.85		Load Balancing				
121.123.020.100	NS		Load Balancing				
121.123.020.101	admin-NetScalerVPX-10.102.122.101		Load Balancing				
121.123.020.111	PartitionsHost-sp-final-NetScalerVPX	121.123.020.111-partition_	Load Balancing				
121.123.020.115	121.123.020.115	121.123.020.115-partition-	Load Balancing				
121.123.020.139	NS1		Load Balancing				
121.123.020.49	NS1		Load Balancing				

b) Select **Schedule Report** the tab to create a schedule to generate and export reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

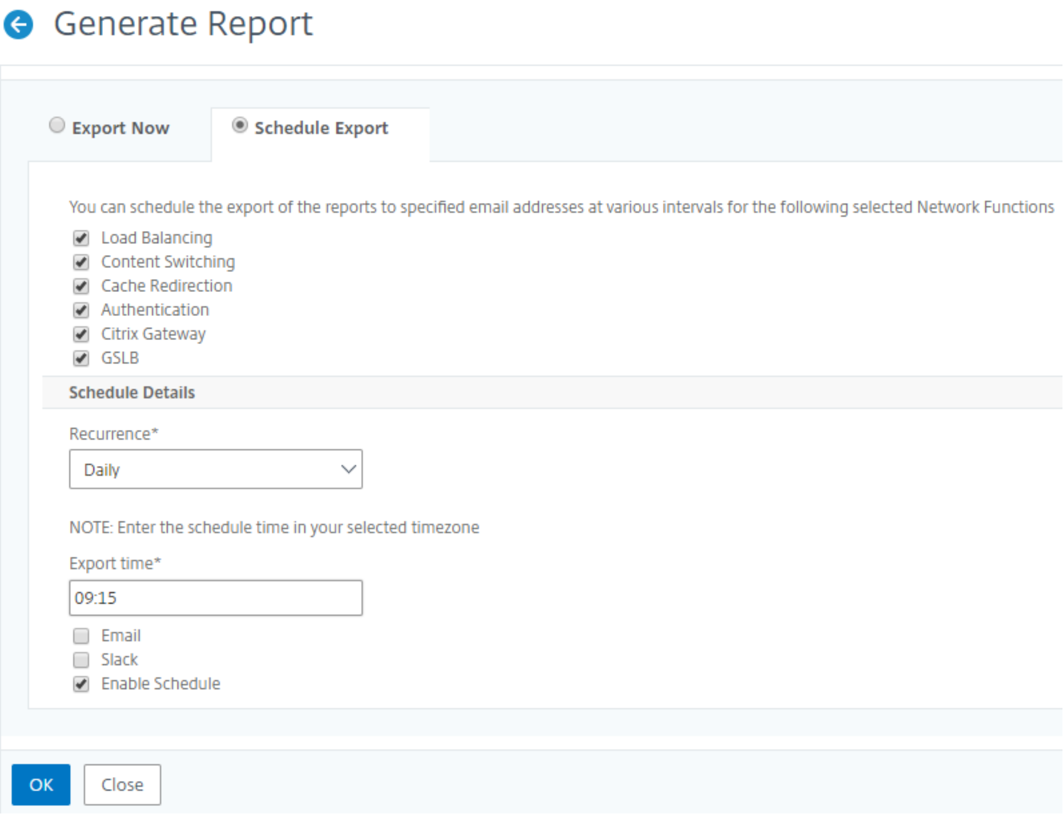
i. **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

ii. **Recurrence time** - Enter the time in the Hour: Minute in 24-hour format.

iii. **Email** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

iv. **Slack** - Select the check box and then select the profile from the drop-down list box, or click **Add** 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.



Generate Report

○ Export Now ● Schedule Export

You can schedule the export of the reports to specified email addresses at various intervals for the following selected Network Functions

☑ Load Balancing
☑ Content Switching
☑ Cache Redirection
☑ Authentication
☑ Citrix Gateway
☑ GSLB

Schedule Details

Recurrence*: Daily

NOTE: Enter the schedule time in your selected timezone

Export time*: 09:15

□ Email
□ Slack
☑ Enable Schedule

Network reporting

September 28, 2021

You can optimize resource usage by monitoring your network reporting on Citrix Application Delivery and Management. 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 (Citrix ADC) 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.

Citrix Application Delivery and Management 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 virtual servers for which you can generate reports are as follows:

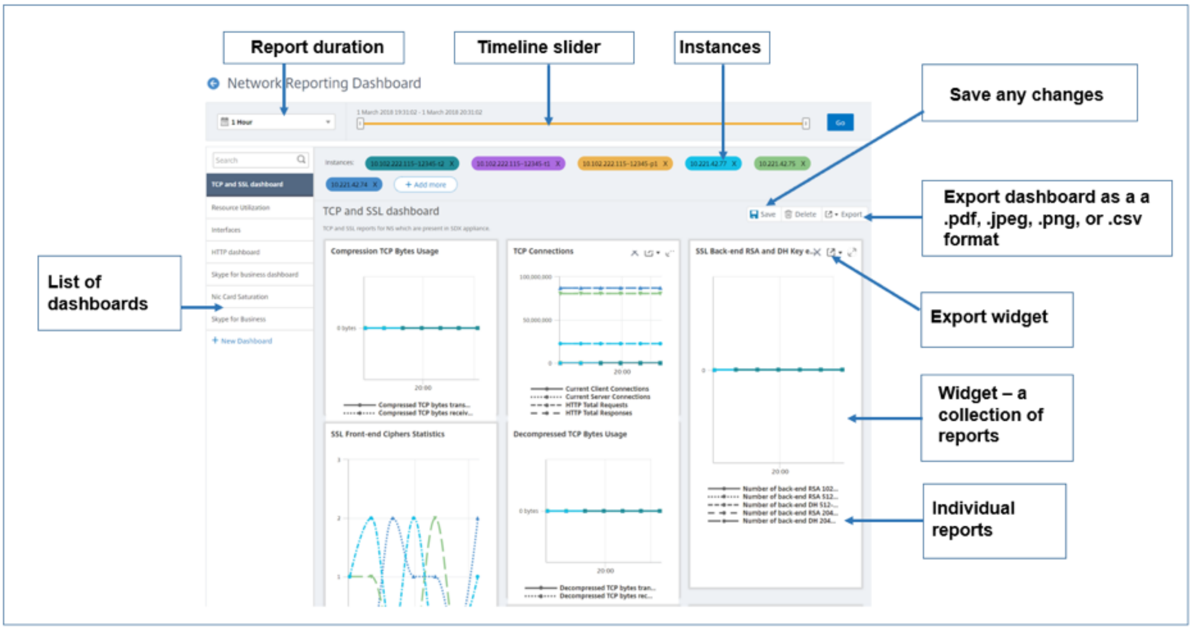
- Load balancing servers, services, and service groups
- Content switching servers
- Cache redirection servers
- Global service load balancing (GSLB)

- Authentication
- Citrix Gateway

The network reporting dashboard in Citrix Application Delivery and Management is a highly customizable. You can 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:


Report duration
Timeline slider
Instances
Save any changes
Export dashboard as a a .pdf, .jpeg, .png, or .csv format
List of dashboards
Export widget
Widget – a collection of reports
Individual reports
Network Reporting Dashboard
TCP and SSL dashboard
Compression TCP Bytes Usage
TCP Connections
SSL Back-end RSA and DH Key e...
SSL Front-end Ciphers Statistics
Decompressed TCP Bytes Usage

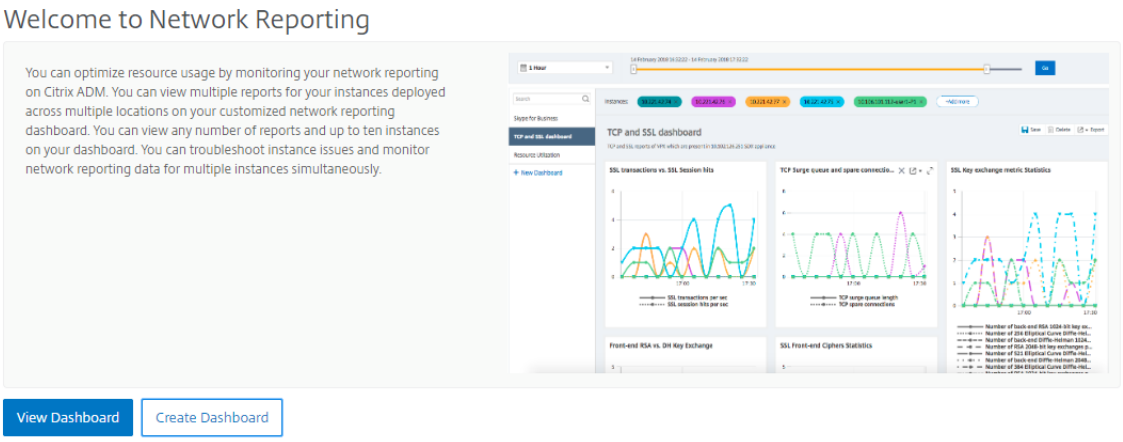
- The left side panel lists all the custom dashboards that are created in Citrix Application Delivery and Management. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- 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 Citrix Application Delivery and Management.
- 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 to generate the report. You can also configure an email distribution list to which you want to send the reports.
- 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 Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, navigate to **Infrastructure > Network Reporting**.



Welcome to Network Reporting

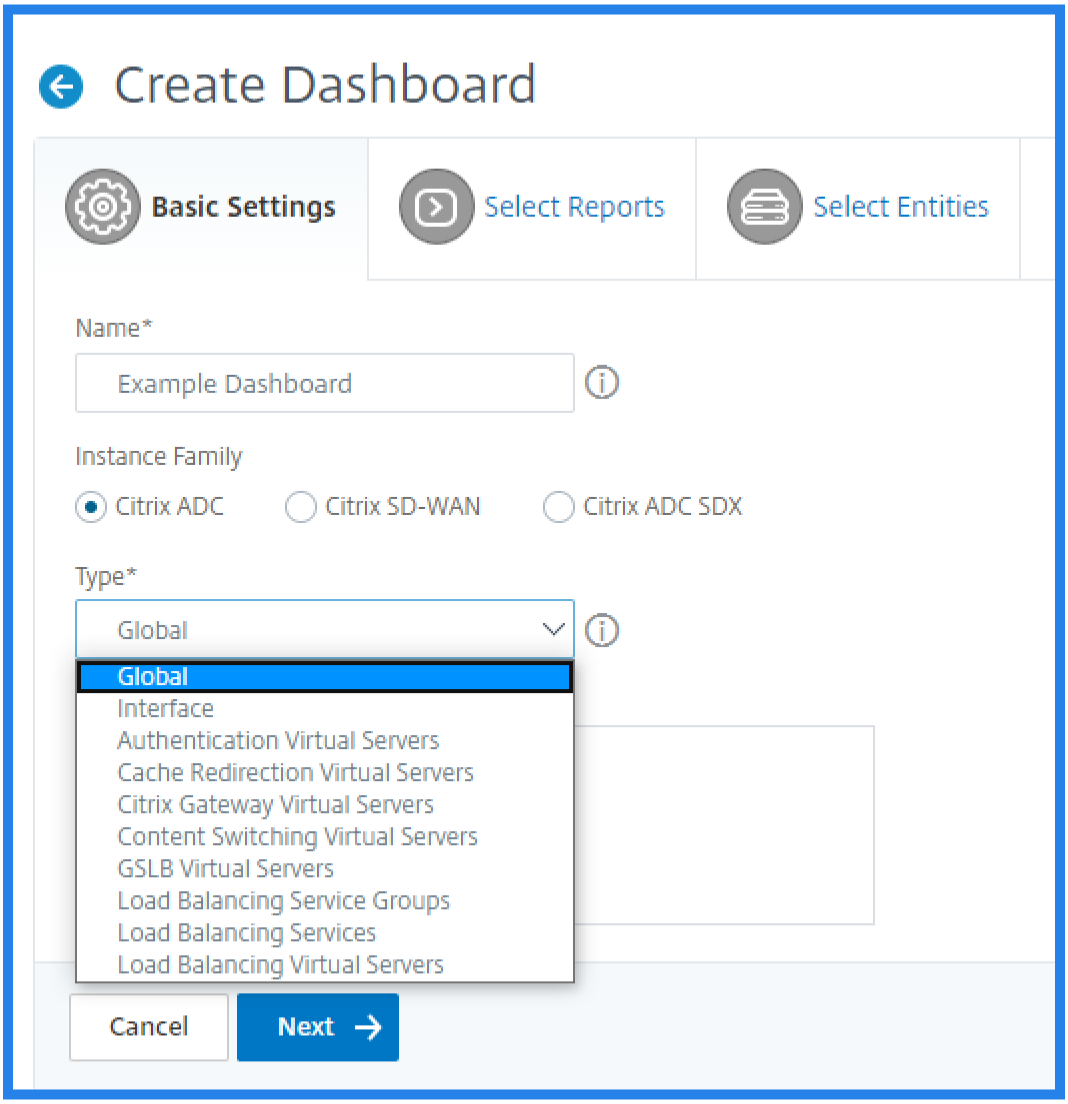
You can optimize resource usage by monitoring your network reporting on Citrix ADM. You can view multiple reports for your instances deployed across multiple locations on your customized network reporting dashboard. You can view any number of reports and up to ten instances on your dashboard. You can troubleshoot instance issues and monitor network reporting data for multiple instances simultaneously.

TCP and SSL dashboard
SSL transactions vs. SSL Session hits
TCP Surge queue and spare connectio...
SSL Key exchange metric Statistics
Front-end RSA vs. DH Key Exchange
SSL Front-end Ciphers Statistics
View Dashboard
Create Dashboard

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 **Create Dashboard**.

   The **Create Dashboard** page opens.



Create Dashboard

Basic Settings | Select Reports | Select Entities

Name*

Example Dashboard

Instance Family

● Citrix ADC ○ Citrix SD-WAN ○ Citrix ADC SDX

Type*

Global

- Global
- Interface
- Authentication Virtual Servers
- Cache Redirection Virtual Servers
- Citrix Gateway Virtual Servers
- Content Switching Virtual Servers
- GSLB Virtual Servers
- Load Balancing Service Groups
- Load Balancing Services
- Load Balancing Virtual Servers

4. In the **Basic Settings** tab, enter the following details:

   a) **Name**. Type the name of the dashboard.

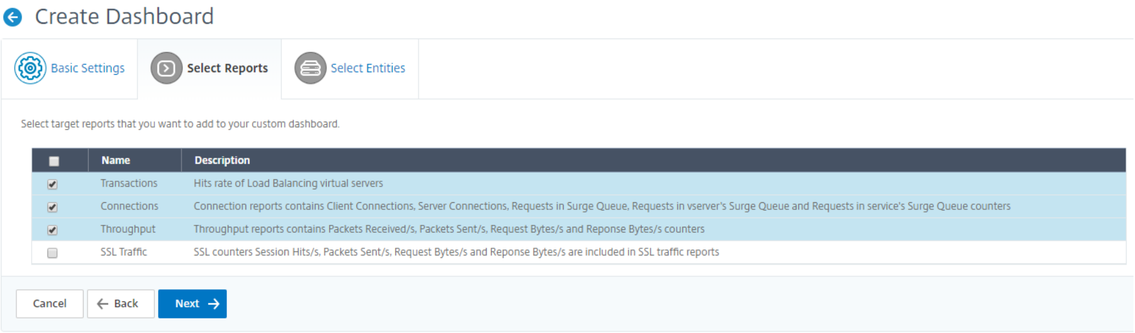
   b) **Instance Family**. Select the type of instance - Citrix ADC or Citrix ADC SDX.

   a) **Type**. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.

   b) **Description**. Type a meaningful description for the dashboard.

5. Click **Next**.

6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.



Create Dashboard

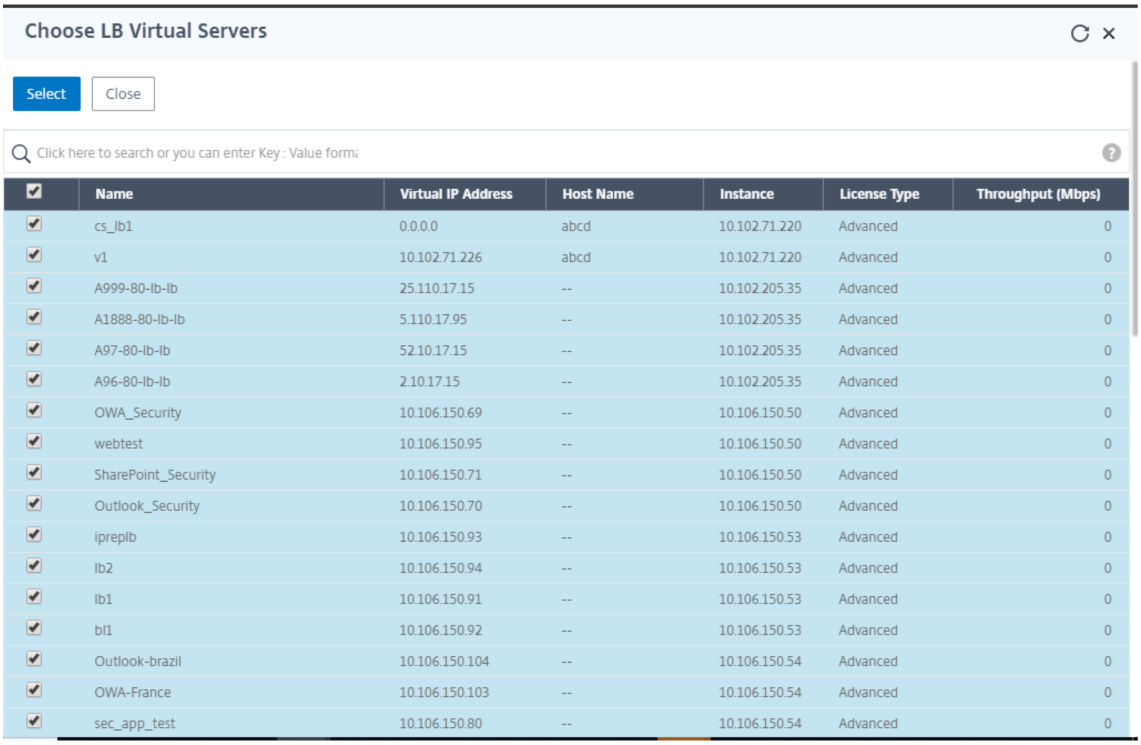
Select target reports that you want to add to your custom dashboard.

□	Name	Description
☑	Transactions	Hits rate of Load Balancing virtual servers
☑	Connections	Connection reports contains Client Connections, Server Connections, Requests in Surge Queue, Requests in vserver's Surge Queue and Requests in service's Surge Queue counters
☑	Throughput	Throughput reports contains Packets Received/s, Packets Sent/s, Request Bytes/s and Reponse Bytes/s counters
□	SSL Traffic	SSL counters Session Hits/s, Packets Sent/s, Request Bytes/s and Reponse Bytes/s are included in SSL traffic reports

7. 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, the **Choose LB Virtual Servers** window appears.

8. Select the entities that you want to monitor.



Choose LB Virtual Servers

☑	Name	Virtual IP Address	Host Name	Instance	License Type	Throughput (Mbps)
☑	cs_lb1	0.0.0.0	abcd	10.102.71.220	Advanced	0
☑	v1	10.102.71.226	abcd	10.102.71.220	Advanced	0
☑	A999-80-lb-lb	25.110.17.15	--	10.102.205.35	Advanced	0
☑	A1888-80-lb-lb	5.110.17.95	--	10.102.205.35	Advanced	0
☑	A97-80-lb-lb	52.10.17.15	--	10.102.205.35	Advanced	0
☑	A96-80-lb-lb	2.10.17.15	--	10.102.205.35	Advanced	0
☑	OWA_Security	10.106.150.69	--	10.106.150.50	Advanced	0
☑	webtest	10.106.150.95	--	10.106.150.50	Advanced	0
☑	SharePoint_Security	10.106.150.71	--	10.106.150.50	Advanced	0
☑	Outlook_Security	10.106.150.70	--	10.106.150.50	Advanced	0
☑	ipreplb	10.106.150.93	--	10.106.150.53	Advanced	0
☑	lb2	10.106.150.94	--	10.106.150.53	Advanced	0
☑	lb1	10.106.150.91	--	10.106.150.53	Advanced	0
☑	bl1	10.106.150.92	--	10.106.150.53	Advanced	0
☑	Outlook-brazil	10.106.150.104	--	10.106.150.54	Advanced	0
☑	OWA-France	10.106.150.103	--	10.106.150.54	Advanced	0
☑	sec_app_test	10.106.150.80	--	10.106.150.54	Advanced	0

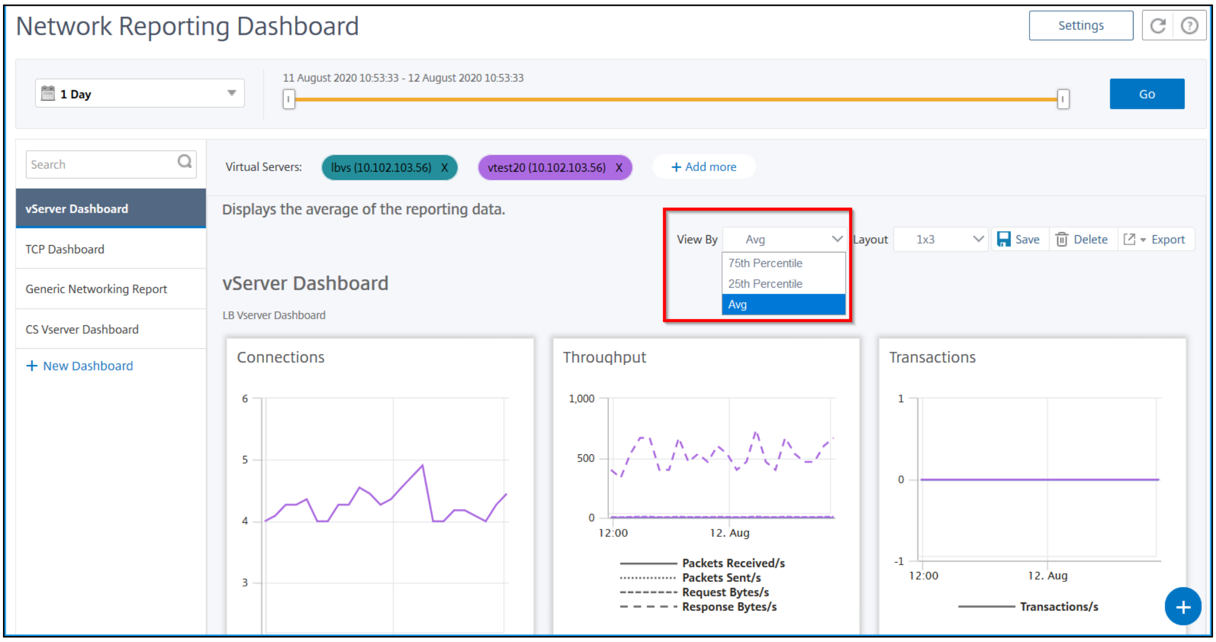
9. Click **Create**.

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.

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 utilized optimally. Navigate to **Network > Network Reporting** and select the time duration 1 day or later to get the **View By** option.



Network Reporting Dashboard

1 Day

11 August 2020 10:53:33 - 12 August 2020 10:53:33

Virtual Servers: lbvs (10.102.103.56) X vtest20 (10.102.103.56) X

Displays the average of the reporting data.

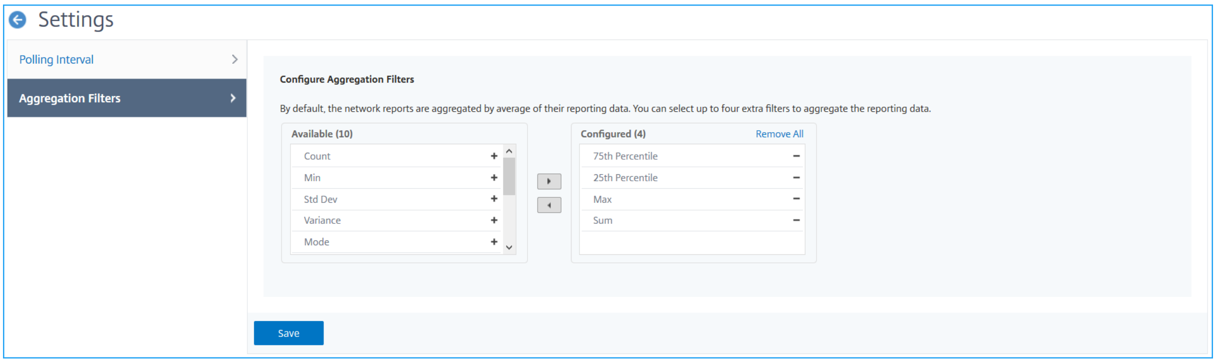
View By: Avg

Layout: 1x3

vServer Dashboard

LB Vserver Dashboard

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**.



Settings

Configure Aggregation Filters

By default, the network reports are aggregated by average of their reporting data. You can select up to four extra filters to aggregate the reporting data.

Available (10): Count, Min, Std Dev, Variance, Mode

Configured (4): 75th Percentile, 25th Percentile, Max, Sum

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, Citrix Application Delivery and Management takes approximately 1 hour to generate reports for the selected aggregation options.

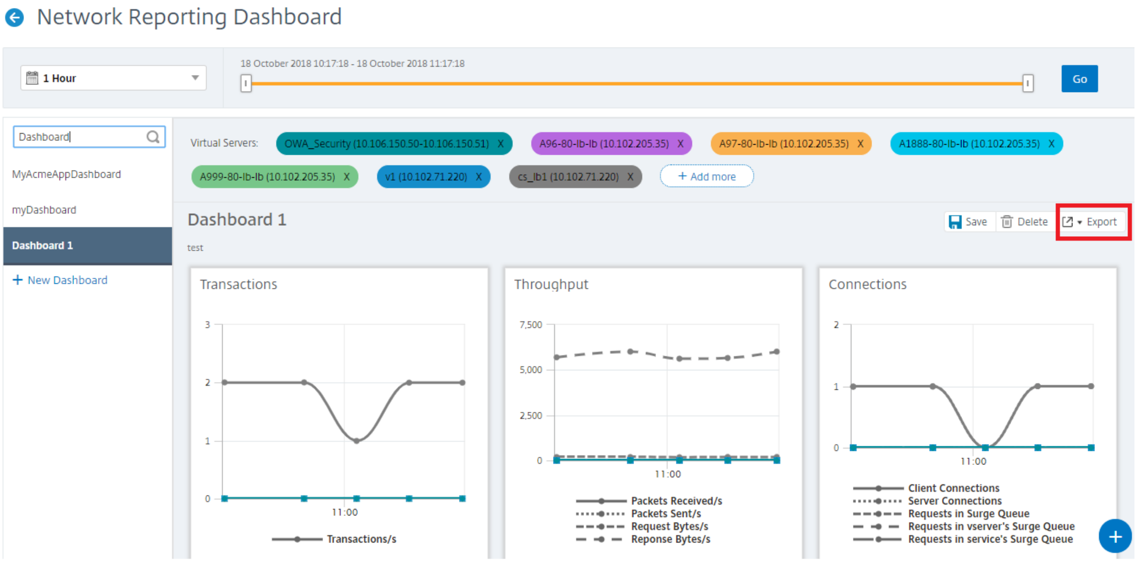
Exporting network reports

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 Citrix Application Delivery and Management if you have read-only permissions. You need an edit permission to be able to create a file in Citrix Application Delivery and Management 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.

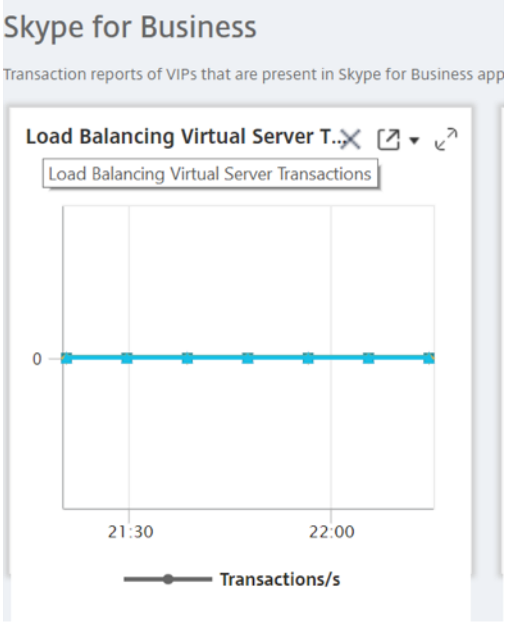
While scheduling network reports, you can customize the heading of the report by entering a text string in the **Subject** field. The report created at the scheduled time has this string as its name.

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.

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**.


Skype for Business
Transaction reports of VIPs that are present in Skype for Business app
Load Balancing Virtual Server T...
Load Balancing Virtual Server Transactions
0
21:30
22:00
Transactions/s

How to manage Thresholds for Network Reports on Citrix Application Delivery and Management

To monitor the state of a Citrix ADC instance, you can set thresholds on counters and receive notifications when a threshold is exceeded. On Citrix Application Delivery and Management, 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.

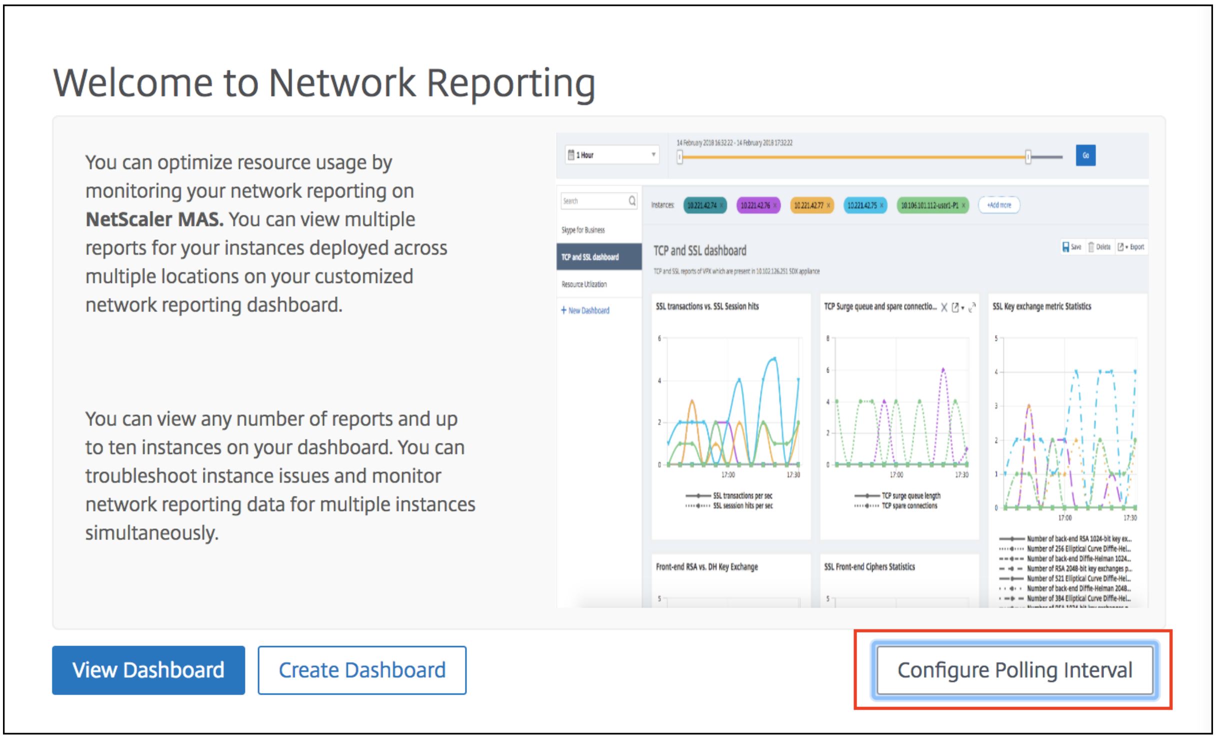
To create a threshold:

1. In Citrix Application Delivery and Management, 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 Citrix ADC.
    - **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. Choose the IP address of the instance or instances for which you want set the threshold.
5. You can also add an **Event Message**. Type a message that you want to appear when the threshold is reached. Citrix Application Delivery and Management 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.
8. Click **Create**.

Set Performance Polling Interval for Network Reports

By default, every 5 minutes, NITRO calls collect performance data for network reporting. The Citrix Application Delivery and Management 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.

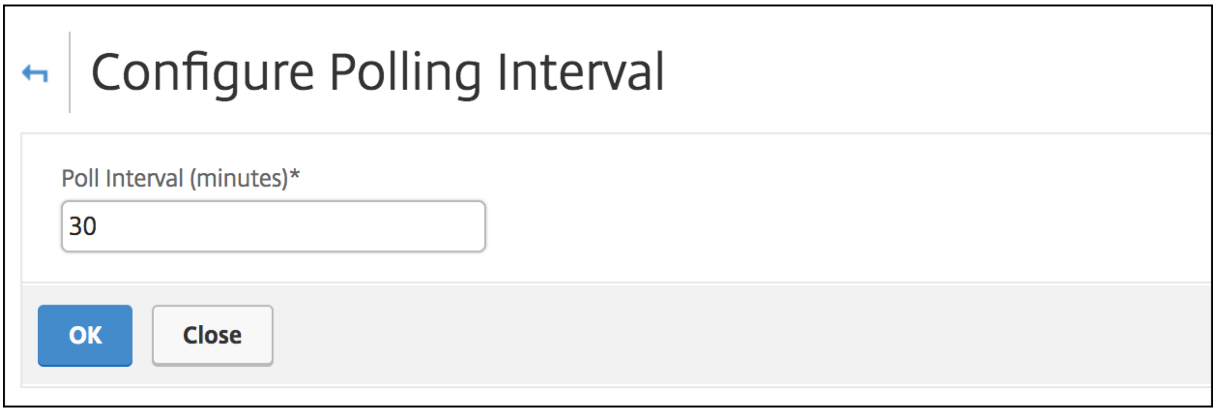
To set the performance polling interval, navigate to **Infrastructure > Network Reporting** and click **Configure Polling Interval**. Your polling interval cannot be less than 5 minutes or more than 60 minutes.



Welcome to Network Reporting

You can optimize resource usage by monitoring your network reporting on **NetScaler MAS.** You can view multiple reports for your instances deployed across multiple locations on your customized network reporting dashboard.

You can view any number of reports and up to ten instances on your dashboard. You can troubleshoot instance issues and monitor network reporting data for multiple instances simultaneously.



Configure Polling Interval

Poll Interval (minutes)*: 30

Configuring Network Reporting Prune Settings

You can configure the purge interval of network reporting data in Citrix Application Delivery and Management. This interval limits the amount of network reporting data being stored in the Citrix Application Delivery and Management 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 90 days or be less than 1 day.

Provisioning Citrix ADC VPX Instances on AWS

September 28, 2021

When you move your applications to the cloud, the components that are part of your application increase, become more distributed, and need to be dynamically managed.

With Citrix ADC VPX instances on AWS, you can seamlessly extend your L4-L7 network stack to AWS. With Citrix ADC VPX, AWS becomes a natural extension of your on-premises IT infrastructure. You can use Citrix ADC VPX on AWS to combine the elasticity and flexibility of the cloud, with the same optimization, security, and control features that support the most demanding websites and applications in the world.

With Citrix Application Delivery and Management monitoring your Citrix ADC instances, you gain visibility into the health, performance, and security of your applications. You can automate the setup, deployment, and management of your application delivery infrastructure across hybrid multi-cloud environments.

AWS terminology

The following section provides a brief description of the AWS terms used in this document:

Term	Definition
Amazon Machine Image (AMI)	A machine image, which provides the information required to launch an instance, which is a virtual server in the cloud.
Elastic Compute Cloud (EC2)	A web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

Term	Definition
Elastic network interface (ENI)	A virtual network interface that you can attach to an instance in a VPC.
Instance type	Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.
Identity and Access Management (IAM) role	An AWS identity with permission policies that determine what the identity can and cannot do in AWS. You can use an IAM role to enable applications running on an EC2 instance to securely access your AWS resources.
Security groups	A named set of allowed inbound network connections for an instance.
Subnets	A segment of the IP address range of a VPC that EC2 instances can be attached to. You can create subnets to group instances according to security and operational needs.
Virtual Private Cloud (VPC)	A web service for provisioning a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.

Prerequisites

This document assumes the following:

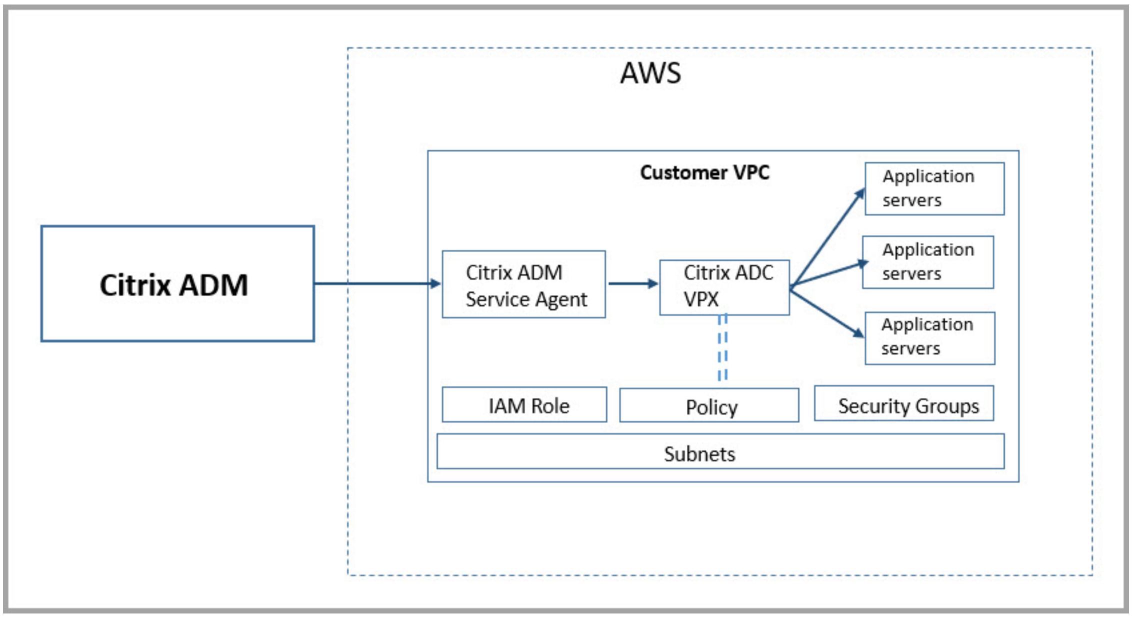
- You possess an AWS account.
- You have created the required VPC and selected the availability zones.
- You have added the Citrix Application Delivery and Management agent in AWS.

For more information on how to create an account and other tasks, see AWS Documentation.

For more information on how to install Citrix Application Delivery and Management agent on AWS, see Installing Citrix Application Delivery and Management agent on AWS.

Architecture Diagram

The following image provides an overview of how Citrix Application Delivery and Management connects with AWS to provision Citrix ADC VPX instances in AWS.



Configuration tasks

Perform the following tasks on AWS before you provision Citrix ADC VPX instances in Citrix Application Delivery and Management:

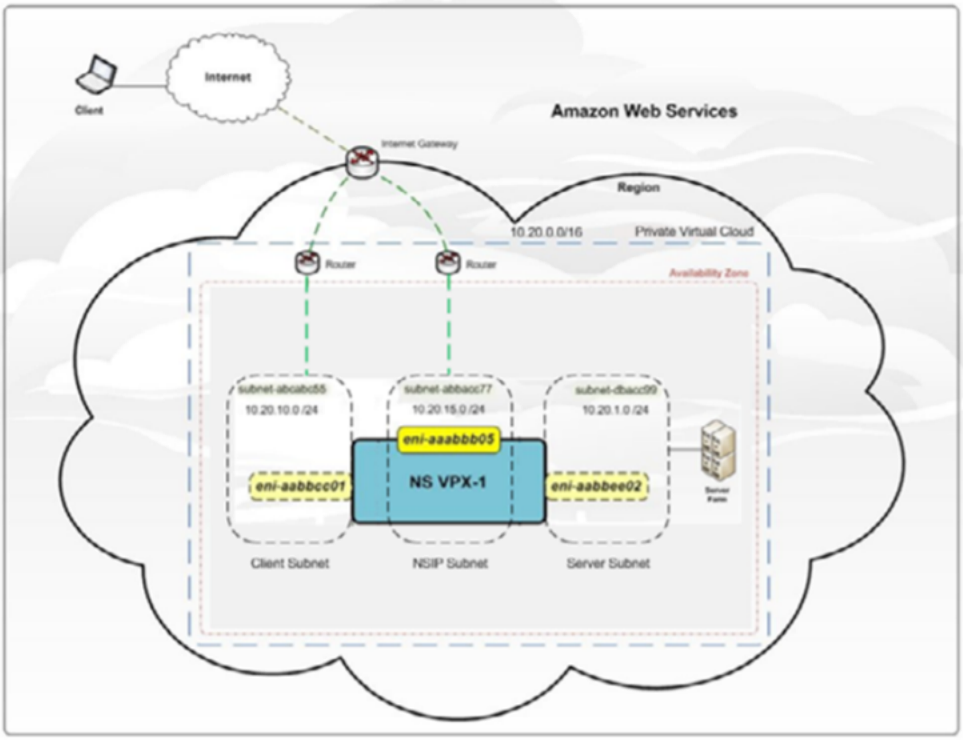
- Create subnets
- Create security groups
- Create an IAM role and define a policy

Perform the following tasks on Citrix Application Delivery and Management to provision the instances on AWS:

- Create site
- Provision Citrix ADC VPX instance on AWS

To create subnets

Create three subnets in your VPC. The three subnets that are required to provision Citrix ADC VPX instances in your VPC - are management, client, and server. Specify an IPv4 CIDR block from the range that is defined in your VPC for each of the subnets. Specify the availability zone in which you want the subnet to reside. Create all the three subnets in the same availability zone. The following image illustrates the three subnets created in your region and their connectivity to the client system.



For more information on VPC and subnets, see VPCs and Subnets.

To create security groups

Create a security group to control inbound and outbound traffic in the Citrix ADC VPX instance. A security group acts as a virtual firewall for your instance. Create security groups at the instance level, and not at the subnet level. It is possible to assign each instance in a subnet in your VPC to a different set of security groups. Add rules for each security group to control the inbound traffic that is passing through the client subnet to instances. You can also add a separate set of rules that control the outbound traffic that passes through the server subnet to the application servers. Although you can use the default security group for your instances, you might want to create your groups. Create three security groups - one for each subnet. Create rules for both incoming and outgoing traffic that you want to control. You can add as many rules as you want.

For more information on security groups, see Security Groups for your VPC.

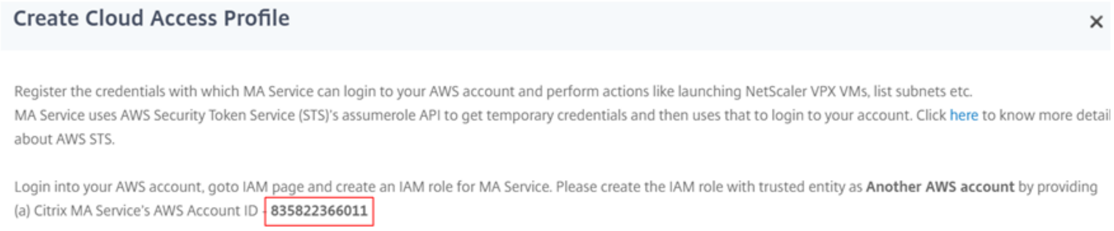
To create an IAM role and define a policy

Create an IAM role so that you can establish a trust relationship between your users and the Citrix trusted AWS account and create a policy with Citrix permissions.

1. In AWS, click **Services**. In the left side navigation pane, select **IAM > Roles**, and click **Create role**.

2. You are connecting your AWS account with the AWS account in Citrix Application Delivery and Management. So, select **Another AWS account** to allow Citrix Application Delivery and Management to perform actions in your AWS account.

   Type in the 12-digit Citrix Application Delivery and Management AWS account ID. The Citrix ID is 835822366011. You can also find the Citrix ID in Citrix Application Delivery and Management when you create the cloud access profile.

   Create Cloud Access Profile

   Register the credentials with which MA Service can login to your AWS account and perform actions like launching NetScaler VPX VMs, list subnets etc.
   MA Service uses AWS Security Token Service (STS)'s assumerole API to get temporary credentials and then uses that to login to your account. Click here to know more detail about AWS STS.

   Login into your AWS account, goto IAM page and create an IAM role for MA Service. Please create the IAM role with trusted entity as **Another AWS account** by providing (a) Citrix MA Service's AWS Account ID - 835822366011

3. Enable **Require external ID** to connect to a third-party account. You can increase the security of your role by requiring an optional external identifier. Type an ID that can be a combination of any characters.

4. Click **Permissions**.

5. In the **Attach permissions policies** page, click **Create policy**.

6. You can create and edit a policy in the visual editor or by using JSON.

   The list of permissions from Citrix is provided in the following box:

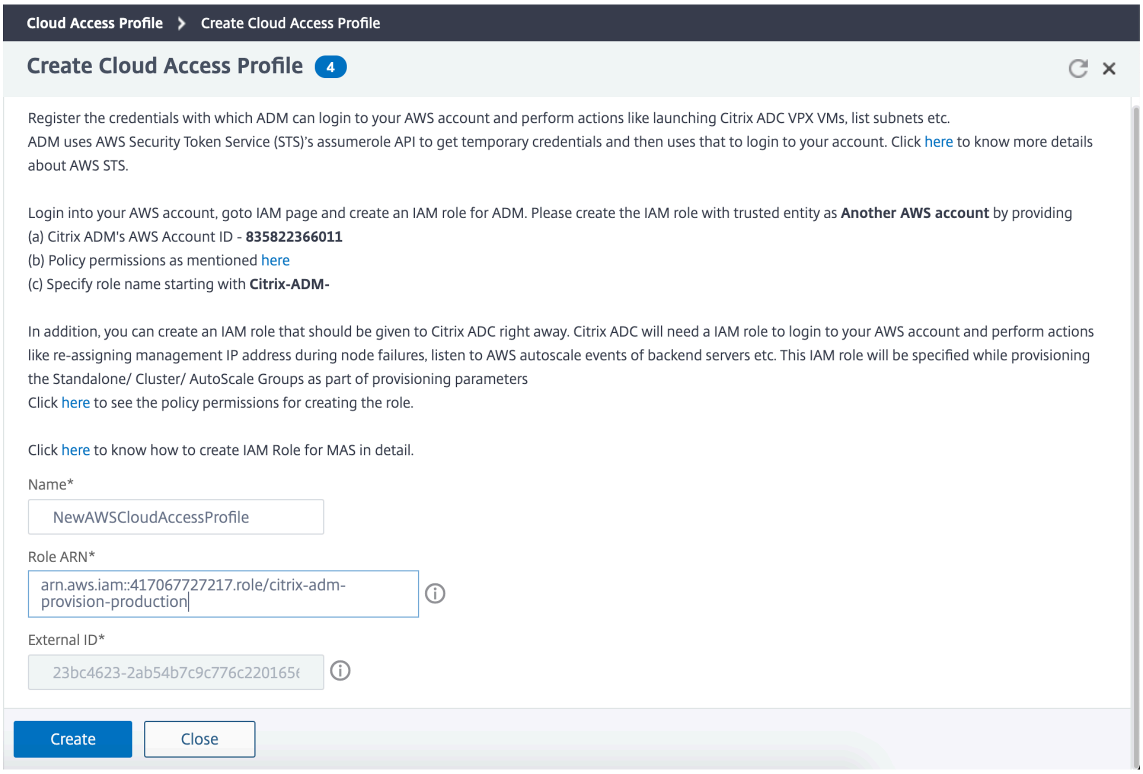
```
{

"Version": "2012-10-17",
"Statement":
[
    {

         "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeImageAttribute",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeHosts",
            "ec2:DescribeImages",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeAddresses",
            "ec2:DescribeKeyPairs",
            "ec2:DescribeTags",
            "ec2:DescribeVolumeStatus",
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeAttribute",
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:CreateKeyPair",
            "ec2:DeleteKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:RunScheduledInstances",
            "ec2:ReportInstanceStatus",
            "ec2:StartInstances",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:AssignPrivateIpAddresses",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:CreateNetworkInterface",
            "ec2:AttachNetworkInterface",
            "ec2:DetachNetworkInterface",
            "ec2:DeleteNetworkInterface",
            "ec2:ResetNetworkInterfaceAttribute",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:AssociateAddress",
            "ec2:AllocateAddress",
            "ec2:ReleaseAddress",
            "ec2:DisassociateAddress",
            "ec2:GetConsoleOutput"
        ],
            "Resource": "*"
     }

]
 }

<!--NeedCopy-->
```

7. Copy and paste the list of permissions in the JSON tab and click **Review policy**.
8. In **Review policy** page, type a name for the policy, enter a description, and click **Create policy**.

To create a site in Citrix Application Delivery and Management

Create a site in Citrix Application Delivery and Management and add the details of the VPC associated with your AWS role.

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Sites**.
2. Click **Add**.
3. Select the service type as AWS and enable **Use existing VPC as a site**.
4. Select the cloud access profile.
5. If the cloud access profile doesn't exist in the field, click **Add** to create a profile.
   a) In the **Create Cloud Access Profile** page, type the name of the profile with which you want to access AWS.
   b) Type the ARN associated with the role that you have created in AWS.
   c) Type the external ID that you provided while creating an Identity and Access Management (IAM) role in AWS. See step 4 in To create an IAM role and define a policy task. Ensure that the IAM role name that you specified in AWS starts with "Citrix-ADM-" and it correctly appears in the Role ARN.



Create Cloud Access Profile 4

Register the credentials with which ADM can login to your AWS account and perform actions like launching Citrix ADC VPX VMs, list subnets etc.
ADM uses AWS Security Token Service (STS)'s assumerole API to get temporary credentials and then uses that to login to your account. Click here to know more details about AWS STS.

Login into your AWS account, goto IAM page and create an IAM role for ADM. Please create the IAM role with trusted entity as **Another AWS account** by providing
(a) Citrix ADM's AWS Account ID - **835822366011**
(b) Policy permissions as mentioned here
(c) Specify role name starting with **Citrix-ADM-**

In addition, you can create an IAM role that should be given to Citrix ADC right away. Citrix ADC will need a IAM role to login to your AWS account and perform actions like re-assigning management IP address during node failures, listen to AWS autoscale events of backend servers etc. This IAM role will be specified while provisioning the Standalone/ Cluster/ AutoScale Groups as part of provisioning parameters
Click here to see the policy permissions for creating the role.

Click here to know how to create IAM Role for MAS in detail.

Name*
NewAWSCloudAccessProfile

Role ARN*
arn.aws.iam::417067727217.role/citrix-adm-provision-production

External ID*
23bc4623-2ab54b7c9c776c220165(

The details of the VPC, such as the region, VPC ID, name and CIDR block, associated with your IAM role in AWS are imported in Citrix Application Delivery and Management.

6. Type a name for the site.
7. Click **Create**.

To provision Citrix ADC VPX on AWS

Use the site that you have created earlier to provision the Citrix ADC VPX instances on AWS. Provide Citrix Application Delivery and Management agent details to provision those instances that are bound to that agent.

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Citrix ADC**.
2. In the **VPX** tab, click **Provision**.

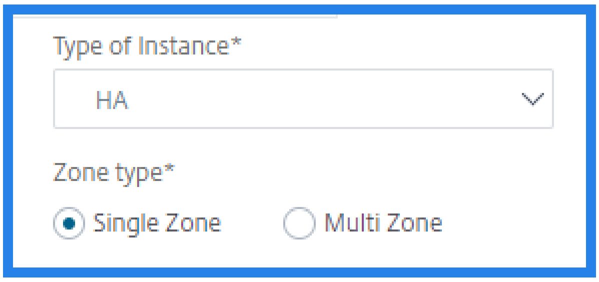
   This option displays the **Provision Citrix ADC VPX on Cloud** page.

3. Select **Amazon Web Services (AWS)** and click **Next**.
4. In the **Basic Parameters** tab,
   a) Select the **Type of Instance** from the list.
      - **Standalone:** This option provisions a standalone Citrix ADC VPX instance on AWS.

- **HA:** This option provisions the high availability Citrix ADC VPX instances on AWS.

  To provision the Citrix ADC VPX instances in the same zone, select the **Single Zone** option under **Zone Type**.

  To provision the Citrix ADC VPX instances across multiple zones, select the **Multi Zone** option under **Zone type**. In the **Provision Parameters** tab, make sure to specify the network details for each zone that are created on AWS.



Type of Instance*

HA

Zone type*

● Single Zone ○ Multi Zone

b) Specify the name of an ADC VPX instance.

c) In **Site**, select the site that you created earlier.

d) In **Agent**, select the agent that is created to manage the ADC VPX instance.

e) In **Cloud Access Profile**, select the cloud access profile created during site creation.

f) In **Device Profile**, select the profile to provide authentication.

   Citrix Application Delivery and Management uses the device profile when it requires to log on to the Citrix ADC VPX instance.

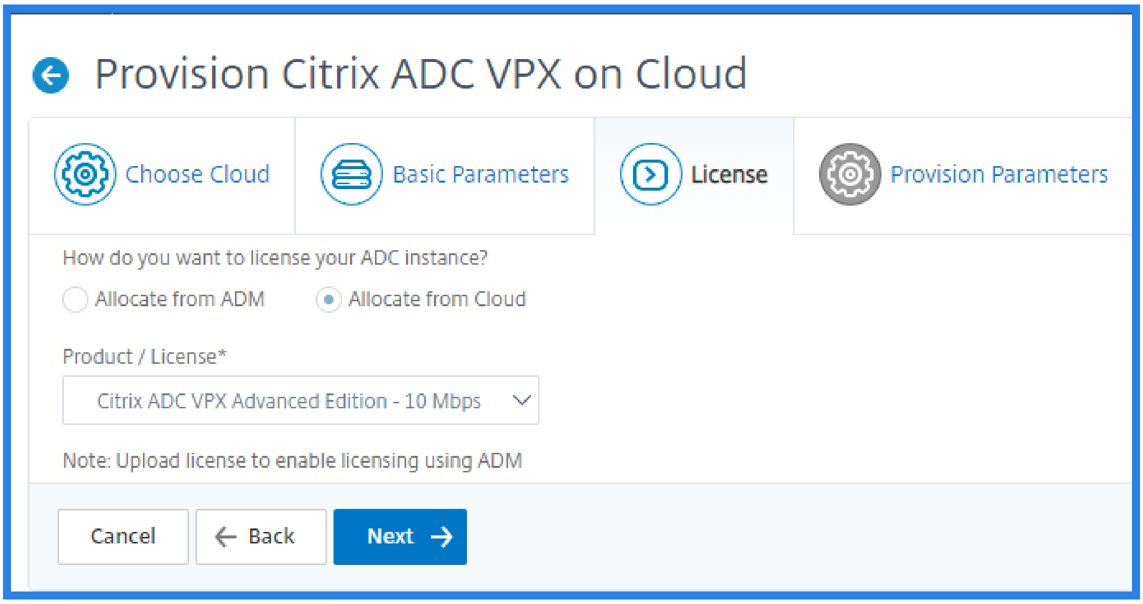
g) Click **Next**.

5. In the **License** tab, Select one of the following modes to apply license to an ADC instance:

   - **Using Citrix Application Delivery and Management**: The instance that you want to provision checks out the licenses from the Citrix Application Delivery and Management.
   - **Using the AWS Cloud**: The **Allocate from Cloud** option uses the Citrix product licenses available in the AWS marketplace. The instance that you want to provision uses the licenses from the marketplace.

     If you choose to use licenses from the AWS marketplace, specify the product or license in the **Provision Parameters** tab.

   For more information, see Licensing Requirements.



Provision Citrix ADC VPX on Cloud

How do you want to license your ADC instance?

○ Allocate from ADM ● Allocate from Cloud

Product / License*

Citrix ADC VPX Advanced Edition - 10 Mbps

Note: Upload license to enable licensing using ADM

6. In the **License** tab if you select the **Allocate from Citrix Application Delivery and Management**, specify the following:

   - License Type - Select either bandwidth or virtual CPU licenses:

     Bandwidth Licenses: You can select one of the following options from the **Bandwidth License Types** list:

     - **Pooled Capacity:** Specify the capacity to allocate to an instance.

       From the common pool, the ADC instance checks out one instance license and only as much bandwidth is specified.

     - **VPX Licenses:** When a Citrix ADC VPX instance is provisioned, the instance checks out the license from the Citrix Application Delivery and Management.

     Virtual CPU Licenses: The provisioned Citrix ADC VPX instance checks out licenses depending on the number of CPUs running in the instance.

     > **Note**
     >
     > When the provisioned instances are removed or destroyed, the applied licenses return to the Citrix Application Delivery and Management license pool. These licenses can be reused to provision new instances.

   a) In **License Edition**, select the license edition. The Citrix Application Delivery and Management uses the specified edition to provision instances.

7. Click **Next**.

8. In the **Provision Parameters** tab,

a) Select the **Citrix IAM Role** created in AWS. An IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.

b) In the **Product** field, select the Citrix ADC product version that you want to provision.

c) Select the EC2 instance type from the **Instance Type** list.

   This list displays the supported AMI instance types for the selected ADC product.

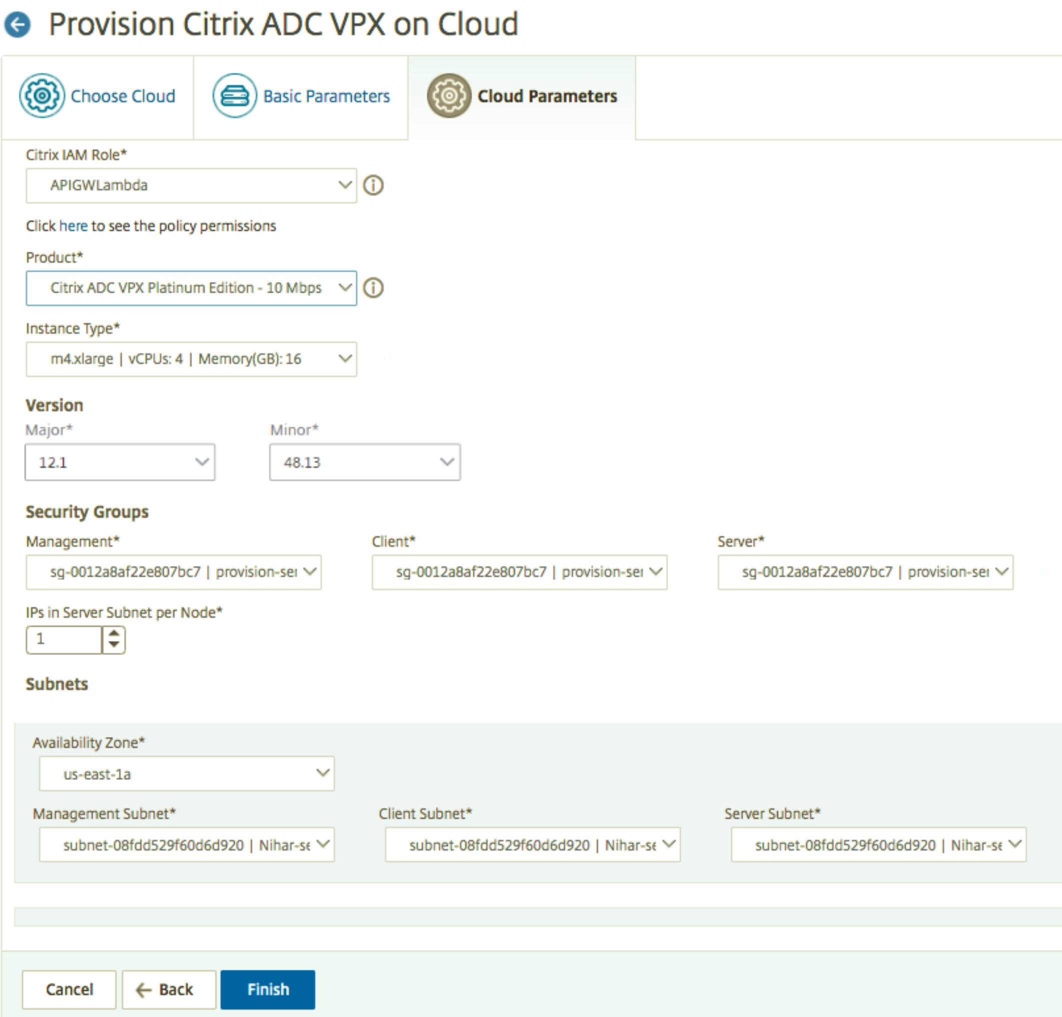
d) Select the **Version** of Citrix ADC that you want to provision. Select both **Major** and **Minor** version of Citrix ADC.

e) In **Security Groups**, select the Management, Client, and Server security groups that you have created in your virtual network.

f) In **IPs in server Subnet per Node**, select the number of IP addresses in server subnet per node for the security group.

g) In **Subnets**, select the Management, Client, and Server subnets for each zone that are created in AWS. You can also select the region from the **Availability Zone** list.

h) Click **Finish**.



Provision Citrix ADC VPX on Cloud

Citrix IAM Role*: APIGWLambda

Click here to see the policy permissions

Product*: Citrix ADC VPX Platinum Edition - 10 Mbps

Instance Type*: m4.xlarge | vCPUs: 4 | Memory(GB): 16

Version

Major*: 12.1

Minor*: 48.13

Security Groups

Management*: sg-0012a8af22e807bc7 | provision-sei

Client*: sg-0012a8af22e807bc7 | provision-sei

Server*: sg-0012a8af22e807bc7 | provision-sei

IPs in Server Subnet per Node*: 1

Subnets

Availability Zone*: us-east-1a

Management Subnet*: subnet-08fdd529f60d6d920 | Nihar-se

Client Subnet*: subnet-08fdd529f60d6d920 | Nihar-se

Server Subnet*: subnet-08fdd529f60d6d920 | Nihar-se

The Citrix ADC VPX instance is now provisioned on AWS.

> **Note**
>
> Currently, Citrix Application Delivery and Management doesn't support deprovisioning of Citrix ADC instances from AWS.

To view the Citrix ADC VPX provisioned in AWS

1. From the AWS home page, navigate to **Services** and click **EC2**.
2. On the **Resources** page, click **Running Instances**.
3. You can view the Citrix ADC VPX provisioned in AWS.

The name of the Citrix ADC VPX instance is the same that you provided while provisioning an instance in the Citrix Application Delivery and Management.

To view the Citrix ADC VPX provisioned in Citrix Application Delivery and Management

1. In Citrix Application Delivery and Management, navigate to **Infrastructure > Instances > Citrix ADC**.
2. Select **Citrix ADC VPX** tab.
3. The Citrix ADC VPX instance provisioned in AWS is listed here.

Pooled capacity

September 25, 2021

Pooled capacity in Citrix ADC is a licensing framework that comprises a common bandwidth and instance pool that is hosted on and served by Citrix Application Delivery and Management. From this common pool, each ADC instance in your data center, regardless of platform or form factor, checks out one instance license and only as much bandwidth as it needs. The license file and, so the bandwidth are not bound to the instance. When the instance no longer requires these resources, it checks them back in to the common pool, making the resources available to other instances that need them.

> **Note**
>
> In Citrix Application Delivery and Management, one of the agents is the license server.

This licensing framework maximizes bandwidth utilization by ensuring that instances are not allocated bandwidth more than their requirement. The ability of the ADC instances to check licenses and bandwidth in and out of a common pool also enables you to automate instance provisioning.

You can increase or decrease the bandwidth allocated to an instance at run time without impacting traffic. You can also transfer the licenses in the pool from one instance to another.

Manage the Kubernetes Ingress configuration

October 20, 2021

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**
>
> - Citrix Application Delivery and Management supports the Ingress feature on the clusters with Kubernetes version 1.14 and above.
> - Citrix Application Delivery and Management supports Citrix ADC VPX and MPX appliances as Ingress devices.
> - In a Kubernetes environment, the Citrix ADC 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 Citrix Application Delivery and Management.

You can specify the following aspects of Kubernetes integration in Citrix Application Delivery and Management:

- **Cluster** – You can register or unregister Kubernetes clusters for which Citrix Application Delivery and Management can deploy Ingress configurations. When you register a cluster in Citrix Application Delivery and Management, specify the Kubernetes API server information. Then, select an Citrix Application Delivery and Management 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 the Kubernetes secret resources.

The Citrix Application Delivery and Management automatically maps the Ingress configurations to ADC instances using Ingress policies.

For each successful Ingress configuration, Citrix Application Delivery and Management 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 > Configuration > Config Packs**.

Before you begin

To use Citrix ADC instances as Ingress devices on Kubernetes clusters, ensure you have:

- Kubernetes cluster in place.
- Citrix Application Delivery and Management agent installed and configured to enable communication between Citrix Application Delivery and Management and Kubernetes cluster or managed instances. You can use the managed instances that are present in your data center or cloud.
- Kubernetes cluster registered in Citrix Application Delivery and Management.

Configure Citrix Application Delivery and Management agent to register with Kubernetes cluster

To enable communication between Kubernetes cluster and Citrix Application Delivery and Management, you must install and configure a Citrix Application Delivery and Management agent. You can deploy an agent on the following platforms:

- Hypervisor (ESX, XenServer, KVM, Hyper-V)
- Public Cloud Services (such as Microsoft Azure, AWS)

Follow the procedure to configure an agent.

> **Note**
>
> You can also use an existing Citrix Application Delivery and Management agent if one is already deployed.

Configure the Citrix Application Delivery and Management with a secret token to manage a Kubernetes cluster

For Citrix Application Delivery and Management to be able to receive events from Kubernetes, you need to create a service account in Kubernetes for Citrix Application Delivery and Management. And, configure the service account with the necessary RBAC permissions in the Cluster.

1. Create a service account for Citrix Application Delivery and Management. 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 Citrix Application Delivery and Management 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 Citrix Application Delivery and Management 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 Citrix Application Delivery and Management

After you configure a Citrix Application Delivery and Management agent and configure static routes, you must register the Kubernetes cluster in Citrix Application Delivery and Management.

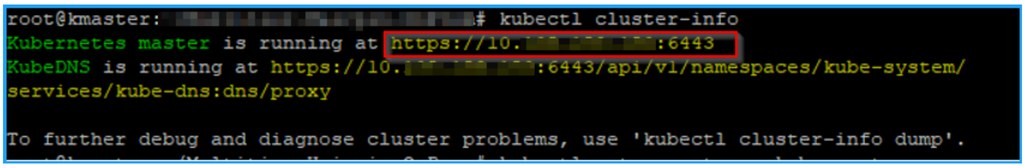
To register the Kubernetes cluster:

1. Log on to Citrix Application Delivery and Management 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 Master node.

      i. On the Kubernetes master node, run the command `kubectl cluster-info`.



```
root@kmaster:[redacted]# kubectl cluster-info
Kubernetes master is running at https://10.[redacted]:6443
KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

      ii. Enter the URL that displays for **"Kubernetes master is running at."**

   c) **Authentication Token** - Specify the authentication token string obtained while you configure Citrix Application Delivery and Management to manage a Kubernetes cluster. The authentication token is required to validate access for communication between Kubernetes cluster and Citrix Application Delivery and Management. To generate an authentication token:

i. On the Kubernetes master node, run the following commands:

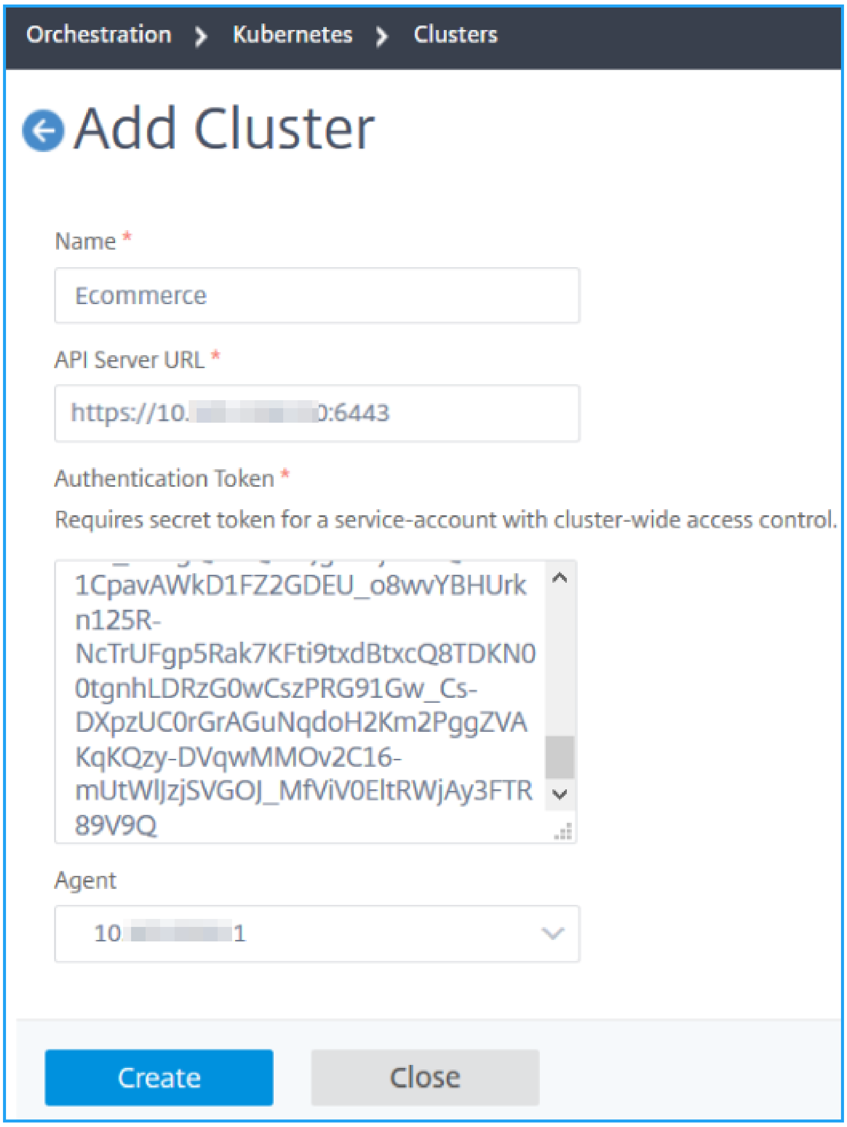
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

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**.



Add Cluster

Name *

Ecommerce

API Server URL *

https://10.[redacted]0:6443

Authentication Token *

Requires secret token for a service-account with cluster-wide access control.

1CpavAWkD1FZ2GDEU_o8wvYBHUrk
n125R-
NcTrUFgp5Rak7KFti9txdBtxcQ8TDKN0
0tgnhLDRzG0wCszPRG91Gw_Cs-
DXpzUC0rGrAGuNqdoH2Km2PggZVA
KqKQzy-DVqwMMOv2C16-
mUtWlJzjSVGOJ_MfViV0EltRWjAy3FTR
89V9Q

Agent

10[redacted]1

Define an Ingress policy

The Ingress policy decides which Citrix ADC is used to deploy an Ingress configuration, based on the Ingress Cluster or Namespace or both.

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 Citrix Application Delivery and Management agent configured with the Kubernetes cluster.
   d) In **Choose Network**, select the network from which Citrix Application Delivery and Management auto-assigns the virtual IP addresses to an Ingress configuration.

      This list displays the networks created in **Settings > 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 Citrix Application Delivery and Management.

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:

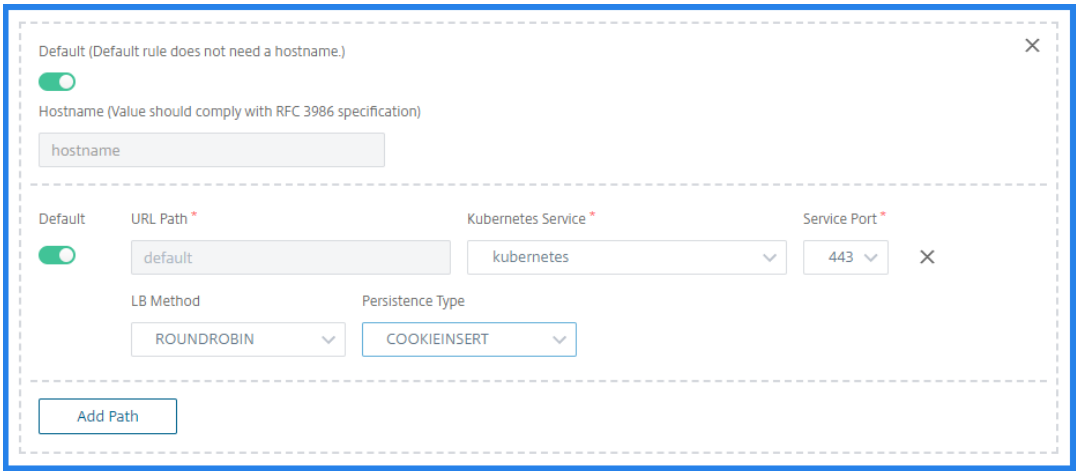
     ```
     "lbmethod":"ROUNDROBIN"
     <!--NeedCopy-->
     ```

   - **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.



Default (Default rule does not need a hostname.)

Hostname (Value should comply with RFC 3986 specification)

hostname

Default | URL Path * | Kubernetes Service * | Service Port *
default | kubernetes | 443

LB Method: ROUNDROBIN

Persistence Type: COOKIEINSERT

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 **System > Licensing & Analytics**.
> 2. Under **Virtual Server License Summary**, enable **Auto-select virtual servers**.

TCP Insight

September 25, 2021

The TCP Insight feature of Citrix Application Delivery and Management provides an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in Citrix ADC appliances to avoid network congestion in data transmission. This feature uses "TCP Speed Report" capability, which measures TCP file download or upload performance with and without TCP optimization.

You can view the key Transport Layer metrics, such as data volume, throughput, and speed, and use that information to measure the traffic volume served by the Citrix ADC instances and validate the benefits of TCP Optimization. Breakdowns by stream direction (from client to Citrix ADC and Citrix ADC to origin server), TCP port, and virtual LAN are provided for the above metrics.

Prerequisites

Before you begin configuring the TCP Insight feature, make sure that the following prerequisites are met:

- The Citrix ADC instances are running on software version 11.1 build 51.21 or later.
- You have installed Citrix Application Delivery and Management running on software version 11.1 build 51.21 or later.
- All the virtual servers configured for an application are licensed for management and monitoring on Citrix Application Delivery and Management. For information about Citrix Application Delivery and Management licensing, see Licensing.

Hardware requirements for Citrix Application Delivery and Management:

Component	Requirement
RAM	8 GB
Virtual CPU	4
	Note Citrix recommends that you use 8 CPUs for better performance.
Storage Space	120 GB
	Note Citrix recommends that you use 500 GB for better performance.

Enabling TCP Insight

Before you can view the TCP Insight metrics, you must enable the feature on Citrix Application Delivery and Management.

To Enable TCP Insight:

1. Navigate to **Settings > Analytics Settings**, and click **Enable Features for Analytics**.

2. On the **Enable Features for Analytics** page, select **Enable TCP Insight**.
3. In the confirmation window, click **OK**.

View the TCP Insight metrics in Citrix Application Delivery and Management

After enabling TCP Insight in Citrix Application Delivery and Management, you can view key transport layer information such as traffic mode (internet or mobile data), data volume, throughput, interfaces, ports, average upload speed, average download speed.

To display TCP Insight metrics in Citrix Application Delivery and Management:

Navigate to **Infrastructure** > **TCP Insight**.

You can hover your mouse pointer on the bar graphs to view the data volume of the corresponding transport techniques. Also you can view the data volume, and other metrics, in the table below the graph.

> **Note** You can customize the metrics displayed in the graph by using the settings icon on the table. You can also select the time period to which the metrics pertain, and use the time slider adjust the time period.

You can also view metrics for such things as interfaces, ports, and bit rates by selecting from the **TCP Insight** list.

Use cases

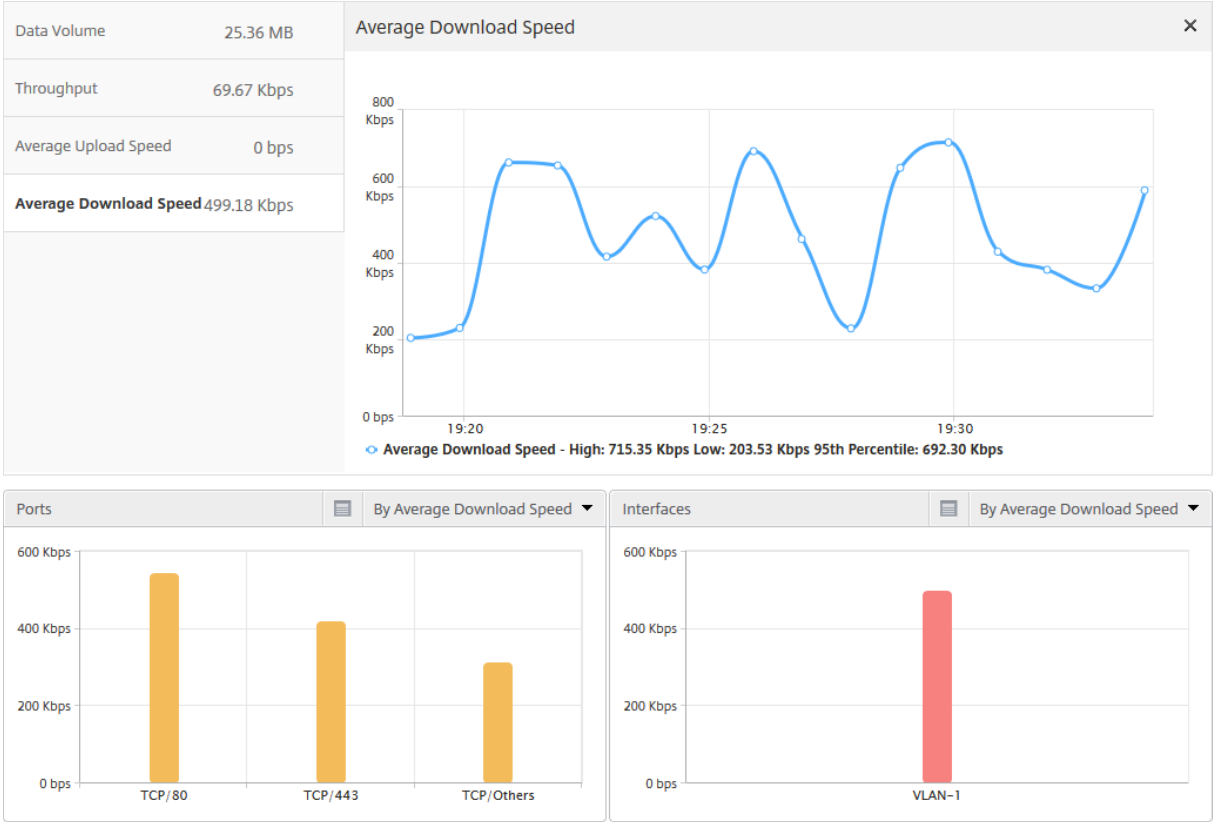
The following use cases illustrate some of the ways to use TCP Insight on Citrix ADC appliances:

- Assess benefits of TCP optimization
- Tune TCP parameters
- Measure impact of TCP optimization on traffic volume

Assess benefits of TCP optimization

How much does Citrix ADC TCP optimization actually benefit a mobile (radio) or enterprise network (internet). You can view the speed of data transfers that take place over TCP, and compare unoptimized and optimized performance. These measurements are displayed separately for the download and upload directions (always on the radio/client side), and for different destination ports, HTTP (80) and HTTPS (443).
By examining the TCP Insight metrics, you can quantify the speed improvement gained by optimizing TCP flows.

To see a summary of these parameters, log on to Citrix Application Delivery and Management and click the **TCP Insight** tab. Then, click **Sides** and select **Internet** or **Radio** from the bar graph or the table below the graph.

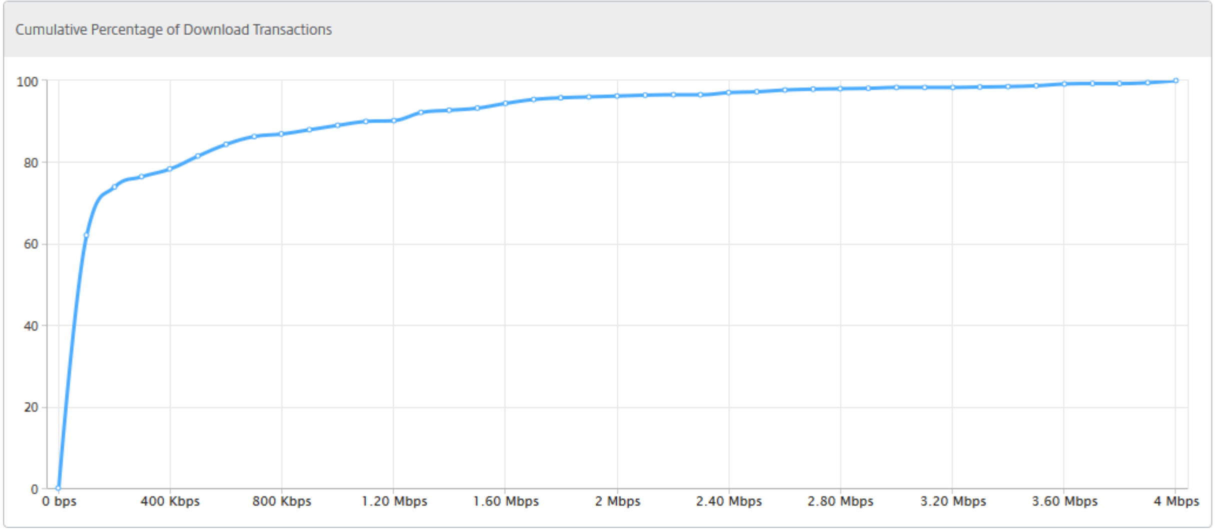


Data Volume	25.36 MB
Throughput	69.67 Kbps
Average Upload Speed	0 bps
Average Download Speed	499.18 Kbps

Tune TCP parameters

Using different TCP Profiles might yield different outputs for the same traffic. In such situations, you might want to view and compare the speed measurements of periods in which Citrix ADC is running different TCP optimization profiles. You can use the results to tune TCP parameters for faster transmission, and develop a TCP profile that maximizes the user-perceived experience in a specific customer network.

To view the reports, log on to Citrix Application Delivery and Management. Then, on the **TCP Insight** tab, click **Bitrates**, and select the desired bitrate form the bar graph or the table below the graph.

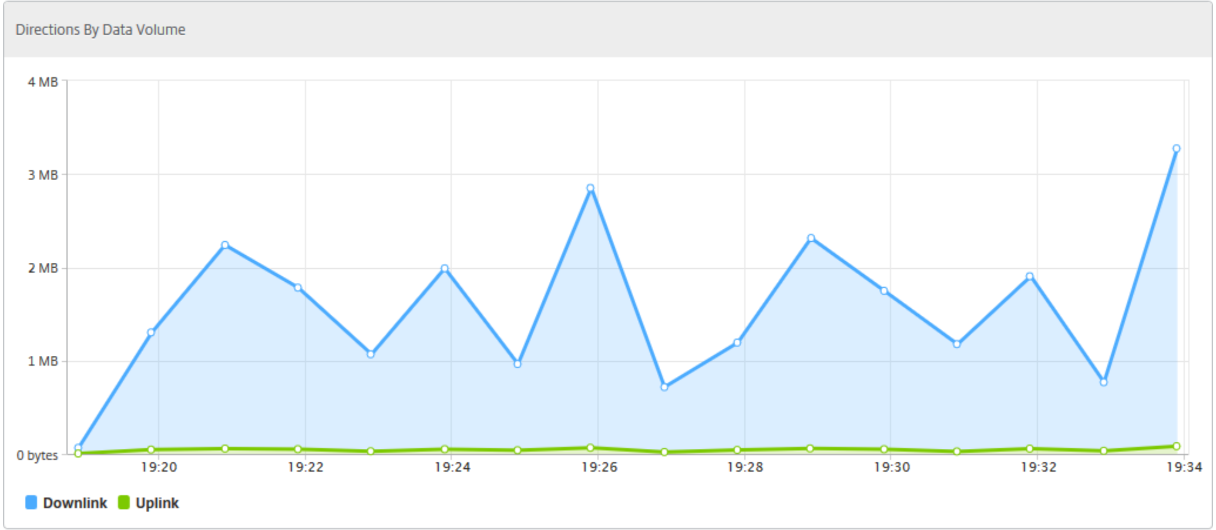


Measure impact of TCP optimization on traffic volume

Measurements of IP-layer Data Volume/Throughput handled by a Citrix ADC instance can be compared between different time periods, to evaluate the effect of TCP optimization on subscriber data consumption. The measurements can be applied separately for each side of the network (radio-side vs. internet-side), for different traffic segments (delineated by different interfaces or VLANs), for each direction (downlink vs. uplink) and for different destination ports (HTTP and HTTPS). The comparison can be used to confirm that TCP optimization encourages subscribers to consume more data.

For a summary of the measurements, log on to Citrix Application Delivery and Management, and on the **TCP Insight** tab click **Sides**, and then select **Internet** or **Radio** from the bar graph or the table below the graph.

You can also select a different timeframe from the time list. You can customize the time frame by using the timeframe slider.



Video Insight

September 24, 2021

The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by Citrix ADC 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 Citrix ADC 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 Citrix ADC Video Optimization feature, see Video Optimization. When you integrate Citrix ADC appliance with Citrix Application Delivery and Management, it collects key information from the video data flowing through the Citrix ADC 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 Citrix Application Delivery and Management corresponds to the sessions that you had selected of random sampling in Citrix ADC appliance. For more information about Random Sampling, see Video Optimization.

Video Insight in Citrix Application Delivery and Management 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 Citrix ADC instances with Citrix ADC Premium license. The Citrix

> ADC Premium license is supported for Citrix ADC Telco platforms (VPX T1000 and VPX-T).

To configure Video insight on a Citrix ADC 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 Citrix Application Delivery and Management server on which you want to monitor the reports.

To configure video insight on a Citrix ADC 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

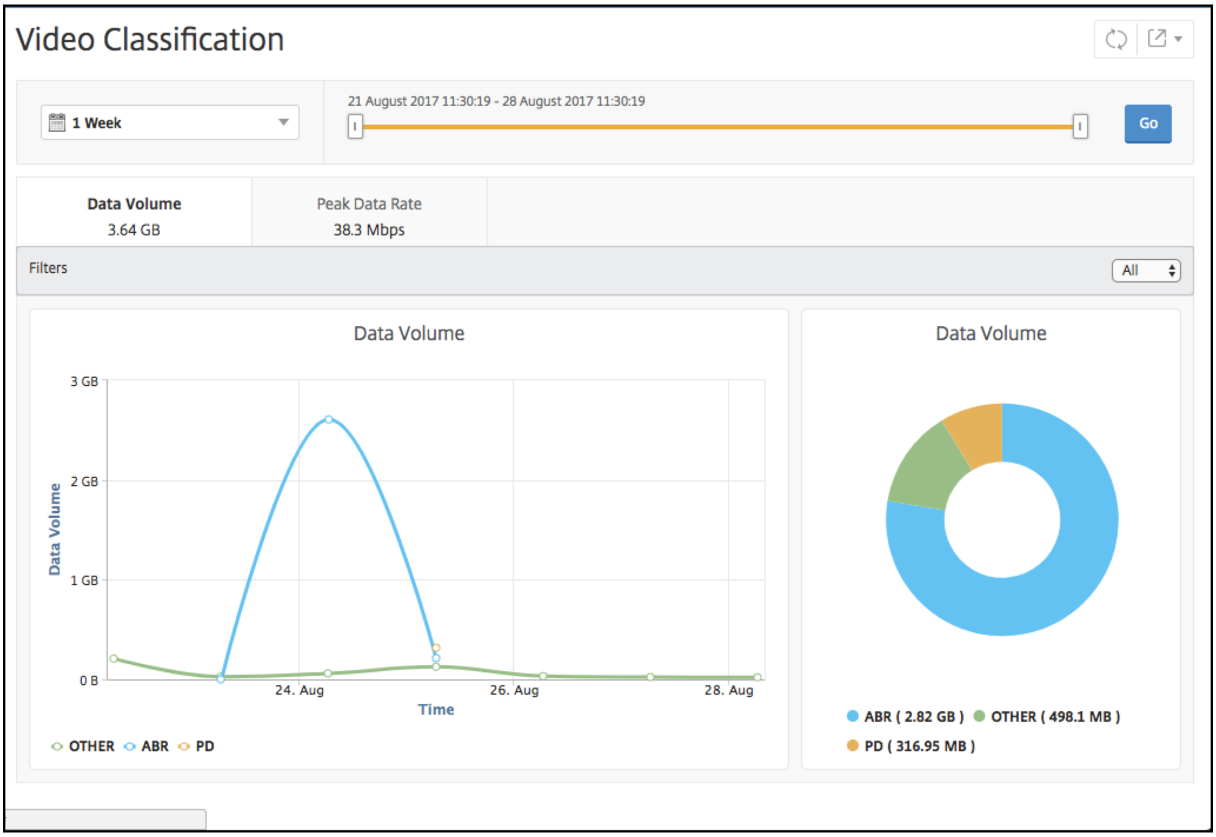
Sample

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
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 Citrix Application Delivery and Management

After enabling Video Insight in Citrix Application Delivery and Management, 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 Citrix Application Delivery and Management, navigate to **Infrastructure > Video Insight**.



Video Classification

1 Week

21 August 2017 11:30:19 - 28 August 2017 11:30:19

Go

Data Volume	Peak Data Rate
3.64 GB	38.3 Mbps

Filters: All

> **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

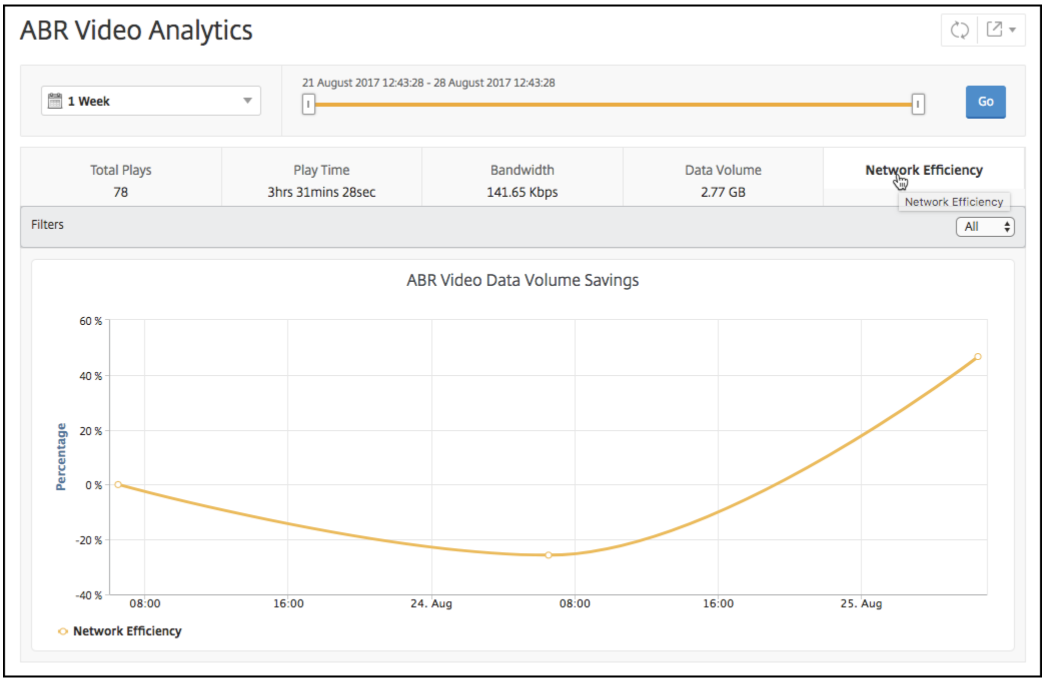
September 24, 2021

For a given time frame, Citrix Application Delivery and Management 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 **Infrastructure > 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

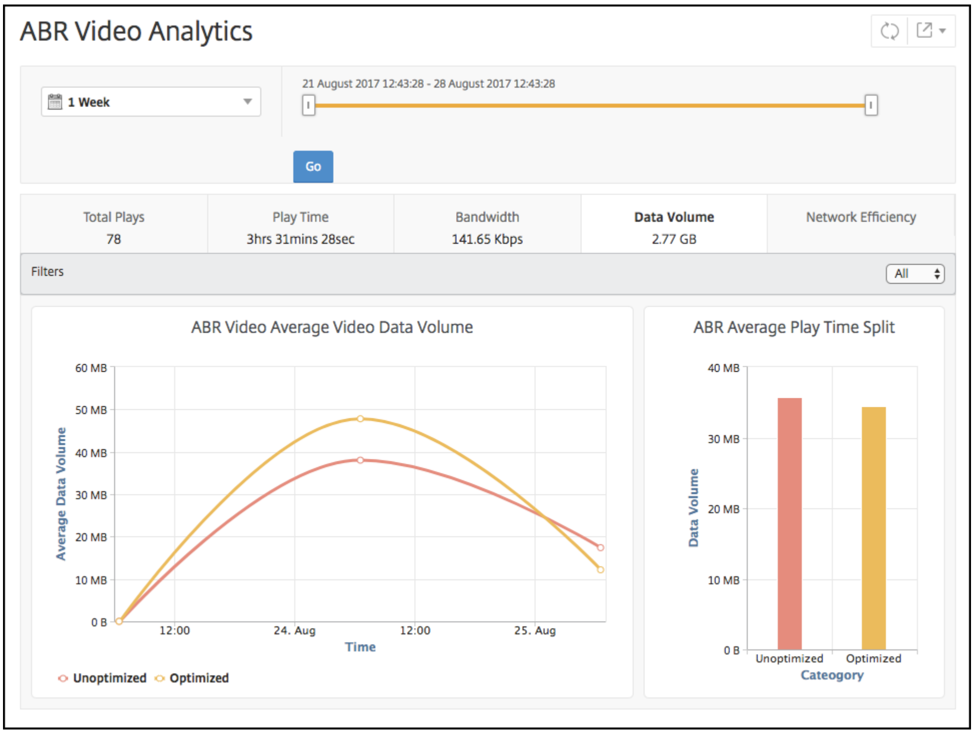
September 24, 2021

For a given time frame, Citrix Application Delivery and Management 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 **Infrastructure > 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.



ABR Video Analytics

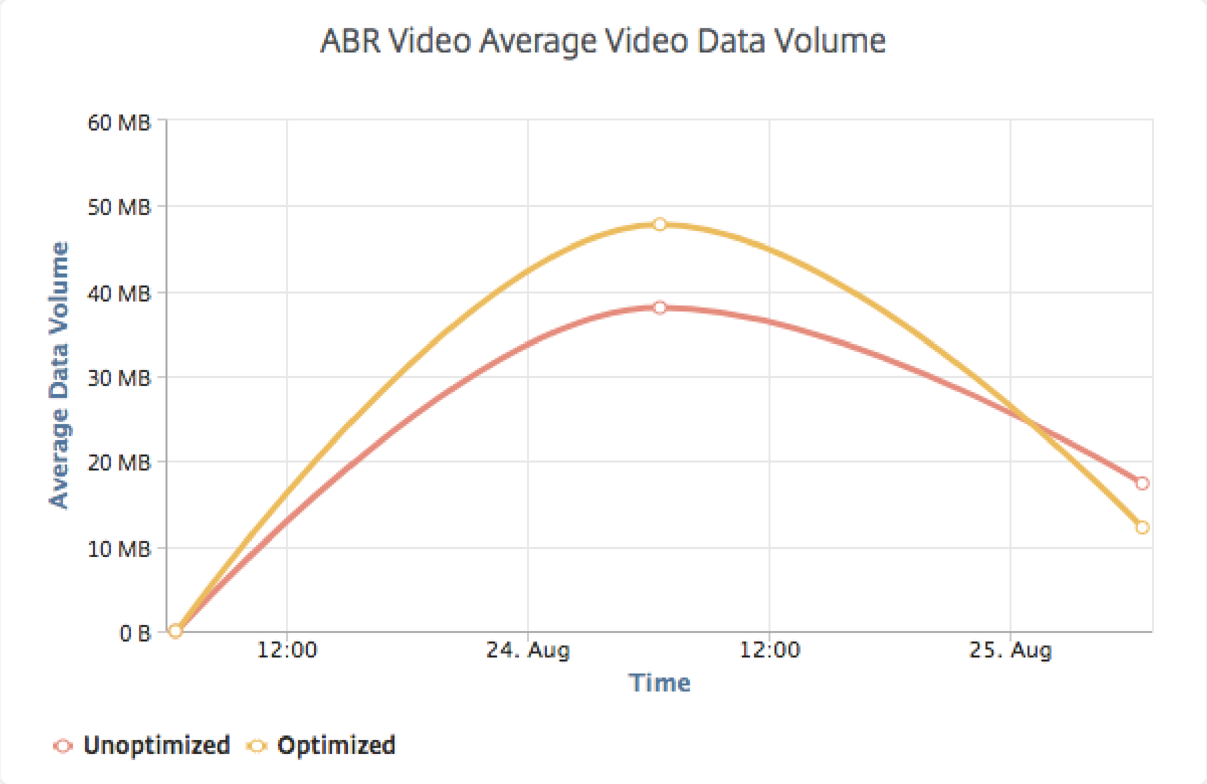
1 Week

21 August 2017 12:43:28 - 28 August 2017 12:43:28

Total Plays	Play Time	Bandwidth	Data Volume	Network Efficiency
78	3hrs 31mins 28sec	141.65 Kbps	2.77 GB	

Filters: All

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

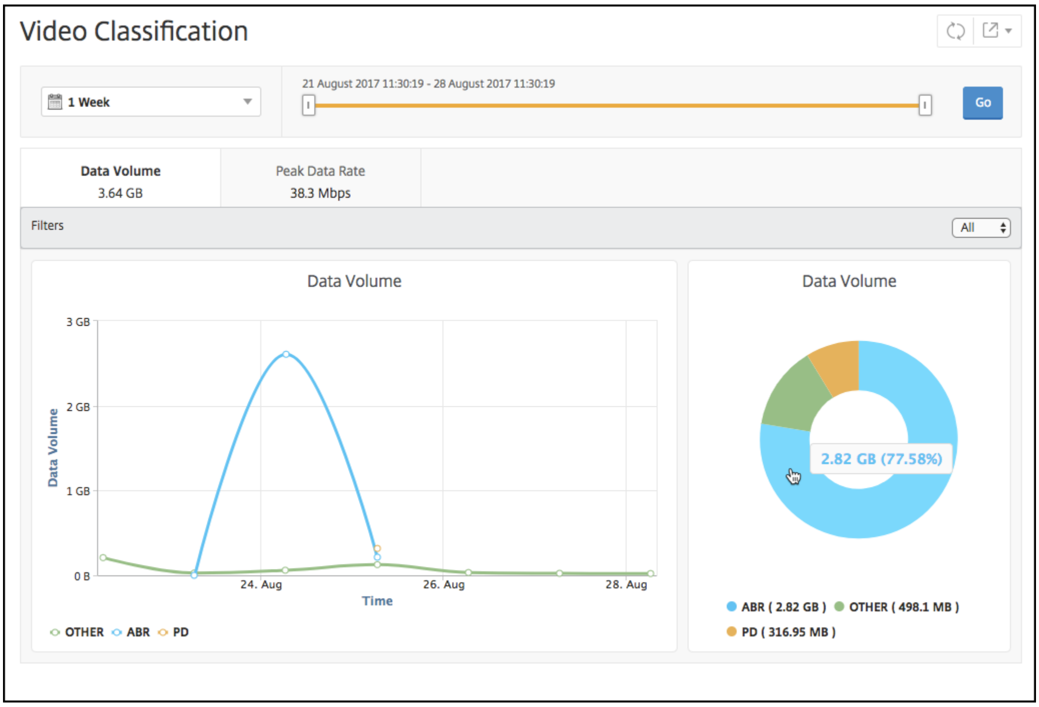
September 24, 2021

The Citrix ADC appliance detects the encrypted or unencrypted video traffic in your network and the type of video streaming (PD or ABR). Citrix Application Delivery and Management displays these metrics and the data volume consumed by the video traffic for a defined time frame.

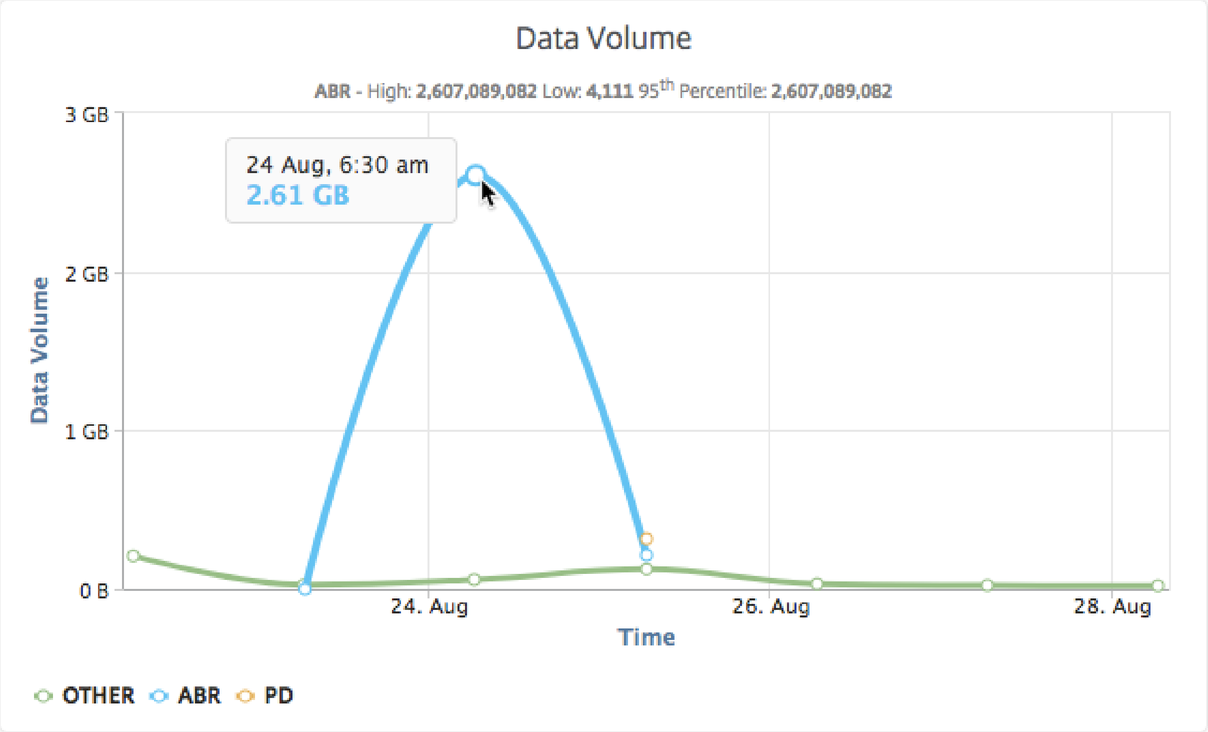
To see the types of videos and the consumed data volume:

1. Navigate to **Infrastructure > 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**.

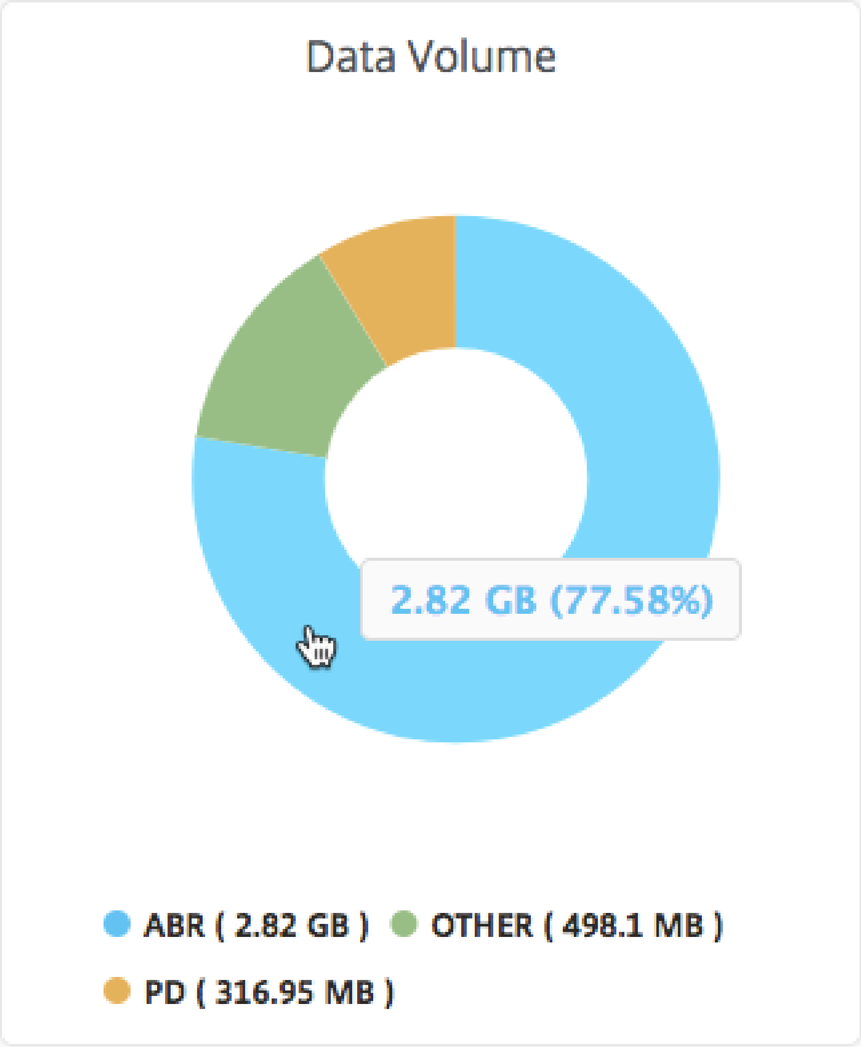
You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.



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

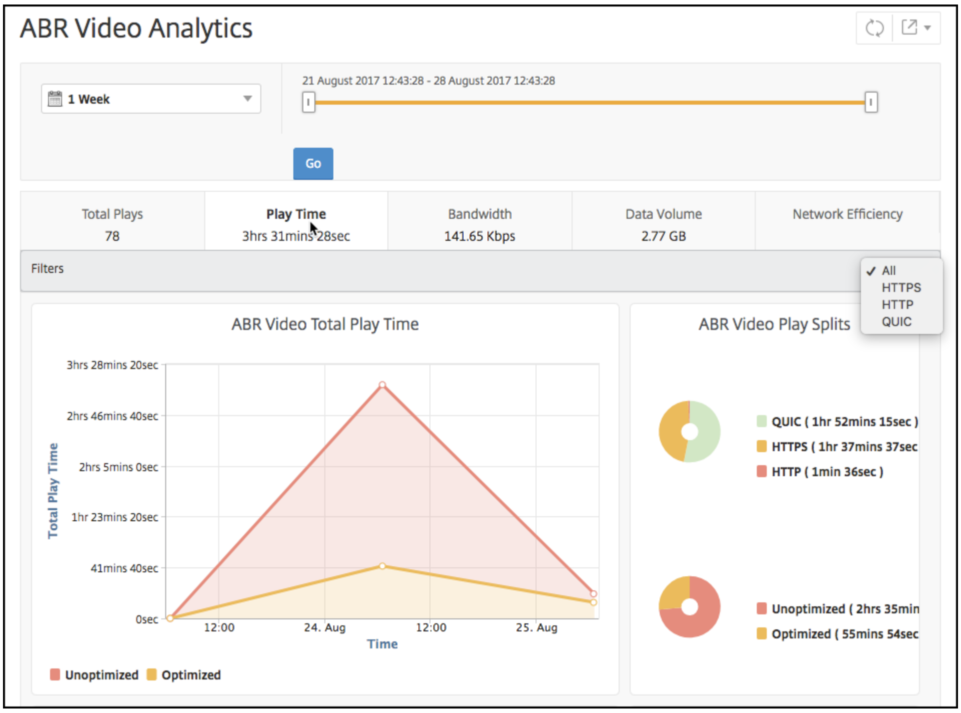
September 24, 2021

For a given time frame, Citrix Application Delivery and Management 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:

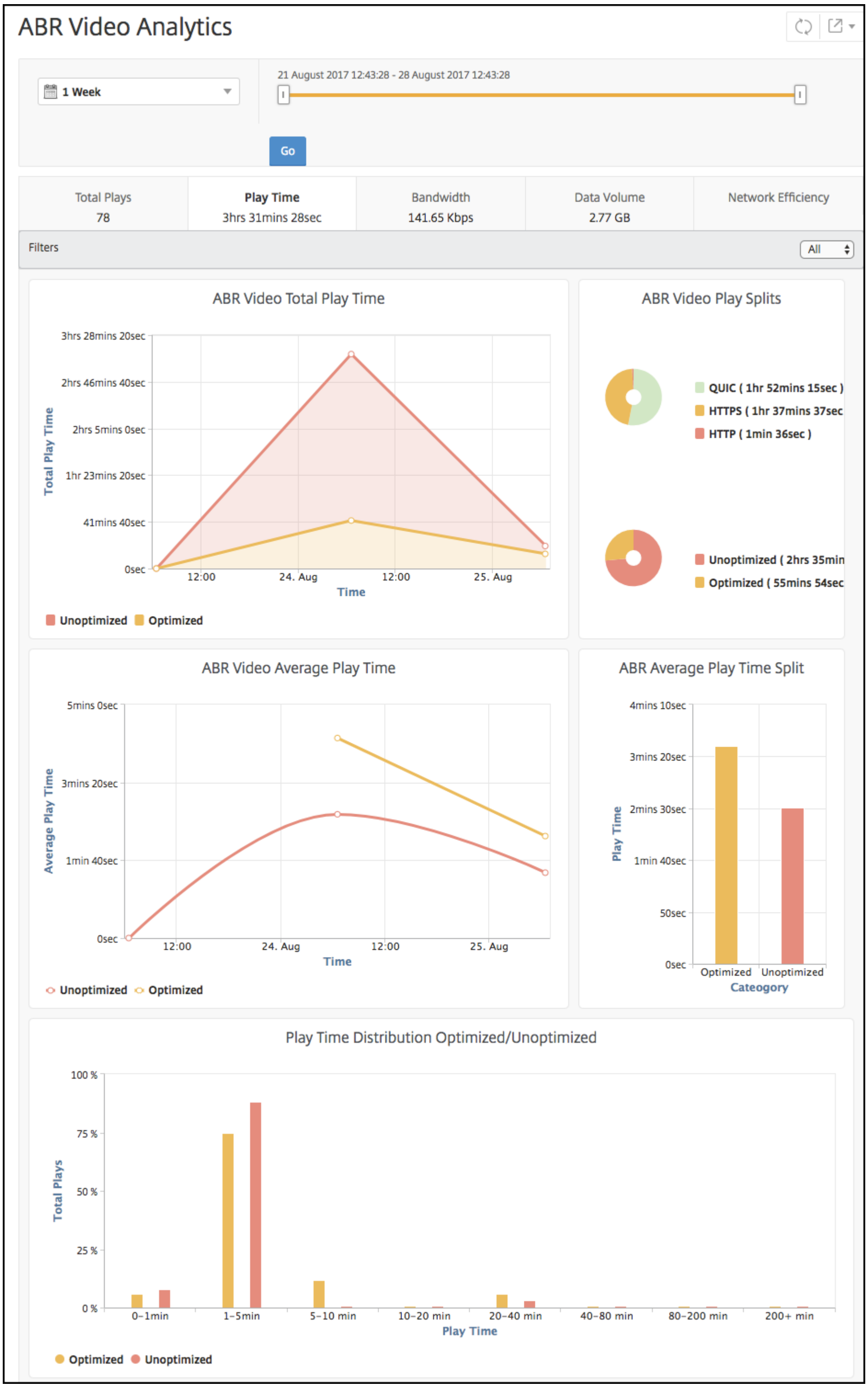
1. Navigate to **Infrastructure > Video Insight** and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Play Time** tab.

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



ABR Video Analytics

1 Week

21 August 2017 12:43:28 - 28 August 2017 12:43:28

Go

Total Plays	Play Time	Bandwidth	Data Volume	Network Efficiency
78	3hrs 31mins 28sec	141.65 Kbps	2.77 GB	

Filters: All

Compare bandwidth consumption of optimized and unoptimized ABR videos

September 24, 2021

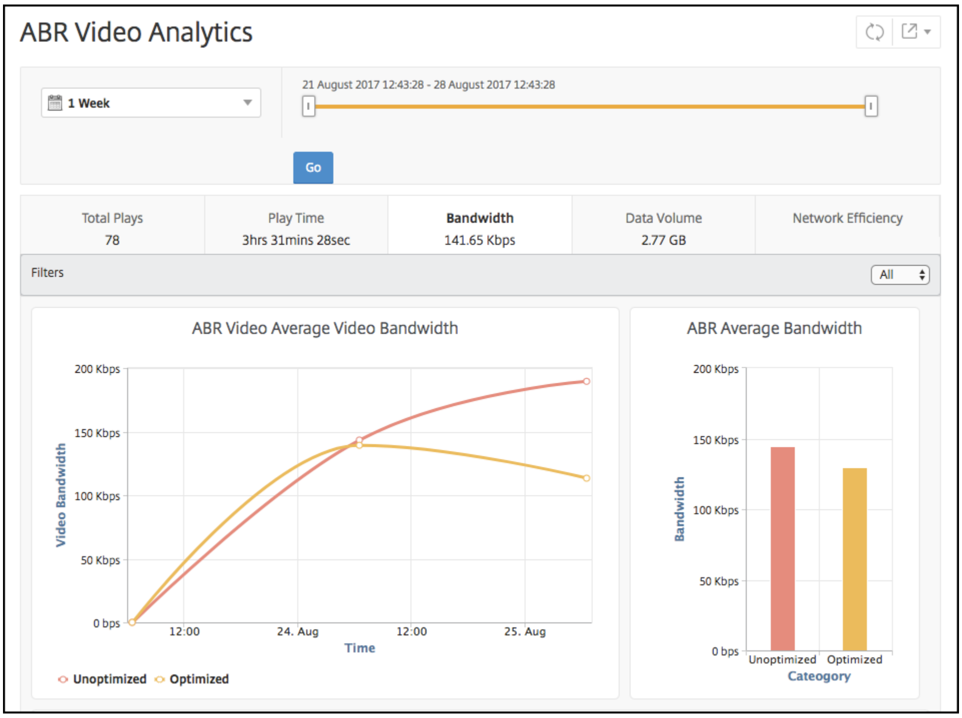
For a given time frame, Citrix Application Delivery and Management provides the bandwidth consumed by optimized and unoptimized of ABR videos and also enables you to compare the bandwidth consumed by optimized and unoptimized ABR videos in your network based on:

- Play Time
- Data Volume

To view the bandwidth consumption:

1. Navigate to **Infrastructure > 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.



ABR Video Analytics

1 Week

21 August 2017 12:43:28 - 28 August 2017 12:43:28

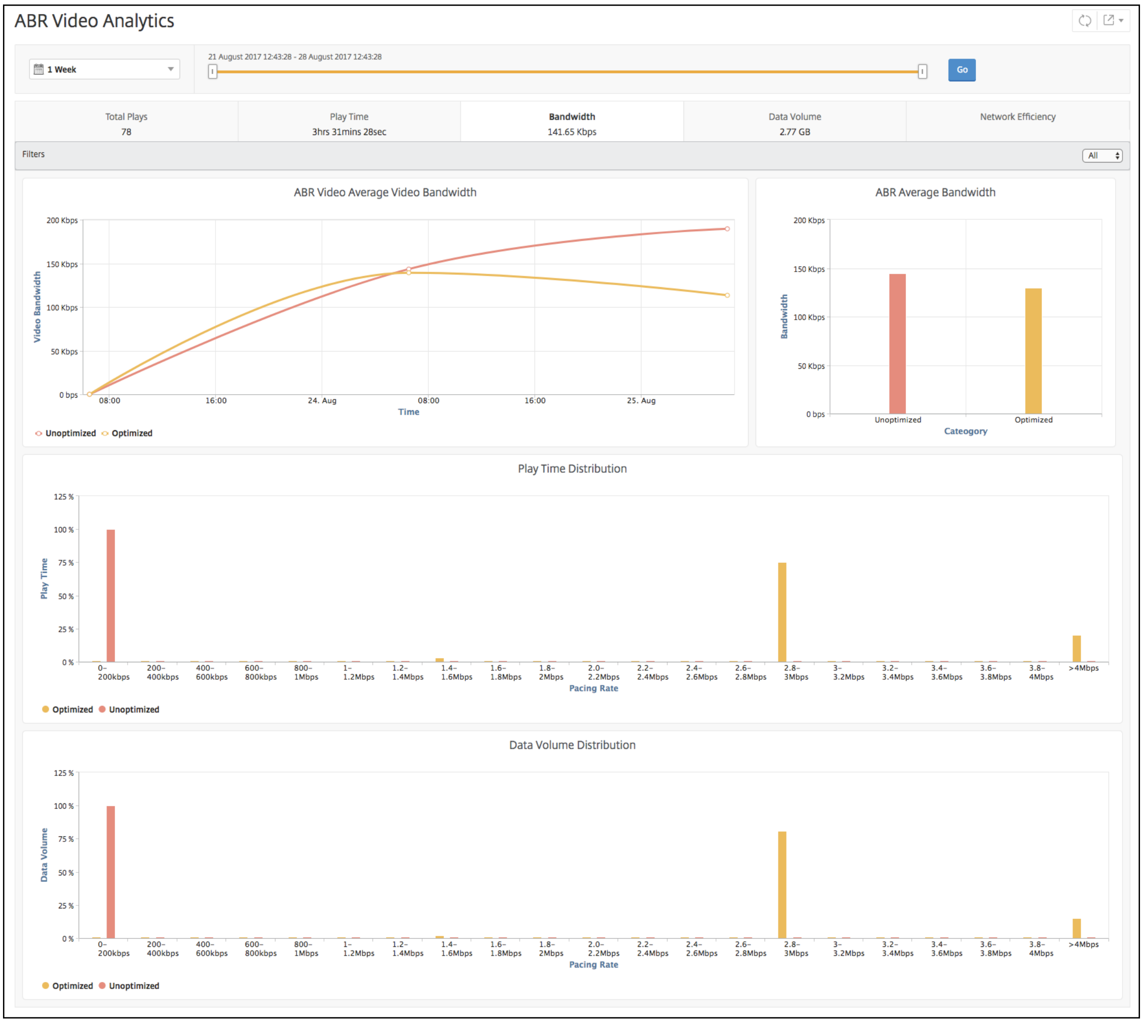
Total Plays	Play Time	Bandwidth	Data Volume	Network Efficiency
78	3hrs 31mins 28sec	141.65 Kbps	2.77 GB	

Filters: All

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.


ABR Video Analytics

1 Week

21 August 2017 12:43:28 - 28 August 2017 12:43:28

Go

Total Plays	Play Time	Bandwidth	Data Volume	Network Efficiency
78	3hrs 31mins 28sec	141.65 Kbps	2.77 GB	

Filters: All

Compare optimized and unoptimized number of plays of ABR videos

September 24, 2021

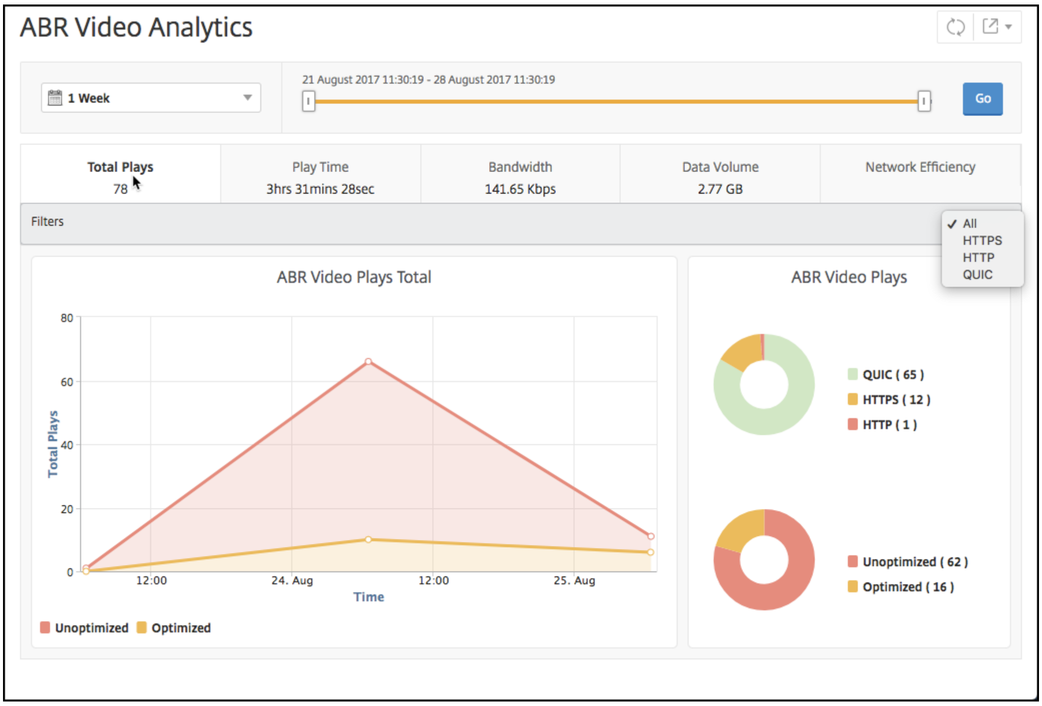
For a given time frame, Citrix Application Delivery and Management shows the number of plays of ABR videos and enables you to compare the number of optimized and unoptimized plays in your network.

To see the number of plays:

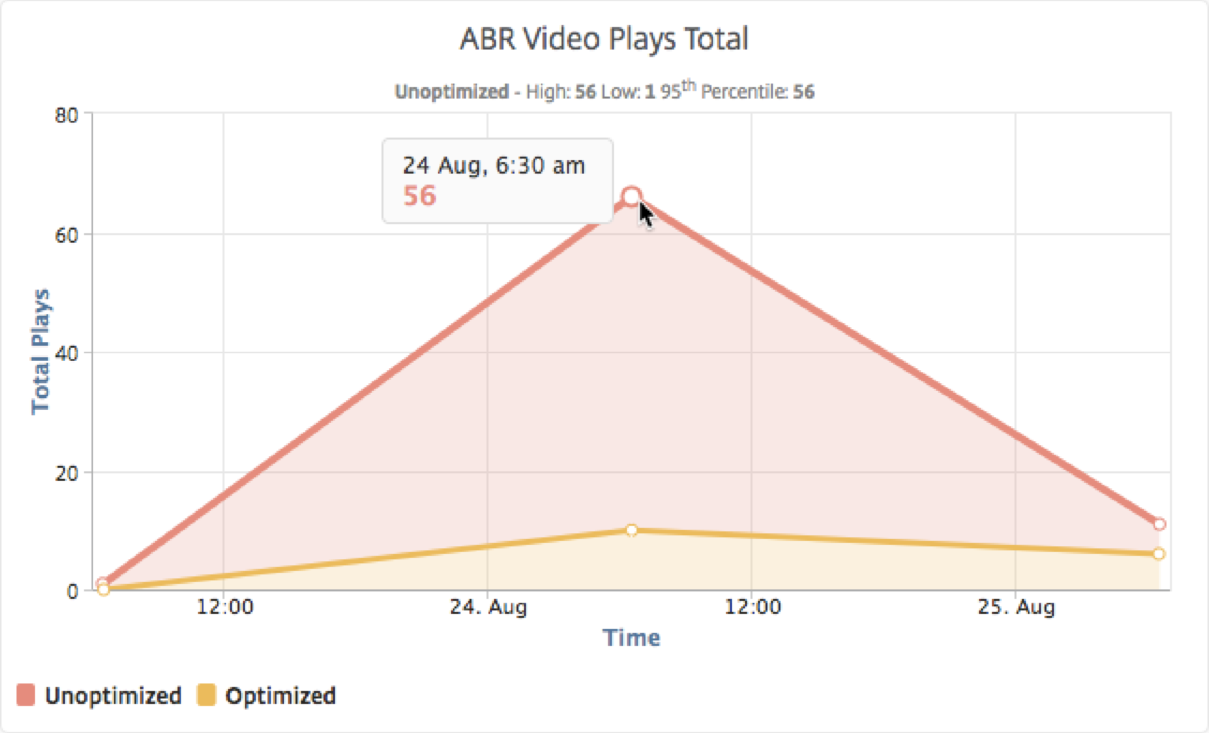
1. Navigate to **Infrastructure > Video Insight**, and click **ABR Video Analytics**.

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.

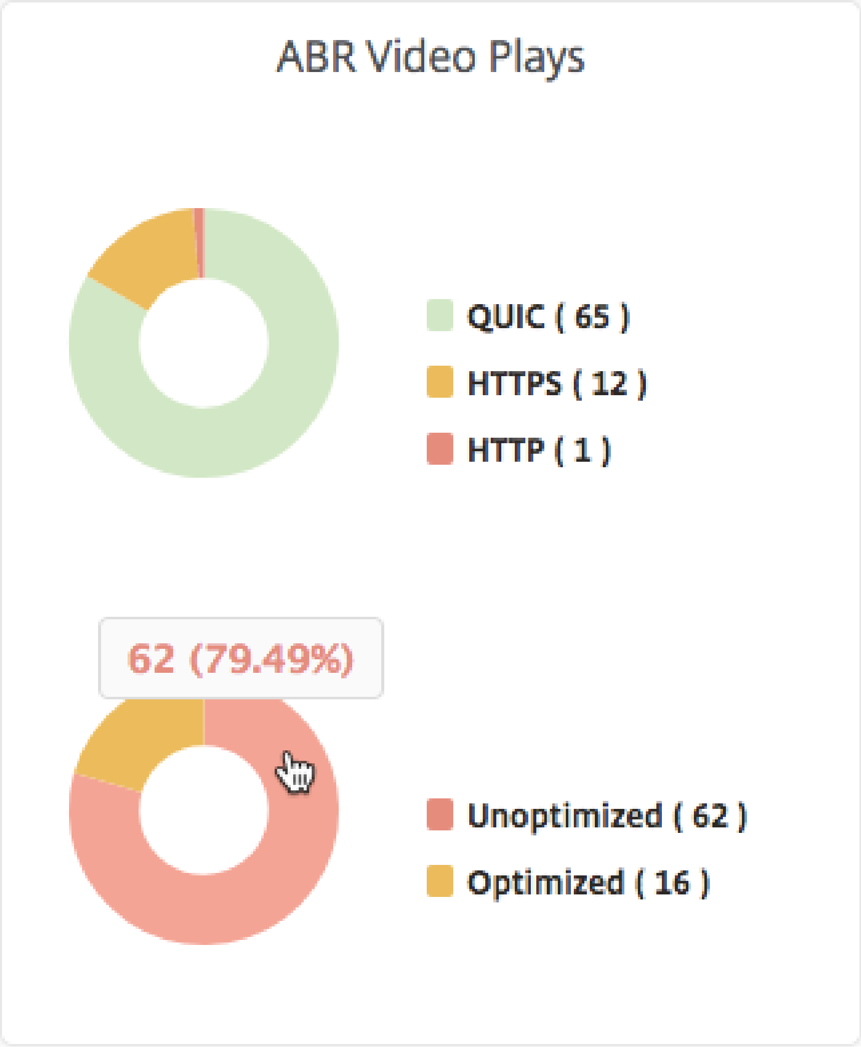
   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



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

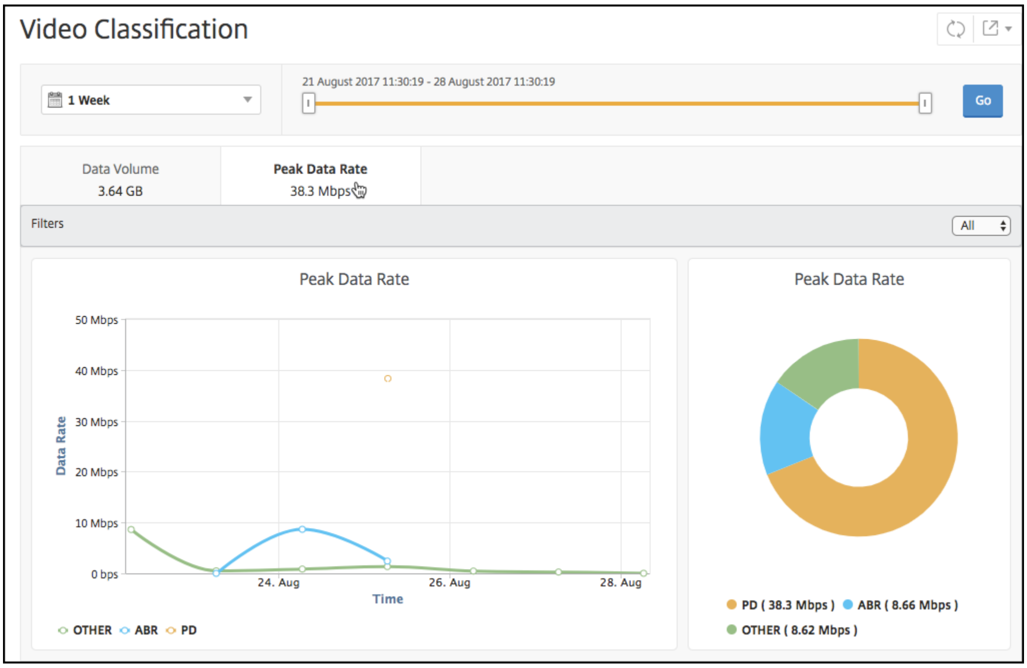
September 24, 2021

Citrix Application Delivery and Management shows you the peak throughput or data rate of the video traffic in your network.

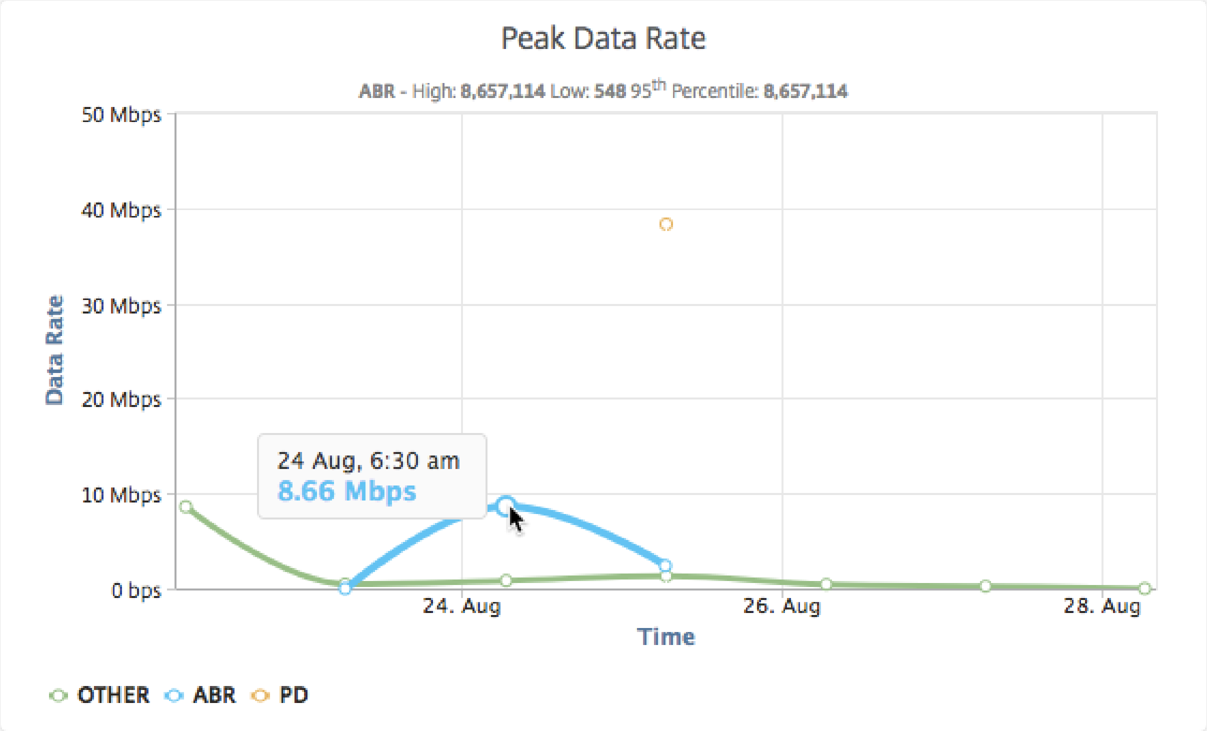
To see the peak data rate of the video traffic:

1. Navigate to **Infrastructure > 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.

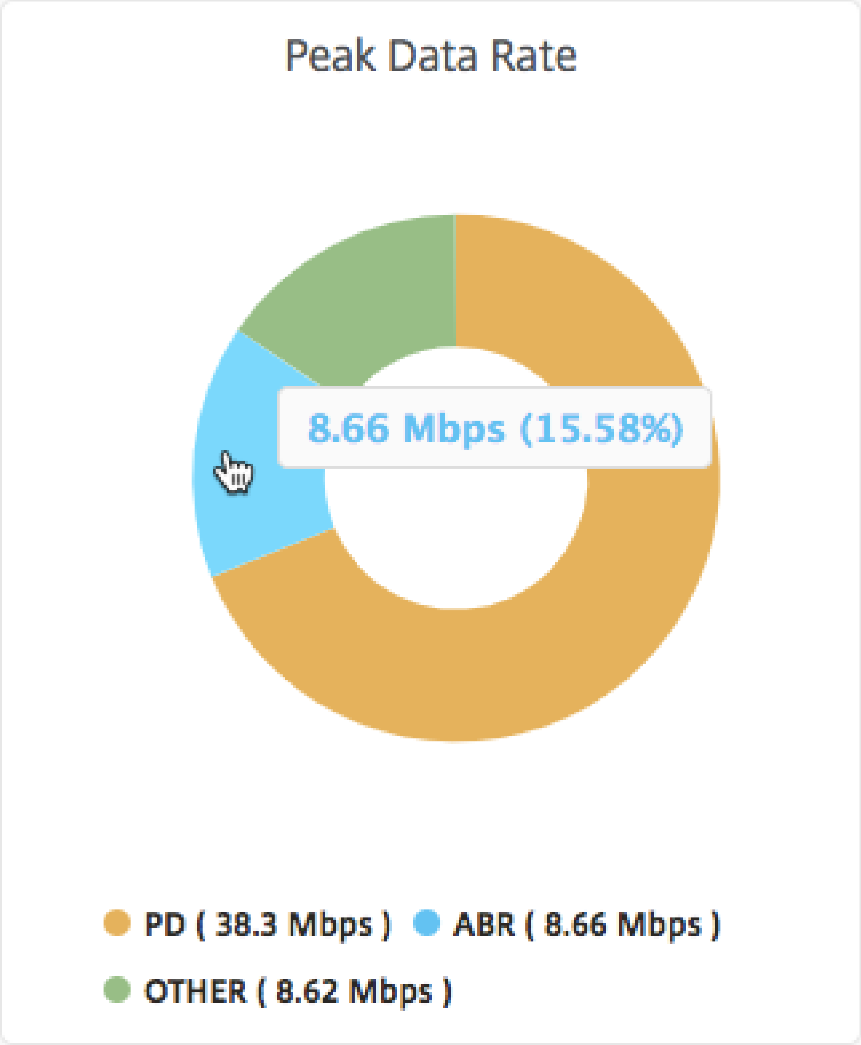
You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.



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.



WAN Insight

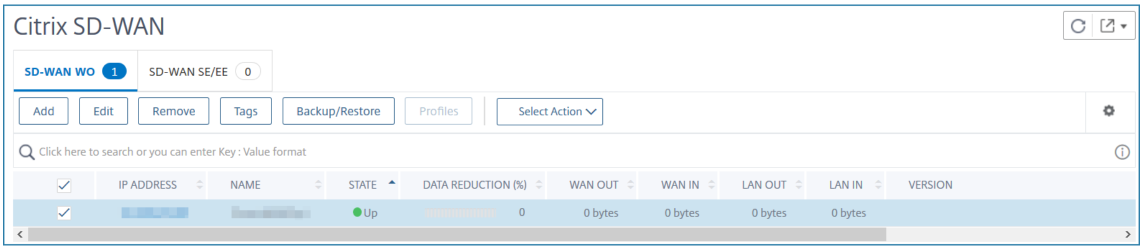
September 24, 2021

The Citrix SD-WAN WAN optimization (WO) appliances optimize the delivery of a large number of applications through the WAN, by improving the efficiency of data flow across the network between the data center and the branch sites. 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 provides visibility into clients, applications, and branches on the network, to help troubleshoot network issues effectively. Live and historical reports enable you to proactively address issues, if any

Enabling analytics on the data center WAN optimization appliance enables the Citrix Application Delivery and Management to collect data and provide reports and statistics for the data center and the branch WAN optimization appliances.

To enable analytics on the WAN optimization appliance:

1. Navigate to **Infrastructure > Instances > Citrix SD-WAN**, and select the SD-WAN WO instance.



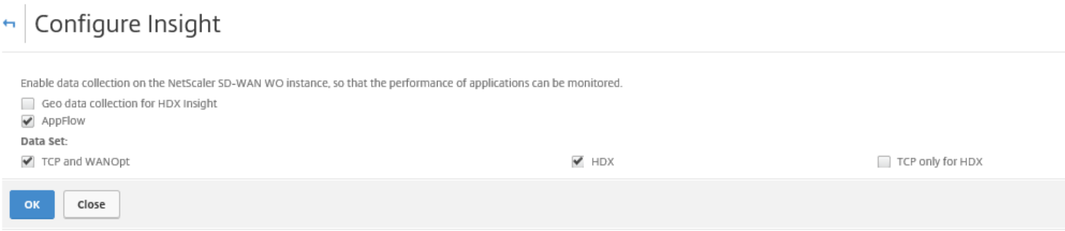
Citrix SD-WAN

☑	IP ADDRESS	NAME	STATE	DATA REDUCTION (%)	WAN OUT	WAN IN	LAN OUT	LAN IN	VERSION
☑	[redacted]	[redacted]	● Up	0	0 bytes	0 bytes	0 bytes	0 bytes	

2. From the **Select Action** list, select **Enable Insight**.

3. Select the following parameters as required:

    - **Geo data collection for HDX Insight**: Shares client IP address with the Google Geo API.
    - **AppFlow**: Starts collecting data from WAN optimization instances.
    - **TCP and WANOpt**: Provides TCP and **WANOpt Insight** reports.
    - **HDX**: Provides HDX Insight reports.
    - **TCP only for HDX**: Provides TCP only for HDX Insight reports.



Configure Insight

Enable data collection on the NetScaler SD-WAN WO instance, so that the performance of applications can be monitored.

☐ Geo data collection for HDX Insight

☑ AppFlow

Data Set:

☑ TCP and WANOpt ☑ HDX ☐ TCP only for HDX

4. Click **OK**.

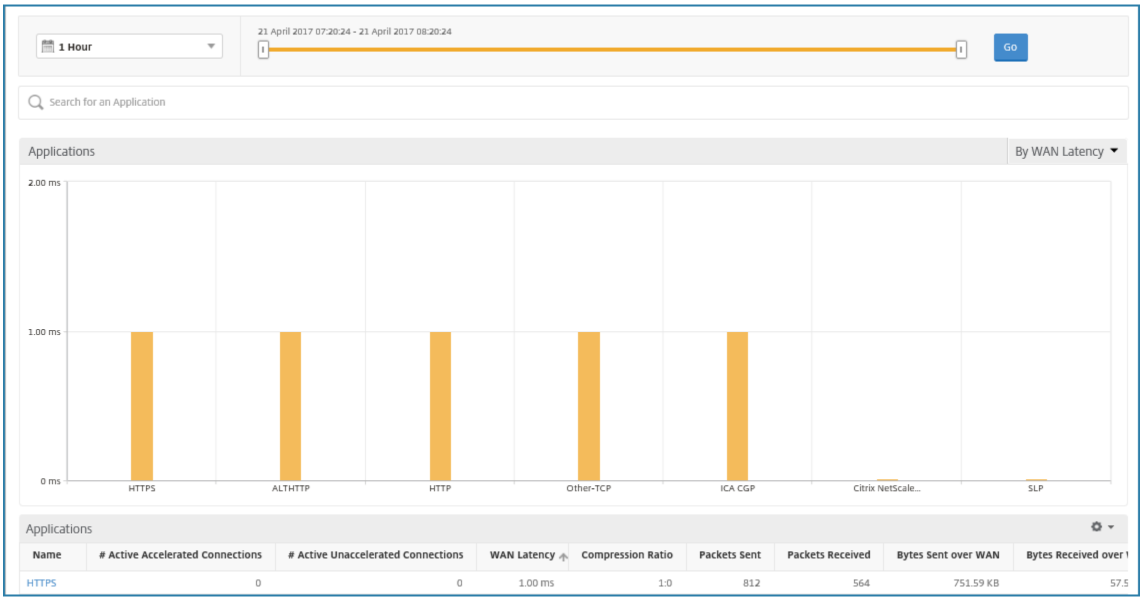
To view WAN Insight reports, navigate to **Infrastructure > WAN Insight**.

> **Note**
>
> The WAN Insight option is visible only after you add an SD-WAN WO instance to Citrix Application Delivery and Management.

You can view the following reports:

- **Applications** - Displays the usage and performance statistics of all the applications for the selected duration.
- **Branches** - Displays the usage and performance statistics of all the WAN optimization branch appliances.

- **Clients** - Displays the usage and performance statistics of all the clients accessing the WAN optimization appliances, in each branch.



1 Hour

21 April 2017 07:20:24 - 21 April 2017 08:20:24

Applications

Name	# Active Accelerated Connections	# Active Unaccelerated Connections	WAN Latency	Compression Ratio	Packets Sent	Packets Received	Bytes Sent over WAN	Bytes Received over \
HTTPS	0	0	1.00 ms	1:0	812	564	751.59 KB	57.5

The following metrics are displayed:

Metric	Description
Active Accelerated Connections	Number of active WAN connections that are accelerated.
Active Unaccelerated Connections	Number of active WAN connections that are not accelerated.
WAN Latency	Delay, in milliseconds, that the user experiences while interacting with an application.
Compression Ratio	Ratio of data compression between the branch office and data center appliances for the selected duration.
Packets Sent	Number of packets that the WAN optimization appliance has sent over the network for the selected duration.
Packets Received	Number of packets that the WAN optimization appliance has received from the network for the selected duration.

Metric	Description
Bytes Sent over WAN	Number of bytes that the Citrix WAN optimization appliance has sent over the WAN for the selected duration.
Bytes Received over WAN	Number of bytes that the WAN optimization appliance received from the WAN for the selected duration.
LAN RTO	Number of times the WAN optimization appliance has timed out retransmission to the LAN for the selected duration.
WAN RTO	Number of times the WAN optimization appliance has timed out retransmission to the WAN for the selected duration.
Retransmit Packets (LAN)	Number of packets the WAN optimization appliance has retransmitted to the LAN network for the selected duration.
Retransmit Packets (WAN)	Number of packets the WAN optimization appliance has retransmitted to the WAN network for the selected duration.

Manage licensing and enable analytics on virtual servers

October 26, 2021

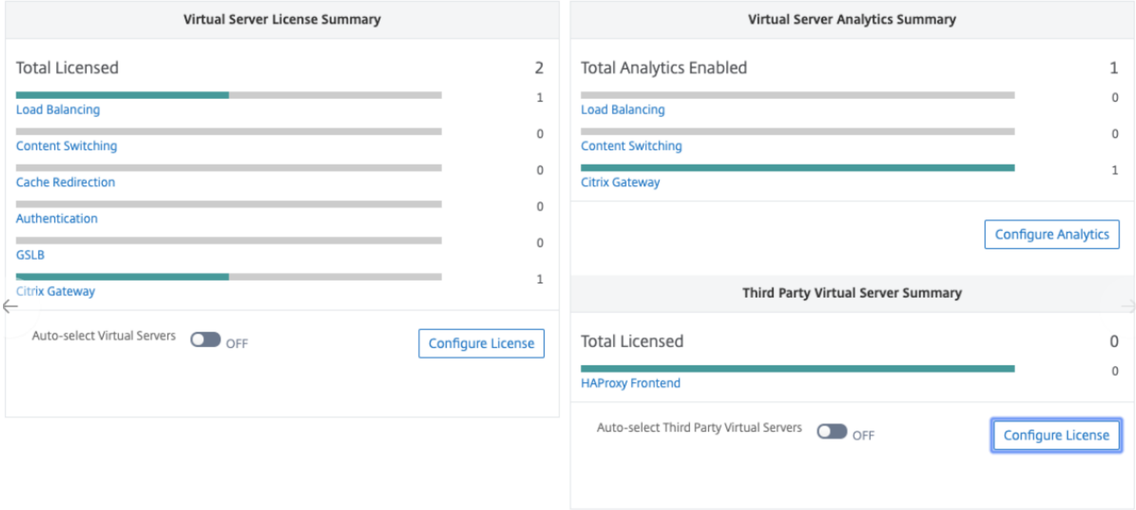
> Note
>
> By default, the **Auto Licensed Virtual Servers** option is enabled. You must ensure to have sufficient licenses to license the virtual servers. If you have limited licenses and want to license only the selective virtual servers based on your requirement, disable the **Auto Licensed Virtual Servers** option. Navigate to **Settings > Licensing & Analytics Config** and disable the **Auto Licensed Virtual Servers** option under **Virtual Server License Allocation**.

The process of enabling analytics is simplified. You can now license the virtual server and enable analytics in a single workflow.

Navigate to **Settings > Licensing & Analytics Config** to:

- View the **Virtual Server Licence Summary**

- View the **Virtual Server Analytics Summary**



Virtual Server License Summary

Total Licensed	2
Load Balancing	1
Content Switching	0
Cache Redirection	0
Authentication	0
GSLB	0
Citrix Gateway	1

Auto-select Virtual Servers OFF

Configure License

Virtual Server Analytics Summary

Total Analytics Enabled	1
Load Balancing	0
Content Switching	0
Citrix Gateway	1

Configure Analytics

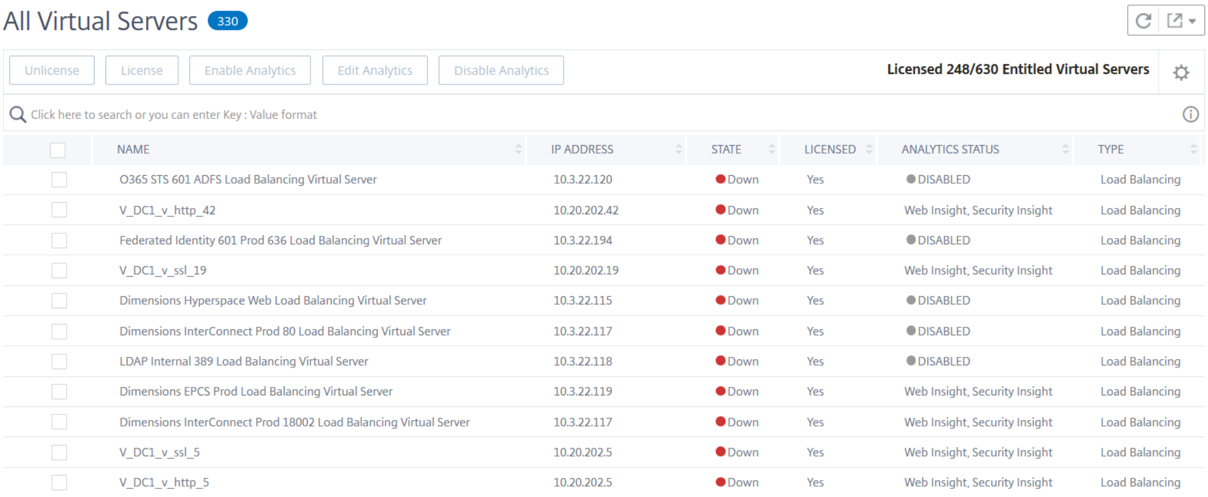
Third Party Virtual Server Summary

Total Licensed	0
HAProxy Frontend	0

Auto-select Third Party Virtual Servers OFF

Configure License

When you click **Configure License** or **Configure Analytics**, the **All Virtual Servers** page is displayed.



All Virtual Servers 330

Licensed 248/630 Entitled Virtual Servers

Click here to search or you can enter Key : Value format

□	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE
□	O365 STS 601 ADFS Load Balancing Virtual Server	10.3.22.120	● Down	Yes	● DISABLED	Load Balancing
□	V_DC1_v_http_42	10.20.202.42	● Down	Yes	Web Insight, Security Insight	Load Balancing
□	Federated Identity 601 Prod 636 Load Balancing Virtual Server	10.3.22.194	● Down	Yes	● DISABLED	Load Balancing
□	V_DC1_v_ssl_19	10.20.202.19	● Down	Yes	Web Insight, Security Insight	Load Balancing
□	Dimensions Hyperspace Web Load Balancing Virtual Server	10.3.22.115	● Down	Yes	● DISABLED	Load Balancing
□	Dimensions InterConnect Prod 80 Load Balancing Virtual Server	10.3.22.117	● Down	Yes	● DISABLED	Load Balancing
□	LDAP Internal 389 Load Balancing Virtual Server	10.3.22.118	● Down	Yes	● DISABLED	Load Balancing
□	Dimensions EPCS Prod Load Balancing Virtual Server	10.3.22.119	● Down	Yes	Web Insight, Security Insight	Load Balancing
□	Dimensions InterConnect Prod 18002 Load Balancing Virtual Server	10.3.22.117	● Down	Yes	Web Insight, Security Insight	Load Balancing
□	V_DC1_v_ssl_5	10.20.202.5	● Down	Yes	Web Insight, Security Insight	Load Balancing
□	V_DC1_v_http_5	10.20.202.5	● Down	Yes	Web Insight, Security Insight	Load Balancing

On the **All Virtual Servers** page, you can:

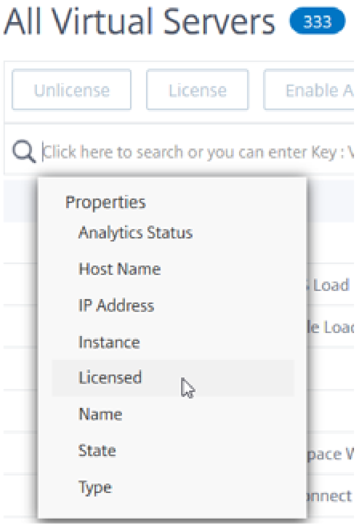
- Apply license for unlicensed virtual servers
- Remove license for licensed virtual servers
- Enable analytics on licensed virtual servers
- Edit analytics
- Disable analytics

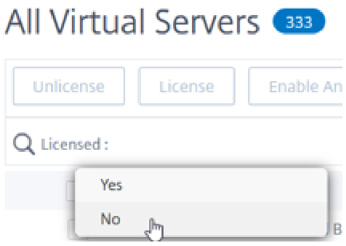
> **Note**
>
> The supported virtual servers to enable analytics are Load Balancing, Content Switching, and Citrix Gateway.

Manage licensing on virtual servers

To license the virtual servers, from the **All Virtual Servers** page:

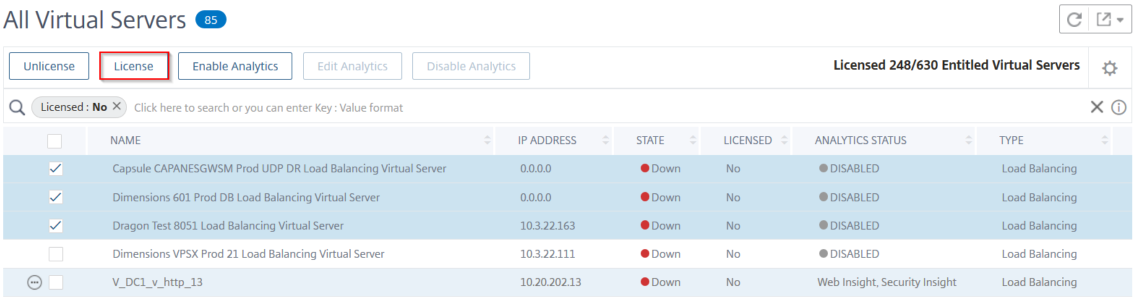
1. Click the search bar, select **Licensed**, and select **No**.





The filter is now applied and only the unlicensed virtual servers are displayed.

2. Select the virtual servers and then click **License**.

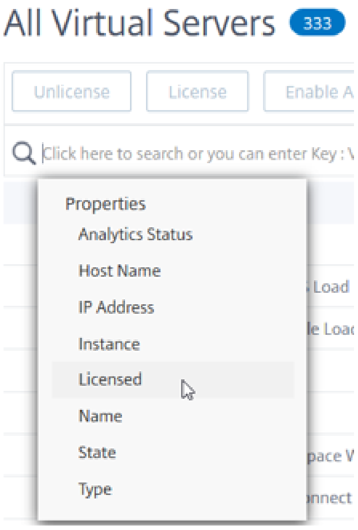


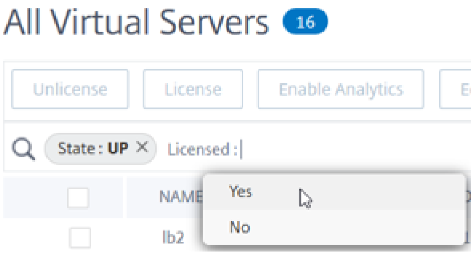
Licensed 248/630 Entitled Virtual Servers

□	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE
☑	Capsule CAPANESGWSM Prod UDP DR Load Balancing Virtual Server	0.0.0.0	● Down	No	● DISABLED	Load Balancing
☑	Dimensions 601 Prod DB Load Balancing Virtual Server	0.0.0.0	● Down	No	● DISABLED	Load Balancing
☑	Dragon Test 8051 Load Balancing Virtual Server	10.3.22.163	● Down	No	● DISABLED	Load Balancing
□	Dimensions VPSX Prod 21 Load Balancing Virtual Server	10.3.22.111	● Down	No	● DISABLED	Load Balancing
□	V_DC1_v_http_13	10.20.202.13	● Down	No	Web Insight, Security Insight	Load Balancing

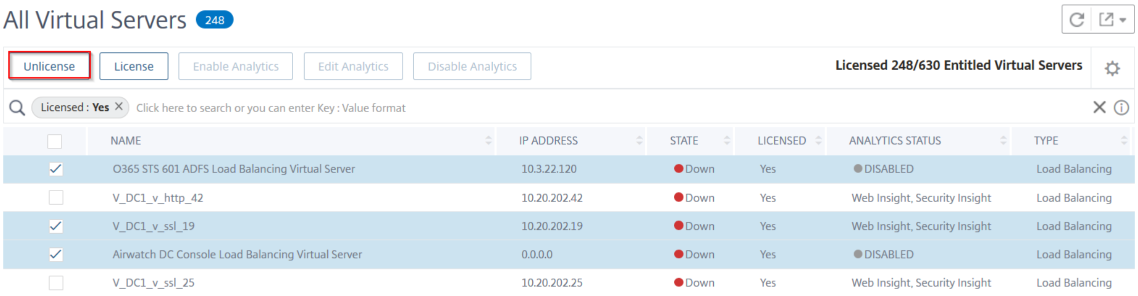
To unlicense the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **Yes**.





2. Select the virtual servers and click **Unlicense**.



□	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE
☑	O365 STS 601 ADFS Load Balancing Virtual Server	10.3.22.120	● Down	Yes	● DISABLED	Load Balancing
□	V_DC1_v_http_42	10.20.202.42	● Down	Yes	Web Insight, Security Insight	Load Balancing
☑	V_DC1_v_ssl_19	10.20.202.19	● Down	Yes	Web Insight, Security Insight	Load Balancing
☑	Airwatch DC Console Load Balancing Virtual Server	0.0.0.0	● Down	Yes	● DISABLED	Load Balancing
□	V_DC1_v_ssl_25	10.20.202.25	● Down	Yes	Web Insight, Security Insight	Load Balancing

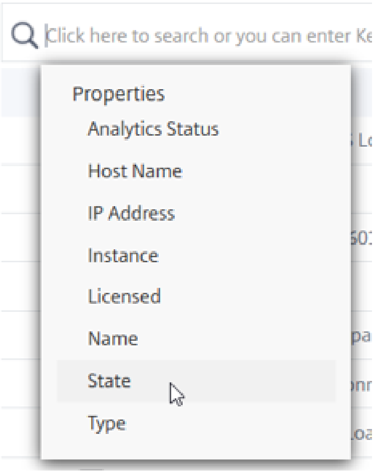
Enable analytics

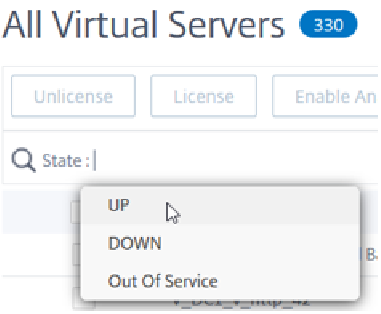
The following are the prerequisites to enable analytics for virtual servers:

- Ensure that virtual servers are **licensed**
- Ensure that analytics status is **Disabled**
- Ensure that virtual servers are in **UP** status

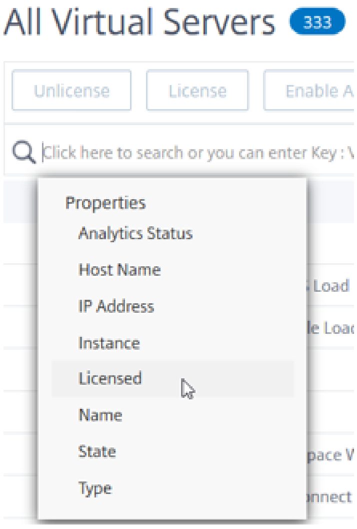
You can filter the results to identify the virtual servers that are mentioned in the prerequisites.

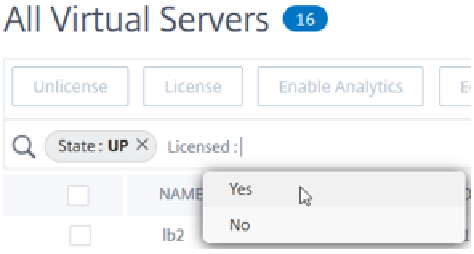
1. Click the search bar and select **State** and then select **UP**.



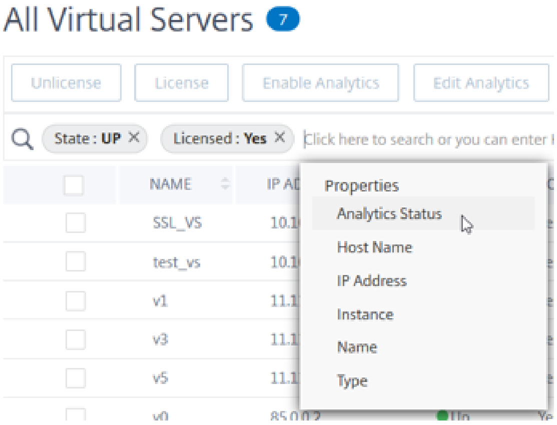


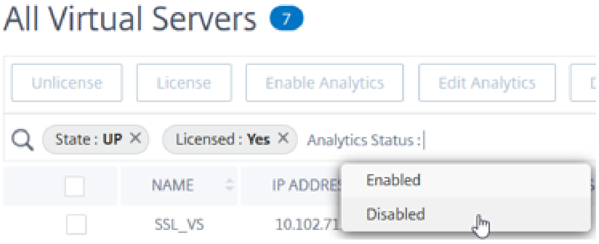
2. Click the search bar and select **Licensed**, and then select **Yes**.



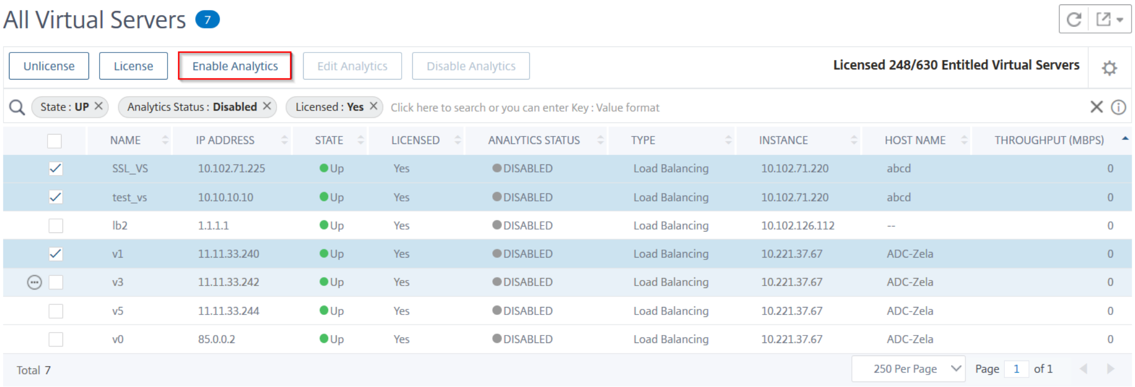


3. Click the search bar and select **Analytics Status**, and then select **Disabled**.





4. After applying the filters, select the virtual servers, and then click **Enable Analytics**.



Licensed 248/630 Entitled Virtual Servers

State : UP × Analytics Status : Disabled × Licensed : Yes × Click here to search or you can enter Key : Value format

	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE	HOST NAME	THROUGHPUT (MBPS)
☑	SSL_VS	10.102.71.225	● Up	Yes	● DISABLED	Load Balancing	10.102.71.220	abcd	0
☑	test_vs	10.10.10.10	● Up	Yes	● DISABLED	Load Balancing	10.102.71.220	abcd	0
□	lb2	1.1.1.1	● Up	Yes	● DISABLED	Load Balancing	10.102.126.112	--	0
☑	v1	11.11.33.240	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
□	v3	11.11.33.242	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
□	v5	11.11.33.244	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0
□	v0	85.0.0.2	● Up	Yes	● DISABLED	Load Balancing	10.221.37.67	ADC-Zela	0

Total 7 | 250 Per Page | Page 1 of 1

5. On the **Enable Analytics** window:

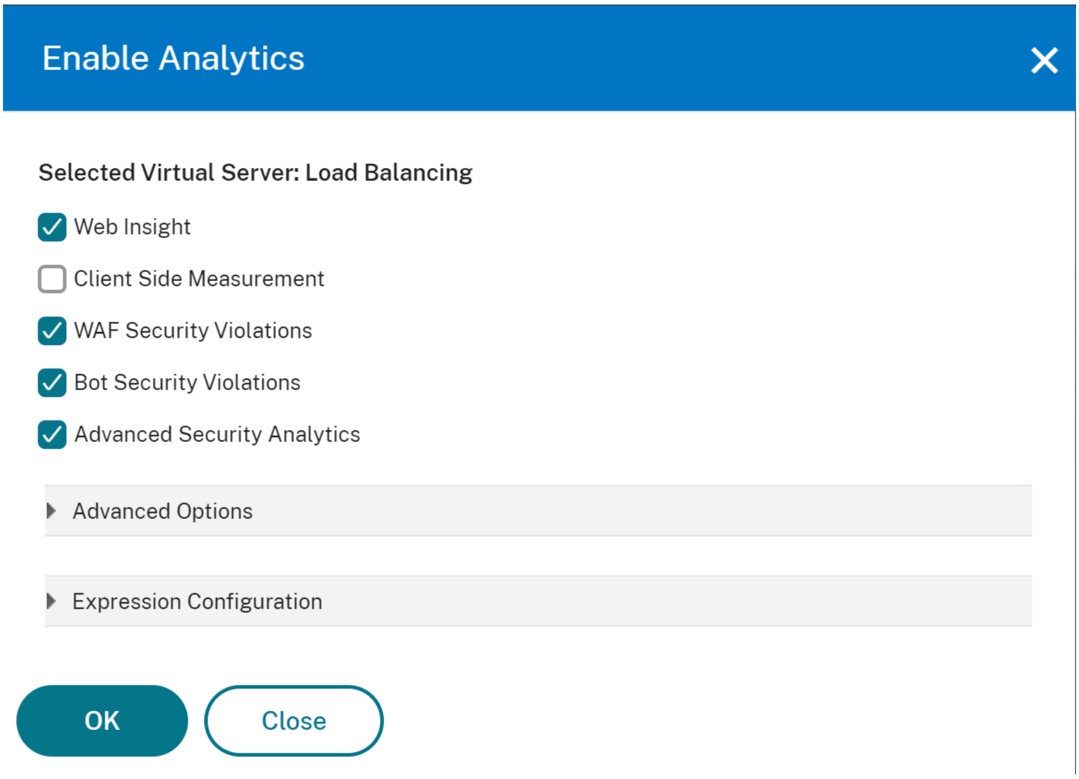
   a) Select the insight types (Web Insight, WAF Security Violations, Bot Security Violations)

   b) Select **Logstream** or **IPFIX** as Transport Mode

   > **Note**
   >
   > For Citrix ADC 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For Citrix ADC 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) The Expression is true by default

d) Click **OK**



Enable Analytics

Selected Virtual Server: Load Balancing

☑ Web Insight

□ Client Side Measurement

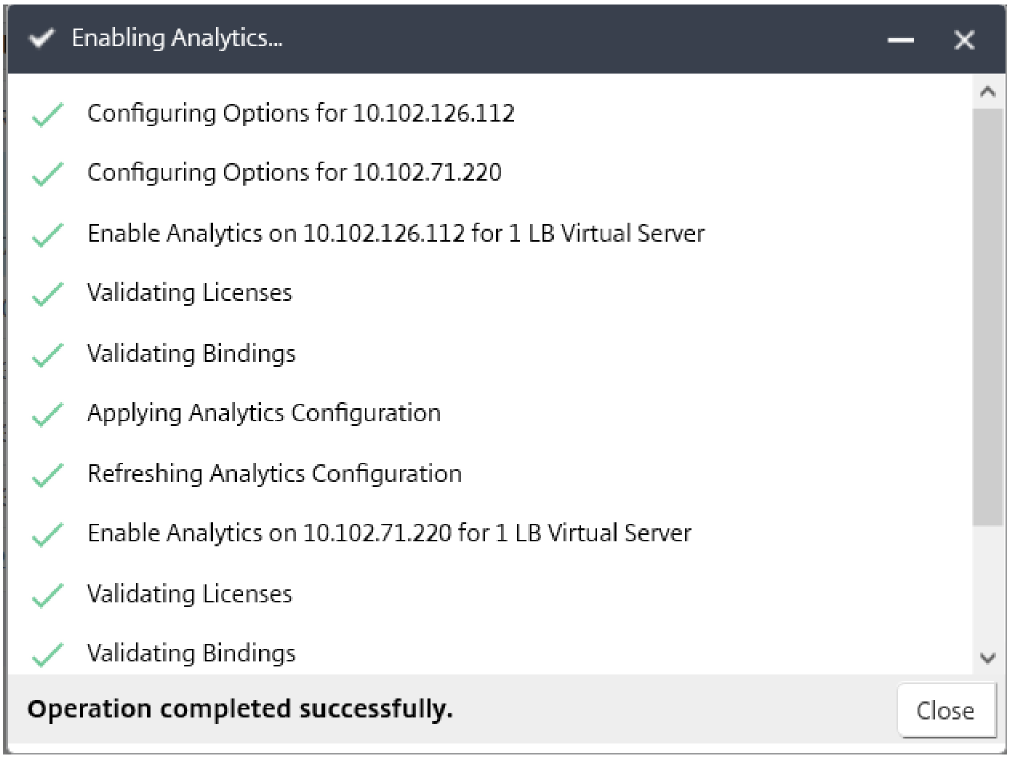
☑ WAF Security Violations

☑ Bot Security Violations

☑ Advanced Security Analytics

> **Note**
>
> - If you select virtual servers that are not licensed, then Citrix Application Delivery and Management 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**, Citrix Application Delivery and Management processes to enable analytics on the selected virtual servers.



✓ Configuring Options for 10.102.126.112

✓ Configuring Options for 10.102.71.220

✓ Enable Analytics on 10.102.126.112 for 1 LB Virtual Server

✓ Validating Licenses

✓ Validating Bindings

✓ Applying Analytics Configuration

✓ Refreshing Analytics Configuration

✓ Enable Analytics on 10.102.71.220 for 1 LB Virtual Server

✓ Validating Licenses

✓ Validating Bindings

Operation completed successfully.

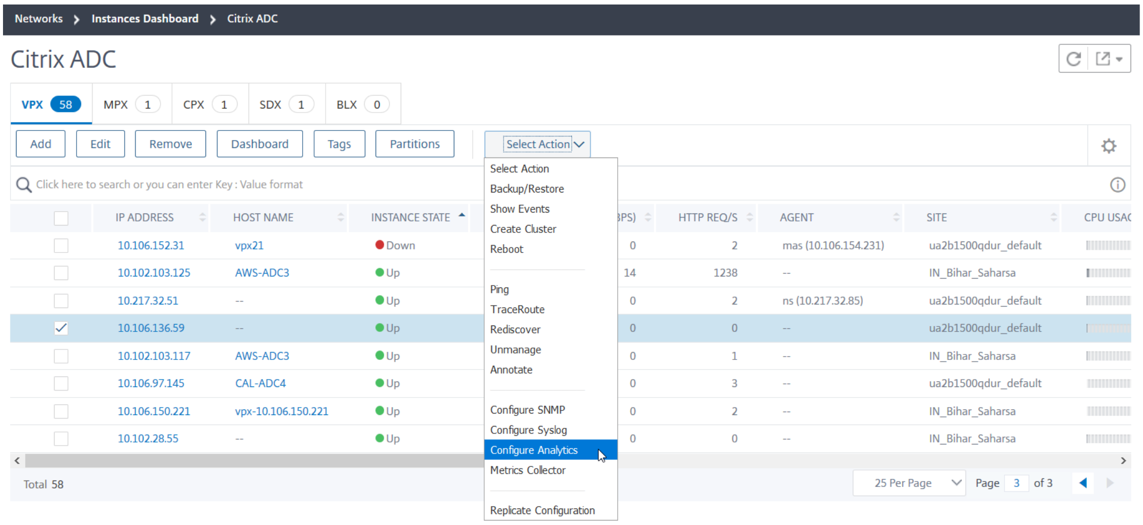
> **Note**
>
> Citrix Application Delivery and Management uses Citrix ADC SNIP for **Logstream** and NSIP for **IPFIX**. If there is a firewall enabled between Citrix Application Delivery and Management agent and Citrix ADC instance, ensure you open the following port to enable Citrix Application Delivery and Management agent to collect AppFlow traffic:

Transport Mode	Source IP	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Enable analytics for an instance

Alternatively, you can also enable analytics for a particular instance:

1. Navigate to **Infrastructure > Instances > Citrix ADC** and then select the instance type. For example, VPX.
2. Select the instance and from the **Select Action** list, select **Configure Analytics**.



Networks > Instances Dashboard > Citrix ADC

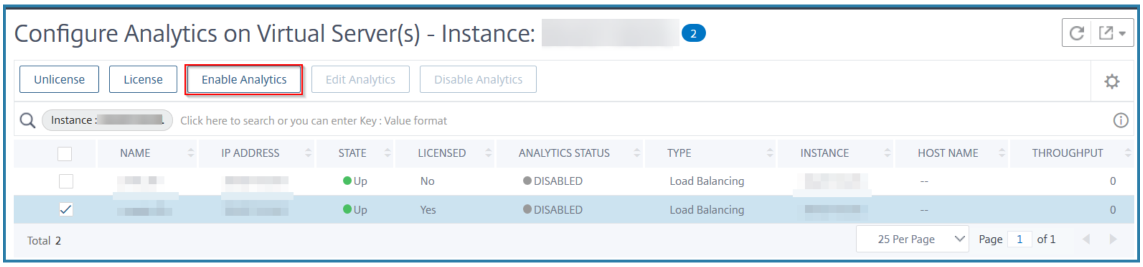
Citrix ADC

Select Action menu: Select Action, Backup/Restore, Show Events, Create Cluster, Reboot, Ping, TraceRoute, Rediscover, Unmanage, Annotate, Configure SNMP, Configure Syslog, Configure Analytics, Metrics Collector, Replicate Configuration

	IP ADDRESS	HOST NAME	INSTANCE STATE	BPS)	HTTP REQ/S	AGENT	SITE	CPU USAG
□	10.106.152.31	vpx21	● Down	0	2	mas (10.106.154.231)	ua2b1500qdur_default	
□	10.102.103.125	AWS-ADC3	● Up	14	1238	--	IN_Bihar_Saharsa	
□	10.217.32.51	--	● Up	0	2	ns (10.217.32.85)	ua2b1500qdur_default	
☑	10.106.136.59	--	● Up	0	0	--	ua2b1500qdur_default	
□	10.102.103.117	AWS-ADC3	● Up	0	1	--	IN_Bihar_Saharsa	
□	10.106.97.145	CAL-ADC4	● Up	0	3	--	ua2b1500qdur_default	
□	10.106.150.221	vpx-10.106.150.221	● Up	0	2	--	IN_Bihar_Saharsa	
□	10.102.28.55	--	● Up	0	0	--	IN_Bihar_Saharsa	

Total 58 — 25 Per Page — Page 3 of 3

3. On the **Configure Analytics on Virtual Server(s)** page, select the virtual server and click **Enable Analytics**.



Configure Analytics on Virtual Server(s) - Instance: [redacted] 2

	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE	HOST NAME	THROUGHPUT
□	[redacted]	[redacted]	● Up	No	● DISABLED	Load Balancing	[redacted]	--	0
☑	[redacted]	[redacted]	● Up	Yes	● DISABLED	Load Balancing	[redacted]	--	0

Total 2 — 25 Per Page — Page 1 of 1

4. On the **Enable Analytics** window:

   a) Select the insight type (Web Insight, WAF Security Violations, Bot Security Violations)

   b) Select **Logstream** or **IPFIX** as Transport Mode

   > **Note**
   >
   > For Citrix ADC 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For Citrix ADC 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.
   >
   > For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

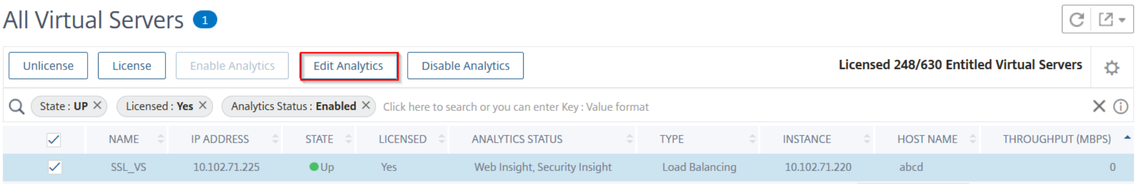
   c) The Expression is true by default

   d) Click **OK**

Edit analytics

To edit analytics on the virtual servers:

1. Select the virtual servers
2. Click **Edit Analytics**

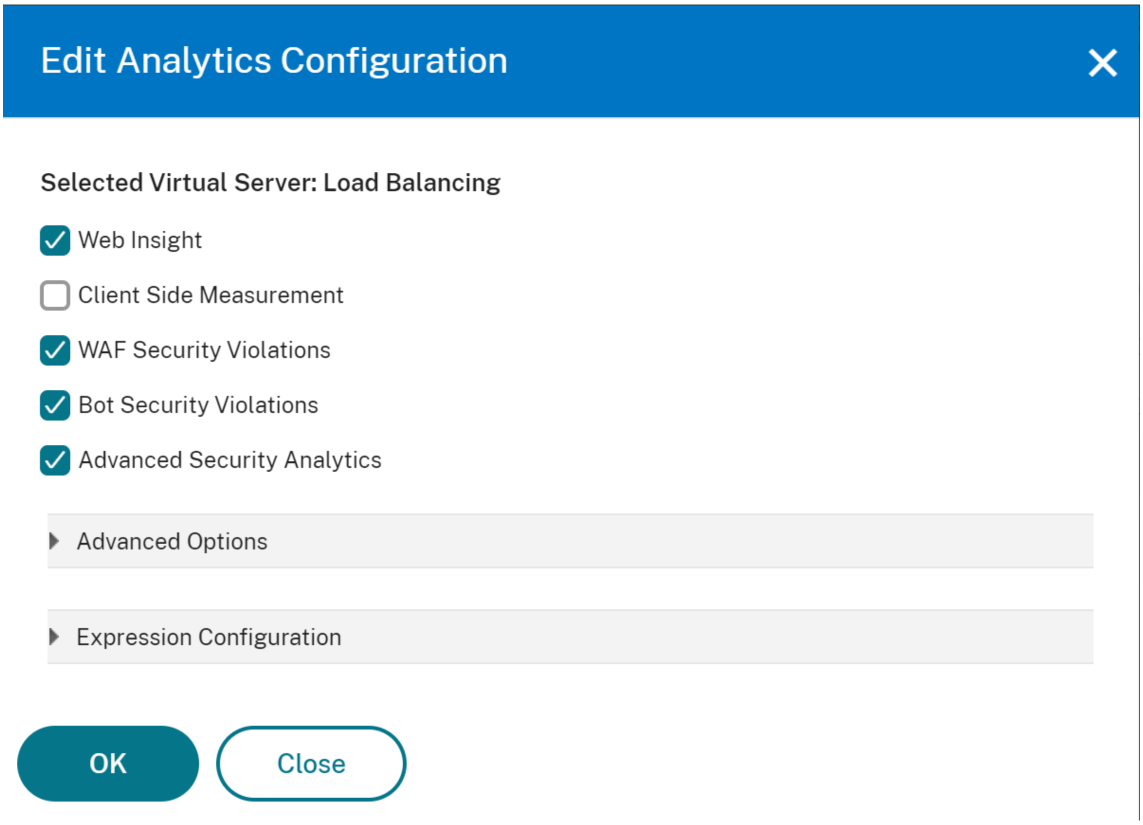


Licensed 248/630 Entitled Virtual Servers

☑	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE	HOST NAME	THROUGHPUT (MBPS)
☑	SSL_VS	10.102.71.225	● Up	Yes	Web Insight, Security Insight	Load Balancing	10.102.71.220	abcd	0

3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window

4. Click **OK**.



Selected Virtual Server: Load Balancing

☑ Web Insight

☐ Client Side Measurement

☑ WAF Security Violations

☑ Bot Security Violations

☑ Advanced Security Analytics

Edit analytics for an instance

Alternatively, you can also disable analytics for a particular instance:

1. Navigate to **Network > Instance > Citrix ADC** and the select the instance type. For example, VPX.

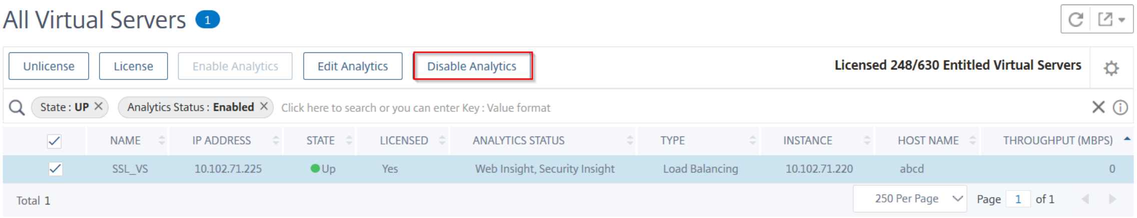
2. Select the instance and click **Edit Analytics**

Disable analytics

To disable analytics on the selected virtual servers:

1. Select the virtual servers

2. Click **Disable Analytics**



All Virtual Servers 1

Licensed 248/630 Entitled Virtual Servers

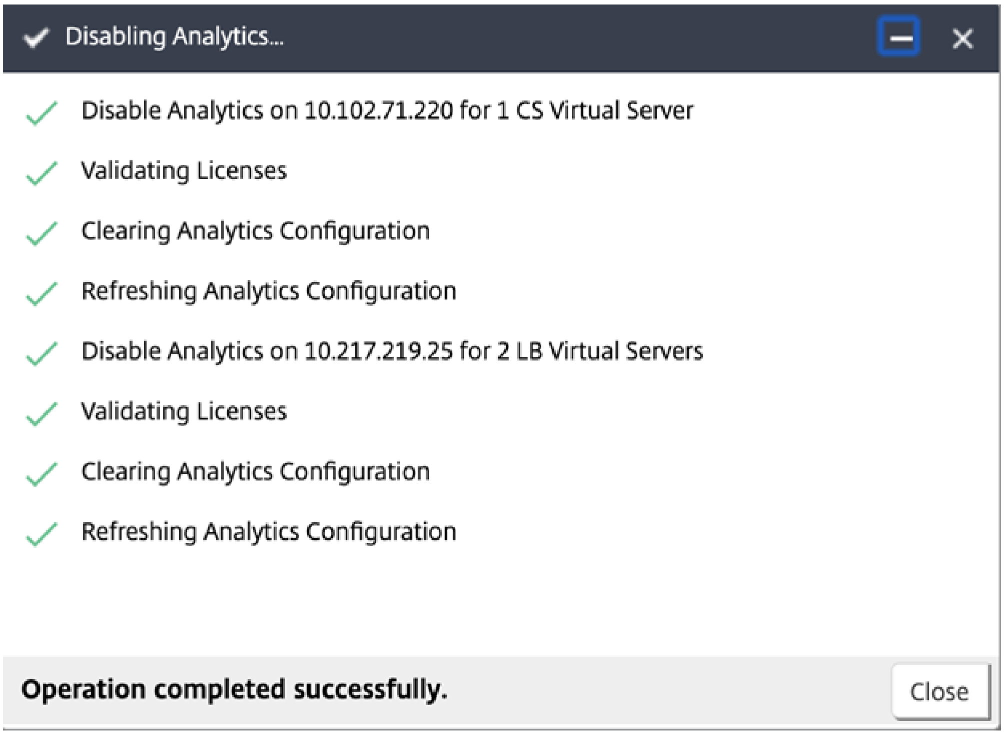
State : **UP** ✕ Analytics Status : **Enabled** ✕ Click here to search or you can enter Key : Value format

☑	NAME	IP ADDRESS	STATE	LICENSED	ANALYTICS STATUS	TYPE	INSTANCE	HOST NAME	THROUGHPUT (MBPS)
☑	SSL_VS	10.102.71.225	● Up	Yes	Web Insight, Security Insight	Load Balancing	10.102.71.220	abcd	0

Total 1

250 Per Page Page 1 of 1

Citrix Application Delivery and Management disables the analytics on the selected virtual servers



✓ Disabling Analytics…

✓ Disable Analytics on 10.102.71.220 for 1 CS Virtual Server

✓ Validating Licenses

✓ Clearing Analytics Configuration

✓ Refreshing Analytics Configuration

✓ Disable Analytics on 10.217.219.25 for 2 LB Virtual Servers

✓ Validating Licenses

✓ Clearing Analytics Configuration

✓ Refreshing Analytics Configuration

Operation completed successfully.

A unified process to enable analytics on virtual servers

October 27, 2021

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 from Citrix Application Delivery and Management:

- 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.

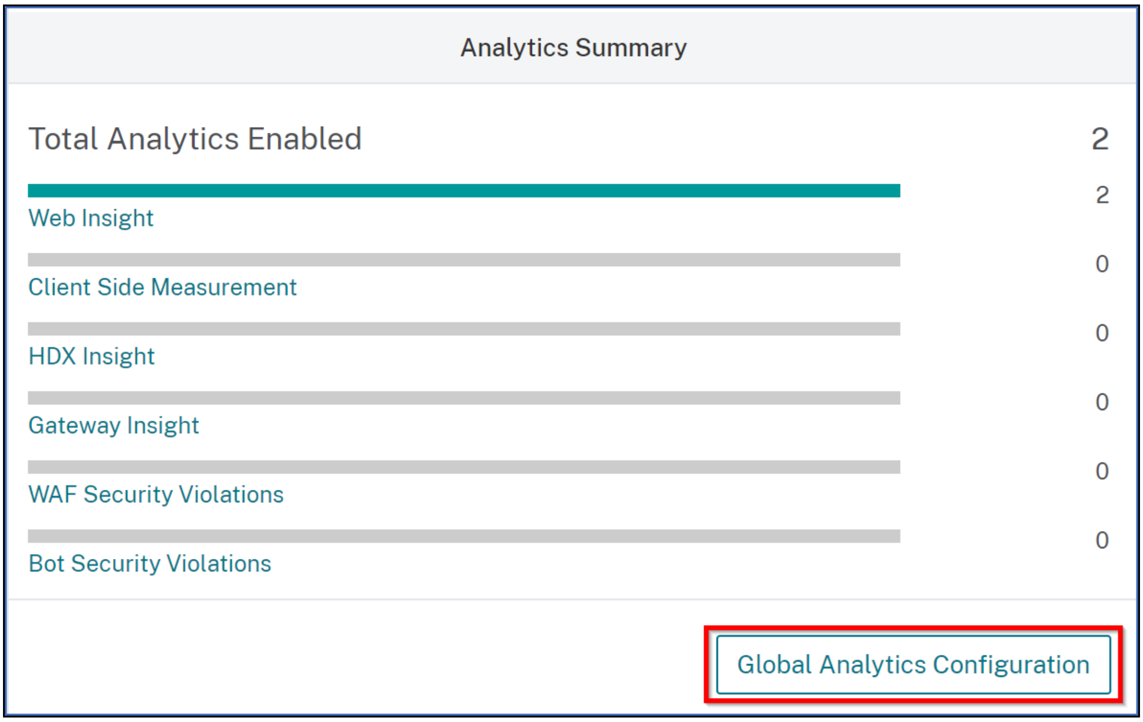
Prerequisites

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**.



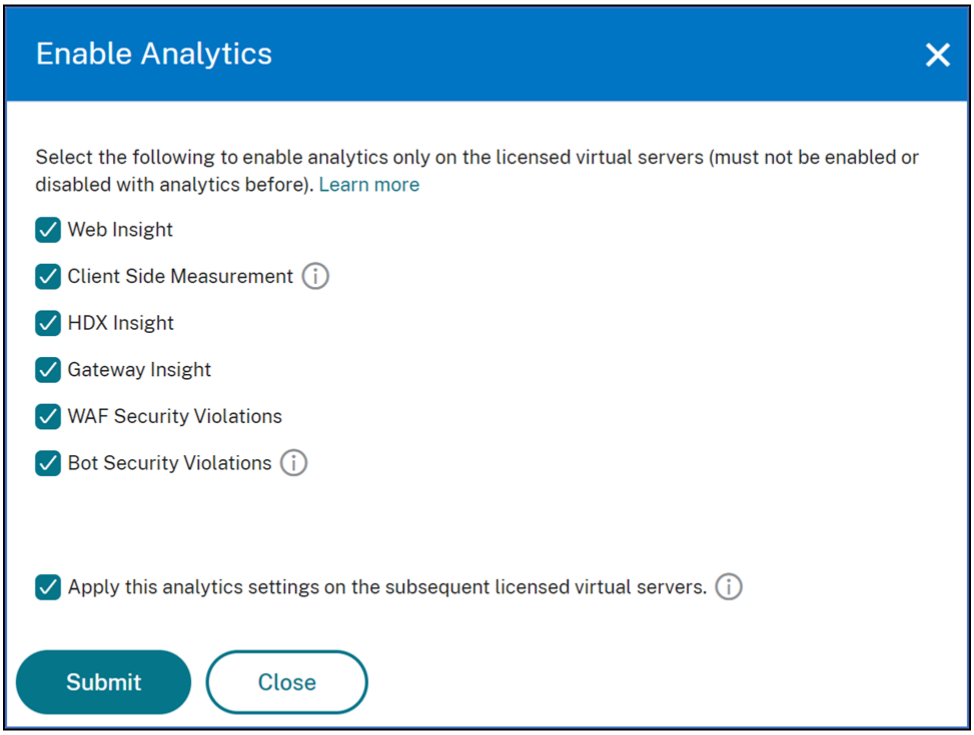
Analytics Summary

Total Analytics Enabled	2
Web Insight	2
Client Side Measurement	0
HDX Insight	0
Gateway Insight	0
WAF Security Violations	0
Bot Security Violations	0

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**.



Enable Analytics

Select the following to enable analytics only on the licensed virtual servers (must not be enabled or disabled with analytics before). Learn more

☑ Web Insight

☑ Client Side Measurement

☑ HDX Insight

☑ Gateway Insight

☑ WAF Security Violations

☑ Bot Security Violations

☑ Apply this analytics settings on the subsequent licensed virtual servers.

Configure role-based access control

September 28, 2021

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, all users are added in Citrix Cloud. As the first user of your organization, you must first create an account in Citrix Cloud and then log on to the Citrix Application Delivery and Management GUI with the Citrix Cloud credentials. You are granted the super admin role, and by default, you have all access permissions in Citrix Application Delivery and Management. Later you can create other users in your organization in Citrix Cloud.

Users who are created later and who log on to Citrix Application Delivery and Management as regular users are known as delegated admins. These users, by default, have all the permissions except user administration permissions. However, you can grant specific user administration permissions to these delegated admin users. You can do that by creating appropriate policies and by assigning them to these delegated users. The user administration permissions are at **Settings** > **User Administration**. For more information on how to assign specific permissions, see How to Assign extra Permissions to Delegated Admin Users.

More information on how to create policies, roles, groups, and how to bind the users to groups is provided in the following sections.

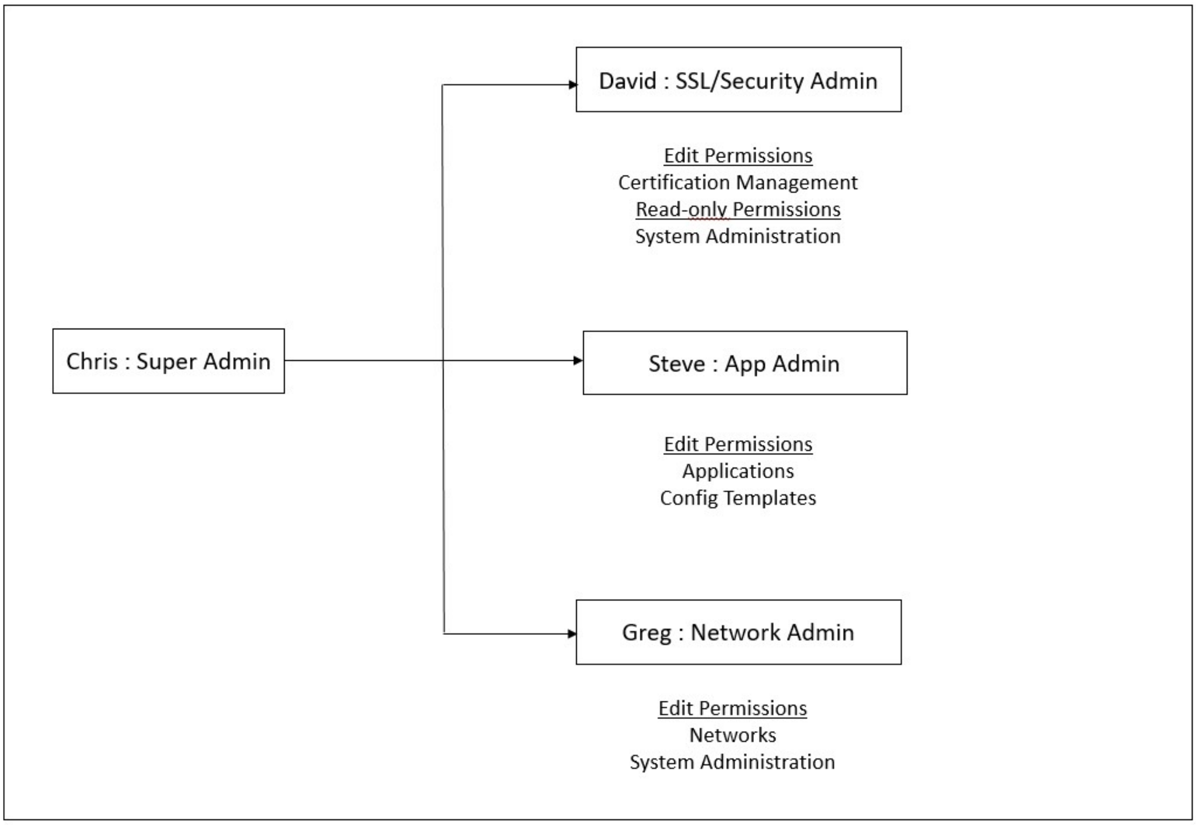
Example:

The following example illustrates how RBAC can be achieved in Citrix Application Delivery and Management.

Chris, the ADC group head, is the super administrator of Citrix Application Delivery and Management in his organization. He 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 must 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.

The following image shows the permissions that the administrators and other users have and their roles in the organization.



To provide role based access control to his users, Chris must first add users in Citrix Cloud and only after that he can see the users in Citrix Application Delivery and Management. Chris must create access policies for each of the users depending on their role. Access policies are tightly bound to roles. So, Chris must also create roles, and then he must create groups as roles can be assigned to groups only and not to individual users.

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 in creating configuration templates.

Roles are determined by policies. After creating policies, you can 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 by adding them to specific groups based on specific conditions. In Citrix Application Delivery and Management, creating roles and policies are specific to the RBAC feature in Citrix ADC. 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. Application administrators are able to access only the resources within their scope.

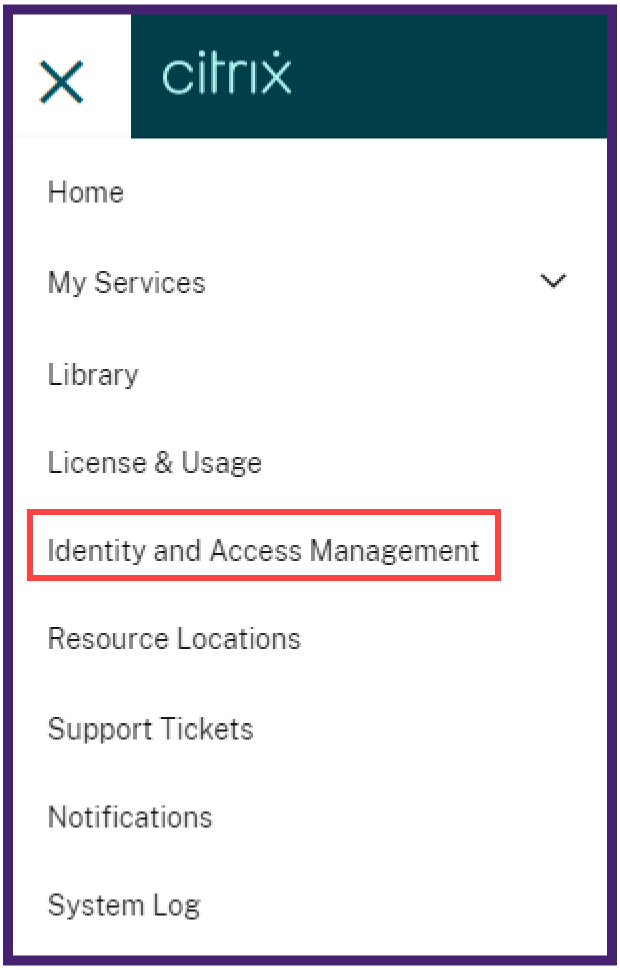
Therefore, in your role as Chris, the super admin, perform the following example tasks in Citrix Application Delivery and Management to configure access policies, roles, and user groups for David who is the security admin in your organization.

Configure Users on Citrix Application Delivery and Management

As a super admin, you can create more users by configuring accounts for them in Citrix Cloud and not in Citrix Application Delivery and Management. When the new users are added to Citrix Application Delivery and Management, you can only define their permissions by assigning the appropriate groups to the user.

To add new users in Citrix Cloud:

1. In the Citrix Application Delivery and Management GUI, click the Hamburger icon at the top left, and select **Identity and Access Management**.

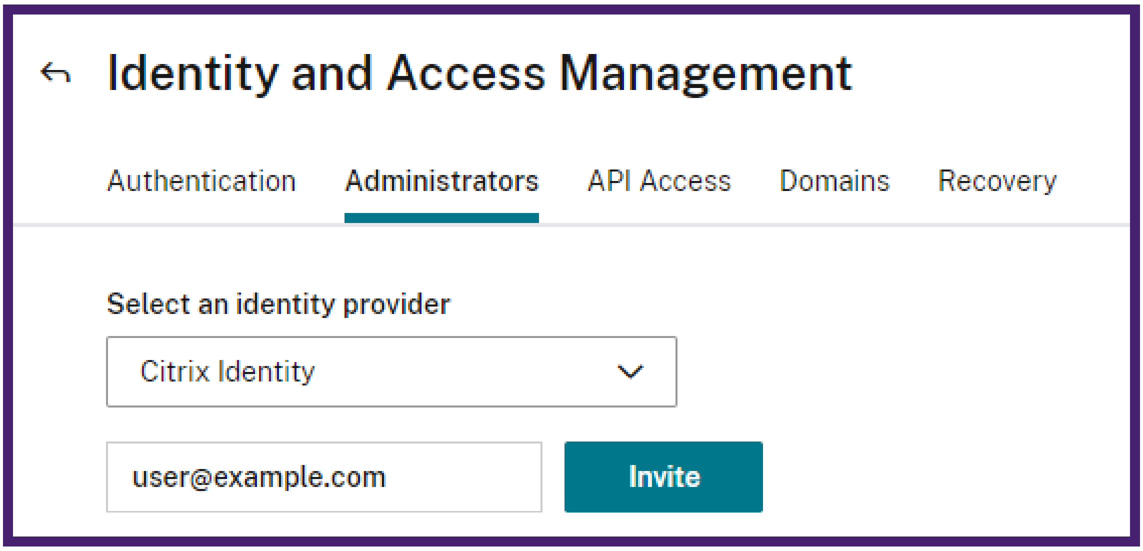


2. On the Identity and Access Management page, select **Administrators** tab.

   This tab lists the users that are created in Citrix Cloud.

3. Select **Citrix Identity** as an identity provider.

4. Type the email address of the user that you want to add in Citrix Application Delivery and Management and click **Invite**.

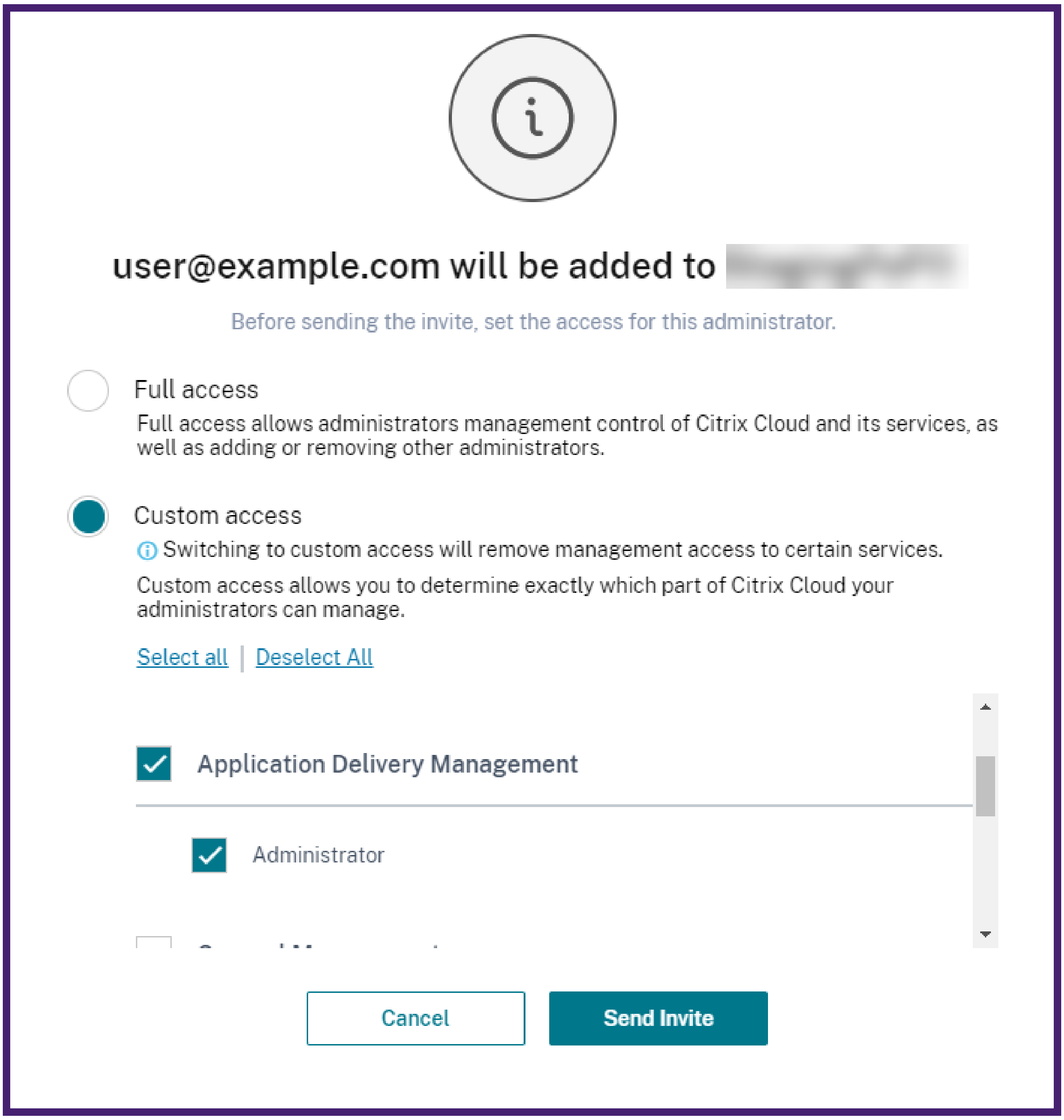
   

   > **Note**
   >
   > The user receives an email invite from Citrix Cloud. The user must click the link provided in the email to complete the registration process by providing their full name and password, and later log on to Citrix Application Delivery and Management using their credentials.

5. Select **Custom access** for the specified user.

6. Select **Application Delivery Managment**.

   This option lists the user groups created in Citrix Application Delivery and Management. Select the group to which you want to add the user.



user@example.com will be added to [redacted]

Before sending the invite, set the access for this administrator.

○ Full access

Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.

● Custom access

ⓘ Switching to custom access will remove management access to certain services.

Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.

Select all | Deselect All

☑ Application Delivery Management

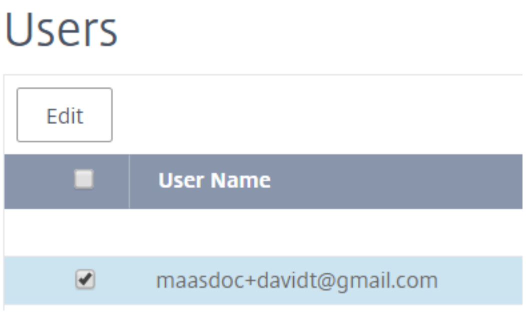
☑ Administrator

7. Click **Send Invite**.

As an admin, you see the new user in the Citrix Application Delivery and Management Users list only after the user logs on to Citrix Application Delivery and Management.

To Configure Users in Citrix Application Delivery and Management:

1. In the Citrix Application Delivery and Management GUI, navigate to **Settings** > **User Administration** > **Users**.
2. The user is displayed on the **Users** page.



☐	User Name
☑	maasdoc+davidt@gmail.com

3. You can edit the privileges provided to the user by selecting the user and clicking **Edit**. You can also edit group permissions on the **Groups** page under the **Settings** node.

   > **Note**
   >
   > - The users are added in Citrix Application Delivery and Management from the Citrix Cloud only. Therefore, even though you have admin permissions, you cannot add or delete users in the Citrix Application Delivery and Management GUI. You can only edit the group permissions. Users can be added or deleted from Citrix Cloud.
   > - The user details appear on the service GUI only after the user has logged on to the Citrix Application Delivery and Management at least once.

Configure Access Policies on Citrix Application Delivery and Management

Access policies define permissions. A policy can be applied to a user group or to multiple groups by creating roles. Roles are determined by policies. After creating policies, you must create roles, bind each role to one or more policies, and assign roles to user groups. Citrix Application Delivery and Management provides five predefined access policies:

- **admin_policy**. Grants access to all Citrix Application Delivery and Management nodes. The user has both view and edit permissions, can view all Citrix Application Delivery and Management content, and can perform all edit operations. That is, the user can add, modify, and delete operations on the resources.
- **adminExceptSystem_policy**. Grants access to users for all nodes in Citrix Application Delivery and Management GUI, except access to the Settings node.
- **readonly_policy**. Grants read-only permissions. The user can view all content on Citrix Application Delivery and Management but is not authorized to perform any operations.
- **appadmin_policy**. Grants administrative permissions for accessing the application features in Citrix Application Delivery and Management. 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, and cache redirection.
- **appreadonly_policy**. 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.

Though you cannot edit these predefined policies, you can create your own (user-defined) policies.

Earlier, when you assigned policies to roles and bound the roles to user groups, you can provide permissions for the user groups at node level in the Citrix Application Delivery and Management GUI. For example, you might only provide access permissions to the entire Load Balancing node. Your users had permission to access all entity-specific subnodes under Load Balancing node (for example, virtual server, services, and others) or they did not have permission to access any node under **Load Balancing**.

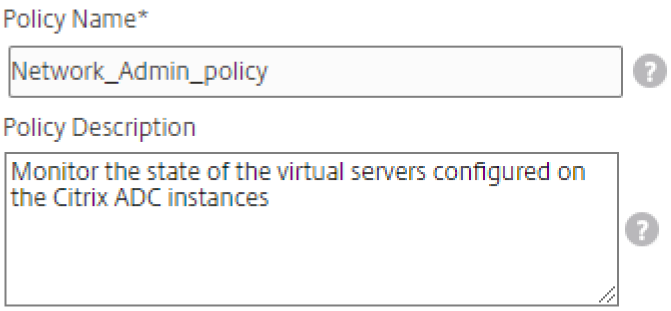
In Citrix Application Delivery and Management 507.x build and later versions, the access policy management is extended to provide permissions for subnodes as well. Access policy settings can be configured for all subnodes such as virtual servers, services, service groups, and servers.

Currently, you can provide such a granular level access permission only for subnodes under a Load Balancing node and also for subnodes under the GSLB node.

For example, as an administrator, you might want to give the user an access permission for only to view virtual servers, but not the back end services, service groups, and application servers in the Load Balancing node. The users with such a policy assigned to them can access only the virtual servers.

To create user-defined access policies:

1. In the Citrix Application Delivery and Management GUI, navigate to **Settings** > **User Administration** > **Access Policies**.
2. Click **Add**.
3. On the **Create Access Policies** page, in the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.



Policy Name*

Network_Admin_policy

Policy Description

Monitor the state of the virtual servers configured on the Citrix ADC instances

The **Permissions** section lists of all Citrix Application Delivery and Management features, with options for specifying read-only, enable-disable, or edit access.

   a) Click the (+) icon to expand each feature group into multiple features.
   b) 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 Citrix Application Delivery and Management.
- **Enable-Disable:** This option is available only for the **Network Functions** features that allow enable or disable action on Citrix Application Delivery and Management. User can enable or disable the feature. And, a user can also perform the **Poll Now** action.

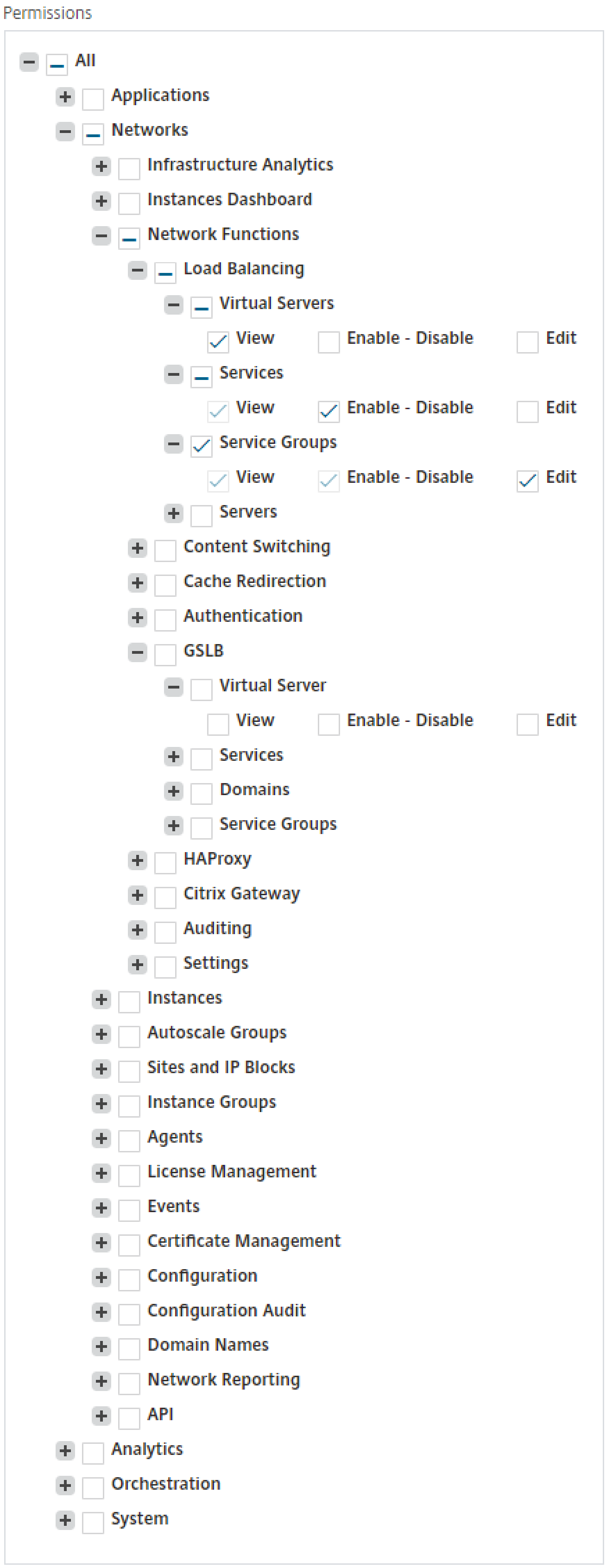
  When you grant the **Enable-Disable** permission to a user, the **View** permission is also granted. You cannot deselect this option.
- **Edit:** This option grants the full access to the user. User can modify the feature and its functions.

  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:



Permissions

- ⊟ ⊟ All
  - ⊞ □ Applications
  - ⊟ ⊟ Networks
    - ⊞ □ Infrastructure Analytics
    - ⊞ □ Instances Dashboard
    - ⊟ ⊟ Network Functions
      - ⊟ ⊟ Load Balancing
        - ⊟ ⊟ Virtual Servers
          - ☑ View □ Enable - Disable □ Edit
        - ⊟ ⊟ Services
          - ☑ View ☑ Enable - Disable □ Edit
        - ⊟ ☑ Service Groups
          - ☑ View ☑ Enable - Disable ☑ Edit
        - ⊞ □ Servers
      - ⊞ □ Content Switching
      - ⊞ □ Cache Redirection
      - ⊞ □ Authentication
      - ⊟ □ GSLB
        - ⊟ □ Virtual Server
          - □ View □ Enable - Disable □ Edit
        - ⊞ □ Services
        - ⊞ □ Domains
        - ⊞ □ Service Groups
      - ⊞ □ HAProxy
      - ⊞ □ Citrix Gateway
      - ⊞ □ Auditing
      - ⊞ □ Settings
    - ⊞ □ Instances
    - ⊞ □ Autoscale Groups
    - ⊞ □ Sites and IP Blocks
    - ⊞ □ Instance Groups
    - ⊞ □ Agents
    - ⊞ □ License Management
    - ⊞ □ Events
    - ⊞ □ Certificate Management
    - ⊞ □ Configuration
    - ⊞ □ Configuration Audit
    - ⊞ □ Domain Names
    - ⊞ □ Network Reporting
    - ⊞ □ API
  - ⊞ □ Analytics
  - ⊞ □ Orchestration
  - ⊞ □ System

The **View** permission is granted to a user for the **Virtual Servers** feature. User can view the load balancing virtual servers in Citrix Application Delivery and Management. 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, the 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.

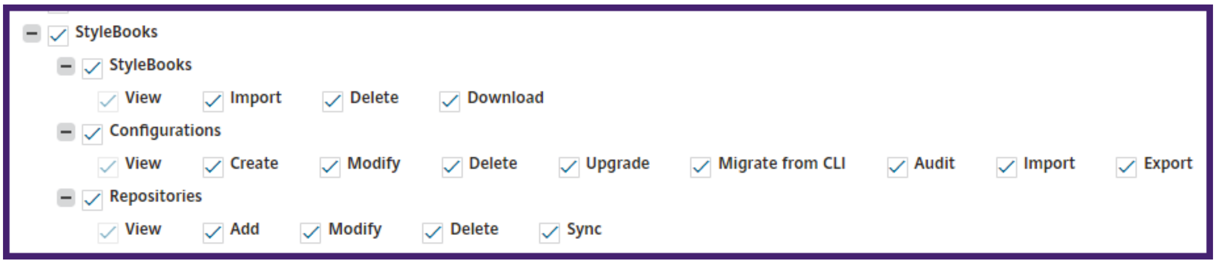
4. Click **Create**.

> **Note**
>
> Selecting **Edit** might internally assign dependent permissions that are not shown as enabled in the Permissions section. For example, when you enable edit permissions for fault management, Citrix Application Delivery and Management internally provides permission for configuring a mail profile or for creating SMTP server setups, so that the user can send the report as a mail.

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.



- ☑ StyleBooks
  - ☑ StyleBooks
    - ☑ View ☑ Import ☑ Delete ☑ Download
  - ☑ Configurations
    - ☑ View ☑ Create ☑ Modify ☑ Delete ☑ Upgrade ☑ Migrate from CLI ☑ Audit ☑ Import ☑ Export
  - ☑ Repositories
    - ☑ View ☑ Add ☑ Modify ☑ Delete ☑ Sync

Configure Roles on Citrix Application Delivery and Management

In Citrix Application Delivery and Management, 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 Citrix ADC instances in Citrix Application Delivery and Management, and the other policy might grant permission to create and deploy a StyleBook and to configure Citrix ADC instances.

When multiple policies define the edit and read-only permissions for a single feature, the edit permissions have priority over read-only permissions.

Citrix Application Delivery and Management provides five predefined roles:

- **admin_role**. Has access to all Citrix Application Delivery and Management features. (This role is bound to `adminpolicy`.)
- **adminExceptSystem_role**. Has access to the Citrix Application Delivery and Management GUI except for the Settings permissions. (This role is bound to adminExceptSystem_policy)
- **readonly_role**. Has read-only access. (This role is bound to `readonlypolicy`.)
- **appAdmin_role**. Has administrative access to only the application features in Citrix Application Delivery and Management. (This role is bound to appAdminPolicy).
- **appReadonly_role**. Has read-only access to the application features. (This role is bound to appReadOnlyPolicy.)

Though you cannot edit the predefined roles, you can create your own (user-defined) roles.

To create roles and assign policies to them:

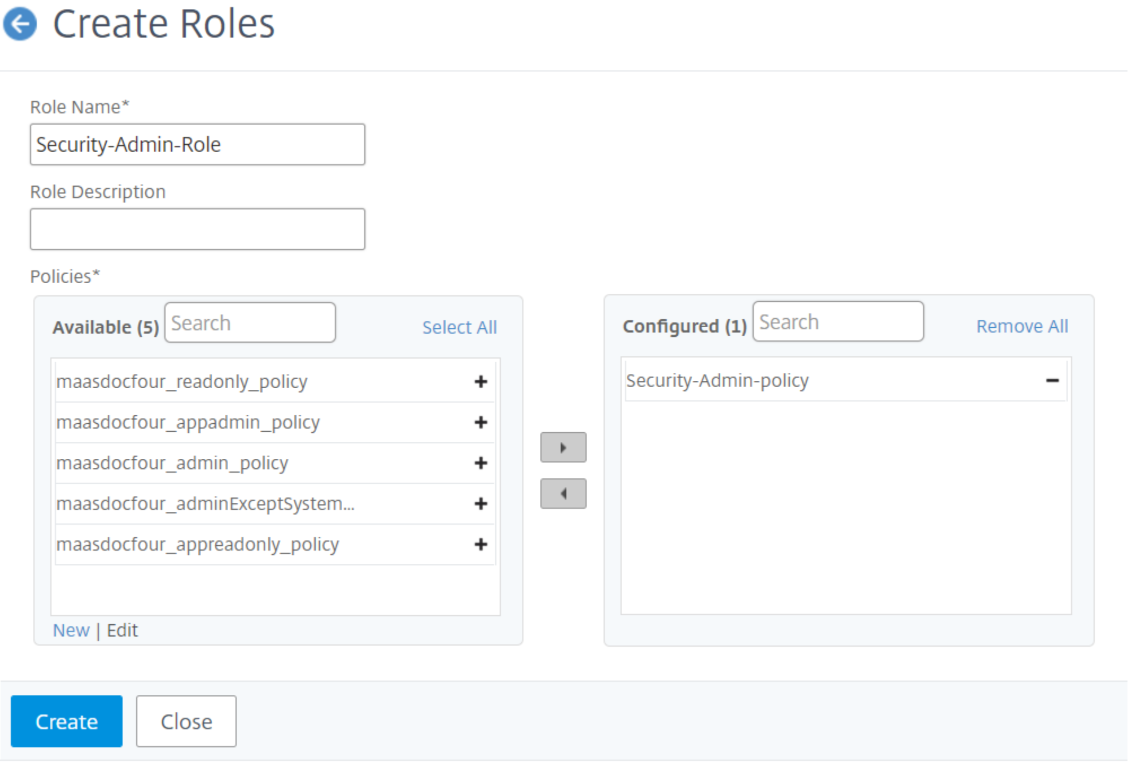
1. In the Citrix Application Delivery and Management GUI, navigate to **Settings** > **User Administration** > **Roles**.

2. Click **Add**.

3. On **Create Roles** page, 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 move one or more policies to the **Configured** list.

> **Note**
>
> The policies are pre-fixed with a tenant ID (for example, `maasdocfour`) that is unique to all tenants.



Create Roles

Role Name*: Security-Admin-Role

Role Description:

Policies*

Available (5)
- maasdocfour_readonly_policy +
- maasdocfour_appadmin_policy +
- maasdocfour_admin_policy +
- maasdocfour_adminExceptSystem... +
- maasdocfour_appreadonly_policy +

Configured (1)
- Security-Admin-policy −

> **Note**
>
> You can create an access policy by clicking **New**, or you can navigate to **Settings** > **User Administration** > **Access Policies,** and create policies.

5. Click **Create**.

Configure Groups on Citrix Application Delivery and Management

In Citrix Application Delivery and Management, a group can have both feature-level and resource-level access. For example, one group of users might have access to only selected Citrix ADC 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 Citrix Application Delivery and Management.

You can manage a user access in Citrix Application Delivery and Management at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.

Citrix Application Delivery and Management 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 Citrix Gateway (`vpn`)
- **Services** - Load balancing and GSLB services
- **Service Group** - Load balancing and GSLB Service groups
- **Servers** - Load balancing Servers

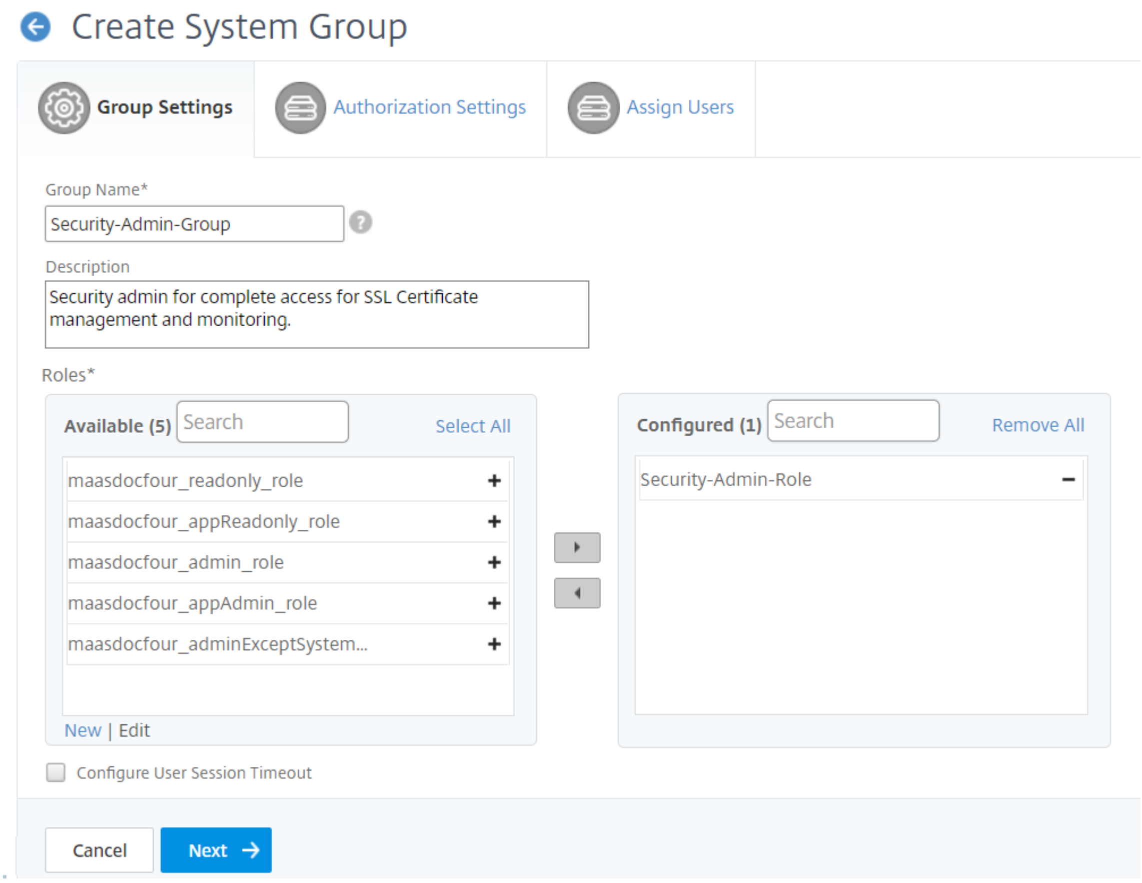
To create a group:

1. In Citrix Application Delivery and Management, navigate to **Settings** > **User Administration** > **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 helps you to understand the role and function of the group.
5. In the **Roles** section, move one or more roles to the **Configured** list.

   > **Note**
   >
   > The roles are pre-fixed with a tenant ID (for example, `maasdocfour`) that is unique to all tenants.
6. In the **Available** list, you can click **New** or **Edit** and create or modify roles.

   Alternatively, you can navigate to **Settings > User Administration > Users**, and create or modify users.



Group Name*

Security-Admin-Group

Description

Security admin for complete access for SSL Certificate management and monitoring.

Roles*

maasdocfour_readonly_role +

maasdocfour_appReadonly_role +

maasdocfour_admin_role +

maasdocfour_appAdmin_role +

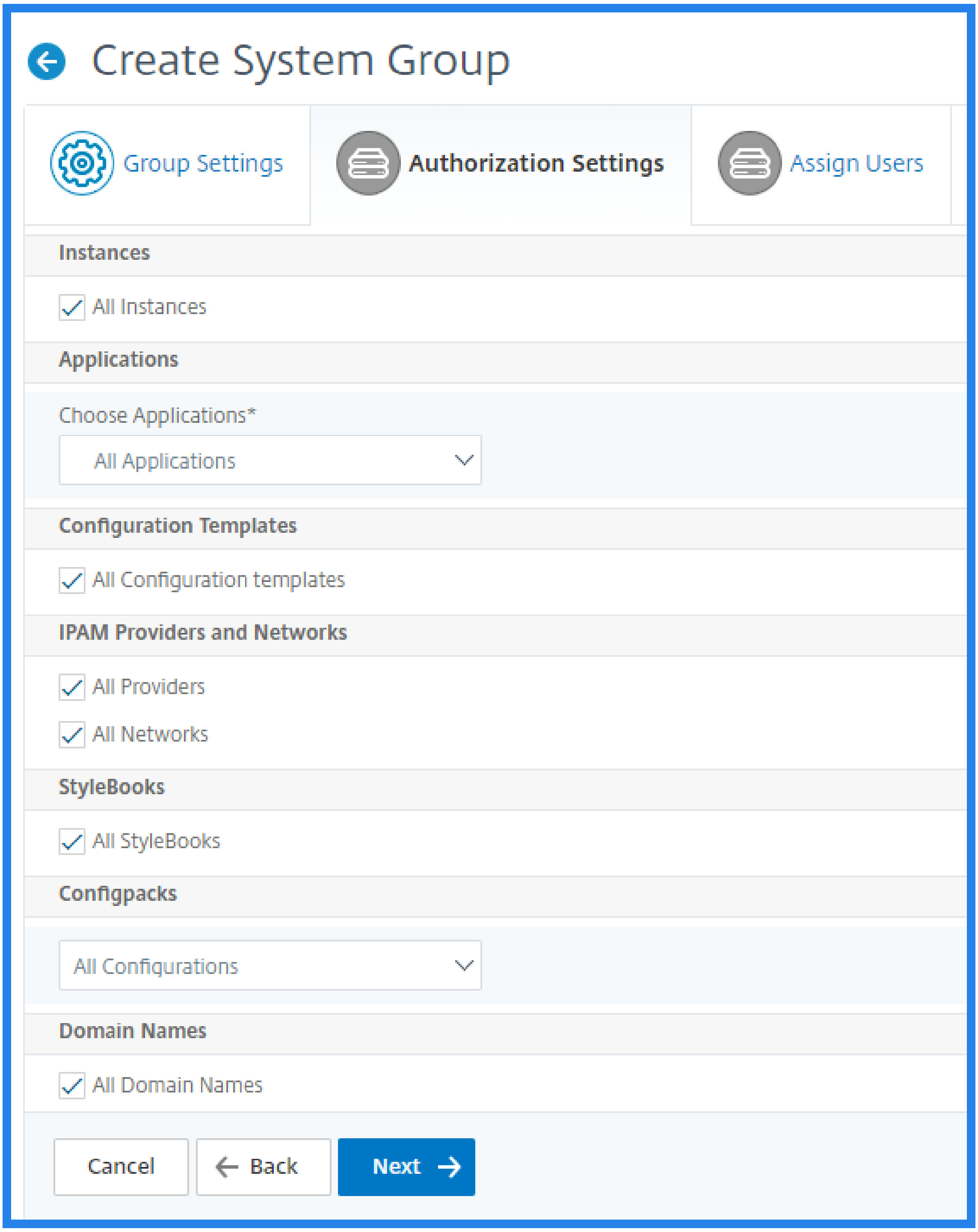
maasdocfour_adminExceptSystem... +

Security-Admin-Role −

□ Configure User Session Timeout

7. Click **Next**.
8. In the **Authorization Settings** tab, you can choose resources from the following categories:

   - **Autoscale Groups**
   - **Instances**
   - **Applications**
   - **Configuration Templates**
   - **IPAM Providers and Networks**
   - **StyleBooks**
   - **Configpacks**
   - **Domain Names**



Create System Group

Group Settings | **Authorization Settings** | Assign Users

Instances

☑ All Instances

Applications

Choose Applications*

All Applications

Configuration Templates

☑ All Configuration templates

IPAM Providers and Networks

☑ All Providers

☑ All Networks

StyleBooks

☑ All StyleBooks

Configpacks

All Configurations

Domain Names

☑ All 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 user can view or manage, perform the following steps:

a) Clear the **All AutoScale Groups** check box and click **Add AutoScale Groups**.

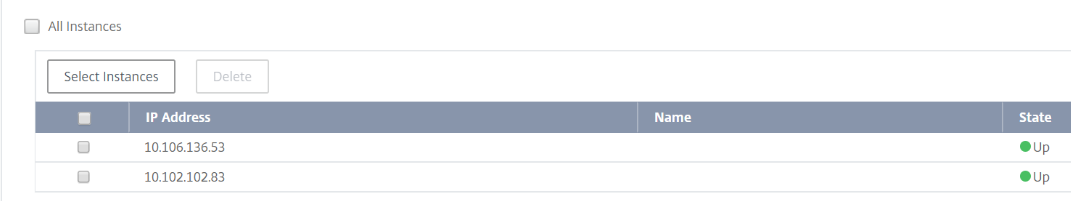
b) Select the required Autoscale groups from the list and click **OK**.

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**.



□ All Instances

Select Instances | Delete

□	IP Address	Name	State
□	10.106.136.53		● Up
□	10.102.102.83		● Up

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 Citrix Application Delivery and Management.
- **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 the 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** , Citrix Application Delivery and Management authorizes all the entities that are bound to the selected application.

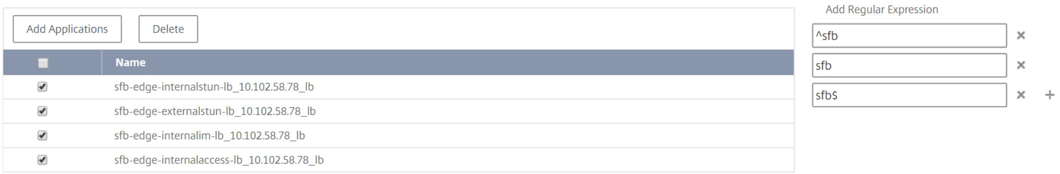
> **Note**
>
> Ensure you have selected only one entity type if you want to authorize bound entities.

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 Citrix Application Delivery and Management. 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:



☐	Name
☑	sfb-edge-internalstun-lb_10.102.58.78_lb
☑	sfb-edge-externalstun-lb_10.102.58.78_lb
☑	sfb-edge-internalim-lb_10.102.58.78_lb
☑	sfb-edge-internalaccess-lb_10.102.58.78_lb

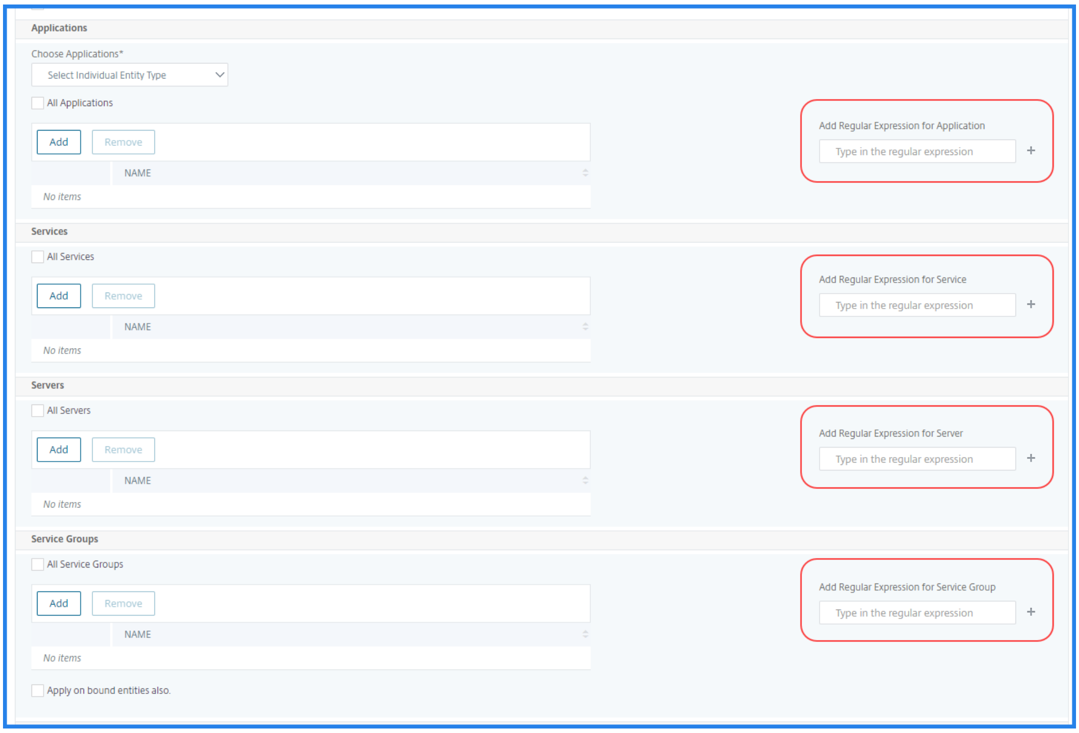
Add Regular Expression

^sfb ×

sfb ×

sfb$ × +

The following image explains how to use regular expression to add network function entities when you choose the **Select the Individual Entity Type** option:



Applications

Choose Applications*: Select Individual Entity Type

☐ All Applications

Add
Remove
NAME
No items
Add Regular Expression for Application
Type in the regular expression
+
Services
☐ All Services
Add
Remove
NAME
No items
Add Regular Expression for Service
Type in the regular expression
+
Servers
☐ All Servers
Add
Remove
NAME
No items
Add Regular Expression for Server
Type in the regular expression
+
Service Groups
☐ All Service Groups
Add
Remove
NAME
No items
Add Regular Expression for Service Group
Type in the regular expression
+

☐ Apply on bound entities also.

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.

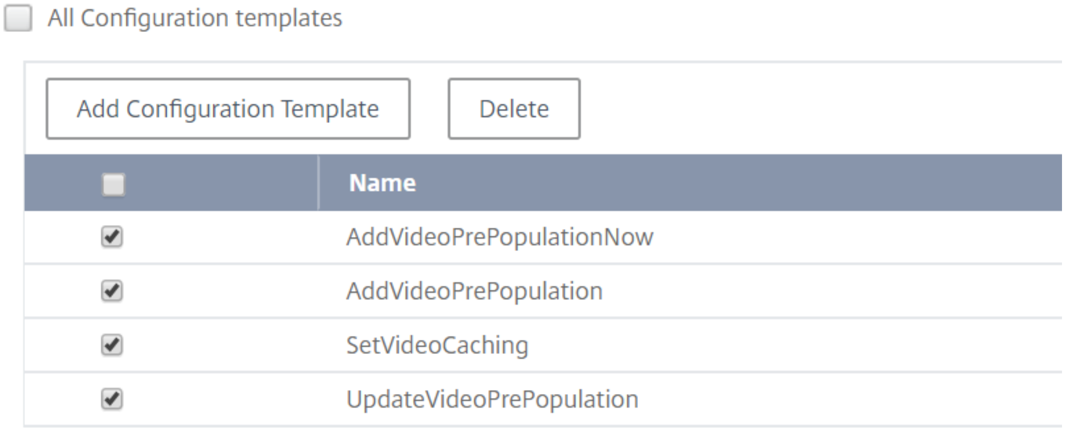
The regular expression is stored in the system to update the authorization scope. When the new entities match the regular expression of their entity type, Citrix Application Delivery and Management updates the authorization scope to the new entities.

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**.



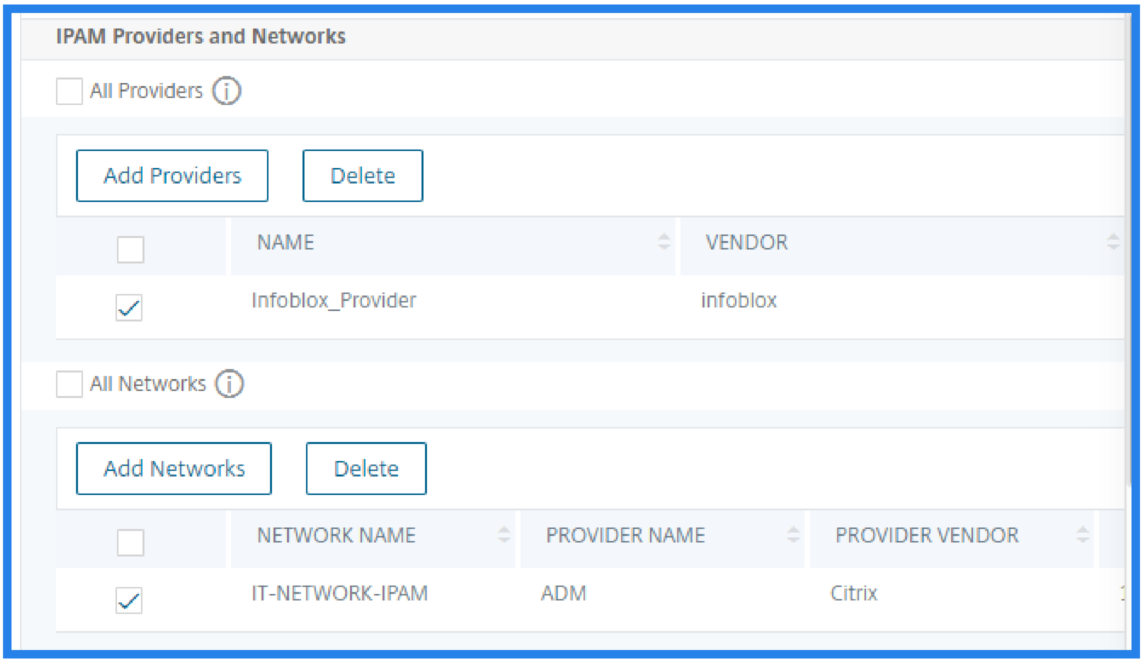
□ All Configuration templates

□	Name
☑	AddVideoPrePopulationNow
☑	AddVideoPrePopulation
☑	SetVideoCaching
☑	UpdateVideoPrePopulation

IPAM Providers and Networks:

If you want to add the specific IPAM providers and networks that a user can view or manage, perform the following:

- **Add providers** - Clear the **All Providers** check box and click **Add Providers**. You can select the required providers and click **OK**.
- **Add networks** - Clear the **All Networks** check box and click **Add Networks**. You can select the required networks and click **OK**.



IPAM Providers and Networks

□ All Providers

□	NAME	VENDOR
☑	Infoblox_Provider	infoblox

□ All Networks

□	NETWORK NAME	PROVIDER NAME	PROVIDER VENDOR
☑	IT-NETWORK-IPAM	ADM	Citrix

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:

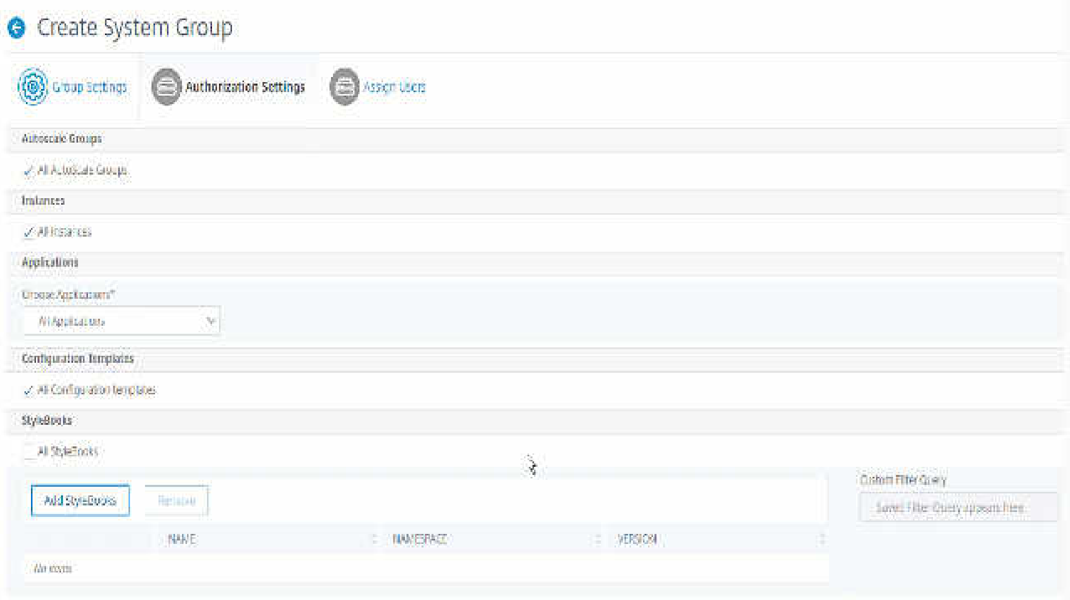
- StyleBook name is either `lb-mon` or `lb`.
- StyleBook namespace is `com.citrix.adc.stylebooks`.
- StyleBook version is `1.0`.

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**.



Autoscale Groups

✓ All Autoscale Groups

Instances

✓ All Instances

Applications

Choose Applications*

All Applications

Configuration Templates

✓ All Configuration templates

StyleBooks

□ All StyleBooks

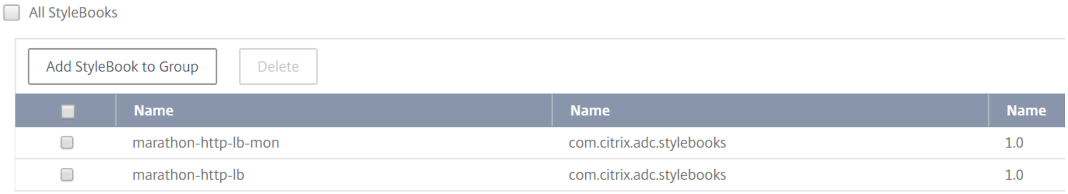
Custom Filter Query

Saved Filter Query appears here

NAME	NAMESPACE	VERSION
No items		

The saved query appears in the **Custom Filters Query**. Based on the saved query, the Citrix Application Delivery and Management provides user access to those StyleBooks.

b) Select the required StyleBooks from the list and click **OK**.



□ All StyleBooks

□	Name	Name	Name
□	marathon-http-lb-mon	com.citrix.adc.stylebooks	1.0
□	marathon-http-lb	com.citrix.adc.stylebooks	1.0

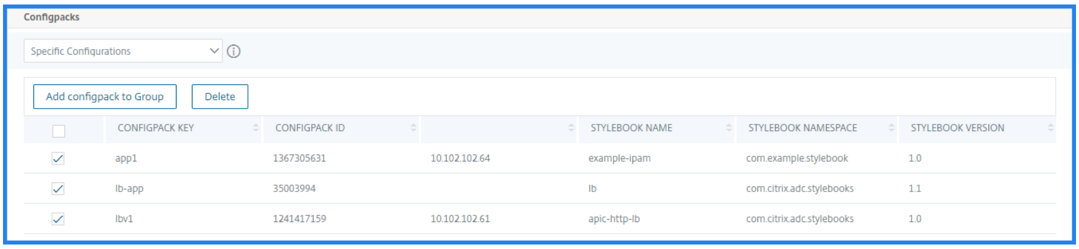
You can select the required StyleBooks when you create groups and add users to that group. When your user selects the permitted StyleBook, all dependent StyleBooks are also selected.

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 Citrix Application Delivery and Management.

- **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.



Configpacks

Specific Configurations

☐	CONFIGPACK KEY	CONFIGPACK ID		STYLEBOOK NAME	STYLEBOOK NAMESPACE	STYLEBOOK VERSION
☑	app1	1367305631	10.102.102.64	example-ipam	com.example.stylebook	1.0
☑	lb-app	35003994		lb	com.citrix.adc.stylebooks	1.1
☑	lbv1	1241417159	10.102.102.61	apic-http-lb	com.citrix.adc.stylebooks	1.0

You can select the required configuration packs when you create groups and add users to that group.

Domain Names:

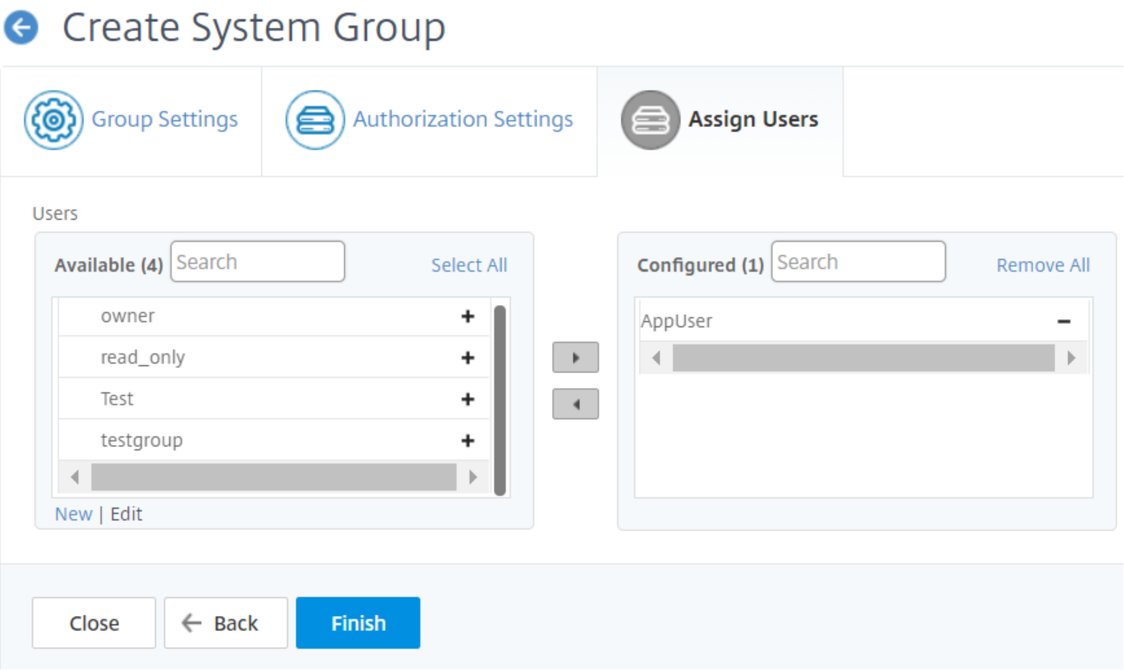
If you want to select the specific domain name that a user can view or manage, perform the following steps:

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**.

9. Click **Create Group**.
10. 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 new users by clicking **New**.



11. Click **Finish**.

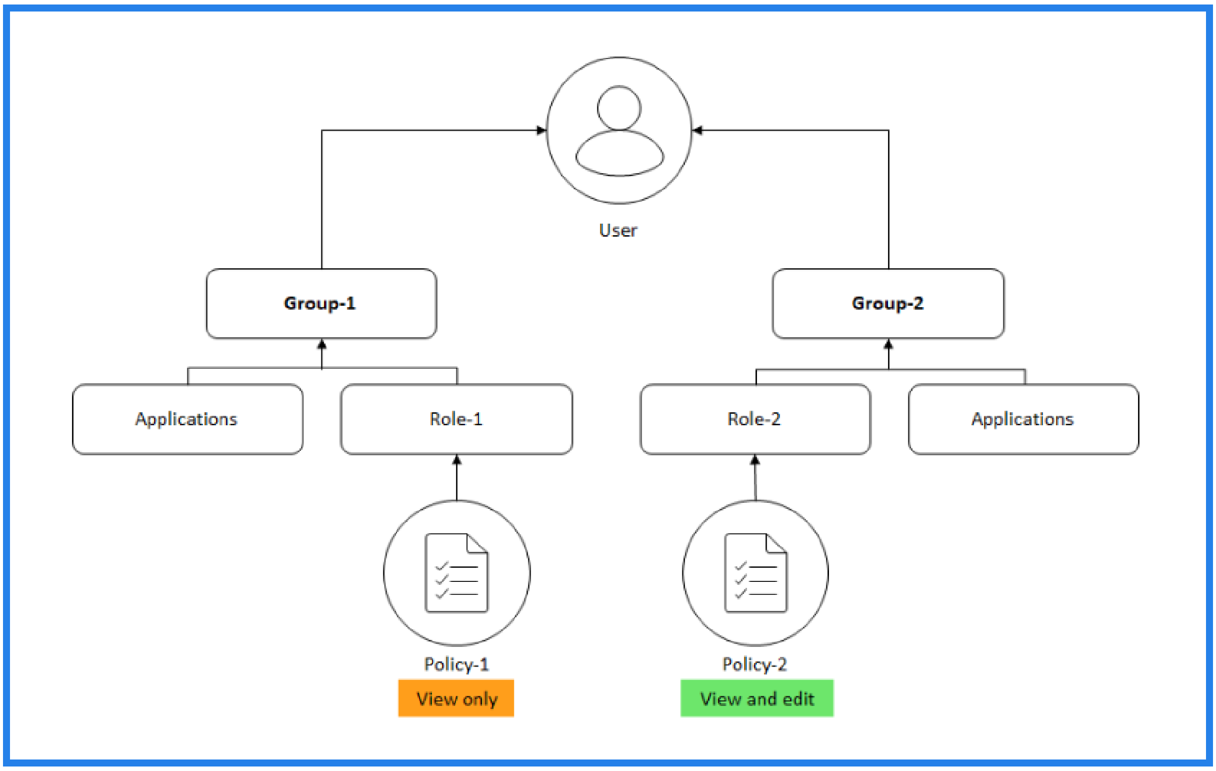
How user access changes based on the authorization scope

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 Citrix Application Delivery and Management 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.

Limitations

RBAC is not fully supported by the following Citrix Application Delivery and Management features:

- Analytics - RBAC is not supported fully by the analytics modules. RBAC support is limited to an instance level, and it is not applicable at the application level in the Gateway Insight, HDX Insight, and Security Insight analytics modules.
    - Example 1: Instance-based RBAC (Supported). An administrator who has been assigned a few instances can see only those instances under **HDX Insight** > **Devices**, and only the corresponding virtual servers under **HDX Insight** > **Applications** because RBAC is supported at the instance level.
    - Example 2: Application based RBAC (Not Supported). An administrator who has been assigned a few applications can see all virtual servers under **HDX Insight** > **Applications** but cannot access them, because RBAC is not supported at the applications level.
- StyleBooks – RBAC is not fully supported for StyleBooks.
    - Consider a situation where multiple users have access to a single StyleBook but have access permissions for different Citrix ADC instances. Users can create and update config packs on their own instances, but not on other instances as they do not have access to

those instances other than their own. But they can still view the config packs and objects created on Citrix ADC instances other than their own.

Configuring Analytics settings

September 24, 2021

Before you start using the Analytics feature on Citrix Application Delivery and Management to gain visibility into your instance and application data, it is recommended that you configure a few analytics settings to ensure optimal experience with this feature.

Creating Thresholds and Alerts for Analytics

You can set thresholds and alerts to monitor the analytics' metrics of the managed virtual servers configured on the discovered instances. When the value of a metric exceeds the threshold, Citrix Application Delivery and Management generates an event to signify a threshold breach.

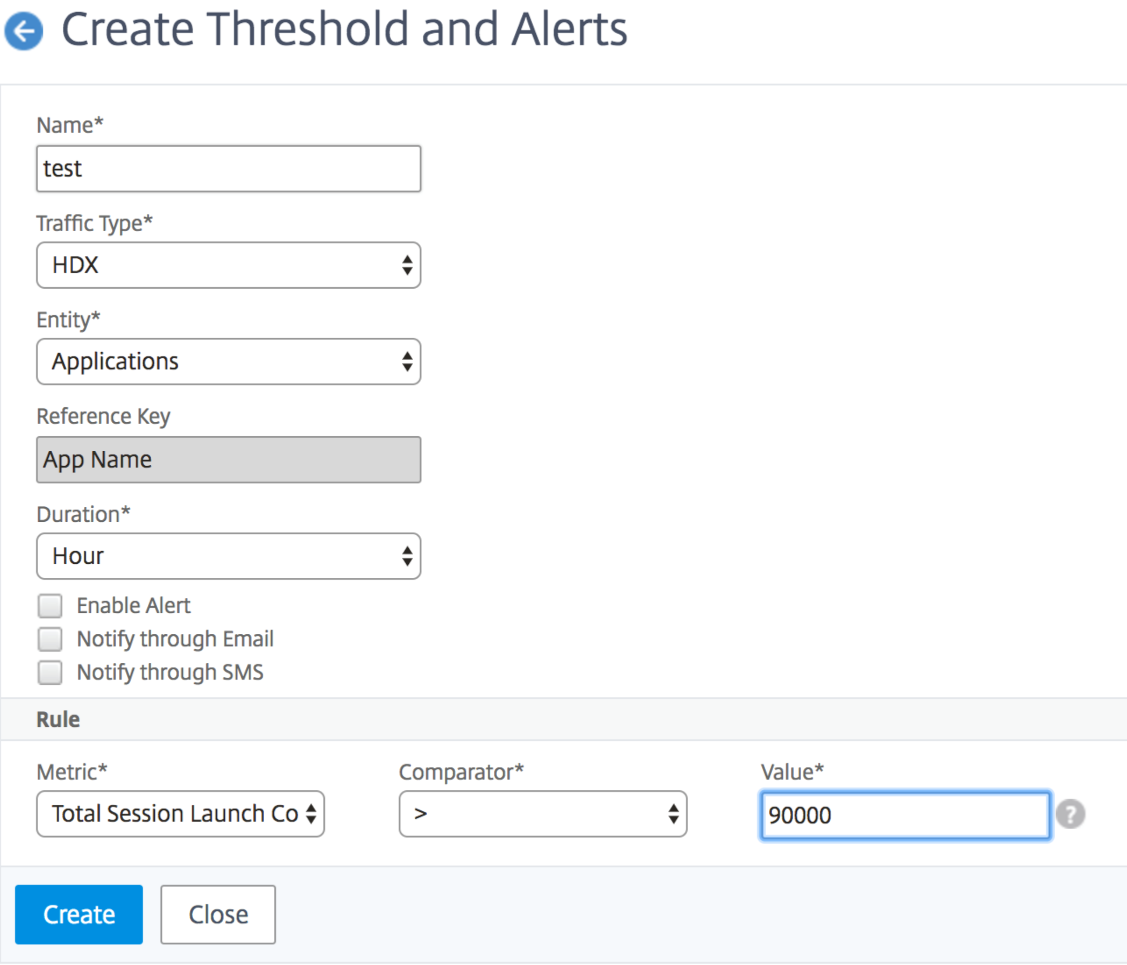
You can also associate actions with the set thresholds. Actions include displaying an alert on the GUI, sending Email as configured.

For example, you can set a threshold to generate an event for HDX insight if any user's ICA RTT value exceeds 1 second. You can also enable alerts for the generated event, and send the threshold breach information to a configured Email list.

To create thresholds and alerts for analytics:

1. Navigate to **Settings** > **Analytics Settings** > **Thresholds**.
2. On the **Thresholds** screen, click **Add** to add a new threshold and configure alerts for the set thresholds.
3. On the **Create Thresholds and Alerts** page, specify the following details:
   - **Name** – Name for configuring the threshold.
   - **Traffic Type** – Type of analytics traffic for which you want to configure the threshold. For example: HDX Insight, Security Insight.
   - **Entity** – Category or resource type for which you want to configure the threshold.
   - **Reference Key** – Automatically generated value based on the selected traffic type and entity.
   - **Duration** - Interval for which you want to configure the threshold.
4. To configure email notifications, select the check box for the set thresholds.

5. In the **Rules** section, specify the following:
   - **Metric** – Metric for the selected Traffic type to configure the threshold.
   - **Comparator** – Comparator to the selected metric (for example: <, >=).
   - **Value** – Value for the metric to set the threshold, and invoke alerts.
6. Click **Create**.



Create Threshold and Alerts

Name*: test

Traffic Type*: HDX

Entity*: Applications

Reference Key: App Name

Duration*: Hour

□ Enable Alert

□ Notify through Email

□ Notify through SMS

Rule

Metric*: Total Session Launch Co

Comparator*: >

Value*: 90000

Configure notifications

September 25, 2021

You can select a notification type to receive notifications for the following features:

- **Events** – List of events that are generated for Citrix ADC 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 Citrix Application Delivery and Management license expiry.
- **SSL Certificates** – List of SSL certificates that are added to Citrix ADC instances. For more information, see The SSL certificate expiry

Citrix Application Delivery and Management supports the following notification types:

- Email
- SMS
- Slack
- PagerDuty
- ServiceNow

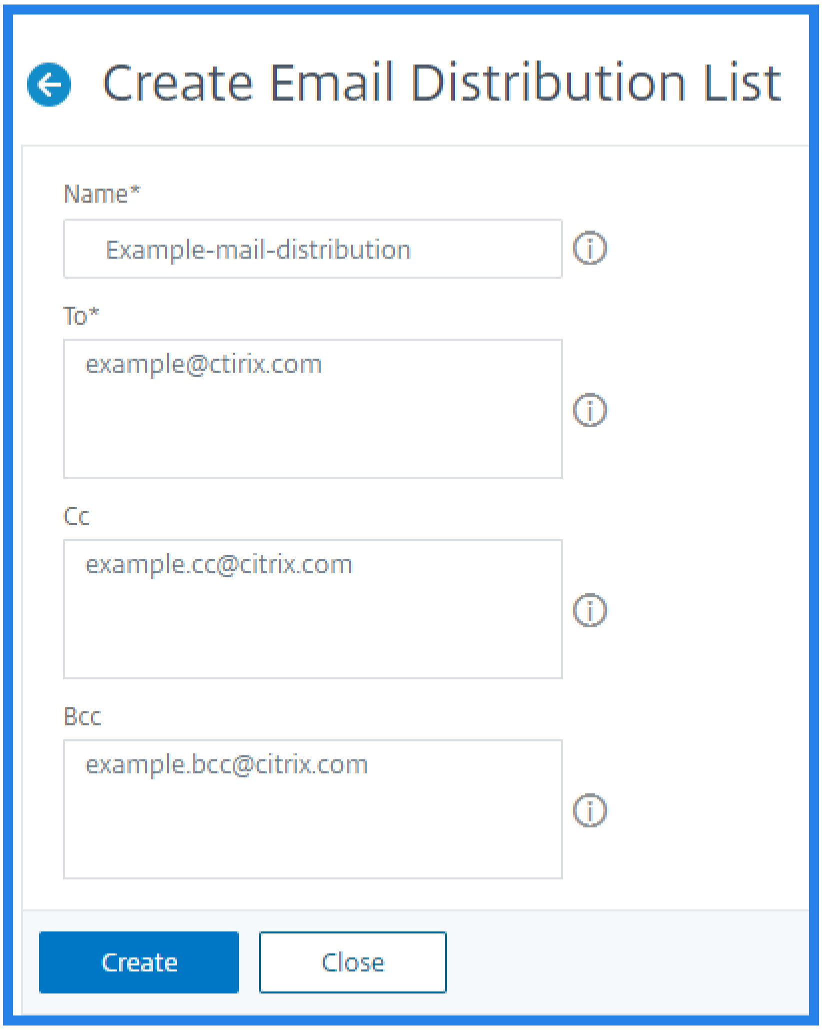
For each notification type, the Citrix Application Delivery and Management GUI displays the configured distribution list or profile. The Citrix Application Delivery and Management sends notifications to the selected distribution list or profile.

Create an email distribution list

To receive email notifications for Citrix Application Delivery and Management 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.
    - **To** - Specify the email addresses to which Citrix Application Delivery and Management has to send messages.
    - **Cc** - Specify the email addresses to which Citrix Application Delivery and Management has to send message copies.
    - **Bcc** - Specify the email addresses to which Citrix Application Delivery and Management has to send message copies without displaying the addresses.



Create Email Distribution List

Name*: Example-mail-distribution

To*: example@ctirix.com

Cc: example.cc@citrix.com

Bcc: example.bcc@citrix.com

4. Click **Create**.

Repeat this procedure to create multiple email distribution lists. The **Email** tab displays all the email distribution lists present in Citrix Application Delivery and Management.

Create an SMS distribution list

To receive SMS notifications for Citrix Application Delivery and Management 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 Citrix Application Delivery and Management has to send messages.

4. Click **Create**.

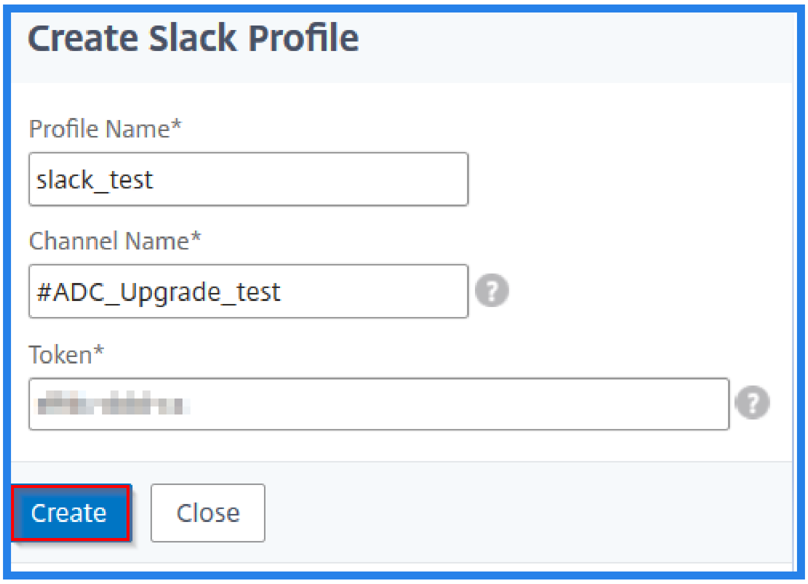
Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in Citrix Application Delivery and Management.

Create a Slack profile

To receive Slack notifications for Citrix Application Delivery and Management 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 Citrix Application Delivery and Management 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 a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



Create Slack Profile

Profile Name*: slack_test

Channel Name*: #ADC_Upgrade_test

Token*: [redacted]

4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in Citrix Application Delivery and Management.

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 Citrix Application Delivery and Management, 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 Citrix Application Delivery and Management.

View the ServiceNow profile

When you want to enable ServiceNow notifications for Citrix ADC events and Citrix Application Delivery and Management events, you must integrate Citrix Application Delivery and Management with the ServiceNow using ITSM connector. For more information, see Integrate Citrix Application Delivery and Management 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 Citrix Application Delivery and Management GUI, select **ServiceNow Tickets**.

Export or schedule export reports

October 20, 2021

In Citrix Application Delivery and Management, you can export a comprehensive report for the selected Citrix Application Delivery and Management feature. This report provides you an overview of the mapping between the instances, partitions, and corresponding details.

Citrix Application Delivery and Management displays feature-specific scheduled export reports under individual Citrix Application Delivery and Management features, which you can view, edit, or delete. For example, to view the export reports of Citrix ADC instances, navigate to **Infrastructure > Instances > Citrix ADC** and click the export icon. You can export these reports in PDF, JPEG, PNG, and CSV file format.

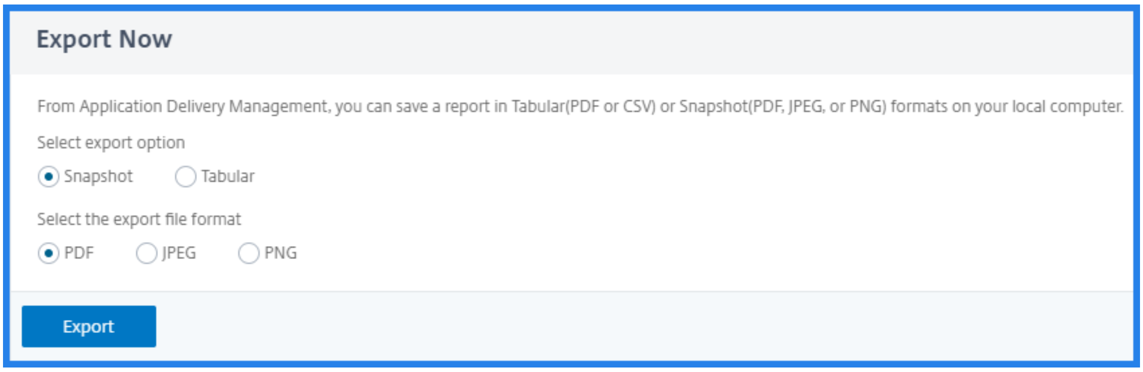
In **Export Reports**, you can perform the following actions:

- 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 Citrix Application Delivery and Management 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 Citrix Application Delivery and Management reports as a snapshot.
   - **Tabular** - This option export Citrix Application Delivery and Management reports in a tabular format. You can also choose how many data records to export in a tabular format



Export Now

From Application Delivery Management, you can save a report in Tabular(PDF or CSV) or Snapshot(PDF, JPEG, or PNG) formats on your local computer.

Select export option

● Snapshot ○ Tabular

Select the export file format

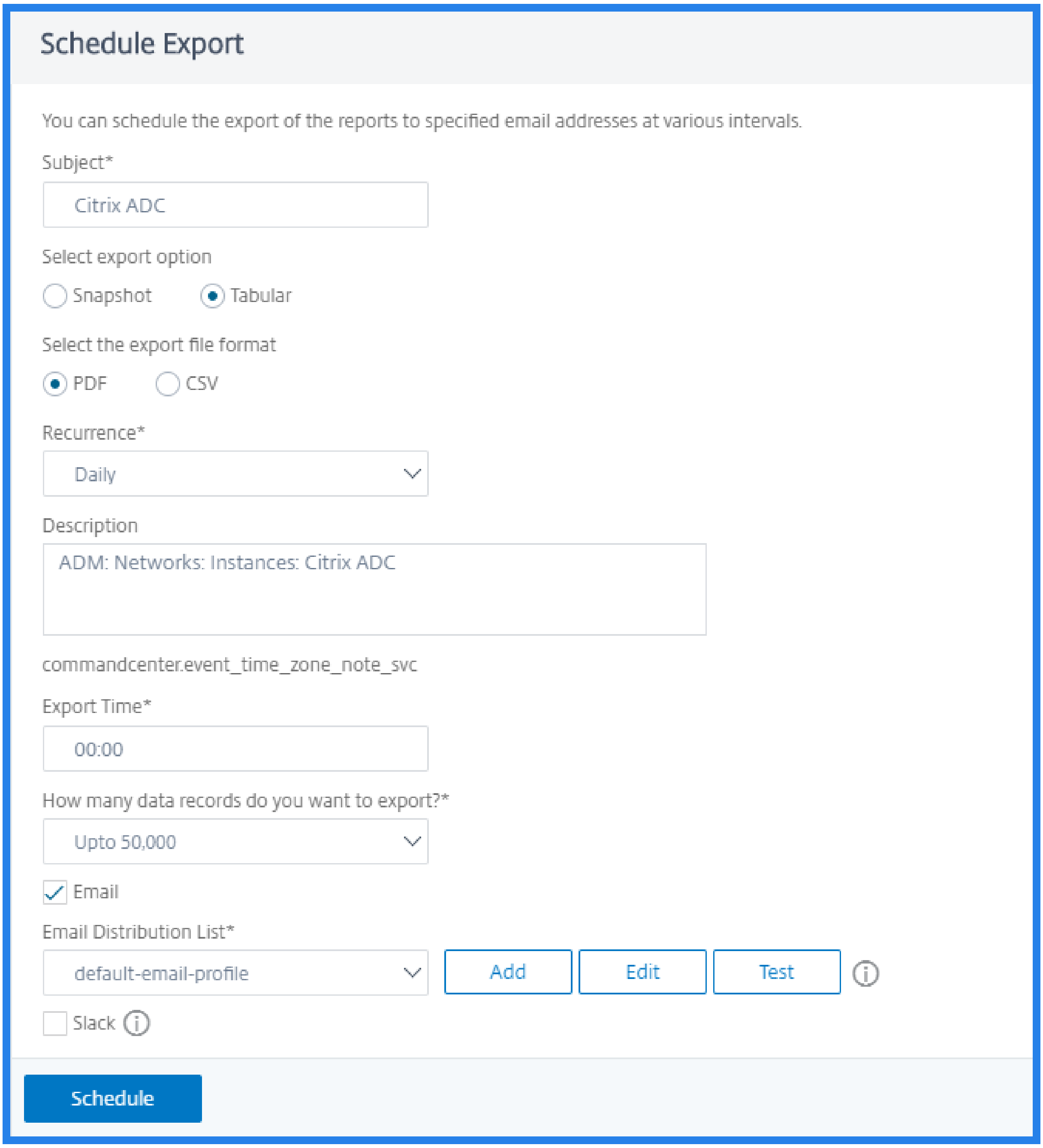
● PDF ○ JPEG ○ PNG

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. Citrix Application Delivery and Management 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 Citrix Application Delivery and Management 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**.



Schedule Export

You can schedule the export of the reports to specified email addresses at various intervals.

Subject*: Citrix ADC

Select export option: ○ Snapshot ● Tabular

Select the export file format: ● PDF ○ CSV

Recurrence*: Daily

Description: ADM: Networks: Instances: Citrix ADC

commandcenter.event_time_zone_note_svc

Export Time*: 00:00

How many data records do you want to export?*: Upto 50,000

☑ Email

Email Distribution List*: default-email-profile

□ Slack

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**.

Instance settings

September 25, 2021

You can manage the discovered instances in Citrix Application Delivery and Management and configure the instance backup settings.

Manage the instance configuration

In **Instance Management**, you can modify the following instance configurations:

- **Communication with instance(s)** - You can choose HTTP or HTTPS communication channel between Citrix Application Delivery and Management and the discovered instances.
- **Enable Certificate Download** - Allows you to download the SSL certificates from a discovered instance.
- **Prompt Credentials for Instance Login** - When you access the instance through the Citrix Application Delivery and Management GUI, the instance login page appears. Specify your login credentials to access an instance.

Configure instance backup settings

In **Instance Backup Settings**, you can configure the backup settings for the discovered ADC instances in Citrix Application Delivery and Management.

In **Configure Instance Backup Settings**, select **Enable Instance Backups**.

- **Backup Security Settings** - Encrypt the backup file to ensure all the sensitive information inside the backup file is secure. Select **Password Protect file** to encrypt the backup file.

  > **Note**
  >
  > When you download the encrypted backup file, the file does not open in the Citrix Application Delivery and Management GUI or in any text editor. This file can be retrieved and used by Citrix Application Delivery and Management only. However, you can open an unencrypted backup file on your system.
  >
  > To restore the encrypted backup file, specify the password that you have mentioned to encrypt the backup file.

- **Backup Scheduling Settings**- You can schedule an instance backup in two ways:
  - **Interval Based** - A backup file is created in Citrix Application Delivery and Management after the specified interval elapses. The default backup interval is 12 hours.

  - **Time Based** - Specify the time in `hours:minutes` format at which you want Citrix Application Delivery and Management to take the instance backup.

- **Citrix ADC settings** - With this option, you can initiate backup based on the trap and to include GeoDB files with the backup. This setting applies to MPX,VPX,CPX, and BLX instances.

  - **Do instance backup when NetScalerConfigSave trap is received** - By default, Citrix Application Delivery and Management 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 Citrix ADC instance sends a `NetScalerConfigSave` trap to Citrix Application Delivery and Management.

    A Citrix ADC instance sends `NetScalerConfigSave` every time the configuration on the instance is saved.

    Specify **Backup on trap delay** in minutes. If the received `NetScalerConfigSave` trap persist for the specified minutes on Citrix Application Delivery and Management, Citrix Application Delivery and Management backs up the instance.

  - **Include GeoDB files** - By default, Citrix Application Delivery and Management does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.

- **Citrix SDX Settings** - To back up SDX instances, specify **Backup Timeout** in minutes. During an SDX instance backup, the connection between Citrix Application Delivery and Management and SDX is maintained for the specified period.

  If the SDX instance backup file size is big, you might want to maintain the connection between Citrix Application Delivery and Management and SDX instance for a longer period to complete the SDX instance backup.

  > **Important**
  >
  > The backup fails if the connection times out.

- **External Transfer** - Citrix Application Delivery and Management allows you to transfer the Citrix ADC instance backup files to an external location:

  1. Specify the IP address of the location.
  2. Specify the user name and the password of the external server to which you want to transfer the backup files.
  3. Specify the transfer protocol and the port number.
  4. Specify the directory path where the file must be stored.
  5. If you want to delete the backup file after you transfer the file to an external server, select **Delete file from Application Delivery Management after transfer**.

Instance settings

September 25, 2021

You can manage the discovered instances in Citrix Application Delivery and Management and configure the instance backup settings.

Manage the instance configuration

In **Instance Management**, you can modify the following instance configurations:

- **Communication with instance(s)** - You can choose HTTP or HTTPS communication channel between Citrix Application Delivery and Management and the discovered instances.
- **Enable Certificate Download** - Allows you to download the SSL certificates from a discovered instance.
- **Prompt Credentials for Instance Login** - When you access the instance through the Citrix Application Delivery and Management GUI, the instance login page appears. Specify your login credentials to access an instance.

Configure instance backup settings

In **Instance Backup Settings**, you can configure the backup settings for the discovered ADC instances in Citrix Application Delivery and Management.

In **Configure Instance Backup Settings**, select **Enable Instance Backups**.

- **Backup Security Settings** - Encrypt the backup file to ensure all the sensitive information inside the backup file is secure. Select **Password Protect file** to encrypt the backup file.

  > **Note**
  >
  > When you download the encrypted backup file, the file does not open in the Citrix Application Delivery and Management GUI or in any text editor. This file can be retrieved and used by Citrix Application Delivery and Management only. However, you can open an unencrypted backup file on your system.
  >
  > To restore the encrypted backup file, specify the password that you have mentioned to encrypt the backup file.

- **Backup Scheduling Settings**- You can schedule an instance backup in two ways:
  - **Interval Based** - A backup file is created in Citrix Application Delivery and Management after the specified interval elapses. The default backup interval is 12 hours.

- **Time Based** - Specify the time in `hours:minutes` format at which you want Citrix Application Delivery and Management to take the instance backup.

- **Citrix ADC settings** - With this option, you can initiate backup based on the trap and to include GeoDB files with the backup. This setting applies to MPX,VPX,CPX, and BLX instances.

  - **Do instance backup when NetScalerConfigSave trap is received** - By default, Citrix Application Delivery and Management 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 Citrix ADC instance sends a `NetScalerConfigSave` trap to Citrix Application Delivery and Management.

    A Citrix ADC instance sends `NetScalerConfigSave` every time the configuration on the instance is saved.

    Specify **Backup on trap delay** in minutes. If the received `NetScalerConfigSave` trap persist for the specified minutes on Citrix Application Delivery and Management, Citrix Application Delivery and Management backs up the instance.

  - **Include GeoDB files** - By default, Citrix Application Delivery and Management does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.

- **Citrix SDX Settings** - To back up SDX instances, specify **Backup Timeout** in minutes. During an SDX instance backup, the connection between Citrix Application Delivery and Management and SDX is maintained for the specified period.

  If the SDX instance backup file size is big, you might want to maintain the connection between Citrix Application Delivery and Management and SDX instance for a longer period to complete the SDX instance backup.

  > **Important**
  >
  > The backup fails if the connection times out.

- **External Transfer** - Citrix Application Delivery and Management allows you to transfer the Citrix ADC instance backup files to an external location:

  1. Specify the IP address of the location.
  2. Specify the user name and the password of the external server to which you want to transfer the backup files.
  3. Specify the transfer protocol and the port number.
  4. Specify the directory path where the file must be stored.
  5. If you want to delete the backup file after you transfer the file to an external server, select **Delete file from Application Delivery Management after transfer**.

System configurations

September 24, 2021

You can modify the Citrix Application Delivery and Management agent's keep-alive interval and the Citrix Application Delivery and Management server timezone.

Set agent's keep-alive interval

Citrix Application Delivery and Management 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 Citrix Application Delivery and Management server.

1. Navigate to **Settings > System Settings**.
2. Select **Agent and Timezone** under **System Configurations**.
3. In **Agent**, specify the keep-alive interval between 30–120 seconds.
4. Click **Save**.

Set the Citrix Application Delivery and Management time zone

You can choose the timezone in which you want to display the time on the Citrix Application Delivery and Management webpage, notifications, and reports.

1. Navigate to **Settings > System Settings**.
2. Select **Agent and Timezone** under **System Configurations**.
3. In **Time zone**, select local or GMT time zone to display time in Citrix Application Delivery and Management.
4. Click **Save**.

Enable or disable features

October 20, 2021

As an administrator, you can enable or disable the following features in the **Settings > Global Settings > 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 Citrix Application Delivery and Management redistributes the ADC instances of the inactive agent with other active agents. For more information, see Configure Citrix Application Delivery and Management 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, Citrix Application Delivery and Management automatically polls configured network function entities every 60 minutes. For more information, see Polling overview.
- **Instance backup** - Back up the current state of a Citrix ADC 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 Citrix ADC instances.
- **Instance configuration audit** - Monitor configuration changes across managed Citrix ADC 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 Citrix ADC instance. Events received in Citrix Application Delivery and Management 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** - Citrix Application Delivery and Management provides a centralized view of SSL certificates installed across all managed Citrix ADC instances. For more information, see SSL Dashboard.
- **Instance Syslog** - You can monitor the syslog events generated on your Citrix ADC instances if you have configured your device to redirect all syslog messages to Citrix Application Delivery and Management. For more information, see Configuring syslog on instances.

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.

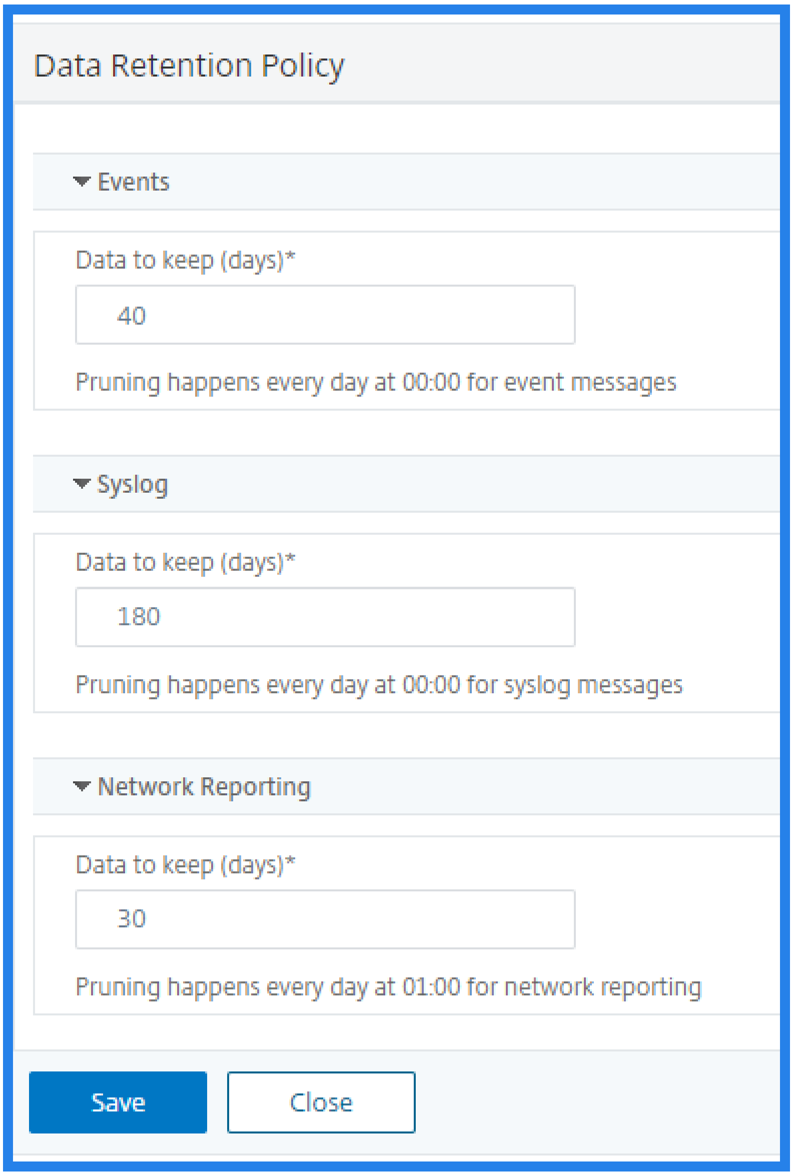
Data retention policy

September 25, 2021

You can access system events, syslog messages, and network reporting data for a specific duration in Citrix Application Delivery and Management.

1. Navigate to **Settings > Global Settings > Data Retention Policy** to configure the data retention.
2. Click the edit button.
3. Specify days to the following options to retain data in Citrix Application Delivery and Management:

Options	Description
Events	Enables you to limit the event messages stored in Citrix Application Delivery and Management up to 40 days. The events are deleted from Citrix Application Delivery and Management after the retention policy is expired. The cleared events are deleted after one day. For more information, see Events.
Syslog	Enables you to limit the amount of syslog data stored in the database up to 180 days. For more information, see Configure syslog on instances.
Network Reporting	Enables you to limit the network reporting data stored in Citrix Application Delivery and Management up to 30 days. For more information, see Network Reporting.



Data Retention Policy

▾ Events

Data to keep (days)*: 40

Pruning happens every day at 00:00 for event messages

▾ Syslog

Data to keep (days)*: 180

Pruning happens every day at 00:00 for syslog messages

▾ Network Reporting

Data to keep (days)*: 30

Pruning happens every day at 01:00 for network reporting

> **Important**
>
> You cannot edit the data retention policy with an Express account.
>
> When your account is converted to an Express account, the Citrix Application Delivery and Management retains the storage data up to 500 MB or one day data, whichever is the lesser. For more information, see Manage Citrix Application Delivery and Management resources using Express account.

Use audit logs for managing and monitoring your infrastructure

October 20, 2021

You can use the Citrix Application Delivery and Management to track all events on Citrix Application Delivery and Management and syslog events generated on Citrix Application Delivery and Management 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 Citrix Application Delivery and Management simplifies the way of reviewing log messages.

You can use filters to search Citrix Application Delivery and Management 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 Citrix Application Delivery and Management GUI:

- ADC instance related audit logs
- Citrix Application Delivery and Management related audit logs
- Application audit logs

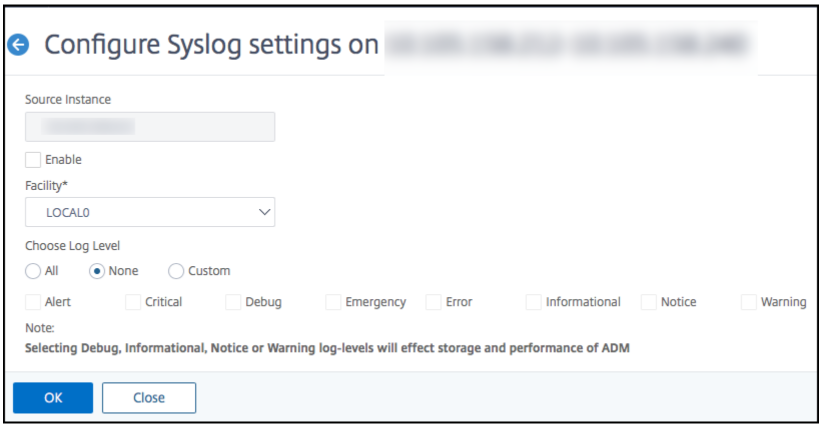
ADC instance related audit logs

Before you can view ADC instance-related syslog messages from Citrix Application Delivery and Management, configure the Citrix Application Delivery and Management as the syslog server for your Citrix ADC instance. After the configuration is complete, all syslog messages are redirected from the instance to Citrix Application Delivery and Management.

Configure Citrix Application Delivery and Management as a syslog server

Follow these steps to configure Citrix Application Delivery and Management as the syslog server:

1. From the Citrix Application Delivery and Management GUI, navigate to **Infrastructure > Instances**.
2. Select the Citrix ADC instance from which you want the syslog messages to be collected and displayed in Citrix Application Delivery and Management.
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**.



Configure Syslog settings on [redacted]

Source Instance

[redacted]

□ Enable

Facility*

LOCAL0

Choose Log Level

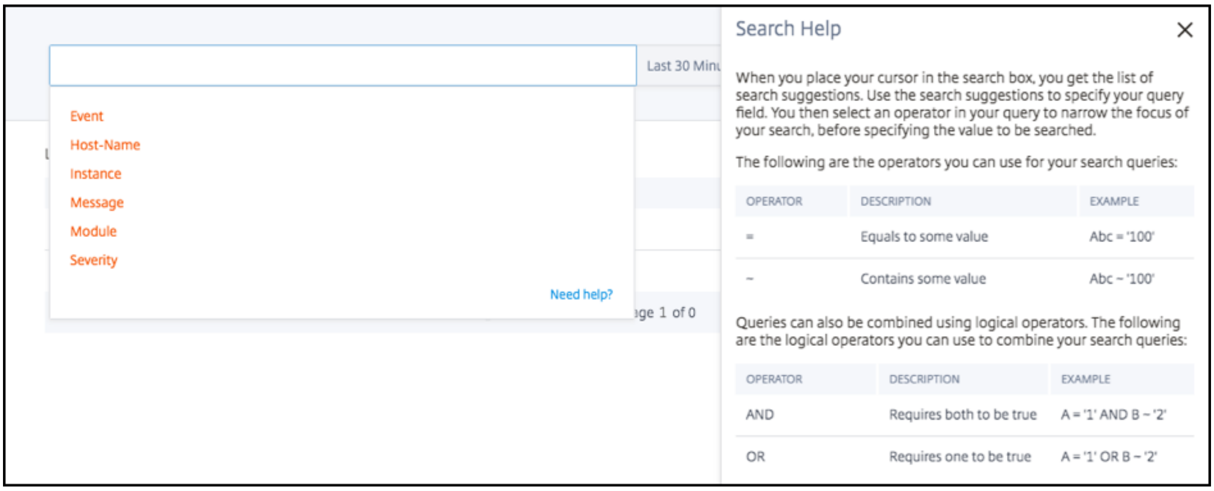
○ All ● None ○ Custom

□ Alert □ Critical □ Debug □ Emergency □ Error □ Informational □ Notice □ Warning

Note:

Selecting Debug, Informational, Notice or Warning log-levels will effect storage and performance of ADM

These steps configure all the syslog commands in the Citrix ADC instance, and Citrix Application Delivery and Management 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.



Search Help

When you place your cursor in the search box, you get the list of search suggestions. Use the search suggestions to specify your query field. You then select an operator in your query to narrow the focus of your search, before specifying the value to be searched.

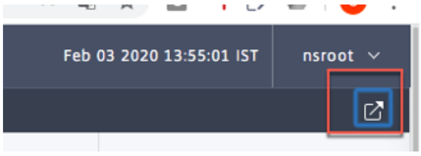
The following are the operators you can use for your search queries:

OPERATOR	DESCRIPTION	EXAMPLE
=	Equals to some value	Abc = '100'
~	Contains some value	Abc ~ '100'

Queries can also be combined using logical operators. The following are the logical operators you can use to combine your search queries:

OPERATOR	DESCRIPTION	EXAMPLE
AND	Requires both to be true	A = '1' AND B ~ '2'
OR	Requires one to be true	A = '1' OR B ~ '2'

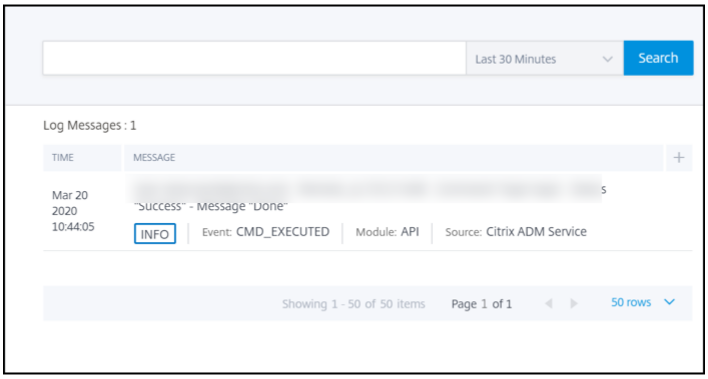
To export the log messages, click the arrow icon on the upper right corner.



Next, click **Export Now** or **Schedule Export**. For more information, see Export syslog messages.

Citrix Application Delivery and Management related audit logs

Based on preconfigured rules, Citrix Application Delivery and Management 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 Citrix Application Delivery and Management, navigate to **Settings->Audit Log Messages**.



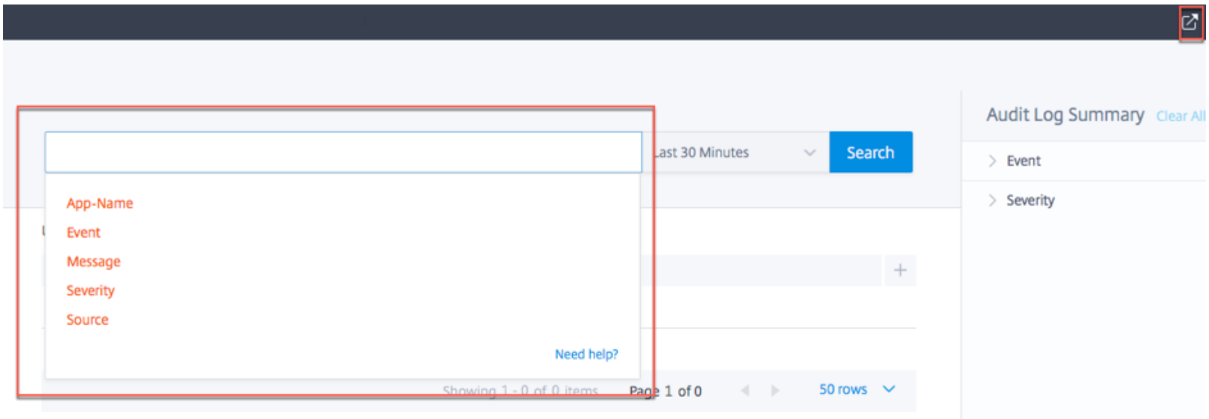
Mar 20 2020 10:44:05 [redacted] "Success" - Message "Done"
INFO | Event: CMD_EXECUTED | Module: API | Source: Citrix ADM Service

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 Citrix Application Delivery and Management applications or for a specific application.

- To view all audit log messages for all applications present in the Citrix Application Delivery and Management, navigate to **Infrastructure > Network Functions > Auditing**.



- To view audit log messages for any specific application in the Citrix Application Delivery and Management, navigate to **Applications > Dashboard > double-click the virtual server > Audit Log**.

> Note
>
> You can forward Citrix Application Delivery and Management audit log messages to an external server. For details, see View auditing information.

Configure IP address management (IPAM)

September 24, 2021

Citrix Application Delivery and Management IPAM provides you an ability to auto-assign and release IP addresses in Citrix Application Delivery and Management managed configurations. You can assign IPs from networks or IP ranges defined using the following IP providers:

- Citrix Application Delivery and Management built-in IPAM provider.
- Infoblox IPAM solution. For more information, see Infoblox DDI.

Currently, you can use Citrix Application Delivery and Management 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.
- **API gateway**: Auto-allocate an IP address to the API proxy.

You can also track the allocated and available IP addresses in each network or IP range managed by Citrix Application Delivery and Management.

Add an external IP address provider

Citrix Application Delivery and Management has a built-in IPAM provider to manage IPs and IP ranges. You can also add an external IP address provider to Citrix Application Delivery and Management.

> **Important**
>
> Before you begin, ensure that the following permissions are enabled in the external IP address provider:
>
> - Ability to query networks that are present in the provider.
> - Register a new network.
> - Unregister an existing network.
> - Reserve an IP address in the network.
> - Free an IP address from the network.
> - Retrieve the used IP addresses from a network.
> - Retrieve available IP addresses from a network.

Perform the following steps to add an external IP provider solution in Citrix Application Delivery and Management:

1. Navigate to **Settings > 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 Citrix Application Delivery and Management.
- **Vendor** - Select an IPAM vendor from the list.
- **URL** - Specify the URL of the IPAM solution that assigns IP addresses in an Citrix Application Delivery and Management environment. Ensure to specify the URL in the following format:

  ```
  https://<host name>
  <!--NeedCopy-->
  ```

  Example: `https://myinfoblox.example.com`

- **User Name** - Specify the user name to log in to the IPAM solution.
- **Password** - Specify the password to log in to the IPAM solution.

4. Click **Add**.

Add a network

Add a network to use IPAM with Citrix Application Delivery and Management managed configurations.

1. Navigate to **Settings > IPAM**.
2. Under **Networks*, click **Add**.
3. Specify the following details:
   - **Network Name** - Specify the network name to identify the network in Citrix Application Delivery and Management.
   - **Provider** - Select the provider from the list.

     This list displays the providers added in Citrix Application Delivery and Management.

   - **Network Type** - Select **IP range** or **CIDR** from the list based on your requirement.
   - **Network Value** - Specify the network value.

     > **Note**
     >
     > Citrix Application Delivery and Management 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:

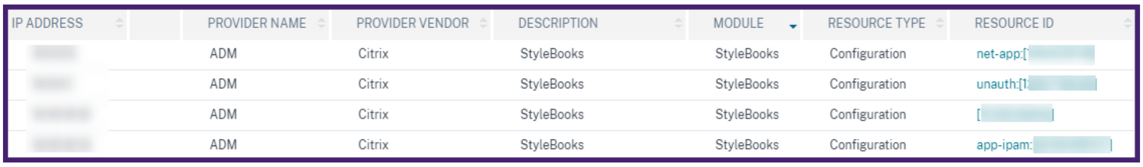
```
10.70.124.0/24
<!--NeedCopy-->
```

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 **Settings > IPAM**.
2. Under the **Networks** tab, click **View All Allocated IPs**.



IP ADDRESS		PROVIDER NAME	PROVIDER VENDOR	DESCRIPTION	MODULE	RESOURCE TYPE	RESOURCE ID
[redacted]		ADM	Citrix	StyleBooks	StyleBooks	Configuration	net-app:[[redacted]
[redacted]		ADM	Citrix	StyleBooks	StyleBooks	Configuration	unauth:[1[redacted]
[redacted]		ADM	Citrix	StyleBooks	StyleBooks	Configuration	[[redacted]
[redacted]		ADM	Citrix	StyleBooks	StyleBooks	Configuration	app-ipam:[redacted]

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 Citrix Application Delivery and Management module that reserved the IP address. For example, if StyleBooks reserved the IP address, 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. So, it displays Configurations under this column.
- **Resource ID**: Displays the exact resource id with a link. Click this link to access the resource that is using the IP address. For the configuration resource type, it displays the configuration pack ID as the resource ID.

> **Note**
>
> If you want to release the IP address, select the IP address that you want to release and click **Release Allocated IPs**.

How-to articles

September 28, 2021

Citrix Application Delivery and Management "How-to Articles" are simple, relevant, and easy to implement articles on the features available with the service. These articles contain information about some of the popular Citrix Application Delivery and Management features such as instance management, configuration management, event management, application management, StyleBooks, and certificate management.

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

TOPICS		
Instance management	Configuration management	Certificate management
StyleBooks	Event management	

Instance management

How to monitor globally distributed sites

How to manage admin partitions of Citrix ADC instances

How to add instances to Citrix Application Delivery and Management

How to create instance groups on Citrix Application Delivery and Management

How to poll Citrix ADC instances and entities in Citrix Application Delivery and Management

How to configure sites for Geomaps in Citrix Application Delivery and Management

How to force a failover to the secondary Citrix ADC instance

How to force a secondary Citrix ADC instance to stay secondary

How to change a Citrix ADC MPX or VPX root password

How to change a Citrix ADC SDX root password

Configuration management

How to use SCP (put) command in configuration jobs

How to upgrade Citrix ADC SDX instances by using Citrix Application Delivery and Management

How to schedule jobs created by using built-in templates in Citrix Application Delivery and Management

How to reschedule jobs that were configured by using built-in templates in Citrix Application Delivery and Management

Reuse run configuration jobs

How to upgrade Citrix ADC instances using Citrix Application Delivery and Management

How to create a configuration job on Citrix Application Delivery and Management

How to use variables in configuration jobs on Citrix Application Delivery and Management

How to use configuration templates to create audit templates on Citrix Application Delivery and Management

How to create configuration jobs from corrective commands on Citrix Application Delivery and Management

How to replicate running and saved configuration commands from one Citrix ADC instance to another on Citrix Application Delivery and Management

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

How to use the master configuration template on Citrix Application Delivery and Management

Certificate management

How to configure an enterprise policy on Citrix Application Delivery and Management

How to install SSL certificates on a Citrix ADC instance from Citrix Application Delivery and Management

How to update an installed certificate from Citrix Application Delivery and Management

How to link and unlink SSL certificates by using Citrix Application Delivery and Management

How to create a certificate signing request (CSR) by using Citrix Application Delivery and Management

How to set up notifications for SSL certificate expiry from Citrix Application Delivery and Management

How to use the SSL dashboard on Citrix Application Delivery and Management

StyleBooks

How to use default StyleBooks in Citrix Application Delivery and Management

How to create your own StyleBooks

How to use user-defined StyleBooks in Citrix Application Delivery and Management

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 SSL certificate and certificate key files to Citrix Application Delivery and Management

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

How to use Microsoft ADFS Proxy StyleBook

How to use Oracle E-business StyleBook

How to use SSO Office 365 StyleBook

How to use SSO Google Apps StyleBook

Event management

How to set event age for events on Citrix Application Delivery and Management

How to schedule an event filter by using Citrix Application Delivery and Management

How to set repeated email notifications for events from Citrix Application Delivery and Management

How to suppress events by using Citrix Application Delivery and Management

How to use the events dashboard to monitor events

How to create event rules on Citrix Application Delivery and Management

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

How to view the events summary in Citrix Application Delivery and Management

How to display event severities and skews of SNMP traps on Citrix Application Delivery and Management

How to export syslog messages using Citrix Application Delivery and Management

How to suppress Syslog messages in Citrix Application Delivery and Management

FAQs

September 25, 2021

How many agents do I need to install?

The number of agents depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

How can I install multiple agents?

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Settings** > **Setup Agents**.

Can I transition from a built-in agent to an external agent?

Yes, you can. For more information, see Transition from a built-in agent to an external agent.

How do I get a new activation code if I lose it?

If you are onboarding for the first time, access the service GUI, navigate to the **Set Up Agent** screen, and click **Generate Activation Code**.

While trying to install a second agent, to generate a new activation code, navigate to **Infrastructure > Instances > Agents > Generate Activation Code.**

How do I log on to the agent VM? What are the default credentials?

If your agent is installed on a hypervisor or Microsoft Azure cloud, the default logon credentials for the Citrix Application Delivery and Management agent are `nsrecover/nsroot`, which opens the shell prompt of the agent.

If your agent is installed on AWS, the default credentials to log on to the Citrix Application Delivery and Management agent is `nsrecover/instance id`.

What are the resource requirements to install an agent on a hypervisor on-premises?

32 GB RAM, 8 Virtual CPU, 500 GB Storage, 1 Virtual Network Interfaces, 1 Gbps Throughput

Do I need to assign an extra disk to the agent while provisioning?

No, you do not have to add an extra disk. The agent is used only as an intermediary between the Citrix Application Delivery and Management and the instances in your enterprise data center or on the cloud. It does not store inventory or analytics data that would require an extra disk.

Can I reuse my activation code with multiple agents?

No, you cannot.

How do I rerun network settings if I have entered an incorrect value?

Access the agent console on your hypervisor, log on to the shell prompt by using the credentials nsrecover/nsroot, and then run the command `networkconfig`.

What do I do if my agent registration fails?

- Make sure your agent has access to the Internet (configure DNS).
- Make sure you have copied the activation code correctly.
- Make sure you have entered the service URL correctly.
- Make sure you have the required ports open.

Registration is successful, but how do I know if the agent is running fine?

After the agent is successfully registered, access Citrix Application Delivery and Management and navigate to the **Set Up Agent** screen. You can see the discovered agent on the screen. If the agent is running fine, a green icon appears. If it is not running, a red icon appears.

How can I connect agents to Citrix Application Delivery and Management using a proxy server?

You can connect agents to Citrix Application Delivery and Management using a proxy server. The agents forward all their data to the proxy server, which then sends the data to the Citrix Application Delivery and Management through the internet.

To forward data using the proxy server, type the proxy server details on the agent using the following script: proxy_input.py, and follow the instructions provided by the script to enter more information. The agent fetches this information while it connects to Citrix Application Delivery and Management using the proxy server.

You can authenticate your proxy server by providing your user name and password information. When the agent sends the data, the proxy server authenticates the user credentials before forwarding it to Citrix Application Delivery and Management.

> **Note**
>
> Citrix Application Delivery and Management supports proxy servers with basic authentication enabled. Citrix Application Delivery and Management also supports proxy servers where authentication is disabled.

I do not see my Analytics Reports

Enable Insight on your virtual servers to see the Analytics Reports. For details, see Enabling Analytics.

Which versions of Citrix ADC instances are supported in Citrix Application Delivery and Management?

For management and monitoring features, Citrix ADC instances running 10.5 and later are supported. Some features are only supported on certain Citrix ADC versions. For details, see System Requirements.

How do I export dashboard reports in Citrix Application Delivery and Management?

To export the report of any dashboard in Citrix Application Delivery and Management, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
   The report downloads to your system.

2. Select **Schedule Report** to set up schedules for generating and exporting reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

   a) **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

   > **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.

   b) **Recurrence time** - Enter the time as `Hour: Minute` in 24-hour format.

   c) **Email** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

   d) **Slack** - Select the check box and then select the profile from the drop-down list box, or click **Add** 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.

What does enabling client-side measurements do?

With client side measurements enabled, Citrix Application Delivery and Management captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States