# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Features and solutions</td>
<td>4</td>
</tr>
<tr>
<td>Release notes</td>
<td>8</td>
</tr>
<tr>
<td>Release Notes for Citrix ADM service Aug 16, 2022 Release</td>
<td>9</td>
</tr>
<tr>
<td>Release Notes for Citrix ADM service July 13, 2022 Release</td>
<td>11</td>
</tr>
<tr>
<td>Release Notes for Citrix ADM service June 29, 2022 Release</td>
<td>13</td>
</tr>
<tr>
<td>Getting started</td>
<td>14</td>
</tr>
<tr>
<td>Configure the ADC built-in agent to manage instances</td>
<td>48</td>
</tr>
<tr>
<td>Install an agent on-premises</td>
<td>54</td>
</tr>
<tr>
<td>Install an agent on Microsoft Azure cloud</td>
<td>56</td>
</tr>
<tr>
<td>Install an agent on Amazon Web Services (AWS)</td>
<td>67</td>
</tr>
<tr>
<td>Install an agent on GCP</td>
<td>82</td>
</tr>
<tr>
<td>Install an agent in Kubernetes cluster</td>
<td>85</td>
</tr>
<tr>
<td>How to Get Help and Support</td>
<td>86</td>
</tr>
<tr>
<td>Low-touch onboarding of Citrix ADC instances using Citrix ADM service connect</td>
<td>93</td>
</tr>
<tr>
<td>Onboard Citrix ADC instances using Citrix ADM service connect</td>
<td>96</td>
</tr>
<tr>
<td>Test onboarding readiness of ADC instances</td>
<td>113</td>
</tr>
<tr>
<td>Email Settings</td>
<td>114</td>
</tr>
<tr>
<td>Troubleshoot issues using the diagnostic tool or the ADM GUI</td>
<td>118</td>
</tr>
<tr>
<td>Transition from a built-in agent to an external agent</td>
<td>126</td>
</tr>
<tr>
<td>System requirements</td>
<td>127</td>
</tr>
<tr>
<td>Licenses</td>
<td>139</td>
</tr>
<tr>
<td>Manage resources using Express account</td>
<td>141</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Upgrade to Citrix ADM Advance account</td>
<td>144</td>
</tr>
<tr>
<td>Differences between Express and Advance entitlements</td>
<td>144</td>
</tr>
<tr>
<td>Managing subscriptions</td>
<td>146</td>
</tr>
<tr>
<td>Upgrade Advisory</td>
<td>155</td>
</tr>
<tr>
<td>Security Advisory</td>
<td>162</td>
</tr>
<tr>
<td>RemEDIATE vulnerability for CVE-2020-8300</td>
<td>172</td>
</tr>
<tr>
<td>RemEDIATE vulnerability for CVE-2021-22927 and CVE-2021-22920</td>
<td>185</td>
</tr>
<tr>
<td>Identify and remEDIATE vulnerability for CVE-2021-22956</td>
<td>197</td>
</tr>
<tr>
<td>Identify and remEDIATE vulnerability for CVE-2022-27509</td>
<td>204</td>
</tr>
<tr>
<td>Unsupported CVEs in Security Advisory</td>
<td>206</td>
</tr>
<tr>
<td>Setting up</td>
<td>206</td>
</tr>
<tr>
<td>Adding multiple agents</td>
<td>207</td>
</tr>
<tr>
<td>Configure agents for multisite deployment</td>
<td>209</td>
</tr>
<tr>
<td>Configuring agent upgrade settings</td>
<td>211</td>
</tr>
<tr>
<td>Dual NIC support on Citrix ADM</td>
<td>212</td>
</tr>
<tr>
<td>Adding instances</td>
<td>215</td>
</tr>
<tr>
<td>Adding HAPProxy instances</td>
<td>222</td>
</tr>
<tr>
<td>Configuring syslog on instances</td>
<td>225</td>
</tr>
<tr>
<td>Logstream overview</td>
<td>227</td>
</tr>
<tr>
<td>How to assign more permissions to delegated admin users</td>
<td>230</td>
</tr>
<tr>
<td>Integration with the ServiceNow instance</td>
<td>235</td>
</tr>
<tr>
<td>A unified dashboard to view instance key metric details</td>
<td>238</td>
</tr>
<tr>
<td>Applications</td>
<td>242</td>
</tr>
<tr>
<td>Web Insight dashboard</td>
<td>244</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Application Delivery Management service

Analyze the root cause for application slowness 250
Service Graph 253
StyleBooks 256
Application Security Dashboard 258
View application security violation details 261
Application overview 267
All Violations 277
API gateway 284
Integration with Splunk 287
WAF learning engine 299
WAF recommendations 302
Gateway Insight 309
HDX Insight 332
Enable HDX Insight data collection 343
Enable data collection for Citrix ADC Gateway appliances deployed in single-hop mode 343
Enable data collection to monitor Citrix ADCs deployed in transparent mode 345
Enable data collection for Citrix ADC Gateway appliances deployed in double-hop mode 348
Enable data collection to monitor Citrix ADCs deployed in LAN user mode 353
Create thresholds and configure alerts for HDX Insight 357
View HDX Insight reports and metrics 362
Troubleshoot HDX Insight issues 362
Metrics information for thresholds 376
Infrastructure Analytics 380
View instance details in Infrastructure Analytics 403
View the capacity issues in an ADC instance 410
Enhanced Infrastructure Analytics with new indicators 413
Instance management 417
How to monitor globally distributed sites 420
How to create tags and assign to instances 427
How to search instances using values of tags and properties 430
Manage admin partitions of Citrix ADC instances 432
Back up and restore Citrix ADC instances 438
Force a failover to the secondary Citrix ADC instance 443
Force a secondary Citrix ADC instance to stay secondary 445
Create instance groups 446
Provision ADC VPX instances on SDX 446
Rediscover multiple Citrix ADC instances 455
Polling overview 456
Unmanage an instance 465
Trace the route to an instance 466
How to change the Citrix ADC MPX or VPX root password 467
How to change a Citrix ADC SDX nsroot password 473
Events 478
Use events dashboard 478
Set event age for events 480
Schedule an event filter 481
Set repeated email notifications for events 482
Suppress events 485
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create event rules</td>
<td>485</td>
</tr>
<tr>
<td>Modify the reported severity of events that occur on Citrix ADC instances</td>
<td>501</td>
</tr>
<tr>
<td>View events summary</td>
<td>502</td>
</tr>
<tr>
<td>Display event severities and SNMP trap details</td>
<td>504</td>
</tr>
<tr>
<td>View and Export syslog messages</td>
<td>506</td>
</tr>
<tr>
<td>Suppress syslog messages</td>
<td>510</td>
</tr>
<tr>
<td>SSL dashboard</td>
<td>513</td>
</tr>
<tr>
<td>Use the SSL dashboard</td>
<td>514</td>
</tr>
<tr>
<td>Set up notifications for SSL certificate expiry</td>
<td>521</td>
</tr>
<tr>
<td>Update an installed certificate</td>
<td>523</td>
</tr>
<tr>
<td>Install SSL certificates on a Citrix ADC instance</td>
<td>524</td>
</tr>
<tr>
<td>Create a Certificate Signing Request (CSR)</td>
<td>526</td>
</tr>
<tr>
<td>Link and unlink SSL certificates</td>
<td>529</td>
</tr>
<tr>
<td>Configure an enterprise policy</td>
<td>529</td>
</tr>
<tr>
<td>Poll SSL certificates from Citrix ADC instances</td>
<td>531</td>
</tr>
<tr>
<td>Configuration jobs</td>
<td>533</td>
</tr>
<tr>
<td>Create a configuration job</td>
<td>535</td>
</tr>
<tr>
<td>Configuration audit</td>
<td>539</td>
</tr>
<tr>
<td>Maintenance jobs</td>
<td>539</td>
</tr>
<tr>
<td>Use jobs to upgrade Citrix ADC instances</td>
<td>557</td>
</tr>
<tr>
<td>Network functions</td>
<td>566</td>
</tr>
<tr>
<td>Generate reports for load balancing entities</td>
<td>567</td>
</tr>
<tr>
<td>Export or schedule export of network functions reports</td>
<td>570</td>
</tr>
<tr>
<td>Network reporting</td>
<td>573</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Provisioning Citrix ADC VPX Instances on AWS</td>
<td>584</td>
</tr>
<tr>
<td>Pooled capacity</td>
<td>595</td>
</tr>
<tr>
<td>Manage the Kubernetes cluster for Service Graph</td>
<td>595</td>
</tr>
<tr>
<td>TCP Insight</td>
<td>599</td>
</tr>
<tr>
<td>Video Insight</td>
<td>604</td>
</tr>
<tr>
<td>View network efficiency</td>
<td>606</td>
</tr>
<tr>
<td>Compare the data volume used by optimized and unoptimized ABR videos</td>
<td>607</td>
</tr>
<tr>
<td>View the type of videos streamed and data volume consumed from your network</td>
<td>609</td>
</tr>
<tr>
<td>Compare optimized and unoptimized play time of ABR videos</td>
<td>611</td>
</tr>
<tr>
<td>Compare bandwidth consumption of optimized and unoptimized ABR videos</td>
<td>614</td>
</tr>
<tr>
<td>Compare optimized and unoptimized number of plays of ABR videos</td>
<td>615</td>
</tr>
<tr>
<td>View peak data rate for a specific time frame</td>
<td>618</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>620</td>
</tr>
<tr>
<td>Manage licensing and enable analytics on virtual servers</td>
<td>623</td>
</tr>
<tr>
<td>A unified process to enable analytics on virtual servers</td>
<td>633</td>
</tr>
<tr>
<td>Configure role-based access control</td>
<td>636</td>
</tr>
<tr>
<td>Configuring Analytics settings</td>
<td>658</td>
</tr>
<tr>
<td>Configure notifications</td>
<td>659</td>
</tr>
<tr>
<td>Export or schedule export reports</td>
<td>663</td>
</tr>
<tr>
<td>Instance settings</td>
<td>667</td>
</tr>
<tr>
<td>Instance settings</td>
<td>668</td>
</tr>
<tr>
<td>System configurations</td>
<td>670</td>
</tr>
<tr>
<td>Email subscriptions</td>
<td>670</td>
</tr>
<tr>
<td>Enable or disable features</td>
<td>673</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Data retention policy</td>
<td>674</td>
</tr>
<tr>
<td>Configure an action policy to receive application event notifications</td>
<td>676</td>
</tr>
<tr>
<td>Use audit logs for managing and monitoring your infrastructure</td>
<td>684</td>
</tr>
<tr>
<td>Configure IP address management (IPAM)</td>
<td>687</td>
</tr>
<tr>
<td>How-to articles</td>
<td>691</td>
</tr>
<tr>
<td>FAQs</td>
<td>693</td>
</tr>
</tbody>
</table>
Overview

March 2, 2022

Citrix Application Delivery and Management (Citrix ADM) 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 ADM 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 ADM provides the following benefits:

- **Agile** – Easy to operate, update, and consume. The service model of Citrix ADM is available over the cloud, making it is easy to operate, update, and use the features provided by Citrix ADM. 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 ADM 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 ADM, 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 ADM, your operational costs are reduced by saving your time, money, and resources on maintaining and upgrading the traditional hardware deployments.

**How Citrix ADM works**

Citrix ADM 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 ADM 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 ADM.
Citrix Application Delivery Management service

When you add an instance to Citrix ADM, 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 ADM periodically polls managed instances to collect information. For more information, see the Data Governance document.

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

Features and solutions

February 15, 2022

This document describes the features that are supported on the Citrix ADM.

Application analytics and management
Application Analytics and Management feature of Citrix ADM 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 ADM. Following are the related features that you can configure or view by using Citrix ADM:

- Creating event rules
- Using Citrix ADM to export syslog messages

**Certificate management**

Citrix ADM 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
Citrix Application Delivery Management service

keeping close tabs on certificates that are unused or soon to expire.

Configuration management

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

Configuration audit

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

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

License management

Allows you to manage Citrix ADC licenses by configuring Citrix ADM 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 ADM allocates licenses Citrix ADC VPX instances on demand. A Citrix ADC VPX instance can check out the license from the Citrix ADM when a Citrix ADC VPX instance is provisioned, or check back in its license to Citrix ADM when an instance is removed or destroyed.

Network reporting

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

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 ADM resources. For more information, see [Manage Citrix ADM resources using Express account](#).

The following Citrix ADM features are currently not available:

• **Deployment**
  – Migrating from Citrix Insight Center to Citrix ADM
  – Integrating Citrix ADM 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

August 16, 2022

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](#).

<table>
<thead>
<tr>
<th>Publication Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 16, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>July 26, 2022</td>
<td>Release notes version 2.0</td>
</tr>
<tr>
<td>July 13, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>June 29, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>June 15, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>June 07, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>May 25, 2022</td>
<td>Release notes version 2.0</td>
</tr>
<tr>
<td>May 10, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>April 27, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>April 12, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>March 31, 2022</td>
<td>Release notes version 2.0</td>
</tr>
<tr>
<td>March 31, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>March 16, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>March 01, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>February 10, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>January 28, 2022</td>
<td>Release notes version 2.0</td>
</tr>
<tr>
<td>January 25, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>January 17, 2022</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>November 29, 2021</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>November 09, 2021</td>
<td>Release notes version 1.0</td>
</tr>
<tr>
<td>October 26, 2021</td>
<td>Release notes version 1.0</td>
</tr>
</tbody>
</table>
Release Notes for Citrix ADM service Aug 16, 2022 Release

August 17, 2022

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build Aug 16, 2022.

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 Aug 16, 2022.

Analytics

App Dashboard - View detailed insights to troubleshoot the application issues
In **App Dashboard**, when you drill down an application, you can now view the **Recommended Actions** for the following application issues that enable you to view detailed insights to troubleshoot the issues:

- Response Time
- Active Services
- Unstable Server
- Service Flaps

For more information, see **Performance indicators (issues)**.

[NSADM-84811]

**Infrastructure**

**Dual NIC support for ADM agent**

You can configure a second NIC on ADM agent to manage access to Citrix ADM. Using the Dual NIC architecture, ADM agent will now be able to:

- Establish communication between ADM agent and ADC instances
- Establish communication between ADM agent and ADM service

For more information, see **Dual NIC support on Citrix ADM**.

[NSADM-85781]

**Recreate a cluster that is part of Google Cloud Autoscale group**

To view and troubleshoot the ADC clusters that are part of a Google Cloud (GCP) Autoscale group, you can now navigate to **Infrastructure > Public Cloud > Autoscale Group**, and click **View Clusters**.

You can select the GCP cluster and click **Recreate** to delete the existing cluster and replace it with a new cluster. All the application configurations are transferred to the new ADC cluster.

For more information, see **View and troubleshoot ADC clusters**.

[NSADM-75731]

**Management and Monitoring**

**View ADM agent details in the unified dashboard**

In the unified dashboard, you can now visualize an overview of ADM agent details. In **Overview > Dashboard**, next to the **ADM Agent Status**, you can view the agents that are available/unavailable.
Click **View Details** to visualize an overview of ADM agent details such as total in-built agents, total external agents, agent IP, status, system usage, diagnostic checks, and so on.

For more information, see [Unified dashboard overview](#).

[NSADM-83096]

**Fixed Issues**

The issues that are addressed in Build Aug 16, 2022.

**Analytics**

- After you enable analytics or when you edit analytics for Citrix Gateway virtual servers configured from the HA pair, the **Instance level options** under **Advanced Settings (optional)** appear disabled, even after these options are enabled.
  
  [NSHELP-32188]

- In **Gateway > HDX Insight > Users**, when you select a user, instead of showing details for the selected user, ADM shows details for all the users.
  
  [NSHELP-32181]

- In **Gateway > HDX Insight > Instances**, when you click a country to drill down for further details, the data under **Current Sessions** are not displayed.
  
  [NSHELP-32125]

**Release Notes for Citrix ADM service July 13, 2022 Release**

July 26, 2022

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build July 13, 2022.

**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 July 13, 2022.
Management and Monitoring

Support for identification and remediation of CVE-2022-27509

Citrix ADM security advisory now supports the identification and remediation of CVE-2022-27509.

Identification of CVE-2022-27509 requires a combination of version scan and custom scan, and remediation requires an upgrade of the vulnerable ADC instances to a release and build that has the fix. If your vulnerable ADC instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized ADC configurations before planning ADC upgrade.

You can also opt out of these Security Advisory custom scans. For more information on Custom Scan Settings and opting out of custom scans, see the Configure Custom Scan settings section on the Security Advisory page.

For more information about how ADM identifies ADCs vulnerable to CVE-2022-27509 and steps to remediation, see Identify and remediate vulnerabilities for CVE-2022-27509.

Note

It might take a couple of hours for the security advisory system scan to conclude and reflect on the impact of CVE-2022-27509 in the security advisory module. To see the impact sooner, you may start an on-demand scan by clicking Scan Now.

[NSADM-85549]

Configure an access policy for Upgrade Jobs

As a super administrator, you can now configure an access policy, set the permissions (View/Edit) for the Upgrade Jobs, and apply the policy to your Citrix ADM users. In Settings > Users & Roles > Access Policies, click Add to configure an access policy by selecting Infrastructure > Upgrade Jobs under Permissions.

For more information, see Configure access policies on Citrix ADM.

[NSADM-82494]

Support for configuration audit in Citrix ADC BLX instances in shared mode

You can now create Configuration Audit templates with certain configurations and monitor the configuration changes in Citrix ADC BLX instances in shared mode. For more information, see Create audit templates.

[NSADM-82323]
Support for CSV format and schedule export in Web transaction analytics

In Web transaction analytics, you can now view the following enhancements when you click the Export icon:

- In Export Now, you can export data in CSV format.
- The Schedule Export option is introduced that enables you to schedule and export the data in CSV format through email and Slack.

For more information, see Web transaction analytics.

Fixed Issues

The issues that are addressed in Build July 13, 2022.

In Citrix ADM Service, when you navigate to Infrastructure > Instances > Agents, and click Settings to change the agent upgrade settings, a confirmation message Modified Agent Upgrade Settings is displayed once the settings are changed.

[NSHELP-32099]

Release Notes for Citrix ADM service June 29, 2022 Release

June 30, 2022

This release notes document describes the enhancements and changes, fixed and known issues that exist for the Citrix ADM service release Build June 29, 2022.

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 June 29, 2022.

Applications

Configure and associate an application to multiple custom applications
Citrix Application Delivery Management service

In **Application Dashboard**, you can now configure an application and associate it to multiple custom applications. Using this feature, you can reuse the same application for multiple custom applications, rather than creating a separate application for each custom app.

For more information, see Configure and associate an application to multiple custom applications. [NSADM-82040]

**Management and Monitoring**

**Supported browsers to access Citrix ADM GUI**

Citrix ADM GUI is now accessible only from the following compatible browser versions:

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge</td>
<td>79 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>51 and later</td>
</tr>
<tr>
<td>Safari</td>
<td>10 and later</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>52 and later</td>
</tr>
</tbody>
</table>

[NSADM-83943]

**Getting started**

June 28, 2022

This document walks you through how to get started with onboarding and setting up Citrix ADM 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 ADM.

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 ADM, 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
Step 2: Manage Citrix ADM 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:

   - South America
   - Asia Pacific
   - EMEA
   - North America
Select a region that best suits your performance and business needs.

- South America
- Asia Pacific
- EMEA
- North America

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Admin</td>
<td>Monitor ADC infrastructure, Automate ADC Configuration, Manage SSL Certificates</td>
</tr>
<tr>
<td>App Admin</td>
<td>Remediate app health anomalies, Assess app usage trend &amp; deviation, Simplified app maintenance management</td>
</tr>
<tr>
<td>Gateway Admin</td>
<td>Track work from home usage, Debug user access issues, Troubleshoot user latency issues</td>
</tr>
<tr>
<td>Security Admin</td>
<td>Assess security configuration posture, Identify WAF, Bot &amp; API security violations, Remediate identified ML based violations</td>
</tr>
<tr>
<td>SRE</td>
<td>Cross microservice interaction visibility, Identify bottlenecks through distributed tracing, Troubleshoot golden signal violations</td>
</tr>
</tbody>
</table>
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 ADM resources. If your Citrix ADM Express account remains inactive for 90 days, the account gets deleted. For more information, see Manage Citrix ADM using Express account.

When you log back on to your Citrix Cloud account, the Citrix ADM GUI screen appears. Click Get Started to begin setting up the service for the first time.
Step 3: Select an ADC deployment type

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

- **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 ADM 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.

  ![Smart deployment diagram]

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

  ![Custom deployment diagram]

**Select smart deployment for AWS**

This deployment option creates the following infrastructure in AWS:
Citrix Application Delivery Management service

- A CloudFormation stack in AWS to create the required infrastructure that includes subnets, security groups, NAT gateways, and so on.
- An Citrix ADM 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](image)

   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

   ![Continue]
The Citrix ADM 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**.
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 ADM 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 ADM 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.
c) Click **Next**.

After successful validation, click **Create** to deploy ADC instances in AWS and create an Autoscale group.
3. After the successful ADC deployment, click **Deploy Application**.

   In **Configure Application**, specify the necessary details and click **Submit**.
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
Citrix Application Delivery Management service

subnets, security groups, NAT gateways, and so on.

• An Citrix ADM 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 ADM and ADC cloud access profile details.
The Citrix ADM uses the Citrix ADM 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.
b) In **Data Center Details**, specify the region, resource group, and virtual network details where you want to deploy ADC instances.

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

- **Availability** - Select the availability zone or set in which you want to create the Auto-scale 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 ADM 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 ADM 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.

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**.

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 ADM 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**.
The Citrix ADM 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.
Citrix Application Delivery Management service

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

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 ADM 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 ADM 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.
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**.

In **Configure Application**, specify the necessary details and click **Submit**.
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 en-
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 ADM Agent to enable communication between the Citrix ADM 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
• 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.

• As a microservice - To deploy an agent as a Kubernetes application.
• **Built-in agent** - To discover built-in agents available with Citrix ADC version 12.0 or 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 ADM agent on a hypervisor:

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

    ![Select hypervisor and download image](image1)

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

2. Copy the service URL and an activation code.

    ![Copy service URL and activation code](image2)

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 ADM 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 ADM. You can add the agents and instances later. To add agents later, navigate to **Set-
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.

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 ADM agent as a microservice in the Kubernetes cluster to view service graph in Citrix ADM.

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

   ![Enable Communication Between Instances and the Application Delivery Management](image)

   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 ADM 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 ADM.
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.

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 ADM**

Instances are network appliances or virtual appliances that you want to discover, manage, and monitor from Citrix ADM. 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.
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**.
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 ADM, see **Adding Instances**.

**Onboard ADC instances by using the Citrix ADM GUI dashboard**

If you’ve skipped onboarding the ADC instances in the **Getting Started** workflow while setting up Citrix ADM for the first time, you can onboard the instances from the Citrix ADM GUI dashboard. If the 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 ADM.
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 ADM, you see only the Citrix ADM landing page with the navigation bar on the left.

**Agent actions**

After you’ve set up your Citrix ADM, 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 ADM agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

**View agent diagnostics and receive alerts for endpoint verification**

Citrix ADM performs a periodic (every one hour) diagnostic check for agent and provides the following information:

- **Endpoint reachability** – Checks if all endpoints are reachable. The ADM agent uses various endpoints for the communication between ADM and ADC instances. For more information, see Software Requirements.

- **Health check probe** – Provides the time stamp of the latest health check.

- **Agent proxy** – Checks if the agent proxy exists.

If the agent endpoint reachability status changes (from **OK** to **Needs Review**), the super administrator receives an email notification comprising the issue details. Navigate to **Infrastructure > Instances > Agents** to view the newly added **Diagnostics Status** option that provides the status such as **Needs Review** or **OK**.

Click to view the diagnostic information of an agent.

- **Category**. Provides the issue category.

- **Status**. Provides the issue status such as **Needs Review** or **OK**.
**Recommendation.** Provides the required recommendation to troubleshoot the issue.

After you troubleshoot and the endpoint reachability status changes from **Needs Review** to **OK**, the super administrator receives an email notification mentioning that the issue is resolved.

**Email notification**

The following example is an email notification after the endpoint reachability status has changed from **OK** to **Needs Review**:

```
From: <admin@citrix.com>
Sent: Wednesday, February 2, 2022 9:05 PM
To: admin@citrix.com
Subject: ADM Agent Diagnostics Alert

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID: [REDACTED]
Agent IP: [REDACTED]
Agent Host Name: [REDACTED]
Diagnostics Alert:
• **https://download.citrixnetworkapi.net** not reachable
```

The following example is an email notification after the endpoint reachability status has changed from **Needs Review** to **OK**:

```
From: <admin@citrix.com>
Sent: Wednesday, February 2, 2022 9:07 PM
To: admin@citrix.com
Subject: ADM Agent Diagnostics Alert Cleared

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID: [REDACTED]
Agent IP: [REDACTED]
Agent Host Name: [REDACTED]
Diagnostics Alert:
• No error detected
```

**Configure the ADC built-in agent to manage instances**

February 15, 2022
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 ADM.

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 ADM 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.
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.

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:

   ![Command for SDX instance]

   - In <user_name>, enter Citrix ADC user name.
Note
Citrix ADM 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.xx or 12.1 57.xx, 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.

<table>
<thead>
<tr>
<th>ADC image version</th>
<th>Is mastools_version 0.0-0.0?</th>
<th>Command for registration with profile</th>
<th>Command for registration without profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower than 13.0 61.xx and 12.1 57.xx</td>
<td>Yes</td>
<td><code>. /mastools_init.sh &lt;device-profile-name&gt; &lt;service-url&gt; &lt;activation-code&gt; -sdx -profile</code></td>
<td><code>. /mastools_init.sh &lt;user_name&gt; &lt;pwd&gt; &lt;service_url&gt; &quot;$MAS;&lt;activation_code&gt;-profile&quot;</code></td>
</tr>
<tr>
<td>Lower than 13.0 61.xx and 12.1 57.xx</td>
<td>No</td>
<td><code>. /mastools_init.sh &lt;device_profile_name&gt;&lt;pwd&gt; &lt;service_url&gt; &lt;activation_code&gt; -profile</code></td>
<td><code>. /mastools_init.sh &lt;user_name&gt; &lt;pwd&gt; &lt;service_url&gt; &lt;activation_code&gt;</code></td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>ADC image version</th>
<th>Is mastools_version 0.0-0.0?</th>
<th>Command for registration with profile</th>
<th>Command for registration without profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher than 13.0 61.x and 12.1 57.xx</td>
<td>Not applicable</td>
<td>./mastools_init.sh &lt; device_profile_name &lt; &lt;service_url&gt; &lt;activation_code&gt; -profile</td>
<td>./mastools_init.sh &lt; user_name&gt; &lt;pwd&gt; &lt;service_url&gt; &lt;activation_code&gt;</td>
</tr>
</tbody>
</table>

- 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 ADM 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**.
6. Click **Done**.

After successful built-in agent configuration, you can access the Citrix ADM 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 ADM GUI.
Citrix Application Delivery Management service

- 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 ADM GUI, check:
  - Mastools_upgrade logs in /var/mastools/logs/mastools_upgrade.log
  - Binary logs in /var/log/mastoolsd.log.

Install an agent on-premises

February 15, 2022

The agent works as an intermediary between the Citrix ADM 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8</td>
</tr>
<tr>
<td>Storage space</td>
<td>30 GB</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

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:
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.

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:

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

```
1 register_agent_cloud.py
2 <!--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.

7. After agent registration is successful, the agent restarts to complete the installation process. After the agent has restarted, access the Citrix ADM 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.

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

August 11, 2022
The agent works as an intermediary between the Citrix ADM 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](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 ADM 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:**

2. Click **Create a resource**.
3. Type **Citrix ADM agent** in the search bar and select **Citrix ADM agent**.
4. Click **Create**.

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**.
• **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.

  For more information about supported virtual disk sizes, see Agent installation requirements and Lightweight agent for pooled licensing.

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

**Networking:**

Specify the required networking details:
- **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.

Advanced:

Optional, specify Extensions, Custom Data, and Proximity placement group.
Create a virtual machine

Basics  Disks  Networking  Management  Advanced  Tags  Review + create

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

Extensions
Extensions provide post-deployment configuration and automation.

Extensions  0  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 codec 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  0  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  0  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  0  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 ADM as instructed in **Getting Started**. Enter the details in the following format:

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

Agent uses this information to auto-register with the Citrix ADM 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 ADM.

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.

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.

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 Application Delivery Management service

- 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 ADM as instructed in **Getting Started**. The agent uses the service URL to locate the service and the activation code to register with the service.

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

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

**Install an agent on Amazon Web Services (AWS)**

February 15, 2022

The Citrix ADM agent works as an intermediary between the Citrix ADM 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 ADM, and the Citrix ADC instances,
Citrix Application Delivery Management service

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 ADM External agent AMI from the available list.
4. On the Citrix ADM External Agent AMI page, click Continue to Subscribe.
5. After the subscription is successful, click Continue to Configuration.
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**

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 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**
7. The launch from a Website is successful.

![Citrix ADM External Agent AMI](image)

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

AMI ID: ami-07a0b88ae68f5d3ad
(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.

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 ADM. 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 ADM as instructed in **Getting Started**. The agent uses the service URL to locate the service and the activation code to register with the service.

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

After the agent has restarted, access Citrix ADM 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**.

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 ADM as instructed in **Getting Started**. Enter the details in the following format.
Agent uses this information to auto-register with the Citrix ADM during boot-up.

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

```python
#!/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 ADM. Pass it in userdata to make Citrix ADM agent in AWS to autoregister on bootup. The workflow is as follows

1) Fetch the Citrix ADM 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 ADM with credentials fetched in step 1

3) Call Citrix ADM 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 ADM Credentials

The secrets value should be in the following json format

```
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_formatter = logging.Formatter(fmt='%(asctime)-2s:%(funcName)30s:%(lineno)4d: [%%(levelname)s] %(message)s',
    datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_formatter)
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 region is %s" % (my_region))

    '''Creating a Boto client 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 ADM credentials from AWS secret failed with error: %s" % (str(e)))
    raise e

'''Initializing common Citrix ADM API handlers

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

'''API to login to the Citrix ADM 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 ADM 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 ADM

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:
This script fetches the authentication details from the AWS secrets manager and runs the deployment.py script to register the agent with the Citrix ADM.

Note

While you can auto-assign public IP address, you can also assign elastic IP address. Assigning 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.
4. On the **Add Tags** page, define the tag for the instance, and click **Next: Configure Security Group**.

5. On the **Configure Security Group** page, add rules to allow specific traffic to your instance and click **Review and Launch**.
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 dialog box](image)

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

February 15, 2022

The Citrix ADM agent works as an intermediary between the Citrix ADM 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 ADM. 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.

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

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

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.

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 ADM as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.
After agent registration is successful, the agent restarts to complete the installation process.

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

Install an agent in Kubernetes cluster

February 15, 2022

**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:

   ```bash
   kubectl create -f <yaml file>
   ```

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

   The agent is successfully created.

In Citrix ADM, navigate to Infrastructure > Instances > Agents to see the agent status.
How to Get Help and Support

October 15, 2020

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 sign-in interface]

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

- Make sure you sign in with the email address and password 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.

- **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 Application Delivery Management service

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.

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.
Citrix Application Delivery Management service

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

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.
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.

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).
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 Citrix ADM service connect**

June 16, 2022

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 ADM launches a new onboarding workflow, which provides you a faster way to get complete visibility into your HMC deployment.
Overview: components of Citrix ADM onboarding workflow

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

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

Citrix ADM 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 ADM 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 ADM 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 ADM to enable this new workflow.

All ADC instances with internet connectivity or Call Home, or instances enabled with Citrix ADM connect are connected to Citrix ADM. Citrix ADM starts collecting relevant metrics from these ADC instances through Call Home route, Citrix ADM 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 ADM creates an inventory of ADC instances for every customer (unique org ID), which shows you a consolidated list of your ADC instances. Citrix ADM 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 ADM.

You can check **Select ADC and Gateway instances to onboard** and select the ADC instances you want to onboard to Citrix ADM. After you start, you are guided to the onboarding process.

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

**Notes**

- 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 ADM. Or if you want both use pooled licensing and the complete analytics suite. The
Citrix Application Delivery Management service

- The metrics collected by ADM Service Connect are directly sent to the ADM Service endpoint. Even if the ADC is a managed/discovered ADC on ADM Service and an external agent has been configured for that ADC, the metrics are sent directly from ADC to the ADM Service endpoint and are not routed through through the external agent.

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 ADM showing some key insights of your ADC infrastructure and inviting you to get started with Citrix ADM. Click Onboard to ADM Service in the email. The Citrix Cloud page appears.

2. In the Citrix Cloud login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of Citrix.com, My Citrix, or Citrix Cloud.
   - If you are not an existing Citrix Cloud customer, sign up to Citrix Cloud. For more information, see Signing Up for Citrix Cloud.

Notes
   - If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials. Then, complete the onboarding workflow for the new Org ID.
   - You can enable or disable the email notifications that you receive as part of ADM Service Connect based low-touch onboarding workflow. For more information, see Email Settings.


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 ADM.

6. Onboard ADC instances to Citrix ADM: Based on the ADC instances selected for onboarding, Citrix ADM guides you with the onboarding process. By default, the built-in agent is selected for auto-onboarding.
7. **Citrix ADM GUI dashboard**: After onboarding completes, you are guided to the Citrix ADM instance dashboard.

For more details on each of these onboarding methods, see [Onboard Citrix ADC instances using Citrix ADM connect](#).

**Onboard Citrix ADC instances using Citrix ADM service connect**

March 16, 2022

Following is a step-by-step guide to help you get started with Citrix ADM. Before you start, read how the Citrix ADM 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 ADM connect](#).

**Step 1: Get started**

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

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.

These new features can 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 onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Cell Home and/or Citrix ADM Service Connect.

ADC instances by platforms

<table>
<thead>
<tr>
<th>Total</th>
<th>VPX</th>
<th>SDX</th>
<th>MPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>20</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Security Advisory**
  - 5 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**
  - 2 ADC instances are on versions that have reached end of life in last 365 days or earlier.
    - 1 ADC instance is on a version that will reach end of life in next 365 days.
    - 3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.
    - 4 ADC instances are on versions that will reach end of maintenance in next 365 days.
    - 2 ADC instances are on older builds and releases.

- **Recent events**
  - 4 ADC instances encountered SSL card failure.
  - 2 ADC instances encountered hard disk failure.

- **Resource utilization**
  - 2 ADC instances CPU usage exceeded 50%.
  - 3 ADC instances memory usage exceeded 50%.

- **ADC deployment**
  - 5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

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

As a first step, you will need to create Citrix Cloud account by clicking on the button below.
1. In the email, click **Onboard to ADM Service**. The **Citrix Cloud** page appears.

2. In the **Citrix Cloud** login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of **Citrix.com**, **My Citrix**, or **Citrix Cloud**.
   - If you are not an existing Citrix Cloud customer, sign up to Citrix Cloud. For more information, see **Signing Up for Citrix Cloud**.

   **Notes**
   - If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials. Then, complete the onboarding workflow for the new Org ID.
   - You can enable or disable the email notifications that you receive as part of ADM Service Connect based low-touch onboarding workflow. For more information, see **Email Settings**.

3. In the Citrix ADM landing page, take a moment to read why you are there and the benefits of using Citrix ADM.

   **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 ADM.
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 ADM can offer and help you onboard your ADC instances onto Citrix ADM seamlessly.

### Step 2: Insights on your ADC and Gateway instances

This insights page uses the data collected through Call Home or Citrix ADM connect or both Call Home and Citrix ADM 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 ADM 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 ADM.

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 ADM 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 ADM to monitor 200+ events regularly, and create rules to get notified over email, PagerDuty, Slack, ServiceNow, take appropriate action.
- **Resource utilization - trends and anomalies**: onboard ADC instances to Citrix ADM 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 ADM and configure them as HA pair, using configuration jobs on Citrix ADM.

1. **Security advisory**: Citrix ADM 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 ADM **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 ADM. After onboarding, Citrix ADM 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 you 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 MPX SDX UNKNOWN

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).

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>VULNERABILITY TYPE</th>
<th>AFFECTED ADC INSTANCES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-8300</td>
<td>Session Hijacking</td>
<td>11 ADC instances</td>
</tr>
<tr>
<td>CVE-2020-8299</td>
<td>Denial of Service</td>
<td>9 ADC instances</td>
</tr>
<tr>
<td>CVE-2020-8247</td>
<td>Escalation of privileges on the management interface</td>
<td>3 ADC instances</td>
</tr>
</tbody>
</table>

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 ADM 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.

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 ADM recommends you to plan a timely upgrade before EOM/EOL
or to benefit from the latest features and fixes.

To perform the upgrade, you must onboard your ADC instances on to Citrix ADM.

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.

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.

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

   - CPU: Predict CPU utilization for the next 24 hours on Citrix ADM.
• Memory: Predict memory utilization for the next 24 hours on Citrix ADM.
• SSL throughput: View SSL real time optimization with intelligent App Analytics on Citrix ADM.
• 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 the way through last step and onboard your ADC and Gateway instances to ADM service.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security advisory</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrade advisory</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recent events</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key Metrics: Get details of key metrics related to CPU, memory, HTTP throughput, SSL throughput, and uncover anomalous trends in metrics.
5. **Deployment guidance**: Have visibility into ADC instances that are deployed as a standalone ADC. Citrix ADM gives the recommendation to configure these ADC instances as an HA pair for better resiliency. This requires you to onboard your ADC instances to Citrix ADM and then use maintenance jobs to configure the instances as an HA pair.
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 ADM and click Next.

1. View and select the ADC instances you want to onboard to Citrix ADM.

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**

<table>
<thead>
<tr>
<th>DEVICE INFORMATION</th>
<th>ADC CONFIGURATION</th>
<th>ADC FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>[Redacted]</td>
<td>450000</td>
</tr>
<tr>
<td>Hostname</td>
<td>[Redacted]</td>
<td>VPX</td>
</tr>
<tr>
<td>platform</td>
<td>[Redacted]</td>
<td>NetScaler NS13.0: Build 47.24.nc</td>
</tr>
<tr>
<td>Platform type</td>
<td>[Redacted]</td>
<td>STANDALONE</td>
</tr>
<tr>
<td>Version</td>
<td>[Redacted]</td>
<td></td>
</tr>
<tr>
<td>High availability state (HA)</td>
<td>STANDALONE</td>
<td></td>
</tr>
<tr>
<td>Serial ID</td>
<td>[Redacted]</td>
<td></td>
</tr>
<tr>
<td>Host ID</td>
<td>[Redacted]</td>
<td></td>
</tr>
<tr>
<td>Platform description</td>
<td>NetScaler Virtual Appliance 3G</td>
<td></td>
</tr>
<tr>
<td>Hypervisor</td>
<td>Hyper</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>AWS</td>
<td></td>
</tr>
<tr>
<td>Encoded serial ID</td>
<td>[Redacted]</td>
<td></td>
</tr>
<tr>
<td>Netscaleruuid</td>
<td>[Redacted]</td>
<td></td>
</tr>
<tr>
<td>Build type</td>
<td>Classic</td>
<td></td>
</tr>
<tr>
<td>sysid</td>
<td>[Redacted]</td>
<td></td>
</tr>
</tbody>
</table>

### Mode(s)

<table>
<thead>
<tr>
<th>MODE</th>
<th>ENABLED ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Route Advertisement</td>
<td>No</td>
</tr>
<tr>
<td>IPv6 Direct Route Advertisement</td>
<td>No</td>
</tr>
<tr>
<td>TCP Buffering</td>
<td>Yes</td>
</tr>
</tbody>
</table>
If your instance is not listed, use the **Don’t find ADC in the list** on the upper-right corner.

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.

**Step 4: Onboard ADC instances to Citrix ADM**

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

You can perform a test run of onboarding to ensure that the ADC instance is ready to onboard. Click **Test** to start the test run. For more information, see **Test onboarding readiness of ADC instances**.

If you want to onboard without the test run, enter the ADC user name and password. The credentials must be ADC user admin credentials, and Citrix ADM uses these credentials to onboard ADC. Click **Start auto onboarding** to onboard your ADC instances on Citrix ADM.

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.

**SCRIPT BASED**

8 ADC instances qualify for script based onboarding.

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

**ADC Selection**

18 ADC instances.

**Device Profile**

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Note

After you specify the ADC credentials and create the Device Profile, the ADM GUI will not prompt for the Username and Password again for each ADC instance. However, you can select the profile from the Device profile drop-down to authenticate the ADC instances.

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.

**Onboarding**

- **Auto**: 10 ADC instances qualify for auto onboarding.
- **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
   ```

   Copy command

- I have run the script or command locally.

Note

If you don’t want the ADC instances to auto-onboard to Citrix ADM, you can disable auto-onboarding and you use the script-based option for 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.
After you’ve on boarded all your instances, click **Go to Citrix ADM** to go to the Citrix ADM instance management UI dashboard and explore the different features.

**Note**

If you are a new customer on Citrix ADM without an Citrix ADM license, your Citrix service account by default is an Express account. For more information about the Citrix ADM account entitlement, see [Manage Citrix ADM 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 ADM or both use pooled licensing and the complete analytics suite.

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

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

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 ADM agent on-premises
4. Click **Register Agent**. When completed, and click **Done** to return to the ADC onboarding Citrix ADM page.

5. Click **Start onboarding**. After you’ve on-boarded all your instances, click **View instance dashboard** to go to the Citrix ADM instance management UI dashboard and explore the different features.

**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 ADM agent on Microsoft Azure cloud
- Install Citrix ADM agent on AWS
- Install Citrix ADM agent on GCP
When you want to onboard an ADC instance to Citrix ADM, you can test whether the instances are ready for onboarding. The test run status suggests you if the instances are ready or needs review.

Click **Test** to start the diagnostic dry run. The ADC Diagnostics Details page displays the issue category, status, and recommendation.

For more information, see [View ADC diagnostic information in ADM GUI](#).
Citrix Application Delivery Management service

If the ADC test run status is in **Needs Review** status, then:

- Review the ADC Login credentials in the Device Profile.
- The following endpoints are unreachable:
  - adm.cloud.com
  - agent.adm.cloud.com
  - trust.citrixworkapi.net
  - download.citrixnetworkapi.net

If you face any issues when you run the test for onboarding readiness, see **Troubleshoot** for recommendations.

### Email Settings

July 25, 2022

Citrix ADM service allows onboarding of Citrix ADC instances using the ADM Service Connect based low-touch onboarding workflow. As a part of this workflow, **customers receive product initiated emails from Citrix ADM Service**. You can enable or disable the email notifications that you receive as part of the ADM Service Connect based low-touch onboarding workflow. You can configure and manage the email notifications in the following ways:

- **Enable emails for all admins** - You will be able to enable the emails for all admins in your org. By default, the emails are enabled for all the admins in the Org.
- **Enable / disable emails for selected admins** - You can customize the email settings so that only specific admins in the org receive emails and the other admins do not.
- **Disable emails for all admins** - You will be able to disable and stop the emails for all admins in your org.

### Configure Email Settings

You can configure the Email Settings and enable or disable the emails that you receive as part of the ADM Service Connect based low-touch onboarding workflow. To configure the **Email Settings**:

1. Click **Onboard to ADM Service** in the product initiated email. The **Citrix Cloud** page appears.
2. In the **Citrix Cloud** login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of Citrix.com, My Citrix, or Citrix Cloud.
Citrix Application Delivery Management service

- If you are not an existing Citrix Cloud customer, sign up to Citrix cloud. For more info, see Sign up for Citrix Cloud.

Note
If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials.

The Citrix Application Delivery and Management landing page appears, providing you with an overview of Citrix Application Delivery and Management and its benefits.

3. In the Citrix Application Delivery and Management landing page, click Next.

The Insights on your ADC and Gateway instances page appears, where you can get insights into your overall ADC infrastructure with recommendations.

4. In the Insights on your ADC and Gateway instances page, click Next.

The Select ADC and Gateway instances to onboard page appears, where you can see a list of ADC instances to onboard and additional options such as Email Settings.

5. Click Email Settings. The Email Settings pane appears.

You can now configure the email settings to enable or disable emails.

Note
If you have onboarded only one ADC instance, then you will not receive these emails.

If you are already on the ADM Service GUI and you want to configure the email settings:

1. In Citrix Application Delivery and Management, navigate to Infrastructure > Instances, and then click Citrix ADC. The Citrix ADC page appears.

2. In the Citrix ADC page, click Asset Inventory.

The Select ADC and Gateway instances to onboard page appears to show the list of ADC instances that are onboarded and additional options such as Email Settings.

3. Click Email Settings. The Email Settings pane appears.
You can now configure the email settings to enable or disable emails.

**Enable emails for all admins**

By default, the emails are enabled for all the admins in the Org.

To enable or subscribe to the email notifications as part of the ADM Service Connect based workflow:

1. In the Email Settings pane, select **Enable emails** for all admins.

2. Click **Save** and **Close**.

All the admins in the org are now subscribed and will receive email notifications as part of the ADM Service Connect based workflow.

**Enable / disable emails for specific admins in the org**

You can customize the email settings so that only specific admins in the org receive emails. You will see the list of admins who have the emails enabled on the left and the list of admins who have the emails disabled on the right.

To disable emails for specific admins in the org:

1. Locate the admin email address in the **Enabled** list.

2. Click the add button (+).
You will see the admin email address added to the **Disabled** list.

3. Click **Save** and **Close**.

The admin is now unsubscribed to not receive email notifications as part of the ADM Service Connect based workflow.

**Note**

If you want to disable emails for multiple admins, select all their email IDs in the **Enabled** email list, and click the add button (+) to add the email IDs to the **Disabled** list. Click **Save** and **Close**.

If you have previously disabled emails for specific or all admins in your org, you will be able to enable emails for all the admins. To enable emails for specific admins in the org:

1. Locate the admin email address in the **Disabled** list.

2. Click the remove button (-). You will see the admin email address removed from the **Disabled** list.
3. Click **Save** and **Close**.

The admin will now start receiving onboarding related emails. The admin is now subscribed to receive email notifications.

**Note**
If you want to enable emails for multiple admins, select all their email IDs in the **Disabled** email list, and click the remove button (-) to add the email IDs to the **Enabled** list. Click **Save** and **Close**.

### Disable emails for all admins

You can select this option if you want to disable or stop the emails for all admins who belong to your org.

To disable or unsubscribe from receiving emails:

1. In the **Email Settings** pane, select **Disable emails for all admins**.

2. Click **Save** and **Close**.

All the admins in the org are now unsubscribed and will not receive any email notifications.

### Troubleshoot issues using the diagnostic tool or the ADM GUI

**March 11, 2022**

**Note**

The diagnostic tool is applicable only for the ADC instances onboarded or to be onboarded using the Citrix ADM connect based low-touch onboarding.

For more information, see [Low-touch onboarding of Citrix ADC instances using Citrix ADM connect](#).

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

- 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 ADM GUI

If ADM service connect is enabled on the ADC instance, the diagnostic details are automatically sent to Citrix and you can view details in the ADM GUI. If ADM service connect is not enabled, you can manually use the diagnostic tool.

**Manually 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:

- nscli
- DNS configuration
- Internet connection
- Instance to ADM connection
- User privilege

If the issues still persist even after troubleshooting, you can contact Citrix support. When you contact Citrix support, you must provide the ADM connect configuration information that is displayed after you run the diagnostic tool.

The following is an example of diagnostic results for an ADC instance that has no issues:
Validating the ADC instance readiness for onboarding using the diagnostic tool

Before you onboard the ADC instance to Citrix ADM, 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 ADM** message.
View ADC diagnostic information in ADM GUI

Navigate to Infrastructure > Instances > Citrix ADC and click Asset Inventory to see the newly added Onboarding Readiness option that provides the ADC instance onboarding readiness status such as Needs Review or OK.

- **Needs Review.** The ADC instance has issues that need to be fixed.
- **OK.** The ADC instance is ready to onboard.

**Note**

If the Onboarding Readiness appears blank, it means the ADC instance is not running with the latest image that has diagnostic support.

If the ADC instance has any issues, the Needs Review option appears, and you can click to view more details.
Citrix Application Delivery Management service

After you click Needs Review, the ADC Diagnostics Details page displays the issue details.

- **Category.** Provides the issue category.
- **Status.** Provides the issue status such as Needs Review, OK, or Not Applicable.
- **Recommendation.** Provides the required recommendation to troubleshoot the issue.

After you fix the issue, the status in the Onboarding Readiness gets changed to OK.

**Troubleshoot**

The following are some of the ADC instance issues and their troubleshooting steps:
Invalid user name or password

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
Citrix Application Delivery Management service

**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 ADM endpoint**

**Workaround:** Ensure to check firewall settings and the following Citrix ADM endpoints are not blocked in the firewall:

```plaintext
1 ADM_GRP_EP = "adm.cloud.com"
2 ADM_AGENT_EP = "agent.adm.cloud.com"
3 ADM_TRUST_EP = "trust.citrixnetworkapi.net"
4 ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
5 <!--NeedCopy-->
```

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

When you perform a test run to ensure that the ADC instance is ready to onboard, the following issues maybe seen:

**Built-in agent dry run timeout**

If the results of the dry run are not fetched within 5 minutes, a Timeout message appears.
**Recommendation:** It is recommended that you verify whether the ADC instance is running with the latest image that has diagnostic support. Also, in the Asset Selection table, the Onboarding Readiness column appears blank.

**Red outline on the device profile dropdown**

ADC authentication fails during the dry run and a red outline appears on the device profile dropdown.

**Recommendation:** Re-enter the ADC user admin credentials again, create the device profile and click Test to run the dry run again.
Transition from a built-in agent to an external agent

February 15, 2022

You might have started with using Citrix ADM 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 ADM agent to an external agent.

The built-in agent supports only management and monitoring features. For other Citrix ADM features such as pooled licensing and analytics, you need an external agent. This document covers the steps for transitioning from an existing Citrix ADM 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 ADM 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 ADM GUI, under Infrastructure > Instances Dashboard > Citrix ADC, select the Citrix ADC instance and click Edit.

2. Select the site and agent and click OK.
3. Select the instance again and click **Select Action > Rediscover**.

### System requirements

**August 3, 2022**

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

### Supported browsers

To access Citrix ADM, your workstation must have a supported web browser.

The following browsers are supported.

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge</td>
<td>79 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>51 and later</td>
</tr>
</tbody>
</table>
Agent installation requirements

Install and configure an agent in your network environment to enable communication between the Citrix ADM 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 ADM agent. The following table lists the agent requirements to avail all Citrix ADM features:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8</td>
</tr>
<tr>
<td>Storage Space</td>
<td>30 GB</td>
</tr>
<tr>
<td>Virtual Network interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

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 ADM features:

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Agent requirements</th>
<th>Preferred virtual machine type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>8 virtual CPU, 32 GB RAM, and 30 GB storage space</td>
<td>m4.2xlarge</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>8 virtual CPU, 32 GB RAM, and 30 GB storage space</td>
<td>Standard_D8s_v3</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>8 virtual CPU, 32 GB RAM, and 30 GB storage space</td>
<td>e2-standard-8</td>
</tr>
</tbody>
</table>
For instructions about installing an agent, see the following links:

- Installing Citrix ADM Agent on Microsoft Azure Cloud.
- Installing Citrix ADM Agent on AWS.
- Installing Citrix ADM Agent on Google Cloud.

**Lightweight agent for pooled licensing**

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>4</td>
</tr>
<tr>
<td>Storage Space</td>
<td>30 GB</td>
</tr>
</tbody>
</table>

Such agents with lower specifications (lightweight) are supported only on Citrix ADM. Citrix recommends you use the following virtual machine types from the respective cloud marketplaces to avail only the pooled licensing feature:

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Agent requirements</th>
<th>Preferred virtual machine type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>4 virtual CPU, 8 GB RAM, and 30 GB storage space</td>
<td>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.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>4 virtual CPU, 8 GB RAM, and 30 GB storage space</td>
<td>Standard_F4s_v2</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>4 virtual CPU, 8 GB RAM, and 30 GB storage space</td>
<td>e2-standard-4</td>
</tr>
</tbody>
</table>
Note
You must disable the default scheduling jobs by navigating to Settings > Global Settings > Configurable Features.

Supported ports
For communications between Citrix ADC instances and Citrix ADM agent, or Citrix SD-WAN instances and Citrix ADM agent, open the required ports.

### Ports for the Citrix ADM agent
This table explains the required ports that must be open on the ADM agent.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Details</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/443</td>
<td>TCP</td>
<td>For NITRO communication from the Citrix ADM service to Citrix ADC or Citrix SD-WAN instance.</td>
<td>Citrix ADM agent to Citrix ADC and Citrix ADC to Citrix ADM agent</td>
</tr>
<tr>
<td>Port</td>
<td>Type</td>
<td>Details</td>
<td>Direction of communication</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>4739</td>
<td>UDP</td>
<td>For AppFlow communication from Citrix ADC or Citrix SD-WAN instance to the Citrix ADM service.</td>
<td>Citrix ADC or Citrix SD-WAN to Citrix ADM agent</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>To receive SNMP events from Citrix ADC instance to the Citrix ADM service.</td>
<td>Citrix ADC to Citrix ADM agent</td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>To receive syslog messages from Citrix ADC or Citrix SD-WAN instance to the Citrix ADM service.</td>
<td>Citrix ADC or Citrix SD-WAN to Citrix ADM agent</td>
</tr>
<tr>
<td>5557/5558</td>
<td>TCP</td>
<td>For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from Citrix ADC to the Citrix ADM service.</td>
<td>Citrix ADC to the Citrix ADM agent</td>
</tr>
<tr>
<td>27000 and 7279</td>
<td>TCP</td>
<td>License ports for communication between Citrix ADM agent and ADC instance. These ports are also used for ADC pooled licenses.</td>
<td>Citrix ADC to Citrix ADM agent</td>
</tr>
<tr>
<td>443/7443/8443</td>
<td>TCP</td>
<td>Ports for communication between Citrix ADM agent and Citrix ADM Service</td>
<td>Citrix ADM agent to Citrix ADM Service</td>
</tr>
</tbody>
</table>
## Ports for ADC and SD-WAN instances

This table explains the required ports that must be open on Citrix ADC and SD-WAN instances.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Details</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/443</td>
<td>TCP</td>
<td>For NITRO communication from Citrix ADM to Citrix ADC or Citrix SD-WAN instance.</td>
<td>Citrix ADM agent to Citrix ADC and Citrix SD-WAN agent</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>For SSH communication from Citrix ADM to Citrix ADC or Citrix SD-WAN instance. And, this port is required for the SSH communication between the ADM agent and Citrix ADC.</td>
<td>Citrix ADM agent to Citrix ADC</td>
</tr>
<tr>
<td>No reserved port</td>
<td>ICMP</td>
<td>To detect network reachability between Citrix ADM agent and Citrix ADC instances, or SD WAN instances.</td>
<td>Citrix ADM agent to Citrix ADC</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>To poll events from ADC instances.</td>
<td>Citrix ADM agent to Citrix ADC</td>
</tr>
</tbody>
</table>

## Ports for services

This table explains the required ports that must be open for the services to run:
### Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Details</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>5563</td>
<td>TCP</td>
<td>This port is required for Citrix ADM Collector service to run. To receive ADC metrics (counters) from Citrix ADC instance to Citrix ADM.</td>
<td>Citrix ADC to Citrix ADM</td>
</tr>
</tbody>
</table>

**Ports for external servers**

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Details</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>To send SMTP notifications from the Citrix ADM service to users.</td>
<td>Citrix ADM agent to users.</td>
</tr>
<tr>
<td>389/636</td>
<td>TCP</td>
<td>Default port for authentication protocol. For communication between the Citrix ADM service and LDAP external authentication server.</td>
<td>Citrix ADM agent to LDAP external authentication server</td>
</tr>
<tr>
<td>5563</td>
<td>TCP</td>
<td>To receive ADC metrics (counters), system events, and Audit Log messages from Citrix ADC instance to Citrix ADM.</td>
<td>Citrix ADC to Citrix ADM</td>
</tr>
</tbody>
</table>
## Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Details</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>UDP</td>
<td>Default NTP server port for, synchronizing with multiple time sources.</td>
<td>Citrix ADM agent to NTP server</td>
</tr>
<tr>
<td>1812</td>
<td>RADIUS</td>
<td>Default port for authentication protocol. For communication between the Citrix ADM service and RADIUS external authentication server.</td>
<td>Citrix ADM agent to RADIUS external authentication server</td>
</tr>
<tr>
<td>49</td>
<td>TACACS</td>
<td>Default port for authentication protocol. For communication between the Citrix ADM service and TACACS external authentication server.</td>
<td>Citrix ADM agent to TACACS external authentication server</td>
</tr>
</tbody>
</table>

### Note
The endpoint of the Citrix ADM service is the same as the “Service URL” generated while trying to register the agent. The agent uses the Service URL to locate the Citrix ADM.

Ensure that the following endpoint urls are allowed access:

- **Download Service:**

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

- **Trust Service:**
• Service URLs:

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

• ADC backup service:

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

• Citrix Cloud connectivity:

```
1 citrix.cloud.com
2 accounts.cloud.com
3 <!--NeedCopy-->
```

For communication between Citrix ADM agent and Citrix Analytics Service, ensure that the following endpoint urls are allowed access:

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>US Region</th>
<th>EU Region</th>
<th>APS Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Hub</td>
<td><a href="https://cas-ehns-alias.servicebus.windows.net">https://cas-ehns-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns-eu-alias.servicebus.windows.net">https://cas-ehns-eu-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns-aps-alias.servicebus.windows.net">https://cas-ehns-aps-alias.servicebus.windows.net</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://cas-ehns2-alias.servicebus.windows.net">https://cas-ehns2-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns2-eu-alias.servicebus.windows.net">https://cas-ehns2-eu-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns2-aps-alias.servicebus.windows.net">https://cas-ehns2-aps-alias.servicebus.windows.net</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://cas-ehns3-alias.servicebus.windows.net">https://cas-ehns3-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns3-eu-alias.servicebus.windows.net">https://cas-ehns3-eu-alias.servicebus.windows.net</a></td>
<td><a href="https://cas-ehns3-aps-alias.servicebus.windows.net">https://cas-ehns3-aps-alias.servicebus.windows.net</a></td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>US Region</th>
<th>EU Region</th>
<th>APS Region</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cas-eh-ns4-alias.servicebus.windows.net">https://cas-eh-ns4-alias.servicebus.windows.net</a></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Deprecated FQDNs**

Some FQDNs are deprecated for the following use of the Citrix ADM. 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.

<table>
<thead>
<tr>
<th>Citrix ADM Endpoints</th>
<th>Old FQDN</th>
<th>New FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADM UI Access</td>
<td>netscalermas.cloud.com</td>
<td>adm.cloud.com</td>
</tr>
<tr>
<td>Service URL</td>
<td>agent.netscalermgmt.net</td>
<td>*agent.adm.cloud.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The value of * would depend on which PoP (point of presence) your data is available.</td>
</tr>
<tr>
<td>API interactions</td>
<td>netscalermas.cloud.com</td>
<td>api.adm.cloud.com</td>
</tr>
</tbody>
</table>

**Minimum Citrix ADC versions required**

<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>Citrix ADC Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>StyleBooks</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>Monitoring/Reporting and Configuring using Jobs</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>Analytics</td>
<td>10.1 and later</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>10.0.65.31 and later</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>11.0.65.31 and later</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>Citrix ADC Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Insight</td>
<td>11.0.65.31 and later</td>
</tr>
</tbody>
</table>

Requirements for Citrix SD-WAN instance management

Minimum Citrix SD-WAN WANOP versions required

<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>Citrix SD-WAN WANOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring/Reporting and Configuration using Jobs</td>
<td>NetScaler SD-WAN WANOP 7.4.0 and later</td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
</tr>
<tr>
<td>HDX Insight</td>
<td>NetScaler SD-WAN WANOP 7.4.0 and later</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>NetScaler SD-WAN WANOP 7.4.0 and later</td>
</tr>
</tbody>
</table>

Inter-operability matrix of Citrix SD-WAN WANOP platform editions and Citrix ADM features

<table>
<thead>
<tr>
<th>Platform Editions</th>
<th>Discovery</th>
<th>Configuration Monitoring</th>
<th>Monitoring (SNMP Traps)</th>
<th>HDX Insight and WAN Analytics</th>
<th>Multi-Hop Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix SD-WAN WANOP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Thin clients supported for Citrix SD-WAN instances

Citrix ADM 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 TX0 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Application Delivery Management service

- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

**Requirements for Citrix ADM Analytics solution**

**Minimum Citrix Virtual Apps and Desktops versions required**

<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>Citrix Virtual Apps and Desktops Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDX Insight</td>
<td>Citrix Virtual Apps and Desktops 7.0 and later</td>
</tr>
</tbody>
</table>

**Note**


Citrix ADM 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 ADM 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 ADM 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.

<table>
<thead>
<tr>
<th>Citrix ADC License/Duration</th>
<th>5 minutes</th>
<th>1 Hour</th>
<th>1 Day</th>
<th>1 Week</th>
<th>1 Month</th>
</tr>
</thead>
</table>
Supported operating systems and Citrix Receiver versions

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Receiver Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>4.0 Standard Edition</td>
</tr>
<tr>
<td>Linux</td>
<td>13.0.265571 and later</td>
</tr>
<tr>
<td>Mac</td>
<td>11.8, build 238301 and later</td>
</tr>
<tr>
<td>HTML5</td>
<td>1.5*</td>
</tr>
<tr>
<td>Chrome App</td>
<td>1.5*</td>
</tr>
</tbody>
</table>

* Applicable with NetScaler SD-WAN release 7.4 and later.

Licenses

March 17, 2022

Citrix ADM requires a verified Citrix ADM license to manage and monitor the Citrix ADC instances.

The following are the license types supported for Citrix ADM for Service:

<table>
<thead>
<tr>
<th>License type</th>
<th>Entitled to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual server</td>
<td>10 virtual servers and 0.5 GB storage per license</td>
</tr>
<tr>
<td>Storage</td>
<td>5 GB per license</td>
</tr>
<tr>
<td>Express license</td>
<td>Citrix ADM Express account is a default account to manage Citrix ADM resources.</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

With an Express account, you can manage limited Citrix ADM resources. For more information, see Manage Citrix ADM 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 ADM 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.

Note:
ADM licenses are hybrid licenses. You can use these licenses for either on-premises ADM or ADM service.

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 ADM. 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 ADM.

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:

<table>
<thead>
<tr>
<th>License Expiry Information</th>
<th>Count</th>
<th>Days To Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise vCPU</td>
<td>100</td>
<td>362</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>300,000</td>
<td>17</td>
</tr>
<tr>
<td>Standard vCPU</td>
<td>300</td>
<td>382</td>
</tr>
</tbody>
</table>

- **Feature**: Type of license that is going to expire.
- **Count**: Number of instances that are affected.
Citrix Application Delivery Management service

- **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 ADM. For more information, see [Integrate Citrix ADM with ServiceNow instance](#).

   ![How would you like to be notified?]

   c) **Expiry of licenses** - Specify the days before the license expires, when you want to get notified.

**Manage resources using Express account**

March 15, 2022

Citrix ADM Express account is a default account to manage Citrix ADM resources. This account is readily available on Citrix Cloud.
With this account, you can manage up to two virtual servers in Citrix ADM. 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 ADM 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 ADM retains the storage data up to 500 MB or one day data, whichever is the lesser.
- If your Citrix ADM 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 ADM resources:

1. Log on to Citrix Cloud with your credentials.
2. Click **Manage** on the **Citrix ADM** tile.

After your Citrix ADM 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 ADM. To renew your license, you can do one of the following:

- Buy Citrix ADM 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. For more information, see Differences between...
Express and Advance entitlements.

Buy ADM licenses

You can 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**.

1. Select **Buy ADM License**.
2. Select **Microsoft Azure** to buy licenses from Azure Marketplace.

The ADM license image opens in the Azure Marketplace.

3. Review the options and select the suitable ADM service virtual server license.
4. Allocate the licenses to your virtual servers in ADM.
5. Complete your purchase in the Azure Marketplace and return to the ADM GUI.
Upgrade to Citrix ADM Advance account

March 15, 2022

When you log in to Citrix ADM for the first time, Citrix assigns an Express account to manage ADM resources. This account has limited ADM options. However, you can upgrade to the ADM Advance account for unlimited options. These options help you manage, monitor, analyze, orchestrate, automate, and troubleshoot ADC instances.

Buy Citrix ADM license to convert your express account to the Citrix ADM Advance account. This account provides higher storage limit than the express account. You can also use extra SKUs to increase the storage limit. To buy a license, visit Citrix Cloud or contact Technical Support.

Note

After upgrading to an advance account, all your configurations continue as before on the same tenant.

For more information, see Differences between Express and Advance entitlements.

Differences between Express and Advance entitlements

March 15, 2022

The following table explains the differences between the Express and Advance entitlements:

<table>
<thead>
<tr>
<th>Features</th>
<th>Options</th>
<th>Express entitlement</th>
<th>Advance entitlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage limit</td>
<td>NA</td>
<td>500 MB or one day</td>
<td>By default, 500 MB data per virtual server license. For example, if you have two virtual servers, the storage limit becomes 1 GB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data, whichever is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the lesser.</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>Application</td>
<td>Up to two virtual</td>
<td>Entitled for all purchased virtual server licenses.</td>
</tr>
<tr>
<td></td>
<td>Dashboard</td>
<td>servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web Insight</td>
<td>Up to two virtual</td>
<td>Entitled for all purchased virtual server licenses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>servers.</td>
<td></td>
</tr>
<tr>
<td>Features</td>
<td>Options</td>
<td>Express entitlement</td>
<td>Advance entitlement</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Service Graph</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td>Configuration &gt; StyleBooks</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Dashboard</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td>Security Violations</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td>API Gateway</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>WAF Recommendations</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>WAF Learning</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Users and endpoints</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDX Insight</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>Up to two virtual servers.</td>
<td>Entitled for all purchased virtual server licenses.</td>
<td></td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Analytics</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Instances</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>(Instance Advisory)</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Upgrade Advisory and Security Advisory</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>SSL Dashboard</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Network Functions</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Features</th>
<th>Options</th>
<th>Express entitlement</th>
<th>Advance entitlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Reporting</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Pooled licenses</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Configuration &gt; Configuration Jobs, Configuration Templates, and Configuration Advice</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Upgrade Jobs</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

Managing subscriptions

March 15, 2022

Citrix ADM 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 ADM resources that you can manage with the Express account, see Manage resources using 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 ADM licenses, see Differences between Express and Advance entitlements and Citrix ADM.

The following table lists the Citrix licenses that are required to use some of the Citrix ADM features.
<table>
<thead>
<tr>
<th>Citrix ADM Feature Group</th>
<th>Citrix ADM Features</th>
<th>Citrix ADC and Gateway License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics</td>
<td>HDX Insight</td>
<td>Advanced (reporting &lt; 1 hour) Premium (reporting = Unlimited)</td>
</tr>
<tr>
<td>Analytics</td>
<td>Security Insight</td>
<td>Premium (or) Advanced with App Firewall license</td>
</tr>
<tr>
<td>Analytics</td>
<td>Gateway Insight</td>
<td>Advanced (reporting &lt; 1 hour) Premium (reporting = Unlimited)</td>
</tr>
<tr>
<td>Applications</td>
<td>Application Statistics (App Dashboard, App Security Dashboard)</td>
<td>Citrix Web App Firewall related information on App dashboard, and app security dashboard needs Premium (or) Advanced with App Firewall license</td>
</tr>
<tr>
<td>Applications</td>
<td>API gateway</td>
<td>Premium (or) Advanced license</td>
</tr>
<tr>
<td>Applications</td>
<td>StyleBooks</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Inventory Management – Infrastructure Dashboard, Instance groups, Instance dashboards &amp; Sites</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Event Management &amp; Syslog</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Configuration Jobs, Configuration Audit, and Configuration Advice</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Network reporting (Instance level)</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Network reporting (virtual server level)</td>
<td>N/A</td>
</tr>
<tr>
<td>Applications</td>
<td>Network Functions (Plain visibility &amp; Management of virtual servers, services, service groups, server)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
View the subscription details

You can view the licenses installed on your Citrix ADM 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.

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 ADM.
Points to note:

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

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

To disable auto-licensing virtual servers:

1. Navigate to Settings > Citrix ADM 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.

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**.

![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 ADM Licensing & Analytics Config** and click the virtual server type in the **Total Licensed** section in the **Virtual Servers License Summary**.

![Virtual Server Licence Summary](Table)
Apply virtual server licenses manually

You can manually apply licenses to an individual virtual server.

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

The All Virtual Servers page is displayed.

2. Filter unlicensed virtual servers using the property: Licensed: No.

3. Select the virtual server that you want to license.

4. Click License.

Configure policy based virtual server licensing

You can configure a policy to apply license to virtual servers. This policy controls the number of virtual servers you want to auto-license. It also applies licenses to selected instances’ virtual servers only.
Click **Edit Policies** and you can specify the following:

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

- Select the priority ADC instances to apply virtual server licenses. Therefore, the Citrix ADM can apply license to selected instances’ virtual servers only.
Configure auto license support for non-addressable virtual servers

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

Citrix ADM provides an option in Citrix ADM 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](image)

**Note**

- Citrix ADM, 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 ADM.

**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.

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.
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.
Upgrade Advisory

February 15, 2022

As a network administrator, you might manage many ADC instances running on different ADC releases in Citrix ADM. 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 ADM 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 ADM, 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.

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](image)

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.
Citrix Application Delivery Management service

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.

   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.
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 ADM GUI displays the instance files that are present in `/var/mps/mps_images`. Select the image from the Citrix ADM 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**.
• **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 ADM finds unsupported classic policies, you can remove such policies to create an upgrade job.

**Note**

If you specify cluster IP address, the Citrix ADM 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.
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**.
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

**July 26, 2022**

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 ADM 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 ADM 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 ADM 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. For information on CVEs that are not supported, see [Unsupported CVEs in Security Advisory](#).

Points to note

Keep the following points in mind while using security advisory:

- **Instances supported for CVE detection**: all ADC (SDX, MPX, VPX) and Gateway.

- **CVEs supported**: All CVEs after Dec 2019.

  **Note**
  
  The detection and remediation of vulnerabilities impacting the Citrix Gateway plug-in for Windows is not supported by the Citrix ADM Security Advisory. For information on CVEs that are not supported, see [Unsupported CVEs in Security Advisory](#).

- **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 ADM to compare the version of an ADC instance with the versions and builds on which the fix is available. This version comparison helps Citrix ADM 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 ADM 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 ADM to connect with the managed ADC instance, push a script to it, and run the script. The script output helps Citrix ADM 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.

- ADM Security Advisory does not support mitigation. If you have applied mitigation (temporary workaround) to the ADC instance, ADM will still identify the ADC as a vulnerable ADC until you have completed remediation.

**How to use the security advisory dashboard**

To access the Security Advisory dashboard, from the Citrix ADM GUI, navigate to **Infrastructure > Instance Advisory > Security Advisory**. The dashboard shows the vulnerability status of all the ADC instances that you manage through Citrix ADM. The instances are scanned once a week; however, you can scan them anytime by clicking **Scan Now**.

The dashboard includes three tabs:

- Current CVEs
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 ADM 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
• Configure Custom Scan Settings

You can click the **Custom Scan Settings** drop-down to view the additional settings check-box. You have the option of selecting the checkbox and opt out of these Security Advisory Custom scans. The impact of the CVEs that need a custom scan will not be evaluated for your ADC instances in the Security Advisory.
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.
Citrix Application Delivery Management service

**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.

In this screen the number of CVEs impacting your instances is 14 CVEs and the instances that are impacted by these CVEs is one.

The **number of ADC instances are impacted by CVEs** tab shows you all the affected Citrix ADM 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.

<table>
<thead>
<tr>
<th>Current CVEs</th>
<th>Scan Log</th>
<th>CVE Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

MPX & VPX
SNX

- [ ] Click here to search or you can enter key: Value format

<table>
<thead>
<tr>
<th>ID</th>
<th>Vendor</th>
<th>Host Name</th>
<th>Model</th>
<th>Build</th>
<th>Release</th>
<th>Upgrade Required</th>
<th>CVE Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The following releases have reached EOL: 10.8, 10.7, 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.

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
If your ADC instances have customizations, see Upgrade considerations for customized ADC configurations before planning ADC upgrade.

To fix the vulnerability issue, select the ADC instance and apply the recommended remediation. Most of the CVEs need upgrade as a remediation, while others need upgrade and an additional step as remediation.

- For CVE-2020-8300 remediation, see Remediates vulnerabilities for CVE-2020-8300.
- For CVE-2021-22927 and CVE-2021-22920, see Remediates vulnerabilities for CVE-2021-22927 and CVE-2021-22920.
- For CVE CVE-2021-22956, see Identify and remediate vulnerabilities for CVE-2021-22956.
- For CVE CVE-2022-27509, see Remediates vulnerabilities for CVE-2022-27509.

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.
Citrix Application Delivery Management service

The upgrade workflow starts. For more information on how to use Citrix ADM 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.

**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.

**Security Advisory**

Files to scan:

- Default system scans
- On-demand user-initiated scans

ADRM scheduler scan everyday. You can also run an on-demand scan using the scan menu option. Scan does not alter any configuration, or impact the resource utilization or affect production traffic.

© 1999‒2022 Citrix Systems, Inc. All rights reserved.
Citrix Application Delivery Management service

**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 06:30:21 Local Time
- Scheduled Scan: May 03, 2021 01:56:00 Local Time

ADM schedules a scan every 7 days. 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.

**Current CVEs**

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>VULNERABILITY TYPE</th>
<th>PUBLICATION DATE</th>
<th>SEVERITY</th>
<th>REMEDIATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-8190</td>
<td>Local elevation of privileges</td>
<td>Jul 07, 2020</td>
<td>Medium</td>
<td>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</td>
</tr>
<tr>
<td>CVE-2019-8177</td>
<td>Denial of service</td>
<td>Jul 07, 2020</td>
<td>Medium</td>
<td>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</td>
</tr>
<tr>
<td>CVE-2019-8190</td>
<td>Local elevation of privileges</td>
<td>Jul 07, 2020</td>
<td>Medium</td>
<td>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</td>
</tr>
<tr>
<td>CVE-2019-8196</td>
<td>Information disclosure</td>
<td>Jul 07, 2020</td>
<td>Low</td>
<td>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</td>
</tr>
<tr>
<td>CVE-2019-8197</td>
<td>Elevation of privileges</td>
<td>Jul 07, 2020</td>
<td>Critical</td>
<td>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</td>
</tr>
</tbody>
</table>

**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 ADM takes a few minutes to complete the scan.

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.
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 ADM GUI.

Remediate vulnerabilities for CVE-2020-8300

February 15, 2022

In the Citrix ADM 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.
Citrix Application Delivery Management service

### Current CVEs

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Publication Date</th>
<th>Severity</th>
<th>Vulnerability Type</th>
<th>Affected ADC PVS</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-8300</td>
<td>Jun 08, 2021</td>
<td>High</td>
<td>Session Hijacking</td>
<td>1</td>
<td>Upgrade Vulnerable ADC instance to ADC release 13.0.58.30 or 12.1.57.18 to remediate the vulnerability 📢</td>
</tr>
<tr>
<td>CVE-2020-8190</td>
<td>Jul 07, 2020</td>
<td>Critical</td>
<td>Stored Cross Site Scripting (XSS)</td>
<td>3</td>
<td>Upgrade Vulnerable ADC instance to ADC release 13.0.58.30 or 12.1.57.18 to remediate the vulnerability 📢</td>
</tr>
<tr>
<td>CVE-2020-8189</td>
<td>Jul 07, 2020</td>
<td>High</td>
<td>Local elevation of privileges</td>
<td>3</td>
<td>Upgrade Vulnerable ADC instance to ADC release 13.0.58.30 or 12.1.57.18 to remediate the vulnerability 📢</td>
</tr>
<tr>
<td>CVE-2020-8245</td>
<td>Sep 17, 2020</td>
<td>Medium</td>
<td>An HTML injection attack against the SSL VPN web portal</td>
<td>3</td>
<td>Upgrade Vulnerable ADC instance to ADC release 13.0.64.30 or 12.1.58.15 to remediate the vulnerability 📢</td>
</tr>
</tbody>
</table>

These CVEs are impacting your ADC instances. Upgrading these ADC instances to the latest recommended release / build will remediate most of the vulnerabilities.

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.
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.

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.
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.

For more information on how to use Citrix ADM to upgrade ADC instances, see Create an ADC upgrade job.
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.

Keep the following points in mind before you select an instance and click `Proceed to configuration job workflow`:

- For an ADC instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click `Proceed to configuration job workflow`, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under `Security Advisory Template` manually to the config job pane on the right side.

- For multiple ADC instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you’ve ADC 1, ADC 2, and ADC 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click `Proceed to configuration job workflow`, and the built-in configuration template auto-populates under `Select configuration`. Refer to the known issue NSADM-80913 in the `release notes`.

- For multiple ADC instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each ADC at a time: when you select these instances and click `Proceed to configuration job workflow`, an error message appears telling you to run the config job on each ADC at a time.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration template auto-populates under `Select configuration`. 
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.

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.
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`.

---

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 $saml_profile_patset$
2 SSH ➔ bind patset $saml_profile_patset$ "$saml_profile_url1$
3 SSH ➔ set samlidPProfile $saml_profile_name$ protocol AAA.LOGIN.RELAYSTATE.REQUIRES_HTTP "$saml_profile_url1$
4 SSH ➔ add patset $saml_profile_patset$
5 SSH ➔ bind patset $saml_profile_patset$ "$saml_profile_url2$
6 SSH ➔ set samlidPProfile $saml_profile_name$ protocol AAA.LOGIN.SAML.REQ.ACS.ROLEراس التأكيد التلقائي "$saml_profile_url2$
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 the 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`.

**Step 2: Select the instance**

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.

**Create Job**

- **Select Configuration**
- **Select Instances**
- **Specify Variable Values**
- **Job Preview**
- **Execute**

Select the nodes on which the job to be executed. This setting is applicable only for ADC HA Pair instances. If more 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.

<table>
<thead>
<tr>
<th>INSTANCE</th>
<th>HOST NAME</th>
<th>STATE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Up</td>
<td>NetScaler NS11.0 Build 83.0.0</td>
</tr>
</tbody>
</table>

**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 in this format `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: enter the same of the SAML profile for which you are configuring the job
Citrix Application Delivery Management service

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.

#### 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.
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 ADM Express account**

The Citrix ADM Express account has limited features, which include limitations of two configuration jobs only. To know more about Citrix ADM Express account, see [Manage Citrix ADM 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 ADM 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 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 the following configuration:

<table>
<thead>
<tr>
<th>Two SAML actions</th>
<th>Two SAML profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML action 1 has one domain, and SAML action 2 has two domains</td>
<td>SAML profile 1 has one URL, and SAML profile 2 has two URLs</td>
</tr>
</tbody>
</table>

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.
The following tables list the variable definitions for customized parameters.

Table 1. Variable definitions for SAML action

<table>
<thead>
<tr>
<th>ADC configuration</th>
<th>Variable definition for patset</th>
<th>Variable definition for SAML action name</th>
<th>Variable definition for domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML action 1 has one domain</td>
<td>saml_action_patset1</td>
<td>saml_action_name1</td>
<td>saml_action_domain1</td>
</tr>
<tr>
<td>SAML action 2 has two domains</td>
<td>saml_action_patset2</td>
<td>saml_action_name2</td>
<td>saml_action_domain2, saml_action_domain3</td>
</tr>
</tbody>
</table>

Table 2. Variable definitions for SAML profile

<table>
<thead>
<tr>
<th>ADC configuration</th>
<th>Variable definition for patset</th>
<th>Variable definition for SAML profile name</th>
<th>Variable definition for URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML profile 1 has one URL</td>
<td>saml_profile_patset1</td>
<td>saml_profile_name1</td>
<td>saml_profile_url1</td>
</tr>
<tr>
<td>SAML profile 2 has two URLs</td>
<td>saml_profile_patset2</td>
<td>saml_profile_name2</td>
<td>saml_profile_url2, saml_profile_url3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml_action_set1</td>
<td>pat1</td>
</tr>
<tr>
<td>saml_action_domain1</td>
<td><a href="https://d1.com/">https://d1.com/</a></td>
</tr>
<tr>
<td>saml_action_name1</td>
<td>samlSPAct1</td>
</tr>
<tr>
<td>saml_action_set2</td>
<td>pat2</td>
</tr>
<tr>
<td>saml_action_domain2</td>
<td><a href="https://d2.com/">https://d2.com/</a></td>
</tr>
<tr>
<td>saml_action_domain3</td>
<td><a href="https://d3.com/">https://d3.com/</a></td>
</tr>
<tr>
<td>saml_action_set2</td>
<td>samlSPAct2</td>
</tr>
<tr>
<td>saml_profile_set1</td>
<td>pat3</td>
</tr>
<tr>
<td>saml_profile_url1</td>
<td><a href="https://example1.com/cgi/samlautl">https://example1.com/cgi/samlautl</a></td>
</tr>
<tr>
<td>saml_profile_name1</td>
<td>samDPProf2</td>
</tr>
<tr>
<td>saml_profile_set2</td>
<td>pat4</td>
</tr>
<tr>
<td>saml_profile_url2</td>
<td><a href="https://example2.com/cgi/samlau">https://example2.com/cgi/samlau</a></td>
</tr>
<tr>
<td>saml_profile_url3</td>
<td><a href="https://example3.com/cgi/samlau">https://example3.com/cgi/samlau</a></td>
</tr>
<tr>
<td>saml_profile_name2</td>
<td>samDPProf2</td>
</tr>
</tbody>
</table>
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 ADM security advisory can help you identify and remediate CVE-2020-8300.

**Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920**

July 29, 2022

In the Citrix ADM 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.
Note

It might take a couple of hours for the 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.
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.

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**.

**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.
For more information on how to use Citrix ADM 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.

Keep the following points in mind before you select an instance and click Proceed to configuration
job workflow:

- For an ADC instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click Proceed to configuration job workflow, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under Security Advisory Template manually to the config job pane on the right side.

- For multiple ADC instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you’ve ADC 1, ADC 2, and ADC 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click Proceed to configuration job workflow, and the built-in configuration template auto-populates under Select configuration. Refer to the known issue NSADM-80913 in the release notes.

- For multiple ADC instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each ADC at a time: when you select these instances and click Proceed to configuration job workflow, an error message appears telling you to run the config job on each ADC at a time.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under Select configuration.

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
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.

<table>
<thead>
<tr>
<th>ADC 1</th>
<th>ADC 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job 1: two SAML actions</td>
<td>Job 2: two SAML actions</td>
</tr>
</tbody>
</table>

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.

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.
Citrix Application Delivery Management service

- **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 example](image)

Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.

![Select Job](image)

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
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.
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
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.

The following table lists the variable definitions for customized parameters.

<table>
<thead>
<tr>
<th>Table. Variable definitions for SAML action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC configuration</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>SAML action 1 has one domain</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>ADC configuration</th>
<th>Variable definition for patset</th>
<th>Variable definition for SAML action name</th>
<th>Variable definition for domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML action 2 has two domains</td>
<td>saml_action_patset2</td>
<td>saml_action_name2</td>
<td>saml_action_domain2, saml_action_domain3</td>
</tr>
</tbody>
</table>

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.

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.

**Identify and remediate vulnerabilities for CVE-2021-22956**

August 1, 2022

In the Citrix ADM security advisory dashboard, under **Current CVEs > number of** ADC instances are impacted by common vulnerabilities and exposures (CVEs), you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2021-22956 impacted instances, select CVE-2021-22956 and click **View Affected Instances**.
The <number> of ADC instances impacted by CVEs window appear. Here you see the count and details of the ADC instances impacted by CVE-2021-22956.

Note

It might take some time for security advisory system scan to conclude and reflect the impact of CVE-2021-22956 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking Scan-Now.

Identify CVE-2021-22956 impacted instances

CVE-2021-22956 requires a custom scan, in which ADM service connects with the managed ADC instance, pushes a script to the instance. The script runs on the ADC instance and checks the Apache configuration file (httpd.conf file) and maximum client connections (maxclient) parameters to determine if an instance is vulnerable or not. The information the script shares with ADM service is the vulnerability status in Boolean (true or false). The script also gives back to ADM service a list of counts for max_clients for different network interfaces, for example local host, NSIP, and SNIP with management access. You can see a detailed report of this list in the CSV file that you can download.
Citrix Application Delivery Management service

from the **Scan Logs** tab on **Security Advisory** page.

This script runs every time your scheduled on-demand scans run. After the scan is completed, the script is deleted from the ADC instance.

**Remediate CVE-2021-22956**

For CVE-2021-22956-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.

**Security Advisory**

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.

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.

**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.
Citrix Application Delivery Management service

For more information on how to use Citrix ADM 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 the instance impacted by CVE-2021-2295 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.

Keep the following points in mind before you select an instance and click Proceed to configuration job workflow:

- For an ADC instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click Proceed to configuration job workflow, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under Security Advisory Template manually to the config job pane on the right side.

- For multiple ADC instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you’ve ADC 1, ADC 2, and ADC 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click Proceed to configuration job workflow, and the built-in configuration template auto-populates under Select configuration. Refer to the known issue NSADM-80913 in the release notes.

- For multiple ADC instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each ADC at a time: when you select these instances and click Proceed to configuration job workflow, an error message appears telling you to run the config job on each ADC at a time.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under Select configuration.
Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.

**Note**

For ADC instances in cluster mode, using ADM security advisory, ADM supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

`rc.netcaler` is synced across all HA and cluster nodes, making the remediation persistent after each restart.

Step 3: Specify variable values
Enter the variable values.

**Create Job**

Select one of the following options to specify variables for your instances:

- **Common variable values for all instances**: Enter a common value for the variable `max_client`.
- **Upload input file for variables values**: Click Download Input Key File to download an input file. In the input file, enter values for the variable `max_client` and then upload the file to the ADM server. Refer to the known issue NSADM-80913 in the release notes notes about an issue with this option.

**Note**

For both options mentioned above, the recommended `max_client` value is 30. You can set the value according to your present value. However, it should not be zero, and it should be less than or equal to the `max_client` set in the `/etc/httpd.conf` file. You can check the present value set in the Apache HTTP Server configuration file `/etc/httpd.conf` by searching the string `MaxClients`, in the ADC instance

**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.

After completing the two remediation steps for all vulnerable ADCs, you can run an on-demand scan to see the revised security posture.
Identify and remediate vulnerabilities for CVE-2022-27509

July 29, 2022

In the Citrix ADM security advisory dashboard, under **Current CVEs** ADC instances are impacted by CVEs, you can see all the instances vulnerable due to CVE-2022-27509. To check the details of the instances impacted by the CVEs, select CVE-2022-27509 and click **View Affected Instances**.

Note

To understand the reason for ADC vulnerability, download the CSV report in Scan logs tab in Security Advisory.

The **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-2022-27509.

For more information about the security advisory dashboard see, **Security Advisory**.
Citrix Application Delivery Management service

**Note**

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2022-27509 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

**Identify CVE-2022-27509 impacted instances**

CVE-2022-27509 requires a combination of custom scan and version scan. As part of the custom scan, ADM service connects with the managed ADC instance and pushes a script to the instance. The script runs on the ADC instance and determines if the instance is vulnerable. This script runs every time your scheduled or on-demand scan runs.

After the scan is completed, the script is deleted from the ADC instance.

You can also opt out of these Security Advisory Custom scans. For more information on Custom Scan Settings and opting out of custom scans, see the **Configure Custom Scan settings** section on the **Security Advisory** page.

**Remediate CVE-2022-27509**

For CVE-2022-27509 impacted ADC instances, the remediation is a single step process and you need to upgrade the vulnerable ADC instances to a release and build that has the fix. In the GUI, under **Current CVEs > ADC instances are impacted by CVEs**, you can see the step to remediate.

Under **Current CVEs> ADC instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

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.

**IMPORTANT**

If your vulnerable ADC instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, see **Upgrade considerations for customized ADC configurations** before planning ADC upgrade.

For more information on how to use Citrix ADM to upgrade ADC instances, see **Create an ADC upgrade job**.
Unsupported CVEs in Security Advisory

April 12, 2022

Citrix ADM security advisory tracks all the new Common Vulnerabilities and Exposures (CVEs) and assesses the impact of CVEs on the infrastructure. You can review the recommendations and take appropriate actions. However, there are a few CVEs that are not supported and the detection and remediation of the vulnerabilities are out of Citrix ADM Security Advisory scope.

- **CVE-2022-21827:**


  The detection and remediation of vulnerabilities impacting the Citrix Gateway plug-in for Windows is not supported by the Citrix ADM. Also, Citrix Gateway plug-in vulnerabilities cannot be assessed by performing any checks on ADC side, verifying the ADC version, or by checking the ADC configuration. The detection & remediation for this CVE can only be assessed based on the version of the Citrix Gateway plug-in for Windows deployed on the client.

  As a result, the detection and remediation of this vulnerability is out of Citrix ADM Security Advisory scope.

**Setting up**

February 15, 2022

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 ADM 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 ADM. To monitor syslog events, you need to first configure Citrix ADM as the syslog server for your Citrix ADC instance.

• **Configuring role-based access control.** Citrix ADM provides fine-grained, role-based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise.

• **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

February 15, 2022

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.**
Citrix Application Delivery Management service

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.

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 ADM 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 ADM Agent on Microsoft Azure Cloud.
- For instructions about installing an agent on AWS, see Installing Citrix ADM Agent on AWS.
Configure agents for multisite deployment

February 15, 2022

Agents work as an intermediary between the Citrix ADM and the discovered instances across different data centers and public clouds. Citrix ADM 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 ADM. Agent does the first level of data processing and sends the processed data in compressed format to the Citrix ADM 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:
The public cloud has four ADC instances and two Citrix ADM agents. The enterprise data center also have four ADC instances and two Citrix ADM 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 ADM in a compressed format. Agents communicate with the Citrix ADM server over a secure channel.

On public cloud, when **Citrix ADM Agent 1** becomes inactive (DOWN state), agent failover occurs. Citrix ADM redistributes the ADC instances of **Citrix ADM Agent 1** with **Citrix ADM 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 ADM agent, see **Install the Citrix ADM Agent**.

**Citrix ADM 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 ADM redistributes the ADC instances of the inactive agent with other active agents.

**Important**

- Citrix ADM 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 ADM features**.
- If an agent is running a script, ensure that script is present on all the agents in the site. Therefore, the changed agent can run the script after agent failover.

To attach a site to an agent in the Citrix ADM 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 ADM 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 ADM detects it and displays the state as down.

When a Citrix ADM agent becomes inactive (Down state) in a site, Citrix ADM waits for few minutes for the agent to become active (Up state). If the agent remains inactive, Citrix ADM automatically redistributes the instances among available agents in the same site. This redistribution may take approximately 10-15 minutes.
Citrix Application Delivery Management service

Citrix ADM 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**

February 15, 2022

In Citrix ADM, agents running on software version 12.0 build 507.110 and later are automatically upgraded to newer and recommended versions by Citrix ADM. 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**.

![Agent Upgrade Screen](image)

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**.
Citrix Application Delivery Management service

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 ADM 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

Click **Save** to save your settings. These settings persist for future agent upgrades until you change the settings.

**Dual NIC support on Citrix ADM**

August 16, 2022

You can configure two NICs on an ADM agent. Using the Dual NIC architecture, ADM agent will be able to:

- Establish communication between ADM agent and ADC instances - You can use the first NIC to isolate the traffic that is received and sent through the Citrix ADM and also to communicate between Citrix ADM and its managed Citrix ADC instances in another network.

- Establish communication between ADM agent and ADM service - You can use the second NIC to manage the ADM service that is on a network and perform administrative tasks

**Note**

You cannot interchange the functionality and configuration of both the NICS.
In this scenario, as an administrator, you can:

- Configure IP address for the traffic between Citrix ADM and its managed Citrix ADC instances.
- Configure IP address for managing the Citrix ADM software to perform all administrative tasks in the software.

**Note**

It is not mandatory to configure Dual NICs for an ADM agent. It is optional and is required only when traffic between ADM agent, ADM Service and ADCs needs to be separated.

**Prerequisites**

- Ensure you have deployed and configured Citrix ADM agent on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).
- Ensure you have added the second NIC on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).

To assign an IP address to a NIC on a Citrix Hypervisor and create a secondary interface, see Assign an IP Address to a NIC.

**Modify the IPV4 NIC network addresses**

1. Open an SSH connection to the Citrix ADM agent console by using an SSH client, such as PuTTY.
2. Log in using the `nsrecover/nsroot` credentials and switch to the shell prompt.
3. Run the command `ifconfig`. You can see the details of the two NICs that you have configured -
   - NIC 1 – For communication between ADM Agent to ADC Communication
   - NIC 2 – For communication between ADM Agent to ADM service
4. Run the command `networkconfig`. A menu appears which allows you to set or modify the IPV4 network addresses.

```
bash-3.2# /mps/networkconfig

Citrix ADM Agent initial network configuration.  
This menu allows you to set and modify the initial IPv4 network addresses.  
The current value is displayed in brackets [()].  
Selecting the listed number allows the address to be changed.  

1. Citrix ADM Agent Host Name [ns]:  
2. Citrix ADM Agent IPv4 address [10.102.103.247]:  
3. Netmask [255.255.255.0]:  
4. Gateway IPv4 address [10.102.103.1]:  
5. DNS IPv4 Address [10.102.166.70]:  
6. Second NIC IPv4 address [10.102.103.250]:  
7. Second NIC Netmask [255.255.255.0]:  
8. Second NIC Network address [10.102.103.251, 10.102.103.252, 10.102.103.252]:  
9. Second NIC Gateway IPv4 address [10.102.103.2]:  
10. Cancel and quit.  
11. Save and quit.  
```

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second NIC Network address can take multiple IP values.</td>
</tr>
</tbody>
</table>

5. Select a menu item to modify. Save and quit the settings.
Adding instances

February 15, 2022
You can add instances either while setting up the Citrix ADM for the first time or later.

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

- 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 ADM 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 ADM after adding the instances in the Citrix ADM. To access the Citrix ADC instances from the Citrix ADM, 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 ADM, 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 ADM
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 ADM, that agent is selected by default.

---

**To add Citrix ADC CPX instance in Citrix ADM**

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 ADM agent from the list of agents.

9. Click OK to initiate the process of adding instances to Citrix ADM.
   
   **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 ADM

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 ADM agent to which you want to associate the instance.
   If there is only one agent configured on your Citrix ADM, that agent is selected by default.

10. Click OK.
To add high-availability Citrix ADC BLX instances in Citrix ADM

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 ADM agent to which you want to associate the instance.

    If there is only one agent configured on your Citrix ADM, that agent is selected by default.

11. Click **OK**.
To access an instance GUI from the Citrix ADM

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.

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 ADM.

  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

February 15, 2022

You can add an HAProxy instance provisioned on a host by providing the details of the host while setting up the Citrix ADM for the **first time** or later.

Citrix ADM supports HAProxy version 1.6.3 or later and you can add HAProxy instances provisioned on the following hosts to Citrix ADM:

- 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 ADM 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 ADM, Citrix ADM accesses the host using SSH protocol. It automatically discovers the HAProxy instances provisioned on the host and adds them to Citrix ADM 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 ADM:

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.

Alternatively, navigate to Infrastructure > Instances. Under Instances, select HAProxy and
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 ADM 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.

---

**Configuring syslog on instances**

February 15, 2022

The syslog protocol provides a transport to allow the Citrix ADC instances to send event notification messages to Citrix ADM, 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 ADM. To monitor syslog events, you need to first configure Citrix ADM as the syslog server for your Citrix ADC instance. After the instance is configured, all the syslog messages are redirected to Citrix ADM, 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 ADM, 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 ADM, navigate to Infrastructure > Instances.
2. Select the Citrix ADC instance from which you want the syslog messages to be collected and displayed in Citrix ADM.
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 ADM starts receiving the syslog messages. You can view the messages by navigating to Infrastructure > Events > Syslog Messages.

Logstream overview

February 15, 2022

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 ADM. 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 ADM.

- 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 ADM. 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 ADM 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...
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**.

3. Select the virtual servers and then click **Enable Analytics**.

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**, **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**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights.
you can select either **Logstream** or **IPFIX** as the transport mode.

c) The Expression is true by default

d) Click **OK**

The following table describes the features of Citrix ADM that supports **Logstream** as the transport mode:

<table>
<thead>
<tr>
<th>Feature</th>
<th>IPFIX</th>
<th>Logstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Insight</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Security Insight</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
How to assign more permissions to delegated admin users

February 15, 2022

When the first user of your organization signs up and logs on to Citrix ADM, 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 ADM 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.
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 ADM 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.
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.
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.”
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`. 
Integration with the ServiceNow instance

February 15, 2022

When you want to enable ServiceNow notifications for Citrix ADC events and Citrix ADM events, you must integrate Citrix ADM with the ServiceNow instance. To integrate Citrix ADM with the ServiceNow instance, use Citrix ITSM connector. The ITSM connector establishes the communication between Citrix ADM and the ServiceNow instance. For more information, see How ITSM Adapter works.

Perform the following steps to integrate Citrix ADM 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.

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 ADM.

   a) Log in to Citrix ADM.
   
   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 ADM 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 ADM GUI:

**Important**

This feature is supported on ServiceNow Cloud.

- **Citrix ADC events**: Citrix ADM 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 ADM by navigating to **Infrastructure > Events > Rules**. For more information, see **Send ServiceNow notifications**.

- **The SSL certificate and Citrix ADM license events**: Citrix ADM can generate the ServiceNow incidents for the SSL certificate expiry and Citrix ADM license expiry events.
  
  To send ServiceNow notifications for an SSL certificate expiry, see **The SSL certificate expiry**.
  
  To send ServiceNow notifications for an Citrix ADM license expiry, see **The Citrix ADM license expiry**.

### A unified dashboard to view instance key metric details

August 16, 2022

In Citrix ADM, you can view various insights about the usage and performance of applications, ADC infrastructure, security (Bot and WAF) violations, and so on. As an administrator, you might have to navigate to various options in the ADM GUI to view multiple insights. For example, to check the virtual servers (applications) and ADC instance insights:

- You must first navigate to **Applications > Dashboard** to view insights for applications.
- Then you must navigate to **Infrastructure > Infrastructure Analytics** to view insights for ADC instances.

For a better monitoring experience, it is necessary for you to have a privilege that contains an overview of all the required insights. Navigate to **Overview > Dashboard** to visualize a single-pane dashboard with an overview of the key metrics details based on the following categories:

- Applications
- ADC Infrastructure
- Application security
- Gateway

**Applications**

Under **Applications**, you can view:

- **Application Health** – Provides an overview of applications that are in **Down** and **Out-of-Service**, and based on their status such as **Critical**, **In Review**, **Good**, and **Not Applicable**. Click **View All Applications** to view details in App Dashboard.
• **Golden Signal Anomalies** – Provides an overview of applications that have server errors and response time anomalies. Click **View Details** for more information.

• **Application Config Optimization** – Provides an overview of total applications that have performance issues. Click **See More** to view issue details in app dashboard.

• **SSL Certificates** – Provides an overview of SSL certificates along with their validity. Click **Manage SSL Certificates** to view more information in SSL dashboard.

• **Application SSL Config Optimization** – Provides an overview of total applications that have SSL related issues. Click **See More** to view issue details.

---

**ADC Infrastructure**

Under **ADC Infrastructure**, you can view the following ADC instance related key metrics:

• **ADC Instance Health** – Provides an overview of total ADC instances based on the instance score.

• **ADC Instances impacted by CVEs** – Provides an overview of total ADC instances that are impacted with Common Vulnerabilities and Exposures (CVEs). For more information, see **Security Advisory**.

• **ADC Instance Issues** – Provides an overview of ADC instance issues depending upon the issue category. For more information, see **Infrastructure Analytics**.

• **ADC Instance Upgrade Summary** – Provides an overview of total ADC instances that are not on the latest build. Click View ADC Instances Dashboard for more information.
Citrix Application Delivery Management service

**Application Security**

Provides an overview of total affected applications and total violations (Bot and WAF) reported for the selected duration. Click **View Security Dashboard** to view the security and bot violation details.

**Gateway**

Provides an overview of total active gateway users, total active ICA users, and total active ICA connections. You can also view errors, user log on details, and a geo map that provides details on the user locations.
Customize dashboard

You can use the Edit dashboard option and customize the dashboard based on your choice. Using the Edit dashboard option, you can:

- Drag widgets
- Remove widgets
- Add widgets
- Reset to default

After making changes, click Save.

Note

By default, all widgets are displayed. If you have customized the dashboard, saved the changes, and use the Reset to default option, the last saved customized dashboard is restored.

View agent details

In the unified dashboard, you can visualize an overview of ADM agent details. In Overview > Dashboard, next to the ADM Agent Status, you can view the following status that enables you to analyze the overall agent availability:
Citrix Application Delivery Management service

- **All available.** Indicates all agents are up and running.
- **All unavailable.** Indicates all agents are down and not accessible.
- **[number of agents] unavailable.** Indicates a few agents are down and not accessible.
- **All out of service.** Indicates all agents are in out of service.
- **[number of agents] out of service.** Indicates a few agents are in out of service.
- **External agent not found.** Indicates no agent (through any hypervisors) is configured.

Click **View Details** to visualize an overview of ADM agent details such as total in-built agents, total external agents, agent IP, status, system usage, diagnostic checks, and so on.

**ADM agent details**

ADM agent ensures communication between Citrix ADC instances and Citrix ADM. For all the features to work on ADM, it is essential for agent to be up and available.

Note: ADC instances that are connected to agents with are down will continue to work in 30 day grace period but no other ADM feature would work while agent remains Down. Follow the diagnostics feedback.

<table>
<thead>
<tr>
<th>Total In-built agents</th>
<th>ADCs managed via in-built agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**External agent status**

<table>
<thead>
<tr>
<th>Total external agents</th>
<th>Down</th>
<th>Out of servcie</th>
<th>Up</th>
<th>ADCs managed via external agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>110</td>
</tr>
</tbody>
</table>

**Details (8)**

<table>
<thead>
<tr>
<th>ADM AGENT IP</th>
<th>AVAILABILITY STATUS</th>
<th>ADC MANAGED VIA AGENT</th>
<th>SYSTEM USAGE (%)</th>
<th>DIAGNOSTICS FEEDBACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.100.1</td>
<td>Down</td>
<td></td>
<td></td>
<td>View recommendation</td>
</tr>
</tbody>
</table>

**Applications**

February 15, 2022

The application analytics and management feature of Citrix ADM enables you to monitor the applications through application-centric approach. This approach helps you to:
Citrix Application Delivery Management service

- 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 ADM
- 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 ADM enables you to add licenses for up to 2 applications. Depending upon your license, you can select and apply licenses for the applications that you want to monitor.

Microservices applications

In a Kubernetes cluster, 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

February 15, 2022

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:

<table>
<thead>
<tr>
<th>Applications</th>
<th>Clients</th>
<th>Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application with Response Time Anomalies</td>
<td>Clients</td>
<td>Instance Metrics</td>
</tr>
<tr>
<td>Applications</td>
<td>Geo Locations</td>
<td>Applications</td>
</tr>
<tr>
<td>Servers</td>
<td>HTTP Request Methods</td>
<td>Domains</td>
</tr>
<tr>
<td>Domains</td>
<td>HTTP Response Status</td>
<td>URLs</td>
</tr>
<tr>
<td>Geo Locations</td>
<td>URLs</td>
<td>HTTP Request Methods</td>
</tr>
<tr>
<td>Applications</td>
<td>Clients</td>
<td>Instances</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>URLs</td>
<td>Operating System</td>
<td>HTTP Response Status</td>
</tr>
<tr>
<td>HTTP Request Methods</td>
<td>Browsers</td>
<td>Clients</td>
</tr>
<tr>
<td>HTTP Response Status</td>
<td>SSL Errors</td>
<td>Servers</td>
</tr>
<tr>
<td>SSL Errors</td>
<td>SSL Usage</td>
<td>Operating System</td>
</tr>
<tr>
<td>SSL Usage</td>
<td></td>
<td>Browsers</td>
</tr>
</tbody>
</table>
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 ADM displays the RTT values as

- **NA** – Displays when the ADC instance cannot calculate the RTT.
- **<1ms** – Displays when the ADC instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

**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.

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
Click the **SSL Cipher name** to see the application and client details.
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.

   The metrics details for the selected server are displayed.

2. Select the Server Network Latency tab to analyze the latency.

   The average latency indicates 10.01s 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.
Analyse the root cause for application slowness

February 15, 2022

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 ADM 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.

<table>
<thead>
<tr>
<th>Application</th>
<th>Total Anomalies and Contributors</th>
<th>Response Time Range</th>
<th>Maximum Anomalous Response Time</th>
<th>Maximum Anomaly Contributor</th>
</tr>
</thead>
<tbody>
<tr>
<td>as_1xserver</td>
<td>112 (Client Network Latency: 25, Server Network Latency: 40, Server Processing Time: 48)</td>
<td>1.37 s</td>
<td>1.7 m</td>
<td>Server processing time</td>
</tr>
</tbody>
</table>

- **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.

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.
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.

The Recommended Actions suggest you the possible resolutions for the anomalies.
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.

---

**Service Graph**

February 15, 2022

The service graph feature in Citrix ADM enables you to monitor all services in a graphical representation. This feature also enables you to view a detailed analysis and actionable metrics of the services. 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
Citrix Application Delivery Management service

- 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 ADM, you can analyze the root cause of issues and take necessary troubleshooting actions faster. Service graph displays your applications into various component services. These services running inside the Kubernetes cluster can communicate with various components within and outside the application. To get started, see Setting up service graph.

**Service graph for 3-tier Web applications**

Navigate to Applications > Service Graph and click the Web Apps tab to view:

- Details on how the application is configured (with content switching virtual server and load balancing virtual server)
  
  For GSLB applications, you can view data center, ADC instance, CS, and LB virtual servers.

- End-to-end transactions from client to service

- The location from where the client is accessing the application

- The data center name where the client requests are processed and the associated data center
  
  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 ADM displays the service status based on service response time and error count.
  
  - **Critical (red)** - Indicates when average service response time > 200 ms AND error count > 0
  
  - **Review (orange)** - Indicates when average service response time > 200 ms OR error count > 0
  
  - **Good (green)** - Indicates no error and average service response time < 200 ms

- The client status such as Critical, Review, and Good. Citrix ADM displays the client status based on client network latency and error count.
  
  - **Critical (red)** - Indicates when average client network latency > 200 ms AND error count > 0
  
  - **Review (orange)** - Indicates when average client network latency > 200 ms OR error count > 0
Citrix Application Delivery Management service

- **Good (green)** - Indicates no error and average client network latency < 200 ms
  - The virtual server status such as **Critical**, **Review**, and **Good**. Citrix ADM displays the virtual server status based on the app score.
    - **Critical (red)** - Indicates when app score < 40
    - **Review (orange)** - Indicates when app score is between 40 and 75
    - **Good (green)** - Indicates when app score is > 75

**Points to note:**

- Only Load Balancing, Content Switching, GSLB virtual servers are displayed in service graph.
- If no virtual server is bound to a custom application, the details are not visible in service graph for the application.
- You can view metrics for clients and services in service graph only if active transactions occur between virtual servers and web application.
- If no active transactions available between virtual servers and web application, you can only view details in service graph based on the configuration data such as load balancing, content switching, GSLB virtual servers, and services.
- If any changes made in the application configuration, it may take 10 minutes to reflect in service graph.

For more information, see [Service graph for applications](#).

**StyleBooks**

February 15, 2022

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 ADM 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 ADM determines the correct order based on their computed dependencies.

- **Atomic**: When you use StyleBooks to deploy configurations, the full configuration is deployed or none of it is deployed and this ensures that the infrastructure is always left in a consistent state.

- **Versioned**: A StyleBook has a name, namespace, and a version number that uniquely distinguishes it from any other StyleBook in the system. Any modification to a StyleBook requires an update to its version number (or to its name or namespace) to maintain this unique character. The version update also allows you to maintain multiple versions of the same StyleBook.

- **Composable**: After a StyleBook is defined, the StyleBook can be used as a unit to build other StyleBooks. You can avoid repeating common patterns of configuration. It also allows you to establish standard building blocks in your organization. Because StyleBooks are versioned, changes to existing StyleBooks results in new StyleBooks, therefore ensuring that dependent StyleBooks are never unintentionally broken.

- **App-Centric**: StyleBooks can be used to define the 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 ADM auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the Citrix ADM GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.

- **API-driven**: All configuration operations are supported by using the Citrix ADM GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

You can use one StyleBook to create multiple configurations. Each configuration is saved as a config pack. For example, consider that you have a StyleBook that defines a typical HTTP load balancing application configuration. You can create a configuration with values for the load balancing entities and 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 ADM and on the ADC instance on which the configuration is run.

You can either use default StyleBooks, shipped with Citrix ADM, to create configurations for your deployment, or design your own StyleBooks and import them to Citrix ADM. You can use the StyleBooks to create configurations either by using the Citrix ADM GUI or by using APIs.

This document includes the following information:
How to view StyleBooks
Default StyleBooks
StyleBooks developed for business applications
Custom StyleBooks
APIs in StyleBooks
StyleBooks grammar

Application Security Dashboard

February 15, 2022

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:

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 ADM 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

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.
You can also click the **Settings** option to select the options that you want to get it displayed.

### Safety index details

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application safety index summary.

The safety index summary gives you information about the effectiveness of the following security configurations:

- **Application Firewall Configuration.** Shows how many signature and security entities are not configured.

- **Citrix ADM System Security.** Shows how many system security settings are not configured.

To view the **Safety Index** details, select a virtual server/application and click the **Safety Index** tab.
Citrix Application Delivery Management service

The details are displayed.

1 - Displays the detailed information for Application Firewall configurations.

2 - Displays the detailed information for System Security. Click each security group to get details on 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

June 28, 2022

Web applications that are exposed to the internet have become vulnerable to attacks drastically. Citrix ADM enables you to visualize actionable violation details to protect applications from attacks. Navigate to Security > Security Violations for a single-pane solution to:
Citrix Application Delivery Management service

- 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**

To view the violations, you must:

- Select Web Transaction Settings to All
- 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 (applicable only for premium licensed ADC instances)

**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.
4. Click **Ok**.

**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 one or more virtual servers and click **Enable Analytics**.

4. On the **Enable Analytics** window, click **Advanced Security Analytics**.

5. On the **Advanced Security Analytics** window:
   a) Select **Create new profile**.
   b) In the **Advanced security profile name** textbox, provide a profile name of your choice.
c) Select the Enable profile check box.

d) Select the behavior-based profile configuration from the list. For Excessive Client Connections, Suspicious Signup Attempts, Website Scanning, and Content Scraping, Unusually large download volume, Unusually large upload volume, Unusually high upload transactions, and Unusually high download transactions violations, you can choose the sensitivity level as Low, Medium, and High.

The following violations require additional configurations:

**Account Takeover:**

a) **Method** - Select the HTTP method type from the list. The available options are GET, PUSH, POST, and UPDATE.

b) **Login URL** - Specify the URL of the web application.

c) **Success response code** - Specify the HTTP status code (for example, 200) for which you want Citrix ADM to report the account takeover violation from bad bots.

d) Click + to add another parameter.

![Account Takeover Configuration Table](image)

**Website Scanning and Content Scraping:**

a) Select **Website Scanning** or **Content Scraping** or both.

b) **Session Tracking Method** - Select the tracking method as Client IP, Citrix Web Application Firewall, Backend Application, or URL.
6. Click **Apply Profile**.

7. Click **Save**.

After you create a profile:

- The profile is accessible under **Use existing security profile**. You can also modify an existing profile later. If you modify an existing profile, the same updates are also applied to all virtual servers using the profile.

- You can view the newly created profile name under **APPSEC PROFILE** by navigating to **Security > Security Violations** and clicking the **Settings** icon.
In this view, you can:

- Click the profile and view details in the read-only mode.
- Click the profile and select the Unbind Profile option.

Note

- If you unbind the profile, you can either continue with a default profile for this application (if eligible) or add a new profile later.
- After you unbind a profile and if it is not associated with any virtual server, the profile is automatically deleted.

Points to note:

- You can select multiple virtual servers, enable Advanced Security Analytics, and apply the same profile.
- You can delete a profile. If you delete a profile, it also gets removed immediately from all virtual servers that are using the profile.
- When you choose to enable Advanced Security Analytics, certain behavior-based violations require to enable WAF Security Violations or Bot Security Violations or Web Insight or all as a prerequisite. For such violations, the prerequisites are automatically selected.
- When a virtual server is not added with any profile, it is automatically enabled with a default profile if the following conditions are met:
### Profile name | Condition | Description | Violations enabled | Priority
--- | --- | --- | --- | ---
**DefaultWafBotAnalyticsProfile** | WAF security violations or Bot security violations | The virtual server is enabled with Bot or WAF insight. | Unusually high upload volume, Unusually high download volume, Excessive client connections, and Unusually high request rate | 1

**DefaultWafBotPolicyProfile** | WAF or Bot profile | The virtual server has a WAF or Bot profile configured. | Unusually high upload volume and Unusually high download volume | 2

- If the application or virtual server is eligible with all these conditions, then the default profile is assigned based on the priority.
- You cannot modify or delete a default profile.

## Application overview

June 2, 2022

The Application Overview page displays applications with full visibility into the threat details associated in both security insight and bot insight. You can also view information such as total violations, total WAF and Bot violations, violation by country, and so on.
1 – Displays the total affected applications, total violations, total WAF violations, and total Bot violations for the selected duration.

2 – Displays the WAF and Bot violation details. Click the WAF and Bot tab to view the top 5 custom or discrete applications based on the total violations occurred. Click View All to view all application details.

3 – Displays the top violations based on the occurrences and the actions applied.

4 – Displays a geo map view that provides visibility from which locations the violations have occurred.

5 – Provides information based on the violations.

For more information on bot and security insights, see:
Citrix Application Delivery Management service

- Bot insight
- Security insight

**Violation categories**

<table>
<thead>
<tr>
<th>WAF</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unusually High Upload Transactions</strong></td>
<td><strong>Excessive Client Connections</strong></td>
</tr>
<tr>
<td><strong>Unusually High Download Transactions</strong></td>
<td><strong>Account Takeover</strong></td>
</tr>
<tr>
<td><strong>Excessive Unique IPs</strong></td>
<td><strong>Unusually High Upload Volume</strong></td>
</tr>
<tr>
<td><strong>Excessive Unique IPs Per Geo</strong></td>
<td><strong>Unusually High Download Volume</strong></td>
</tr>
<tr>
<td><strong>Cookie Hijack</strong></td>
<td><strong>Unusually High Request Rate</strong></td>
</tr>
<tr>
<td><strong>Infer Content Type XML</strong></td>
<td><strong>Website Scanners</strong></td>
</tr>
<tr>
<td><strong>Buffer Overflow</strong></td>
<td><strong>Account Takeover for Citrix Gateway</strong></td>
</tr>
<tr>
<td><strong>Content Type</strong></td>
<td><strong>API Abuse</strong></td>
</tr>
<tr>
<td><strong>Cookie Consistency</strong></td>
<td><strong>Content Scrapers</strong></td>
</tr>
<tr>
<td><strong>CSRF Form Tagging</strong></td>
<td><strong>Keystroke and mouse dynamics based bot detection</strong></td>
</tr>
<tr>
<td><strong>Deny URL</strong></td>
<td><strong>Scraper</strong></td>
</tr>
<tr>
<td><strong>Form Field Consistency</strong></td>
<td><strong>Screenshot Creator</strong></td>
</tr>
<tr>
<td><strong>Field Formats</strong></td>
<td><strong>Search Engine</strong></td>
</tr>
<tr>
<td><strong>Maximum Uploads</strong></td>
<td><strong>Service Agent</strong></td>
</tr>
<tr>
<td><strong>Referrer Header</strong></td>
<td><strong>Site Monitor</strong></td>
</tr>
<tr>
<td><strong>Safe Commerce</strong></td>
<td><strong>Speed Tester</strong></td>
</tr>
<tr>
<td><strong>Safe Object</strong></td>
<td><strong>Tool</strong></td>
</tr>
<tr>
<td><strong>HTML SQL Inject</strong></td>
<td><strong>Uncategorized</strong></td>
</tr>
<tr>
<td><strong>Start URL</strong></td>
<td><strong>Virus Scanner</strong></td>
</tr>
<tr>
<td><strong>Cross-site scripting</strong></td>
<td><strong>Vulnerability Scanner</strong></td>
</tr>
<tr>
<td><strong>XML DoS</strong></td>
<td><strong>DeviceFP Wait Exceeded</strong></td>
</tr>
<tr>
<td><strong>XML Format</strong></td>
<td><strong>Invalid DeviceFP</strong></td>
</tr>
<tr>
<td><strong>XML WSI</strong></td>
<td><strong>Invalid Captcha Response</strong></td>
</tr>
<tr>
<td><strong>XML SSL</strong></td>
<td><strong>Captcha Attempts Exceeded</strong></td>
</tr>
</tbody>
</table>
### View WAF violation details

Click an application from the **Top Applications** or from the **View All** option to view the WAF details.

<table>
<thead>
<tr>
<th>WAF</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Attachment</td>
<td>Valid Captcha Response</td>
</tr>
<tr>
<td>XML SOAP Fault</td>
<td>Captcha Client Muted</td>
</tr>
<tr>
<td>XML Validation</td>
<td>Captcha Wait Time Exceeded</td>
</tr>
<tr>
<td>Others</td>
<td>Request Size Limit Exceeded</td>
</tr>
<tr>
<td>IP Reputation</td>
<td>Rate Limit Exceeded</td>
</tr>
<tr>
<td>HTTP DOS</td>
<td>Block list (IP, subnet, policy expression)</td>
</tr>
<tr>
<td>TCP Small Window</td>
<td>Allow list (IP, subnet, policy expression)</td>
</tr>
<tr>
<td>Signature Violation</td>
<td>Zero Pixel Request</td>
</tr>
<tr>
<td>File Upload Type</td>
<td>Source IP</td>
</tr>
<tr>
<td>JSON cross-site scripting</td>
<td>Host</td>
</tr>
<tr>
<td>JSON SQL</td>
<td>Geo Location</td>
</tr>
<tr>
<td>JSON DOS</td>
<td>URL</td>
</tr>
<tr>
<td>Command Injection</td>
<td>Crawler</td>
</tr>
<tr>
<td></td>
<td>Feed Fetcher</td>
</tr>
<tr>
<td></td>
<td>Link Checker</td>
</tr>
<tr>
<td></td>
<td>Marketing</td>
</tr>
</tbody>
</table>

**Note**

If you select a custom app, you can view the consolidated applications details in the **Security**
Overview page. From the list, select an application to view details for the selected application. The Security Overview page for the selected application is displayed. Under WAF, you can view:

- A graph view that indicates the total violations, threat index score, safety index score for the application.

![Graph view of security overview](image)

Click View Details to see the Application Firewall and Citrix ADC System Security configuration details.

![Security overview details](image)

- The violations based on types, severity, and actions applied.

![Violation types](image)

Click Logs to view details based on the severity or action taken. You can also view the client IP...
The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

**Note**
For a custom app, violations that are applicable for all applications are displayed. You can click an application from the list to view the violations affected for the selected application.

Click each violation to view details such as:

- **What Happened** – Indicates the total occurrences and the last occurred date and time.
- **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.
View bot violation details

From the Bot tab, click an application from the Top Applications or from the View All option to view the bot details.

Note

If you select a custom app, you can view the consolidated applications details in the Security Overview page. From the list, select an application to view details for the selected application.
The **Security Overview** page for the selected application is displayed. Under **Bot**, you can view:

- A graph indicating total bots, total bad bots, total good bots, and total ratio between human users and bots accessing the application.

![Graph showing total bots, bad bots, good bots, and ratio]

- The violations based on the bot types, severity, and actions applied.

![Table showing bot violation types, severity, and actions]

Click **Logs** to view details based on severity or actions taken. If a detected bot is a Signature type bot, you can view more details such as Bot developer and Signature ID. The Signature ID enables you to identify if the detected bot is a good bot or a bad bot.

![Log view showing specific details for detected bots]
If a detected bot is any other bot type apart from Signature bot, the Signature ID and Bot developer are displayed as N/A.

The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

Click each violation to view details such as:

- **What Happened** – Indicates the total occurrences and the last occurred date and time.
- **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.
Note

Under **WAF** and **Bot**, you can view analytics for content switching virtual server that is bound with load balancing virtual servers. Click the content switching virtual server and under **Bound Load Balancing Server**, you can view the list of load balancing servers bound to the content switching virtual server.
View events history

Click the Events tab to view the bot and WAF events.

All Violations

February 28, 2022

The All Violations page displays the application security violation details based on the Network, WAF, and Bot categories. To view the security violations in Citrix ADM, ensure:

- You have a premium license for the Citrix ADC instance (for WAF and BOT violations).
- You have applied license on the load balancing or content switching virtual servers (for WAF and BOT). For more information, see Manage licensing on virtual servers.
- You enable more settings. For more information, see the procedure available at Setting up.

Violation categories

Citrix ADM enables you to view the following violations. Under Violation Details, you can click each violation tab to view the violation details.
<table>
<thead>
<tr>
<th>Network</th>
<th>WAF</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Slow Loris</td>
<td>Unusually High Upload Transactions</td>
<td>Excessive Client Connections</td>
</tr>
<tr>
<td>DNS Slow Loris</td>
<td>Unusually High Download Transactions</td>
<td>Account Takeover</td>
</tr>
<tr>
<td>HTTP Slow Post</td>
<td>Excessive Unique IPs</td>
<td>Unusually High Upload Volume</td>
</tr>
<tr>
<td>NXDomain Flood Attack</td>
<td>Excessive Unique IPs Per Geo</td>
<td>Unusually High Request Rate</td>
</tr>
<tr>
<td>HTTP desync attack</td>
<td>JSON SQL Injection Grammar</td>
<td>Unusually High Download Volume</td>
</tr>
<tr>
<td>Bleichenbacher Attack</td>
<td>Infer Content Type XML</td>
<td>Website Scanners</td>
</tr>
<tr>
<td>Segment smack Attack</td>
<td>Buffer Overflow</td>
<td>Account Takeover for Citrix Gateway</td>
</tr>
<tr>
<td>SYN Flood Attack</td>
<td>Content Type</td>
<td>API Abuse</td>
</tr>
<tr>
<td>Small Window Attack</td>
<td>Cookie Consistency</td>
<td>Content Scapers</td>
</tr>
<tr>
<td></td>
<td>CSRF Form Tagging</td>
<td>Keystroke and mouse dynamics based bot detection</td>
</tr>
<tr>
<td></td>
<td>Deny URL</td>
<td>Scraper</td>
</tr>
<tr>
<td></td>
<td>Form Field Consistency</td>
<td>Screenshot Creator</td>
</tr>
<tr>
<td></td>
<td>Field Formats</td>
<td>Search Engine</td>
</tr>
<tr>
<td></td>
<td>Maximum Uploads</td>
<td>Service Agent</td>
</tr>
<tr>
<td></td>
<td>Referrer Header</td>
<td>Site Monitor</td>
</tr>
<tr>
<td></td>
<td>Safe Commerce</td>
<td>Speed Tester</td>
</tr>
<tr>
<td></td>
<td>Safe Object</td>
<td>Tool</td>
</tr>
<tr>
<td></td>
<td>HTML SQL Inject</td>
<td>Uncategorized</td>
</tr>
<tr>
<td></td>
<td>Start URL</td>
<td>Virus Scanner</td>
</tr>
<tr>
<td></td>
<td>Cross-site scripting</td>
<td>Vulnerability Scanner</td>
</tr>
<tr>
<td></td>
<td>XML DoS</td>
<td>DeviceFP Wait Exceeded</td>
</tr>
<tr>
<td></td>
<td>XML Format</td>
<td>Invalid DeviceFP</td>
</tr>
<tr>
<td></td>
<td>XML WSI</td>
<td>Invalid Captcha Response</td>
</tr>
<tr>
<td></td>
<td>XML SSL</td>
<td>Captcha Attempts Exceeded</td>
</tr>
</tbody>
</table>
### Security violations dashboard

In the security violations dashboard, you can view:

- Total violations occurred across all ADC instances and applications. The total violations are displayed based on the selected time duration.

- Total violations under each category.

<table>
<thead>
<tr>
<th>Network</th>
<th>WAF</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Attachment</td>
<td>Valid Captcha Response</td>
<td></td>
</tr>
<tr>
<td>XML SOAP Fault</td>
<td>Captcha Client Muted</td>
<td></td>
</tr>
<tr>
<td>XML Validation</td>
<td>Captcha Wait Time Exceeded</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>Request Size Limit Exceeded</td>
<td></td>
</tr>
<tr>
<td>IP Reputation</td>
<td>Rate Limit Exceeded</td>
<td></td>
</tr>
<tr>
<td>HTTP DOS</td>
<td>Block list (IP, subnet, policy expression)</td>
<td></td>
</tr>
<tr>
<td>TCP Small Window</td>
<td>Allow list (IP, subnet, policy expression)</td>
<td></td>
</tr>
<tr>
<td>Signature Violation</td>
<td>Zero Pixel Request</td>
<td></td>
</tr>
<tr>
<td>File Upload Type</td>
<td>Source IP</td>
<td></td>
</tr>
<tr>
<td>JSON cross-site scripting</td>
<td>Host</td>
<td></td>
</tr>
<tr>
<td>JSON SQL</td>
<td>Geo Location</td>
<td></td>
</tr>
<tr>
<td>JSON DOS</td>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>Command Injection</td>
<td>Crawler</td>
<td></td>
</tr>
<tr>
<td>Cookie Hijack</td>
<td>Feed Fetcher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Link Checker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marketing</td>
<td></td>
</tr>
</tbody>
</table>
• Total ADCs affected, total applications affected, and top violations based on the total occurrences and the affected applications.

<table>
<thead>
<tr>
<th>ADCs Affected</th>
<th>Applications Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>7</td>
</tr>
</tbody>
</table>

**Top Violations**

Based on the number of occurrences and the affected applications.

Drag and select on graph

Search result

---

**Violation details**

For each violation, Citrix ADM monitors the behavior for a specific time duration and detects violations for unusual behaviors. Click each tab to view the violation details. You can view details such as:

• The total occurrences, last occurred, and total applications affected

• Under event details, you can view:
  - The affected application. You can also select the application from the list if two or more applications are affected with violations.
  - The graph indicating violations.

Drag and select on the graph that lists the violations to narrow down the violation search.

Click **Reset Zoom** to reset the zoom result.

  - **Recommended Actions** that suggest you troubleshoot the issue.
Citrix Application Delivery Management service

- Other violation details such as violence occurrence time and detection message.

**Behavior checks with no violations**

Apart from violation details, you can visualize a 3-week traffic prediction based on the machine learning algorithm. As an administrator, this 3-week prediction enables you to:

- Analyze the traffic pattern even if no violations are observed.
- Take troubleshooting actions for any unusual traffic patterns observed from the predictions.
- Observe that Citrix ADM is processing data, apart from the anomalies.

In the Security Violations page, click the Behavior checks with no violation tab to view the 3-week traffic prediction.
The security violations are displayed. Consider that you want to view the traffic prediction for Excessive Unique IPs Per Geo.
From the example image, you can view:

- Expected Unique IP Range – Citrix ADM has predicted the expected IP range based on the traffic pattern.
- Unique IP – Citrix ADM has predicted about 1970 unique IPs that will be transacting with the app from Malaysia.

Using this data, you can proactively take precautionary steps to avoid these excessive unique IPs.

If Citrix ADM does not have any predictions for a security violation, you can view the following message:
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.

See the Setting Up topic to ensure if all the required settings are enabled to view the app security violation details.
Note

In Citrix ADM, 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 ADM. 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.

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:
Integration with Splunk

July 28, 2022

You can now integrate Citrix ADM with Splunk to view analytics for WAF, Bot, and behavior-based 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 ADM collects Bot, WAF, behavior-based 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, Bot, and behavior-based 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](image)

   **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.

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 ADM.
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.
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.
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 ADM to integrate with Splunk.

1. Log on to Citrix ADM.

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** - The selected violations are exported to Splunk immediately.
   - **Periodic Export** - The selected violations are exported 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.

5. In the **Subscribe** page:

   a) **Export Frequency** – Select Daily or Hourly from the list. Based on the selection, Citrix ADM exports the details to Splunk.

   **Note**
   
   Applicable only if you have selected violations in **Periodic Export**.

   b) **Subscription Name** – Specify a name of your choice.

   c) Click **Submit**.

   **Note**
   
   • When you configure with **Periodic Export** option for the first time, the selected features data get pushed to Splunk immediately. The next export frequency happens based on your selection (daily or hourly).

   • When you configure with **Realtime Export** option for the first time, the selected features data pushed to Splunk immediately as soon as the violations are detected in Citrix ADM.

**Verify details in Splunk**

After you add details in Citrix ADM, you can verify if Splunk receives the events.
1. From the Splunk home page, click **Search & Reporting**.

![Search & Reporting](image)

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"` or `sourcetype="ml"` to check the details.

![Search Result](image)

The following search result is an example for a WAF violation:
The following search result is an example for a Bot violation:
The following search result is an example for the behavior-based violations:

<table>
<thead>
<tr>
<th>i</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7/21/22 10:00:00</td>
<td>appname: F99_custom_app &lt;br&gt; ctitname: P99_PRIVATE &lt;br&gt; ind_category: Bot &lt;br&gt; ind_desc: This indicator detects bot sessions based on keystroke and mouse dynamics. &lt;br&gt; ind_detection_msg: Inc of anomalies:1,unique_client_text:1 &lt;br&gt; ind_id: 2014 &lt;br&gt; ind_name: Keystroke and Mouse dynamics based bot detection &lt;br&gt; ind_recommend_desc: This might be a malicious activity, Please further investigate the detected IPs and take necessary action. &lt;br&gt; ind_value: 1 &lt;br&gt; ind_weight: 50 &lt;br&gt; ip_address: 16.102.38.139 &lt;br&gt; rtp_sample_time: 1650440600 &lt;br&gt; severity: MEDIUM &lt;br&gt; svcname: tenant_id: c1012911119649129</td>
</tr>
</tbody>
</table>

Show as raw text

```text
host = 332.101.103.8098 | source = http.test | sourcetype = inf
```
Access Pivot details

You must identify the Data Model type to see the pivot details. For example, the Splunk add-on converts the WAF, Bot, and behavior-based 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.

3. Select a Dataset. In the following example, the IDS Attacks option is selected.

The total count of IDS Attacks is displayed.

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:
Splunk dashboard

Using a dashboard, you can view details of WAF, Bot, and behavior-based violation analytics with panels such as charts, tables, lists, and so on. You can configure:

- 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

May 10, 2022

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 ADM 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 ADM works:
1 – Citrix ADC instances with its WAF profiles

2 – Configure a learning profile in Citrix ADM, add the WAF profiles, and select to auto deploy or manually deploy the relaxation rules

3 – Administrator can validate the relaxation rules in Citrix ADM 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 ADM generates a list of exceptions (relaxations) for the configured security check. As an administrator, you can review the list of exceptions in Citrix ADM and decide to deploy or skip.

Using the WAF learning feature in Citrix ADM, 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 -sqlinjectionTransformSpecialChars ON` and `set -sqlinjectiontype sqlspclcharorkeywords` in Citrix ADC instance.

- HTML Command Injection
  
  **Note**
  
  Supported only in ADC instance 13.0-72.12 or later.

- JSON SQL
  
  **Note**
  
  Supported only in ADC instance 13.1-14.10 or later.

- JSON Command Injection
  
  **Note**
  
  Supported only in ADC instance 13.1-14.10 or later.

- JSON XSS
  
  **Note**
  
  Supported only in ADC instance 13.1-14.10 or later.

- Check the relaxation rules in Citrix ADM 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 ADM:
Citrix Application Delivery Management service

1. Configure the learning profile
2. See the relaxation rules
3. Use the WAF learning Action Summary page

WAF recommendations

February 15, 2022

Citrix Web App Firewall (WAF) Profile 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 ADM 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.
Note
The ADC instance must be **13.0 41.28 or later** (for security checks) and **13.0 or later** (for signatures).

**Prerequisites**

The applications:

- Must have the premium license.
- Must be the load balancing virtual server.

**Configure the WAF scan settings**

In Citrix ADM, navigate to **Security > WAF Recommendation** and under **Applications**, click **Start Scan** to configure the WAF scan settings for an application.

![WAF Recommendations](image)

In the WAF Recommendations page:

- **Domain Name** – Specify the publicly accessible/publicly reachable domain name that is associated with the application VIP. For example: [www.example.com](http://www.example.com).

  Note
  Start URL, Login URL and Logout URL must match the specified domain.

- **Traffic and Start URL** – Provide the URL details of the application (server).
  - **HTTP/HTTPS Protocol** – Select the protocol of the application.
  - **Traffic Timeout** – The wait time (in seconds) for a single request during the scan. The value must be greater than 0.
Citrix Application Delivery Management service

- **Start URL** – The home page of the application to initiate the scan. For example, `https://www.example.com/home`. The URL must be a valid IPv4 address. Internal IP address in the range 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 are not allowed.

- **Login URLs** – Specify the login credentials, URLs, if any, to access the application.
  - **Login URL** – The URL to which the login data is sent for authentication. In HTML, this URL is commonly known as the action URL.
  - **Authentication Method** – Select the supported authentication method (form based or header based) for your application.
    - Form-based authentication requires submitting a form to the login URL with the login credentials. These credentials must be in the form of form fields and their values. The application then shares the session cookie that is used to maintain sessions during the scan.
    - Header-based authentication requires the Authentication header and its value in the headers section. The Authentication header must have a valid value and is used to maintain sessions during the scan. The form-fields should be left empty for Header-based.
  - **RequestMethod** – Select the HTTP method used when submitting form data to the login URL. The allowed request method is POST, GET, and PUT.
  - **Form Fields** – Specify the form data to be submitted to the login URL. Form Fields are required only if you select the form-based authentication. You must specify in the key-value pairs, where Field Name is the Key and Field Value is the Value. Ensure that all form fields needed for login to work are added correctly, including passwords. The values are encrypted before storing it in the database. You can click the Add button to add multiple form fields. For example, Field Name – user name and Field Value – admin.
  - **HTTP Headers** – The HTTP headers maybe required for the login to succeed. You must specify in the key-value pairs, where Header Name is the Key and Header Value is the Value. You can click the Add button to add multiple HTTP headers. One of the most common required HTTP headers is Content-Type header.

© 1999–2022 Citrix Systems, Inc. All rights reserved. 310
• **Logout URLs** – Specify the URL that terminates the session after accessing. For example: https://www.example.com/customer/logout.

• **Vulnerability** – Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to report the potential vulnerability. It is recommended to enable this detection that is not in the production environment. All other vulnerabilities are also reported, without simulating these attacks on the application.

• **Additional Settings**
  - **Requests Concurrency** – The total requests sent to the web application in parallel.
  - **Scan Depth** - The depth of the web application up to which the scan must go on. For example, for a scan depth of value 2, the Start URL and all the links found in this URL are...
scanned. You must specify a value greater than or equal to 1.

- **Response size limit** – The maximum limit on the response size. Any responses beyond the mentioned value are not scanned. The recommended limit is 3 MB (300000 bytes).

The WAF scan settings configuration is complete. You can click **Scan** to start the scanning process or you can click **Save for later** to save the configurations and scan later.

### WAF scan recommendation process

When you start the scan, the WAF recommendation engine:

- Scans the provided web application through the provided URL.
- Inspects the web application to discover the technologies used by the web application.
- Simulates security attacks on the web application to detect potential vulnerabilities.
- Recommends signatures based on the web technologies detected.
- Recommends security checks based on vulnerabilities found and the analysis of the traffic.
- Analyzes the web application responses to generate more granular settings.

The following security checks are supported:

- Buffer Overflow
- Field Formats
- Credit Card
- Cookie Consistency
- HTML SQL Injection
- HTML Cross Site Scripting
- Form Field Consistency
- CSRF Form Tagging
View scan report

After the scan is complete, click **View Report** to view the results.

The scan result provides:

- **WAF Recommendation** – Enables you to view the summary of the total signatures and security checks recommended for the application.

- **Scan Detections** – Enables you to view the collection of information such as technologies and violation details performed on the application. Click **View Details** to see the information about the detections and other details of the scan.

Under **WAF Recommendation**, click **Review Recommendation** to view the details for **Security Checks** and **Signatures**.

The recommended security settings suggest the recommended security checks and signatures for the application. You can edit the recommendations from the list and click **view or edit** to view details or edit changes according to the requirement. The Reset to default resets all changes made and brings
back to the original recommendations.

After reviewing details, click **Apply Recommendation**. The recommendations are configured using the StyleBooks. You must ensure to apply recommendation in the **Security Checks** and **Signature** tabs separately.

It is recommended to apply the signatures first and then the security checks. This binds the signatures to the profile automatically.

When you apply signatures successfully:

- The configuration is applied on the ADC instance through the `appfw-import-object` StyleBook.
- The signatures file with recommendations configured is imported in the ADC instance.

**Note**

Signatures are supported in ADC 13.0 or later version.

Before you proceed to apply the **Security Check** recommendations, navigate to **Applications > Configuration > Config Packs** and ensure that the signatures configpack is successfully created.

When you apply security checks successfully:

- The configuration is applied on the ADC instance through StyleBooks, depending upon the ADC version. For ADC 13.0, `waf-default-130` StyleBook is used and for ADC 13.1, `waf-default-131` stylebook is used.
- The `Appfw` profile is created on your ADC and bound to the application using the `policylabel`.
- The signatures are bound to the `appfw` profile, if the recommended signatures are already applied.
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 ADM database, so you can view error details for any time period. You can also view a summary of the logon failures and determine at what stage of the logon process a failure has occurred.

**Points to Note:**

- Gateway Insight is supported on the following deployments:
  - Access Gateway
  - Unified Gateway
- The Citrix ADM 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 ADM. You must then enable AppFlow for the virtual server representing the VPN
application. For information about adding device to Citrix ADM, see Adding Instances.

**Note**

To view end-point analysis (EPA) failures in Citrix ADM, 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 ADM**

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Under **Virtual Server Analytics Summary**, click **Configure Analytics**.
3. In the **All Virtual Servers** page, select the Citrix Gateway virtual server, and click **Enable Analytics**.
4. Select **Gateway Insight**.
5. Click **Save**.
Enable Analytics

Enable AppFlow user name logging on an ADC Gateway appliance by using the GUI


2. In the Configure AppFlow Settings screen, select AAA Username, and then click OK.

View Gateway Insight reports

In Citrix ADM, 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.
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 ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see [Configure Groups on Citrix ADM](#).

**View EPA, SSO, authentication, authorization, and application launch failures**

1. In Citrix ADM, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.

**View summary of session modes, clients, and the number of users**

In Citrix ADM, 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.

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 ADM, navigate to Gateway > Gateway Insight > Users.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click Go.
3. You can view the number of active users, number of active sessions, and bytes by all users during the time period.

Scroll down to view a list of available users and active users.

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.
Citrix Application Delivery Management service

- **View details by clicking the bar graph** – When you click a bar graph, you can view the relevant details. For example, navigate to *Gateway > Gateway Insight > Gateway* and click the gateway bar graph to view the gateway details.

- The user **Active Sessions** and **Terminated Sessions**.

- The gateway domain name and gateway IP address in **Active Sessions**.
• The user login duration.

• The reason for the user logout session. The logout reasons can be:
  - Session timed out
  - Logged out because of internal error
  - Logged out because of inactive session timed out
  - User has logged out
  - Administrator has stopped the session

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.
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 ADM, navigate to **Gateway > Gateway Insight > Applications**.
2. Select the time period for which you want to view the application details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.
Scroll down to view the numbers of sessions, bandwidth, and total bytes consumed by ICA and other applications.

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 ADM, navigate to Gateway > Gateway Insight > Gateways.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click Go.
You can now view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with an ADC Gateway appliance at any given time.

Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, ADC IP address, session modes, and Total Bytes.

You can click a gateway in the **Gateway Domain Name** column to display the EPA, authentication, single sign-on, and application launch failures and other details for a gateway.

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 ADM 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 ADM, and you want to see why a user is unable to log in, or at what stage of the login process the failure has occurred.

Citrix ADM enables you to view the user login error details in the following stages of the login process:

- Authentication
- End-point analysis (EPA)
- Single sign-on

In Citrix ADM, you can search for a particular user and then view all the details for that user.

To search for a user:

In Citrix ADM, navigate to Gateway > Gateway Insight and, in the Search for Users text box, specify the user you want to search.

Authentication Failures

You can view authentication errors such as incorrect credentials or no response from the authentication server. 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 ADM, navigate to Gateway > Gateway Insight.

2. In the Overview section, select the time period for which you want to view the authentication errors. You can use the time slider to further customize the selected time period. Click Go.

Overview

1. Click the Authentication tab. You can view the number of authentication errors at any given time in the Failures graph.
Citrix Application Delivery Management service

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.

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.
EPA Failures

You can view EPA failures at pre- or post-authentication stage.

View EPA failure details

1. In Citrix ADM, navigate to Gateway > Gateway Insight.

2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click Go.

3. Click the EPA (End Point Analysis) tab. You can view the number of EPA errors at any given time in the Failures graph.

Scroll down to view details of each EPA error such as Username, ADC IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name and more from the table on the same page.
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.

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.

**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 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 ADM, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.

Scroll down to view details of each SSO error such as **Username**, **ADC IP Address**, **Error Time**, **Error Description**, **Resource Name** and more from the table on the same tab.

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.
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 ADM, navigate to Gateway > Gateway Insight.

2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click Go.

3. Click the Application Launch tab. You can view the number of application launch failures at any given time in the Failures graph.

Scroll down to view details of each application launch error, such as 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.
Citrix Application Delivery Management service

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.

<table>
<thead>
<tr>
<th>Username</th>
<th>NetScaler IP Address</th>
<th>Client IP Address</th>
<th>Gateway IP Address</th>
<th>VPN</th>
<th>STA IP Address</th>
<th>Error Time</th>
<th>Error Description</th>
<th>Error Count</th>
<th>Resource Name</th>
<th>Gateway Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>10.102.81.201</td>
<td>10.102.61.121</td>
<td>10.252.241.48</td>
<td>atest</td>
<td>-NA-</td>
<td>2/22/2016, 3:00 PM</td>
<td>Gateway timed out HTTP: (c)</td>
<td>1</td>
<td>c-go-mupus.com</td>
<td>atest.citrix.com</td>
</tr>
<tr>
<td>user2</td>
<td>10.102.81.201</td>
<td>10.102.61.121</td>
<td>10.252.241.48</td>
<td>atest</td>
<td>-NA-</td>
<td>2/22/2016, 4:30 PM</td>
<td>Gateway timed out HTTP: (c)</td>
<td>1</td>
<td>c-go-mupus.com</td>
<td>atest.citrix.com</td>
</tr>
<tr>
<td>user3</td>
<td>10.102.81.201</td>
<td>10.102.61.121</td>
<td>10.252.241.48</td>
<td>atest</td>
<td>-NA-</td>
<td>2/22/2016, 4:30 PM</td>
<td>Gateway timed out HTTP: (c)</td>
<td>1</td>
<td>code4query.com</td>
<td>atest.citrix.com</td>
</tr>
<tr>
<td>user4</td>
<td>10.102.81.201</td>
<td>10.102.61.121</td>
<td>10.252.241.48</td>
<td>atest</td>
<td>-NA-</td>
<td>2/22/2016, 4:30 PM</td>
<td>Gateway timed out HTTP: (c)</td>
<td>1</td>
<td>cits.kendosstatic.com</td>
<td>atest.citrix.com</td>
</tr>
</tbody>
</table>

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 ADM, you can view the total bytes and bandwidth consumed by that application.

**View total bytes and bandwidth consumed by an application**

In Citrix ADM, navigate to **Gateway > Gateway Insight > Applications**, scroll down and, on the **Other Applications** tab, click the application for which you want to view the details.

You can view the number of sessions and the total number of bytes consumed by that application.

You can also view the bandwidth consumed by that application.
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 ADM, navigate to Gateway > Gateway Insight > Applications.

2. On the screen that appears, scroll down, and on the Other Applications tab, select the application to which the user was unable to log on to.

On the screen that appears, scroll down, and in the Users table, all the users that have access to that application are displayed.
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 ADM, navigate to Gateway > Gateway Insight.
2. In the Overview section, scroll down to view the Session Mode, Operating Systems, Browsers, and User Logon Activity charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.
HDX Insight

April 5, 2022

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 ADM 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.

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 ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configuring Groups on Citrix ADM.

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.
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.
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.
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 ADM running software 11.1 build 51.21 or later. To view these metrics, navigate to **Gateway > HDX Insight > Users**, and select a user name. The user metrics appear in the table next to the graph.
Geo map for HDX Insight

Geo map feature in Citrix ADM 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 ADM automatically enables geoms for private IP addresses or public IP addresses, when you enable Web insight.

Create a private IP block

Citrix ADM can recognize the location of a client when the client private IP address is added to the Citrix ADM 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 ADM recognizes that the traffic is originating from City A for this client.

To create an IP block:

1. In Citrix ADM, 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.
Public IP blocks

Citrix ADM can also recognize the client location if the client uses public IP address. Citrix ADM 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 ADM 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.
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.

### 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.
Limitations

If ADC instances have Advanced license, thresholds set on Citrix ADM 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

February 15, 2022

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

February 15, 2022

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 ADM inventory and enable AppFlow on Citrix ADM. The following image illustrates a Citrix ADM deployed in single-hop mode
Enable the AppFlow feature from Citrix ADM

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
Enable data collection to monitor Citrix ADCs deployed in transparent mode

April 5, 2022

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 ADM inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add Citrix ADM 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 ADM configuration utility.
- For detailed information about the commands and their usage, see *Command Reference*.
- For information on policy expressions, see *Policies and Expressions*.

The following image shows the network deployment of a Citrix ADM 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.

   1. `set ns param --icaPorts \<port\>...
   2. `<!--NeedCopy-->`

   **Example:**

   1. `set ns param -icaPorts 2598 1494`
   2. `<!--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.

   1. `add appflow collector <name> -IPAddress <ip_addr>
   2. `<!--NeedCopy-->`
Example:

```
1 add appflow collector MyInsight IPAddress 192.168.1.101
2 <!--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.

```
1 add appflow action <name> -collectors <string> ...
2 <!--NeedCopy-->  
```

Example:

```
1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->  
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
1 add appflow policy <policyname> <rule> <action>
2 <!--NeedCopy-->  
```

Example:

```
1 add appflow policy pol true act
2 <!--NeedCopy-->  
```

6. Bind the AppFlow policy to a global bind point.

```
1 bind appflow global <policyname> <priority> -type <type>
2 <!--NeedCopy-->  
```

Example:
Enable data collection for Citrix ADC Gateway appliances deployed in double-hop mode

February 15, 2022

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 ADM, 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 ADM 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 ADM 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 ADM collects TCP records from one appliance and ICA records from the other appliance. After you add the Citrix ADC Gateway appliances to the Citrix ADM inventory and enable data collection, each appliance export the reports by keeping track of the hop count and connection chain ID.

For Citrix ADM to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of 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 ADM 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 ADM inventory, enable AppFlow on Citrix ADM, and then view the reports on the
Citrix ADM dashboard.

**Enabling data collection on Citrix ADM**

If you enable Citrix ADM to start collecting the ICA details from both the appliances, the details collected are redundant. To overcome this situation, you must enable AppFlow for TCP on the first Citrix ADC Gateway appliance, and then enable AppFlow for ICA on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

**To enable the AppFlow feature from Citrix ADM:**

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 ADM:

- 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> [-secure (ON
<nextHopPort> [-imgGifToPng] ...

1  add vpn nextHopServer nh1 10.102.2.33 8443 - secure ON
2  <!--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>

1  bind vpn vserver vs1 -nextHopServer nh1
2  <!--NeedCopy--> 

3. Enable double hop and AppFlow on the Citrix ADC Gateway in the second DMZ.

set vpn vserver <name> [-doubleHop (ENABLED)] [-appflowLog (DISABLED)]

1  set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
2  <!--NeedCopy--> 

4. Disable authentication on the Citrix ADC Gateway virtual server in the second DMZ.

set vpn vserver <name> [-authentication (ON OFF)]

1  set vpn vserver vs -authentication OFF
2  <!--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>]
6. Enable the other Citrix ADC Gateway appliance to export ICA records:

```bash
bind vpn vserver <name> [-policy <string> -priority <positive_integer>] [-type <type>]
```

7. Enable connection chaining on both the Citrix ADC Gateway appliances:

```bash
set appFlow param [-connectionChaining <value>]
```

**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

April 5, 2022
Citrix Application Delivery Management service

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 Apps and Desktops 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 ADM deployed in **LAN User Mode**.

![Citrix ADM in LAN User Mode](image)

Note

Citrix ADC Gateway appliance must be able to reach the Citrix ADM 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 ADM 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
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.

```
1 add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [-cltTimeout <secs>]
```

Example:

```
1 add cr vserver cr1 HDX 10.12.2.2 443 -cacheType FORWARD -cltTimeout 180
```

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.

```
1 add vpn trafficAction** 
2 add vpn trafficPolicy** 
```

Example:

```
1 add vpn trafficAction act1 tcp -HDX ON
2 add vpn trafficPolicy poll "REQ.IP.DESTIP == 10.102.69.17" act1
```
3. Add Citrix ADM as an AppFlow collector on the Citrix ADC appliance.

```bash
add appflow collector** \<name\> **-IPAddress** \<ip\>_addr
```

**Example:**

```bash
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Create an AppFlow action and associate the collector with the action.

```bash
add appflow action** \<name\> **-collectors** \<string\> ...
```

**Example:**

```bash
add appflow action act -collectors MyInsight
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```bash
add appflow policy** \<policyname\> \<rule\> \<action\>
```

**Example:**

```bash
add appflow policy pol true act
```

6. Bind the AppFlow policy to a global bind point.

```bash
bind appflow global** \<policyname\> \<priority\> **-type** \<type \>
```

**Example:**

```bash
bind appflow global pol priority type
```
Citrix Application Delivery Management service

Example:

1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--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.

1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->

Example:

1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->

8. Save the configuration.

1 save ns config
2 <!--NeedCopy-->

Create thresholds and configure alerts for HDX Insight

August 18, 2022

HDX Insight on Citrix ADM allows you to monitor the HDX traffic passing through the Citrix ADC instances. Citrix ADM allows you to set thresholds on various counters used to monitor the Insight traffic. You can also configure rules and create alerts in Citrix ADM.

HDX traffic type is associated with various entities such as applications, desktops, gateways, licenses, and users. Every entity can contain different metrics associated with them. For example, application entity is associated with 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 ADM allowed you to proactively create rules and configure alerts whenever the thresholds set are breached. Now, this threshold management is extended to configure a group of threshold rules. You can now monitor the group instead of individual rules. A threshold rule group comprises one or more user-defined threshold rules for metrics chosen from entities such as users, applications, and desktops. Each rule is monitored against an expected value that you enter when you create the rule. In users entity, the threshold group can be associated with a geolocation as well.

An alert is generated on Citrix ADM only if all the rules in the configured threshold group are breached. For example, you can monitor an application on total session launch count and also on application launch count as one threshold group. An alert is generated only if both rules are breached. This allows you to set more realistic thresholds on an entity.

A few examples are listed as follows:

- Threshold rule1: ICA RTT(metric) for users(entity) must be \( \leq 100 \) ms
- Threshold rule2: WAN Latency (metric) for users(entity) must be \( \leq 100 \) ms

An example of threshold group can be: \( \{ \text{Threshold rule 1} + \text{Threshold rule 2} \} \)

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 TotalSessionLaunchCount or AppLaunchCount. You can create one rule for every combination of an entity and a metric. Use the comparators provided (\( >, <, \geq, \) and \( \leq \)) 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 ADM generates an event to signify a threshold breach, and an alert is created for every event.

You must configure how you receive the alert. You can enable the alert to be displayed on Citrix ADM 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 ADM.

Threshold groups can also be bound to Geolocations for geo-specific monitoring for user entity.

**Example Use Cases**

ABC Inc. is a global firm and has offices in over 50 countries. The firm has two data centers, one in Singapore and other in California that host the Citrix Virtual Apps and Desktops. Employees of the firm access the Citrix Virtual Apps and Desktops throughout the globe using 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 for HDX Insight portfolio metrics.

Create a threshold rule group and configure alerts for HDX Insight using Citrix ADM

1. In Citrix ADM, navigate to Settings> Analytics Settings > Thresholds. On Thresholds page that opens, click Add.

2. On the Create Thresholds and Alerts page, specify the following details:
   a) **Name.** Type in a name for creating an event for which Citrix ADM generates an alert.
   b) **Traffic Type.** From the list, select HDX.
   c) **Entity.** From the list, select the category or the resource type. The entities differ for each traffic type that you have selected earlier.
   d) **Reference Key.** A reference key is automatically generated based on the traffic type and entity that you have selected.
   e) **Duration.** From the list, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.
3. Creating threshold rules group for all entities:

For HDX traffic, you must create a rule by clicking **Add Rule**. 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.
4. **Configuring Geolocation tagging for Users entity:**

   Optionally, you can create a location-based alert for the user entity in the *Configure Geo Details* section. The following image shows an example of creating a geolocation based tagging to monitor WAN latency performance for users on the west coast of the United States.

5. Click **Enable Thresholds** to allow Citrix ADM to start monitoring the entities.

6. Optionally, configure actions such as email and Slack notifications.

7. Click **Create** to create a threshold rule group.
View HDX Insight reports and metrics

April 5, 2022

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

April 5, 2022

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 ADM.
- Record generation for HDX/ICA traffic in Citrix ADC.
- Population of records in Citrix ADM.
**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;

  ```shell
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  For transparent mode, the bind type must be ICA_REQ_DEFAULT. For example;

  ```shell
  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 ADM 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.

<table>
<thead>
<tr>
<th>Skip Code</th>
<th>Error message</th>
<th>Cause of error</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>NS_ICA_ERR_NULL_FRAG</td>
<td>Error handling ICA fragments, likely due to memory conditions</td>
</tr>
<tr>
<td>101</td>
<td>NS_ICA_ERR_INVALID_HS_CMD</td>
<td>Invalid handshake command received</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>102</td>
<td>NS_ICA_ERR_REDUCC_PARAM_CNT</td>
<td>Invalid parameter specified for V3 expander initialization</td>
</tr>
<tr>
<td>103</td>
<td>NS_ICA_ERR_REDUCC_INIT</td>
<td>Unable to initialize the V3 expander correctly</td>
</tr>
<tr>
<td>104</td>
<td>NS_ICA_ERR_REDUCC_PARAM_BYTES</td>
<td>Insufficient bytes to assign a coder to a channel</td>
</tr>
<tr>
<td>105</td>
<td>NS_ICA_ERR INVALID_CHANNEL</td>
<td>Invalid ICA channel number</td>
</tr>
<tr>
<td>106</td>
<td>NS_ICA_ERR INVALID DECODE</td>
<td>Invalid decoder specified for a channel</td>
</tr>
<tr>
<td>107</td>
<td>NS_ICA_ERR INVALID_TW_PARAM</td>
<td>Invalid parameter count specified on Thinwire channel</td>
</tr>
<tr>
<td>108</td>
<td>NS_ICA_ERR INVALID_TW_DEC</td>
<td>Invalid decoder for Thinwire channel</td>
</tr>
<tr>
<td>109</td>
<td>NS_ICA_ERR REUC NO DECODER</td>
<td>No decoder defined for channel</td>
</tr>
<tr>
<td>110</td>
<td>NS_ICA_ERR REUC V3 EXPAND</td>
<td>Failed to expand channel data</td>
</tr>
<tr>
<td>111</td>
<td>NS_ICA_ERR REUC_BYTES V3 EXPAND</td>
<td>Encoder error: Bytes consumed more than bytes available</td>
</tr>
<tr>
<td>112</td>
<td>NS_ICA_ERR REUC_BYTES O</td>
<td>Error: Uncompressed data overrun</td>
</tr>
<tr>
<td>113</td>
<td>NS_ICA_ERR REUC INVALID CMD</td>
<td>Defined Expander command</td>
</tr>
<tr>
<td>114</td>
<td>NS_ICA_ERR CGP_FILL HOLE</td>
<td>Error while handling split CGP frames</td>
</tr>
<tr>
<td>115</td>
<td>NS_ICA_ERR MEM NSB_ALLOC</td>
<td>NSB allocation error – due to low memory conditions</td>
</tr>
<tr>
<td>116</td>
<td>NS_ICA_ERR MEM REDUC_CTX</td>
<td>Memory allocation error for expander context</td>
</tr>
<tr>
<td>117</td>
<td>NS_ICA_ERR ICA OLD SERVER</td>
<td>Old server, capability blocks not supported</td>
</tr>
<tr>
<td>118</td>
<td>NS_ICA_ERR PIR MANY FRAG</td>
<td>Packet Init request is fragmented, unable to process</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>119</td>
<td>NS_ICA_ERR_INIT_ICA_CAPS</td>
<td>ICA capability initialization error</td>
</tr>
<tr>
<td>120</td>
<td>NS_ICA_ERR_NO_MSI_SUPPOR</td>
<td>Host does not support MSI feature. Indicates for XenApp version lower than 6.5 or XenDesktop versions lower than 5.0</td>
</tr>
<tr>
<td>121</td>
<td>NS_ICA_ERR_CGP_INVALID_CMD</td>
<td>Invalid CGP command encountered</td>
</tr>
<tr>
<td>122</td>
<td>NS_ICA_ERR_INSUFFICIENT_CH</td>
<td>Insufficient bytes over channel</td>
</tr>
<tr>
<td>123</td>
<td>NS_ICA_ERR_CHANNEL_DATA</td>
<td>Incorrect data on EUEM, CONTROL, or SEAMLESS channel</td>
</tr>
<tr>
<td>124</td>
<td>NS_ICA_ERR_INVALID_PURE_CMD</td>
<td>Invalid command received while processing pure ICA channel data</td>
</tr>
<tr>
<td>125</td>
<td>NS_ICA_ERR_INVALID_PURE_LEN</td>
<td>Invalid length encountered while processing pure ICA channel data</td>
</tr>
<tr>
<td>126</td>
<td>NS_ICA_ERR_INVALID_PURE_LEN0</td>
<td>Invalid length encountered while processing PURE ICA channel data</td>
</tr>
<tr>
<td>127</td>
<td>NS_ICA_ERR_INVALID_CLNT_DATA</td>
<td>Invalid data length received from client</td>
</tr>
<tr>
<td>128</td>
<td>NS_ICA_ERR_MSI_GUID_SZ</td>
<td>Error in MSI GUID size</td>
</tr>
<tr>
<td>129</td>
<td>NS_ICA_ERR_INVALID_CHANNEL_HEADER</td>
<td>Invalid channel header</td>
</tr>
<tr>
<td>130</td>
<td>NS_ICA_ERR_CGP_PARSE_RECONNECT</td>
<td>Retrieval of reconnected session failed</td>
</tr>
<tr>
<td>131</td>
<td>NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT</td>
<td>Error in disabling SR</td>
</tr>
<tr>
<td>132</td>
<td>NS_ICA_ERR_REDUCE_NOT_V3</td>
<td>Unsupported ICA Reducer version</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>133</td>
<td>NS_ICA_ERR_HS_COMPRESSION_DISABLED</td>
<td>Compression disabled, not honored by host</td>
</tr>
<tr>
<td>134</td>
<td>NS_ICA_ERR_IDENT_PROTO</td>
<td>Unable to identify ICA or CGP protocol, seen with incorrect receivers</td>
</tr>
<tr>
<td>135</td>
<td>NS_ICA_ERR_INVALID_SIGNATURE</td>
<td>Incorrect ICA signature or magic string</td>
</tr>
<tr>
<td>136</td>
<td>NS_ICA_ERR_PARSE_RAW</td>
<td>Error while parsing the ICA handshake packet</td>
</tr>
<tr>
<td>137</td>
<td>NS_ICA_ERR_INCOMPLETE_PKT</td>
<td>Incomplete packet received in handshake</td>
</tr>
<tr>
<td>138</td>
<td>NS_ICA_ERR_ICAFRAME_TOO_LARGE</td>
<td>ICA frame is too large, exceeds 1,460 bytes</td>
</tr>
<tr>
<td>139</td>
<td>NS_ICA_ERR_FORWARD</td>
<td>Error while forwarding the ICA data</td>
</tr>
<tr>
<td>140</td>
<td>NS_ICA_ERR_MAX_HOLES</td>
<td>Unable to process CGP command as it is split beyond supported limit</td>
</tr>
<tr>
<td>141</td>
<td>NS_ICA_ERR_ASSEMBLE_FRAME</td>
<td>Unable to reassemble ICA frame correctly</td>
</tr>
<tr>
<td>142</td>
<td>NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION</td>
<td>Skipped ICA parsing for this receiver (client) as it is not in the allow list</td>
</tr>
<tr>
<td>143</td>
<td>NS_ICA_ERR_LOOKUP_RECONNECT_ID</td>
<td>Unable to detect parsing state for client reconnect cookie</td>
</tr>
<tr>
<td>144</td>
<td>NS_ICA_ERR_SYNCUP_RECONNECT_ID</td>
<td>Invalid reconnect cookie length detected post client reconnect</td>
</tr>
<tr>
<td>145</td>
<td>NS_ICA_ERR_INVALID_RECONNECT_ID</td>
<td>Client reconnects cookie missed the needed constraint</td>
</tr>
<tr>
<td>146</td>
<td>NS_ICA_ERR_INVALID_CLIENT_VERSION</td>
<td>Invalid receiver version string received from client</td>
</tr>
<tr>
<td>147</td>
<td>NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID</td>
<td>Invalid product ID received from client</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>148</td>
<td>NS_ICA_ERR_V3_HDR_CORRUPT</td>
<td>Invalid channel length post expansion</td>
</tr>
<tr>
<td>149</td>
<td>NS_ICA_ERR_SPECIAL_THINWIRE</td>
<td>Decompression error</td>
</tr>
<tr>
<td>150</td>
<td>NS_ICA_ERR_SEAMLESS_INSUFFBYTE</td>
<td>Encountered insufficient bytes for seamless command</td>
</tr>
<tr>
<td>151</td>
<td>NS_ICA_ERR_EUEM_INSUFFBYTE</td>
<td>Encountered insufficient bytes for EUEM command</td>
</tr>
<tr>
<td>152</td>
<td>NS_ICA_ERR_SEAMLESS_INVALID_EVENT</td>
<td>Invalid event for seamless channel parsing</td>
</tr>
<tr>
<td>153</td>
<td>NS_ICA_ERR_CTRL_INVALID_EVENT</td>
<td>Invalid event for CTRL channel parsing</td>
</tr>
<tr>
<td>154</td>
<td>NS_ICA_ERR_EUEM_INVALID_EVENT</td>
<td>Invalid event for EUEM channel parsing</td>
</tr>
<tr>
<td>155</td>
<td>NS_ICA_ERR_USB_INVALID_EVENT</td>
<td>Invalid event for USB channel parsing</td>
</tr>
<tr>
<td>156</td>
<td>NS_ICA_ERR_PURE_INVALID_EVENT</td>
<td>Invalid event for pure channel parsing</td>
</tr>
<tr>
<td>157</td>
<td>NS_ICA_ERR_VCP_INVALID_EVENT</td>
<td>Invalid event for virtual channel parsing</td>
</tr>
<tr>
<td>158</td>
<td>NS_ICA_ERR_ICAP_INVALID_EVENT</td>
<td>Invalid event for ICA data parsing</td>
</tr>
<tr>
<td>159</td>
<td>NS_ICA_ERR.CGPP_INVALID_EVENT</td>
<td>Invalid event for CGP data parsing</td>
</tr>
<tr>
<td>160</td>
<td>NS_ICA_ERR_BASICCRYPT_INVALIDSTATE</td>
<td>Invalid state for a crypt command in basic encryption</td>
</tr>
<tr>
<td>161</td>
<td>NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD</td>
<td>Invalid crypt command in basic encryption</td>
</tr>
<tr>
<td>162</td>
<td>NS_ICA_ERR_ADVCRYPT_INVALIDSTATE</td>
<td>Invalid state for a crypt command in RC5 encryption</td>
</tr>
<tr>
<td>163</td>
<td>NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD</td>
<td>Invalid crypt command in RC5 encryption</td>
</tr>
<tr>
<td>164</td>
<td>NS_ICA_ERR_ADVCRYPT_ENC</td>
<td>Error in RC5 encryption/decryption</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>165</td>
<td>NS_ICA_ERR_ADVCRYPT_DEC</td>
<td>Error in RC5 encryption/decryption</td>
</tr>
<tr>
<td>166</td>
<td>NS_ICA_ERR_SERVER_NOT_RECERVER</td>
<td>VDA does not support Reducer Version 3</td>
</tr>
<tr>
<td>167</td>
<td>NS_ICA_ERR_CLIENT_NOT_RECERVER</td>
<td>Receiver does not support Reducer Version 3</td>
</tr>
<tr>
<td>168</td>
<td>NS_ICA_ERR_ICAP_INSUFFBYTE</td>
<td>Unexpected number of bytes in ICA handshake</td>
</tr>
<tr>
<td>169</td>
<td>NS_ICA_ERR_HIGHER_RECONS</td>
<td>Higher CGP resumption sequence number from peer post reconnects</td>
</tr>
<tr>
<td>170</td>
<td>NS_ICA_ERR_DESCRINFO_ABSENT</td>
<td>Unable to restore ICA parsing state post reconnect</td>
</tr>
<tr>
<td>171</td>
<td>NS_ICA_ERR_NSAP_PARSING</td>
<td>Error while parsing Insight channel data</td>
</tr>
<tr>
<td>172</td>
<td>NS_ICA_ERR_NSAP_APP</td>
<td>Error while parsing app details from Insight channel data</td>
</tr>
<tr>
<td>173</td>
<td>NS_ICA_ERR_NSAP_ACR</td>
<td>Error while parsing ACR details from Insight channel data</td>
</tr>
<tr>
<td>174</td>
<td>NS_ICA_ERR_NSAP_SESSION_END</td>
<td>Error while parsing session end details from Insight channel data</td>
</tr>
<tr>
<td>175</td>
<td>NS_ICA_ERR_NON_NSAP_SN</td>
<td>Skipped ICA parsing on service node due to the absence of Insight channel support</td>
</tr>
<tr>
<td>176</td>
<td>NS_ICA_ERR_NON_NSAP_CLIEI</td>
<td>NSAP is not supported by client</td>
</tr>
<tr>
<td>177</td>
<td>NS_ICA_ERR_NON_NSAP_SERVER</td>
<td>NSAP is not supported by VDA</td>
</tr>
<tr>
<td>178</td>
<td>NS_ICA_ERR_NSAP_NEG.Fail</td>
<td>Error while NSAP data negotiation</td>
</tr>
<tr>
<td>Skip Code</td>
<td>Error message</td>
<td>Cause of error</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>179</td>
<td>NS_ICA_ERR_SN_RECONNECT_TKT_FETCH</td>
<td>Error in fetching service reconnects ticket in service node</td>
</tr>
<tr>
<td>180</td>
<td>NS_ICA_ERR_SN_HIGHER_RECONSEQ</td>
<td>Error when receiving higher reconnect sequence number in service node</td>
</tr>
<tr>
<td>181</td>
<td>NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP</td>
<td>Error while disabling HDX Insight for non-NSAP connections</td>
</tr>
</tbody>
</table>

**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 [57af35043e624ab0f5e6af7fd22c], 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 [0x88202202028], 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 [4e3a91175ebce686af175e9c7e0200], 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 [0x88202202008], 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.
<table>
<thead>
<tr>
<th>HDX counter name</th>
<th>Purpose</th>
<th>Category(Stats/Error/Diagnostics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdx_tot_ica_conn</td>
<td>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.</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_tot_cgp_conn</td>
<td>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.</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_dbg_tot_udt_conn</td>
<td>Indicates total number of UDP ICA connections detected by NS</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_dbg_tot_nsap_conn</td>
<td>Indicates total number of NSAP supported connections detected by NS</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_tot_skip_conn</td>
<td>Indicates how many ICA connections were skipped by parser due to invalid ICA or CGP signature.</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_dbg_active_conn</td>
<td>Total Active EDT/CGP/ICA connections at that instant.</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_dbg_active_nsap_conn</td>
<td>Total Active EDT/CGP/ICA NSAP connections at that instant.</td>
<td>Stats</td>
</tr>
<tr>
<td>hdx_dbg_skip_appflow_disabled</td>
<td>Total number of instances where AppFlow was detached from a session because of disabling AppFlow</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>HDX counter name</td>
<td>Purpose</td>
<td>Category(Stats/Error/Diagnostics)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>hdx dbg transparent_user</td>
<td>Total number of transparent user access</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx dbg ag_user</td>
<td>Total number of Access Gateway user access</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx dbg lan_user</td>
<td>Total number of LAN user mode access</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx_basic_enc</td>
<td>Indicates the number of ICA connections using basic encryption</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx_advanced_enc</td>
<td>Indicates the number of ICA connections using advanced RC5 based encryption</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx dbg reconnected_session</td>
<td>Total number of reconnect requests from client without any Citrix ADC error</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx dbg host_rejected ns rec</td>
<td>Total number of hosts rejected reconnects requests by client</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx_euem_available</td>
<td>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.</td>
<td>Stats/Diagnostics</td>
</tr>
<tr>
<td>hdx_err_disabled_sr</td>
<td>Session Reliability is disabled using nsapimgr knob. Session does not work for this session.</td>
<td>Error</td>
</tr>
<tr>
<td>HDX counter name</td>
<td>Purpose</td>
<td>Category (Stats/Error/Diagnostics)</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>hdx_err_skip_no_msi</td>
<td>XA/XD server is Missing MSI capability. This indicates an older server version, HDX Insight skips this connection.</td>
<td>Error</td>
</tr>
<tr>
<td>hdx_err_skip_old_server</td>
<td>Old unsupported server version</td>
<td>Error</td>
</tr>
<tr>
<td>hdx_err_clnt_not_whitelist</td>
<td>Client receiver not in allow list, HDX Insight skips this connection</td>
<td>Error</td>
</tr>
<tr>
<td>hdx_sm_ica_cam_channel_disabled</td>
<td>Total number of NS_ICA_CAM_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_usb_channel_disabled</td>
<td>Total number of NS_ICA_USB_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_clip_channel_disabled</td>
<td>Total number of NS_ICA_CLIP_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_ccm_channel_disabled</td>
<td>Total number of NS_ICA_CCM_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_cdm_channel_disabled</td>
<td>Total number of NS_ICA_CDM_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_com1_channel_disabled</td>
<td>Total number of NS_ICA_COM1_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>HDX counter name</td>
<td>Purpose</td>
<td>Category (Stats/Error/Diagnostics)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>hdx_sm_ica_com2_channel_disabled</td>
<td>Total number of NS_ICA_COM2_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_cpm_channel_disabled</td>
<td>Total number of NS_ICA_CPM_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_lpt1_channel_disabled</td>
<td>Total number of NS_ICA_LPT1_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_lpt2_channel_disabled</td>
<td>Total number of NS_ICA_LPT2_CHANNEL disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>dx_dbg_sm_ica_msi_disabled</td>
<td>Total number of cases where MSI is disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_sm_ica_file_channel_disabled</td>
<td>Total number of NS_ICA_FILE_CHANNEL is disabled via SmartAccess policy</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_accept_device</td>
<td>Total number of USB devices accepted</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_reject_device</td>
<td>Total number of USB devices rejected</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_reset_endpoint</td>
<td>Total number of USB endpoints reset</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_reset_device</td>
<td>Total number of USB devices reset</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_stop_device</td>
<td>Total number of USB devices stopped</td>
<td>Diagnostics</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>HDX counter name</th>
<th>Purpose</th>
<th>Category(Stats/Error/Diagnostics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdx_dbg_usb_stop_device_response</td>
<td>Total number of responses from stopped USB devices</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_device_gone</td>
<td>Total number of USB devices gone</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>hdx_dbg_usb_device_stopped</td>
<td>Total number of USB devices stopped</td>
<td>Diagnostics</td>
</tr>
</tbody>
</table>

**nstrace validation**

Check for CFLOW protocol to see all AppFlow records going out of Citrix ADC.

**Population of records in Citrix ADM checklist**

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` and check logs to confirm Citrix ADM is receiving AppFlow records.
  - Confirm Citrix ADC instance is added to Citrix ADM.
  - Validate Citrix Gateway/VPN virtual server is licensed in Citrix ADM.
  - 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 ADM 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 ADM.
Citrix Application Delivery Management service

- 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**

February 15, 2022

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**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Hits</td>
<td>Total number of hits received by a virtual server (application)</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by the virtual server (application)</td>
</tr>
<tr>
<td></td>
<td>Response Time (ms)</td>
<td>The time taken for the virtual server to respond</td>
</tr>
<tr>
<td>Clients</td>
<td>Requests</td>
<td>The total request received by a client</td>
</tr>
<tr>
<td>Metrics</td>
<td>Entity</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Render Time (ms)</td>
<td></td>
<td>The time taken to render server response by the client</td>
</tr>
<tr>
<td>Client Network Latency</td>
<td></td>
<td>The time taken for requests from the client network</td>
</tr>
<tr>
<td>Devices</td>
<td>Hits</td>
<td>Total number of hits received by a device. For example: laptop, mobile phone</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by a device</td>
</tr>
<tr>
<td>Domains</td>
<td>Hits</td>
<td>Total number of hits received by a network domain</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by a network domain</td>
</tr>
<tr>
<td></td>
<td>Response Time (ms)</td>
<td>The time taken to respond requests by a network domain</td>
</tr>
<tr>
<td>Operating System</td>
<td>Hits</td>
<td>Total number of hits received by an operating system</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by an operating system</td>
</tr>
<tr>
<td></td>
<td>Render Time (ms)</td>
<td>The time taken to render server response by an operating system</td>
</tr>
<tr>
<td>Request Methods</td>
<td>Hits</td>
<td>Total number of requests received by a Request Method. For example: GET, POST</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by a Request Method</td>
</tr>
<tr>
<td>Response Status</td>
<td>Hits</td>
<td>Total number of hits received with response codes</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by response code</td>
</tr>
</tbody>
</table>
## Metrics Entity Description

<table>
<thead>
<tr>
<th>Servers</th>
<th>Hits</th>
<th>Total number of requests/hits received by a server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by a server</td>
</tr>
<tr>
<td></td>
<td>Server Network Latency (ms)</td>
<td>The time taken for requests from the server network</td>
</tr>
<tr>
<td></td>
<td>Server Processing Time (ms)</td>
<td>The time taken by a server to respond to requests</td>
</tr>
<tr>
<td>URLs</td>
<td>Hits</td>
<td>Total number of hits received by a URL. For example: <a href="http://www.Citrix.com">www.Citrix.com</a></td>
</tr>
<tr>
<td></td>
<td>Load Time (ms)</td>
<td>The time taken for a URL to load from the server</td>
</tr>
<tr>
<td></td>
<td>Render Time (ms)</td>
<td>The time taken by the URL to render and display</td>
</tr>
<tr>
<td>User Agents</td>
<td>Hits</td>
<td>Total number of requests received by a user agent. For example: Chrome web browser</td>
</tr>
<tr>
<td></td>
<td>Bandwidth (MB)</td>
<td>Total bandwidth consumed by the user agent</td>
</tr>
<tr>
<td></td>
<td>Render Time (ms)</td>
<td>The time taken to render the server response by the user agent</td>
</tr>
</tbody>
</table>

### Security

© 1999–2022 Citrix Systems, Inc. All rights reserved.
## Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Metric</th>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications</strong></td>
<td>Threat Index</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Safety Index</td>
<td>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.</td>
</tr>
</tbody>
</table>

### APPANALYTICS

<table>
<thead>
<tr>
<th>Metric</th>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications</strong></td>
<td>AppScore</td>
<td>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.</td>
</tr>
</tbody>
</table>

### HDX

For information on HDX thresholds, see [Create thresholds and configure alerts for HDX Insight](#)
Infrastructure Analytics

February 15, 2022

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 ADM

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 ADM.

  - **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 ADM that are configured with critical severity.

  - **HA sync failure.** Configuration sync between the ADC instances in high availability has failed on the secondary server.
- **HA no heartbeats.** The primary server in a pair of ADC instances in high availability is not receiving heartbeats from 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 ADM, 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 issues 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 usage value crosses the high threshold.

**Infrastructure analytics dashboard**

Navigate to **Infrastructure > Infrastructure Analytics**.

The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.

- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view formats, the Summary Panel displays details of all the instances in your network.

**Circle pack view**

Circle packing diagrams show instance groups as tightly organized circles. They often show hierarchies where smaller instance groups are either colored similarly to others in the same category, or nested within larger groups. Circle packs represent hierarchical data sets and shows different levels in the hierarchy and how they interact with each other.
Instance circles

Color. Each instance is represented in Circle Pack as a colored circle. The color of the circle indicates the health of that instance.

- **Green** - instance score is between 100 and 80. The instance is healthy.
- **Yellow** - instance score is between 80 and 50. Some issues have been noticed and in need of review.
- **Red** - instance score is below 50. The instance is in a critical stage as there are multiple issues noticed on that instance.
**Size.** The size of these colored circles indicates the number of virtual servers configured on that instance. A bigger circle indicates that there are a greater number of virtual servers.

You can hover the mouse pointer on each of the instance circles (colored circles) to view a summary. The hover tool tip displays the host name of the instance, the number of active virtual servers and the number of applications configured on that instance.
Grouped instance circles

The Circle Pack at the outset, comprises instance circles that are grouped, nested, or packed inside another circle based on the following criteria:

- the site where they are deployed
- the type of instances deployed - VPX, MPX, SDX, and CPX
- the virtual or physical model of the ADC instance
- the ADC image version installed on the instances

The following image shows a Circle Pack where the instances are first grouped by the site or data center where they are deployed, and then they are further grouped based on their type, VPX, and MPX.
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the Citrix ADM (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

**Clustered instance circles**

Citrix ADM monitors many instances. To ease the monitoring and maintenance of these instances, Infrastructure Analytics allows you to cluster them at two levels. That is, the instance groupings can be nested within another grouping.

For example, the BLR data center has two types of ADC instances - VPX and MPX, deployed in it. You can first group the ADC instances by their type and then group all instances by the site where they are grouped. You can now easily identify how many types of instances are deployed in the sites that you are managing.
A few more examples of two-level clustering are as follows:

**Site and model:**
Type and version:
Site and version:
How to use Circle Pack

Click each of the colored circle to highlight that instance.
Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.

You can also click the health indicators to get more details on the number of instances that have reported that risk indicator. For example, click Not recommended Algo to view the summary report of that risk indicator.
Tabular view

The tabular view displays the instances and the details of those instances in a tabular format. 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
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.

![Diagram showing instances in multiple ranges](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.
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.

• Set the low and high threshold values for high CPU usage, high disk usage, and high memory usage.

• Select the instance metrics, configure thresholds, and assign weightage for those metrics to calculate the instance score

• Select the required issues, enable notifications for issues that breach the configured thresholds, and receive notifications only for the selected issues.

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 ADM.

• Circle Pack - Instance Size. Allow the size of the instance circle to be 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.
Select metrics and customize weightage for instance score calculation

You can select the instance metrics, configure thresholds, and assign weightage for those metrics to calculate the instance score. By default, all metrics are selected, and default weightage is assigned to each metric. You can select metrics depending upon your requirement and assign a suitable weightage to determine the instance score calculation.

Click the Settings icon and select the Score Indicator Settings tab to:

- Select the required metrics and add thresholds
- Assign the weightage for metrics.

After you configure thresholds and assign weightage, click Save. The instance score is updated only based on the selected metrics and their weightage.
Configure notifications

You can select the required issues, enable notifications for issues that breach the configured thresholds, and receive notifications only for the selected issues. This enhancement enables you to receive notifications only for the selected issues that you want to monitor.

Note

By default, issues under all categories are selected. You can enable notification only for the issues that you can configure thresholds.

1. Click the **Settings** icon and select the **Score Indicator Settings** tab.
2. Select the issues that you want to receive notifications.
3. For the issues under **System Resource** and **Capacity** categories, enable the **Notification**.
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 find out 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**

February 15, 2022

1. Navigate to Infrastructure > Infrastructure Analytics.
2. Click the circle pack view and select the IP address.

![Diagram showing instance details in Infrastructure Analytics](image)

You can also click an IP address from the table view.
- **Hostname** – 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.

- **HOST NAME**: 217ns
- **SYSTEM IP ADDRESS**: 10.106.181.217
- **SYSTEM NAME**: NetScaler
- **TYPE**: Citrix ADC VPX
- **HA MASTER STATE**: Primary
- **HOST ID**: 000c29e1c592
- **SYSTEM SERVICES**: 72
- **NETMASK**: 255.255.255.0
- **GATEWAY**: 10.106.181.1
- **SYSTEM CUSTOM ID**: Default
- **PACKET ENGINES**: 1
- **SSL CARDS**: 0
- **CPU**: 2099MHZ
- **VERSION**: NetScaler NS11.1: Build 62.8nc
- **HARDWARE VERSION**: NetScaler Virtual Appliance
- **LOM VERSION**: -NA-
- **HA SYNC STATUS**: ENABLED
- **SERIAL NUMBER**: HE2H81J47
- **ENCODED SERIAL NUMBER**: 891e0000cb254307ee9a
- **LOCATION**: Citrix ADC UUID
- **CONTACT PERSON**: WebMaster (default)
- **DESCRIPTION**: 25 days, 19 hours, 42 minutes

• **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.
Citrix Application Delivery Management service

The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**

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).

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.
Citrix Application Delivery Management service

- **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:

<table>
<thead>
<tr>
<th>Issue Category</th>
<th>Description</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Resources</td>
<td>Displays all issues related to the Citrix ADC system resource such as CPU, Memory, disk usage, and so on.</td>
<td>- High CPU Usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- High Memory Usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- High Disk Usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SSL Card Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Power Failure</td>
</tr>
<tr>
<td>SSL Config</td>
<td>Displays all issues related to the SSL configuration on the Citrix ADC instance.</td>
<td>- SSL Certs Expired</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Not Recommended Issuer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Not Recommended Algo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Not Recommended Key Strength</td>
</tr>
<tr>
<td>Config Deviation</td>
<td>Displays all issues related to the configuration jobs applied in Citrix ADC instance.</td>
<td>- Config Drift</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Running vs Template</td>
</tr>
</tbody>
</table>
## Issue Category | Description | Issues
--- | --- | ---
**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
- HA Version Mismatch

**Capacity issues** | Displays ADC capacity issues. The Citrix ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters. | - Throughput Limit Reached
- 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:
- The **Current** tab displays the issues that are currently affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

**View the capacity issues in an ADC instance**

February 15, 2022

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 ADM recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

1. In **Infrastructure > Infrastructure Analytics**, select the tabular view.
2. Select the instance that has capacity issues and click **Details**.
3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.

The Citrix ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists.

The Citrix ADM calculates the instance score on the defined capacity threshold.

- **Low threshold** – 1 packet drop or rate-limit counter increment
- **High threshold** – 10000 packets drop or rate-limit counter increment

Therefore, when an ADC instance breaches the capacity threshold, the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the **ADCCapacityBreach** category. To view these events, navigate to **Settings > Citrix ADM System Events**.
Enhanced Infrastructure Analytics with new indicators

February 15, 2022

Using the Citrix ADM 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 ADM, navigate to Infrastructure > Infrastructure Analytics to view indicators for:

<table>
<thead>
<tr>
<th>Indicator name in Infrastructure Analytics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port allocation failure</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Session Buildup</strong></td>
<td>Detects when Citrix ADC memory is held up by SSL sessions.</td>
</tr>
<tr>
<td><strong>No default route configuration</strong></td>
<td>Detects when the traffic gets dropped because of non-availability of routes.</td>
</tr>
<tr>
<td><strong>IP conflict</strong></td>
<td>Detects if a same IP address is configured or applied on two or more instances in a network.</td>
</tr>
<tr>
<td>Indicator name in Infrastructure Analytics</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>VRID conflict</strong></td>
<td>Detects when intermittent access problems occur for the specified VRID.</td>
</tr>
<tr>
<td><strong>VLAN mismatch</strong></td>
<td>Detects if any errors occur during VLAN configuration bound to IP subnets.</td>
</tr>
<tr>
<td><strong>TCP small window attack</strong></td>
<td>Detects when there is a possible small window attack in progress. This alert is just for informational, because ADC already mitigates this attack.</td>
</tr>
<tr>
<td><strong>Rate control threshold</strong></td>
<td>Detects when packets are dropped based on the configured rate control threshold.</td>
</tr>
<tr>
<td><strong>Persistence Limit</strong></td>
<td>Detects when maximum hits are imposed on the Citrix ADC memory.</td>
</tr>
<tr>
<td><strong>GSLB site name mismatch</strong></td>
<td>Detects when GSLB configuration synchronization failures occur because of site name mismatch.</td>
</tr>
<tr>
<td><strong>Malformed IP header</strong></td>
<td>Detects when sanity checks on IPv4 packets are failed.</td>
</tr>
<tr>
<td><strong>Bad L4 checksums</strong></td>
<td>Detects when checksum validation for TCP packets is failed.</td>
</tr>
<tr>
<td><strong>Increased CPU usage due to IP move</strong></td>
<td>Detects if a large number of macs need to be updated.</td>
</tr>
<tr>
<td><strong>Excessive packet steering</strong></td>
<td>Detects high levels of software packet steering due to the usage of asymmetric rss key type.</td>
</tr>
<tr>
<td><strong>Layer 2 loop</strong></td>
<td>Detects the presence of layer 2 loops in the network.</td>
</tr>
<tr>
<td><strong>Tagged VLAN mismatch</strong></td>
<td>Detects when tagged VLAN packets are received on an untagged interface.</td>
</tr>
</tbody>
</table>
Tabular view

You can also view anomalies using the tabular view option in Infrastructure Analytics. Navigate to Infrastructure > Infrastructure Analytics and then click to display all managed instances. Click to expand for details.
View details of an anomaly

For example, if you want to view details for IP address conflict in the network, click the anomaly that is displayed for IP address conflict.
Instance management

February 15, 2022

Instances are Citrix Application Delivery Controller (ADC) appliances that you can manage, monitor, and troubleshoot using Citrix ADM. Add instances to Citrix ADM to monitor them. Instances can be added when you set up Citrix ADM or later as well. After you add instances to Citrix ADM, they are continuously polled to collect information that can later be used to resolve issues or as reporting data.

Instances can be grouped as a static group or as a private IP-block. A static group of instances can be useful when you want to run specific tasks such as configuration jobs, and 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 ADM 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 ADM, see Add Instances to Citrix ADM.

When you add an instance to the Citrix ADM 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 ADM 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 ADM displays data in a tabular and graphical format for the selected instance. Data collected from your instance during the polling process is displayed on the dashboard.

By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.
To view a specific instance's dashboard, navigate to **Infrastructure > Instances > Citrix ADC**. On the Citrix ADC page, choose the instance type and then, select the instance you want to view and click **Dashboard**.

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:
• **Overview.** The overview tab displays the CPU and memory usage of the chosen instance. You can also view events generated by the instance and the throughput data. Instance-specific information such as the IP address, its hardware and LOM versions, the profile details, serial number, contact person, and 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

February 15, 2022

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 ADM provides you with a graphical representation of your sites and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

The following sections explain how you can monitor data centers in Citrix ADM.

#### Monitoring globally distributed sites in Citrix ADM

Citrix ADM 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 ADM manages and monitors all Citrix ADC instances connected to all sites. You can use Citrix ADM to monitor and collect syslog, AppFlow, SNMP, and any such data originating from the managed instances.

Geomaps in Citrix ADM provides you with a graphical representation of your sites. Geomaps also breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor all network issues. You can click **Infras-**
structure 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.
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.
Example Company 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 ADM. You must also add the instance to the site, add an agent, and bind the agent to the site. Citrix ADM 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 ADM. Providing location information allows you to locate the site precisely.

1. In Citrix ADM, 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.
Citrix Application Delivery Management service

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 automatically.

d) Click **Create** to create a site in Bangalore.

**To add instances and select sites:**

After creating sites, you must add instances in Citrix ADM. You can select the previously created site,
or you can also create a site and associate the instance.

1. In Citrix ADM, 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.

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**.

   a) Select the site from the list and click **Save**.
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 ADM agent with the site:**

1. In Citrix ADM, navigate to Infrastructure > Instances > Agents.
2. Select the agent, and click Attach Site.
3. You can associate the site and click Save.

Citrix ADM 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

February 15, 2022

Citrix ADM 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 ADM, 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.
You can also add multiple tags by clicking “+”. Adding multiple and meaningful tags allows you to efficiently search for the instances.
You can add multiple values to a keyword by separating them with commas.

For example, you are assigning 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 ADM recognizes the comma separated values into two different values.

To know more about how to search for instances based on tags, see How to search instances using values of tags and properties.
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

February 15, 2022

There might be a situation where Citrix ADM 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 ADM 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 ADM has a few default parameters or properties associated with that instance. For example, each instance has its own host name, IP address, version, host ID, hardware model ID and so on. You can search for instances by specifying values for any of these properties.

For example, consider a situation where you want to find out the list of 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 ADM, 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 ADM 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.
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”.

**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**

February 15, 2022

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 ADM provides a seamless way of managing all partitions owned by an administrator from a single console. You can manage these partitions without disrupting other partition configurations.

To allow multiple users to manage different admin partitions, you have to create groups and then, assign users and partitions to those groups. 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 ADM.
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**.

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.
- “User1” is assigned to the 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:

- 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.

![Configuration Audit Dashboard](image1.png)

2. Select the partitioned Citrix ADC instance.

3. From the Action box, click **Revision History Diff**.

![Revision History Diff](image2.png)

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:
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).

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:
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.
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

February 15, 2022

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 ADM to perform automatic backups and manual restores. Citrix ADM 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 ADM creates a complete backup and restores the following Citrix ADC instance types:

- Citrix ADC SDX
Citrix Application Delivery Management service

- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

For more information, see Backup and restore an ADC instance.

**Note**
- From Citrix ADM, 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/
```

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 ADM. 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 ADM**

Perform this task if you want to back up a selected Citrix ADC instance or multiple instances:

1. In Citrix ADM, 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 ADM server and then perform the restore operation.

To transfer a Citrix ADM 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.

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.
Restore a Citrix ADC instance by using Citrix ADM

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
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 ADM**

In Citrix ADM, 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 ADM 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**.

   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

February 15, 2022
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 ADM:**

1. In Citrix ADM, 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.
Force a secondary Citrix ADC instance to stay secondary

February 15, 2022

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 ADM:

1. In Citrix ADM, 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.
Create instance groups

February 15, 2022

To create an instance group, you must first add all your Citrix ADC instances to Citrix ADM. After you have added the instances successfully, create instance groups based on their instance family. Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

To create an instance group using Citrix ADM

1. In Citrix ADM, 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.

Provision ADC VPX instances on SDX

February 15, 2022

You can provision one or more ADC VPX instances on the SDX appliance by using Citrix ADM. The number of instances that you can deploy depends on the license you have purchased. If the number of
Citrix Application Delivery Management service

instances added is equal to the number specified in the license, the Citrix ADM does not allow you to provision more Citrix ADC instances.

Before you begin, ensure to add an SDX instance in Citrix ADM 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.

Step 1 - Add a VPX instance

The Citrix ADM uses the following information to configure VPX instances in an SDX appliance:

- **Name** - Specify a name to an ADC instance.
- **Establish a communication network between SDX and VPX. To do so, select the required options from the list:
  
  - **Manage through internal network** - This option establishes an internal network for a communication between the Citrix ADM 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 ADM 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 ADM file browser.
• **Admin Profile** - This profile provides access to provision VPX instances. With this profile, Citrix ADM retrieves the configuration data from an instance. If you have to add a profile, click **Add**.

• **Agent** - Select the agent with which you want to associate the instances

• **Site** - Select the site where you want the instance to be added.
Step 2 - Allocate licenses

In the License Allocation section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- Allocation mode - You can choose Fixed or Burstable modes for the bandwidth pool.

  If you choose Burstable mode, you can use extra bandwidth when the fixed bandwidth is reached.

- Throughput - Assign the total throughput (in Mbps) to an instance.

Note

Buy a separate license (SDX 2-Instance Add-On Pack for Secure Web Gateway) for Citrix Secure Web Gateway (SWG) instances on SDX appliances. This instance pack is different from the SDX platform license or SDX instance pack.

For more information, see Deploying a Citrix Secure Web Gateway Instance on an SDX Appliance.

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.

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.
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.
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.
Click Add.

**Step 6 - Specify Management VLAN settings**

The Management Service and the management address (NSIP) of the VPX instance are in the same subnetwork, and communication is over a management interface.

If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

If your deployment requires the NSIP is accessible only through the selected interface while provisioning the VPX instance, select **NSVLAN**. And, the NSIP becomes inaccessible through other interfaces.

- HA heartbeats are sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from the VPX XVA build 9.3-53.4 and later.
Important

- You cannot change this setting after you provision the VPX instance.
- The `clear config full` command on the VPX instance deletes the VLAN configuration if NSVLAN is not selected.

Click **Done** to provision a VPX instance.

**View the provisioned VPX instance**

To view the newly provisioned instance, do the following:

1. Navigate to **Infrastructure > Instances > Citrix ADC**.
2. In the **VPX** tab, search an instance by the **Host IP address** property and specify SDX instance IP to it.
Rediscover multiple Citrix ADC instances

February 15, 2022

You can rediscover multiple Citrix Application Delivery Controller (Citrix ADC) instances (VPX, MPX, SDX, BLX, and CPX) in your Citrix ADM setup. After you rediscover the instances, you can view the latest states and configurations of those instances. The Citrix ADM 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.

The screen reports the progress of rediscovery of each of the ADC instances.
Polling overview

February 15, 2022

Polling is a process, where Citrix ADM 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 ADM, Citrix ADM 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 ADM and the managed instances:

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

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

How Citrix ADM polls managed instances and entities

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

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

<table>
<thead>
<tr>
<th>Polling type</th>
<th>Polling interval</th>
<th>Polled information</th>
<th>Protocol used</th>
<th>Polling interval configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance polling</strong></td>
<td>Every 5 minutes (by default)</td>
<td>Statistical information such as state, HTTP requests per second, CPU usage, memory usage, and throughput.</td>
<td>NITRO call.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Inventory polling</strong></td>
<td>Every 60 minutes (by default)</td>
<td>Inventory details such as build version, system information, licensed features, and modes.</td>
<td>NITRO calls and SSH</td>
<td>No</td>
</tr>
<tr>
<td><strong>Performance data collection</strong></td>
<td>Every 5 minutes (by default)</td>
<td>Network reporting information</td>
<td>NITRO call</td>
<td>No</td>
</tr>
</tbody>
</table>
### Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Polling type</th>
<th>Polling interval</th>
<th>Polled information</th>
<th>Protocol used</th>
<th>Polling interval configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance backup polling</strong></td>
<td>Every 12 hours (by default)</td>
<td>The backup file of the current state of the managed ADC instances</td>
<td>NITRO calls, SSH, and SCP.</td>
<td>Yes. Navigate to Infrastructure &gt; Instances &gt; Citrix ADC. Select the instance and from the <strong>Select Action</strong> list, click <strong>Backup/Restore</strong>.</td>
</tr>
<tr>
<td><strong>Configuration audit polling</strong></td>
<td>Every 10 hours (by default)</td>
<td>Configuration changes that occur on ADC instances (for example, running vs. saved configuration)</td>
<td>SSH, SCP, and NITRO call</td>
<td>Yes. Navigate to Infrastructure &gt; Configuration &gt; Configuration Audit. On the Configuration Audit page, click <strong>Settings</strong> and configure the polling interval for Configuration Audit Polling.</td>
</tr>
<tr>
<td>Polling type</td>
<td>Polling interval</td>
<td>Polled information</td>
<td>Protocol used</td>
<td>Polling interval configuration</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>SSL certificates polling</td>
<td>Every 24 hours (by default)</td>
<td>SSL certificates that are installed on Citrix ADC instances.</td>
<td>NITRO calls and SCP</td>
<td>Yes. Navigate to Infrastructure &gt; SSL Dashboard. On the SSL Dashboard page, click Settings to configure the polling interval.</td>
</tr>
</tbody>
</table>
You can poll SSL certificates manually and add all certificates of the instances immediately to Citrix ADM. 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.

### Entity polling

<table>
<thead>
<tr>
<th>Polling type</th>
<th>Polling interval</th>
<th>Polled information</th>
<th>Protocol used</th>
<th>Polling interval configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity polling</td>
<td>Every 60 minutes (by default)</td>
<td>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 <strong>Enable or disable Citrix ADM features</strong>.</td>
<td>NITRO calls.</td>
<td>Yes, but cannot be set to less than 10 minutes. To configure, navigate to <strong>Infrastructure &gt; Network Functions</strong>. On the Networks Function page, click <strong>Settings</strong> to configure the polling interval.</td>
</tr>
</tbody>
</table>
You can poll entities manually and add all entities of the instances immediately to Citrix ADM. 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 ADM through SNMP traps sent to the instances. For example, an event is generated when there is a system failure or change in configuration.

During instance backup, SSL files, CA certificate files, ADC templates, database information, and so on are downloaded to Citrix ADM. 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 ADM performs on the managed instances:

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

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

In Citrix ADM, 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 ADM does not recognize the new instance or the updates made to an entity until the next polling happens. And, there is no way to immediately get a list of virtual IP addresses for further operations. You must wait for the minimum polling interval period to elapse. Though you can do a manual poll to discover newly added instances, this leads to the entire Citrix ADC network to be polled, which creates a heavy load on the network.

Instead of polling the entire network, Citrix ADM now allows you to poll only selected instances and entities at any given time.

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

To poll specific instances in Citrix ADM:

1. In Citrix ADM, navigate to Infrastructure > Network Functions.
2. On Network Functions page, at the top right-hand corner, click Poll Now.
3. The pop-up page Poll Now provides you an option to poll all 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.
Citrix ADM initiates manual polling and adds all the entities.
Manual polling of entities

Citrix ADM 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 ADM polls only that entity and updates the status in the Citrix ADM 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 ADM:**

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

1. In Citrix ADM, 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**.
Unmanage an instance

February 15, 2022

If you want to stop the exchange of information between Citrix ADM 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**.

The status of the selected instance changes to **Out of Service**.

The instance is no longer managed by Citrix ADM, and it no longer exchanges data with Citrix ADM.
Trace the route to an instance

February 15, 2022

By tracing the route of a packet from the Citrix ADM 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.
How to change the Citrix ADC MPX or VPX root password

February 15, 2022

Occasionally, you must change the root password of the Citrix ADC appliance for security reasons or compliance of password rotation policy.

This document describes the steps required to change the root password of the Citrix ADC MPX and VPX appliances managed through Citrix ADM cloud.

If you change the ADC password, you must modify the Citrix ADM admin profile that is associated with the ADC. An Citrix ADM admin profile maintains the ADC credentials for REST API, SSH, SCP, or SNMP based communication with the ADC appliance. Through admin profiles, Citrix ADM manages Citrix ADC MPX and VPX appliances.
Change password using the Configuration Jobs feature

By using the Citrix ADM Configuration Jobs feature, you can simplify the repetitive password change process and apply the changes to the Citrix ADC appliances, without accessing the individual instances.

Follow these steps to change the password:

• Step 1. Create a Configuration Template.
• Step 2. Create a Configuration Job.
• Step 3. Create an admin profile and modify it.

Note: If the ADC appliances are managed by other tools as well, you must change the credentials on those tools as well.

Create a Configuration Template

1. From the Citrix ADM GUI, navigate to Infrastructure > Configuration Jobs > Configuration Templates.

2. Select Add. Create a Configuration Template with by typing the SSH command set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$.
3. Select the $ROOT_USER_NAME$ variable, and select **TextField as Type**.

4. Optionally, provide the default value for the root user name. Select **Done** to save the variable settings.

5. Select the $ROOT_USER_PASSWORD$ variable, and select **Password Field as Type**. Select **Done** to save the variable settings.

6. Select **OK** to save the Configuration Template.

7. The new Configuration Template appears under **Configuration Templates**.
1. From the Citrix ADM GUI, navigate to Infrastructure > Configuration Jobs.

2. Select Create Job and click the “+” icon of the new configuration template. Select Next.

3. Select the ADC instance or instances for which the password must be modified.
4. In the **Select Instances** pane, select the instances, and click **Next**.

5. In the **Specify Variable Values** pane provide values for user name and password, and click **Next**.

6. Under **Job Preview**, check the actual CLI commands that the Citrix ADM will run on the ADC instances. If the preview looks fine, click **Next**.

7. In the **Execute** pane, you have the choice to run the Job immediately or schedule it for later. You can also choose to run the Job in parallel on all the selected instances or do it sequentially. Select Finish after you’ve provided the execution details.

8. Configuration Job shows if the execution succeeded or failed.

9. Select the **Job** and click **Details**. The execution details show the status at individual instance level.

**Modify the admin profile**

After you’ve modified the ADC passwords, you must add and modify the admin profiles of the instances. Follow these steps:
1. Navigate to **Infrastructure > Instances > Citrix ADC**.

2. Click **Profiles** to see all the admin profiles.

3. Select **Add** to create an admin profile and provide new Citrix ADC credentials.

4. The newly created profile appears under **Admin Profiles**.

5. Go to **Network > Instances > Citrix ADC**. Select the Citrix ADC instance for which the password has been modified, and select **Edit**.

6. Select the newly created Profile Name and click **OK**.

7. Select the instance again, right-click, and select **Rediscover**.
You’ve successfully changed the password.

For information about changing the password of an SDX appliance, see How to change a Citrix ADC SDX root password.

**How to change a Citrix ADC SDX nsroot password**

February 15, 2022

Occasionally, you must change the nsroot password of the Citrix ADC appliance for security reasons or compliance of password rotation policy.

This document describes the steps required to change the nsroot password of a Citrix ADC SDX appliance managed through Citrix ADM cloud.

If you change the ADC password, you must modify the Citrix ADM admin profile that is associated with the ADC. An Citrix ADM admin profile maintains the ADC credentials for REST API, SSH, SCP, or SNMP based communication with the ADC appliance. Through admin profiles, Citrix ADM manages Citrix ADC SDX appliances.

**Change password**

Follow these steps to change the password:

- Step 1. Change the SDX password from the SDX Management Service GUI.
- Step 2. Modify the Citrix ADM admin profile associated with the SDX.
Note: If the SDX appliance is managed by other tools as well, you must change the credentials on those tools as well.

**Change the SDX password from the SDX Management Service GUI**

1. From SDX Management Service, navigate to **System > User Administration > Users**.
2. Select the user name for which you want to change the password and click **Edit**.
3. Select **Change Password**.
4. Enter a new password and click **OK**.
5. The SDX password has been changed

Modify the Citrix ADM admin profile

After you’ve modified the SDX passwords, you must modify the admin profiles of the instances. Follow these steps:

1. Navigate to Infrastructure > Instances Dashboard > Citrix ADC > SDX.

2. Select Profiles to see all the admin profiles.

3. Select Add to create an admin profile.

4. Provide new Citrix ADC credentials, and click Create.
5. The newly created profile appears under **Admin Profiles**.

6. Go to **Network > Instances > Citrix ADC > SDX**. Select the instance for which the password has been modified, and select **Edit**.

7. Select the newly created profile name and click **OK**.
8. Select the instance again, right-click, click Rediscover.

You’ve successfully changed the password.

For information about changing the password of an SDX appliance, see How to change a Citrix ADC MPX or VPX root password.
Events

February 15, 2022

When the IP address of a Citrix Application Delivery Controller (Citrix ADC) instance is added to Citrix ADM, Citrix ADM sends a NITRO call and implicitly adds itself as a trap destination for the instance to receive its traps or events.

Events represent occurrences of events or errors on a managed Citrix ADC instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on the Citrix ADM server. Events received in Citrix ADM are displayed on the Events Summary page (Infrastructure > Events), and all active events are displayed in the Event Messages page (Infrastructure > Events > Event Messages).

Citrix ADM 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

February 15, 2022

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 ADM 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**

February 15, 2022

You can set the event age option to specify the time interval (in seconds). Citrix ADM monitors the appliances until the set duration and generates an event only if the event age exceeds the set duration.

**Note:**
- The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event is occurred.

For example, consider that you want to manage various ADC appliances and get notified by email when any of your virtual servers goes down for 60 seconds or longer. You can create an event rule with the necessary filters and set the rule’s event age to 60 seconds. Then, whenever a virtual server remains down for 60 or more seconds, you receive an email notification with details such as entity name, status change, and time.
To set event age in Citrix ADM:

1. In the Citrix ADM, navigate to Infrastructure > Events > Rules, and click Add.
2. On the Create Rule page, set the rule parameters.
3. Specify the event age in seconds.

Schedule an event filter

February 15, 2022

After creating a filter for your rule, if you do not want the Citrix ADM 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 ADM receives these traps. If you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using Citrix ADM:

1. In the Citrix ADM, navigate to Infrastructure > Events > Rules.
2. Select the rule you want to schedule a filter for, and click View Schedule.
3. On the Scheduled Rule page, click Schedule and specify the following parameters:
   - Enable Rule – Select this check box to enable the scheduled event rule.
   - Recurrence - Interval at which to schedule the rule.
• **Scheduled Time Interval (Hours)** – Hours, at which to schedule the rule (use the 24 hour format).

4. Click **Schedule**.

---

**Set repeated email notifications for events**

February 15, 2022

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 ADM:**

1. In Citrix ADM, navigate to **Infrastructure > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters.
3. Under **Event Rule Actions**, click **Add Action**. Then, select **Send e-mail Action** from the **Action Type** drop-down list and select an **Email Distribution List**.
4. You can also add a customized subject line and user message, and upload an attachment to your email when an incoming event matches the configured rule.
5. Select the **Repeat Email Notification until the event is cleared** check box.
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
Choose File ▼

Message
Ensure that disk failure issues are resolved.

OK Close
**Suppress events**

February 15, 2022

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 ADM considers the suppress time as zero and it never expires.

To suppress events by using Citrix ADM:

1. In Citrix ADM, 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**.

---

**Create event rules**

February 15, 2022

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
Citrix Application Delivery Management service

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 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 ADM refreshes an event rule.

Note:
The minimum value for the event age is 60 seconds. If you keep the Event Age field blank, the event rule is applied immediately after the event is occurred.

Based on the example above, you may want to be notified by email every time your 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.

You can also filter event rules by Instance Family to track the Citrix ADC instance from which Citrix ADM receives an event.

If you want to include a regular expression other than asterisk (*) pattern matching, select Enable Advanced Filter with Regex Matching.

Step 2 - Choose the severity of the event

You can create event rules that use the default severity settings. Severity specifies the current severity of the events 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 ADM, navigate to Infrastructure > Events > Event Settings. Choose the Category for which you want to configure event severity and click Configure Severity. Assign a new severity level and click OK.

Step 3 - Specify the event category

You can specify the category or categories of the events generated by your Citrix ADC instances. All categories are created on Citrix ADC instances. These categories are then mapped with the Citrix ADM that can be used to define event rules. Select the category you want to consider and move it from the Available table to the Configured table.

In the example above, you must choose “cpuUsageHigh” as the event category from the table displayed.
Step 4 - Specify 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.

![Select Instances screen](image)

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.

![Failure Objects screen](image)

Step 6 - Specify advanced filters

You can further filter an event rule by:
• **Configuration Commands** - You can specify the complete configuration command, or specify a regular expression to filter events.

You can further filter the event rule by the command’s authentication status and/or its execution status. For example, for a `NetscalerConfigChange` event, type `[*bind system global policy_name[*]`.

- **Messages** - You can specify the complete message description, or specify a regular expression to filter the events.

For example, for a `NetscalerConfigChange` event, type `[*ns_client_ipaddress :10.122.132.142[*]` or `ns_client_ipaddress :^[[]*10.122.132.142[*]`.

**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 ADM, you might receive a high number of emails every day. The emails have a default subject line that provides information about the severity of the event, the category of the event and the failure object. But the subject line does not carry any information about the name of the virtual server where these events originate from. You now have an option to include some additional information like the name of the affected entity, 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.
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 ADM for events matching a particular filter criterion.

You can also set the following parameters for the **Run Command Action** script:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$source</td>
<td>This parameter corresponds to the source IP address of the received event.</td>
</tr>
</tbody>
</table>
$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 ADM, you can:

- Write a script (.sh) file.

  The following is a sample script (.sh) file:

```bash
#!/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":"
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.
PASSIVE”, ”appflowlog”: ”ENABLED”, ”
9     bypassaaa”: ”NO”, ”retainconnectionsoncluster”: ”NO”, ”comment”: ”” } 
10 }
11 
12 url= ”http://$source/nitro/v1/config/lbvserver”
13 curl --insecure --basic -u nsroot:nsroot -H ”Content-type: application/json” -X POST -d $payload $url
14
15 <!--NeedCopy--> 

- Save the .sh file in any persistent location on the Citrix ADM agent. For example, /var.
- Provide the .sh file location in Citrix ADM to run when the rule criteria are met.

To set the Run Command action for creating a new virtual server:

1. Define the rule
2. Select the severity of the event
3. Select the event category entitydown
4. Select the instance that has the virtual server configured
5. Select or create a failure object for the virtual server
6. Under Event Rule Actions, click Add Action and select Run Command Action from the Action Type list.

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 ADM 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 ADM server log files. If you do not enable these options, Citrix ADM discards all outputs and errors generated while running the command script.

   d) Click Create.
7. In the Add Event Action page, click OK.
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 ADM server log files. If you do not enable these options, Citrix ADM discards all outputs and errors generated while running the command script.

**To set the Execute Job Action**

By creating a profile with configuration jobs, a job is run as a built-in job or a custom job for 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.
To set the Suppress Action

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.

To set Slack notifications from Citrix ADM

Configure the required Slack channel by providing the profile name and the webhook URL in the Citrix ADM GUI. The event notifications are then sent to this channel. You can configure multiple Slack channels to receive these notifications.

1. In Citrix ADM, 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 ADM
   b) **Channel Name.** Type the name of the Slack channel to which the event notifications are to be sent.
   c) **Webhook URL.** Type the Webhook URL of the channel that you have entered earlier. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name and all event notifications are sent to this URL to be posted on the designated Slack channel. An example of a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTTS1Fl6oEOVirK

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 ADM**

You can add a PagerDuty profile as an option in Citrix ADM to monitor the incident notifications based on your PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in Citrix ADM, ensure you have completed the required configurations in PagerDuty. For more information, see [PagerDuty documentation](#).

You can select your PagerDuty profile as one of the options to get notifications for the following features:

- **Events** – List of events that are generated for 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 ADM:**

1. Log on to Citrix ADM 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**.

**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](image)

ii. Select your PagerDuty profile and click **OK**.

![Add Event Action](image)

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 ADM**

You can auto-generate ServiceNow incidents for Citrix ADM events by selecting the ServiceNow profile on the Citrix ADM GUI. You must choose the **ServiceNow** profile in Citrix ADM to configure an event rule.
Before you configure an event rule to auto-generate ServiceNow incidents, integrate the Citrix ADM 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 ServiceNow Notifications**.

   b) In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.

   c) Click **OK**.

---

**Modify the reported severity of events that occur on Citrix ADC instances**

**August 13, 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**

View events summary

February 15, 2022

You can now view an Events Summary page to monitor the events and traps received on your Citrix ADM. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by Citrix ADM**. The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a Citrix Application Delivery Controller (Citrix ADC) instance goes down and stops sending information to the Citrix ADM. 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.
**Citrix Application Delivery Management service**

- **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 ADM has an assigned severity, but as the network administrator, you can specify its severity in the Citrix ADM GUI.

  If you click a category type or a trap, you are taken to the **Events** page, on which filters such as the Category and Severity are preselected. This page displays more information about the event, such as the 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.

  You can configure the number of days between 1 and 40, for which you want to view the events in Citrix ADM. For example, if you select 30 days, Citrix ADM 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 Retention 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

February 15, 2022

When you create an event and its settings in Citrix ADM, you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all Citrix Application Delivery Controller (Citrix ADC) instances added to your Citrix ADM server in minute detail on the Infrastructure Dashboard.

On the Infrastructure dashboard, you can now mask irrelevant values so that you can more easily view and monitor information such as event by severities, health, up time, models, and version of 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 ADM:

1. Log on to Citrix ADM, 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 ADM:

You can now view the details of each SNMP trap received from its managed Citrix ADC instances on the Citrix ADM on the **Event Settings** page. Navigate to **Infrastructure > Events > Event Settings**. For a specific trap received from your instance, you can view the following details in tabular format:

- **Category** - Specifies the category of the instance to which the event belongs.
- **Severity** - The severity of the event is indicated by colors and its severity type.
- **Description** - Specifies the messages associated with the event.

For example, an event with the trap category **monRespTimeoutBelowThresh**, the description of the trap is displayed as “This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set.”

View and Export syslog messages

February 15, 2022
You can view syslog messages without logging into Citrix ADM, 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 ADM 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.

**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 ADM software, from the Citrix ADM GUI, navigate to *Infrastructure > Events > Syslog Messages*. The new filter categories are instance, module, event, severity, and message.
To search all Citrix ADM system audit log messages present in the Citrix ADM software, from the Citrix ADM 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 ADM, from the Citrix ADM GUI, navigate to **Infrastructure > Network Functions > Auditing**.

To search the audit log messages for a specific application on the Citrix ADM, from the Citrix ADM 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.
Export syslog messages

To export a syslog messages report by using Citrix ADM:

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.

To schedule the export of syslog messages report by using Citrix ADM:

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.
Suppress syslog messages

February 15, 2022

When configured as a syslog server, Citrix ADM 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 ADM by setting up some filters. Citrix ADM drops all messages that match with the criteria. These dropped messages do not appear on the Citrix ADM GUI and these messages are also not stored in the customer’s Citrix ADM database.

You can suppress some of the logged syslog messages coming into Citrix ADM by setting up some filters. The two filters that can be used for suppressing syslog messages are severity and facility. You can also suppress messages coming from a particular Citrix ADC instance or multiple instances. You can also provide a text pattern for Citrix ADM to search and suppress messages. Citrix ADM drops all messages that match with the criteria. These dropped messages do not appear on the Citrix ADM GUI and these messages are also not stored in the customer database. Therefore, a good amount of space
Citrix Application Delivery Management service 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 ADM, 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.
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.

**Disabling the filter**

To allow the messages to be viewed on Citrix ADM, 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

February 15, 2022

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

Use the SSL dashboard

February 15, 2022
You can use the SSL certificate dashboard in Citrix ADM 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 ADM 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 ADM, navigate to Infrastructure > SSL Dashboard.
Citrix ADM allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to Citrix ADM. 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 ADM 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.

The Citrix ADM SSL Dashboard also shows the distribution of SSL protocols that are running on your virtual servers. As an administrator, you can specify the protocols that you want to monitor through the SSL policy, for more information, see Configuring SSL Policies. The protocols supported are SSLv2, SSLv3, 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.
View audit logs for SSL certificates

You can now view log details of SSL certificates on Citrix ADM. The log details display operations performed using SSL certificates on Citrix ADM 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 ADM using SSL certificates, navigate to **Infrastructure > SSL Dashboard** and select **Audit Logs**.

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.
Exclude default Citrix ADC certificates on the SSL Dashboard

Citrix ADM 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 ADM GUI.
2. On SSL Dashboard page, click Settings.
4. In Certificate Filter section, disable the Show Default Certificates and select Save and Exit.
Download SSL certificates

SSL certificates have to be individually managed per instance. Citrix ADM 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 ADM 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 want 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

February 15, 2022

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 ADM:

1. In Citrix ADM, 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 ADM. For more information, see [Integrate Citrix ADM with ServiceNow instance](#).

6. Click **Save and Exit**.
Update an installed certificate

February 15, 2022

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from Citrix ADM without needing to log on to individual Citrix ADC instances.

To update an SSL certificate, key, or both from Citrix ADM:

1. In Citrix ADM, navigate to Infrastructure > SSL Dashboard.
2. Click any of the graphs to see the list of SSL certificates.
3. On the SSL Certificates page, select a certificate and click Update. Alternatively, click the SSL certificate to view its details, and then click Update in the upper-right corner of the SSL Certificate page.
4. On the Update SSL Certificate page, make the required modifications to the certificate, key, or both and click OK.
Install SSL certificates on a Citrix ADC instance

February 15, 2022

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 ADM 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.
To install an SSL certificate from Citrix ADM:

1. In Citrix ADM, 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 ADM virtual instance).
   - **Key File** - Upload the key file.
   - **Certificate Name** – Specify a name for the certificate key.
   - **Password** - Password to encrypt the private key. You can use this option to upload encrypted private keys.
- **Select Instances** - Select the 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**.

---

**Create a Certificate Signing Request (CSR)**

February 15, 2022

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 ADM:**

1. In Citrix ADM, navigate to **Infrastructure > SSL Dashboard**.

2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select **Create CSR** from the **Select Action** 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 ADM virtual
Create a key - Select the I do not have a Key option, and then specify the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm</td>
<td>Type of key. For example, RSA.</td>
</tr>
<tr>
<td>Key File Name</td>
<td>Name for your file in which the RSA key is stored.</td>
</tr>
<tr>
<td>Key Size</td>
<td>Key size in bits.</td>
</tr>
<tr>
<td>Public Exponent Value</td>
<td>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.</td>
</tr>
<tr>
<td>Key Format</td>
<td>Be default PEM is selected. PEM is the recommended key format for your SSL certificate.</td>
</tr>
<tr>
<td>PEM Encoding Algorithm</td>
<td>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.</td>
</tr>
<tr>
<td>PEM Passphrase</td>
<td>If you've chosen the PEM Encoding Algorithm, enter a passphrase.</td>
</tr>
<tr>
<td>Confirm PEM Passphrase</td>
<td>Confirm your PEM passphrase.</td>
</tr>
</tbody>
</table>

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:

```
1 DNS:<Domain name>, IP:<IP address>
```
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

February 15, 2022

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 ADM:

1. In Citrix ADM, navigate to Infrastructure > SSL Dashboard.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select Link from the 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 ADM:

1. In Citrix ADM, navigate to Infrastructure > SSL Dashboard.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select Unlink from the 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

March 31, 2022

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 ADM. 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 ADM:

1. In Citrix ADM, 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.
Note

The SSL dashboard displays only the **Signature Algorithms** that are selected through the **Settings** option and others are displayed as **Not Recommended**.

**Poll SSL certificates from Citrix ADC instances**

February 15, 2022

Citrix ADM automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix 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 ADM, navigate to **Infrastructure > SSL Dashboard**.
2. On SSL Dashboard page, in the top right-hand corner, click Poll Now.

3. The Poll Now page pops up, giving you the option to poll all 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.

   ![Poll Now page](image)

   Start Polling all Citrix ADC instances. This may take some minutes

   ![Start Polling button](image)

   - To poll specific instances, select the Select Instances tab, select the instances from the list, and click Poll Now.

   ![Select Instances tab](image)

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

February 15, 2022

Citrix ADM 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 ADM allows you to create configuration jobs that help you to perform all these activities with ease on several devices as a single task. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on Citrix ADM. A configuration job contains a set of configuration commands that you can run on one or multiple managed devices.

Configuration Jobs can either use SSH commands to do configuration commands or use SCP to do file copy from either locally or to another appliance, for example, we can schedule a HA-failover or HA-upgrade.

You can create a configuration job by using one of the following four options in Citrix ADM. Use one of these to create a reusable source of commands and instructions to the system to run a configuration job.

1. Configuration Template
2. Instance
3. File
4. Record and Play

## Configuration Template

You can create configuration templates while creating a job and saving a set of configuration commands as a template. When you save these templates on the Create Jobs page, they are automatically
displayed on the Create Template page. For more information, see How to Use the Master Configuration Template on Citrix ADM.

**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.

For more information, see How to Use Configuration Templates to Create Audit Templates

**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 ADM. 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 ADM. See, How to Use Record-and-Play to Create Configuration Jobs.

**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.

**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

**Create a configuration job**

February 15, 2022

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 ADM GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of Citrix ADM to create a configuration job, send email notifications, and check execution logs of the jobs created.

**To create a configuration job on Citrix ADM:**

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, Inbuilt 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 ADM 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 ADM must perform if the command fails:

   • **Ignore error and continue**: Citrix ADM 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 ADM stops the remaining commands if any command fails during execution.

   • **Rollback successful commands**: Citrix ADM restores the successfully run commands if any command fails during execution.

   If the custom rollback is enabled, the Citrix ADM 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.

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
Configuration audit

February 15, 2022

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 ADM instances
- Generate configuration audit diff for ConfigChange SNMP traps

Maintenance jobs

June 7, 2022

You can create the following maintenance tasks using Citrix ADM. 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 BLX 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 ADM, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.

2. In **Create Maintenance Jobs**, select **Upgrade Citrix ADC (Standalone/High-Availability/Cluster)** and click **Proceed**.

3. In **Select Instance**, type a name of your choice for **Job Name**.

4. Click **Add Instances** to add ADC instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
5. Click Next to select the image. Select one of the following options from the Software Image list:

- **Local** - Select the instance upgrade file from your local machine.

- **Appliance** - Select the instance upgrade file from an Citrix ADM file browser. The Citrix ADM GUI displays the instance files that are present at /var/mps/mps_images.
  
  - **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the Citrix ADC instance.
  
  - **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.

6. Click Next to start the pre-upgrade validation on the selected instances.

The Pre-upgrade validation tab displays the failed instances. Remove the failed instances and click Next.

**Important**

If you specify cluster IP address, the Citrix ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in Custom scripts, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

- **Import commands from file** - Select the command input file from your local computer.

- **Type commands** - Enter commands directly on the GUI.
You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. **Click Next.** In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an ADC HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. **Click Next.** In **Create Job**, specify the following details:

   a) Specify when you want to upload the image to an instance:
• **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.

• **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.

• **Backup the ADC instances before starting the upgrade.** - Creates a backup of the selected ADC instances.

• **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.

• **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

• **Citrix ADM Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, Citrix ADM Service Connect is enabled automatically. For more information, see [Low-touch onboarding of Citrix ADC instances using Citrix ADM service connect](#).

• **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see [Create an email distribution list](#).

• **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see [Create a Slack profile](#).

10. Click **Create Job**.
Schedule upgrading of Citrix ADC SDX instances

1. In Citrix ADM, navigate to Infrastructure > Upgrade Jobs. Click Create Job.

2. Select Upgrade Citrix ADC SDX and click Proceed.

3. On the Upgrade Citrix ADC SDX page, in the Instance Selection tab:
   a) Add a Task Name.
   b) From the Software Image list, select either Local (your local machine) or Appliance (the build file must be present on the Citrix ADM virtual appliance).

   The upload process begins.

   c) Add the Citrix ADC SDX instances on which you want to run the upgrade process.
   d) Click Next.
4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a 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**.
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 of Citrix ADC BLX instances**

1. In Citrix ADM, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. In **Create Maintenance Jobs**, select **Upgrade Citrix ADC BLX** and click **Proceed**.

3. In **Select Instance**, type a name of your choice for **Job Name**.

4. Click **Add Instances** to add the BLX instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.

5. Click **Next** to select the image. 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 ADM file browser. The Citrix ADM GUI displays the instance files that are present at `/var/mps/mps_images`.

  – **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the Citrix ADC instance.

  – **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.

6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   **Important**

   If you specify cluster IP address, the Citrix ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

   • **Import commands from file** - Select the command input file from your local computer.

   • **Type commands** - Enter commands directly on the GUI.
You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. Click **Next**. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

   If you want to upgrade an HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

   Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. Click **Next**. In **Create Job**, specify the following details:

   a) Specify when you want to upload the image to an instance:
- **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.

- **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.

- **Backup the ADC instances before starting the upgrade** - Creates a backup of the selected ADC instances.

- **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.

- **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

- **Citrix ADM Service Connect** - If you are upgrading to build 13.0-64 or later and 12.1-58 or later, Citrix ADM Service Connect is enabled automatically. For more information, see Low-touch onboarding of Citrix ADC instances using Citrix ADM service connect.

- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.

- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

10. Click **Create Job**.
Schedule upgrading Autoscale group

Perform the following steps to upgrade all the instances in the cloud services that are part of the Autoscale group:

1. In Citrix ADM, navigate to Infrastructure > Upgrade Jobs. Click Create Job.
2. Select Upgrade Autoscale Group and click Proceed.
3. In the Upgrade Settings tab:
   a) Select the Autoscale Group that you want to upgrade.
   b) In Image, select the 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 ADM, navigate to Infrastructure > Upgrade Jobs. Click Create Job.
2. Select Configure HA Pair of Citrix ADC Instances and click Proceed.
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.
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**.
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 ADM, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.
3. On the **Migrate NetScaler HA to Cluster** page, in the **Instance Selection** tab, add a **Task Name**. Specify the Primary IP address, Secondary IP address, Primary Node ID, Secondary Node ID, Cluster IP Address, Cluster ID, and Backplane, and then click **Next**.
4. On the Schedule Task tab, select Now from the Execution Mode list to upgrade a 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

July 26, 2022

In Citrix ADM, 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

ADM will perform the following pre-validation checks 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.

Upgrade considerations for customized ADC configurations

It is important that both the upgrade changes and your customizations are applied to an upgraded Citrix ADC appliance. So, if you have customized configuration files in the /etc directory, see Upgrade considerations for customized configuration files before you proceed with the Citrix ADC appliance upgrade. Following are broad steps that you must perform:

1. Pre upgrade steps in ADC
   - Backup customized file before the upgrade
   - Delete the symlink of the customized file before the upgrade
2. Upgrade ADC using ADM. To upgrade, follow the instructions available at the beginning of the page.
3. Post upgrade steps in ADC
Citrix Application Delivery Management service

- **Restore customizations after the upgrade**

Both the pre upgrade and post upgrade steps are to be performed on each ADC. However, in step 2, to upgrade ADC using ADM, all the vulnerable ADC instances can be selected and upgraded together.

**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 ADM 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**.
2. In Create Maintenance Jobs, select Upgrade Citrix ADC (Standalone/High-Availability/Cluster) and click Proceed.

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.
   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.
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 ADM GUI displays the instance files that are present in `/var/mps/ns_images`. Select the image from the Citrix ADM 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**.
Citrix Application Delivery Management service

- **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 ADM finds unsupported classic policies, you can remove such policies to create an upgrade job.

**Important**

If you specify cluster IP address, the Citrix ADM 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.

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 ADM 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**.
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.
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 ADM 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.

**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](#).

**Download a consolidated diff report of an ADC upgrade job**

In Citrix ADM, 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.
Citrix Application Delivery Management service

**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

**Network functions**

February 15, 2022

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)
Citrix Application Delivery Management service

- 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

February 15, 2022

Citrix ADM 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 ADM > Network Functions - consolidated reports and individual reports.

Consolidated reports: You can download and view a consolidated or a summarized report for all entities that are managed on 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.

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**: \(<\text{name_of_the_virtual_server}>\#\text{virtual_IP_address}:\text{port_number}\)
- **Services**: \(<\text{name_of_the_service}>\#\text{service-IP_address}:\text{port_number}\)
- **Service Groups**: \(<\text{name_of_service_group}>\#\text{server_member1_IP_address}:\text{port},\text{server_member2_IP_address}:\text{port},\ldots,\text{server_membern_IP_address}:\text{port}\)
Note

- If there is no host name available, the corresponding IP address is displayed.
- Blank columns indicate that the respective entities are not configured for that 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 ADM allows you to download the report instantly. You can also schedule the report to be generated at a fixed time once a day, once a week, or once a month.

Generate a combined load balancing report

1. In Citrix ADM, navigate to Infrastructure > Network Functions.
2. Click Generate Report.

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.

<table>
<thead>
<tr>
<th>Recurrence*</th>
<th>Weekly</th>
</tr>
</thead>
</table>

**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 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 ADM, 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 ADM GUI.

Export or schedule export of network functions reports

February 15, 2022

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 ADM. 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
Citrix Application Delivery Management service

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 ADM.
• 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**

The following image shows an example of a network functions report.

- **Recurrence** - Select Daily, Weekly, or Monthly from the drop-down list box.
- **Recurrence time** - Enter the time in the Hour: Minute in 24-hour format.
- **Email** - Select the check box and then select the profile from the drop-down list box, or click Add to create an email profile.
- **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.
Network reporting

February 15, 2022

You can optimize resource usage by monitoring your network reporting on Citrix ADM. You may have a distributed deployment with many applications deployed at multiple locations. To ensure optimal performance of your applications, you have also deployed multiple Citrix Application Delivery Controller (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 ADM 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)
The network reporting dashboard in Citrix ADM 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:

- The left side panel lists all the custom dashboards that are created in Citrix ADM. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each dashboard with multiple widgets to display various reports. A widget represents a report on the dashboard, that is a collection of more related reports. For example, a compression TCP Bytes Usage report contains reports for compressed TCP bytes transferred and received per second.
- You can display reports for one hour, one day, one week, or for one month. In addition, you can now use the timeline slider option to customize the duration of reports being generated on the Citrix ADM.
- You can remove a report by clicking “X”. You can also export the report as a .pdf, .jpeg, .png, or .csv format to your system. You can also schedule a time and recurrence of when 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 ADM allows you to view reports for 10 instances.

You can also export the entire dashboard as a .pdf, .jpeg, .png, or .csv format to your system. Any changes made to the dashboard must be saved. Click Save to save the changes.

The following section explains in detail the tasks to create a dashboard, generate reports, and to export reports.

To view or to create a dashboard:

1. In Citrix ADM, navigate to **Infrastructure > Network Reporting**.

2. To view the existing dashboards, click **View Dashboard**. The Network Reporting **Dashboard** page opens where you can view all your dashboards and report widgets.

3. To create a dashboard, click **Create Dashboard**.

   The **Create Dashboard** page opens.
4. In the **Basic Settings** tab, enter the following details:
   a) **Name**. Type the name of the dashboard.
   b) **Instance Family**. Select the type of instance - 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**.
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.

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.

In the existing average data, you can apply aggregations by selecting the option from the **View By** list. When you apply aggregation, the data is updated for each metric in the dashboard. Click **Settings** and select **Aggregation Filters**.

The following are the aggregations that you can add:

- Count
- Max
- Min
- Sum
Citrix Application Delivery Management service

- 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 ADM 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 ADM if you have read-only permissions. You need an edit permission to be able to create a file in Citrix ADM and to be able to export the file.

To export dashboard reports:

1. Navigate to **Infrastructure > Network Reporting**
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example, click **Dashboard 1**.
4. Click the export button at the top right corner of the page.
5. Under the **Export Now** tab, select the required format, and then click **Export**.
On the Export page, you can do one of the following:

6. Select Export Now tab. To view and save the report in PDF, JPEG, PNG, or CSV format.

7. Select Schedule Export tab. To schedule the report daily, weekly, or monthly and send the report over an email or slack message.

You can schedule an export of the Network Reporting Dashboard page on a recurrent basis. For example, you can set an option to generate a dashboard report every week for the previous one hour at a particular time. The report is generated every week then and shows the status of the dashboard. The report overrides the time and date stamp, if set by the user.

**Note**

- if you select Weekly recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select Monthly recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

While scheduling network reports, you can customize the heading of the report by entering a text string in the Subject field. The report created at the scheduled time has this string as its name.

For example, for network reports originating from a particular virtual server, you can type in the subject as “authentication-reports-10.106.118.120,” where 10.106.118.120 is the IP address of the monitored virtual server.

**Note**

Currently, this option is available only when you schedule the export of reports. You cannot add a heading to the report when you export them instantly.

To export widget reports:
1. Navigate to **Infrastructure > Network Reporting**.

2. Click **View Dashboards** to view all the dashboards that you have created.

3. In the left pane, click a dashboard. In this example also click **Skype for Business**.

4. Select a widget. For example, select **Load Balancing Virtual Server Transactions**.

5. Click the export button at the top right corner of the page

6. Under the **Export Now** tab, select the required format, and then click **Export**.

---

**How to manage Thresholds for Network Reports on Citrix ADM**

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 ADM, you can configure thresholds and view, edit, and delete them.

For example, you can receive an email notification when the Connections counter for a content switching virtual server reaches a specified value. You can define a threshold for a specific instance type. You can also choose the reports you want to generate for specific counter metrics from your chosen instance.

When the value of a counter exceeds or falls below (as specified by the rule) the threshold value, an event of the specified severity is generated to signify a performance related issue. When the counter value returns to a value that you consider normal, the event is cleared. These events can be viewed by navigating to **Infrastructure > Events > Reports**. On the **Reports** page, you can click the **Events by Severity** donut to view events by their severity.
You can also associate an action with a threshold such as sending an email or SMS message when the threshold is breached.

**To create a threshold:**

1. In Citrix ADM, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.

2. On the **Create Threshold** page, specify the following details:
   - **Name**: Name of the threshold.
   - **Instance Type**: Choose 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 ADM appends the monitored value and the threshold value to this message.

6. Select **Enable** to enable the threshold to generate alarms.

7. Optionally, you can configure **Actions** such as email or Slack notifications.

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 ADM retrieves instance statistics such as counter information and aggregates them based on per minute, per hour, per day, or per week. You can view this aggregated data in predefined reports.

To set the performance polling interval, navigate to Infrastructure > Network Reporting and click Configure Polling Interval. Your polling interval cannot be less than 5 minutes or more than 60 minutes.

Configuring Network Reporting Prune Settings

You can configure the purge interval of network reporting data in Citrix ADM. This interval limits the amount of network reporting data being stored in the Citrix ADM server’s database. By default, prun-
Provisioning Citrix ADC VPX Instances on AWS

February 15, 2022

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 ADM 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:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Machine Image (AMI)</td>
<td>A machine image, which provides the information required to launch an instance, which is a virtual server in the cloud.</td>
</tr>
<tr>
<td>Elastic Compute Cloud (EC2)</td>
<td>A web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.</td>
</tr>
<tr>
<td>Elastic network interface (ENI)</td>
<td>A virtual network interface that you can attach to an instance in a VPC.</td>
</tr>
</tbody>
</table>
Term | Definition
--- | ---
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 ADM agent in AWS.

For more information on how to create an account and other tasks, see [AWS Documentation](https://aws.amazon.com/documentation). For more information on how to install Citrix ADM agent on AWS, see [Installing Citrix ADM agent on AWS](https://docs.citrix.com/en-us/app-delivery-management/uninstall.html).
**Architecture Diagram**

The following image provides an overview of how Citrix ADM 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 ADM:

- Create subnets
- Create security groups
- Create an IAM role and define a policy

Perform the following tasks on Citrix ADM 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.
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 ADM. So, select **Another AWS account** to allow Citrix ADM to perform actions in your AWS account. Type in the 12-digit Citrix ADM AWS account ID. The Citrix ID is 835822366011. You can also find the Citrix ID in Citrix ADM when you create the cloud access profile.

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:

```json
{
  "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": "*
}
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 ADM**

Create a site in Citrix ADM and add the details of the VPC associated with your AWS role.

1. In Citrix ADM, 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.
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 ADM.

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 ADM agent details to provision those instances that are bound to that agent.

1. In Citrix ADM, 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 and Zone type options]

   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 ADM 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 ADM**: The instance that you want to provision checks out the licenses from the Citrix ADM.

   - **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](image)

6. In the **License** tab if you select the **Allocate from Citrix ADM**, 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 ADM.
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 ADM license pool. These licenses can be reused to provision new 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.
The Citrix ADC VPX instance is now provisioned on AWS.

**Note**

Currently, Citrix ADM 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 ADM.
To view the Citrix ADC VPX provisioned in Citrix ADM

1. In Citrix ADM, 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

February 15, 2022

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 ADM. 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 ADM, 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 cluster for Service Graph

March 30, 2022

Kubernetes (K8s) is an open source container orchestration platform that automates the deployment, scaling, and management of cloud-native applications.

Note
- Citrix ADM supports the visibility of clusters for Service graph with Kubernetes version 1.14–1.23.

You can specify the following aspects of Kubernetes integration in Citrix ADM:
• **Cluster** – You can register or unregister Kubernetes clusters for which Citrix ADM monitors all microservices and populates the Service graph. When you register a cluster in Citrix ADM, specify the Kubernetes API server information. Then, select an Citrix ADM agent that can reach the Kubernetes cluster.

**Before you begin**

To monitor and visualize your microservices on Kubernetes clusters and get started on Service Graph, ensure you have:

- Kubernetes cluster in place.
- Citrix ADM agent installed and configured to enable communication between Citrix ADM 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 ADM.

**Configure Citrix ADM agent to register with Kubernetes cluster**

To enable communication between Kubernetes cluster and Citrix ADM, you must install and configure a Citrix ADM 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 ADM agent if one is already deployed.

**Configure the Citrix ADM with a secret token to manage a Kubernetes cluster**

For Citrix ADM to be able to receive events from Kubernetes, you need to create a service account in Kubernetes for Citrix ADM. And, configure the service account with the necessary RBAC permissions in the Cluster.

1. Create a service account for Citrix ADM. For example, the service account name can be `citrixadm-sa`. To create a service account, see Use Multiple Service Accounts.

2. Use the `cluster-admin` role to bind the Citrix ADM 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.
After binding the Citrix ADM 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
   ```

4. Run the following command to obtain the secret string of the token:

   ```
   kubectl describe secret <token-name>
   ```

**Add the Kubernetes cluster in Citrix ADM**

After you configure a Citrix ADM agent and configure static routes, you must register the Kubernetes cluster in Citrix ADM.

To register the Kubernetes cluster:

1. Log on to Citrix ADM with administrator credentials.

2. Navigate to Orchestration > Kubernetes > Cluster.
   The Clusters page is displayed.

3. Click Add.

4. In the Add Cluster page, specify the following parameters:
   a) **Name** - Specify a name of your choice.
   b) **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.
      i. On the Kubernetes master node, run the command `kubectl cluster-info`.

   ![Kubernetes Cluster Info](https://example.com/kubectl_cluster-info.png)

© 1999–2022 Citrix Systems, Inc. All rights reserved.
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 ADM to manage a Kubernetes cluster. The authentication token is required to validate access for communication between Kubernetes cluster and Citrix ADM. To generate an authentication token:

i. On the Kubernetes master node, run the following commands:

```
1 kubectl describe secret <token-name>
2 <!--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**.
TCP Insight

February 15, 2022

The TCP Insight feature of Citrix ADM 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
Citrix Application Delivery Management service

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 ADM 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 ADM. For information about Citrix ADM licensing, see Licensing.

Hardware requirements for Citrix ADM:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>4</td>
</tr>
<tr>
<td>Storage Space</td>
<td>120 GB</td>
</tr>
</tbody>
</table>

*Note* Citrix recommends that you use 8 CPUs for better performance.

Enabling TCP Insight

Before you can view the TCP Insight metrics, you must enable the feature on Citrix ADM.

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 ADM

After enabling TCP Insight in Citrix ADM, 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 ADM:

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 ADM and click the TCP Insight tab. Then, click Sides and select Internet or Radio from the bar graph or the table below the graph.
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 ADM. 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 ADM, 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

February 15, 2022

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 ADM, 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 ADM 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 ADM provides metrics for the following types of video traffic:

- Progressive Download (PD) videos over HTTP
- ABR videos over HTTP
- ABR videos over HTTPS
- YouTube ABR videos over QUIC

**Configuring Video Insight**

**Note**

Video Insight is supported on 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 ADM 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**

```
1 add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -Transport logstream
2 set appflow param -videoInsight ENABLED
3 add appflow action act1 -collectors col1 -videoAnalytics ENABLED
4 add appflow policy appol true act1
5 bind appflow global appol 1
6 enable ns mode ulfd
7 enable feature appflow
8 <!--NeedCopy-->`

**Viewing the Video Insight metrics in Citrix ADM**

After enabling Video Insight in Citrix ADM, you can view video optimization metrics such as, video classification, data volume, peak data rate, and ABR video plays. These metrics help you analyze your network and optimize the videos for improved subscriber experience, operational efficiency, and other performance criteria.

To view the Video Insight metrics in Citrix ADM, navigate to **Infrastructure > Video Insight**.
Note

The values provided by the legend OTHER in the charts represent the non-ABR and non-PD data in the video traffic depending on the filter you have selected:

- **All** – Sum of non-ABR (HTTP, HTTPS, and QUIC) and non-PD (HTTP) data in the video traffic.
- **HTTP** – Sum of non-ABR and non-PD data in the video traffic.
- **HTTPS** – Sum of non-ABR video data in the video traffic.
- **QUIC** – Sum of non-ABR video data in the video traffic.

**View network efficiency**

February 15, 2022

For a given time frame, Citrix ADM provides a graph that shows the ratio of optimized to unoptimized video sessions in the time frame. It also displays the percentage of bandwidth saved by optimization. The percentage of bandwidth saved is calculated with the following formula:

\[
\text{Percentage of bandwidth saved} = \frac{\text{Average optimized ABR video Data Volume}}{\text{Average of unoptimized ABR Video Data Volume}}.
\]

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.

![ABR Video Analytics](image)

**Compare the data volume used by optimized and unoptimized ABR videos**

February 15, 2022

For a given time frame, Citrix ADM shows the data volume used by optimized and unoptimized ABR videos, so that you can compare the two volumes.

To see the data volume used by ABR videos:

1. Navigate to **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.
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

February 15, 2022

The Citrix ADC appliance detects the encrypted or unencrypted video traffic in your network and the type of video streaming (PD or ABR). Citrix ADM displays these metrics and the data volume consumed by the video traffic for a defined time frame.

To see the types of videos and the consumed data volume:

1. Navigate to 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:

![Data Volume Graph]

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

February 15, 2022

For a given time frame, Citrix ADM provides the play time of ABR videos and also enables you to compare the play time of optimized and unoptimized ABR videos in your network.

To view the play time:

1. Navigate to **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
Citrix Application Delivery Management service

**Compare bandwidth consumption of optimized and unoptimized ABR videos**

February 15, 2022

For a given time frame, Citrix ADM provides the bandwidth consumed by optimized and unoptimized 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.

For the selected time frame, the **Bandwidth** tab provides a line graph and pie chart describing the:

- Average bandwidth consumed by optimized and unoptimized ABR videos.
• Bandwidth consumed based on the play time distribution between optimized and unoptimized ABR videos.

• Bandwidth consumed based on the data volume distributed between optimized and unoptimized ABR videos.

Compare optimized and unoptimized number of plays of ABR videos

February 15, 2022

For a given time frame, Citrix ADM shows the number of plays of ABR videos and enables you to compare the number of optimized and unoptimized plays in your network.

To see the number of plays:

1. Navigate to 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 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

February 15, 2022

Citrix ADM shows you the peak throughput or data rate of the video traffic in your network.

To see the peak data rate of the video traffic:

1. Navigate to **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 show the percentage of the peak data rate consumed by the type of video traffic streamed during the selected time frame.
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 ADM to collect data and provide reports and statistics for the data center and the branch WAN optimization appli-
To enable analytics on the WAN optimization appliance:

1. Navigate to **Infrastructure > Instances > Citrix SD-WAN**, and select the SD-WAN WO instance.

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.

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 ADM.

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.

The following metrics are displayed:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Accelerated Connections</td>
<td>Number of active WAN connections that are accelerated.</td>
</tr>
<tr>
<td>Active Unaccelerated Connections</td>
<td>Number of active WAN connections that are not accelerated.</td>
</tr>
<tr>
<td>WAN Latency</td>
<td>Delay, in milliseconds, that the user experiences while interacting with an application.</td>
</tr>
<tr>
<td>Compression Ratio</td>
<td>Ratio of data compression between the branch office and data center appliances for the selected duration.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of packets that the WAN optimization appliance has sent over the network for the selected duration.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Number of packets that the WAN optimization appliance has received from the network for the selected duration.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bytes Sent over WAN</td>
<td>Number of bytes that the Citrix WAN optimization appliance has sent over the WAN for the selected duration.</td>
</tr>
<tr>
<td>Bytes Received over WAN</td>
<td>Number of bytes that the WAN optimization appliance received from the WAN for the selected duration.</td>
</tr>
<tr>
<td>LAN RTO</td>
<td>Number of times the WAN optimization appliance has timed out retransmission to the LAN for the selected duration.</td>
</tr>
<tr>
<td>WAN RTO</td>
<td>Number of times the WAN optimization appliance has timed out retransmission to the WAN for the selected duration.</td>
</tr>
<tr>
<td>Retransmit Packets (LAN)</td>
<td>Number of packets the WAN optimization appliance has retransmitted to the LAN network for the selected duration.</td>
</tr>
<tr>
<td>Retransmit Packets (WAN)</td>
<td>Number of packets the WAN optimization appliance has retransmitted to the WAN network for the selected duration.</td>
</tr>
</tbody>
</table>

**Manage licensing and enable analytics on virtual servers**

February 15, 2022

**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**

When you click **Configure License** or **Configure Analytics**, the **All Virtual Servers** page is displayed.

On the **All Virtual Servers** page, you can:

- Apply license for unlicensed virtual servers
- Remove license for licensed virtual servers
- Enable analytics on licensed virtual servers
- Edit analytics
- Disable analytics

**Note**

The supported virtual servers to enable analytics are Load Balancing, Content Switching, and 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.

   ![All Virtual Servers page with licensed status filter applied]

   The filter is now applied and only the unlicensed virtual servers are displayed.

2. Select the virtual servers and then click License.

   ![All Virtual Servers page with licensed virtual servers]

To unlicense the virtual servers, from the All Virtual Servers page:

1. Click the search bar, select Licensed, and select Yes.
2. Select the virtual servers and click Unlicense.

Enable analytics

The following are the prerequisites to enable analytics for virtual servers:

- Ensure that virtual servers are licensed
- Ensure that analytics status is Disabled
- Ensure that virtual servers are in UP status

You can filter the results to identify the virtual servers that are mentioned in the prerequisites.

1. Click the search bar and select State and then select UP.
2. Click the search bar and select **Licensed**, and then select **Yes**.
3. Click the search bar and select **Analytics Status**, and then select **Disabled**.

4. After applying the filters, select the virtual servers, and then click **Enable Analytics**.

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 dialog box]

**Selected Virtual Server: Load Balancing**
- Web Insight
- Client Side Measurement
- WAF Security Violations
- Bot Security Violations
- Advanced Security Analytics

- **Advanced Options**
- **Expression Configuration**

**Note**
- If you select virtual servers that are not licensed, then Citrix ADM first licenses those virtual servers and then enables analytics.
- For admin partitions, only **Web Insight** is supported.
- For virtual servers such as **Cache Redirection**, **Authentication**, and **GSLB**, you cannot enable analytics. An error message is displayed.

After you click **OK**, Citrix ADM processes to enable analytics on the selected virtual servers.
Citrix ADP uses Citrix ADC SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between Citrix ADP agent and Citrix ADC instance, ensure you open the following port to enable Citrix ADP agent to collect AppFlow traffic:

<table>
<thead>
<tr>
<th>Transport Mode</th>
<th>Source IP</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPFIX</td>
<td>NSIP</td>
<td>UDP</td>
<td>4739</td>
</tr>
<tr>
<td>Logstream</td>
<td>SNIP</td>
<td>TCP</td>
<td>5557</td>
</tr>
</tbody>
</table>

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.
3. On the **Configure Analytics on Virtual Server(s)** page, select the virtual server and click **Enable Analytics**.

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**
3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window.

4. Click **OK**.

---

**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**

Citrix ADM disables the analytics on the selected virtual servers

- 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**

February 15, 2022

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 ADM:

- When you configure this feature for the first time, you must ensure that the prerequisites mentioned in this document are met.
- Modify the analytics settings later.

Consider that you have configured the analytics settings for the first time by selecting Web Insight, HDX Insight, and Gateway Insight. If you want to modify the analytics settings later and deselect Gateway Insight, the changes do not impact the virtual servers that are already enabled with analytics.

- The virtual servers that are already enabled with analytics.

Consider that you have 10 licensed virtual servers and two of them are already enabled with analytics. In this scenario, this feature enables analytics only for the remaining eight virtual servers.

- The virtual servers that are manually disabled with analytics.

Consider that you have 10 licensed virtual servers and you have manually disabled analytics for two virtual servers. In this scenario, this feature enables analytics only for the remaining eight virtual servers and skips the virtual servers that are manually disabled with analytics.

- Bot Security Violations and WAF Security Violations options are supported only in premium licensed virtual servers. If the virtual servers are not premium licensed, then Bot Security Violations and WAF Security Violations are not enabled.

Prerequisites

Ensure that:

- All existing virtual servers are licensed.

- Auto-licensed option is enabled to license all the subsequent virtual servers. Navigate to Settings > Licensing & Analytics Config and under Virtual Server License Allocation, turn on the Auto Licensed Virtual Servers option.

Enable analytics

1. Navigate to Settings > Licensing & Analytics Config.
2. Under Analytics Summary, click Global Analytics Configuration.
3. Select the analytics features that you want to enable analytics on the virtual servers.

4. To enable analytics on the subsequent virtual servers, select the **Apply this analytics settings on the subsequent licensed virtual servers** check box.

5. Click **Submit**.
Configure role-based access control

July 12, 2022

Citrix ADM provides fine-grained, role based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise.

In Citrix ADM, 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 ADM GUI with the Citrix Cloud credentials. You are granted the super admin role, and by default, you have all access permissions in Citrix ADM. Later you can create other users in your organization in Citrix Cloud.

Users who are created later and who log on to Citrix ADM 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 > Users & Roles. 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 ADM.

Chris, the ADC group head, is the super administrator of Citrix ADM 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 ADM. 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 ADM, 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 admin-
Citrix Application Delivery Management service

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 ADM to configure access policies, roles, and user groups for David who is the security admin in your organization.

**Configure Users on Citrix ADM**

As a super admin, you can create more users by configuring accounts for them in Citrix Cloud and not in Citrix ADM. When the new users are added to Citrix ADM, 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 ADM GUI, click the Hamburger icon at the top left, and select **Identity and Access Management**.

This tab lists the users that are created in Citrix Cloud.

3. Select the identity provider from the list.

- **Citrix Identity**: Type the email address of the user that you want to add in Citrix ADM and click **Invite**.

![Identity and Access Management](image)

**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 ADM using their credentials.

- **Azure Active Directory (AD)**: This option appears only if your Azure AD is connected to Citrix Cloud, see [Connect Azure Active Directory to Citrix Cloud](#). When you select this option to invite users or groups, you can specify only **Custom Access** for the selected user or group. The users can log in to Citrix ADM using their Azure AD credentials. And, you don’t require to create a Citrix Identity for the users who are part of the selected Azure AD. If a user is added to the invited group, you don’t require to send an invite for the newly added user. This user can access Citrix ADM using the Azure AD credentials.

![Identity and Access Management](image)

4. Select **Custom access** for the specified user or group.

5. Select **Application Delivery Management**.

This option lists the user groups created in Citrix ADM. Select the group to which you want to add the user.
As an admin, you see the new user in the Citrix ADM Users list only after the user logs on to Citrix ADM.

**To Configure Users in Citrix ADM:**

1. In the Citrix ADM GUI, navigate to **Settings > Users & Roles > Users**.
2. The user is displayed on the **Users page**.

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 ADM from the Citrix Cloud only. Therefore, even though you have admin permissions, you cannot add or delete users in the Citrix ADM 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 ADM at least once.

**Configure Access Policies on Citrix ADM**

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 ADM provides five predefined access policies:

- **admin_policy.** Grants access to all Citrix ADM nodes. The user has both view and edit permissions, can view all Citrix ADM 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 ADM GUI, except access to the Settings node.
- **readonly_policy.** Grants read-only permissions. The user can view all content on Citrix ADM but is not authorized to perform any operations.
- **appadmin_policy.** Grants administrative permissions for accessing the application features in Citrix ADM. A user bound to this policy can add, modify, and delete custom applications, and can enable or disable the services, service groups, and the various virtual servers, such as content switching, 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 ADM 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 ADM 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 ADM GUI, navigate to Settings > Users & Roles > 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 all Citrix ADM 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 ADM.

- **Enable-Disable**: This option is available only for the Network Functions features that allow enable or disable action on Citrix ADM. 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:
The **View** permission is granted to a user for the **Virtual Servers** feature. User can view the load balancing virtual servers in Citrix ADM. To view virtual servers, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Virtual Servers** tab.

The **Enable-Disable** permission is granted to a user for the **Services** feature. This permission also grants the **View** permission. User can enable or disable the services bound to a load balancing virtual server. Also, 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 ADM 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.
Configure Roles on Citrix ADM

In Citrix ADM, each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add Citrix ADC instances in Citrix ADM, 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 ADM provides five predefined roles:

- **admin_role.** Has access to all Citrix ADM features. (This role is bound to adminpolicy.)
- **adminExceptSystem_role.** Has access to the Citrix ADM 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 ADM. (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 ADM GUI, navigate to Settings > Users & Roles > 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.

© 1999-2022 Citrix Systems, Inc. All rights reserved.
Note
The policies are pre-fixed with a tenant ID (for example, maasdocfour) that is unique to all tenants.

Create Roles

You can create an access policy by clicking New, or you can navigate to Settings > Users & Roles > Access Policies, and create policies.

5. Click Create.

Configure Groups on Citrix ADM

In Citrix ADM, 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 ADM.

You can manage a user access in Citrix ADM at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.
Citrix ADM treats virtual server, services, service groups, and servers as network function entities.

- **Virtual server (Applications)** - Load Balancing (lb), GSLB, Context Switching (CS), Cache Redirection (CR), Authentication (Auth), and 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 ADM, navigate to **Settings > Users & Roles > Groups**.
2. Click **Add**.
   
   The **Create System Group** page is displayed.
3. In the **GroupName** 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 > Users & Roles > Users**, and create or modify users.
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
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.

**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 ADM.

- **All Applications of selected instances:** This option appears only if you select instances from the All Instances category. It adds all the applications present on the selected instance.

- **Specific Applications:** This option allows you to add the required applications that you want users to access. Click Add Applications and select the required applications from the list.

- **Select Individual Entity Type:** This option allows you to select 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 ADM authorizes all the entities that are bound to the selected application.
Note

Ensure you have selected only one entity type if you want to authorize bound entities.

You can use regular expressions to search and add the network function entities that meet the regex criteria for the groups. The specified regex expression is persisted in Citrix ADM. To add regular expression, perform the following steps:

a) Click **Add Regular Expression**.

b) Specify the regular expression in the text box.

The following image explains how to use regular expression to add an application when you select the **Specific Applications** option:

If you want to add more regular expressions, click the + icon.
Citrix Application Delivery Management service

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 ADM updates the authorization scope to the new entities.

**Configuration Templates:**

If you want to select the specific configuration template that a user can view or manage, perform the following steps:

a) Clear the **All Configuration templates** check box and click **Add Configuration Template**.

b) Select the required template from the list and click **OK**.

![Configuration Templates Table]

**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**.
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:

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND version=1.0
2 <!--NeedCopy--> 
```

This query lists the StyleBooks that meet the following conditions:

- StyleBook name is either lb-mon or lb.
- StyleBook namespace is com.citrix.adc.stylebooks.
• StyleBook version is 1.0.

Use an or operation between value expressions that is defined to the key expression.

Example:

• The name=lb-mon|lb query is valid. It returns the StyleBooks having a name either lb-mon or lb.
• The name=lb-mon | version=1.0 query is invalid.

Press Enter to view the search results and click Save Query.

The saved query appears in the Custom Filters Query. Based on the saved query, the Citrix ADM provides user access to those StyleBooks.

b) Select the required StyleBooks from the list and click OK.

You can select the required StyleBooks when you create groups and add users to that group. When your user selects the permitted StyleBook, all dependent StyleBooks are also selected.

Configpacks:

In Configpacks, select one of the following options:

- All Configurations: This option is selected by default. It adds all the configuration packs that are in Citrix ADM.
• **All Configurations 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 configuration packs.

![Configuration Table]

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 ADM grants the user access to applications depending on the specific authorization scope.

Consider a user who is assigned to a group that has two policies Policy-1 and Policy-2.

- **Policy-1** – View only permission to applications.
- **Policy-2** – View and Edit permission to applications.
The user can view the applications specified in Policy-1. Also, this user can view and edit the applications specified in Policy-2. The edit access to Group-1 applications are restricted as it is not under Group-1 authorization scope.

**Limitations**

RBAC is not fully supported by the following Citrix ADM 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

February 15, 2022

Before you start using the Analytics feature on Citrix ADM 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 ADM 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**.

---

**Configure notifications**

February 15, 2022

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**.
Citrix Application Delivery Management service

- **Licenses** – List of licenses that are currently active, about to expire, and so on. For more information, see The Citrix ADM license expiry.

- **SSL Certificates** – List of SSL certificates that are added to Citrix ADC instances. For more information, see The SSL certificate expiry

Citrix ADM supports the following notification types:

- Email
- SMS
- Slack
- PagerDuty
- ServiceNow

For each notification type, the Citrix ADM GUI displays the configured distribution list or profile. The Citrix ADM sends notifications to the selected distribution list or profile.

**Create an email distribution list**

To receive email notifications for Citrix ADM functions, you must add an email server and a distribution list.

Perform the following steps to create an email distribution list:

1. Navigate to **Settings > Notifications**.
2. In **Email**, click **Add**.
3. In **Create Email Distribution List**, specify the following details:
   - **Name** - Specify the distribution list name.
   - **To** - Specify the email addresses to which Citrix ADM has to send messages.
   - **Cc** - Specify the email addresses to which Citrix ADM has to send message copies.
   - **Bcc** - Specify the email addresses to which Citrix ADM has to send message copies without displaying the addresses.
4. Click Create.

Repeat this procedure to create multiple email distribution lists. The Email tab displays all the email distribution lists present in Citrix ADM.

**Create an SMS distribution list**

To receive SMS notifications for Citrix ADM functions, you must add an SMS server and phone numbers.

Perform the following steps to configure SMS notification settings:

1. Navigate to Settings > Notifications.
2. In SMS, click Add.
3. In Create SMS Distribution List, specify the following details:
   - **Name** - Specify the distribution list name.
   - **SMS Server** - Select the SMS server that sends SMS notification.
Citrix Application Delivery Management service

- **To** - Specify the phone number to which Citrix ADM has to send messages.

4. Click **Create**.

Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in Citrix ADM.

**Create a Slack profile**

To receive Slack notifications for Citrix ADM functions, you must create a slack profile.

Perform the following steps to create a Slack profile:

1. Navigate to **Settings > Notifications**.

2. In **Slack**, click **Add**.

3. In **Create Slack Profile**, specify the following details:
   
   - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
   
   - **Channel Name** - Specify the Slack channel name to which Citrix ADM has to send notifications.
   
   - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. And, all event notifications are sent to this URL are posted on the designated Slack channel. An example of a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT5IFl6oEOVirK

4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in Citrix ADM.
Create a PagerDuty profile

You can add a PagerDuty profile to monitor the incident notifications based on the PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in Citrix ADM, ensure you have completed the required configurations in PagerDuty. To get started with PagerDuty, see PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. Navigate to Settings > Notifications.
2. In PagerDuty, click Add.
3. In Create PagerDuty Profile, specify the following details:
   - Profile Name - Specify a profile name of your choice.
   - Integration Key - Specify the integration key. You can obtain this key from your PagerDuty portal.
4. Click Create.

For more information, see Services and Integrations in the PagerDuty documentation.

Repeat this procedure to create multiple PagerDuty profiles. The PagerDuty tab displays all the PagerDuty profiles present in Citrix ADM.

View the ServiceNow profile

When you want to enable ServiceNow notifications for Citrix ADC events and Citrix ADM events, you must integrate Citrix ADM with the ServiceNow using ITSM connector. For more information, see Integrate Citrix ADM with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. Navigate to Settings > Notifications.
2. In ServiceNow, select the Citrix_Workspace_SN profile from the list.
3. Click Test to auto-generate a ServiceNow ticket and verify the configuration.

If you want to view ServiceNow tickets in the Citrix ADM GUI, select ServiceNow Tickets.

Export or schedule export reports

February 15, 2022
In Citrix ADM, you can export a comprehensive report for the selected Citrix ADM feature. This report provides you an overview of the mapping between the instances, partitions, and corresponding details.

Citrix ADM displays feature-specific scheduled export reports under individual Citrix ADM 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 ADM to the local computer, perform the following steps:

1. Click the export icon at the top-right corner of the page.
2. Select **Export Now**.
3. Select one of the following the export options:
   - **Snapshot** - This option export Citrix ADM reports as a snapshot.
   - **Tabular** - This option export Citrix ADM reports in a tabular format. You can also choose how many data records to export in a tabular format
4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

**Schedule export report**

To schedule the export report at regular intervals, specify the recurrence interval. Citrix ADM sends the exported report to the configured email or slack profile.
1. Click the export icon at the top-right corner of the page.

2. Select **Schedule Export** and specify the following:
   - **Subject** - By default, this field auto-populates the selected feature name. However, you can rewrite it with a meaningful title.
   - **Export option** - Export Citrix ADM reports in a snapshot or a tabular format. You can also choose how many data records to export in a tabular format
   - **Format** - Select the file format that you want to receive the report on the configured email or slack profile.
   - **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the list.
   - **Description** - Specify the meaningful description to a report.
   - **Export Time** - Specify at what time you want to export the report.
   - **Email** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
   - **Slack** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.

3. Click **Schedule**.
View and edit the scheduled export reports

To view the export reports, perform the following:

1. Click the export icon at the top-right corner of the page.
   
   The Export Report page displays all the feature-specific export reports.

2. Select the report that you want to edit and click Edit.
Instance settings

You can manage the discovered instances in Citrix ADM 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 ADM 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 ADM 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 ADM.

In Configure Instance Backup Settings, select Enable Instance Backups.

- Backup Scheduling Settings - You can schedule an instance backup in two ways:
  - Interval Based - A backup file is created in Citrix ADM 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 ADM 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 ADM does not create a backup file when it receives the “NetScalerConfigSave” trap. But, you can enable the option to create a backup file whenever a Citrix ADC instance sends a NetScalerConfigSave trap to Citrix ADM.
    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 ADM, Citrix ADM backs up the instance.
– **Include GeoDB files** - By default, Citrix ADM 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 ADM 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 ADM 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 ADM 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

May 13, 2022

You can manage the discovered instances in Citrix ADM 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 ADM 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 ADM 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 ADM.

In **Configure Instance Backup Settings**, select **Enable Instance Backups**.

- **Backup Scheduling Settings** - You can schedule an instance backup in two ways:
  - **Interval Based** - A backup file is created in Citrix ADM 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 ADM 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 ADM does not create a backup file when it receives the “NetScalerConfigSave” trap. But, you can enable the option to create a backup file whenever a Citrix ADC instance sends a `NetScalerConfigSave` trap to Citrix ADM.

  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 ADM, Citrix ADM backs up the instance.

  - **Include GeoDB files** - By default, Citrix ADM 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 ADM 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 ADM 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 ADM 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

**February 15, 2022**

You can modify the Citrix ADM agent’s keep-alive interval and the Citrix ADM server timezone.

#### Set agent’s keep-alive interval

Citrix ADM server and agent maintain the same TCP connection for the specified keep-alive interval. An agent uses this connection to send the managed instances data to the Citrix ADM 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 ADM time zone

You can choose the timezone in which you want to display the time on the Citrix ADM 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 ADM.
4. Click **Save.**

### Email subscriptions

**April 11, 2022**

Citrix ADM sends in email notifications to all the inactive and the new users.

Inactive customers receive an email notification if:
Citrix Application Delivery Management service

- ADC instances are not configured
- The tenant license expires in less than 30 days

Note:
By default, all such inactive customers receive an email notification.

New ADM customers receive an email from Citrix ADM inviting them to onboard the ADC instances to ADM service where they are able to manage and monitor critical events on ADC instances, troubleshoot, and automate tasks like ADC configuration.
Manage, monitor, troubleshoot, automate with Citrix ADM Service

Congratulations on getting started with ADM service successfully! You can now onboard your ADC instances to ADM service to:

- Monitor critical events on your ADC instances through alerts.
- Automate mundane tasks like ADC configuration.
- Get rich analytics pertaining to ADC and Applications health, performance, and security.

All this is easy to set up and we have resources below to get you started.

Onboard ADC instances on ADM service in 3 quick steps

Start with this brief video to know the exact steps to onboard ADC instances to ADM service quickly. Learn more

Onboard ADC Instances

Sign in using Citrix Cloud/ My Citrix credentials

Your free ADM use cases resources

- Get bird's eye visibility into entire ADC infra and debug critical issues on your ADC instances.
- Manage the complete SSL cert lifecycle using Citrix ADM.
- Always stay on top of critical events with Citrix ADM ServiceNow integration.

Join ADM community

©2022 Citrix System, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems,Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and trademark Office and in other countries. All other marks appearing in this place are the property of their respective owners. Privacy and terms

To unsubscribe this email communication, turn off email notifications in the ADM GUI. For detailed steps, see Unsubscribe email notifications.
Citrix Application Delivery Management service

Unsubscribe Email Notifications

You can subscribe or unsubscribe from the email notifications that you receive from ADM Service. To Unsubscribe Email Notifications:

1. In Citrix Application Delivery and Management, navigate to Settings > Global Settings > System Configurations, and then click Email Subscriptions. The Unsubscribe Email Notifications window appears.

![Unsubscribe Email Notifications](image)

Note:

By default, the toggle button for turning off email notifications is in the off position and the email notifications are enabled for all inactive users.

2. In the Unsubscribe Email Notifications window, turn on the toggle button. Click OK.

You have now unsubscribed the email notifications and will not receive any emails to Onboard ADC instances.

Enable or disable features

February 15, 2022

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 ADM redistributes the ADC instances of the inactive agent with other active agents. For more information, see Configure Citrix ADM 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 ADM automatically polls configured network function entities every 60 minutes. For more information, see Polling overview.
Citrix Application Delivery Management service

- **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 ADM are displayed on the **Events Summary** page (Infrastructure > Events). And all active events are displayed in the Event Messages page (Infrastructure > Events > Event Messages). For more information, see [Events](#).

- **Instance network reporting** - You can generate reports for instances at a global level. Also, for entities such as the virtual servers and network interfaces. For more information, see [Network Reporting](#).

- **Instance SSL certificates** - Citrix ADM 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 ADM. 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

February 15, 2022

You can access system events, syslog messages, and network reporting data for a specific duration in Citrix ADM.

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 ADM:
<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Enables you to limit the event messages stored in Citrix ADM up to 40 days. The events are deleted from Citrix ADM after the retention policy is expired. The cleared events are deleted after one day. For more information, see Events.</td>
</tr>
<tr>
<td>Syslog</td>
<td>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.</td>
</tr>
<tr>
<td>Network Reporting</td>
<td>Enables you to limit the network reporting data stored in Citrix ADM up to 30 days. For more information, see Network Reporting.</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management service

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 ADM retains the storage data up to 500 MB or one day data, whichever is the lesser. For more information, see Manage Citrix ADM resources using Express account.

**Configure an action policy to receive application event notifications**

April 12, 2022
Apart from the existing analytics view of application events, you can configure an action policy to get application event notifications through Slack, Email, PagerDuty, or ServiceNow. The application events include performance issues, bot and WAF violations, and service graph violations. As an administrator, using the action policy, you can get event notifications in real time.

Using the action policy, you can:

- Predefine certain conditions for the application events.
- Get notified for the following events through Slack, Email, PagerDuty, and ServiceNow:
  - All Bot Violations
  (For more information on the list of bot violation, see violation categories.
  - Bot Violation per Client
  - WAF SQL Violation
  - WAF XSS Violation
  - WAF Infer XML Violation
    
    Note
    To receive the WAF violation notification, the minimum violation transactions must be 20%. For example, out of 100 transactions, minimum 20 must be violation transactions.
  - WAF Violation per Client
  - App score violation
  - Client network latency
  - Server network latency
  - Server processing time
  - Service graph violation

Configure an action policy

2. Click Add.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
3. In the **Create Action Policy** page:
   
a) **Policy Name** – Provide a policy name of your choice.

b) **Enabled** – This option is selected by default.

c) If the **Following Event Occurs** – From the list, select an event.

d) **And the Following Condition is Met** – From the list, select to define a condition for which you want to get notified. You can click + to add more conditions. To remove a condition, click –.

   You can configure the action policy using the following operators. The operators appear based on the conditions you select.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal to</td>
<td>Equals to a defined value</td>
</tr>
<tr>
<td>Not Equal to</td>
<td>Not equals to a defined value</td>
</tr>
<tr>
<td>Greater than</td>
<td>Greater than a defined value</td>
</tr>
<tr>
<td>Greater than or Equal to</td>
<td>Greater than or equal to a defined value</td>
</tr>
<tr>
<td>Less than</td>
<td>Lesser than a defined value</td>
</tr>
<tr>
<td>Less than or Equal to</td>
<td>Lesser than or equal to a defined value</td>
</tr>
<tr>
<td>Contains</td>
<td>Contains the defined term or value</td>
</tr>
<tr>
<td>Starts with</td>
<td>Starts with a defined term or value</td>
</tr>
<tr>
<td>Ends with</td>
<td>Ends with a defined term or value</td>
</tr>
</tbody>
</table>

e) **Then Do the Following** – Select Notify. After you select Notify, the Notification Type option is displayed.

f) **Notification Type** – Select the notification type Email, Slack, PagerDuty, or ServiceNow. Depending upon the notification type you select, the corresponding option (Distribution list, Slack Profile, PagerDuty Profile, or ServiceNow profile) appears. Select a profile from the list.

If you want to create a new profile, click **Add**.

g) Click **Create Policy**.

The policy is configured. You can view the configured policy details.
After you configure the policy, you can select the policy and click:

- **Edit** to update or change the action policy. After you update, click Update Policy.
- **Delete** to remove the action policy. You can select multiple policies and click **Delete** to remove them.
- **Action History** to view details such as time, action taken, policy name, alert type, and alert message.

The following table describes the details of action policy configuration.

<table>
<thead>
<tr>
<th>Violation name</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Bot violations</strong></td>
<td>Bot profile</td>
<td>The bot profile name that is used for configuring bot management on the ADC instance.</td>
</tr>
<tr>
<td>Instance IP</td>
<td></td>
<td>IP address of the ADC instance. Select the IP address from the list.</td>
</tr>
<tr>
<td>Violation Count</td>
<td></td>
<td>The violation count for which you want to get notified. For example, if you configure violation count as less or equal to 10, you will get notified if 10 or less bot violation transactions are received.</td>
</tr>
<tr>
<td>Violation name</td>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Violation Ratio</td>
<td></td>
<td>This value indicates the total violations from specific transactions and the value must be between 0 and 1. For example, out of 100 transactions, 20 are violations and if you wanted to get notified for such a scenario, you must enter 0.2.</td>
</tr>
</tbody>
</table>

### Bot Violation per Client

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>The custom application name. Select the application from the list. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
<tr>
<td>Instance IP</td>
<td>IP address of the ADC instance. Select the IP address from the list.</td>
</tr>
<tr>
<td>Client IP</td>
<td>The source from where the Bot originates. Specify the IP address.</td>
</tr>
<tr>
<td>Total Attacks</td>
<td>The total attacks for which you want to get notified.</td>
</tr>
<tr>
<td>Violation Type</td>
<td>Select the bot violation from the list.</td>
</tr>
<tr>
<td>Request URL</td>
<td>The URL that you want to configure to block. Specify the URL.</td>
</tr>
<tr>
<td>Vserver name</td>
<td>The associated applications configured for custom applications. Select the application from the list. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
<tr>
<td>Violation name</td>
<td>Condition</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>WAF SQL Violation, WAF XSS Violation, WAF Infer XML Violation</strong></td>
<td>WAF Profile</td>
</tr>
<tr>
<td>Instance IP</td>
<td></td>
</tr>
<tr>
<td>Violation Count</td>
<td></td>
</tr>
<tr>
<td>Violation Ratio</td>
<td></td>
</tr>
<tr>
<td><strong>WAF Violation per Client</strong></td>
<td>Application Name</td>
</tr>
<tr>
<td>Instance IP</td>
<td></td>
</tr>
<tr>
<td>Client IP</td>
<td></td>
</tr>
<tr>
<td>Total Attacks</td>
<td></td>
</tr>
<tr>
<td>Violation name</td>
<td>Condition</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Violation Type</td>
<td></td>
</tr>
<tr>
<td>Request URL</td>
<td></td>
</tr>
<tr>
<td>Vserver name</td>
<td></td>
</tr>
</tbody>
</table>

**App Score Violation**

<table>
<thead>
<tr>
<th>Performance Indicator</th>
<th>Performance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The app score components and their threshold values. Select the app score component from the list. For more information, see Select App Score components and set thresholds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Breach Count</th>
<th>Breach Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The breach count for which you want to get notified. For example, if you configure breach count Equal to 5 for response time, you will get notified when the response time threshold is breached 5 times.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Application Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select the application that you want to get the app score violation notified. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
</tbody>
</table>
### Citrix Application Delivery Management service

<table>
<thead>
<tr>
<th>Violation name</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Network Latency</strong></td>
<td>Client Network Latency (milliseconds)</td>
<td>Specify the client latency (client to ADC) value in milliseconds for which you want to get notified.</td>
</tr>
<tr>
<td></td>
<td>Application Name</td>
<td>Select the application that you want to get the violation notified. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
<tr>
<td><strong>Server Network Latency</strong></td>
<td>Server Network Latency (milliseconds)</td>
<td>Specify the server latency (server to ADC) value in milliseconds for which you want to get notified.</td>
</tr>
<tr>
<td></td>
<td>Application Name</td>
<td>Select the application that you want to get the violation notified. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
<tr>
<td><strong>Server Processing Time</strong></td>
<td>Server Processing Time (milliseconds)</td>
<td>Specify the server processing (server to ADC) value in milliseconds for which you want to get notified.</td>
</tr>
<tr>
<td></td>
<td>Application Name</td>
<td>Select the application that you want to get the violation notified. If you do not add this condition, then all applications from the ADC instance are considered.</td>
</tr>
<tr>
<td><strong>Service Graph Violation</strong></td>
<td></td>
<td>Microservices that breach the configured thresholds. For more information, see Configure thresholds in service graph.</td>
</tr>
</tbody>
</table>
Use the search bar

The search bar enables you to filter results. When you click the search bar, it gives you a list of search suggestions. You can select the component and filter results based on your requirements.

Use the audit logs option

Click Audit Logs and select the duration from the list to view the action policies that are created, modified, and deleted for the selected duration.

Use audit logs for managing and monitoring your infrastructure

February 15, 2022
You can use the Citrix ADM to track all events on Citrix ADM and syslog events generated on Citrix ADM 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 ADM simplifies the way of reviewing log messages. 

You can use filters to search Citrix ADM syslog and audit log messages. The filters help to narrow down your results and find exactly what you are looking for and in real time. The built-in Search Help guides you to filter the logs. Another way to view log messages is to export them in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses at various intervals. 

You can review the following types of log messages from the Citrix ADM GUI:

- ADC instance related audit logs
- Citrix ADM related audit logs
- Application audit logs

**ADC instance related audit logs**

Before you can view ADC instance-related syslog messages from Citrix ADM, configure the Citrix ADM as the syslog server for your Citrix ADC instance. After the configuration is complete, all syslog messages are redirected from the instance to Citrix ADM. 

**Configure Citrix ADM as a syslog server**

Follow these steps to configure Citrix ADM as the syslog server:

1. From the Citrix ADM 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 ADM.
3. In the Select Action list, select Configure Syslog.
4. Click Enable.
5. In the Facility drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click OK.
Citrix Application Delivery Management service

These steps configure all the syslog commands in the Citrix ADC instance, and Citrix ADM starts receiving the syslog messages. You can view the messages by navigating to Infrastructure > Events > Syslog Messages. Click Need Help? to open the built-in search help. For more information, see View and Export syslog messages.

To export the log messages, click the arrow icon on the upper right corner.

Next, click Export Now or Schedule Export. For more information, see Export syslog messages.

Citrix ADM related audit logs

Based on preconfigured rules, Citrix ADM generates audit log messages for all events on, helping you monitor the health of your infrastructure. To view all audit log messages present in the Citrix ADM, navigate to Settings->Audit Log Messages.
To export the log messages, click the arrow icon on the upper right corner.

**Application related audit logs**

You can view the audit log messages for all Citrix ADM applications or for a specific application.

- To view all audit log messages for all applications present in the Citrix ADM, navigate to **Infrastructure > Network Functions > Auditing**.

- To view audit log messages for any specific application in the Citrix ADM, navigate to **Applications > Dashboard > double-click the virtual server > Audit Log**.

**Note**

You can forward Citrix ADM audit log messages to an external server. For details, see **View auditing information**.

**Configure IP address management (IPAM)**

February 15, 2022
Citrix ADM IPAM provides you an ability to auto-assign and release IP addresses in Citrix ADM managed configurations. You can assign IPs from networks or IP ranges defined using the following IP providers:

- Citrix ADM built-in IPAM provider.
- Infoblox IPAM solution. For more information, see Infoblox DDI.

Currently, you can use Citrix ADM IPAM in:

- **StyleBooks**: Auto-Allocate IPs to virtual servers when you create configurations.
- **Kubernetes Ingress**: Auto-assign a virtual IP address to an Ingress configuration in a Kubernetes cluster.
- **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 ADM.

### Add an external IP address provider

Citrix ADM has a built-in IPAM provider to manage IPs and IP ranges. You can also add an external IP address provider to Citrix ADM.

**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 ADM:

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 ADM.
   - **Vendor** - Select an IPAM vendor from the list.
   - **URL** - Specify the URL of the IPAM solution that assigns IP addresses in an Citrix ADM environment. Ensure to specify the URL in the following format:
Citrix Application Delivery Management service

```
1  https://<host name>
2  <!--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 ADM 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 ADM.
   - **Provider** - Select the provider from the list.
     This list displays the providers added in Citrix ADM.
   - **Network Type** - Select **IP range** or **CIDR** from the list based on your requirement.
   - **Network Value** - Specify the network value.

   **Note**

   Citrix ADM IPAM supports only IPv4 addresses.

   For **IP range**, specify the network value in the following format:

   ```
   1  <first-IP-address>-<last-IP-address>
   2  <!--NeedCopy-->
   ```

   Example:

   ```
   1  10.0.0.20-10.0.0.100
   2  <!--NeedCopy-->
   ```

   For **CIDR**, specify the network value in the following format:
1. `<IP-address>/subnet-mask`
2. `<!--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**.

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 ADM 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

February 15, 2022

Citrix ADM "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 ADM 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.

<table>
<thead>
<tr>
<th>TOPICS</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance management</td>
<td>Configuration management</td>
<td>Certificate management</td>
</tr>
<tr>
<td>StyleBooks</td>
<td>Event management</td>
<td></td>
</tr>
</tbody>
</table>

**Instance management**

- How to monitor globally distributed sites
- How to manage admin partitions of Citrix ADC instances
- How to add instances to Citrix ADM
- How to create instance groups on Citrix ADM
- How to poll Citrix ADC instances and entities in Citrix ADM
- How to configure sites for Geomaps in Citrix ADM
- 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 ADM
- How to schedule jobs created by using built-in templates in Citrix ADM
- How to reschedule jobs that were configured by using built-in templates in Citrix ADM

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Application Delivery Management service

Reuse run configuration jobs
How to upgrade Citrix ADC instances using Citrix ADM
How to create a configuration job on Citrix ADM
How to use variables in configuration jobs on Citrix ADM
How to use configuration templates to create audit templates on Citrix ADM
How to create configuration jobs from corrective commands on Citrix ADM
How to replicate running and saved configuration commands from one Citrix ADC instance to another on Citrix ADM
How to use configuration jobs to replicate configuration from one instance to multiple instances
How to use the master configuration template on Citrix ADM

Certificate management
How to configure an enterprise policy on Citrix ADM
How to install SSL certificates on a Citrix ADC instance from Citrix ADM
How to update an installed certificate from Citrix ADM
How to link and unlink SSL certificates by using Citrix ADM
How to create a certificate signing request (CSR) by using Citrix ADM
How to set up notifications for SSL certificate expiry from Citrix ADM
How to use the SSL dashboard on Citrix ADM

StyleBooks
How to use default StyleBooks in Citrix ADM
How to create your own StyleBooks
How to use user-defined StyleBooks in Citrix ADM
How to use API to create configurations from StyleBooks
How to enable analytics and configure alarms on a virtual server defined in a StyleBook
How to create a StyleBook to upload SSL certificate and certificate key files to Citrix ADM
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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
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 ADM
How to schedule an event filter by using Citrix ADM
How to set repeated email notifications for events from Citrix ADM
How to suppress events by using Citrix ADM
How to use the events dashboard to monitor events
How to create event rules on Citrix ADM
How to modify the reported severity of events that occur on Citrix ADC instances
How to view the events summary in Citrix ADM
How to display event severities and skews of SNMP traps on Citrix ADM
How to export syslog messages using Citrix ADM
How to suppress Syslog messages in Citrix ADM

FAQs

June 10, 2022

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.
Does Citrix ADM agent support AMD processors?
Yes.

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 ADM 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 ADM 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 ADM 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?

Ensure that:

- Your agent has access to the Internet (configure DNS).
- You have copied the activation code correctly.
- You have entered the service URL correctly.
- 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 ADM 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 ADM using a proxy server?

You can connect agents to Citrix ADM using a proxy server. The agents forward all their data to the proxy server, which then sends the data to the Citrix ADM 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 ADM 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 ADM.

For more information, see [Citrix ADM as an API proxy server](#).

**Note**

Citrix ADM supports proxy servers with basic authentication enabled. Citrix ADM 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 ADM?

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 ADM?

To export the report of any dashboard in Citrix ADM, 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 ADM captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.