# Contents

**Release notes** 3

**All how to articles** 4

**Overview** 9

**Features and solutions** 9

**Architecture** 12

**How Citrix ADM discovers instances** 13

**Polling overview** 15

**Data governance** 23

**Licensing** 24

**System requirements** 33

**Get started** 42

**Deploy** 46

**Prerequisites for installing Citrix ADM** 47

**Citrix ADM with Citrix Hypervisor** 48

**Citrix ADM with Microsoft Hyper-V** 50

**Citrix ADM with VMware ESXi** 57

**Citrix ADM with Linux KVM server** 62

**Configure high availability deployment** 68

**Configure disaster recovery for high availability** 84

**Configure on-prem agents for multisite deployment** 92

**Migrate Citrix ADM single-server deployment to a high availability deployment** 103

**Migrate from NetScaler Insight Center to Citrix ADM** 108

**Migrate Command Center configurations to Citrix ADM** 110

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Integrate Citrix ADM with Citrix Director 117
Attach an additional disk to Citrix ADM 119
Configure 131
Add instances to Citrix ADM 132
Add Citrix ADC VPX instances deployed in cloud to Citrix ADM 139
Enable analytics on virtual servers 141
Configure NTP server 144
Configure system settings 145
Upgrade 148
Authentication 159
How to extract an authentication server group 167
How to add LDAP authentication servers 170
How to enable fallback local authentication 172
How to add RADIUS authentication servers 173
How to add TACACS authentication servers 177
How to cascade external authentication servers 178
Access control 180
Role-based access control 180
Configure access policies 183
Configure groups 187
Configure roles 191
Configure users 192
Multi-tenancy: Provide exclusive management environment to your tenants 194
Applications 203
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application performance analytics</td>
<td>216</td>
</tr>
<tr>
<td>Application security analytics</td>
<td>219</td>
</tr>
<tr>
<td>Create an application definition</td>
<td>219</td>
</tr>
<tr>
<td>Create a threshold and alert for application analytics</td>
<td>225</td>
</tr>
<tr>
<td>StyleBooks</td>
<td>226</td>
</tr>
<tr>
<td>StyleBook groups</td>
<td>228</td>
</tr>
<tr>
<td>Use default StyleBooks</td>
<td>235</td>
</tr>
<tr>
<td>Hide all default StyleBooks</td>
<td>240</td>
</tr>
<tr>
<td>SSO Google Apps StyleBook</td>
<td>241</td>
</tr>
<tr>
<td>SSO Office 365 StyleBook</td>
<td>245</td>
</tr>
<tr>
<td>Microsoft Skype for Business StyleBook</td>
<td>254</td>
</tr>
<tr>
<td>Microsoft Exchange StyleBook</td>
<td>262</td>
</tr>
<tr>
<td>Microsoft SharePoint StyleBook</td>
<td>265</td>
</tr>
<tr>
<td>Microsoft ADFS proxy StyleBook</td>
<td>273</td>
</tr>
<tr>
<td>Oracle e-business Stylebook</td>
<td>291</td>
</tr>
<tr>
<td>Create and use custom StyleBooks</td>
<td>293</td>
</tr>
<tr>
<td>StyleBook to create a load balancing virtual server</td>
<td>295</td>
</tr>
<tr>
<td>StyleBook to create a basic load balancing configuration</td>
<td>302</td>
</tr>
<tr>
<td>Create a composite StyleBook</td>
<td>311</td>
</tr>
<tr>
<td>Use GUI attributes in a custom StyleBook</td>
<td>313</td>
</tr>
<tr>
<td>Use custom StyleBooks</td>
<td>315</td>
</tr>
<tr>
<td>Create a StyleBook to upload files to Citrix ADM</td>
<td>320</td>
</tr>
<tr>
<td>Create a StyleBook to upload SSL certificate and certificate key files to Citrix ADM</td>
<td>323</td>
</tr>
<tr>
<td>Enable analytics and configure alarms on a virtual server defined in a StyleBook</td>
<td>331</td>
</tr>
<tr>
<td>Instance roles</td>
<td>332</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Create a Stylebook to perform non-CRUD operations</td>
<td>342</td>
</tr>
<tr>
<td>Use API to create configurations from StyleBooks</td>
<td>343</td>
</tr>
<tr>
<td>Use API to create configurations to upload certificate and key files</td>
<td>351</td>
</tr>
<tr>
<td>Use API to create configurations to upload any file type</td>
<td>354</td>
</tr>
<tr>
<td>Use API to import custom StyleBooks</td>
<td>355</td>
</tr>
<tr>
<td>Use API to download custom StyleBooks</td>
<td>356</td>
</tr>
<tr>
<td>Use API to delete custom StyleBooks</td>
<td>357</td>
</tr>
<tr>
<td>StyleBooks grammar</td>
<td>358</td>
</tr>
<tr>
<td>Header</td>
<td>359</td>
</tr>
<tr>
<td>Import StyleBooks</td>
<td>360</td>
</tr>
<tr>
<td>Parameters</td>
<td>362</td>
</tr>
<tr>
<td>Parameters-default-sources construct</td>
<td>372</td>
</tr>
<tr>
<td>Substitutions</td>
<td>375</td>
</tr>
<tr>
<td>Components</td>
<td>381</td>
</tr>
<tr>
<td>Helper components</td>
<td>383</td>
</tr>
<tr>
<td>Optional properties</td>
<td>385</td>
</tr>
<tr>
<td>Properties-default-sources construct</td>
<td>386</td>
</tr>
<tr>
<td>Nested components</td>
<td>388</td>
</tr>
<tr>
<td>Condition construct</td>
<td>389</td>
</tr>
<tr>
<td>Repeat construct</td>
<td>391</td>
</tr>
<tr>
<td>Repeat-condition construct</td>
<td>393</td>
</tr>
<tr>
<td>Nested repeats</td>
<td>394</td>
</tr>
<tr>
<td>Outputs</td>
<td>395</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Parameter reference</td>
<td>396</td>
</tr>
<tr>
<td>Parent reference</td>
<td>397</td>
</tr>
<tr>
<td>Components reference</td>
<td>399</td>
</tr>
<tr>
<td>Substitutions reference</td>
<td>400</td>
</tr>
<tr>
<td>Variable reference</td>
<td>400</td>
</tr>
<tr>
<td>Operations</td>
<td>401</td>
</tr>
<tr>
<td>Analytics</td>
<td>403</td>
</tr>
<tr>
<td>Alarms</td>
<td>405</td>
</tr>
<tr>
<td>Expressions</td>
<td>410</td>
</tr>
<tr>
<td>In-place interpolations</td>
<td>414</td>
</tr>
<tr>
<td>Built-in functions</td>
<td>418</td>
</tr>
<tr>
<td>Dependency detection</td>
<td>427</td>
</tr>
<tr>
<td>Instance management</td>
<td>429</td>
</tr>
<tr>
<td>Monitor globally distributed sites</td>
<td>432</td>
</tr>
<tr>
<td>How to create tags and assign to instances</td>
<td>437</td>
</tr>
<tr>
<td>How to search instances using values of tags and properties</td>
<td>440</td>
</tr>
<tr>
<td>Manage admin partitions of Citrix ADC instances</td>
<td>443</td>
</tr>
<tr>
<td>Back up and restore Citrix ADC instances</td>
<td>447</td>
</tr>
<tr>
<td>Force a failover to the secondary Citrix ADC instance</td>
<td>453</td>
</tr>
<tr>
<td>Force a secondary Citrix ADC instance to stay secondary</td>
<td>454</td>
</tr>
<tr>
<td>Create instance groups</td>
<td>455</td>
</tr>
<tr>
<td>Rediscover multiple Citrix VPX instances</td>
<td>456</td>
</tr>
<tr>
<td>Unmanage an instance</td>
<td>457</td>
</tr>
<tr>
<td>Trace the route to an instance</td>
<td>457</td>
</tr>
</tbody>
</table>
Events 458
Use events dashboard 458
Set event age for events 460
Schedule an event filter 461
Set repeated email notifications for events 462
Suppress events 464
Create event rules 464
Modify the reported severity of events that occur on Citrix ADC instances 474
View events summary 475
Display event severities and SNMP trap details 476
Export syslog messages 478
Suppress syslog messages 481
Configure prune settings for instance events 483
SSL Dashboard 484
Use the SSL Dashboard 485
Set up notifications for SSL certificate expiry 488
Update an installed certificate 489
Install SSL certificates on a Citrix ADC instance 490
Create a Certificate Signing Request (CSR) 492
Link and unlink SSL certificates 494
Configure an enterprise policy 495
Poll SSL certificates from Citrix ADC instances 495
Configuration jobs 496
Create a configuration job 498
Use record-and-play to create configuration jobs 500
Use configuration jobs to replicate configuration from one instance to multiple instances 505
Use variables in configuration jobs 508
Create configuration jobs from corrective commands 514
Replicate running and saved configuration from one NetScaler instance to another 515
Reuse executed configuration jobs 517
Schedule jobs created by using built in templates 518
Use maintenance jobs to upgrade NetScaler SDX instances 520
Create configuration jobs for Citrix SD-WAN WANOP instances 521
Use the master configuration template 527
Use jobs to upgrade Citrix ADC instances 533
Use configuration templates to create audit templates 537
Use SCP (put) command in configuration jobs 540
Reschedule jobs configured by using built in templates 543
Reuse configuration audit templates in configuration jobs 544
Import and export configuration templates 549
Maintenance jobs 552
Configuration audit 562
Create audit templates 562
View audit reports 567
Audit configuration changes across instances 570
Get configuration advice on network configuration 574
Poll configuration audit of Citrix ADC instances 576
Generate configuration audit diff for ConfigChange SNMP Traps 578
Network functions  578
Generate reports for load balancing entities  579
Export or schedule export of network functions reports  583
Network reporting  586
Analytics  597
License requirements  598
Logstream overview  599
Disable URL data collection  603
Create thresholds and alerts  603
Configure adaptive thresholds  604
Configure database persistence  605
Self-service diagnostics for Analytics  606
Web Insight  610
HDX Insight  636
Create thresholds and configure alerts for HDX Insight  643
Viewing HDX Insight reports and metrics  647
Application View Reports and Metrics  694
Desktop View Reports and Metrics  702
User View Reports and Metrics  715
Instance View Reports and Metrics  732
License View Reports and Metrics  739
Enabling HDX Insight data collection  740
Enable data collection for Citrix Gateway appliances deployed in single-hop mode  754
Enable data collection to monitor NetScaler ADCs deployed in transparent mode  756
Enable data collection for Citrix Gateway appliances deployed in double-hop mode
Enable data collection to monitor NetScaler ADCs deployed in LAN user mode
Gateway Insight
Security Insight
SSL Insight
TCP Insight
WAN Insight
Video Insight
View network efficiency
Compare the data volume used by optimized and unoptimized ABR videos
View the type of videos streamed and data volume consumed from your network
Compare optimized and unoptimized play time of ABR videos
Compare bandwidth consumption of optimized and unoptimized ABR videos
Compare optimized and unoptimized number of plays of ABR videos
View peak data rate for a specific time frame
Secure Web Gateway Analytics
Dashboards
Use cases
Orchestration
OpenStack: Integrate Citrix ADC instances
Prerequisites
Pre-configuration tasks in Citrix ADM and OpenStack
Configure LBaaS V1 using Horizon
Configure LBaaS V2 using command line
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure layer 7 content switching</td>
<td>881</td>
</tr>
<tr>
<td>Manual provisioning of Citrix ADC VPX instance on OpenStack</td>
<td>888</td>
</tr>
<tr>
<td>Provisioning of Citrix ADC VPX instance on OpenStack using StyleBook</td>
<td>890</td>
</tr>
<tr>
<td>VPX check-in and check-out license and pooled license support for OpenStack environment</td>
<td>891</td>
</tr>
<tr>
<td>Shared VLAN support for admin partitions</td>
<td>894</td>
</tr>
<tr>
<td>Trial licensing workflow</td>
<td>896</td>
</tr>
<tr>
<td>Integrate with OpenStack Heat services</td>
<td>897</td>
</tr>
<tr>
<td>Service package isolation policies</td>
<td>902</td>
</tr>
<tr>
<td>Flexible policy-based device allotment</td>
<td>903</td>
</tr>
<tr>
<td>NSX Manager: manual provisioning of Citrix ADC instances</td>
<td>907</td>
</tr>
<tr>
<td>NSX Manager: auto provisioning of Citrix ADC instances</td>
<td>924</td>
</tr>
<tr>
<td>Citrix ADC automation using Citrix ADM in Cisco ACI hybrid mode</td>
<td>935</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>938</td>
</tr>
<tr>
<td>Configure Citrix ADC in hybrid mode using Cisco APIC and Citrix ADM</td>
<td>938</td>
</tr>
<tr>
<td>Create a StyleBook for an application using Citrix ADM</td>
<td>939</td>
</tr>
<tr>
<td>Import Citrix ADC hybrid-mode device package into Cisco APIC</td>
<td>940</td>
</tr>
<tr>
<td>Create and deploy a service graph</td>
<td>941</td>
</tr>
<tr>
<td>Configure L4-L7 parameters from Citrix ADM using StyleBook</td>
<td>952</td>
</tr>
<tr>
<td>APIC fault reports</td>
<td>956</td>
</tr>
<tr>
<td>Logs generated by Citrix ADM</td>
<td>957</td>
</tr>
<tr>
<td>Logs generated by hybrid-mode device package</td>
<td>962</td>
</tr>
<tr>
<td>Citrix ADC device package in Cisco ACI’s cloud orchestrator mode</td>
<td>967</td>
</tr>
<tr>
<td>Licenses for Citrix ADM License server in high availability</td>
<td>972</td>
</tr>
<tr>
<td>Citrix ADC pooled capacity</td>
<td>973</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Configure Citrix ADC pooled capacity 978
Upgrade a Perpetual License in Citrix ADC MPX to Citrix ADC Pooled Capacity 989
Upgrade a perpetual license in Citrix ADC SDX to Citrix ADC pooled capacity 1000
Citrix ADC pooled capacity on Citrix ADC instances in cluster mode 1003
Health monitoring 1006
Expected behaviors when issues arise 1007
Configure expiry checks for pooled capacity licenses 1008
Citrix ADC VPX check-in and check-out licensing 1010
Citrix ADC virtual CPU licensing 1018
Manage Citrix SD-WAN instances 1024
Add Citrix SD-WAN SE/PE instances 1028
View Citrix SD-WAN analytics data for multi-hop deployment 1031
View event reports for Citrix SD-WAN WANOP Instances 1035
View network reports for Citrix SD-WAN WANOP Instances 1035
Back up Citrix SD-WAN WANOP instances 1037
Manage HAProxy instances 1044
Add HAProxy instances to Citrix ADM 1045
HAProxy app dashboard 1048
Third-party licensing 1053
Role-based access control for HAProxy instances 1056
Monitor HAProxy instances 1056
View the details of frontends configured on HAProxy instances 1057
View the details of backends configured on HAProxy instances 1058
View the details of servers configured on HAProxy instances 1059
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the HAProxy instances with the highest number of frontends or servers</td>
<td>1060</td>
</tr>
<tr>
<td>Restart an HAProxy instance</td>
<td>1061</td>
</tr>
<tr>
<td>Back up and restore an HAProxy instance</td>
<td>1062</td>
</tr>
<tr>
<td>Edit the HAProxy configuration file</td>
<td>1063</td>
</tr>
<tr>
<td>Manage system settings</td>
<td>1065</td>
</tr>
<tr>
<td>Configure system backup settings</td>
<td>1077</td>
</tr>
<tr>
<td>Configure a NTP server</td>
<td>1078</td>
</tr>
<tr>
<td>Upgrade Citrix ADM</td>
<td>1079</td>
</tr>
<tr>
<td>How to reset the password for Citrix ADM</td>
<td>1080</td>
</tr>
<tr>
<td>Configure syslog purging interval</td>
<td>1087</td>
</tr>
<tr>
<td>Configure system prune settings</td>
<td>1088</td>
</tr>
<tr>
<td>Enable shell access for non-default users</td>
<td>1090</td>
</tr>
<tr>
<td>Recover inaccessible Citrix ADM servers</td>
<td>1091</td>
</tr>
<tr>
<td>Assign a host name to a Citrix ADM server</td>
<td>1096</td>
</tr>
<tr>
<td>Back up and restore your Citrix ADM server in a single-server deployment</td>
<td>1096</td>
</tr>
<tr>
<td>View auditing information</td>
<td>1100</td>
</tr>
<tr>
<td>Configure SSL settings</td>
<td>1101</td>
</tr>
<tr>
<td>Monitor CPU, memory, and disk usage</td>
<td>1102</td>
</tr>
<tr>
<td>Configure system notification settings</td>
<td>1103</td>
</tr>
<tr>
<td>Generate a tech support file</td>
<td>1107</td>
</tr>
<tr>
<td>Diagnose and troubleshoot Citrix ADC instances</td>
<td>1108</td>
</tr>
<tr>
<td>Back up and restore a Citrix ADM configuration in an HA pair</td>
<td>1111</td>
</tr>
<tr>
<td>Configure a cipher group</td>
<td>1112</td>
</tr>
<tr>
<td>Create SNMP trap destination, manager community, and users</td>
<td>1113</td>
</tr>
</tbody>
</table>
Configure and view system alarms 1114

Citrix ADM as an API proxy server 1116

Autoscaling of Citrix ADC in AWS using Citrix ADM 1121

Architecture 1127

Autoscale configuration 1131

Dashboard 1146

FAQs 1147
August 1, 2019

The Citrix Application Delivery Management (ADM) 12.1 release notes describe the new features, enhancements to existing features, and the known issues in a build. The release notes for the 12.1 release includes the following sections:

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

To view the complete release notes document, click the following link.

<table>
<thead>
<tr>
<th>Release Notes</th>
<th>Publishing Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release notes for Build 53.12 of Citrix ADM 12.1 Release</td>
<td>Published: July 18, 2019</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 52.15 of Citrix ADM 12.1 Release</td>
<td>Published: June 10, 2019</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 50.43 of Citrix ADM 12.1 Release</td>
<td>Published: May 17, 2019</td>
<td>Release note version: 2.0</td>
</tr>
<tr>
<td>Release notes for Build 50.39 of Citrix ADM 12.1 Release</td>
<td>Published: May 17, 2019</td>
<td>Release note version: 2.0</td>
</tr>
<tr>
<td>Release notes for Build 50.33 of Citrix ADM 12.1 Release</td>
<td>Published: April 16, 2019</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 50.30 of Citrix ADM 12.1 Release</td>
<td>Published: January 14, 2019</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 50.28 of Citrix ADM 12.1 Release</td>
<td>Published: December 1, 2018</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 49.23 of Citrix ADM 12.1 Release</td>
<td>Published: August 29, 2018</td>
<td>Release note version: 1.0</td>
</tr>
<tr>
<td>Release notes for Build 48.18 of Citrix ADM 12.1 Release</td>
<td>Published: June 18, 2018</td>
<td>Release note version: 2.0</td>
</tr>
</tbody>
</table>

**Note**

These release notes do not document security related fixes. For a list of security related fixes and
All how to articles

August 1, 2019

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

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

<table>
<thead>
<tr>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance management</td>
</tr>
<tr>
<td>Event management</td>
</tr>
<tr>
<td>StyleBooks</td>
</tr>
<tr>
<td>Certificate management</td>
</tr>
<tr>
<td>Citrix ADM System</td>
</tr>
<tr>
<td>Application management</td>
</tr>
<tr>
<td>Configuration management</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Analytics</td>
</tr>
<tr>
<td>Network functions</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 configure sites for Geomaps in Citrix ADM
How to force a failover to the secondary Citrix ADC instance by using Citrix ADM
How to force a secondary Citrix ADC instance to stay secondary by using Citrix ADM
How to back up and restore an instance using Citrix ADM
How to use the Citrix ADM dashboard to monitor an HAProxy instance
How to display the details of the frontends configured on HAProxy instances
How to display the details of the backends configured on HAProxy instances
How to display the details of the servers configured on HAProxy instances
How to restart an HAProxy instance from Citrix ADM
How to back up and restore an HAProxy instance by using Citrix ADM
How to edit the HAProxy configuration file by using Citrix ADM
How to rediscover multiple Citrix ADC VPX instances
How to poll Citrix ADC instances and entities in Citrix ADM
How to unmanage an instance on Citrix ADM
How to trace the route to an instance from Citrix ADM

Configuration management

How to create a configuration job on Citrix ADM
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
How to reuse executed configuration jobs
How to upgrade Citrix ADC instances using 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 create configuration jobs for Citrix SD-WAN WO instances in Citrix ADM
How to use Record-and-Play to create configuration jobs
How to use configuration jobs to replicate configuration from one instance to multiple instances
How to use the master configuration template on Citrix ADM
How to poll configuration audit of Citrix ADC instances
How to reuse configuration audit templates in configuration jobs
How to import and export configuration templates
How to generate configuration audit diff for ConfigChange SNMP traps
Certificate management

How to configure an enterprise policy on 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
How to poll SSL certificates from Citrix ADC Instances

Application management

How to create an application definition in Citrix ADM

StyleBooks

How to view different groups of StyleBooks
How to use StyleBooks shipped with 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 files to Citrix ADM
How to use API to create configurations to upload any file type
How to create a StyleBook to upload SSL certificate and certificate key files to Citrix ADM
How to use API to create configurations to upload cert and key files
How to use Microsoft Skype for Business StyleBook in business enterprises
How to use Microsoft Exchange StyleBook in business enterprises
How to use Microsoft SharePoint StyleBook in business enterprises
Analytics

How to enable analytics on instances
How to configure adaptive thresholds
How to configure SLA management
How to configure database summarization for analytics
How to create thresholds and alerts using Citrix ADM
How to disable URL data collection for analytics from Citrix ADM
How to view the type of videos streamed and the data volume consumed from your network
How to view the peak data rate for a particular time frame
How to compare the optimized and un-optimized number of plays of ABR videos
How to compare the optimized and un-optimized play time of ABR videos
How to compare bandwidth consumption of optimized and un-optimized ABR videos
How to compare the data volume used by optimized and un-optimized ABR videos
How to view the network efficiency

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
How to configure prune settings for instance events
Authentication

How to cascade external authentication servers
How to add RADIUS authentication servers
How to add LDAP authentication servers
How to add TACACS authentication servers
How to extract authentication server group in Citrix ADM
How to enable fallback local authentication

Citrix ADM system

How to upgrade Citrix ADM
How to reset the password for Citrix ADM
How to generate a tech support file for Citrix ADM
How to back up and restore your Citrix ADM server in a single server deployment
How to back up and restore a Citrix ADM configuration in an HA pair
How to enable shell access for non-default users in Citrix ADM
How to configure NTP server on Citrix ADM
How to configure SSL settings for Citrix ADM
How to configure syslog purging interval for Citrix ADM
How to view auditing information of Citrix ADM
How to configure system notification settings of Citrix ADM
How to monitor CPU, memory, and disk usage of Citrix ADM
How to configure a cipher group for Citrix ADM
How to create SNMP traps, managers, and users on Citrix ADM
How to assign a host name to a Citrix ADM server
How to configure system prune settings for Citrix ADM
How to configure system backup settings by using Citrix ADM
How to configure and view system alarms on Citrix ADM
How to diagnose and troubleshoot Citrix ADC instances
Network functions

How to generate reports for load balancing entities
How to export or schedule export of network functions reports

Overview

August 1, 2019

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

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

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

ADM enables IT administrators to troubleshoot as well as proactively monitor customer issues in matter of minutes.

Features and solutions

August 1, 2019

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

Application Analytics and Management

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

Application security analytics

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

Networks

Instances

Enables you to manage the Citrix ADC, Citrix Gateway, Citrix SD-WAN, and HAProxy instances.

Instance groups

Enables you to group your instances as follows:

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

Event management

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

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

Certificate management

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 ADM’s SSL dashboard and its functionalities, you must understand what an SSL certificate is and how you can use ADM to keep track of your SSL certificates.

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 ADM.

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

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

Network reporting

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

Analytics

Web Insight

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

HDX Insight

Provides end-to-end visibility for ICA traffic passing through 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.

Gateway Insight

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

Security Insight

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

SSL Insight

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

TCP Insight

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

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

**WAN Insight**

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

**Orchestration**

**Cloud Orchestration**

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

**Orchestration**

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

**Architecture**

**August 1, 2019**

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

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

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

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

**How Citrix ADM discovers instances**

August 1, 2019

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

- Citrix ADC instances
  - Citrix MPX
Citrix Application Delivery Management 12.1

- Citrix VPX
- Citrix SDX
- Citrix CPX

- Citrix Gateway instances
- Citrix SD-WAN instances

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

**Note**

Citrix ADM uses the NetScaler IP (NSIP) address of the Citrix ADC instances for communication. ADM can also discover ADC instances with subnet IP (SNIP) address that has management access enabled on it. For information about the ports that must be open between the ADC instances and ADM, see Ports.

For Citrix SD-WAN WO, ADM uses the management IP address of the instances for communication.

You cannot add Citrix SD-WAN SE / EE instances in ADM. You can configure ADM as an AppFlow collector on the Citrix SD-WAN SE/EE appliances.

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

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

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

1. Citrix ADM uses the instance profile details to log on to the instance. Using a ADC NITRO call, ADM retrieves the license information of the instance. Based on the licensing information, it determines whether the instance is a ADC instance and the type of ADC platform (for example, Citrix ADC MPX, ADC VPX, ADC SDX, or Citrix Gateway). On successful detection of the instance, it is added to the ADM’s database.
For Citrix SD-WAN WO instances, ADM does not detect the instance by using licensing information. It sends a NITRO request to the instance to check for the instance type and version.

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

**Note**

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

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

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

For Citrix SD-WAN WO instances, ADM adds its IP address as the SNMP manager on the instance.

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

This step might fail because of network or firewall issues.

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

**Polling overview**

**August 1, 2019**

Polling is a process, where Citrix Application Delivery Management (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, and so on from all managed ADC instances. The following are the different types of polling that occur between ADM and the managed instances:

- Instance polling
- Inventory polling
- Performance data collection
- Instance backup polling
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 30 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>
<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>
</tbody>
</table>
| Instance backup polling | Every 12 hours (by default) | Backup file of the current state of the managed ADC instances | NITRO calls, SSH, and SCP | Yes. Navigate to 
Networks > Instances > Citrix ADC. Select the instance and from the Select Action list, click Backup/Restore. |
| Configuration audit polling | Every 10 hours (by default) | Configuration changes that occur on ADC instances (for example, running vs. saved configuration) | SSH, SCP, and NITRO call | Yes. Navigate to 
Networks > Configuration Audit. On the Configuration Audit page, click Settings and configure the polling interval for Configuration Audit Polling. |
You can poll configuration audits manually and add all configuration audits of the instances immediately to Citrix ADM. To do so, navigate to **Networks > Configuration Audit** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network.

<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>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 <strong>Networks &gt; SSL Dashboard</strong>. On the SSL Dashboard page, click <strong>Settings</strong> to configure the polling interval</td>
</tr>
</tbody>
</table>
Polling type | Polling interval | Polled information | Protocol used | Polling interval configuration
--- | --- | --- | --- | ---
Entity polling | Every 30 minutes (by default) | All entities that are configured on the instances. An entity is either a policy, virtual server, service, or action attached to an ADC instance. | NITRO calls. | You can poll SSL certificates manually and add all certificates of the instances immediately to Citrix ADM. To do so, navigate to **Networks > SSL Dashboard** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network. Yes, but cannot be set to less than 10 minutes. To configure, navigate to **Networks > Network Functions**. On the Networks Function page, click **Settings** to configure the polling interval.
You can poll entities manually and add all entities of the instances immediately to Citrix ADM. To do so, navigate to Networks > 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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 30 minutes, you can set the interval depending on your requirements by navigating to Networks > 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 NetScaler 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 Networks > 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 a particular instance. For example, you can use this option to know the latest status of a particular entity in an instance. In such a case, you need not poll the instance as a whole to know the status of one updated entity. When you select and poll an entity, NCitrix ADM polls only that entity and updates the status in the Citrix ADM GUI.

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

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

**Note**

If you poll a virtual server, only that virtual server is polled. The associated entities such as 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 **Networks > Network Functions > Load Balancing > Virtual Servers**.
2. Select the virtual server that shows the state as DOWN, and click **Poll Now**. The status of the virtual server now changes to UP.
Data governance

August 1, 2019

Customer authentication is of vital importance to an organization because it enables the organization to protect its network resources by permitting only authenticated customers or users to access its network. As an admin, it is important that you identify your users before you let them connect to the resources in the Citrix network.

From 12.1 release 50.x build onwards, Citrix Application Delivery Management (ADM) requires that you authenticate yourself on the ADM GUI before you begin accessing the information. It is a requirement that you must register yourself on Citrix cloud services before you authenticate yourself on ADM. You must provide the Citrix cloud user credentials on ADM GUI. For more info, see Sign up for Citrix Cloud.

There are different ways to authenticate yourself on Citrix ADM. The following sections describe the workflows if you are a new user or an existing user on ADM.

Workflow if you are a new user

1. Complete the installation of Citrix ADM on the selected hypervisor.
2. Configure the various required IP addresses.
3. In a web browser, type the IP address of the Citrix ADM.
4. In the User Name and Password fields, enter the administrator credentials.
5. The Configure Customer Identity page opens where you must identify yourself with your Citrix cloud credentials.
   If you haven’t created an account on Citrix cloud, click Citrix Cloud to register.
6. Click Authenticate and provide your email address which you have used to register on Citrix cloud.
7. Select the check box next to “I agree to share data for telemetry” and click Submit.

Workflow if you are an existing user upgrading to 12.1 release latest version

1. After upgrading Citrix ADM to the latest version in 12.1 release, in a web browser, type the IP address of the Citrix ADM.
2. In the User Name and Password fields, enter the administrator credentials. The default administrator credentials are nsroot/nsroot.
3. The Configure Customer Identity page opens where you must identify yourself with your Citrix cloud credentials.
   If you haven’t created an account on Citrix cloud, click Citrix Cloud to register.
4. Click Authenticate and provide your email address which you have used to register on Citrix cloud.
5. Select the check box next to “I agree to share data for telemetry” and click Submit.

As an existing user, you can also configure your identity on ADM at a later time in one of the following two ways:

   • by navigating to System > System Administration, and click Authentication.
   • by clicking the cloud symbol at the top right side of the ADM GUI. After successful authentication, the “X” turns into a green colored check mark.

**Note**
Ensure that the following domains are whitelisted:

   • *.citrixnetworkapi.net
   • *.blob.core.windows.net

By uploading your data to Citrix ADM and by using the features of Citrix ADM, you agree and consent that Citrix may collect, store, transmit, maintain, process and use technical, user, or related information about your Citrix products and services.

At all times, information received by Citrix will be treated in accordance with [Citrix.com Privacy Policy](#).

**Licensing**

August 1, 2019

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

You can manage and monitor any number of instances and entities without a license. However, you can only manage 30 discovered applications on the App Dashboard and view analytics data for only 30 virtual servers without applying a license. To manage more than 30 discovered applications or to view analytics for more than 30 virtual servers, you must purchase and apply licenses.
<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>[FREE] Citrix ADM License is not required irrespective of the virtual server count</th>
<th>Citrix ADM License is Required for &gt; 30 virtual servers</th>
<th>Citrix ADC License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics</td>
<td>Web Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>HDX Insight*</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Security Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SSL Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Gateway Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>TCP Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Video Insight</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>WAN Insight</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Applications
<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>Citrix ADM License is not required irrespective of the virtual server count</th>
<th>Citrix ADM License is Required for &gt; 30 virtual servers</th>
<th>Citrix ADC License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Statistics (App Dashboard, App Security Dashboard)</td>
<td>No</td>
<td>Yes</td>
<td>Citrix ADC Web App Firewall related information on App dashboard and app security dashboard needs Platinum (or) Enterprise with App Firewall license.</td>
</tr>
<tr>
<td>Stylebooks</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License Server</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Inventory Management – Infrastructure Dashboard, Instance groups, Instance Dashboard and Sites</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Event Management &amp; Syslog</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Configuration Jobs, Configuration Audit &amp; Configuration Advice</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Citrix ADM Feature</td>
<td>[FREE] Citrix ADM License is not required irrespective of the virtual server count</td>
<td>Citrix ADM License is Required for &gt; 30 virtual servers</td>
<td>Citrix ADC License Requirement</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Network Reporting (instance level)</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Network Reporting (virtual server level)</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Network Functions (visibility &amp; management of virtual servers, services, service groups, server)</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>SSL Certificate Management, Monitoring, and Dashboard (instance level)</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>SSL Certificate Dashboard (virtual server level)</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**System**

<table>
<thead>
<tr>
<th>System</th>
<th>RBAC &amp; External Authentication (instance level)</th>
<th>Yes</th>
<th>No</th>
<th>Not Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RBAC &amp; External Authentication</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Orchestration
<table>
<thead>
<tr>
<th>Citrix ADM Feature</th>
<th>[FREE] Citrix ADM License is not required irrespective of the virtual server count</th>
<th>Citrix ADM License is Required for &gt; 30 virtual servers</th>
<th>Citrix ADC License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Integration</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>VMware NSX Integration</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Cisco APIC Integration</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Container Integration</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Third Party Load Balancers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAPProxy: Visibility across host/instance/backend/servers/frontend, Download or upload configuration, and Restarting appliance.</td>
<td>Yes</td>
<td>No</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>App Dashboard</td>
<td>No</td>
<td>Yes (requires a separate license)</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

*For Citrix Director integration with Citrix ADM support – Citrix Director should have platinum license.
Licenses for additional virtual servers are available in virtual server packs of 100. You can obtain a valid license and add the licenses on the Citrix ADM servers through the Citrix ADM GUI.
High Availability

Licenses are locked to the instances and you have to use a specific appliance’s IP address (active node’s) for license-related operations on a high availability pair. When licensing, apply licenses on active node, that will be in charge of licensing, and apply all future licenses on that instance. You can delete licenses only from the node on which you have installed the licenses.

When fail-over occurs, the new active node maintains the licensing for a grace period of 30 days.

Note

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

Orchestration

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

Upgrade the virtual server licenses

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

To upgrade your appliance licenses:

1. Log on to Citrix ADM using the administrator credentials.
2. Navigate to Networks > Licenses > Settings.
3. In the details pane, go to License Files, and select one of the following options:
   - **Upload license files from a local computer.** If a license is already present on your local computer, click Browse and select the license file (.lic) that you want to use to allocate your licenses. Click Finish.
   - **Use License Activation Code.** Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box and then click Get Licenses.
4. You can add more licenses from the License Settings page at any time.

Verification

You can verify the licenses installed on your Citrix ADM by navigating to Networks > Licenses > System Licenses.

License the virtual servers

You can select the virtual servers to manage and monitor through Citrix ADM. If the total number of virtual servers hosted by the discovered Citrix ADC instances is lower than the number of installed virtual server licenses, Citrix ADM licenses all the virtual servers.

You can select the 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.

• Citrix ADM does not license the non-addressable virtual servers. To manage them, you need to manually license them.

**To manage the licensed virtual servers:**

1. Log on to Citrix ADM using the administrator credentials.

2. Navigate to **Networks > Licenses > System Licenses**.
   
   The System License dashboard is displayed.

3. Under **Licensed Virtual Servers**, disable **Auto-select Virtual servers** and click the **Click to select** option.

4. In the **License Virtual Server** screen, select the type of virtual servers by clicking the relevant tab.

5. From the **Unlicensed** tab, select the virtual servers that you want to license and click **License**. From the **Licensed** tab, select the virtual servers that you want to unlicense and click **Unlicense**.

6. Click **Next** to move to the other virtual servers’ tab, or click **Save and Exit** to license the selected virtual servers.
Configure auto license support for non-addressable virtual servers

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 a new option under Networks > Licenses > System Licenses. That is, the new option Auto-select nonaddressable Virtual Servers. Enabling this option now allows you to explicitly specify that the licensing must include non-addressable virtual servers also.

Expiry checks for virtual server licenses

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

To view the status of the licenses:

1. Navigate to Networks > Licenses > System Licenses.
2. In the License Expiry Information section, you can find the details of the licenses that are going to expire:

   - **Feature**: Type of license that is going to expire.
   - **Count**: Number of virtual servers or instances that are affected.
• **Days to expiry:** Number of days remaining before expiry.

**To configure the notification settings of licenses:**

1. Navigate to **Networks > Licenses > Settings.**

2. In the **Notification Settings** section, click the pencil icon and edit the parameters.

   - **Email profile:** Email profile or distribution list for sending notifications when licenses reach threshold, or going to expire.
   
   - **SMS Profile:** SMS profile or distribution list for sending notifications when licenses reach threshold, or going to expire.
   
   - **Alert Threshold:** Set percentage of pooled licenses to notify administrators by Email or SMS.
   
   - **License Expiry Threshold:** Number of days before the number of licenses determined by Alert Threshold expire.
   
   - **Days to expiry:** Number of days remaining before expiry.

---

**System requirements**

August 1, 2019

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

**Requirements for Citrix ADM**

<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 CPUs</td>
</tr>
</tbody>
</table>

**Note:** Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments.
### Component Requirement

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage space</td>
<td>The default value is 120 GB. Actual storage requirement depends on Citrix ADM sizing estimation. Use the sizing calculator mentioned in the section <strong>Maximum limits</strong> in the Citrix ADM HA Deployment Guide. This guide is available at our download site, under NetScaler MAS Release 12.1. <strong>Note:</strong> you need a Citrix account to access the deployment guide and sizing calculator. If your Citrix ADM storage requirement exceeds 120 GB, you have to attach an additional disk. You can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see <a href="#">How to Attach an Additional Disk to Citrix ADM</a>.</td>
</tr>
<tr>
<td>Virtual network interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

### Requirements for Citrix ADM on-prem agent

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>2 CPUs</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
</tr>
<tr>
<td>Storage space</td>
<td>30 GB</td>
</tr>
<tr>
<td>Virtual network interfaces</td>
<td>1</td>
</tr>
</tbody>
</table>
Component Requirement

| Throughput       | 1 Gbps |

**Minimum Citrix ADC versions required for Citrix ADM features**

**Important**

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

<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>OpenStack/CloudStack Support</td>
<td>11.0 and later, if a partition is required</td>
</tr>
<tr>
<td></td>
<td>11.1 and later, if partition on shared virtual LAN is required</td>
</tr>
<tr>
<td>NSX Support</td>
<td>11.1 Build 47.14 and later (VPX)</td>
</tr>
<tr>
<td>Mesos/Marathon Support</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>Backup/Restore</td>
<td>For Citrix ADC, 10.1 and later</td>
</tr>
<tr>
<td></td>
<td>For Citrix SDX, 11.0 and later</td>
</tr>
<tr>
<td>Monitoring/Reporting and Configuration using Jobs</td>
<td>10.1 and later</td>
</tr>
<tr>
<td><strong>Analytics Features</strong></td>
<td></td>
</tr>
<tr>
<td>Web Insight</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>10.1 and later</td>
</tr>
<tr>
<td>Security Insight</td>
<td>11.0.65.31 and later</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>11.0.65.31 and later</td>
</tr>
<tr>
<td>Cache Insight</td>
<td>10.5 and later*</td>
</tr>
<tr>
<td>SSL Insight</td>
<td>12.0 and later</td>
</tr>
</tbody>
</table>

* Integrated Cache Metrics are not supported in Citrix ADM with Citrix ADC instances running version 11.0 build 66.x.
Requirements for Citrix SD-WAN instance management

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

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>Citrix SD-WAN WANOP</th>
<th>Citrix SD-WAN SE</th>
<th>Citrix SD-WAN EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reporting (Network Reports)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Event Management</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HDX Insight (Multi-hop Deployment)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</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
- Dell Wyse Zx0 Z90D7 (WES7) Thin Client

Requirements for Citrix ADM analytics

Minimum Citrix Virtual Apps and Desktops versions required for Citrix ADM features
Citrix ADM can generate reports for applications that are published on Citrix Virtual Apps or Citrix Virtual Desktops and accessed through Citrix Receiver. However, this capability depends on the operating system on which 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**

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

**Citrix ADC instance license required for HDX insight**

The data collected by Citrix ADM for HDX Insight depends on the version and licenses of the Citrix ADC instances being monitored. HDX Insight reports are displayed only for Citrix ADC Platinum and Enterprise appliances running release 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>&gt; 1 Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Supported hypervisors

The following table lists the hypervisors supported by Citrix ADM.

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Hypervisor</td>
<td>7.1 and 7.4</td>
</tr>
<tr>
<td>VMware ESX</td>
<td>6.0, 6.5, and 6.7</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012 R2 and 2016</td>
</tr>
<tr>
<td>Generic KVM</td>
<td>RHEL 7.4 and Ubuntu 16.04</td>
</tr>
</tbody>
</table>

Supported operating systems and 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 Citrix CloudBridge (Citrix SD-WAN WANOP) release 7.4 and later.

Supported browsers

The following table lists the web browsers supported by Citrix ADM:
Citrix Application Delivery Management 12.1

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>11.0 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Chrome 19 and later</td>
</tr>
<tr>
<td>Safari</td>
<td>Safari 5.1.1 and later</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Firefox 3.6.25 and later</td>
</tr>
</tbody>
</table>

**Supported ports**

Citrix ADM uses the Citrix ADC’s NetScaler IP (NSIP) address to communicate with the ADC. For communication purposes, the following ports must be open between the Citrix ADC and/or SD-WAN instances and Citrix ADM.

**Note**

If you have configured Citrix ADCs in High Availability mode, Citrix ADM uses the Citrix ADC’s subnet IP (Management SNIP) address to communicate with Citrix ADC. For communication using SNIP with Citrix ADM, the following ports remain the same.

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80/443</td>
<td>For NITRO communication from Citrix ADM to Citrix ADC or Citrix SD-WAN instance. 443. For NITRO communication between Citrix ADM servers in high availability mode.</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>For SSH communication from Citrix ADM to Citrix ADC or Citrix SD-WAN instance. For synchronization between Citrix ADM servers deployed in high availability mode.</td>
</tr>
<tr>
<td>UDP</td>
<td>4739</td>
<td>For AppFlow communication from Citrix ADC or Citrix SD-WAN instance to Citrix ADM.</td>
</tr>
<tr>
<td>Type</td>
<td>Port</td>
<td>Details</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICMP</td>
<td>No reserved port</td>
<td>To detect network reachability between Citrix ADM and Citrix ADC instances, SD WAN instances, or the secondary Citrix ADM server deployed in high availability mode.</td>
</tr>
<tr>
<td>UDP</td>
<td>161, 162</td>
<td>To receive SNMP events from Citrix ADC instance to Citrix ADM.</td>
</tr>
<tr>
<td>UDP</td>
<td>514</td>
<td>To receive syslog messages in Citrix ADM from Citrix ADC or Citrix SD-WAN instance.</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>To send SMTP notifications from Citrix ADM to users.</td>
</tr>
<tr>
<td>TCP</td>
<td>389/636</td>
<td>Default port for authentication protocol. For communication between Citrix ADM and LDAP external authentication server.</td>
</tr>
<tr>
<td>UDP</td>
<td>123</td>
<td>Default NTP server port for, synchronizing with multiple time sources.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
<td>Default port for authentication protocol. For communication between Citrix ADM and RADIUS external authentication server.</td>
</tr>
<tr>
<td>TACACS</td>
<td>49</td>
<td>Default port for authentication protocol. For communication between Citrix ADM and TACACS external authentication server.</td>
</tr>
<tr>
<td>Type</td>
<td>Port</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>5557, 5558</td>
<td>For logstream communication (for security insight, web insight, and HDX insight) from Citrix ADC to Citrix ADM.</td>
</tr>
<tr>
<td>TCP</td>
<td>5454</td>
<td>Default port for communication, and database synchronization in between Citrix ADM nodes in high availability mode.</td>
</tr>
<tr>
<td>TCP</td>
<td>27000</td>
<td>License port for communication between Citrix ADM license server and CPX instance.</td>
</tr>
<tr>
<td>TCP</td>
<td>7279</td>
<td>Citrix vendor daemon port.</td>
</tr>
</tbody>
</table>

**Limitations**

In 12.1 Citrix ADM, the following features support IPv6 format of IP addresses:

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

The following features do not support IPv6:
1. High availability floating IP
2. Syslogs received from ADCs that support IPv6
3. StyleBooks on ADCs that support IPv6
4. Analytics
5. Pooled licensing

**Get started**

August 1, 2019

This document walks you through how to get started with deploying and setting up Citrix Application Delivery Management (ADM) for the first time. This document is intended for network and application administrators who manages Citrix network devices (Citrix SD-WAN WO, Citrix Gateway, and so on) and also third-party devices such as HAProxy. You must follow the steps in this document irrespective of the type of device you plan to manage using Citrix ADM.

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

**Step 1 - Review the system requirements**

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

- **License information.** You can manage and monitor any number of instances and entities without a license. However, you can only manage 30 discovered apps and view analytics information for only 30 virtual servers without applying a license. To manage more than 30 apps or to view analytics for more than 30 virtual servers, you must purchase appropriate licenses. Learn More.

- **Operating system and receiver requirements.** Review this information to make sure you have the correct receiver version for the supported operating systems. Learn More.

- **Browser requirements.** To access Citrix ADM GUI, you must make sure you have the required browser and the correct version. Learn More.

- **Ports.** Ensure the required ports are open for Citrix ADM to communicate with Citrix ADC and/or SD-WAN instances. Learn More.
Citrix ADC instance requirements. Different Citrix ADM features are supported on different Citrix ADC software versions. Review this information to make sure you have upgraded your Citrix ADC instances to the correct version. Learn More.

Citrix SD-WAN instance requirements. Review this information to make sure you have upgraded your Citrix SD-WAN instances to the correct version and you have the correct platform editions. Learn More.

Step 2 - Deploy Citrix ADM

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

• Single-server deployment. In a Citrix ADM single server deployment, the database is integrated with the server and a single server processes all the traffic. You can deploy Citrix ADM with Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V, and Linux KVM. See:
  – Citrix ADM with Citrix Hypervisor
  – Citrix ADM with Microsoft Hyper-V
  – Citrix ADM with VMware ESXi
  – Citrix ADM with Linux KVM server

• High availability deployment. A high availability deployment (HA) of two Citrix ADM servers provides uninterrupted operations. In a high availability setup, both the Citrix ADM nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have same configurations. With HA deployment the ability to configure the floating IP address on the Citrix ADM primary node eliminates the need of separate Citrix ADC load balancer. To learn more, see Configure in high availability deployment.

Step 3 - Add instances to Citrix ADM

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

• Citrix ADC ADC
  – Citrix ADC MPX
When you add an instance to the Citrix ADM server, the server implicitly communicates with the instances and collects inventory of these instances.

**Step 4 - Enable analytics on virtual servers**

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

**Step 5 - Configure NTP server on Citrix ADM**

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

**Step 6 - Configure system settings for optimal Citrix ADM performance**

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

- **Configure system alarms.** You should configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server.

- **Configure system notifications.** You can send notifications to select groups of users for a number of system-related functions. You can set up a notification server in Citrix ADM, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. This ensures that you are notified of any system-level activities such as user login or system restart.
• **Configure system prune settings.** To limit the amount of reporting data being stored in your Citrix ADM server’s database, you can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

• **Configure system backup settings.** Citrix ADM automatically backs up the system everyday at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system.

• **Configure instance backup settings.** If you back up the current state of a Citrix ADC instance, you can use the backup files to restore stability in the event that the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.

• **Configure instance event prune settings.** To limit the amount of event messages data being stored in your Citrix ADM server’s database, you can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).

• **Configure instance syslog purge settings.** To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the following syslog data will be deleted from Citrix ADM:
  - Generic Syslog data
  - AppFirewall data
  - Citrix Gateway data.

**What’s next**

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

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

**Managing Citrix ADC SD-WAN instances.** Not all Citrix ADM features are supported on SD-WAN WO instances, for example, certificate management or configuration audit are not supported. To learn about what features are supported and how to use them, see Managing Citrix SD-WAN WO Using Citrix ADM.

**Managing HAProxy instances and applications.** You can monitor the frontends, backends, and servers configured in an HAProxy deployment. You can also use the Application Management feature...
to monitor real-time statistics of the frontends monitored by Citrix ADM. To learn about what features are supported for HAProxy and how to use them, see Managing and Monitoring HAProxy Instances Using Citrix ADM.

Deploy

August 1, 2019

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

- **Single-Server Deployment.** In a Citrix ADM single server deployment, the database is integrated with the server and a single server processes all the traffic. You can deploy Citrix ADM with Citrix Hypervisor, VMWare ESXi, Microsoft Hyper-V, and Linux KVM. See:
  - Citrix ADM with Citrix Hypervisor
  - Citrix ADM with Microsoft Hyper-V
  - Citrix ADM with VMware ESXi
  - Citrix ADM with Linux KVM server

- **High Availability (HA) Deployment.** An HA deployment of two Citrix Citrix ADM servers provides uninterrupted operations. In a high availability setup, both the Citrix ADM nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have same configurations. With HA deployment the ability to configure the floating IP address on the Citrix ADM primary node eliminates the need of separate NetScaler load balancer. See: Configure in high availability deployment.

- **Migrate from NetScaler Insight Center to Citrix ADM.** You can migrate your NetScaler Insight Center deployment to Citrix ADM without losing the existing configuration, settings, or data. With Citrix ADM you can not only view the various analytics generated by the NetScaler and NetScaler SD-WAN instances, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console. See: Migrating from NetScaler Insight Center to Citrix ADM

- **Integrate Citrix ADM with Director.** Director integrates with Citrix ADM for network analysis and performance management. See: Integrate Citrix ADM with Director
Prerequisites for installing Citrix ADM

August 1, 2019

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

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

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

General requirements for Citrix ADM release 12.1

<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 CPUs</td>
</tr>
<tr>
<td>Storage space</td>
<td>Citrix recommends using solidstate drive (SSD) technology for Citrix ADM deployments.</td>
</tr>
<tr>
<td></td>
<td>The default storage space required is 120 GB. Actual storage requirement depends on Citrix ADM sizing estimation.</td>
</tr>
<tr>
<td></td>
<td>If your Citrix ADM storage requirement exceeds 120 GB, you have to attach an additional disk.</td>
</tr>
<tr>
<td></td>
<td>Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. You can add only one additional disk.</td>
</tr>
<tr>
<td></td>
<td>For more information, see How to Attach an Additional Disk to Citrix ADM.</td>
</tr>
<tr>
<td>Virtual network interfaces</td>
<td>1</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management 12.1

Component Requirement

Throughput 1 Gbps

Note:
Citrix recommends you to host the Citrix ADM VHD on a local storage. Citrix ADM software requires a minimum of 4000 IOPS for satisfactory operation when hosted on storage area network (SAN).

Citrix ADM with Citrix Hypervisor

August 1, 2019

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

Prerequisites

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

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

XenCenter system requirements

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows 7, Windows Server 2003, or Windows 10</td>
</tr>
<tr>
<td>.NET framework</td>
<td>Version 2.0 or later</td>
</tr>
</tbody>
</table>
## Component Requirement

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>750 megahertz (MHz), Recommended: 1 gigahertz (GHz) or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB, Recommended: 2 GB</td>
</tr>
<tr>
<td>Network Interface Card</td>
<td>100 megabits per second (Mbps) or faster NIC</td>
</tr>
</tbody>
</table>

### Install Citrix Application Delivery Management

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

2. After specifying the required IP addresses, save the configuration settings.

3. When prompted, log on using nsrecover/nsroot credentials.

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

5. Select the deployment type as **Citrix ADM Server**. If you do not select any option, by default, it is deployed as a server.
6. Type Yes to deploy Citrix ADM as a standalone deployment.

7. Type Yes to restart the Citrix ADM server.

Note

After you install Citrix ADM, you can update the initial configuration settings later.

To update the network configuration in Citrix ADM, type `networkconfig` in the Citrix ADM console. The console displays the Citrix ADM network configuration options. You can then update the following parameters on the console:

- Host name of Citrix ADM
- Citrix ADM IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address

**Verification**

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

The browser displays the Citrix ADM configuration utility.

**Citrix ADM with Microsoft Hyper-V**

August 1, 2019
To install Citrix ADM on Microsoft Hyper-V, you must first download the Citrix ADM image file to your local computer. Also, ensure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available.

**Prerequisites**

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

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

**Microsoft Hyper-V system requirements**

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>.NET framework</td>
<td>Version 2.0 or later</td>
</tr>
<tr>
<td>CPU</td>
<td>750 megahertz (MHz), Recommended: 1 gigahertz (GHz) or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB, Recommended: 2 GB</td>
</tr>
<tr>
<td>Network Interface Card</td>
<td>100 megabits per second (Mbps) or faster NIC</td>
</tr>
</tbody>
</table>

**Installing Citrix Application Delivery Management**

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

**To install Citrix ADM:**

1. Start Hyper-V Manager client on your workstation.
2. On the **Action** menu, click **Import Virtual Machine**.
3. Import the Hyper-V image, and do the following:

   a) In the Import Virtual Machine dialog box, in **Locate Folder** section, browse to the folder in which you saved the Citrix ADM Hyper-V image, select the folder, and click **Next**.

   b) In the Select virtual machine section, select the appropriate virtual machine name.

   c) In the **Choose Import Type** section, select Copy the virtual machine (create a new unique ID) option and click Next.

   d) In the **Choose Destination** section, you can specify the folders to store the virtual machine files.

   **Note**

   By default the wizard imports the virtual machine files to default Hyper-V folders on your local host.
e) In the Choose Storage Folders section, you can select the location in which you want to store the virtual hard disks, and then click Next.

f) You can verify the Virtual Machine details in the summary pane, click Finish.
The Citrix ADM Hyper-V image is displayed in the right pane.

4. Right-click the Citrix ADM Hyper-V image, and then click **Settings**.

5. In the left pane of the dialog box that appears, navigate to **Hardware > VM_Bus Network Adapter**, and in the right pane, from the Network drop-down list, select the appropriate network.
6. Click **Apply**, and then click **OK**.

7. Right-click the Citrix ADM Hyper-V image and click **Connect**.

8. On the Console window, click **Start** button.

9. Configure the initial network configuration options.

10. After specifying the required IP addresses, save the configuration settings.

11. When prompted, logon using nsrecover/nsroot credentials.
12. Execute the deployment script by typing the command at the shell prompt:

```
$ deployment_type.py
```

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

14. Type **Yes** to deploy Citrix ADM as a standalone deployment.

15. Type **Yes** to restart the Citrix ADM server.

**Note**

After you install Citrix ADM, you can update the initial configuration settings at a later time.

To update the initial configuration in the Citrix ADM, type `networkconfig` in the Citrix ADM console. The console displays the Citrix ADM initial network configuration options. You can then update the following parameters on the console:

- Host name of Citrix ADM
- Citrix ADM IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address

**Verification**

After the server is installed, you can access the graphical user interface (GUI) by typing the IP address of the Citrix ADM server in the address bar of your browser. The default administrator credentials to
log on to the server are nsroot/nsroot.
The browser displays the Citrix ADM configuration utility.

Citrix ADM with VMware ESXi

August 1, 2019

To install Citrix ADM virtual appliances on VMware ESXi, use VMware vSphere client.

Prerequisites

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

• Install VMware ESXi version 4.1 or later hardware that meets the minimum requirements.
• Install VMware Client on a management workstation that meets the minimum system requirements.
• Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
• Download the Citrix ADM setup files.

Note
VMotion is not supported on Citrix ADM.

To install Citrix ADM

1. Start the VMware vSphere client on your workstation.
2. In the IP address / Name text box, type the IP address of the VMware ESXi server that you want to connect to.
3. In the User Name and Password text boxes, type the administrator credentials, and then click Login.
4. On the File menu, click Deploy OVF Template.
5. In the Deploy OVF Template dialog box, in Deploy from a file or URL, select the .ovf file, and click Next.
6. On the **OVF Template Details** page, click **Next**.

7. Type a name for the Citrix ADM virtual appliance, and then click **Next**.

8. Specify the Disk Format by selecting either Thin provisioned format or Thick provisioned format. **Note**
   
   Citrix recommends that you select **Thick provisioned format**.

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

10. You are now ready to start the Citrix ADM virtual appliance.

11. In the navigation pane, select the virtual appliance that you installed. From the **Inventory**
menu, right-click on the **Virtual Machine**, and then click **Upgrade Virtual Hardware**. In the **Confirm Virtual Machine** dialog box, click **Yes**.

12. In the **Inventory** menu, click **Virtual Machine**, and then click **Edit Settings**.

13. In the **Virtual Machine Properties** dialog box, on the **Hardware** tab, click **Memory**, and then in the right pane specify the **Memory Size** as 32 GB.

14. Click **CPUs**, and then in the right pane, specify the CPUs as 8. Click **OK**.

15. Add an additional disk as per your requirement.
16. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, click **Virtual Machine**, click **Power**, and then click **Power On**.

17. Click the **Console** tab to display the Citrix ADM Initial Network Configuration options.

18. After specifying the required IP addresses, save the configuration settings.

19. When prompted, log on using nsrecover/nsroot credentials.
20. Execute the deployment script by typing the command at the shell prompt:

```bash
$ deployment_type.py
```

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

22. Type **Yes** to deploy Citrix ADM as a standalone deployment.

23. Type **Yes** to restart the Citrix ADM server.

**Note**

After you install Citrix ADM, you can update the initial configuration settings later.

To update the initial configuration in the Citrix ADM, type `networkconfig` in the Citrix ADM console. The console displays the Citrix ADM initial network configuration options. You can then update the following parameters on the console:

- Host name of Citrix ADM
- Citrix ADM IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address
**Verification**

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

The browser displays the Citrix ADM configuration utility.

---

**Note**

When deployed on VMware ESXi, Citrix ADM might take up to 30 minutes or more to come up.

---

**Citrix ADM with Linux KVM server**

August 1, 2019

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

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

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

---

**Prerequisites**

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

---

**Hardware requirements**
Component | Requirement
--- | ---
CPU | A 64-bit x86 processor with the hardware virtualization features that are included in the AMD-V and Intel VT-X processors. Provide at least 2 CPU cores to host Linux-KVM. **Note** To test whether your CPU supports Linux host, enter the following command at the host Linux shell prompt: `egrep '^flags.* ( vmx | svm )' /proc/cpuinfo` If the BIOS settings for the above extension are disabled, you must enable them in BIOS. There is no specific recommendation for processor speed, but higher the speed, better is the performance of the Citrix ADM.

Memory (RAM) | Minimum 4 GB for the host Linux kernel. Add additional memory as required by the VMs.

Hard Disk | Calculate the space for Host Linux kernel and VM requirements. A single Citrix ADM VM requires 120 GB of disk space.

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

**Software requirements**

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

**Network requirements**

Citrix ADM supports only one virtIO para-virtualized network interface. This interface should be connected to the management network of the Linux-KVM host, so that the Citrix ADM and Linux-KVM can communicate.
Download Citrix ADM setup files

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

1. Open a web browser and type www.citrix.com in the address bar.
2. Hover over the Sign In option and click My Account, enter your Citrix credentials, and then again click Sign In.
3. Navigate to Downloads section.
4. From the Downloads drop-down list, select Citrix Application Delivery Management.
5. On the Citrix Application Delivery Management page, select the release. For example, select Release 12.1.
6. Click Product Software to expand it, and click the latest build. For example, select Citrix ADM Release (Feature Phase) 12.1 Build 49.23/49.37.
   The selected build page is displayed.
7. On the Jump to Download drop-down list, select Citrix ADM image for KVM, 12.1 Build xx.xx
8. Click Download File, accept the end-user license agreement, and download the compressed image file to any folder on your local machine.

Install the Citrix Application Delivery Management on Linux-KVM

1. Using SSH, log on to the KVM host.
2. At the CLI prompt, by using any of the file transfer programs, copy the image to a folder on the server.
3. Navigate to the directory where you have saved the downloaded image.
4. Perform these at the command line:
   a) List the files in the directory verify the presence of the image file.
   b) Use the tar command to untar the Citrix Application Delivery Management image file. The unzipped package contains the following components:
      i. A domain XML file that specifies the Citrix ADM attributes
      ii. A text file that specifies the check sum of the domain disk image
      iii. A domain disk image

```
1  tar -xvfz MAS-KVM.tgz
2  MAS-KVM.xml
3  MAS-KVM.qcow2
4  checksum.txt
```
iv. Create a copy of MAS-KVM.xml as MAS1-KVM.xml, as a back-up option. Open the MAS1-KVM.xml file by using the vi editor.

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

A. name - Specify the name.
B. mac - Specify the MAC address.
C. source file - Specify the absolute disk-image source path. The file path has to be absolute.

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

D. mode - Specify the mode.
E. model type - Set to virtIO.
F. source dev - Specify the interface.

vi. Define the VM attributes in the MAS1-KVM.xml file by using the following command:

```
virsh define <FileName>.xml
```

```
1 virsh define MAS-KVM.xml
2 Domain MAS defined from MAS-KVM.xml
```

Start the Citrix ADM by entering the following command:
```
virsh start [<DomainName>] <DomainUUID>]
```
vii. You can connect to the Citrix ADM virtual machine by using the following command: 
\texttt{virsh console <DomainName>}

```bash
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
```

Configure the Citrix Application Delivery Management

\textbf{Note}

On some Linux KVM hosts, FreeBSD guests fail to restart properly if they have more than one CPU. When The Citrix ADM virtual appliance is restarted, the Citrix ADM CLI and GUI become unresponsive. For details, see [https://bugs.launchpad.net/qemu/+bug/1329956](https://bugs.launchpad.net/qemu/+bug/1329956)

To avoid the Citrix ADM CLI and GUI from becoming unresponsive when the Citrix ADM virtual appliance is restarted, shut down all the virtual machines on the KVM host, and perform the following on the KVM host:

1. Remove the \texttt{kvm\_intel} module using the following command:
   \texttt{rmmod \text{\texttt{kvm\_intel}}}
2. Disable APICv and reload \texttt{kvm\_intel} module using the following command:
   \texttt{modprobe \text{\texttt{kvm\_intel enable\_apicv}=N}}
3. Start the virtual machines on the KVM host.

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

1. At the command line, use the default system administrator credentials to log on to the system:
   - Username: \texttt{nsroot}
• Password: nsroot

Note

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

2. At the prompt, type: shell

3. Type networkconfig to enter the Citrix ADM initial network configuration menu. Configure the management IP address.

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

5. Execute the deployment script by typing the command at the shell prompt: deployment_type.py

6. In the deployment screen that appears, select the deployment type as Citrix ADM server.
7. Type **Yes** to deploy Citrix ADM as a standalone deployment.

8. Type **Yes** to restart the Citrix ADM server.

9. After Citrix ADM server restarts, log on to Citrix ADM by using the default administrator credentials as nsroot/nsroot through the command line or the GUI.

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

---

**Configure high availability deployment**

August 1, 2019

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

The validated maximum storage limit for a single Citrix ADM HA deployment is 3 TB. For more information, see the deployment guide.

**Important**

To access Citrix ADM 12.1 build 48.18 or later versions using HTTPS:
If you have configured a Citrix ADC instance to load balance Citrix ADM in a high availability mode, first remove the Citrix ADC instance. Then, configure a floating IP address to access Citrix ADM in high availability mode.

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

- An improved mechanism to monitor heartbeats between the primary and secondary node.
- Provides physical streaming replication of database instead of a logical bi-directional replication.
- Ability to configure the floating IP address on the primary node to eliminate the need of separate Citrix ADC load balancer.
- Provides easy access to the Citrix ADM user interface using the floating IP address.
- Citrix ADM user interface is provided only on the primary node. By using the primary node, you can eliminate the risk of accessing and making changes to the secondary node.
- Configuring the floating IP address handles the failover situation and reconfiguring the instances is not required.
- Provides built in ability to detect and handle split-brain situation.

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

<table>
<thead>
<tr>
<th>Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary node</td>
<td>First node registered in the high availability deployment.</td>
</tr>
<tr>
<td>Secondary node</td>
<td>Second node registered in the high availability deployment.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>A mechanism used to exchange messages between primary and secondary node in the high availability setup. The messages determine status and health of the application on each individual node.</td>
</tr>
</tbody>
</table>
Floating IP address

A floating IP is an IP address that can be instantly moved from one node to another in the same subnet. Internally it is set up as an alias on the network interface of the primary node. If there is a failover, the floating IP address is seamlessly moved from the old primary to the new one. It is useful in high availability setup because it allows clients to communicate with the high availability nodes using a single IP address.

Components of high availability architecture

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

Note

For more information on port and protocol details, see Ports.
In high availability deployment, one Citrix ADM node is configured as the primary node (MAS 1) and the other as the secondary node (MAS 2). If the primary node goes down due to any reason, the secondary node takes over as the new primary node.

**Monitoring tool**

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

**Primary node**

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

**Secondary node**

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

**Physical streaming replication**

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

**Heartbeat messages**

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

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

Key points to note

- In a high availability setup, both the Citrix ADM nodes are deployed in active-passive mode. They must be on the same subnets using the same software version and build, and have same configurations.
- Floating IP address:
  - Floating IP address is configured on the primary node.
  - Instances need not be reconfigured if there is a failover.
  - You can access a high availability node from the user interface, either by using the primary node IP or floating IP address.

  Note

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

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

- Citrix ADM upgrade:
  - Internal processes implicitly upgrades Citrix ADM from the earlier versions.

  Note

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

- UDP default port 5005 is available on both the nodes for heartbeats to be sent and for messages to be received.

- MAC address
  The setting for the “MAC Address Changes” option in a hypervisor affects the traffic that a virtual
machine receives. Allow MAC address changes to be enabled on the virtual switch so that the floating IP address moves seamlessly to the new primary node after failover. For example, when deploying Citrix ADM on a high availability on VMware ESXi, make sure you accept changes to MAC address. ESXi now allows requests to change the active MAC address to other than the initial MAC address.

Prerequisites

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

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

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

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

<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 CPUs</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management 12.1

Component Requirement

Storage Space
Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments. The default value is 120 GB. Actual storage requirement depends on Citrix ADM sizing estimation. If your Citrix ADM storage requirement exceeds 120 GB, you have to attach an additional disk. **Note** You can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to Citrix ADM.

Virtual network interfaces 1

Throughput 1 Gbps or 100 Mbps

**Hypervisor**

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Hypervisor</td>
<td>6.2 and 6.5</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5 and 6.0</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012 R2</td>
</tr>
<tr>
<td>Linux KVM</td>
<td>Ubuntu and Fedora</td>
</tr>
</tbody>
</table>

To set up Citrix ADM in high availability mode

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

**Register and deploy the first server (primary node)**

To register the first node:

1. Use the .xva image file downloaded from the Citrix download site and import it in to your hypervisor.
It might take a few minutes for the .xva image file to import and get started. You can see the status on the bottom of the screen.

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

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

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

5. To deploy the primary node, enter `/mps/deployment_type.py`. The Citrix ADM deployment configuration menu is displayed.
6. Select **1** to register Citrix ADM server as primary node.

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

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

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

**Register and deploy the second server (secondary node)**

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

2. From the Console tab, configure Citrix ADM with the initial network configurations as displayed in the following image.

3. After the initial network configuration is completed, the system prompts for login. Log on using following credentials – nsrecover/nsroot.
4. To deploy the secondary node, enter `/mps/deployment_type.py`. The Citrix ADM deployment configuration menu is displayed.

5. Select 1 to register Citrix ADM server as secondary node.

6. The console prompts you to select the Citrix ADM as standalone deployment. Enter No to confirm the deployment as high availability.

7. The console prompts you to select the first server node. Enter No to confirm the node as the second server.

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

9. The console prompts you to enter the floating IP address.
The console prompts you to restart the system. Enter Yes to restart.

Note

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

Deploy the primary and secondary node as a high availability pair

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

Note

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

To deploy nodes as a high availability pair:

1. Open a web browser and enter the IP address of the first Citrix ADM server node.
2. In the user Name and password fields, enter the administrator credentials.
3. Click Get Started in the home page.
4. Select the deployment type as Two Servers deployed in High Availability Mode, and click Next.
5. On the Deployment page, click **Deploy**.

6. A confirmation message is displayed. Click **Yes**.

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

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

7. Log on to Citrix ADM using administrator credentials, click **Get Started** in the home page, and optionally, complete the following:
a) Add Citrix ADC instances

b) Configure Customer Identity

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

8. Navigate to System > Deployment to validate the deployment.

For more information, see the Frequently Asked Questions.

Disable high availability

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

Note
Disable high availability from the primary node.

To disable the high availability:

1. In a web browser, enter the IP address of the Citrix ADM server primary node.
2. In the User Name and Password fields, enter the administrator credentials.
3. On the System tab, navigate to Deployment and click Break HA.
A dialogue box is displayed. Click **Yes** to break the high availability deployment.

**Redeploy high availability**

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

**High availability failover scenarios**

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

- **Node failure**: Primary node goes down, no heartbeat is detected from primary node for 180 seconds.

- **Application health failure**: Primary node is up and running but one of the Citrix ADM processes is down.

**Split-brain scenario**

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

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

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

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

**Note**

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

**Configure disaster recovery for high availability**

August 1, 2019

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

The Citrix ADM 12.1 disaster recovery (DR) feature provides full system backup and recovery capabilities for Citrix ADM deployed in high availability mode. At the time of recovery, certificates, configuration files, and a complete backup of the database is available in the recovery site.

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

<table>
<thead>
<tr>
<th>Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary site (Data center A)</td>
<td>The primary site has Citrix ADM nodes deployed in high availability mode.</td>
</tr>
<tr>
<td>Recovery site (Data center B)</td>
<td>The recovery site has a disaster recovery node deployed in standalone mode. This node is in read-only mode and is not operational until the primary site is down.</td>
</tr>
</tbody>
</table>
Terms |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disaster recovery node</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The recovery node is a standalone node deployed in the recovery site. This node is made operational (to the new primary) in case a disaster hits the primary site and it is non-functional.</td>
</tr>
</tbody>
</table>

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

Disaster recovery workflow

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

Initial setup before disaster

The image shows the disaster recovery setup before disaster.

The primary site has Citrix ADM nodes deployed in the high availability mode. To learn more, see *High availability deployment*. The recovery site has a standalone Citrix ADM disaster recovery node deployed remotely. The disaster recovery node is in read-only mode and receives data from the primary node to create data backup. Citrix ADC instances in the recovery site are also discovered but, they do not have any traffic flowing through them. During the backup process, all data, files, and configurations are replicated on the disaster recovery node from the primary node.
Prerequisites

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

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

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

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

<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 CPUs</td>
</tr>
<tr>
<td>Storage Space</td>
<td>Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments. The default value is 120 GB. Actual storage requirement depends on Citrix ADM sizing estimation. If your Citrix ADM storage requirement exceeds 120 GB, you have to attach an additional disk. <strong>Note</strong> You can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see <a href="#">How to Attach an Additional Disk to Citrix ADM</a>.</td>
</tr>
<tr>
<td>Virtual network interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Hypervisor Versions**

- Citrix Hypervisor: 6.2 and 6.5
- VMware ESXi: 5.5 and 6.0
- Microsoft Hyper-V: 2012 R2
First time disaster recovery setup

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

Deploy Citrix ADM in high availability mode

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

Note
- Citrix ADM deployed in high availability mode must be upgraded to Citrix ADM release version 12.1.
- Floating IP address is mandatory to register disaster recovery node with the primary node.

Deploy and register the Citrix ADM disaster recovery node

To register the Citrix ADM disaster recovery node:

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

Note
The disaster recovery node can be on a different subnet.
3. After the initial network configuration is complete, the system prompts for login. Log on using the following credentials – nsrecover/nsroot.

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

5. Select 2 to register disaster recovery node.

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

![Backup node Configuration](image1)

The disaster recovery node is now registered successfully.

![Backup node Registration successful](image2)

**Note**
The disaster recovery node does not have a GUI.

**Enable disaster recovery settings from the Citrix ADM GUI**

After the disaster recovery node is registered successfully, you can enable the disaster recovery settings from the Citrix ADM primary site user interface.

1. Navigate to **System > System Administration > Disaster Recovery Settings**.

2. On the **Configure Disaster Recovery Settings** page, select Enable Disaster Recovery check box, and click **Apply Settings**.

![Configure Disaster Recovery Settings](image3)

3. A confirmation dialogue box is displayed. Click **Yes** to continue.
Note
The time taken for system backup depends on the data size and the WAN (Wide Area Network) link speed.

To disable the disaster recovery settings, clear the Enable Disaster Recovery check box and click Apply Settings.

A confirmation dialogue box is displayed. Click Yes to continue.

Important
- It is the responsibility of the administrator to detect that a disaster has occurred on the primary site.
- The disaster recovery workflow is not automated and the administrator has to manually initiate after the primary site goes down.
- An administrator must manually initiate the process by executing a recovery script on the disaster recovery node at the recovery site.
- If you upgrade the HA pair in primary site, you must manually upgrade the standalone node in the DR site.

If you disable the Enable Disaster Recovery option and click Apply Settings, Citrix ADM does not allow you to select the Enable Disaster Recovery option again.

The following error message is displayed, when you click Disaster Recovery Settings:
To enable the DR node again, reconfigure the DR node for your high availability pair:

a) Log on to the DR node using a hypervisor or an SSH console.

b) Configure the DR node, by following the procedure available at Deploy and register the Citrix ADM disaster recovery node.

c) Enable the disaster recovery option.

For more information, see the Frequently Asked Questions.

**Workflow after the disaster**

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

1. The administrator identifies that a disaster has struck the primary site and it is not operational.
2. The administrator initiates the recovery process.
3. The administrator must manually execute the following recovery script on the disaster recovery node (at the recovery site): `/mps/scripts/pgsql/pgsql_restore_remote_backup.sh`

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

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

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

Important

- If you have installed Citrix ADM 12.1.49.x or earlier releases, you get a grace period of 30 days to contact Citrix to rehost the original license on the Citrix ADM (at the DR site).
- For 12.1.50.x or later releases, the Citrix ADM license is automatically synchronized to the DR site (Not a requirement to contact Citrix for the license).
- Pooled license for the DR site is supported from 12.1.50.x or later releases. If you have applied pooled licenses for the instances, manually reconfigure the instances to the DR site.

Configure on-prem agents for multisite deployment

August 1, 2019

In the earlier versions of Citrix ADM, Citrix ADC instances deployed in remote data center(s) could be managed and monitored from Citrix ADM running in a primary data center. Citrix ADC instances sent data directly to the primary Citrix ADM that resulted in consumption of WAN (Wide Area Network) bandwidth. Additionally, processing of analytics data utilizes CPU and memory resources of primary Citrix ADM.
Customers have their data centers located across the globe. Agents play a vital role in following scenarios where the customers can choose:

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

**Note**

- Installing agents for instances in remote data center is recommended but not mandatory. If required, users can directly add Citrix ADC instances to primary Citrix ADM.
- If you have installed agents for the remote datacenter(s), then the communication between the agents and the primary site is through floating IP address. For more information, see port.
- You can install agents and apply pooled licenses to the instances at the remote data center(s). In this scenario, the communication between the primary site and the remote data center(s) is through the floating IP address.

In Citrix ADM 12.1, instances can be configured with agents to communicate with the primary Citrix ADM located in a different data center.

**Note**

On-prem agents for multisite deployment is supported only with Citrix ADM high availability deployment.

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

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

**Note**

The number of agents to be installed per site depends on the traffic being processed. Currently, Citrix has validated two agents per site for agent failover scenario. Citrix recom-
mends that you install at least two agents per site, so that the traffic flows to another agent in case of an agent failover.

**Architecture**

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

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

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

**Get started**

- Install the agent in a data center
  - Register the agent
  - Add the agent
- Add Citrix ADC instances
  - Add new instance
  - Update an existing instance
Install the agent in a data center

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

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

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

Note

On-prem agents for multisite deployment is supported only with Citrix ADM high availability deployment.

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>2 CPUs</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Citrix recommends that you increase the default value to 8 CPUs for better performance.</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>

Ports

For communication purposes, the following ports must be open between the agent and Citrix ADM on-prem server.
### Type Port Details

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>8443, 7443, 443</td>
<td>For outbound and inbound communication between agent and the Citrix ADM on-prem server.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80</td>
<td>For NITRO communication between agent and Citrix ADC or Citrix SD-WAN instance.</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>For SSH communication between agent and Citrix ADC or Citrix SD-WAN instance. For synchronization between Citrix ADM servers deployed in high availability mode.</td>
</tr>
<tr>
<td>UDP</td>
<td>4739</td>
<td>For AppFlow communication between agent and Citrix ADC or Citrix SD-WAN instance.</td>
</tr>
<tr>
<td>ICMP</td>
<td>No reserved port</td>
<td>To detect network reachability between Citrix ADM and Citrix ADC instances, SD WAN instances, or the secondary Citrix ADM server deployed in high availability mode.</td>
</tr>
<tr>
<td>SNMP</td>
<td>161, 162</td>
<td>To receive SNMP events from Citrix ADC instance to agent.</td>
</tr>
<tr>
<td>Syslog</td>
<td>514</td>
<td>To receive syslog messages from Citrix ADC or Citrix SD-WAN instance to agent.</td>
</tr>
</tbody>
</table>
Register the agent

1. Use the agent image file downloaded from the Citrix download site and import it in to your hypervisor. The naming pattern of the agent image file is as follows, `MASAGENT-<HYPERVISOR>-<Version.no>`. For example: `MASAGENT-XEN-12.1-xy.xva`

2. From the Console tab, configure Citrix ADM with the initial network configurations.

3. Enter the Citrix ADM host name, IPv4 address, and gateway IPv4 address. Select option 7 to save and quit the configuration.

4. After the registration is successful, the console prompts to log on. Use `nsrecover/nsroot` as the credentials.

5. To register the agent, enter `/mps/register_agent_onprem.py`. The Citrix ADM agent registration credentials are displayed as shown in the following image.

6. Enter the Citrix ADM floating IP address and the user credentials.
After the registration is successful, the agent restarts to complete the installation process.

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

**Agents**

<table>
<thead>
<tr>
<th>View Details</th>
<th>Delete</th>
<th>Rediscover</th>
<th>Attach Site</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Version</th>
<th>State</th>
<th>Platform</th>
<th>Country</th>
<th>Region</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.1012</td>
<td>ns</td>
<td>121-47</td>
<td>Down</td>
<td>XenServer</td>
<td>India</td>
<td>Karnataka</td>
<td>Bangalore</td>
</tr>
<tr>
<td>10.10.1.1097</td>
<td>ns</td>
<td>121-463</td>
<td>Up</td>
<td>XenServer</td>
<td>India</td>
<td>Karnataka</td>
<td>Bangalore</td>
</tr>
<tr>
<td>10.10.1.1064</td>
<td>ns</td>
<td>121-462</td>
<td>Up</td>
<td>XenServer</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>10.10.1.10017</td>
<td>ns</td>
<td>121-47</td>
<td>Down</td>
<td>XenServer</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

**Note**

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

**Add agent to site**

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

**Note**

- By default, all newly registered agents are added to the default datacenter.
- It is important to associate the agent with the correct site. In the event of an agent failure, the Citrix ADC instances assigned to it are automatically switched to other func-
Add Citrix ADC instances

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

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WO

Add a new instance

1. Navigate to Networks > Instances and select the instance type. For example, Citrix ADC.
2. Click Add to add a new instance.

```plaintext
Citrix ADC

<table>
<thead>
<tr>
<th>VPX</th>
<th>MPX</th>
<th>CPX</th>
<th>SDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Add
```

3. Check Enter Device IP Address and enter the IP address.
4. From Profile Name, select the appropriate instance profile, or create a new profile by clicking the + icon.
Note

For each instance type, a default profile is available. For example, the ns-root-profile is the default profile for Citrix ADC instances.

5. Select the **Site** with which you want to associate the instance.

Note

Based on the site selected, the list of agents associated to that site is displayed. Ensure you select the **Site** with which you want to associate the instance.

Add Citrix ADC VPX

6. Click to select the agent. From **Agent** page, select the agent with which you want to associate the instance and then click **Select**.

7. On the Add Citrix VPX page, click **OK**.
Update an existing instance to attach it to an agent

If an instance is already added to primary Citrix ADM, you can attach it to an agent by editing the adding instances workflow and selecting an agent.

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

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

Access the GUI of an instance to validate events

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

In Citrix ADM, navigate to Networks > Instances. Under Instances, select the type of instance you want to access (for example, Citrix ADC VPX), and then click the IP address of a specific instance.
The GUI of the selected instance is displayed in a pop-up window.

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

**Important**

Adding an agent for Citrix ADC instances in remote datacenters is recommended but not mandatory.

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

**Cluster the agent**

The term **Agent cluster** refers to a mechanism wherein agents attached to a site are logically grouped, so that if one of the agents fails, the Citrix ADC instances sending traffic to it are automatically reconfigured to start sending traffic to the other healthy agent(s) in that group or site.

The advantage of having agents clustered in a remote site is that if one agent fails, it is detected by Citrix ADM and implicitly all the instances are redistributed to other available agents in that cluster.

For example, we have two agents 10.106.1xx.2x and 10.106.1xx.7x that are attached and operational in the Bangalore site as shown below.

If one agent goes down, Citrix ADM will detect it and displays the state as **down**.

The instances attached to that agent are automatically reconfigured to use the other agent from the same cluster for trap destination, syslog server, and so on.
Migrate Citrix ADM single-server deployment to a high availability deployment

August 1, 2019

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

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

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

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

Modify the existing Citrix ADM server node

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

1. On a workstation or laptop, open the console of the existing Citrix ADM server node. For example, consider that you have deployed a Citrix ADM with IP address as 10.106.171.17 as a standalone server.
2. Log on to Citrix ADM. The default credentials are nsroot and nsroot.
3. In the shell prompt, type /mps/deployment_type.py, and press Enter.
4. Select the deployment type as Citrix ADM server. If you do not select any option, by default, it is deployed as a server.
5. The deployment console prompts you to select the server deployment (as standalone). Type **No** to confirm the deployment as high availability pair.

6. The console prompts you to select the (first server node). Enter **Yes** to confirm the node as the first server node.

7. The console prompts you to restart the server.

8. Type **Yes** to restart.

---

**Provision the second server node**

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

1. Import the image file to your hypervisor, and then from the Console tab configure the initial network configuration options as explained on the following screen:
2. After specifying the required IP addresses, in the shell prompt, type `/mps/deployment_type.py`, and press enter.

3. Select the deployment type as **Citrix ADM server**.

4. The deployment console prompts you to select the server deployment (as standalone). Type **No** to confirm the deployment as high availability pair.

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

6. Enter the first server's IP address and password.
7. Enter the floating IP address of the first node.

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

**Deploy the two servers in a high availability mode**

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

1. In a web browser, type the IP address of the previously existing Citrix ADM server node.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **System** tab, navigate to **Deployment** and click **Deploy**.

4. A confirmation message appears. Click **Yes**.

5. Though you have entered the floating IP while configuring the second server node, you have an option to update the FIP on the **Systems** page. Click **HA Settings > Configure Floating IP Address for High Availability Mode**. You can view the floating IP address you configured earlier. You can enter a new IP address and click **OK**.
You can now migrate your NetScaler Insight Center deployment to Citrix ADM without losing the existing configuration, settings, or data. With Citrix ADM you can not only view the various analytics generated by the NetScaler instances associated with an application, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

**Note**

Migration is currently supported only on NetScaler Insight Center Standalone instances.

**Prerequisites**

Before migrating the NetScaler Insight Center virtual appliance to Citrix ADM, verify that the following requirements have been met:

- NetScaler Insight Center 11.1 Build 47.14 or later is installed.
- You have downloaded the Citrix ADM 12.0 build 57.24 .tgz image file.

**Note**

You need to install Citrix ADM 12.0 build 57.24 and then upgrade to the latest Citrix ADM 12.1 build. For more information, see Upgrade.

- You have downloaded the Citrix ADM 12.1 latest build .tgz image file.

**Hardware Requirement**
### Component Requirement

<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 CPUs</td>
</tr>
<tr>
<td>Storage space</td>
<td>120 GB</td>
</tr>
</tbody>
</table>

**Note** Citrix recommends that you use 500 GB for better performance. Also, Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments.

<table>
<thead>
<tr>
<th>Virtual Network Interfaces</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

#### Hypervisor Requirements

- Citrix Hypervisor: 6.2, 6.5
- VMWare ESX: 5.5, 6.0
- Microsoft Hyper-V: 2012 R2
- Linux - KVM: Ubuntu, Fedora

### Installation procedure

**To migrate NetScaler Insight Center to Citrix ADM:**

1. Log on to shell prompt of NetScaler Insight Center.
2. Download the Citrix ADM 12.0 build 57.24 to the /var/mps/mps_images folder.
3. Untar the TGZ file by using the `tar-zxvf build-mas-12.0-57.24.tgz` command.
4. Install Citrix ADM by using the `./installmas` command.

```
bash-3.2# ./installmas
```

5. After installing Citrix ADM 12.0 build 57.24, you need to upgrade to the latest Citrix ADM 12.1 build by performing the above steps.

After the migration, all the NetScaler instances that were discovered in the NetScaler Insight Center inventory appear in the **Networks > Instances** section of Citrix ADM. However, for the first time you need to manually poll the virtual servers hosted in the discovered appliances.
Note
In Citrix ADM, by default, there is no licensing cost to manage and monitor 30 virtual servers created within the discovered NetScaler instances. To monitor and manage more than 30 virtual servers, install the required MAS licenses. For more details, see Citrix ADM Licensing.

Migrate Command Center configurations to Citrix ADM

August 1, 2019
You can now migrate your Command Center configurations to the Citrix Application Delivery Management (ADM) without losing the existing configuration, settings, or data of your Command Center deployment and Citrix ADM deployment. You can view the migrated Command Center configurations in Citrix ADM after the migration process is completed.

Points to note

- Migrating Command Center configurations to Citrix ADM is supported on the following deployments:
  - Command Center standalone to Citrix ADM standalone deployment or Citrix ADM high availability deployment.
  - Command Center high availability to Citrix ADM standalone deployment or Citrix ADM high availability deployment.

Note
You must use only the primary node IP address of Command Center and Citrix ADM high availability deployment while migrating the Command Center standalone or high availability deployment to Citrix ADM standalone or high availability deployment.

- You can run the Command Center tool multiple times on same or different Citrix ADM deployments:
  - Whenever you run the Command Center tool beyond the first time for the same Citrix ADM, the logs will be shown as failed for the configurations that have already been migrated and exist in Citrix ADM.
  - If any new configuration has been added in Command Center from the time the tool was run earlier to now for the same Citrix ADM, all such configuration except the new Custom tasks will be migrated to Citrix ADM.
Migrating Command Center configurations to Citrix ADM is supported for Citrix ADC, Citrix ADC SDX, and Citrix SD-WAN WO devices.

All communication between Command Center and Citrix ADM is on an HTTPS connection.

Backing up of existing data of Citrix ADM before migrating the Command Center configurations is highly recommended.

After the Command Center migration is completed, the Admin Partitions of Citrix ADC are auto-discovered in the Citrix ADM.

**Limitations**

The following Command Center configurations are not migrated from the Command Center appliance to the Citrix ADM:

- Device backup configuration files
- Timeout details in SD-WAN WO device profiles
- The following details under event and alarm triggers are not migrated:
  - Abort details for run command action
  - Run task details
  - Triggers with all empty parameters (severity/category/instances/failure objects) are not migrated
  - Triggers having instances with the state as HA cluster, primary, and secondary are not migrated if all the three states of the instances are selected
- Custom tasks without description are not migrated
- Event severities settings
- Event rule schedule details
- Syslog suppress filters
- Configuration task details
- Audit templates
- Audit policies without devices
- Audit policy schedule details
- Groups RBAC authorized scope settings
- Database monitor and management settings
- Performance custom reports
• Performance thresholds
• Custom views of fault/syslog/reports/Entity Monitoring
• AppFirewall and NS gateway reports and its schedule details
• SD-WAN WO auto configuration details
• High Availability settings
• Scheduled system backup settings
• Database retry settings
• Syslog purge schedule time
• All statistic data like syslog, events, and audit logs of all modules.

Prerequisites

Before migrating the Command Center configurations to Citrix ADM, ensure that the following prerequisites are met:

• You are running Command Center version 5.2 build 48.2 or later.
• You have installed and configured Citrix ADM version 12.0 build 51.24 or later.
• Only the Admin user will run the Command Center configuration migration.
• For successful migration of custom tasks, the description field is mandatory in Command Center.
• Communication between the Command Center and Citrix ADM is NITRO based. You must configure and open the necessary SSL (Secure Socket Layer) and TLS (Transport Layer Security) protocol settings on Command Center and Citrix ADM for NITRO communication.

Note

If you are using a Command Center version earlier than 5.2 build 48.2, you must upgrade the Command Center version to 5.2 build 48.2 and then migrate the Command Center configurations to Citrix ADM. For detailed information about upgrading the Command Center appliance, see Upgrading Command Center.

Migrate the configurations

To migrate a Command Center configuration to Citrix ADM, you need the Command Center appliance IP address and administrator credentials.

To migrate Command Center Configurations to Citrix ADM:
1. In a web browser, type the IP address of the Command Center appliance.

2. In the **User Name** and **Password** fields, type the administrator credentials and log in.

3. After successful login, on the screen that appears, select the **Administration** tab and do one of the following:

   - In the right pane, under **Citrix ADM Migration**, select **Migrate Configuration**, as shown in the following figure.

   ![Citrix Command Center with Migrate Configuration selected](image1)

   - In the left pane, select **Citrix ADM Migration**, and then click **Migrate Configuration**, as shown in the following figure.

   ![Citrix Command Center with Migrate Configuration selected](image2)

4. In the **Command Center to MAS Migration** dialog box, enter the IP address of the Citrix ADM server, and the administrator credentials, and then click **OK**.

   **Note**

   In case of Citrix ADM high availability deployment, enter the primary node IP address.
5. At the confirmation prompt, click Yes.

The screen reports the progress of the migration tasks.

The **Migrate Configuration** operation takes the details of the Citrix ADM deployment and its admin credentials as input. The **Migrate Configuration** operation then migrates the configuration of Command Center deployment to Citrix ADM deployment.

When the tasks are completed, you can verify the migrated Command Center configuration from Command Center migration logs and Citrix ADM data.
To use the Command Center migration logs to verify the migration

1. In the Command Center GUI, on the **Administration** tab, do one of the following:
   - In the right pane, under **Citrix ADM Migration**, click **Migration Log**.
   - In the left pane, select **Citrix ADM Migration**, and then click **Migration Log**.

2. Review the list of migration logs.

3. To display more detail, select **Module Name**, or to display details for a particular module, select that module, and then click **Details**.
4. The following example shows the log details for a selected module.

To use the Citrix ADM to verify the migration

During the migration process, the Command Center configurations are migrated to Citrix ADM and are shown as Citrix ADM configurations in the Citrix ADM GUI.

After the migration process is completed, the Citrix ADM server reboots and there might be a momentary downtime. When the Citrix ADM server is up and running, access the Citrix ADM GUI by typing the IP address of the Citrix ADM server in the address bar of your browser.

The following table shows how the Citrix ADM terminology for the migrated configurations corresponds to the terminology used in Command Center.

<table>
<thead>
<tr>
<th>Command Center Terminology</th>
<th>Citrix ADM Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device profiles</td>
<td>Instance profiles</td>
</tr>
<tr>
<td>Devices and its state (like managed/unmanaged)</td>
<td>Instances and its state (like managed/unmanaged)</td>
</tr>
<tr>
<td>Device annotations</td>
<td>Instance annotations</td>
</tr>
<tr>
<td>Device groups</td>
<td>Instance groups</td>
</tr>
<tr>
<td>Maps</td>
<td>Instance groups</td>
</tr>
<tr>
<td>Event and alarm triggers</td>
<td>Event rules</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
**Integrate Citrix ADM with Citrix Director**

August 1, 2019

Director integrates with Citrix ADM for network analysis and performance management.

- Network analysis obtains HDX Insight reports from Citrix ADM and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment.
Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you integrate Citrix ADM with Director, HDX Insight reports provide you with the following information in Director:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

**Prerequisites**

**Hardware Requirements for HDX Insight to Citrix ADM Migration**

<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>500 GB. Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Software Requirements**

Before migrating to the Citrix ADM virtual appliance, verify that the following requirements have been met:

- Director version 1811 is installed
- NetScaler HDX Insight version 10.1 or later is installed
- HDX Insight and Citrix ADM supports Citrix VDA version 7.0 and later
- Citrix Workspace is supported on Citrix Virtual Apps and Desktops version 7.0 and later
- Ensure that MAC Citrix Receiver for Mac version 11.8 and later, and Windows Citrix Receiver for Windows 14.0 and later are available to display accurate ICA RTT metrics
• Citrix ADM version 11.0 and later is installed. For more information on how to install Citrix ADM, see Deploy Citrix ADM.

Limitations

• The availability of this feature depends on your organization’s license and your administrator permissions.

• ICA session Round Trip Time (RTT) shows data correctly for Citrix Receiver for Windows 3.4 or later and for Citrix Receiver for Mac 11.8 or later. For earlier versions of these Receivers, the data does not display correctly.

• In the Trends view, HDX connection logon data is not collected for VDAs earlier than version 7. For earlier VDAs, the chart data is displayed as 0.

• For deployments that already have an external hard disk with storage space less than 500 GB, you cannot add another hard disk.

Note

– For more information on Director and for steps to integrate Citrix ADM with Director, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html.

– For more information on HDX Insight, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Attach an additional disk to Citrix ADM

August 1, 2019

Citrix Application Delivery Management (ADM) storage requirement is determined based on your Citrix ADM sizing estimation. By default, Citrix ADM provides you a storage capacity of 120 GB. If you need more than 120 GB for storing your data, you can attach an additional disk.

Note

• Estimate storage requirements and attach an additional disk to the server at the time of initial deployment of Citrix ADM.

• For a Citrix ADM single-server deployment, you can attach only one disk to the server in addition to the default disk.

• For a Citrix ADM high availability deployment, you must attach an additional disk to each node. The size of both disks must be identical.
• If you had earlier attached an external disk of lower capacity, you must remove the disk before attaching a new disk.

• You can attach an additional disk of capacity greater than 2 terabytes. If necessary, the size of the disk can be lower than 2 terabytes also.

• Citrix recommends using solid-state drive (SSD) technology for Citrix ADM deployments.

This document explains the following scenarios about attaching a new additional disk, creating partitions, and resizing the additional disks:

1. Attach a new additional disk
2. Launch the disk partitioning tool
3. Create partitions in the new additional disk
4. Resize the existing additional disk
5. Remove partitions on the additional disk

**Attach an additional disk in a standalone Citrix ADM**

Perform the following steps to attach a disk to the virtual machine:

1. Shut down the Citrix ADM virtual machine.
2. In the hypervisor, attach an additional disk of the required disk size to Citrix ADM virtual machine.

   The newly attached larger disk stores the database data and Citrix ADM log files. The existing 120-gigabytes default disk is now used to store the core files, operating system log files, and so on.
3. Start the Citrix ADM virtual machine.

**Citrix ADM disk partition tool**

Citrix ADM now provides **Citrix ADM disk partition tool**, a new command line tool. The functionalities of this tool are described in detail as follows:

1. Using the tool, you can create partitions in the newly added additional disk.
2. You can also resize existing additional disk using this tool. But the existing external disk should not be greater than 2 terabytes.

   **Note**
   - It is not possible to resize existing disks beyond 2 terabytes without losing data. This
is due to a known limitation on the platform.

- To create a storage capacity greater than 2 terabytes, you must remove the existing partitions and create partitions using this new tool.

3. Using this new tool, you can perform any partition action on the disk explicitly. The tool provides you with clear visibility and control over the disk and the associated data.

Note
You can only use this tool on the additional disk that you have attached to the Citrix ADM server. You cannot create partitions in the primary (default) 120-gigabytes disk using this tool.

Launch the disk partition tool

1. Open an SSH connection to the Citrix ADM by using an SSH client, such as PuTTY.
2. Log on to the Citrix ADM by using the administrator credentials.
3. Switch to the shell prompt and type:

   ```
   /mps/DiskPartitionTool.py
   ```

   Note
   For Citrix ADM in high availability deployment, you must launch the tool in both nodes and create or resize partitions after attaching disks to the respective virtual machines.

Create partitions in the new additional disk

The `create` command is used to create partitions whenever a new secondary disk is added. You can also use this command to create partitions on an existing secondary disk after the existing partitions are deleted using the “remove” command.
Note

There is no 2 terabytes size limitation while creating partitions with the disk partition tool. The tool can create partitions larger than 2 terabytes. When you partition the disk, a swap partition of size 32 GB is automatically added. The primary partition then uses all the remaining space on the disk.

Once the command is executed, a GUID partition table (GPT) partition scheme is created. Also a 32 GB swap partition and data partition are created to use rest of the space. A new file system is then created on the primary partition.

Note

This process can take a few seconds, and you must not interrupt the process.

```bash
(dpt): create
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect. Are you sure you want to continue (Y/N): y
Creating GPT partition scheme...
d1 created
Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
dsp1 added
Creating partition 2 for swap using remaining 32G...
dsp2 added
Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrupt the process...
```

Once the create command completes, the virtual machine is automatically restarted for the new partition to get mounted.

```bash
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...
*** FINAL System shutdown message from nsroot@ns-mgmt-system ***
System going down IMMEDIATELY
```

After the restart, the new partition is mounted at /var/mps.
The swap partition added shows up as swap space in the output of the “create” command.

```
bash-3.2# df -k
Filesystem 1024-blocks   Used   Avail Capacity Mounted on
/dev/md0        456046   374346    72580    84%   /
/dev/ndsfs     1        1          0    100%   /dev
/procfs         4        0          0    100%   /proc
/fdescsfs       1        1          0    100%   /dev/fg
/dev/da0s1a    1623950  284466  1209568    19%   /flash
/dev/da0s1e    116073918 2812298 103975708     3%   /var
/dev/da1p1     495168802 43854  455511444     0%   /var/mps
```

**Note**

The tool restarts the virtual machine after you have created the partition.

### Resize the partitions in the existing additional disk

You can use the `resize` command to resize the attached (secondary) disk. You can resize a disk that has a master boot record (MBR) or GPT scheme. The size of the disk should be less than 2 terabytes in size to a maximum of 2 terabytes.

**Note**

- The “resize” command is designed to function without losing any existing data. But Citrix recommends that you back up critical data in this disk to external storage before attempting the resize. Data backup is helpful in cases where the disk data can get corrupted during the resize operation.
- Ensure to increase the disk space in increments of 100 GB of space while resizing the partitions. Such an incremental increase ensures that you would not have to resize more frequently.

```
(dpt): Resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capacity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

******** WARNING !! ********
Resizing the partition/disk works without affecting the existing data.
However, we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```
The “resize” command checks for all preconditions and proceeds if all preconditions are met and after you have given consent to resizing. It stops the processes accessing the disk, which includes the Citrix ADM subsystems, PostgreSQL DB processes, and Citrix ADM monitor process. Once the processes are stopped, the disk is unmounted to prepare it for resizing. The resizing is done by extending the partition to occupy the complete available space and then growing the file system. If a swap partition exists on the disk, it is deleted and recreated at the end of the disk after resizing. The swap partition is discussed in the Create command section of the document.

Note

The “growing file system” process can take some to complete and take care that you do not interrupt the process while it is in progress. The tool restarts the virtual machine after you have resized the partition.

```
(dpt): resize

**************
*** WARNING!! ***
**************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
Are you sure you want to resize (Y/N): y
```

Unmounting partition: /dev/dalp1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/dalp2
Deleting swap partition: dalp2
Resizing partition dalp1...
dalp1 resized
Adding a swap partition dalp2...
dalp2 added
Formatting the newly added portions of the partition. This may take some time (<10 seconds). Please be patient and don’t interrupt the process...

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

All the intermediate steps in the resize process (stopping applications, resizing disk, growing filesystem) are shown on the console. Once the process completes, the following message is seen.

After rebooting, the increase in size can be observed using the “df” command. Here is the before and after details after you increase the size:
Remove the partitions in the additional disk

An existing partition on the secondary disk can be resized up to 2 terabytes. This is due to a known limitation on the partition. If you want a disk larger than 2 terabytes, either attach a new disk and partition it by using the disk partition tool. You can also remove the existing partition by using the `remove` command, and then create a partition.

Note

Removing the existing partition deletes all existing data. So, any critical data must be backed up to external storage before using this command.

```
(dpt): remove
Removes existing partition from attached disk.

*** WARNING ***
***************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Running the “remove” command asks you for confirmation and once confirmed, it stops all processes (such as ADM subsystems, PostgreSQL processes, and ADM monitor) using the secondary disk. If a swap partition exists and swap is enabled on the partition, then the swap is disabled.

```
(dpt): remove

*** WARNING ***
***************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
Are you sure you want to continue (Y/N): y
```

When you type “y,” the command unmounts the disk and removes all partitions on the disk.
Note
The tool restarts the virtual machine after you have removed the partition.

Restart the virtual machine

When a partition is created or resized, or when a swap file is created, restart the virtual machine. The changes take effect only after restarting. For this purpose, a **reboot** command is provided in the tool.

You are prompted for confirmation and once confirmed, it stops all processes (such as ADM subsystems, PostgreSQL processes, and ADM monitor.) The virtual machine is then restarted.

Create a backup file of the disk data

Here are the steps to follow to backup Citrix ADM data before resizing or removing the partitions.

**Note**
Creating a backup file requires disk space. Citrix recommends that you ensure there is enough free disk space available (50% or more) before backup commands are executed.

1. Stop ADM.
1. Stop PostgreSQL.

   `su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh`

2. Stop PostgreSQL.

   `su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh`


   `su -l mpspostgres /mps/scripts/stop_mas_monit.sh`

4. Create tarball.

   1. `cd /var`
   2. `tar cvfz /var/mps/mps_backup.tgz`

   **Note**
   
   The operation takes time depending on the size of the data to be backed up.

5. Generate checksum.

   `md5 mps_backup.tgz > mps_backup_checksum`

6. Remote copy the tarball and checksum.

   `scp`

7. Validate the correctness of the copied tarball. Generate a checksum of the transferred file and compare with the source checksum.

8. Remove the tarball from the ADM virtual machine.

   `rm mps_backup.tgz mps_backup_checksum`

**Additional commands**

In addition to the commands listed earlier, you can also use the following commands in the tool:

**Help command:**

To list the supported commands, type `help` or `?` and press enter. To get further help on each of the command press `help` or `?` followed by the command name and press the **Enter** key.
Info command:
The **info** command provides information about the attached secondary disk if the disk exists. The command provides the device name, the partition scheme, size in human-readable form, and the number of disk blocks. The scheme can be MBR or GPT. An MBR scheme means the disk was partitioned using an earlier version of Citrix ADM version. The MBR/GPT based partition can be resized but not beyond 2 terabytes. GPT partition scheme means that the disk was partitioned using Citrix ADM 12.1 or later.

**Note**
A GPT partition can be greater than 2 terabytes but when it is created. But you cannot resize the disk to a size greater than 2 terabytes after creating a disk with a smaller size. This is a known limitation of the platform.

Create_swapfile command:
The default swap partition on the primary disk of Citrix ADM is 4 GB and therefore, the default swap space is 4 GB. For the default memory configuration of Citrix ADM which is 2 GB, this swap space is sufficient. However, when you run Citrix ADM with a higher memory configuration, you need to have more swap space allocated on the disk.
Swap partition is usually a dedicated partition that is created on a hard disk drive (HDD) during the installation of the operating system. Such a partition is also referred to as a swap space. Swap partition is used for virtual memory that simulates the additional main memory.

Secondary disks that were added in the earlier versions of Citrix ADM do not have a swap partition created by default. The “create_swapfile” command is meant for secondary disks created using older Citrix ADM versions which don’t have a swap partition. The command checks for the following:

- Presence of a secondary disk
- Disk being mounted
- Size of the disk (at least 500 GB)
- The existence of the swap file

The “create_swapfile” command is useful only when the memory is greater or equal to 16 GB and not when memory is low. Therefore, this command also checks for memory before proceeding with swap file creation.

If all the conditions are met, and the user consents to proceed, a 32 GB swap file is created on the secondary disk. The swap file creation process takes a few minutes to complete and take care that you do not interrupt the process while in progress. After successful completion, a restart is done for the swap file to take effect.

After reboot, the increase in swap can be observed using the top command.

Exit command:
To exit from the tool, type exit and press the Enter key.

Attach additional disks to Citrix ADM deployed in high availability

Let us consider a scenario where you have configured a pair of Citrix ADM servers in a high availability set up without any secondary disks. Also, let us consider you have added two or more Citrix ADC instances, checked and ensured all processes are running. You might want to add secondary disks to the virtual machines in this setup. In a high availability set up, you must add additional disks to both nodes as detailed in this task:

1. Assume that the Citrix ADM node names are “ADM_Primary” and “ADM_Secondary.”
2. First, run the partition tool on ADM_Secondary and then add a secondary disk. The virtual machine restarts after the disk is added.
3. Shut down the ADM_Secondary after it restarts.
4. Now run the partition tool on ADM_Primary and add a secondary disk. The virtual machine restarts after the disk is added.
   
   Ensure that you add disks of similar capacity to both nodes. For example, if you add a disk of the capacity of 500 GB to the primary node, add a disk of 500 GB capacity to the secondary node also.
5. After the ADM_Primary restarts, check that it is the primary node.
6. Now start the ADM_Secondary node. Ensure that it has come up as the secondary node and the databases have synchronized.
7. Confirm that all data still exists.

Perform the following steps to increase the capacity of RAM on both the nodes:

1. Shutdown ADM_Secondary and increase the RAM size as required. Don’t restart the node.
2. Shutdown ADM_Primary and increase the RAM size as required.
   
   Ensure that you increase the RAM size equally on both nodes. For example, if you increase the RAM size on the primary node to 16 GB, do the same on the secondary node as well.
3. Restart the ADM_Primary.
4. After the ADM_Primary reboots, check that it is the primary node.
5. Now start the ADM_Secondary node. After it restarts, ensure that it has come up as secondary and the DB sync is working.

6. Now confirm that all data still exists.

Note
After you add the secondary disk, the primary node takes some time to come up. Also, the entire process of adding secondary disks to both nodes and increasing RAM capacity requires both nodes to be down for some time. Consider this downtime while planning this maintenance activity.

Configure

August 1, 2019

You can access a Citrix ADM server only by using the graphical user interface (GUI). You have to access the GUI to add instances, manage and monitor your instances and apps, view analytics, and configure the Citrix ADM server.

Your workstation must have a supported web browser to access the configuration utility and Dashboard.

The following browsers are supported.

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>11.0 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Chrome 19 and later</td>
</tr>
<tr>
<td>Safari</td>
<td>Safari 5.1.1 and later</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Firefox 3.6.25 and later</td>
</tr>
</tbody>
</table>

To access the Citrix ADM GUI:

1. In a web browser, type the IP address of Citrix ADM (for example, http://192.168.100.1). This is the same IP address that you had specified while installing the server.

2. In the User Name and Password fields, enter the administrator credentials. The default administrator credentials are nsroot/nsroot.

   After you log on to Citrix ADM, you have to do the following to get started:

   • Add instances to Citrix ADM. You must add instances to the Citrix ADM server if you want to
manage and monitor these instances.

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

- **Configure NTP server on Citrix ADM.** You have to configure a Network Time Protocol (NTP) server in Citrix ADM to synchronize its clock with the NTP server.

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

## Add instances to Citrix ADM

August 1, 2019

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

- **Citrix ADC**
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
- **Citrix Gateway**
- **Citrix SD-WAN**

You can add instances either while setting up the Citrix ADM server for the first time or at a later time. You must then specify an instance profile that Citrix ADM can use to access the instance.

**Note**

- Citrix ADM uses the NetScaler IP (NSIP) address of the Citrix ADC instances for communication. For information about the ports that must be open between the Citrix ADC instances and Citrix ADM, see Ports.

- For Citrix SD-WAN WO and Citrix SD-WAN EE instances, Citrix ADM uses the management IP address of the instances for communication.
How to create a Citrix ADC Profile

Citrix ADC profile contains the user name, password, communication ports, and authentication types of the instances that you want to add to Citrix ADM. For each instance type, a default profile is available. For example, the nsroot is the default profile for Citrix ADC instances. The default profile is defined by using the default Citrix ADC administrator credentials. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a profile, and then rediscover the instance.

You can create a Citrix ADC profile from the Instance page or while adding or changing an instance.

To create a Citrix ADC profile from the Instance page:

1. Navigate to Networks > Instances.
2. Select an Instance. For example, Citrix ADC.
3. On the Instance page, select Profiles.
4. On the Admin Profiles page, select Add.
5. On the Create Citrix ADC Profile page, do the following:
a) **Profile Name**: Specify a profile name for the Citrix ADC instance.

b) **UserName**: Specify a user name to log on to the Citrix ADC instance.

c) **Password**: Specify a password to log on to the Citrix ADC instance.

d) **SSH Port**: Specify the port for SSH communication between Citrix ADM and the Citrix ADC instance.

e) **HTTP Port**: Specify the port for HTTP communication between Citrix ADM and the Citrix ADC instance.
Note
The default HTTP port is 80. You can also specify the non-default or customized HTTP port that you might have configured in your Citrix ADC CPX instance. The customized HTTP port can be used for communication only between Citrix ADM and Citrix ADC CPX.

f) HTTPS Port: Specify the port for HTTPS communication between Citrix ADM and the Citrix ADC instance.

Note
The default HTTPS port is 443. You can also specify the non-default or customized HTTPS port that you might have configured in your Citrix ADC CPX instance. The customized HTTPS port can be used for communication only between Citrix ADM and Citrix ADC CPX.

g) Use global settings for Citrix ADC communication: Select this option if you want to use the system settings for communication between Citrix ADM and Citrix ADC instance, otherwise select either http or https.

h) SNMP Version: Select either SNMPv2 or SNMPv3 and do the following:

i. If you select SNMPv2, specify the Community name for authentication.

ii. If you select SNMPv3, specify the Security Name and Security Level. Based on the security level, select the Authentication Type and Privacy Type.
i) **Timeout Settings**: Specify the time that Citrix ADM must wait before sending a connection request to the Citrix ADC instance after a restart.

j) Select **Create**.

### Add ADC instances to Citrix ADM

You can add instances either while setting up the Citrix ADM server for the first time or at a later time. 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. Note that Citrix ADM supports only Citrix SD-WAN WO and Citrix SD-WAN EE editions.

**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 is represented by the cluster IP address only.

- For Citrix ADC instances set up as an HA pair, when you add one instance, the other instance...
In the pair is automatically added.

If two Citrix ADM servers are set up in high availability mode, when an instance is added, load balancing comes into effect and the instances are distributed across the two Citrix ADM server nodes by using the round-robin method.

**To add an instance to Citrix ADM:**

1. In a web browser, type the IP address of the Citrix Application Delivery Management (for example, http://192.168.100.1).
2. In the **UserName** and **Password** fields, enter the administrator credentials. The default administrator credentials are nsroot/nsroot.
3. Navigate to **Networks** > **Dashboard** and click **All Instances**. On the **Instances** page, click **Add**. On the **Add Instance** page, from **Instance Type**, select the type of instance you want to add, and then follow the instructions in step 4.

Alternatively, navigate to **Networks** > **Instances**. Under **Instances**, select the type of instance you want to add (for example, Citrix ADC VPX) and click **Add**.

4. 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. For SD-WAN instances, specify the 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.
5. From **Profile Name**, select the appropriate instance profile, or create a new profile by clicking the + icon.
6. From **Site**, select the location where you want to add the instance, or create a new location by clicking the + icon.
7. Click **OK** to initiate the process of adding instances to Citrix ADM.
Note
If you want to rediscover an instance, navigate to Networks > Instances > Citrix ADC <Instance Type>, select the instance you want to rediscover, and then from the Action drop-down list, click Rediscover.

Add ADC CPX instances to Citrix ADM

Citrix ADM has been enhanced to provide support to the improvements that has been accomplished in CPX functionalities. Citrix ADC CPX instance is now added in Citrix ADM by providing an IP address for the CPX along with a device profile. The process of addition of a CPX instance is now similar to how other ADC types such as VPX or MPX is added in ADM. Also, the registration of CPX in ADM has been enhanced. When a CPX starts, Citrix ADM automatically discovers and registers the CPX instance. A CPX instance is no longer discovered through Docker host.

1. Navigate to Networks > Instances > Citrix ADC and click CPX tab.
2. Click Add to add new CPX instances in Citrix ADM.
3. The Add Citrix ADC CPX page opens. Enter the values for the following parameters:
   a) You can add CPX instances by providing either the reachable IP address of the CPX instance or the IP address of the Docker container where the CPX instance is hosted.
   b) Select the profile of the CPX instance.
   c) Select the site where the instances is to be deployed.
   d) Select the agent.
   e) As an option, you can enter the key-value pair to the instance. Adding key-value pair makes it easy for you to search for the instance later.
For Citrix ADC CPX instances, you must specify the HTTP, HTTPS, SSH, and SNMP port details of the host while creating the CPX instance profile. You can also specify the range of ports that were published by the host in the Start Port and Number of ports field.

4. Click OK.

Add Citrix ADC VPX instances deployed in cloud to Citrix ADM

August 1, 2019

You can use Citrix ADM to manage and monitor the Citrix ADC VPX instances deployed on a public cloud such as Amazon Web Services (AWS) or Microsoft Azure. You need to establish Layer 3 connectivity between Citrix ADM and the Citrix ADC VPX instances deployed on the public cloud. To establish the Layer 3 connectivity, you can use solutions such as NetScaler CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN in Azure, or third-party connectors such as Equinix and so on.

The following sample topology uses NetScaler CloudBridge Connector for Layer 3 connectivity between Citrix ADM and the Citrix ADC VPX instances deployed in the cloud.
A CloudBridge Connector tunnel is set up between Citrix ADC appliance NS_Appliance-DC, in data-center DC, and Citrix ADC virtual appliance (VPX) NS_VPX_CBC in the public cloud. NS_Appliance-DC and NS_VPX_CBC enable the communication between Citrix ADM and the Citrix ADC VPX instance, NS_VPX_1, deployed in the public cloud. After the communication is established, you can discover NS_VPX_1 in Citrix ADM.

To configure this topology:

1. Install, configure, and start a Citrix ADC VPX instance in the public cloud.
   - For instructions, see Installing Citrix ADC VPX on AWS.
   - For instructions, see Installing Citrix ADC VPX on Microsoft Azure.
2. Deploy and configure a Citrix ADC physical appliance, or provision and configure a Citrix ADC virtual appliance (VPX) on a virtualization platform in the datacenter.
   - For instructions, see Installing Citrix ADC Virtual Appliances on Citrix Hypervisor.
   - For instructions, see Installing Citrix virtual appliances on VMware ESXi.
   - For instructions, see Installing Citrix ADC virtual appliances on Microsoft Hyper-V.
3. Configure the CloudBridge Connector between the datacenter and the public cloud. For instructions, see Configuring CloudBridge Connector.
4. Configure the static route for establishing connection between Citrix ADM and the Citrix ADC VPX instances deployed on the cloud, as follows:
   a) Log on to Citrix ADM.
   b) Navigate to System > Static Routes and click Add.
c) In the **Network Address** field, enter the address of the network that you want to establish a static route from Citrix ADM through the connector.

d) In the **Netmask** field, enter the netmask for the network.

e) In the **Gateway** field, enter the address of the gateway.

5. Add the Citrix ADC VPX cloud instances to the Citrix ADM by specifying the range of IP addresses of Citrix ADC VPX instances in the public cloud. For detailed instructions, [Add Instances to Citrix ADM](#).

## Enable analytics on virtual servers

**August 1, 2019**

You can enable analytics for a specific virtual server on the selected instance, representing an application server, and monitor the traffic of that application server. Analytics provide statistics for the virtual server.

**Note**

For Citrix ADC instances of 11.0 release, 65.30 build and later, there is no option on Citrix ADM to enable Security Insight explicitly. Ensure that you configure the AppFlow parameters on the Citrix ADC instances. After AppFlow parameters configuration is complete, Citrix ADM starts receiving the Security Insight traffic along with the Web Insight traffic. For more information on how to set the AppFlow parameters on Citrix ADC instances, see [To set the AppFlow parameters by using the configuration utility](#).

**To enable Analytics on each instance on Citrix ADM:**
1. In a web browser, type the IP address of the Citrix Application Delivery Management (for example, http://192.168.100.1).

2. In Username and Password, enter the administrator credentials.

3. Navigate to Networks > Instances, and select the Citrix ADC instance you want to enable analytics. For example, Citrix ADC.

4. From the list of instances, select an instance.

5. From Select Action drop-down, select Configure Analytics.

6. In Application List, select the virtual servers and click Enable AppFlow.

7. In the Enable AppFlow field, type true, and based on the analytics you want to enable, select Security Insight or Web Insight, or both.

![Enable AppFlow]

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the UDP port 4739 is open. This is to allow ADM to collect AppFlow traffic. SSL Insight will not be available if IPFIX Transport mode is used.

- For HDX Insight and Gateway Insight, while clicking Enable AppFlow, you need select VPN virtual server configured on your Citrix ADC instance, and select ICA or HTTP check boxes accordingly.
For **TCP Insight**, navigate to **System > Analytics Settings > Configure Features**, and select **Enable TCP Insight**.

For **Video Insight**, you need to make the configuration changes on the Citrix ADC Appliance. For more details on how to enable analytics for Video insight, see Video Insight.

For **WAN Insight**,

a) Navigate to **Infrastructure > Instances > NetScaler SD-WAN WO**, and select the datacenter WAN optimization appliance.

b) From the **Action** drop-down, select **Enable Insight**.

c) 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.

You can select the **AppFlow transportation mode** to IPFIX or Logstream while enabling AppFlow on the discovered Citrix ADC instances in Citrix ADM.
To select the transportation mode from the Enable Insight window, select the transport mode to **IP-FIX** or **Logstream**.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Transport Mode = IPFIX</th>
<th>Transport Mode = Logstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Insight</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Insight</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL Insight</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP Reputation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AppFirewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client Side Measurement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Syslog/Auditlog</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You can also enable or disable the processing of the Web Insight traffic by using the **Enable Web Insight** option in Citrix ADM. If you do not want to monitor the Web Insight traffic, you can disable the option. For more information, see [Processing of the Web Insight traffic by Citrix ADM](#).

**Configure NTP server**

**August 1, 2019**

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

**To configure an NTP server on Citrix ADM:**

1. Navigate to **System > NTP Servers**, and then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
   - **Server Name/IP Address** – Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - **Minimum Poll Interval** – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as $2^6$, enter $6$.
• **Maximum Poll Interval** – Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2^8, enter 8.

• **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.

• **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.

• **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

**To enable NTP synchronization on Citrix ADM:**

1. Navigate to **System > NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** checkbox.
3. Click **OK**.

**Configure system settings**

August 1, 2019

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

**Configure system alarms**

You should configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, loginFailure), a message is recorded in the system and you can view the message as syslog message.

**To configure system alarms:**

1. Navigate to **System > Alarms**, select the alarm you want to configure, and click **Edit**.
2. On the Configure Alarm page, select the alarm severity, and set the Threshold.

3. To view the alarms that have breached the threshold or for which an event has occurred, navigate to System > Auditing and click Syslog Messages.

**Configure system notifications**

You can send notifications to select groups of users for a number of system-related functions. You can set up a notification server in Citrix ADM, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. This ensures that you are notified of any system-level activities such as user login or system restart.

**To configure system notifications:**


2. On the Configure System Notification Settings page, select the category or category of events generated by Citrix ADM.

3. Then, configure either the email server or the SMS server to receive notification through email or SMS or both.

**Configure system prune settings**

To limit the amount of reporting data being stored in your Citrix ADM server’s database, you can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

**To configure system prune setting:**

1. Navigate to System > System Administration. Under Prune Settings, click System Prune Settings.

2. In the Configure System Prune Settings page, specify the number of days for which to retain data, and click OK.

**Configure system backup settings**

Citrix ADM automatically backs up the system everyday at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system. You can also encrypt the backup file. You can also choose to save the backup on an external server.

**To configure system backup settings:**

1. Navigate to System > System Administration.
2. Under **Backup Settings**, click **System Backup Settings**.

3. On the **Configure System Backup Settings** page, specify the required values.

**Configure instance backup settings**

If you back up the current state of a Citrix ADC instance, you can use the backup files to restore stability in the event that the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.

**To configure instance backup settings:**

1. Navigate to **System > System Administration**.

2. Under **Backup Settings**, select **Instance Backup Settings**, and specify the required values.

**Configure instance event prune settings**

To limit the amount of event messages data being stored in your Citrix ADM server’s database, you can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).

**To configure instance event prune settings:**

1. Navigate to **System > System Administration**.

2. Under **Prune Settings**, click **Instance Events Prune Settings**.

3. Enter the time interval, in days, for which you want to retain data on the Citrix ADM server and click **OK**.

**Configure instance syslog purge settings**

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the Generic syslog data will be deleted from Citrix ADM.

**To configure instance syslog purge settings:**

1. Navigate to **System > System Administration**. Under Prune Settings, click **Instance Syslog Purge Settings**.

2. In Configure Instance Syslog Purge Settings page, specify the number of days between 1 and 180 in **Retain Syslog Generic Data** field.

3. Click **OK**.
Upgrade

August 1, 2019

Each Citrix ADM release offers new and updated features with increased functionality. Citrix recommends you upgrade Citrix ADM to the latest release to avail of the new features and bug fixes. A comprehensive list of enhancements, known issues, and bug fixes is included in the release notes accompanying every release announcement. It is also important to understand the licensing framework and types of licenses that can be used before you start to upgrade. For Citrix ADM licensing information, see Licensing.

Before you upgrade

Download the upgrade package from the Citrix ADM Downloads page and follow the instructions in this article to upgrade your system to the latest 12.1 build. After the upgrade operation is started, Citrix ADM restarts and the existing connections are terminated and reconnected when the upgrade is completed successfully. The existing configuration is preserved, but Citrix ADM does not process any data until the upgrade is successfully completed.

Points to note before upgrading to 12.1:

• If you are upgrading to Citrix ADM 12.1 build 48.18 version from either version 11.1 or from version 12.0 build earlier than 56.x, perform the following steps.
  – Upgrade from existing version to 12.0 build 57.24.
  – Then, upgrade to the latest build of version 12.1.

  You must follow this two-step process because there are certain clean-up procedures required to upgrade successfully to 12.1 release. These procedures are available only from 12.0 build 56.x onwards.

• With 12.1, the high availability deployment has the ability to configure a floating IP address on the primary node and eliminate the need for a separate Citrix ADC load balancer. Because of this improvement, the high availability deployment must be on the same subnet. If your current deployment is on different subnets, you must review this article to learn about the upgrade process.

• With 12.1, the advanced backup support has been removed. The advanced backup feature is no longer available after you upgrade to Citrix ADM 12.1. Review this article for more details.

Note

You cannot downgrade Citrix ADM from a 12.1 build to any build of an earlier release.
Recommended precautions:

- Back up the Citrix ADM server before you upgrade.
- After the upgrade, you might have to reestablish connections between the Citrix ADM server and the managed instances. A confirmation prompt warns you that connections can fail if you proceed.
- For Citrix ADM servers in high availability setup, when upgrading, do not make any configuration changes on either of the nodes.

**Warning**

Do not refresh the browser until the upgrade process is successfully completed. It might take a few minutes for the upgrade process to finish.

- After upgrade, the active node can change in a high availability pair.

Upgrade single Citrix ADM server

To upgrade single Citrix ADM Server:

1. In a web browser, type the IP address of the Citrix ADM server.

   **Note**
   
   For Citrix ADM servers in a high availability mode, type the IP address of either of the Citrix ADM servers in the HA pair, or the load balancing virtual server.

2. In the **User Name** and **Password** fields, enter the administrator credentials.

3. Navigate to **System > System Administrations**. Under the **System Administration** sub-heading, click **Upgrade Citrix ADM**.

4. On the **Upgrade Citrix ADM** page, select the **Clean software image on successful upgrade** check box to delete image files after upgrade. Selecting this option removes the Citrix ADM image files automatically upon upgrade.
Note

This option is selected by default. If you do not select this check box before starting the upgrade process, you must manually delete the images.

5. You can then upload a new image file by selecting either Local (your local machine) or Appliance. The build file must be present on the Citrix ADM virtual appliance.

The Confirm dialog box is displayed. Click OK.

6. Click OK.

The upgrade process starts.

Upgrade a high availability pair from earlier releases to 12.1

For Citrix ADM servers in a high availability mode, you can upgrade by either accessing the active node or the load balancing virtual server IP address. Both the Citrix ADM servers are automatically upgraded to the latest build once you initiate the upgrade process in either of the servers.
Important

Points to note while upgrading Citrix ADM in a high availability mode

While upgrading Citrix ADM in high availability mode to 12.1 from an earlier release, the high availability connection is established internally by the “join HA” script that runs on the secondary node. The time taken for the upgrade process is dependent on the network infrastructure, the data present in the database, and the speed of the link. It might take a few hours to reestablish the connection between the two nodes. During this period, the primary node does not receive any heartbeat from the secondary node. You see a notification for missing heartbeat on the primary UI until the upgrade process gets completed. After the upgrade process is over, the secondary node restarts and the high availability deployment is complete.

Note

To know the status of upgrade, log on to each node using SSH, run the following commands and check the output:

```
pgrep -lf installmas
pgrep -lf maintenance
pgrep -lf join_streaming_replication
pgrep -lf pg_basebackup
```

If any of these commands shows a running process on any of the nodes, then the upgrade is in progress and should not be interrupted. Do not restart Citrix ADM during this time or do not try force failover on the secondary node.

After the upgrade process is complete, sometimes you might not be able to log on with the nsroot/nsroot or your user credentials. This is because the Citrix ADM subsystem has not completely restarted or migration might still be in progress. Do not restart Citrix ADM or do not attempt password recovery. This might have an undesired effect and the system might behave inconsistently. If required, you can try to log on using the nsrecover/<your_password_for_the_nsroot_user> credentials.

After the upgrade and before starting the operations, ensure that both the primary and the secondary nodes are upgraded and the reboot is complete.

Note

You cannot upgrade Citrix ADM in high availability mode using the CLI.

Pooled licensing in Citrix ADM servers in a high availability:

When Citrix ADM servers are deployed in a high availability mode, the license file is attached to the primary node and configured (node-locked) with the hostID or the MAC address of the primary server. Pooled licenses feature is now supported by Citrix ADM in high availability from 12.1 build onwards. To
configure pooled licensing feature on both nodes, you must have identical license files on both nodes. To install an identical license on the secondary node, you must rehost the license to the hostID (MAC address) of the secondary node.

Consider a scenario where the Citrix ADM has two server nodes S1 and S2 in high availability mode. The original license file, L1 is installed on server S1. The rehosted license file L2 should now be assigned to S2.

Follow the steps to upgrade Citrix ADM in high availability mode from 12.0 to 12.1 and configure pooled license feature:

1. Log on to the primary node of the Citrix ADM servers in high availability mode and perform the upgrade process.
2. Install the rehosted license file L2 on the secondary server node S2.
   At this time:
   • If S2 is the primary node, you can install the L2 license by accessing the GUI of that instance.
   • If S2 is the secondary node, you must manually perform a failover so that S2 now becomes the primary node. Install the license L2 on the new primary node by using the GUI. This is because you can access only the primary server in high availability through the GUI.
3. Configure the floating IP address on the new primary node.
4. Delete the license server IP addresses on the Citrix ADC instances and reconfigure them to use the floating IP address. Perform this on all Citrix ADC instances.

Citrix recommends that you perform Citrix ADM high availability pooled licensing upgrade by creating a maintenance window on the Citrix ADC instances. This is because removing the license server and adding floating IP address causes the Citrix ADC instances to move back temporarily to the minimum bandwidth support.

**High availability upgrade scenarios**

There might be two scenarios in which the Citrix ADM servers are deployed in high availability mode.

• The primary and secondary servers are deployed on the same subnet.
• The primary and the secondary servers are deployed in different subnets.

This upgrade document assists you in upgrading the Citrix ADM in both these scenarios.

• Upgrading a high availability setup on the same subnet
• Upgrading a high availability setup in different subnets
Upgrade a high availability setup on the same subnet

Upgrading of Citrix ADM servers deployed in high availability mode on the same subnet is handled automatically by Citrix ADM 12.1.

To upgrade Citrix ADM deployed in high availability mode on the same subnet:

1. Log on to the primary node and navigate to System > System Administrations.
2. Under System Administration, click Upgrade Citrix ADM.
3. If there is an error during upgrade, the following error message is displayed. Follow the instructions as mentioned in the message on the primary server.

![Error message](image)
4. As part of the upgrade process, you must perform clean-up procedure through the CLI. During the clean-up process, the secondary node becomes the primary node. The old primary node cannot be accessed through its GUI. Do not restart the old primary node as well as the new primary node while the clean-up process is in progress. After the clean-up process is complete, continue the upgrade procedure through the new primary node.

5. After the upgrade process is complete, the two nodes must synchronize their databases. The time taken for complete synchronization and the new secondary node to come up depends on the data present in the databases.

   **Note**

   After the upgrade is successful, you must configure the floating IP address using the Citrix ADM user interface.

6. To configure floating IP address, navigate to **System > Deployment > Configure Floating IP Address for High Availability Mode**.

7. Specify the floating IP address as shown in the following image and click **OK**.

   ![Configure Floating IP Address](Image)

**Upgrade a high availability setup in different subnets**

Upgrading of Citrix ADM servers deployed in high availability mode on different subnets must be handled by an administrator.

In this scenario, Citrix ADM HA node 1 (primary) is in subnet 1, and Citrix ADM HA node 2 (secondary) is in subnet 2.

**To upgrade Citrix ADM deployed in high availability mode on different subnets:**

1. Manually break the high availability setup. For more information, see [Disabling high availability](#).

2. Upgrade the Citrix ADM standalone node 1. For more information on how to upgrade Citrix ADM, see [Upgrade single Citrix ADM server](#).

3. Setup and register a new Citrix ADM standalone node 3 in subnet 1.
4. After registering node 1 and node 3, deploy both these nodes in high availability mode. For details see, Deploying the primary and secondary node as a high availability pair.

Note
Configuring the floating IP address is mandatory.

5. Delete the Citrix ADM node 2.

Upgrade a high availability pair from previous 12.1 versions to the latest version

You can upgrade Citrix ADM servers deployed in high availability from an earlier 12.1 build to a later 12.1 build.

To upgrade Citrix ADM deployed in high availability mode:

1. Download the Citrix ADM 12.1 build 49.37 image file from Citrix.com downloads page.
2. Log on to the primary node and navigate to System > System Administrations.
3. Under System Administration, click Upgrade Citrix ADM.
4. Navigate to the folder where the image is located.

While upgrading, do not make any configuration changes to either of the nodes.

Warning
• Do not refresh the browser until the upgrade process is successfully completed. It might take a few minutes for the upgrade process to finish.

After upgrade, the active node can change in a high availability pair.

Upgrade Citrix ADM disaster recovery deployment

Upgrading Citrix ADM disaster recovery deployment is a two-step process:

You must first upgrade the Citrix ADM nodes configured in high availability mode in the primary site. Later you must upgrade the disaster recovery node.

Ensure that you have upgraded the Citrix ADM servers that are deployed in high availability before upgrading the disaster recovery node.

• If you are upgrading the Citrix ADM servers in high availability mode from older releases to 12.1, see Upgrade a high availability pair from earlier releases to 12.1 in this document.

• If you are upgrading from an earlier 12.1 build to a later 12.1 build on the high availability pair, see Upgrade a high availability pair from previous 12.1 versions to the latest version in this document.
Upgrade the Citrix ADM disaster recovery node

1. Download Citrix ADM upgrade image file from Citrix download site.
2. Upload this file to the disaster recovery node using “nsrecover” credentials.
3. Log on to the disaster recovery node using the “nsrecover” credentials.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. Navigate to the folder where you placed the image file and unzip the file.
5. Run the following script:

   `./installmas`

Upgrade on-prem agents for multisite deployment

Upgrading Citrix ADM agent deployment is a three-step process. Ensure that you have completed the following tasks before upgrading the on-prem agents:

1. Upgrade the Citrix ADM servers that are deployed in high availability.
   - If you are upgrading the Citrix ADM servers in high availability mode from older releases to 12.1, see Upgrade a high availability pair from earlier releases to 12.1 in this document.
   - If you are upgrading from an earlier 12.1 build to a later 12.1 build on the high availability pair, see Upgrade a high availability pair from previous 12.1 versions to the latest version

2. Upgrade the Citrix ADM disaster recovery node.
   For more information, see Upgrade Citrix ADM disaster recovery deployment.

Upgrade the on-prem agent

1. Download Citrix ADM agent upgrade image file from Citrix download site.
2. Upload this file to Agent node using “nsrecover” credentials.
3. Ensure that you download the correct agent upgrade image. The image file name is of the following format:
4. Log on to the on-prem agent using the “nsrecover” credentials.

5. Navigate to the folder where you placed the image file and unzip the file.

   ```bash
   login as: nsrecover
   Using keyboard-interactive authentication.
   Password:
   Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
   bash-3.2# cd /var/mps/mps_images/
   bash-3.2# tar xzf build-masagent-12.1-502.109.tgz
   ```

6. Run the following script:

   ```bash
   ./installmasagent
   ```

---

**Remove support for the Advanced Backup and Restore feature of Citrix ADM**

Instead of using the advanced backup capability to take a complete backup of your Citrix ADM server, you can now use the new **Disaster Recovery** feature made available in Citrix ADM version 12.1 to take a complete backup of your Citrix ADM high availability setup and help with business continuity use cases.

**Important**

1. The advanced backup feature is no longer available after you upgrade to Citrix ADM 12.1. To remove the advanced backup feature, and to continue backing up using the Disaster Recovery feature, see Back up your Citrix ADM after upgrading to Citrix ADM 12.1. Disaster Recovery is supported only with Citrix ADM HA.

2. To continue to take a partial backup of the Citrix ADM server that includes the configuration files, instance details, system data, and so on and then, to restore your Citrix ADM server in a standalone deployment (partial backup), see How to back up and restore your Citrix ADM server in a single-server deployment.

In case of a disaster on the primary server, use the Disaster Recovery feature to start and configure Citrix ADM on the same primary server without losing data. The feature is only available on Citrix ADM servers deployed in a high availability setup from Citrix ADM version 12.1.

**Back up your Citrix ADM server after upgrading to Citrix ADM 12.1**

To continue to back up your Citrix ADM server Citrix recommends the following:
1. Delete your remote backup settings on Citrix ADM by doing the following:
   a) Navigate to **System > System Administration > Advanced System Backup Settings.**
   b) In the Configure Advanced Backup Settings page, select **No** to disable remote backups.
   c) Click **Apply Settings.** Please wait for your Citrix ADM server to reboot and apply the changed settings.
   d) Delete your remote backup node.
2. Deploy and configure a new Citrix ADM server, create a high availability setup with the existing Citrix ADM server that was rebooted in the step above.
   - To learn more about Citrix ADM standalone deployment see [Deploy Citrix ADM](#).
   - To learn more about Citrix ADM HA deployment see [High Availability deployment](#).
3. Configure Disaster Recovery to continue to backup and restore data. For more information about Disaster Recovery, see [Configure disaster recovery for high availability](#).

### Add an additional disk to the Citrix ADM server

If your Citrix ADM storage requirement exceeds the default disk space (120 gigabytes), you can attach an additional disk. You can attach additional disk in both single-server and high availability deployments.

When you upgrade Citrix ADM from release version 12.0 to 12.1, the partitions that you had created on the additional disk in the earlier version remain the same. The partitions are not removed nor are they resized.

The procedure to attach additional disk remains the same in the upgraded build. You can now use the new disk partitioning tool in Citrix ADM to create partitions in the newly added disk. You can also use tool to resize the partitions in the existing additional disk. For more information on how to attach additional disks and to use the new disk partitioning tool, see [How to attach an additional disk to Citrix ADM](#).

### Provision Citrix ADC instances in OpenStack using StyleBooks

From Citrix ADM 12.1 build 49.23 onwards, the architecture of OpenStack orchestration workflow has been updated. The workflow now uses Citrix ADM StyleBooks to configure Citrix ADC instances. If you are upgrading to Citrix ADM 12.1 build 49.23 from either version 12.0 or from version 12.1 build 48.18, you must run the following migration script:

```
mps/scripts/migration_scripts/migrate_configurations.py
```
Users can be authenticated either internally by Citrix Application Delivery Management (ADM), externally by an authenticating server, or both. If local authentication is used, the user must be in the Citrix ADM security database. If the user is authenticated externally, the user’s “external name” should match the external user identity registered with the authenticating server, depending on the selected authentication protocol.

Citrix ADM supports external authentication by means of RADIUS, LDAP and TACACS protocols. This unified support provides a common interface to authenticate and authorize all the local and external authentication, authorization and accounting (AAA) server users who are accessing the system. Citrix ADM can authenticate users regardless of the actual protocols they use to communicate with the system. When a user attempts to access a Citrix ADM implementation that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP or TACACS server for authentication. If the authentication is successful, the corresponding protocol is used to identify the user in Citrix ADM.

You can authenticate your users in Citrix ADM in two ways:

- By using Citrix ADM local servers
- By using external authentication servers

The following flow chart shows the workflow to follow when you are authenticating local or external users:
Configure external authentication servers

Citrix ADM supports various protocols to provide external Authentication, Authorization, and Accounting (AAA) services.

Citrix ADM sends all authentication, authorization, and accounting (AAA) service requests to the remote RADIUS, LDAP, or TACACS+ server. The remote AAA server receives the request, validates the request, and sends a response back to Citrix ADM. When configured to use a remote RADIUS, TACACS+, or LDAP server for authentication, Citrix ADM becomes a RADIUS, TACACS+, or LDAP client. In any of these configurations, authentication records are stored in the remote host server database. Login and logout account name, assigned permissions, and time-accounting records are also stored on the AAA server for each user.

Additionally, you can use the internal database of Citrix ADM to authenticate users locally. You create entries in the database for users and their passwords and default roles. You can also create groups of servers for specific types of authentication. The list of servers in a server group is an ordered list. The first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers of different types in a group, and you can also include the internal database as a fallback authentication backup to the configured list of AAA servers.
Configure a RADIUS authentication server

You can configure Citrix ADM to authenticate user access with one or more RADIUS servers. Your configuration might require using a network access server IP (NAS IP) address or a network access server identifier (NAS ID). When configuring Citrix ADM to use a RADIUS authentication server, use the following guidelines:

- If you enable use of the NAS IP address, the appliance sends its configured IP address to the RADIUS server, rather than sending the source IP address used in establishing the RADIUS connection.
- If you configure the NAS ID, the appliance sends the identifier to the RADIUS server. If you do not configure the NAS ID, the appliance sends its host name to the RADIUS server.
- If you enable the NAS IP address, the appliance ignores any NAS ID that is configured, and uses the NAS IP to communicate with the RADIUS server.

To configure a RADIUS authentication server:

1. In Citrix ADM, navigate to **System > Authentication > RADIUS**.
2. On the **RADIUS** page, click **Add**.
3. On the **Create RADIUS Server** page, set the parameters and click **Create** to add the server to the list of RADIUS authentication servers. The following parameters are mandatory:
   a) **Name**. Name of the RADIUS server.
   b) **Server Name / IP Address**. Server name or IP address of the RADIUS server.
   c) **Port**. By default, port 1812 is used for RADIUS authentication. You can specify a different port number if necessary.
   d) **Time-out (seconds)**. Time, in seconds, that the Citrix ADM system waits for a response from the RADIUS server.
   e) **Secret Key**. Any alphanumeric expression. This is the key that is shared between Citrix ADM and the RADIUS server to enable communication.
4. Click **Details** to expand the section and set the additional parameters, and then click **Create**.

For more details on how to add RADIUS servers, see [How to add RADIUS authentication servers](#).

Configure an LDAP authentication server

You can configure the Citrix ADM to authenticate user access with one or more LDAP servers. LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on Citrix ADM. The characters and case must also match.

To configure an LDAP authentication server:

1. In Citrix ADM, navigate to **System > Authentication > LDAP**.
2. On the **LDAP** page, click **Add**.

3. On the **Create LDAP Server** page, set the parameters and click **Create** to add the server to the list of LDAP authentication servers. The following parameters are mandatory:

   a) **Name**. Name of the LDAP server.

   b) **Server Name / IP Address**. Server name or IP address of the LDAP server.

   c) **Security Type**. Type of communication required between the system and the LDAP server. Select from the drop-down list. If plain text communication is inadequate, you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL.

   d) **Port**. By default, port 389 is used for LDAP authentication. You can specify a different port number if necessary.

   e) **Server Type**. Select **Active Directory (AD)** or **Novell Directory Service (NDS)** as the type of LDAP server.

   f) **Time-out (seconds)**. Time, in seconds for which the Citrix ADM system waits for a response from the LDAP server.

You can provide additional details. You can also validate the LDAP certificate by selecting the **Validate LDAP Certificate** check box and specifying the host name to be entered on the certificate. Some of the additional parameters you can add are Domain Nameserver (DN) details for queries against a directory service, default authentication group, group attributes, and other attributes.

The base DN is usually derived from the Bind DN by removing the user name and specifying the group to which the users belong. In Administrator Bind DN text box, type the administrator bind DN for queries to the LDAP directory.

Examples of syntax for base DN are:

- `ou=users,dc=ace,dc=com`
- `cn=Users,dc=ace,dc=com`

Examples of syntax for bind DN are:

- `domain/user name`
- `ou=administrator,dc=ace,dc=com`
- `user@domain.name` (for Active Directory)
- `cn=Administrator,cn=Users,dc=ace,dc=com`

The group name and the name of the users that you define in Citrix ADM must be similar to those configured on the LDAP server.
Note
While configuring a RADIUS or LDAP server, in the Details section, you can enter the name of a default authentication group. This default group is chosen to authorize the user when the authentication succeeds irrespective of the fact that the user is tied to a group or not. The user then receives a combination of permissions configured on this default group and the other groups whether the user is assigned to the group or not.

For more details on how to add LDAP servers, see How to add LDAP authentication servers.
For more details on how to cascade external auth servers, see How to cascade external authentication servers.

Configure a TACACS authentication server

TACACS, like RADIUS and LDAP, handles remote authentication services for network access.

Configure a TACACS authentication server:

1. In Citrix ADM, navigate to System > Authentication > TACACS.
2. On the TACACS page, click Add.
3. On the Create TACACS Server page, enter the following details:
   a) Name of the TACACS server
   b) IP address of the TACACS server
   c) Port and timeout (in seconds)
   d) The key that is shared by the system and the TACACS server for communication.
   e) Select Accounting if you want the appliance to log audit information with TACACS server.
4. Click Create.

For more details on how to add TACACS servers, see How to add TACACS authentication servers.

Note
To search for authentication servers added in Citrix ADM, click in the search bar and select the required search criteria.
Configure a local authentication of users in Citrix ADM

If you are using local authentication, create users and then add them to groups that you create on Citrix ADM. After configuring users and groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP address of file shares and servers to which users have access.

To configure a local authentication in Citrix ADM:

1. In Citrix ADM, navigate to System > Authentication, and click Authentication Configuration.
2. On the Authentication Configuration page, select LOCAL from the Server Type drop-down box, and click OK.

Configure an external authentication in Citrix ADM

When you configure external authentication servers in Citrix ADM, the user groups that are authenticated on those external servers are imported into Citrix ADM. You do not need to create users on Citrix ADM. The users are managed on the external servers from Citrix ADM. But you must ensure that the permission levels that the user groups have on the external authentication servers are maintained in Citrix ADM. Citrix ADM performs the authorization of users by assigning group permissions for access to specific load balancing virtual servers and to specific applications on the system. If an authentication server is later removed from the system, the groups and users will be automatically removed from the system.

To configure an external authentication in Citrix ADM:

1. In Citrix ADM, navigate to System > Authentication, and click Authentication Configuration.
2. On the Authentication Configuration page, select EXTERNAL from the Server Type dropdown list.

3. Click Insert.

4. On the External Servers page, select an authentication server. Optionally, you can select multiple authentication servers to cascade.

   **Note**
   Only external servers can be cascaded.

5. Select Enable fallback local authentication if you want the local authentication to take over if the external authentication fails.

6. Click OK to close the page.

   The selected servers are displayed on the Authentication Servers page.

   You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.

**Configure groups in Citrix ADM**

Citrix ADM allows you to authenticate and authorize your users by creating groups and adding the users to the groups. A group can have either “admin” or “read-only” permissions and all users in that group will receive equal permissions.

In Citrix ADM, a group is defined as a collection of users having similar permissions. A group can have one or multiple roles. A user is defined as an entity that can have access based on the permissions assigned. A user can belong to one or more groups.

You can create local groups in Citrix ADM and use local authentication for the users in the groups. If you are using external servers for authentication, configure the groups on Citrix ADM to match the groups configured on authentication servers in the internal network. When a user logs on and is authenticated, if a group name matches a group on an authentication server, the user inherits the settings for the group on Citrix ADM.

After you configure groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP addresses of file shares and servers to which the user has access.

If you are using local authentication, create users and add them to groups that are configured on Citrix ADM. The users then inherit the settings for those groups.

**Note**
If the users are members of an Active Directory group, the name of the group and the names of the users on Citrix ADM must be the same as in the Active Directory group.

To configure user groups in Citrix ADM:

1. In Citrix ADM, navigate to System > User Administration > Groups.

2. On the Groups page, click Add to create a group. By default, two groups are created in Citrix ADM, with permissions set to admin and read only. You can add your users to these groups, or you can create other groups for your users.

3. On the Group Settings tab on the Create System Group page, type the name of the group, and set Roles either as admin or read-only. You can select Configure User Session Timeout to set a timeout limit for the user sessions logged in for that group.

   Note

   Ensure that the name of the user group created on Citrix ADM is the same as as on the external authentication servers. If not, the system will not recognize the group, and the group members will not be extracted into the system.

4. In the Authorization Settings tab, select the required groups. Click Create Group.

5. In the Assign Users tab, select the users that you want to add to the group. The users are added to this table when you configure users in Configure Users in Citrix ADM.

6. Click Finish.

When you finish creating a group in the system, all the users in the external authentication server are extracted into the system. If the group name matches the group name on the external authentication server, the user inherits all the authorization definitions when logged on to the system.

Configure users in Citrix ADM

You can create user accounts locally on Citrix ADM to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server. If you are locally authenticating users that are present on external authentication servers, make sure that the same users are present on both the authenticating servers and Citrix ADM.

To configure users in Citrix ADM:

1. In Citrix ADM, navigate to System > User Administration > Users.

2. On the Users page, click Add to add users to Citrix ADM.

3. On the Create System User page, set the following parameters:
   a) User Name. Name of the user
b) **Password.** Password that the user will use to log on to Citrix ADM

c) **Enable External Authentication.** If this is not enabled, the user will be authenticated as a local user.

d) **Configure User Session Timeout.** Time for which a user can remain active. This time period can be set in minutes or hours.

4. In the **Groups** table, select the group to which to add the user. The group members are added to this table when you configure groups in Configuring User Groups in Citrix ADM.

5. Click **Create.**

**Note**

If the users are on Active Directory, make sure that the group name in Citrix ADM is same as the one for the Active Directory group on the external server.

---

**How to extract an authentication server group**

August 1, 2019

Citrix Application Delivery Management (ADM) allows you to extract the group of users existing on the external authentication server, and assign them permissions as their role demands and as per the Citrix ADC definitions. This has two advantages:

1. You do not have to create users on Citrix ADM. Though the groups are extracted into the Citrix ADM server, they are managed on the external servers from the Citrix ADM rather than adding them on the system.

2. Citrix ADM performs the authorization of users by assigning group permissions to access specific load balancer virtual servers, and for specific applications on the system. In future, when the particular authentication server is removed from the system, the groups and users will be automatically removed from the system.

**Configuring groups and assigning group permissions**

1. In Citrix ADM, navigate to **System > User Administration > Groups.**

2. Click **Add** to create a group.
3. In the **Group Settings** tab, type the name of the group, set the permissions as admin, read-only, appReadonly, or appAdmin. The other options that you can configure are session timeout, where you can set a timeout limit for the sessions logged in the users of that group, and you can also set the VM instances that can be accessed by the group members.

**Note**

Make sure that the name of the user group created on Citrix ADM is exactly the same as that created on external authentication servers. If not, the system will not recognize the group and the group members will not be extracted into the system.
4. In the **Authorization Settings** tab, you can provide authorization settings for the following four groups:
   - Instances
   - Applications
   - Configuration Templates
   - StyleBooks

   By default, your user can access all the above groups. You can clear the checkboxes and provide selective access for each of these groups.

   For example:
   - You can clear **Instances** checkbox and select only the required instances that you want to provide access to your users.
   - Clear **All Applications** checkbox and select only the required applications and templates. When you add applications to a group in Citrix ADM, you can use regex to search and add the applications that meet the regex criteria for the groups. The users who are bound to these groups can access only those specific applications. The regex expression specified is persisted in Citrix
ADM. That is, Citrix ADM allows the regex provided in the Add Regular Expression text box to be stored in the system and dynamically updates the authorization scope whenever new applications meet this regex expression. When new applications are added to the system, Citrix ADM applies the search criteria to the new applications, and the application that meets the criteria is dynamically added to the group. You do not have to manually add the new applications to the group. The applications are updated dynamically in the system, and the respective group users can see the applications under appropriate modules in Citrix ADM.

- Clear All Configuration templates checkbox to allow access to only the required templates.
- Clear All StyleBooks checkbox and select the required StyleBooks that your user can access.
- 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. The config packs of that StyleBook are also included in what the user has access to.

When you finish creating a group in the system, all the users in external authentication server are extracted into the system. You can check this by selecting the group and clicking Edit. The Users table in Create System Group displays the list of users connected with the group. You can also assign users to the group in the Assign users tab.

If the group name matches the group name on the external authentication server, the user inherits all of the authorization definitions when logged on to the system.

### How to add LDAP authentication servers

August 1, 2019
Citrix Application Delivery Management 12.1

The LDAP protocol that is integrated in Citrix Application Delivery Management (ADM) along with RADIUS and TACACS authentication servers, allows the system to search for user credentials from the distributed directories and authenticate the users.

**Configuring an LDAP authentication server**

1. In Citrix ADM, navigate to **System > Authentication > LDAP**.
2. On the **LDAP** page, click **Add**.
3. On the **Create LDAP Server** page, set the parameters and click **Create** to add the server to the list of LDAP authentication servers.
4. The following parameters are mandatory to create the LDAP server:
   - **Name** – type the name of the LDAP server.
   - **Server Name / IP Address** – type the Server Name or the IP address of the LDAP server.
   - **Security Type** – select the type of communication required between the system and the LDAP server from the drop-down list. Apart from plaintext communication you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL.
   - **Port** – by default, port 389 is used for LDAP authentication. You can specify a different port number, if required.
   - **Server Type** – select **Active Directory (AD)** or **Novell Directory Service (NDS)** as the type of LDAP server.
   - **Time-out (seconds)** – type the number of seconds. This is the time that the Citrix ADM system waits for a response from the LDAP server.

You can provide more optional details while creating an LDAP server. You can also validate the LDAP certificate by checking the box and specifying the host name to be entered on the certificate. Some of the additional parameters you can add are Domain Nameserver (DN) details for queries against a directory service, default authentication group, group attributes, and other attributes.
How to enable fallback local authentication

August 1, 2019

Fallback local authentication feature enables local authentication to take over if the external authentication fails. A user configured on both Citrix Application Delivery Management (ADM) and on an external authentication server can log on to Citrix ADM, even though the configured external authentication server is down or unreachable. For Fallback Local Authentication to work, make sure about these three factors:

- You should be able to access Citrix ADM even after external authentication server goes down.
- You should be configured on both Citrix ADM and the external authentication server.
- You should add at least one external server.

To enable Fallback Local Authentication, do the following:

1. In Citrix ADM, navigate to System > Authentication, and click Authentication Configuration.
2. Select EXTERNAL from the Server Type list.
   
   Note If you select LOCAL from the list, authentication of users happens at the default local authentication server.
3. Click Insert, select an external server from the list of external servers displayed, and click OK to add the external server.
   
   Note You should have already added the external servers before this step to make them appear in the list. For more information as to how to add external servers, see the following articles:
   - How to add Radius Servers
   - How to add LDAP Servers
   - How to add TACACS Servers
4. Select the Enable fallback local authentication option.
How to add RADIUS authentication servers

August 1, 2019

A RADIUS authentication server operates by using the User Datagram Protocol (UDP). The RADIUS server receives a user’s connection request, authenticates the user. The server then returns the configuration information to the system that delivers services to the user. The RADIUS server is connected to a network access server (NAS). When the NAS sends an Access-Request, the RADIUS server searches its database for the user name and other details. If the user name does not exist in the database, the RADIUS server immediately sends an Access-Reject message, or it can load a default profile on Citrix ADM. In RADIUS, authentication and authorization are coupled together. If the user details are authenticated, the RADIUS server returns an Access-Accept response. It also sends a list of attribute-value pairs that describe the parameters to be used for that particular session.
Configuring a RADIUS authentication server

1. In Citrix ADM, navigate to System > Authentication > RADIUS.
2. On the RADIUS page, click Add.
3. On the Create RADIUS Server page, set the parameters, and click Create to add the server to the list of RADIUS authentication servers.
4. The following parameters are mandatory to create the RADIUS server:
   - **Name** – type the name of the RADIUS server
   - **Server Name / IP Address** – type the Server name or the IP address of the RADIUS server
   - **Port** – by default, port 1812 is used for RADIUS authentication messages. You can specify a different port number, if necessary.
   - **Time-out (seconds)** – type the number of seconds. The time that the Citrix ADM system waits for a response from the RADIUS server.
   - **Secret Key** – type any alphanumeric expression. The key that is shared between the Citrix ADM and the RADIUS server for communication.
5. Click Details to expand the section and set the additional parameters.
You can provide more optional details while adding a RADIUS server. Some of the additional parameters you can enter are NAS details, vendor information, attribute information, and type of password authentication.

**Note**

For RADIUS authentication to work, ensure that the group configured on Citrix ADM and the group extracted through the RADIUS user is the same. The user is authorized based on the permissions assigned to the group.

For example, consider a scenario in FreeRADIUS server, where,

- Cleartext-Password = “1.citrix”
- Group-Names = “radiusgroup1, group1”
In this case, the user belongs to two groups - radiusgroup1 and group1. The group separator in this case is ",,"

If you are logging on Citrix ADM as a RADIUS user “RadiusUser1” who belongs to group “radiusgroup1,” ensure that the same group name “radiusgroup1” is configured on Citrix ADM as well.

Provide the details regarding the vendor ID, attribute type, group separator (if applicable) for the group extraction to happen as shown in the following image.

```
# Created for Citrix Use
# currently only using attribute 6 in this setup.
VENDOR Citrix 66
BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```
How to add TACACS authentication servers

August 1, 2019

TACACS, along with RADIUS and LDAP, handles remote authentication services for network access.

Configuring a TACACS authentication server

1. In Citrix ADM, navigate to System > Authentication > TACACS.
2. On the TACACS page, click Add.
3. On the Create TACACS Server page, enter the following details:
   a) Name of the TACACS server
   b) IP address of the TACACS server
   c) Port and timeout in seconds
   d) Type the key that is shared by the system and the TACACS server for communication.
4. Select Accounting if you want the appliance to log audit information with the TACACS server.
5. Click Create.
How to cascade external authentication servers

August 1, 2019

A Citrix Application Delivery Management (ADM) supports a unified system of authentication, authorization, and accounting (AAA) protocols, including RADIUS, LDAP, and TACACS, in addition to supporting local servers for authenticating local users and groups. The unified support provides a common interface to authenticate and authorize all of the local and external AAA clients who are accessing the system. Citrix ADM can authenticate users regardless of the actual protocols they to communicate with the system.

Cascading external authentication servers provides a continuous non-failing process for authenticating and authorizing external users. If authentication fails on the first authentication server, Citrix ADM
Citrix Application Delivery Management 12.1

attempts to authenticate the user by using the second external authentication server, and so on. To enable cascading authentication, you need to add the external authentication servers to Citrix ADM. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS). For example, if you want to add four external authentication servers for cascading authentication, you can add two RADIUS servers, one LDAP server, and one TACACS server, or all servers can be of RADIUS type. You can configure up to 32 external authentication servers in Citrix ADM.

Configuring cascading external authentication servers

1. In Citrix ADM, navigate to System > Authentication.
2. On the Authentication page, click Authentication Configuration.
3. On the Authentication Configuration page, select EXTERNAL from the Server Type drop-down list (only external servers can be cascaded).
4. Click Insert, and on the External Servers page, select one or multiple authentication servers that you would like to cascade.
5. Select Enable fallback local authentication if you want the local authentication to take over if the external authentication fails.
6. Click OK to close the page.

The selected servers are displayed under External Servers as shown in the figure below. You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.
Access control

August 1, 2019

Authentication is a process by which you verify that someone is who they claim they are. In order to perform authentication, a user must already have an account created in a system which can be interrogated by the authentication mechanism, or an account must be created as part of the process of the very first authentication. Citrix Application Delivery Management (ADM) provides a method for authenticating both local users and external users. While local users are authenticated internally, Citrix ADM supports external authentication by means of RADIUS, LDAP and TACACS protocols. When a user attempts to access Citrix ADM that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. Once authenticated, the required protocol is used to identify the user on Citrix ADM.

Access Control is the process of enforcing the required security for a particular resource. It is a security technique that can be used to regulate who can view or use resources in a computing environment. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control through a reference monitor. Citrix ADM allows fine-grained, role-based access control (RBAC) by which the administrators can provide access permissions to users based on the roles of individual users within an enterprise. RBAC in Citrix ADM is achieved by creating access policies, roles, groups, and users.

Role-based access control

August 1, 2019

Citrix Application Delivery Management (ADM) provides fine-grained, role based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise. In this context, access is the ability to perform a specific task, such as view, create, modify, or delete a file. Roles are defined according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and assist in creating configuration templates.

Roles are determined by in policies. After creating policies, you create roles, bind each role to one or more policies, and assign roles to users. You can also assign roles to groups of users.
A group is a collection of users who have permissions in common. For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users or groups on the basis of specific conditions. In Citrix ADM, creating roles and policies is 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 should have read-only access for system administration operations. An application administrator should be able to access only the resources within his or her scope.

**Example:**

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 should 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, external, or a multi-tenant.

Citrix ADM users may be locally authenticated or may be authenticated through an external server (RADIUS/LDAP/TACACS). RBAC settings must be applicable to all users irrespective of the authentication method adopted.

The following image shows the permissions that the administrators and other users have and their roles in the organization.
Limitations

RBAC is not fully supported for the following Citrix ADM features:

- **Analytics** - RBAC is not supported fully in the analytics modules. RBAC support is limited to instance level, and it is not applicable at application level in the Web Insight, SSL Insight, Gateway Insight, HDX Insight, and Security Insight analytics modules. For example:

**Example 1**: Instance based RBAC (Supported)

An administrator who has been assigned a few instances can see only those instances under **Web Insight > Instances**, and only the corresponding virtual servers under **Web Insight > Applications**, because RBAC is supported at instance level.

**Example 2**: Application based RBAC (Not Supported)

An administrator who has been assigned a few applications can see all virtual servers under **Web Insight > Applications** but cannot access them, because RBAC is not supported at applications level.

- **StyleBooks** – RBAC is not fully supported for StyleBooks.

  - In Citrix ADM, Stylebooks and configuration packs are considered as separate resources. Access permissions, either view, edit, or both, can be provided for Stylebook and configu-
ration packs separately or concurrently. A view or edit permission on configuration packs implicitly allows the user to view the StyleBooks, which is essential for getting the config-pack details and creating new configuration packs.

- Access permission for specific Stylebook or configuration packs is not supported
  Example: If there is already a configpack on the instance, users can modify the configuration on a target Citrix ADC instance even if they don’t have access to that instance.

- **Orchestration** - RBAC is not supported for Orchestration.

Configure access policies

August 1, 2019

Access policies define permissions. A policy can be applied to a single user or group, or to multiple users and multiple groups. Citrix Application Delivery Management (ADM) provides four predefined access policies:

1. **adminpolicy**. Grants access all Citrix ADM features. 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 perform add, modify, and delete operations on the resources.

2. **readonlypolicy**. Grants read-only permissions. The user can view all content on Citrix ADM, but is not authorized to perform any operations.

3. **appAdminPolicy**. 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, cache redirection, and HAProxy virtual servers.

4. **appReadOnlyPolicy**. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.

**Note** The predefined policies cannot be edited.

You can also create your own (user-defined) policies.

**To create user-defined access policies:**

1. In Citrix ADM, navigate to **System > User Administration > Access Policies**.

2. Click **Add**.

3. In the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.
4. The **Permissions** section lists all Citrix ADM features, with options for specifying read-only or edit access. Click the (+) icon to expand each feature group into multiple features. You must select the check box next to the feature name to give the users either the View or Edit Permissions. The Edit option includes permission to view. Select **View** for read-only, or **Edit** for full access.

   - **Note**: Expand Load Balancing and GSLB to view more configuration options.
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.

Example:

David is the administrator for SSL certificate management/security in Citrix ADM. In the policy assigned to David, the administrator selects the following check boxes in the Permissions section:

- **Networks > Configuration > Edit**
- **Networks > Certificate Management > Edit**
- **System > SSL Settings > Edit**
- **System > System Configuration > Edit**

5. Click Create.
Configure groups

August 1, 2019

In Citrix Application Delivery Management (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 to 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.

To create user groups and assign roles to user groups:

1. In Citrix ADM, navigate to System > User Administration > Groups.
2. Click Add.
3. In the Group Name field, enter the name of the group.
4. In the Group Description field, type in a description of your group. Providing a good description of the group helps you to understand the role and function of the group in a better way at a later point.
5. In the Roles section, add or move one or more roles to the Configured list.

   Note Under the Available list, you can click New or Edit and create or modify roles. Alternatively, you can navigate to System > User Administration > Users and create or modify users.
6. Click **Next**. On the **Authorization Settings** tab, you can provide authorization settings for the following four groups:

- Instances
- Applications
- Configuration Templates
- StyleBooks

By default, your user can access all the above groups. You can clear the check boxes and provide selective access for each of these groups.

For example:

- You can clear **Instances** check box and select only the required instances that you want to provide access to your users.
- Clear All Applications check box and select only the required applications and templates. When you add applications to a group in Citrix ADM, you can use regex to search and add the applications that meet the regex criteria for the groups. The users who are bound to these groups can access only those specific applications. The regex expression specified is persisted in Citrix ADM. That is, Citrix ADM allows the regex provided in the Add Regular Expression text box to be stored in the system and dynamically updates the authorization scope whenever new applications meet this regex expression. When new applications are added to the system, Citrix ADM applies the search criteria to the new applications, and the application that meets the criteria is dynamically added to the group. You do not have to manually add the new applications to the group. The applications are updated dynamically in the system, and the respective group users can see the applications under appropriate modules in Citrix ADM.

When you add applications to a group in Citrix ADM, you can use regex to search and add the applications that meet the regex criteria to the groups. The users who are bound to these groups can access only those specific applications. The regex expression specified is persisted in Citrix ADM. That is, Citrix ADM allows the regex provided in the Add Regular Expression text box to be stored in the system and dynamically updates the authorization scope whenever new applications meet this regex expression. When new applications are added to the system, Citrix ADM applies the search criteria to the new applications, and the application that meets the criteria is dynamically added to the group. You do not have to manually add the new applications to the group. The applications are updated dynamically in the system, and the respective group users can see the applications under appropriate modules in Citrix ADM.

- Clear All Configuration templates check box to allow access to only the required templates.

- Clear All StyleBooks check box and select the required StyleBooks that your user can access.

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. The config packs of that StyleBook are also included in what the user has access to.
7. Click Create Group.

8. In the Assign Users tab, select the user from the Available list and add the user to the Configured list. For example, “dadmin”.

   **Note** You can also add new users by clicking New.

9. Click Finish.

   **Note**

   As a Citrix ADM admin, you can provide either “view-only” permission or “view and edit” permission to your users for individual ADM module UIs based on access policy settings in RBAC. If the user is assigned to two or more groups, that is, if the user is internally mapped to more than one authorization scope and more than one access policy, ADM takes a union of all those groups’ permissions and authorizes the user accordingly.

   For example, consider that User1 is assigned to a group that has two access policies, P1 and P2. Each policy has a different type of permission. P1 has “read-only” permission, while P2 has “view and edit” permission. You want your user to view a set of applications as part of the P1 policy, and edit a different set of applications as part of the P2 policy. But as a default behavior, Citrix ADM combines the two permission types and assigns the “view and edit” permission to the user. So your user will now be able to view and edit all the applications.

   ADM doesn’t support such use cases where you can assign different types of permissions to the same user. You can assign only one type of permission to your users. ADM can either allow User1 to view all apps or a selected set of apps, or allow User1 to view and edit all apps or selected set of apps.
Mapping of RBAC when upgrading Citrix ADM from 12.0 to 12.1

When you upgrade Citrix ADM from 12.0 to 12.1, you do not see the options to provide “read-write” or “read” permissions while creating groups. These permissions have been replaced by “roles and access policies,” which give you more flexibility to provide role-based permissions to the users. The following table shows how the permissions in release 12.0 are mapped to release 12.1:

<table>
<thead>
<tr>
<th>12.0</th>
<th>Allow Applications Only</th>
<th>12.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin read-write</td>
<td>False</td>
<td>admin</td>
</tr>
<tr>
<td>admin read-write</td>
<td>True</td>
<td>appAdmin</td>
</tr>
<tr>
<td>admin read-only</td>
<td>False</td>
<td>readonly</td>
</tr>
<tr>
<td>admin read-only</td>
<td>True</td>
<td>appReadonly</td>
</tr>
</tbody>
</table>

Configure roles

August 1, 2019

In Citrix Application Delivery Management (ADM), each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add Citrix ADC instances in Citrix ADM, and the other policy might grant permission to create and deploy StyleBooks and to configure Citrix ADC instances.

When multiple policies define edit and read-only permissions for a single feature, the edit permissions have priority.

Citrix ADM provides four predefined roles:

- **admin.** Has access to all Citrix ADM features. (This role is bound to adminpolicy.)
- **readonly.** Has read-only access. (This role is bound to readonlypolicy.)
- **appAdmin.** Has administrative access to only the application features in Citrix ADM. (This role is bound to appAdminPolicy).
- **appReadonly.** Has read-only access to the application features. (This role is bound to appRead-OnlyPolicy.)
**Note** The predefined roles cannot be edited.

You can also create your own (user-defined) roles.

**To create roles and assign policies to them:**

1. In Citrix ADM, navigate to **System > User Administration > Roles**.
2. Click **Add**.
3. In the **Role Name** field, enter the name of the role, and provide the description in the **Role Description** field (optional.)
4. In the **Policies** section, add or move one or more policies to the **Configured** list.
5. Click **Create**.

Configure users

August 1, 2019
By default, Citrix Application Delivery Management (ADM) has one user:

nsroot - The root user (nsroot) has full administrative privileges on the appliance. The nsroot user is the super admin of Citrix ADM.

You can create additional users by configuring accounts for them. When you add new users to Citrix ADM, you can define their permissions by assigning the appropriate groups, roles, and policies.

You can assign a user to a group and bind the group to roles. You can define one-to-one, one-to-many, or many-to-many relationship between users, groups, roles, and access policies. A user can be assigned to multiple groups. A group can have multiple roles, and multiple groups can have identical roles.

To configure users in Citrix ADM:

1. In Citrix ADM, navigate to System > User Administration > Users.
2. Click Add.
3. Enter the following details:
   a) **User Name**. Name of the user
   b) **Password**. Password with which the user logs on to Citrix ADM
4. Optionally, select **Enable External Authentication**, so that the user can be authenticated through an external authentication server.
5. If you have created groups and want to assign the user to a group, in the **Groups** section, move one or more groups from the **Available** list to the **Configured** list.
6. Click **Create**.

Multi-tenancy: Provide exclusive management environment to your tenants

August 1, 2019

Citrix Application Delivery Management (ADM) provides multi-tenancy functionality where you can configure the system for multiple tenants. Each tenant can add their network instances, manage, and monitor these instances and applications, and create their own users and groups. No tenant has visibility into the instances and applications of the other tenants. Only the system admin has visibility into all instances, applications, and reports of all tenants. However, the system admin cannot create users for the tenants. All system-level tasks can be performed only by the system admin.

Consider a scenario where an organization such as example.com has an infrastructure group and multiple business units within it. They want to centrally manage all instances in their network. However,
they want to provide exclusive environment to each business unit.

The following image shows how the example.com organization infrastructure group is structured. They want each of the four business units to have exclusive management environments. This image also shows the number of instances each business unit wants to manage.

Chris, the ADC group head, is the system admin of Citrix ADM. Chris creates two tenants for the two business units, Example-online and Example-Retail, and assigns two users as administrators of these tenants. Each tenant administrator can now add more users, add instances they want to manage, and create sub-tenants within their tenant environment.

The following image shows the tenants and users that are created in Citrix ADM for this example.
**Add tenants**

In this example, Chris, the system admin creates two tenants: example-online and example-retail. While creating the tenants, Chris also creates a default admin user for each tenant.

**To add tenants**

1. Navigate to **System > Tenants**, and click **Add**.

2. On the **Create Tenant** page, specify the tenant name and the tenant user name whom you want to assign as the administrator for this tenant. Also, provide the password.

3. Click **Create**.
On the Tenants page, you can view the list of tenants that are created.

You can also view the list of admin users for each tenant on the System > User Administration > Users page.
When you create the tenants, two default system groups are created, admin group and read-only group for each tenant as shown in the image below. For example, example-online_admin_group and example-online_readonly_group are created for tenant example-online.

Log on to Citrix ADM as a tenant user

After the tenants are created, a tenant user can log on to Citrix ADM using the tenant user credentials. To do so, a tenant has to provide both the domain name and the user name, for example, example-online\John.
Add instances as a tenant user

After a tenant logs on, Citrix ADM prompts the tenant to add instances. Click + New to add the instances you want to manage. Alternatively, you can click Do it Later and add the instances at a later time from the Infrastructure tab. For details, see Adding an Instance to Citrix ADM.

In this example, John adds two Citrix ADC SDX instances.

Specify the instance type, the IP addresses (separated by comma), and the profile name that Citrix ADM can use to access the instances, and then click OK.
Create a user

John, the tenant admin, now wants to create a user for David so that David can monitor all the instances and applications of this tenant. However, Chris does not want David to perform any configuration task on the instances or change any system settings for the tenant. So, Chris creates a user david with readonly permissions.

To create a user:

1. Navigate to System > User Administration > Users and click Add.
2. On the Create System User page, specify the user name and password for the user you want to create.
3. Under Groups, select the group you want to assign to this user. In this example, the example-online_readonly_group is assigned to user david.

© 1999-2019 Citrix Systems, Inc. All rights reserved.


Create tenants within tenants

A tenant administrator can create sub-tenants if he wants to partition his tenant further. However, he can create only one level of sub-tenants. In this example, John creates two sub-tenants, example-digital and example-ecommerce. While creating these two sub-tenants, Chris assigns Jane and Mike as the admin user respectively.

To create a tenant within a tenant, follow the steps described in Add Tenants.

You can view the tenants created on the Tenants page.

You can also view the permissions assigned to the users. Navigate to System > User Administration > Users, select a user, and click Edit.

On the Configure System User page, under Groups, you can view the groups assigned to that user. In this example, you can see that example-digital_admin_group is assigned to Jane.
As a tenant admin if you have already added instances to Citrix ADM, you can assign the instances to users in your tenant or sub-tenants for management and monitoring. For example, John can assign one VPX instance to Jane for management purposes.

1. Navigate to **System > User Administration > Group**.

2. Select the group to which the user is assigned and click **Edit**.

3. On the **Modify System Group** page, on the **Authorization Settings** tab, clear the **All Instances** check box.
4. Select the instances that you want the user to manage and then click **Select Instances**.

5. Click **Next** and then click **Finish**.

**Applications**

August 1, 2019

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 health score of applications, helps you determine the security risks, and helps you detect anomalies in the application traffic flows and take corrective actions.

The following illustration provides an overview of the various tasks you can perform for Application Management and Analytics:
Applications can be either discovered applications, HAProxy applications or custom applications.

**Discovered applications**

Applications that are created automatically for every managed virtual server. Discovered applications will always have one virtual server, and these applications can not be edited or deleted directly.

**Custom applications**

Applications created by users from discovered applications. Citrix ADM allows you to add, edit, and delete these applications. Custom applications are created by:

- One or more virtual servers
- One or more HAProxy frontends.

When you create a custom application, all the discovered applications added to the custom application are removed from the app dashboard.

**Points to note**

- You cannot add a discovered application across multiple custom applications.
- You cannot create a custom application if all the discovered applications are already assigned to other custom application. You need to delete an existing custom application to free up the discovered applications for further composition of new custom applications.
• You cannot create a custom application containing virtual servers and HAProxy frontends.

**HAProxy applications**

HAProxy discrete applications are created automatically for every managed HAProxy frontend. You can also group these applications to form custom applications similar to Citrix ADC applications. For more information, see Managing and Monitoring HAProxy Instances with Citrix ADM.

**Points to note**

The following App Dashboard features or metrics are not supported for HAProxy applications:

- App Activity investigator
- App Score
- Threat Index
- Peak Usage trend
- Throughput
- Server Connections
- Transactions

**Creating a custom application**

You can create custom applications by adding one or more discovered applications while defining an application.

**To create a custom application:**

1. Navigate to Applications > Dashboard, and click Define Custom App.
2. On the Define Application Screen, set the following parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the custom application</td>
</tr>
<tr>
<td>Category</td>
<td>Name of the category for which all the applications related to that category will be grouped together on the application dashboard.</td>
</tr>
</tbody>
</table>
Field Description

Select Existing Applications Option to add virtual servers if the definition criteria are based on the licensed virtual servers monitored by Citrix ADM.

Define Selection Criteria Option to define application by virtual server range, or by origin server/service IP address range.

- **Server.** You specify the server or service IP address, server name, or the port of the backend server on which the applications are running. You can enter one IP address, a range of IP addresses, or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

- **Virtual Servers.** You can specify either one of the following: the virtual server IP address, virtual server name, or the port of the backend server on which the applications are running. You can enter one IP address or a range of IP addresses or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

3. Click OK.

**Note**

Currently, Application Dashboard supports only load balancing and content switching virtual servers.
Grouping your applications enables you to manage and monitor them with ease. You can group your applications by selecting or creating a category when defining an application. To create or select the category, while defining the application, click on the > button next to the Category field.

Applications that are not added to any category are displayed under Others category.
Application dashboard

The Application Dashboard provides a holistic view of all the applications monitored by Citrix ADM and provides key information related to all the applications. For example, the dashboard displays performance and security metrics, counters, and the health status of the applications. To display information about a particular application, select the application. And in the Summary panel, bar graphs show metrics such as app score and threat indexes, for all monitored applications.

View your applications

The application dashboard displays applications as nodes on a treemap, which are sized according to the data volume of the application. The color of a tile indicates the application's app score, with red denoting minimal health and blue denoting good health.

You can switch your application dashboard view to treemap or tiles by selecting one of the options from the application dashboard screen, wherein you can see the applications' details in the form of cards. By default, 250 applications are displayed on the application dashboard, to view more applications, click the next page option.

Applications are grouped by the categories that were selected when the applications were defined. Applications can be sorted or made visible by selecting application metrics from the application summary panel. For example, if you want to show the applications that have a app score in the range...
20-40, select the appropriate bar graph from the App Score section of the App Summary Panel. Similarly, you can select other metrics in the App Summary Panel.

**App summary panel**

The App Summary Panel displays all the metrics of the applications that are visible on the application dashboard. This panel enables you to sort and view the applications on the dashboard by selecting or deselecting application metrics. The App Summary Panel displays the following metrics:

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Family</td>
<td>A bar graph that groups the number of applications depending on the type of Citrix ADC instances on which they are configured.</td>
</tr>
<tr>
<td>App Score</td>
<td>A scoring system that defines how an application is performing</td>
</tr>
<tr>
<td>App Category</td>
<td>A bar graph that displays a histogram for all categories defined in Citrix ADM. All discrete applications now appear under; “Others” category, and custom applications appear under their respective category names.</td>
</tr>
<tr>
<td>Virtual Server Health</td>
<td>A bar graph that displays the number of applications under each category. The applications are categorized to have a health score value at 0%, 20%, 40%, 60%, 80% and 100%.</td>
</tr>
<tr>
<td>Data Volume</td>
<td>A scoring system that groups the number of applications depending on the data volume of the application. Data volume is calculated by the total number of bytes requested by the applications and the number of bytes received as responses from the applications.</td>
</tr>
<tr>
<td>Threat Index</td>
<td>A single-digit rating system that indicates the criticality of attacks on the application, regardless of whether or not the application is protected by a Citrix ADC appliance.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Descriptions</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Safety Index</td>
<td>A single-digit rating system that indicates how securely you have configured</td>
</tr>
<tr>
<td></td>
<td>the Citrix ADC instances to protect applications from external threats and</td>
</tr>
<tr>
<td></td>
<td>vulnerabilities.</td>
</tr>
<tr>
<td>Total Attacks</td>
<td>The total number of attacks against the applications.</td>
</tr>
<tr>
<td>Transactions</td>
<td>The range of transactions performed by the applications.</td>
</tr>
<tr>
<td>Client Connections</td>
<td>The number of client connections established by the applications.</td>
</tr>
<tr>
<td>Server Connections</td>
<td>The number of server connections established by the applications.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>The number of packets sent by the applications.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>The number of packets that are received by the applications.</td>
</tr>
<tr>
<td>Application Class</td>
<td>A bar graph that groups the number of applications depending on whether</td>
</tr>
<tr>
<td></td>
<td>they are discrete or custom applications.</td>
</tr>
</tbody>
</table>
For example, in the app summary panel, scroll down to find “Virtual Server Health” bar graph. In virtual server health bar graph, Citrix ADM classifies applications based on the percentage of the virtual server health. The bar graph displays the number of applications that have the health value of the virtual servers between 0% to 100%.

Virtual server health represents health of virtual servers that are grouped under discrete applications. But if there are custom applications that comprise two or more virtual servers, the least virtual server health is considered among the group.

You can now apply a filter and see only those applications in the application dashboard that match the selection criteria. Click the bar that says 0%. This bar displays the number of applications that have a virtual server health between 0% and 20%. You can now segregate applications that have low virtual server health and take remedial measures.

**App info panel**

The App Info panel is at the first level when you drill down on an application. It displays the key metrics and components of the application, along with its state. For example, for any selected application, the App Info panel shows the total number of virtual servers, total number of services, app score, and other information. To show the app info panel, click any application tile on the application dashboard. The App Info panel then replaces the App Summary panel.

![App Info Panel](image)

**App activity investigator**

The App Activity Investigator is one of the second level when you drill down from an application. You can reach the App Activity Investigator by selecting the search icon on the App Info panel, or by double-clicking the application tile on the Application Dashboard.
The App Activity Investigator displays key information such as App Score components, Errors, Events, and Anomalies.

Each of the legends are aggregated at one minute interval if the selected duration is one hour, and at one hour interval if the selected duration is one day.

These deviations are displayed as rectangular legends on the graph. These legends are aggregated, and are color coded according to the number of events that have occurred. Blue denotes the lowest number of events and red the maximum. You can hover your mouse pointer on a legend to show details such as error type, time, and the number of events aggregated for the selected legend. You can customize the time period of the graph by selecting the time from time-period drop down.

**App usage trend**

In most cases, you as a business owner make decisions on your application effectiveness and usage trends based on statistics and data. To understand the application usage trend, you have to collate information from multiple entities in your deployment, such as, backend infrastructure, proxies, CDN networks and so on. Then, correlate the collected information to get proper analytics, this consumes lot of time.

Instead, the Citrix ADC appliance deployed as an ADC in your deployment contains all the information about the application and the usage statistics of the application. You can forward this information to Citrix ADM. Citrix ADM collects this information and provides detailed insights about the application usage and performance. You can use these insights to take effective decisions based on the application usage and performance.
The App Info Panel in the Application Dashboard provides the peak usage trend of an application. You can use the peak usage trend to assess the performance of the application and take appropriate action to improve the performance of the application.

To view the peak usage trend of an application, navigate to Applications > App Dashboard. Select the application and the peak usage trend of the application is displayed under Peak Usage section in the App Info Panel.

You can further click on the Peak Usage section to view the App Score and the application usage. Using this information, you can identify the peak usage of the application and associate it with the corresponding App Score to assess the performance impact on the application during the peak usage duration.
Citrix ADM allows you to take a snapshot of the current App Dashboard and App Security Dashboard pages and export them as reports. At a frequent interval of time, the App administrators might need to use these reports to update on app usage and performance penalties.

With this feature, the administrators are able to extract this data as .png or .pdf reports.

**Note**

Unlike other report export options in Citrix ADM, you can export the App Dashboard and Security Dashboard reports only as .pdf or .png files. Other options such as, .jpg and .csv are not supported currently.

1. On the Application Dashboard or App Security Dashboard page, click the export icon at the top right side of the page.
2. Choose the export option as either .pdf or .png file.
3. Click OK.

The report downloads onto your system. From the App Dashboard and App Security Dashboard pages, you can also navigate to second-level pages and export them as reports. Currently, you can download reports of only one application at a time.

Application performance analytics

August 1, 2019

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, and has all systems up and running. App Score is displayed at the application level. Calculation of the score is based on the following three key components:

- **App Performance Score (APDEX score of the application).** Derived from the server response time variation of the application.

- **Citrix ADC System Resource.** Derived based on three more components:
  - CPU Usage
  - Memory Usage
  - NIC Card Saturation

- **App Server Resource.** Derived from two more components:
  - Percentage of Active Services
  - Surge Queue Requests

App Score is calculated from these scores where, Citrix ADC System Resource Score and App Server Resource Score is subtracted from App Performance score. App Score is available for all the applications which are defined with load balancing and content switching virtual servers that are discovered as well as the custom applications you define on the application dashboard.

To configure app score in Citrix ADM:

1. In Citrix ADM, navigate to Analytics > Settings.
2. On the Settings page, click Configure App Score.
3. On the Configure App Score page, enter the values for the following parameters:
   a) **Lower Surge Queue Threshold.** The lower threshold value of the ratio of the total number of connections that are pending submission for the virtual server and the established connections.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
b) **Higher Surge Queue Threshold.** The higher threshold value of the ratio of the total number of connections that are pending submission for the virtual server and the established connections.

c) **Low CPU Threshold (%)**. The lower threshold value of the total CPU usage in the Citrix ADC instance.

d) **High CPU Threshold (%)**. The higher threshold value of the total CPU usage in the Citrix ADC instance.

e) **Low Memory Threshold (%)**. The lower threshold value of the total memory usage in the Citrix ADC instance.

f) **High Memory Threshold (%)**. The higher threshold value of the total memory usage in the Citrix ADC instance.

g) **Low NIC Discards**. The lower threshold value of packets discarded by the interfaces.

h) **High NIC Discards**. The higher threshold value of packets discarded by the interfaces.

i) **Response Time**. The time interval between sending a request packet and receiving the first response packet from the service configured on the virtual server. Default value configured in Citrix ADM is 500 ms.

j) **Active Services Threshold**. The threshold value of the percentage of services that must be active which are bound to the virtual server.
4. Click **OK**.
Application security analytics

August 1, 2019

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.

**Note**

To view the metrics of the App Security Dashboard, AppFlow for Security insight should be enabled on the Citrix ADC instances that you want to monitor.

**To view the security metrics of a Citrix ADC instances on app security dashboard:**

1. In a web browser, type the IP address of the Citrix Application Delivery Management (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Applications** > **App Security Dashboard**, and select the instance IP address from the **Devices** drop-down list.

You can further drill-down on the discrepancies reported on the App Security Investigator by clicking on the bubbles plotted on the graph.

Create an application definition

August 1, 2019

You can define a custom application based on a collection of discovered applications in Citrix ADM. In Citrix ADM, when you navigate to **Application Dashboard**, the **Application Overview** page displays default applications. These default applications or “discrete applications” are the 30 applications for which you have the default licenses. You discover these applications when you install Citrix ADM in your business environment.

As you create “custom applications,” the custom applications replace the discrete applications. The custom applications are arranged on the dashboard according to the category you have chosen while creating them.

You can view these applications, both discovered and custom, in two ways - treemap and tiles.
You can create a custom application through either a static or dynamic configuration.

1. **Static Definition of Applications** - In a static definition, you can define an application. This definition does not get updated when new virtual servers are configured on your Citrix ADC instance. You must manually update this list to include more virtual servers.

2. **Dynamic Definition of Applications** - In a dynamic definition, you can use one of the three criteria listed below to define an application:
   
   a) **Servers**. Specify the server or service IP address, server name, or the port of the backend server on which the applications are running. You can enter one IP address, a range of IP addresses, or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
   
   b) **Virtual Servers**. You can specify either one of the following:
      
      i. Virtual server IP address
      
      ii. Virtual server name, or
      
      iii. Port of the backend server on which the applications are running.

   You can enter one IP address or a range of IP addresses or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

3. **StyleBooks**. You can create custom applications by using either a default or custom StyleBook that is already present in the Citrix ADM. StyleBooks simplify the task of managing complex Citrix ADC configurations for your applications. Select a StyleBook that is present in Citrix ADM and type in the StyleBook parameter values Citrix ADM creates the configuration (configpack) on the target Citrix ADC instances based on the selected StyleBook. Citrix ADM also creates a custom application that includes all the virtual servers defined in the configpack.
Note

A custom application and config pack are created if sufficient Citrix ADC licenses are available.

When you create an application that meets these conditions defined above in one of the three criteria, the application gets updated in the Application Dashboard automatically when Citrix ADM polls the entities. To initiate a poll manually, click Poll Now located in the Applications tab.

To create an application

1. In Citrix ADM, navigate to Applications > dashboard and click Define Custom App to create a custom application.

2. In the Define Application window, type the name of the application in the Name field.

3. Select the application category from the Category section. Citrix ADM allows you to define categories to group the user-defined applications. You can also add more categories if required.

4. You can create a custom application in one of the following three methods:
   a) Select Existing Applications. To select existing applications, make sure that the Select Existing Applications is enabled. Choose the application from the list in the Applications section. Click Add Applications to add new applications to the list.
   
   b) Define Selection Criteria. You can also define a selection criterion to add applications in Citrix ADM. You can add apps in one of the following three methods:
      i. Specifying the IP address of the virtual server. You can enter one IP address or a range of IP addresses or a combination of both separated by commas.
      
      ii. Specifying the name of the server on which the applications or services are running.

      Note
      You can also search for server names by using wildcard extensions. For example, ssl* will add all ssl virtual servers to the application.
      
      iii. Specifying the port number at which the application is listening to on the selected server.

   c) Create a new application from StyleBook. Select the required StyleBook in Citrix ADM to create config packs on the Citrix ADC instances and associate the virtual servers with a custom application.
5. Click **OK**. If you have opted to create applications from StyleBooks, the **Choose StyleBook** page opens. This page contains a list of all StyleBooks present in Citrix ADM.

6. Select the StyleBook. The StyleBook opens as a user interface form. Type the values for all
parameters in the StyleBook. You can also click View Definition to view the construct of the StyleBook before using it. For more information on how to use custom or default StyleBooks, see Use default StyleBooks.

7. A custom application and the config pack are now created on the Citrix ADC instances that you have selected in the target section in the StyleBook

**Note**

A custom application and config pack are created if sufficient Citrix ADM licenses are available.

**To auto-select virtual servers for licensing**

You must allow Citrix ADM to auto select the virtual servers for licensing when you use the StyleBook option to create configurations. If you have not enabled auto-select, you might get an error message as shown in the image below:

![Error message](image)

**To enable auto-selection of virtual servers:**

1. In Citrix ADM, navigate to Networks > Licenses > System Licenses.
2. Click Auto-select Virtual Servers to enable the option in Licensed Virtual Servers section.

![Licensed Virtual Servers](image)

When enabled, Citrix ADM automatically selects the virtual servers to license. And when it is not enabled, you must explicitly select the virtual servers.
To View Application Details in Citrix ADM

Citrix ADM displays all details of an application in a separate pane at the rightmost side known as App Info Panel.

To view the App Info Panel:

1. In Citrix ADM, navigate to Application > Dashboard.
2. In the Application Overview section, click the application for which you want to see the details.

The entities that are bound to the application that you have selected are arranged vertically in the App Info Panel pane. Vertically arranged boxes in the pane display the following:

- name of each entity
- the number of entities that are active
- entities that are inactive
- entities that are out of service
Citrix Application Delivery Management 12.1

The entities that are displayed here are the virtual servers, services, service groups, and the application servers. The pane also displays other data like App Score, data volume, throughput, both server and client connections, and the transactions that happen in each application.

You can view the count of virtual servers, services, service groups that are in different states for each application. You can click the name of the entity or the displayed count to directly enable or disable the entities. You can also enable or disable other bound entities such as virtual servers, services, and service groups.

For more information on how to configure load balancing servers, see Create Load Balancing Support through Application Dashboard.

Create a threshold and alert for application analytics

August 1, 2019

Application analytics on Citrix ADM allows you to monitor the various types of traffic passing through Citrix 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.

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

2. On the Create Threshold 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 box, select APPANALYTICS.
   c) **Entity**. From the list box, select the category or the resource type. By default, “applications” is selected as the entity.
   d) **Reference Key**. A reference key is automatically generated based on the traffic type and entity that you have selected.
   e) **Duration**. From the list box, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week’s duration.
3. In the **Configure Rule** section, create a rule by choosing the **App Score** metric, a required comparator, and provide a threshold value.

4. Click **Enable Threshold** to allow Citrix ADM to start monitoring the entities.

5. Optionally, configure actions such as email notifications and SMS notifications. Click **Create**.
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 Citrix ADC instance. Citrix application Delivery Management (ADM) computes the diff between existing state on a Citrix 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 Citrix 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 Citrix ADCs, 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 execute 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 execute it on the same or a different Citrix ADC instance. A new config pack is created for this configuration. A config pack is saved both on Citrix ADM and on the Citrix ADC instance on which the configuration is executed.

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

**StyleBook groups**

August 1, 2019

StyleBooks in Citrix Application Delivery Management (ADM) can be grouped in two ways. They can be grouped as either default StyleBooks or custom StyleBooks. Or, they can also be grouped as public or private StyleBooks. In Citrix ADM, you can view all the StyleBooks that are present in the system. Citrix ADM also allows you to sort and view the StyleBooks. You can also view a graphical display of how StyleBooks are connected with each other.

This document also tells you how to download and delete custom StyleBooks. You can download a custom StyleBook to make modifications or to create a new StyleBook based on the earlier one. You can also delete a custom StyleBook.
**Default and custom StyleBooks**

- Default StyleBooks are the StyleBooks that are present in the Citrix ADM file system and they allow you to create configurations you can deploy on your Citrix ADC instances.
- Custom StyleBooks are your own StyleBooks that you can write and import to Citrix ADM, and create configuration objects.

Both default and custom StyleBooks can be either public or private.

**Public and private StyleBooks**

StyleBooks from which you can create configuration packs to be deployed on the Citrix ADC instances can be categorized as “public” StyleBooks. That is, they are all available for your direct usage to create configurations.

But, some StyleBooks are used as building blocks for other StyleBooks. These building blocks are the built-in StyleBooks that the default StyleBooks are composed of. Such StyleBooks are called “private” StyleBooks. Though they are not directly used to create configuration packs on the instances, you might want to display these StyleBooks on the Citrix ADM. To mark a StyleBook as private, you can use the private attribute to prevent a StyleBook from being listed on the Citrix ADM.

```plaintext
name: basic-lb-config
description: This StyleBook defines a simple load balancing configuration and is a building block to build other load balancing configurations.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
```

**Viewing StyleBooks**

The number of StyleBooks - both default and private are increasing in Citrix ADM. You might want to search for the particular StyleBook that you want to access. You might also want to view both types of StyleBooks separately.

In Citrix ADM, when you navigate to Applications > StyleBooks, you can view a list of StyleBooks that are present in the system.

A default public StyleBook has the following icon on its panel:
Whereas, a default private StyleBook has an icon that declares it as a private StyleBook:

While you can view the definition and dependencies of a private StyleBook, you cannot create a config pack from a private StyleBook. You can still use a private StyleBook in your own StyleBook.

A custom-built public StyleBook has a different icon as shown in the following image:

While, a custom-built private StyleBook appears with this icon:

At the top right-side of the page, you can see an option to sort the StyleBooks. There are three options - all, public, or private StyleBooks. Click one of the options.
You can also search for a particular StyleBook by clicking the search icon. The three search options available are name, namespace, and version. The search operation is not case-sensitive.

**Viewing StyleBook dependencies**

Citrix ADM allows you to view a graphical display of how StyleBooks are connected with each other. In Citrix ADM, you can either use the default StyleBooks to create configurations for your deployment. You can also design your own StyleBooks and import them to Citrix ADM.

An important and powerful feature of StyleBooks is that they can be used as building blocks for other StyleBooks. You can import a StyleBook into another StyleBook. An imported Stylebook is declared as a type and is used by components or parameters of the second StyleBook.

A StyleBook used by other StyleBooks cannot be removed from the system. However, a graphical dis-
play of StyleBooks allows you to know which StyleBooks are preventing the removal of a StyleBook. By looking at the graph, it is possible to see the relationships among multiple StyleBooks.

**To view StyleBook dependencies**

In Citrix ADM, navigate to Applications > StyleBooks. The StyleBooks page displays all the StyleBooks available for your use in Citrix ADM. Scroll down and find your StyleBook. The StyleBook panel displays links to create a configuration, to view the StyleBook definition, and to view the StyleBook dependencies. Click **View Dependencies**.

**Forward dependencies**

The Forward Dependencies tab allows you to view the different default StyleBooks that your StyleBook is using. Follow the arrows to find the StyleBook that a StyleBook is using. When you point your mouse to one of the arrows, the arrow and the StyleBooks that are connected to one another are highlighted. You can also click the StyleBook names to view the definition of that StyleBook.

![Dependencies: vserver-certs-binds - com.citrix.adc.stylebooks - 1.1](image)

**Reverse dependencies**

The Reverse Dependencies tab allows you to graphically view the StyleBooks that are using your StyleBook. If you follow the arrows, you can see that all StyleBooks in the display point towards your StyleBook. Some StyleBooks might be directly using the StyleBook and some StyleBooks might be using the StyleBook through another StyleBook.
Downloading custom StyleBooks

To download custom Stylebooks from Citrix ADM, navigate to Applications > StyleBooks > Configurations. In the list of StyleBooks that are displayed on the right-side panel, the custom-defined StyleBooks have an option to download them. Click Download. If the StyleBook has dependent custom StyleBooks, even those StyleBooks are downloaded to your system.

Note

You cannot download default or custom StyleBooks that are marked as either public or private.

Note

You cannot download Citrix ADM default StyleBooks. You can, however, view their definitions and dependencies by clicking View Definition and View Dependencies links on the StyleBook panel.
Deleting custom StyleBooks

You can also delete custom StyleBooks by clicking “X” icon in the right-side of the StyleBook panel. A pop-up window prompts you to confirm if you want to remove the StyleBook from Citrix ADM. If the StyleBook uses other custom StyleBooks (that are not used by other StyleBooks), you can choose to remove them also by selecting the checkbox.

Note

You cannot delete a custom StyleBook that has other StyleBooks in Citrix ADM that depend on it.
Use default StyleBooks

August 1, 2019

A set of default StyleBooks are provided with Citrix Application Delivery Management (ADM). When you use a default StyleBook, you have to specify values for the parameters in the StyleBook and select the IP addresses of the Citrix ADC instances where you want to execute the configuration. After you submit the configuration, Citrix ADM validates the parameter values you have specified, creates a graph of the configuration, connects to the Citrix ADC instances, and executes the configuration on the instances.

To create a configuration from a default StyleBook

1. Navigate to Applications > Configurations > StyleBooks. The StyleBooks page displays all StyleBooks in Citrix ADM. This list includes both default and custom StyleBooks. You can type the name of the StyleBook in the search field and press the Enter key. Else, you can scroll down the list to find the Stylebook.
2. Click **Create Configuration**. Specify the required values for the parameters.
3. Under **Target Instances**, click and select the IP address of the Citrix ADC instance where you want to execute the configuration. If you want to execute this configuration on multiple instances, click “+” to add more instances.

If the **Prompt Credentials for Instance Login** option is enabled in **Citrix ADM > System > Change System Settings > Modify System Settings**, you are prompted for your Citrix ADC instance credentials when you execute the configurations on the selected Citrix ADC instances. Else, Citrix ADM uses the instance credentials stored in the instance profile for logging into the instance.
If you want to test or validate your configuration before executing it on the Citrix ADC instance, select **Dry Run** and then click **Create**. If your configuration is valid, the objects that are created on the basis of the values you have provided are displayed.
4. Clear the **Dry Run** check box and click **Create** to create the configuration and execute the configuration on the Citrix ADC instance. The StyleBook configuration that you have created appears in the list of configurations, as shown below.

**Note**
You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.

You can now examine, update, or remove this configuration pack by using Citrix ADM.
Hide all default StyleBooks

August 1, 2019

Citrix ADM lists all StyleBooks present in Citrix ADM folder system. The list of StyleBooks includes def-

dault and custom StyleBooks that can be both private and public. As an administrator, you might want
to hide all default StyleBooks. You can allow your users to view and access only custom StyleBooks
built by you or by the users.

Citrix ADM allows you to display your custom StyleBooks and hide all default StyleBooks that are
shipped with Citrix ADM. A new GUI option is provided where you can hide all default StyleBooks.

To hide all default StyleBooks:
1. In Citrix ADM, navigate to Applications > Configurations > Settings.
2. The Settings page displays information whether the default StyleBooks are visible to users or not.
3. To hide the default StyleBooks, click the edit icon at the top right side.
5. Click OK.

The Configure StyleBook Settings page is still visible to users if you have not opted to hide the page
using the RBAC feature. The users might still have the option to unhide the default StyleBooks.

To hide the Configure StyleBook Settings page, you must create a policy and assign that policy to
those users who should not see the default StyleBooks.

To create an RBAC policy:
1. In Citrix ADM, navigate to Account > User Administration > Access Policies.
2. Click Add to create a policy.
3. Enter the policy name.
4. In the Permissions section, make sure that under All > Applications > Configuration > Settings
   is not selected, and click OK.
After creating policies, you must create roles, bind each role to one or more policies, and assign roles to user groups. To know more about how to associate policies with users, see Configuring Role-Based Access Control.

**SSO Google Apps StyleBook**

August 1, 2019

Google Apps is a collection of cloud computing, productivity and collaboration tools, software and products that are developed by Google. Single Sign-On (SSO) enables users to access all of their enterprise cloud applications—including administrators signing in to the admin console—by signing in one time for all services using their enterprise credentials.

The Citrix ADM SSO Google Apps StyleBook allows you to enable SSO for Google Apps through Citrix ADC instances. The StyleBook configures the Citrix ADC instance as a SAML identity provider for authenticating users to access Google Apps.
Enabling SSO for Google apps in a Citrix ADC instance using this StyleBook results in the following steps:

1. Configuring the authentication virtual server
2. Configuring a SAML IDP policy and profile
3. Binding the policy and profile to the authentication virtual server
4. Configuring an LDAP authentication server and policy on the instance
5. Binding the LDAP authentication server and policy to your authentication virtual server configured on the instance

**Configuration details:**

The table below lists the minimum required software versions for this integration to work successfully. The integration process should also work with higher versions of the same.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC</td>
<td>Release 11.0, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

The following instructions assume that you have already created the appropriate external and/or internal DNS entries to route authentication requests to a Citrix ADC-monitored IP address.

**Deploying SSO Google apps StyleBook configurations:**

The following task assists you in deploying the Microsoft SSO Google Apps StyleBook in your business network.

**To deploy SSO Google apps StyleBook**

1. In Citrix ADM, navigate to Applications > Configurations > StyleBooks. The StyleBooks page displays all the StyleBooks available for your use in Citrix ADM. Scroll down and find SSO Google Apps StyleBook. Click Create Configuration.

2. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

3. Enter values for the following parameters:
   a) **Application Name.** Name of the SSO Google apps configuration to deploy in your network.
   b) **Authentication Virtual IP address.** Virtual IP address used by the AAA virtual server to which the Google apps SAML IdP policy is bound.
   c) **SAML Rule Expression.** By default, the following Citrix ADC Policy (PI) expression is used: HTTP.REQ.HEADER(“Referer”).CONTAINS(“google”). Update this field with another
expression if your requirement is different. This policy expression matches the traffic to
which these SAML SSO settings are applied and makes sure that the Referer header is
coming from a Google domain.

4. The SAML Idp Settings section allows you to configure your Citrix ADC Instance as a SAML iden-
tity provider by creating the SAML IDP profile and policy that is used by the AAA virtual server
created in step 3.

a) **SAML Issuer Name.** In this field, enter the public FQDN of your authentication virtual
server. Example: https://<Citrix ADC Auth VIP>/saml/login

b) **SAML Service Provider (SP) ID.** (optional) Citrix ADC identity provider accepts SAML au-
thentication requests from an issuer name that matches this ID.

c) **Assertion Consumer Service URL.** Enter the service provider’s URL where Citrix ADC iden-
tity provider needs to send the SAML assertions after successful user authentication. The
assertion consumer service URL can be initiated at the identity provider server site or the
service provider site.

d) There are other optional fields that you can enter in this section. For example, you can set
the following options:

i. SAML binding profile (the default is the “POST” profile).

ii. Signature algorithm to verify/sign SAML requests/responses (default is “RSA-SHA1”).

iii. Method to digest hash for SAML requests/responses (default is “SHA-1”).

iv. Encryption algorithm (default is AES256), and other settings.

**Note**

Citrix recommends that you retain the default settings as these settings have been
tested to work with Google Apps.

e) You can also enable User Attributes check box to enter the user details such as:

i. Name of the user attribute

ii. Citrix ADC PI expression that is evaluated to extract the attribute's value

iii. User-friendly name of the attribute

iv. Select the format of the user attribute.

These values are included in the issued SAML Assertion. You can include as many as five
sets of user attributes in an Assertion issued by Citrix ADC using this StyleBook.

5. In LDAP Settings section, enter the following details to authenticate Google Apps users. For
domain users to be able to log on to the Citrix ADC instance by using their corporate email ad-
addresses, you must configure the following:
a) **LDAP (Active Directory) Base.** Enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. For example, dc=netscaler,dc=com

b) **LDAP (Active Directory) Bind DN.** Add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. For example, cn=Manager,dc=netscaler,dc=com

c) **LDAP (Active Directory) Bind DN Password.** Enter the password of the domain account for authentication.

d) A few other fields that you need to enter in this section are as follows:

   i. LDAP server IP Address that Citrix ADC connects to for authenticating users

   ii. LDAP server’s FQDN name

   Note

   You must specify at least one of the above two - the LDAP server IP address or the FQDN name.

   iii. LDAP server port that Citrix ADC connects to for authenticating users (default is 389).

   iv. LDAP hostname. This is used to validate the LDAP Certificate if validation is turned on (by default, it is turned off).

   v. LDAP login name attribute. The default attribute used to extract login names is “samAccountname.”

   vi. Other optional miscellaneous LDAP settings

6. In SAML IdP SSL Certificate section, you can specify the details of the SSL certificate:

   a) **Certificate Name.** Enter the name of the SSL certificate.

   b) **Certificate File.** Choose the SSL certificate file from the directory on your local system or on Citrix ADM.

   c) **CertKey Format.** Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are .pem and .der file extensions.

   d) **Certificate Key Name.** Enter the name of the certificate private key.

   e) **Certificate Key File.** Select the file containing the private key of the certificate from your local system or from Citrix ADM.

   f) **Private Key Password.** If your private key file is protected by a passphrase, enter it in this field.

   g) You can also enable Advanced Certificate Settings check box to enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.
7. Optionally, you can select IdP SSL CA Certificate if the SAML IdP Certificate entered above requires a CA public Certificate to be installed on Citrix ADC. Make sure you select “Is a CA Certificate” in the advanced settings.

8. Optionally, you can select SAML SP SSL Certificate to specify Google SSL certificate (public key) used to validate authentication requests from Google Apps (SAML SP).

9. Click Target Instances and select the Citrix ADC instance(s) on which to deploy this Google Apps SSO configuration. Click Create to create the configuration and deploy the configuration on the selected Citrix ADC instance(s).

   **Note**
   You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.

**Also**

**Tip**
- Citrix recommends that before executing the actual configuration, you select Dry Run to visually confirm the configuration objects that are created on the target Citrix ADC instance(s) by the StyleBook.

---

**SSO Office 365 StyleBook**

August 1, 2019

Microsoft™ Office 365 is a suite of cloud-based productivity and collaboration applications provided by Microsoft on a subscription basis. It includes Microsoft’s popular server-based applications such as Exchange, SharePoint, Office, and Skype for Business. Single Sign-On (SSO) enables users to access all their enterprise cloud applications:

- Including administrators signing in to the admin console
- One-time sign on for all Microsoft Office 365 services using their enterprise credentials.

The SSO Office 365 StyleBook allows you to enable SSO for Microsoft Office 365 through Citrix ADC instances. You can now configure SAML authentication with Citrix ADC as the SAML Identity Provider (IdP) and Microsoft Office 365 as the SAML service provider.

Enabling SSO for Microsoft Office 365 in a Citrix ADC instance using this StyleBook involves the following steps:

1. Configuring the authentication virtual server
2. Configuring a SAML IDP policy and profile
3. Binding the policy and profile to the authentication virtual server
4. Configuring an LDAP authentication server and policy on the instance
5. Binding the LDAP authentication server and policy to your authentication virtual server configured on the instance.

The table lists the minimum required software versions for this integration to work successfully. The integration process should also work with higher versions of the same.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC</td>
<td>11.0, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

The following instructions assume that you have already created the appropriate external and internal DNS entries. These entries are essential to route authentication requests to a Citrix ADC-monitored IP address.

The following instructions assist you in implementing the SSO Office 365 StyleBook in your business network.

To deploy SSO Microsoft Office 365 StyleBook

1. In Citrix Application Delivery Management (ADM), navigate to Applications > StyleBooks. The StyleBooks page displays all the StyleBooks available for your use in Citrix ADM. Scroll down and find SSO Office 365 StyleBook. Click Create Configuration.

2. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

3. Enter values for the following parameters:
   a) Application Name. Name of the SSO Microsoft Office 365 configuration to deploy in your network.
   b) Authentication Virtual IP address. Virtual IP address to be used by the AAA virtual server to which the Microsoft Office 365 SAML IdP policy is bound.

4. In SSL Certificates Settings section, enter the names of the SSL certificate and the certificate key.
Note

This is not the Office 365 service provider certificate. This SSL certificate is bound to the virtual authentication server on the Citrix ADC instance.

5. Select the respective files from your local storage folder. You can also type in the private key password to load encrypted private keys in PEM format.

6. You can also enable Advanced Certificate Settings check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.

7. Optionally, you can select SSL CA Certificate for the authentication virtual IP check box if the SSL certificate requires a CA public certificate to be installed on Citrix ADC. Make sure you choose “Is a CA Certificate” in the above Advanced Certificate Settings section.

8. In LDAP Settings for SSO Office 365 section, enter the following details to authenticate Office 365 users. To allow domain users to log on to the Citrix ADC instance by using their corporate email addresses, configure the following:

   • **LDAP (Active Directory) Base.** Enter the base domain name for the domain in which the
user accounts reside within the Active Directory (AD) to allow authentication. For example, dc=netscaler,dc=com

- **LDAP (Active Directory) Bind DN.** Add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. For example, cn=Manager,dc=netscaler,dc=com

- **LDAP (Active Directory) Bind DN Password.** Enter the password of the domain account for authentication.

- A few other fields that you need to enter in this section are as follows:
  - LDAP server IP Address that Citrix ADC connects to for authenticating users.
  - LDAP server’s FQDN name.

  **Note**
  You must specify at least one of the above two - the LDAP server IP address or the FQDN name.

  - LDAP server port that Citrix ADC connects to for authenticating users (default is 389). LDAPS uses 636.
  - LDAP hostname. The hostname is used to validate the LDAP Certificate if validation is turned on (by default, it is turned off).
  - LDAP login name attribute. The default attribute used to extract login names is “samAccountname.”
  - Other optional miscellaneous LDAP settings.
9. In **SAML IdP Certificate** section, you can specify the details of the SSL certificates used for SAML assertion.

   - **Certificate Name.** Enter the name of the SSL certificate.
   - **Certificate File.** Choose the SSL certificate file from the directory on your local system.
   - **CertKey Format.** Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are .pem and .der file extensions.
- **Certificate Key Name.** Enter the name of the certificate private key.

- **Certificate Key File.** Select the file containing the private key of the certificate from your local system.

- **Private Key Password.** Type in the passphrase that protects your private key file.

You can also enable **Advanced Certificate Settings** check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.

10. Optionally, you can select **SAML IdP CA Certificate** if the SAML IdP certificate entered above requires a CA public certificate to be installed on Citrix ADC. Make sure you select **Is a CA Certificate** in the above **Advanced Certificate Settings** section.

11. In the **SAML SP Certificate** section, enter the following details for the Office 365 SSL public certificate. This certificate is used by the Citrix ADC instance to verify incoming SAML authentication
requests.

- **Certificate Name.** Type the name of the SSL certificate.

- **Certificate File.** Choose the SSL certificate file from the directory on your local system.

- **CertKey Format.** Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are .pem and .der file extensions.

- You can also enable **Advanced Certificate Settings** check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.

12. The **SAML Idp Settings** section allows you to configure your Citrix ADC Instance as a SAML identity provider by creating the SAML IDP profile and policy that is used by the AAA virtual server created in step 3.

- **SAML Issuer Name.** In this field, type the public FQDN of your authentication virtual server. Example: `https://<Citrix ADC Auth VIP>/saml/login`

- **Name Identifier Expression.** Type in the Citrix ADC expression that is evaluated to extract the SAML NameIdentifier sent in the SAML assertion. Example: "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"

- **Signature algorithm:** Select the algorithm to verify/sign SAML requests/responses (default is “RSA-SHA256”).

- **Digest Method.** Select the method to digest hash for SAML requests/responses (default is “SHA256”).

- **Audience name.** Type in the entity name or URL that represents the service provider (Microsoft Office 365).

- **SAML Service Provider (SP) ID.** (optional) Citrix ADC identity provider accepts SAML authentication requests from an issuer name that matches this ID.

- **Assertion Consumer Service URL.** Enter the service provider’s URL where Citrix ADC identity provider needs to send the SAML assertions after successful user authentication.
assertion consumer service URL can be initiated at the identity provider server site or the service provider site.

- There are other optional fields that you can enter in this section. For example, you can set the following options:
  - **SAML attribute name.** Name of user attribute sent in SAML Assertion.
  - **SAML attribute friendly name.** Friendly Name of the user attribute sent in SAML Assertion.
  - **PI expression for SAML attribute.** By default, the following Citrix ADC Policy (PI) expression is used: HTTP.REQ.USER.ATTRIBUTE(1). This field specifies the first user attribute sent from the LDAP server (mail) as the SAML authentication attribute.
  - Select the format of the user attribute.

These values are included in the issued SAML Assertion.

**Tip**

Citrix recommends that you retain the default settings as these settings have been tested to work with Microsoft Office 365 apps.
13. Click **Target Instances** and select the Citrix ADC instance(s) on which to deploy this Microsoft Office 365 SSO configuration. Click **Create** to create the configuration and deploy the configuration on the selected Citrix ADC instance(s).
Microsoft Skype for Business StyleBook

August 1, 2019

The Skype for Business 2015 application relies on several external components to function. The Skype for Business network consists of various systems, such as servers and their operating systems, databases, authentication and authorizing systems, networking systems and infrastructure, and telephone PBX systems. Skype for Business Server 2015 is available in two versions, Standard Edition and Enterprise Edition. The primary difference is in support for high-availability features that are only included in the Enterprise Edition. To implement high availability, multiple Front-End servers must be deployed to a pool and SQL servers must be mirrored.

An Enterprise Edition deployment enables the creation of multiple servers with different roles.

Primary components

The primary components in Skype for Business 2015 application are:

- Front-end servers
- Edge servers
- Director servers
- Database (SQL) servers
**Front-end servers**

In the Skype for Business application, the Front-End server is the core server in your network. It provides the links and services for user authentication, registration, presence, address book, A/V conferencing, application sharing, instant messaging, and web conferencing. If you are deploying Skype for Business 2015 Enterprise edition, the topology typically consists of at least two Front-End servers load balanced in a Front-End pool with a database server that hosts the SQL Server instance holding the Skype for Business database.

**Edge servers**

Deploying Edge servers for Skype for Business is necessary if external users who are not logged into your organization’s internal network need to be able to interact with internal users. These external users could be authenticated and anonymous remote users, federated partners, or other mobile clients.

There are four types of roles in Skype For Business Edge server:

- **Access Edge**, which handles SIP Traffic and authenticates external connections, allows remote connection and allows federation Connection
- **Web Conferencing**, which handles Data Conferencing Packets, and allows external users to access Skype for Business
- **A/V Conferencing**, which handles A/V Conferencing Packets, and extends audio and video, app sharing and file transfer to external users
- **XMPP Proxy**, which handles XMPP packets, and allows XMPP based servers or clients to connect to Skype for Business.

**Director servers**

The main function of the Director server in Skype for Business 2015 is to authenticate endpoints and “direct” the users to the pool that contains their account. In Skype for Business 2015, though the Director is a completely dedicated and specific role on a standalone server, it is an optional server. This facilitates security by making it easier to deploy or remove the configurations.

Directors are most useful where multiple pools exist because they provide a single point of contact for authenticating endpoints. Also, for remote users, a Director serves as an extra hop between the Edge pool and Front-End pool, adding an extra layer of protection against attacks.

The following figure diagrammatically represents the deployment of Skype servers in the network:
Configuring Citrix ADC instances in an enterprise

The following table lists the IP addresses used in the sample configuration included in the instructions below:

<table>
<thead>
<tr>
<th>Skype for Business Servers</th>
<th>Virtual IP Address</th>
<th>Server IP Addresses</th>
<th>Citrix ADC Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Servers</td>
<td>External VIP - 192.20.20.20</td>
<td>192.20.20.21; 192.20.20.22</td>
<td>10.102.29.141</td>
</tr>
<tr>
<td></td>
<td>Internal VIP - 10.10.10.20</td>
<td>10.10.10.21; 10.10.10.22</td>
<td></td>
</tr>
<tr>
<td>Front-end Servers</td>
<td>10.10.10.10</td>
<td>10.10.10.11; 10.10.10.12</td>
<td>10.102.29.60</td>
</tr>
<tr>
<td>Director Server</td>
<td>10.10.10.30</td>
<td>10.10.10.31; 10.10.10.32</td>
<td>10.102.29.93</td>
</tr>
</tbody>
</table>

To configure front-end servers

1. In Citrix Application Delivery Management (ADM), navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks available for your use in Citrix ADM. Scroll down and select Microsoft Skype for Business 2015 StyleBook. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. In the **Edge Server** section, enter the following virtual IP (VIP) addresses and IP addresses of all the Edge servers in the network.
   a) External VIP address and IP addresses for the Edge servers that will be used for Access Edge, web conferencing Edge, and A/V Edge.
   b) Internal VIP address and IP addresses for the Edge servers that will be connected to the internal network.
   c) Two external and two internal Edge servers in your network.

3. In the **Front-End Server** section, enter the IP address of the virtual Front-End server (VIP) that is to be created for the Skype for Business Front-End servers. Also, enter the IP addresses of all the Skype for Business Front-End servers in the network.

4. In the **Director Server** section, enter the virtual IP address (VIP) for the Director servers that is to be created for the Skype for Business application. Also, enter the IP addresses for all the Skype for Business Director servers in the network. Create at least two Director servers for high-availability.

5. The **Advanced Settings** section lists all the default ports configured on the Citrix ADC instances for the three Skype servers.

The following table provides you a list of all default ports and protocols:

<table>
<thead>
<tr>
<th>Label</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td>HTTP</td>
<td>Used for communication from Front-End Servers to the web farm FQDNs when HTTPS is not used.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for communication from Front-End Servers to the web farm FQDNs.</td>
</tr>
<tr>
<td>AutoDiscover Internal</td>
<td>4443</td>
<td>HTTPS</td>
<td>HTTPS (from Reverse Proxy) and HTTPS Front-End inter-pool communications for AutoDiscover sign-in.</td>
</tr>
<tr>
<td>Label</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPC Port</td>
<td>135</td>
<td>DCOM and remote procedure call (RPC)</td>
<td>Used for DCOM based operations such as moving users, user replicator synchronization, and address book synchronization.</td>
</tr>
<tr>
<td>SIP Port</td>
<td>5061</td>
<td>TCP (TLS)</td>
<td>Used by Front-End servers for all internal SIP communications.</td>
</tr>
<tr>
<td>SIP Focus Port</td>
<td>444</td>
<td>HTTPS, TCP</td>
<td>Used for HTTPS communication between the Focus (the component that manages the Skype conference state) and the individual servers.</td>
</tr>
<tr>
<td>SIP Group Port</td>
<td>5071</td>
<td>TCP</td>
<td>Used for incoming SIP requests for the response group application.</td>
</tr>
<tr>
<td>SIP AppSharing Port</td>
<td>5065</td>
<td>TCP</td>
<td>Used for incoming SIP listening requests for application sharing.</td>
</tr>
<tr>
<td>SIP Attendant Port</td>
<td>5072</td>
<td>TCP</td>
<td>Used for incoming SIP requests for the attendant (that is, for dial-in conferencing).</td>
</tr>
<tr>
<td>SIP Conf Announcement Port</td>
<td>5073</td>
<td>TCP</td>
<td>Used for incoming SIP requests for the Skype for Business server conferencing announcement service (that is, for dial-in conferencing).</td>
</tr>
<tr>
<td>Label</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP CallPark Port</td>
<td>5075</td>
<td>TCP</td>
<td>Used for incoming SIP requests for the CallPark application.</td>
</tr>
<tr>
<td>SIP Call Admission Port</td>
<td>448</td>
<td>TCP</td>
<td>Used for call admission control by the Skype for Business server bandwidth policy service.</td>
</tr>
<tr>
<td>SIP Call Admission TURN Port</td>
<td>5080</td>
<td>TCP</td>
<td>Used for call admission control by the bandwidth policy service for Audio/Video Edge TURN traffic.</td>
</tr>
<tr>
<td>SIP Audio Test Port</td>
<td>5076</td>
<td>TCP</td>
<td>Used for incoming SIP requests for the audio test service.</td>
</tr>
<tr>
<td>HTTPS External Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for external ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.</td>
</tr>
<tr>
<td>Label</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTPS Internal Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for internal ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.</td>
</tr>
<tr>
<td>SIP External Remote Access Port</td>
<td>5061</td>
<td>TCP</td>
<td>Used for external ports for SIP/MTLS communication for remote user access or federation.</td>
</tr>
<tr>
<td>SIP Internal Remote Access Port</td>
<td>5061</td>
<td>TCP</td>
<td>Used for internal ports for SIP/MTLS communication for remote user access or federation.</td>
</tr>
<tr>
<td>SIP External STUN UDP Port</td>
<td>3478</td>
<td>UDP</td>
<td>Used for external ports for STUN/UDP inbound and outbound media communications.</td>
</tr>
<tr>
<td>SIP Internal STUN UDP Port</td>
<td>3478</td>
<td>UDP</td>
<td>Used for internal ports for STUN/UDP inbound and outbound media communications.</td>
</tr>
<tr>
<td>Label</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP Internal IM Port</td>
<td>5062</td>
<td>TCP</td>
<td>Used for internal ports for SIP/MTLS authentication of IM communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>flowing outbound through the internal firewall.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td>TCP</td>
<td>Used for initial communication from Directors to the web farm FQDNs.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for communication from Directors to the web farm FQDNs.</td>
</tr>
<tr>
<td>AutoDiscover Internal Port</td>
<td>4443</td>
<td>HTTPS</td>
<td>Used for HTTPS (from Reverse Proxy) and HTTPS Director inter-pool communications for AutoDiscover sign-in.</td>
</tr>
<tr>
<td>SIP Internal Port</td>
<td>5061</td>
<td>TCP</td>
<td>Used for internal communications between servers and for client connections.</td>
</tr>
</tbody>
</table>

6. In the **Target Instances** section, select the three different Citrix ADC instance on which to deploy the three Skype for Business servers.

**Note**

You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.

7. Click **Create** to create the configuration on the selected Citrix ADC instances.
Tip

Citrix recommends that you select **Dry Run** to check the configuration objects that must be created on the target instance before you execute the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates 25 load balancing virtual servers. That is, for each port, one load balancing virtual server is defined along with one service group, and the service group is bound to the load balancing virtual server. The configuration also adds the Front-End servers as service group members and binds them to the service group. The number of service group members created is equal to the number of Front-End servers created.

The following figure shows the objects created in each server:

Microsoft Exchange StyleBook

August 1, 2019

You can use the Microsoft Exchange 2016 StyleBook to deploy a Citrix ADC configuration that optimizes and secures a Microsoft Exchange 2016 enterprise application in your network. Microsoft Exchange 2016 is a key enterprise application for providing email, personal information management, and messaging services to your employees and other stakeholders.

Citrix ADC features configured by using Microsoft Exchange StyleBook

The Microsoft Exchange 2016 StyleBook enables and configures the following Citrix ADC features for Microsoft Exchange 2016 servers:

- Load balancing - Basic load balancing that enables load balancing of multiple Exchange servers
- Content switching - Content switching that enables single-IP access and redirection of queries to the correct load balancing virtual servers
Citrix Application Delivery Management 12.1

- Rewrite - Redirects users to secure pages
- SSL offload - Offloads SSL processing to the Citrix ADC, therefore reducing the load on the Exchange server

The following figure diagrammatically represents the deployment of Exchange servers in the network:

Prerequisites

- For certificate-based authentication, all addressable hosts that are part of the network setup must have resolvable domain names and not just IP addresses.
- Ensure that the SIP ports are accessible in Microsoft Exchange 2016 server.

Configuring Microsoft Exchange StyleBook

Configure the Microsoft Exchange StyleBook in your business enterprise to deploy the Citrix ADC configuration.

To configure Microsoft Exchange application

1. In Citrix ADM, navigate to **Applications > StyleBooks**.
2. Search for **Microsoft Exchange 2016 StyleBook** and click **Create Configuration**.

   The StyleBook appears as a user interface form on which you can enter the values for all the parameters defined in this StyleBook.

3. Enter the details for the following parameters:

   - **Exchange Application Name** - Name of the Microsoft Exchange Application in your network
   - **Exchange VIP** - Virtual IP address on Citrix ADC that receives client requests for the Microsoft Exchange application
   - **Exchange Server IPs** - IP addresses of all the Exchange servers in the network.

     If you want to add more IP addresses, click the plus (+) icon. Usually, two Exchange servers are configured in the network.
4. In the Exchange Certificates section, upload exchange certificates to Citrix ADM. Enter the names of both the certificate and the key files and upload from the local storage. You can also provide a private key password to encrypt the key file.

   **Note**
   Ensure that the certificate files are of “.pem” or “.der” format. Citrix ADM rejects the files of other formats.

   If you want to specify certificate expiration details or any advanced settings, select Advanced Certificate Settings.

5. In the Exchange Active Directory Authentication config section, configure the AD Settings by entering the data.

   • **Active Directory Authentication VIP** - The virtual IP address used to create and configure the AD (LDAP) virtual server on a Citrix ADC appliance.

   • **Active Directory Server IP** - The IP address of your Active Directory domain controller.

   • **Active Directory Base String** - The LDAP Base String in Active Directory. For example, CN=Users,DC=CTXNSSFB,DC=COM.

   • **Active Directory LDAP Bind Distinguished Name (DN)** - LDAP Bind Distinguished Name (DN) is used to bind this object to the LDAP server (AD). For example “cn=Administrator,cn=Users,dc=acme,dc=com”.

   • **Active Directory LDAP Bind Distinguished Name (DN) Password** - LDAP Bind Distinguished Name (DN) is the password for AD Authentication.

   • **Active Directory User Name Attribute** - AD attribute for the user name. The Citrix ADC uses the LDAP attribute to query external Active Directory Servers. For example, “sAMAccountName”.

   • **Active Directory group Attribute Name** - the LDAP group attribute names configured on the LDAP server. For example, “memberOf” for the group attribute in LDAP.

   • **Active Directory Sub-AttributeName** - the LDAP subattribute names configured on the LDAP server. For example, “cn” for the subattribute in LDAP.

   • **Active Directory Authentication Domain** - The AD/LDAP domain name used for authentication. For example, ctxnssfb.com.

6. In the Target Instances section, select the Citrix ADC instance on which to deploy this Exchange configuration.

   **Note**
   If you want to view the recently discovered Citrix ADC instances, click the refresh icon.

7. Click Create to create the configuration file and execute the configuration on the selected Citrix ADC instance.
Citrix recommends that you first select **Dry Run** to check the configuration objects that are created on the target instance before executing the actual configuration on the instance.

When the configuration has been created successfully, the StyleBook has created a content switching virtual server, five load balancing virtual servers, and one LDAP policy bound to one LDAP authentication virtual server. Also, the corresponding service groups created and bound to the load balancing virtual servers.

**Microsoft SharePoint StyleBook**

August 1, 2019

Microsoft SharePoint 2016 is a key enterprise application that primarily provides a document management and storage system, which is highly configurable and supported by all major browsers.

You can use the Microsoft SharePoint 2016 StyleBook to deploy a Citrix ADC configuration that optimizes and secures the Microsoft SharePoint 2016 enterprise application in your network.

**Prerequisites**

- Microsoft SharePoint 2016
- Citrix ADM, version 12.0 and later
- Citrix ADC, version 10.5 and later

**Citrix ADC features configured by the Microsoft SharePoint 2016 StyleBook**

You can use the Microsoft SharePoint 2016 StyleBook to enable and configure the following Citrix ADC features for Microsoft SharePoint 2016:

- Load balancing
- Content Switching
- Responder
- Rewrite
- Compression
- Integrated Caching

**Load balancing**

Citrix ADC load balancing evenly distributes requests to backend SharePoint servers. Intelligent monitoring of backend servers prevents requests from being sent to malfunctioning servers.
The SharePoint StyleBook configures 12 load balancing virtual servers, each dedicated to load balancing requests for a certain type of content, such as documents, images, audio, video, and other file types.

The SharePoint StyleBook now supports SSL Mode of SharePoint application by configuring SSL based LB virtual servers. Make sure SSL is selected as the front-end protocol. Note that the virtual port is set to 443 by default. You can also select SSL to bind service groups (SharePoint application servers) to the target load balancing virtual servers. Note that the backend protocol by default is set to HTTP.

**Content switching**

The content switching feature is used to distribute client requests across multiple load balancing virtual servers on the basis of specific types of requested SharePoint content (for example, documents, images, and audio or video files). The content switching module directs incoming traffic to an optimal matching load balancing virtual server that can process that type of content. You can therefore apply different optimization policies to different types of traffic. For example, you might want to use different compression or caching policies for video than for text documents.

**Responder**

The responder functionality of a Citrix ADC instance can be used to seamlessly redirect users from HTTP to HTTPS. Responder can also be configured to provide customized error pages. The Responder policy determines the requests (traffic) on which an action has to be taken, and binds each policy to a load balancing virtual server. The SharePoint StyleBook includes a configuration that redirects users from HTTP to HTTPS URLs.

**Rewrite**

The rewrite module is used to modify request/response headers, URLs, or content on the fly. This module works in-line with traffic processing and can therefore change the traffic flow as appropriate for particular use cases. For example, rewriting can provide access to the requested content without exposing unnecessary details about the website’s server.

In the SharePoint StyleBook, the rewrite feature is used to removed unnecessary headers from user requests.

**Compression**

The Citrix ADC compression engine identifies and compresses content that is compressible. This process improves data transmission time and reduces network bandwidth requirements for the clients,
while saving CPU cycles on SharePoint content servers. A Citrix ADC instance can compress both static and dynamically generated data. It applies the GZIP or the DEFLATE compression algorithm to remove extraneous and repetitive information from the server responses and represent the original information in a more compact and efficient format. The client browser’s ability to decompress the data depends on which algorithm or algorithms it supports: GZIP, DEFLATE, or both of these.

A Citrix ADC instance is configured to compress the text in HTML, XML, plain text, Cascading Style Sheet (CSS), and Microsoft Office documents, but does not compress images in GIF or JPG format. The major benefits of compressed traffic include reduced bandwidth costs, WAN latency reduction, and better server performance.

**Integrated caching**

The Citrix ADC in-memory cache can store SharePoint objects in order to quickly deliver frequently requested content to users. Cached content includes downloaded documents and audio, video, and image files.

The following figure diagrammatically represents the deployment of SharePoint servers in a network front-ended by a Citrix ADC instance on which Citrix ADM is used to deploy a SharePoint StyleBook configuration.

![Diagram of SharePoint deployment](image-url)

**Deploying SharePoint StyleBook configurations**

The following task will assist you in deploying the Microsoft SharePoint 2016 StyleBook in your business network.
To deploy Microsoft SharePoint 2016 StyleBook:

1. In Citrix ADM, navigate to Applications > Administration > Configuration, and click Create New.

The Choose StyleBook page displays all the StyleBooks available for your use in Citrix ADM.

2. Scroll down and select Microsoft SharePoint 2016 StyleBook.

   Note
   In Citrix ADM, navigate to Applications > Configurations > StyleBooks. Scroll down to find the Microsoft SharePoint 2016 StyleBook, and click Create Configuration.

The StyleBook opens as a user interface form on which you can enter the values for all the parameters defined in this StyleBook.

Enter values for the following parameters:

   a) SharePoint Application Name. Name of the SharePoint configuration to deploy in your network.

   b) SharePoint Virtual IP. Virtual IP address at which the Citrix ADC instance receives client requests for the Microsoft SharePoint application.

   c) SharePoint Virtual Port. The TCP Port to be used by the Users in accessing the SharePoint application.

   d) SharePoint frontend Protocol. Select the SharePoint frontend protocol from the drop-down list. The options available are HTTP or SSL.

      Note
      If you select SSL, make sure that the Rewrite Configuration parameter is enabled in the SharePoint Advanced Settings section in this StyleBook.

   e) SharePoint Server IPs. IP addresses of all the SharePoint servers in the network.

   f) SharePoint Servers Port. TCP port number used by the SharePoint servers. By default, this is 80. You can edit this value if required, but make sure that this port is accessible on Microsoft SharePoint 2016 servers.
3. In the **SSL Certificates settings** section, click + to enter the name of the SSL certificate, the certificate key, and select the respective files from your local storage folder.
4. Optionally click **Advanced Certificate Settings** to enable or disable SSL certificate expiry monitoring. If you enable the certificate expiry monitoring, set the number of days so that Citrix ADM issues an alarm after these many days when the certificate is about to expire. You also have an option to make the OCSP checking as an optional feature or a mandatory feature.

5. The SharePoint **Advanced Settings** section allows you to enable the Citrix ADC features that will be configured on the Citrix ADC instances. While the load balancing and content switching features are configured on the instances by default, you can choose the other features, that is, responder configuration, rewrite configuration, compression configuration, and integrated caching configuration, that you want to be configured on the instance.

6. Click **Target Instances** and select the Citrix ADC instance on which to deploy this SharePoint configuration. Click **Create** to create the configuration and deploy the configuration on the selected Citrix ADC instance.

**Note**

You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.
Citrix recommends that before executing the actual configuration, you select **Dry Run** to check the configuration objects that will be created on the target instance.

When the configuration is created and successfully deployed, the SharePoint StyleBook creates one content switching virtual server and 12 load balancing virtual servers. It also creates policies and service groups and binds them to the load balancing virtual servers. Which policies are created depends on the features selected in the StyleBook during creation of the configuration pack.

**Viewing the objects defined on the Citrix ADC instance**

After the configuration pack is created on Citrix ADM, you can view all the objects created on the Citrix ADC instance for the SharePoint StyleBook. Navigate to **Applications > Administration > Configuration**, and click **View Objects Created**. The following figure shows some of the created objects, with the IP addresses specified in the example shown in “Deploying SharePoint StyleBook Configurations from Citrix ADM.”
**Type : lbvserver**

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ip6v6 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint-application-test-frontpage-services-lb
persistencetypebackup : SOURCEIP
persistencetype : COOKEINSERT
port : 0
servicetype : HTTP
timeout : 20

**Type : servicegroup**

cip : DISABLED
clic : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcp : NO
useproxyport : NO
usip : NO

**Type : lbvserver_servicegroup_binding**

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

**Type : servicegroup_servicegroupmember_binding**

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

**Type : servicegroup_servicegroupmember_binding**

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

**Type : csaction**

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

**Type : cspolicy**

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP,REQ,HEADER\("X-Vermeir\-Content\-Type\"\),EXISTS

**Type : csvserver_cspolicy_binding**

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10
Microsoft ADFS proxy StyleBook

August 1, 2019

Microsoft™ ADFS proxy plays a significant role by giving single sign-on access for both internal federation-enabled resources and cloud resources. One such example of cloud resources is Office 365. The purpose of the ADFS proxy server is to receive and forward requests to ADFS servers that are not accessible from the internet. ADFS proxy is a reverse proxy and typically resides in your organization’s perimeter network (DMZ). The ADFS proxy plays a critical role in remote user connectivity and application access.

Citrix ADC has the precise technology to enable secure connectivity, authentication, and handling of federated identity. Using Citrix ADC as ADFS proxy avoids the need to deploy an extra component in the DMZ.

The Microsoft ADFS Proxy StyleBook in Citrix Application Delivery Management (ADM) allows you to configure an ADFS proxy server on a Citrix ADC instance.

The following image shows the deployment of a Citrix ADC instance as an ADFS proxy server in the enterprise DMZ.

Benefits of using Citrix ADC as ADFS proxy

1. Caters to both load balancing and ADFS proxy needs
2. Supports both internal and external user access scenarios
3. Supports rich methods for pre-authentication
4. Provides a single sign-on experience for users
5. Supports both active and passive protocols
   a) Examples of active protocol apps are – Microsoft Outlook, Microsoft Skype for Business
Citrix Application Delivery Management 12.1

b) Examples of passive protocol apps are –Microsoft Outlook web app, web browsers

6. Hardened device for DMZ-based deployment

7. Adds value by using additional core Citrix ADC ADC features
   a) Content Switching
   b) SSL offload
   c) Rewrite
   d) Security (Citrix ADC AAA)

For active protocol-based scenarios, you can connect to Office 365 and provide your credentials. Microsoft Federation Gateway contacts the ADFS service (through ADFS Proxy) on behalf of the active protocol client. The gateway then submits the credentials using basic authentication (401). Citrix ADC handles the client authentication before access to ADFS service. Post authentication, the ADFS service provides a SAML token to the Federation Gateway. The Federation Gateway, in turn, submits the token to Office 365 to provide client access.

For passive clients, the ADFS Proxy StyleBook creates Kerberos Constrained Delegation (KCD) user account. The KCD account is necessary for Kerberos SSO authentication to connect to the ADFS servers. The StyleBook also generates an LDAP policy and a session policy. These policies are later bound to the Citrix ADC AAA virtual server that handles the authentication for passive clients.

The StyleBook can also ensure that the DNS servers on the Citrix ADC are configured for ADFS.

The configuration section below describes how to set up Citrix ADC for handling both active and passive protocol-based client authentication.

Configuration details

The table below lists the minimum required software versions for this integration to be deployed successfully.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC</td>
<td>11.0, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

The following instructions assume that you have already created the appropriate external and internal DNS entries.

Deploying Microsoft ADFS proxy StyleBook configurations from Citrix ADM

The following instructions assist you when implementing the Microsoft ADFS proxy StyleBook in your business network.
To deploy Microsoft ADFS proxy StyleBook

1. In Citrix ADM, navigate to Applications > StyleBooks. The StyleBooks page displays all the StyleBooks available for your use in Citrix ADM.

2. Scroll down and find the Microsoft ADFS proxy StyleBook. Click Create Configuration. The StyleBook opens as a user interface page on which you can type the values for all the parameters defined in this StyleBook.

3. Type values for the following parameters:
   a) ADFS Proxy Deployment Name. Select a name for the ADFS proxy configuration deployed in your network.
   b) ADFS Servers FQDNs or IPs. Type the IP addresses or FQDNs (domain names) of all ADFS servers in the network.
   c) ADFS Proxy Public VIP IP. Type the public virtual IP address on the Citrix ADC that performs as an ADFS proxy server.

4. In the ADFS Proxy Certificates section, type the details of the SSL certificate and the certificate key.
   This SSL certificate is bound to all the virtual servers created on the Citrix ADC instance.
   Select the respective files from your local storage folder. You can also type in the private key password to load encrypted private keys in .pem format.
You can also enable **Advanced Certificate Settings** check box. Here you can type details such as certificate expiry notification period, enable, or disable the certificate expiry monitor.

5. Optionally, you can select **SSL CA Certificate** check box if the SSL certificate requires a CA public certificate to be installed on Citrix ADC. Ensure that you select **Is a CA Certificate** in the **Advanced Certificate Settings** section.

6. Enable authentication for active and passive clients. Type the DNS Domain Name used in Active Directory for user authentication. You can then configure authentication either for active or passive clients, or both.
7. Type the following details to enable authentication for active clients:

**Note**
It is optional to configure support for active clients.

a) **ADFS Proxy Active Authentication VIP.** Type the virtual IP address of the virtual authentication server on the Citrix ADC instance where the active clients are redirected for authentication.

b) **Service Account Username.** Type the service account user name used by Citrix ADC to authenticate your users to the active directory.

c) **Service Account Password.** Type the password used by Citrix ADC to authenticate your users to the active directory.

8. Configure authentication for passive clients by enabling the corresponding option and configuring the LDAP settings.
It is optional to configure support for passive clients. Type the following details to enable authentication for passive clients:

a) **LDAP (Active Directory) Base.** Type the base domain name for the domain in which the user accounts reside within the active directory (AD) to allow authentication. For example, `dc=netscaler,dc=com`

b) **LDAP (Active Directory) Bind DN.** Add a domain account (using an email address for ease of configuration) that has privileges to browse the AD tree. For example, `cn=Manager,dc=netscaler,dc=com`

c) **LDAP (Active Directory) Bind DN Password.** Type the password of the domain account for authentication.

A few other fields that you must type in the values in this section are as follows:

d) **LDAP Server (Active Directory) IP.** Type the IP address of the active directory server for AD authentication to work correctly.

e) **LDAP Server FQDN name.** Type the FQDN name of the active directory server. FQDN name is optional. Provide the IP address as in step 1 or the FQDN name.

f) **LDAP Server Active Directory port.** By default, the TCP and UDP ports for LDAP protocol are 389, whereas the TCP port for Secure LDAP is 636.

g) **LDAP (Active Directory) login username.** Type the username as “sAMAccountName.”

h) **ADFS Proxy Passive Authentication VIP.** Type the IP address of the ADFS proxy virtual server for passive clients.

---

**Note**

The fields marked with “*” are mandatory.
Enable Passive Clients Authentication

Parameters for configuring AD Auth for ADFSProxy

LDAP (Active Directory) Base*

dc=netScaler,dc=com

LDAP (Active Directory) Bind DN*

cn=Manager,dc=netScaler,dc=com

LDAP (Active Directory) Bind DN Password*

******

LDAP Server (Active Directory) IP

10.30.30.3

LDAP Server FQDN name

adfs.citrix.com

LDAP Server (Active Directory) Port

389

LDAP Host name


Active Directory LDAP?

Validate LDAP Certificate

LDAP (Active Directory) Login username

samAccountname

LDAP (Active Directory) Group Attribute Name


LDAP (Active Directory) Group Sub-Attribute username


LDAP (Active Directory) default group


LDAP (Active Directory) SSO Attribute

userPrincipalName

Secure LDAP (Active Directory) Connection using SSL or TLS
9. Optionally, you can also configure a DNS VIP for your DNS servers.

10. Click **Target Instances** and select the Citrix ADC instances to deploy this Microsoft ADFS proxy configuration. Click **Create** to create the configuration and deploy the configuration on the selected Citrix ADC instances.
Citrix recommends that before executing the actual configuration, you select **Dry Run**. You can first view the configuration objects that are created on the target Citrix ADC instances by the Style-Book. You can then click **Create** to deploy the configuration on the selected instances.

**Objects created**

Several configuration objects are created when the ADFS proxy configuration is deployed on the Citrix ADC instance. The following image displays the list of objects created.
### Objects Added on Instance: 192.168.153.160 | Count: 57

<table>
<thead>
<tr>
<th>Type</th>
<th>Meta Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsfeature</td>
<td>action: enable</td>
</tr>
<tr>
<td></td>
<td>feature: cs lb ssl rewrite aaa</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>lbvserver</td>
<td>ipv4: 192.50.50.12</td>
</tr>
<tr>
<td></td>
<td>name: ns-adfs-dep01-adfs-dns</td>
</tr>
<tr>
<td></td>
<td>port: 53</td>
</tr>
<tr>
<td></td>
<td>servicetype: DNS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>ip: 10.30.30.5</td>
</tr>
<tr>
<td></td>
<td>name: ns-adfs-dep01-dns-svc-1</td>
</tr>
<tr>
<td></td>
<td>port: 53</td>
</tr>
<tr>
<td></td>
<td>servicetype: DNS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>lbvserver_service_binding</td>
<td>name: ns-adfs-dep01-adfs-dns</td>
</tr>
<tr>
<td></td>
<td>servicename: ns-adfs-dep01-dns-svc-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticationnegotiateaction</td>
<td>domain: ADFS.CITRIX.COM</td>
</tr>
<tr>
<td></td>
<td>domainuser: nsroot</td>
</tr>
<tr>
<td></td>
<td>domainuserpasswd: nsroot</td>
</tr>
<tr>
<td></td>
<td>name: ns-adfs-dep01-negotiate-action</td>
</tr>
<tr>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>ns-adfs-dep01-negotiate-action</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>ns-adfs-dep01-negotiate-policy</td>
</tr>
<tr>
<td><strong>rule</strong></td>
<td>true</td>
</tr>
<tr>
<td><strong>delegateduser</strong></td>
<td>nsroot</td>
</tr>
<tr>
<td><strong>kcdaccount</strong></td>
<td>ns-adfs-dep01-adfs-auth401-kcd</td>
</tr>
<tr>
<td><strong>kcdpassword</strong></td>
<td>nsroot</td>
</tr>
<tr>
<td><strong>realmstr</strong></td>
<td>ADFS.CITRIX.COM</td>
</tr>
<tr>
<td><strong>kcddaccount</strong></td>
<td>ns-adfs-dep01-adfs-auth401-kcd</td>
</tr>
<tr>
<td><strong>persistentcookie</strong></td>
<td>ON</td>
</tr>
<tr>
<td><strong>sso</strong></td>
<td>ns_true</td>
</tr>
<tr>
<td><strong>authenticationvserver</strong></td>
<td>ADFS.CITRIX.COM</td>
</tr>
<tr>
<td><strong>ipv46</strong></td>
<td>192.50.50.40</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>ns-adfs-dep01-adfs-auth401-auth-vserver</td>
</tr>
<tr>
<td><strong>servicetype</strong></td>
<td>SSL</td>
</tr>
</tbody>
</table>
**Type : sslvserver_sslcertkey_binding**

- **certkeyname**: adfs-certificate
- **vservername**: ns-adfs-dep01-adfs-auth401-auth-vserver

**Type : authenticationvserver_authorizationpolicy_binding**

- **name**: ns-adfs-dep01-adfs-auth401-auth-vserver
- **policy**: ns-adfs-dep01-negotiate-policy
- **priority**: 10

**Type : authenticationvserver_tmsessionpolicy_binding**

- **name**: ns-adfs-dep01-adfs-auth401-auth-vserver
- **policy**: ns-adfs-dep01-adfs-auth401-tmsession-policy
- **priority**: 10

**Type : authenticationldapaction**

- **authentication**: ENABLED
- **authtimeout**: 30
- **followreferrals**: OFF
- **ldapbase**: dc=netscaler,dc=com
- **ldapbinddn**: cn=Manager,dc=netscaler,dc=com
- **ldapbinddnpassword**: nsroot
- **ldaploginname**: samAccountname
- **name**: ns-adfs-dep01-ldap-action
- **passwdchange**: DISABLED
- **sectype**: PLAINTEXT
- **serverip**: 10.30.30.3
- **serverport**: 369
- **ssonameattribute**: userPrincipalName
- **svrtype**: AD
- **validateservercert**: NO

**Type : authenticationpolicy**

- **action**: ns-adfs-dep01-ldap-action
- **name**: ns-adfs-dep01-ldap-policy
- **rule**: true
<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kcdaccount</code></td>
<td>ns-adfs-dep01-adfs-ldap-kcd-acc</td>
</tr>
<tr>
<td><code>realmstr</code></td>
<td>ADFS.CITRIX.COM</td>
</tr>
<tr>
<td><code>kmsessionaction</code></td>
<td>ns-adfs-dep01-adfs-ldap-kmsession-action</td>
</tr>
<tr>
<td><code>name</code></td>
<td>ns-adfs-dep01-adfs-ldap-kmsession-policy</td>
</tr>
<tr>
<td><code>rule</code></td>
<td>ns_true</td>
</tr>
<tr>
<td><code>authvserver</code></td>
<td>ns-adfs-dep01-adfs-ldap-auth-vserver</td>
</tr>
<tr>
<td><code>port</code></td>
<td>443</td>
</tr>
<tr>
<td><code>servicetype</code></td>
<td>SSL</td>
</tr>
<tr>
<td><code>sslserver_sslcertkey_binding</code></td>
<td>adfs-certificate</td>
</tr>
<tr>
<td><code>vservername</code></td>
<td>ns-adfs-dep01-adfs-ldap-auth-vserver</td>
</tr>
<tr>
<td><code>authvserver_authenticationpolicy_binding</code></td>
<td>ns-adfs-dep01-adfs-ldap-auth-vserver</td>
</tr>
<tr>
<td><code>policy</code></td>
<td>ns-adfs-dep01-ldap-policy</td>
</tr>
<tr>
<td><code>priority</code></td>
<td>10</td>
</tr>
</tbody>
</table>
**Type**: authenticationvserver_tmsessionpolicy_binding

- **name**: ns-adafs-dep01-adafs-ldep-auth-vserver
- **policy**: ns-adafs-dep01-adafs-ldep-tmsession-policy
- **priority**: 10

**Type**: csvserver

- **ipv4**: 192.50.50.50
- **name**: ns-adafs-dep01-cs
- **port**: 443
- **servicetype**: SSL

**Type**: lbvserver

- **ipv4**: 192.50.50.50
- **name**: ns-adafs-dep01-ns-adafs-dep01-adafs-federationproxy-lb
- **port**: 445
- **servicetype**: SSL

**Type**: servicegroup

- **servicegroupname**: ns-adafs-dep01-ns-adafs-dep01-adafs-federationproxy-svcgrp
- **servicetype**: SSL

**Type**: lbvserver_servicegroup_binding

- **name**: ns-adafs-dep01-ns-adafs-dep01-adafs-federationproxy-lb
- **servicegroupname**: ns-adafs-dep01-ns-adafs-dep01-adafs-federationproxy-svcgrp

**Type**: server

- **ipaddress**: 192.30.30.30
- **name**: 192.30.30.30

**Type**: servicegroup_servicegroupmember_binding

- **ip**: 192.30.30.30
- **port**: 443
- **servicegroupname**: ns-adafs-dep01-ns-adafs-dep01-adafs-federationproxy-svcgrp
<table>
<thead>
<tr>
<th>Type</th>
<th>sslvserver_sslcertkey_binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>certkeyname</td>
<td>adfs-certificate</td>
</tr>
<tr>
<td>vservename</td>
<td>ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>csaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction</td>
</tr>
<tr>
<td>targetlbvserver</td>
<td>ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>cspolicy</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction</td>
</tr>
<tr>
<td>policymame</td>
<td>ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol</td>
</tr>
<tr>
<td>rule</td>
<td>HTTPREQ.URL.CONTAINS(&quot;/adfs/services/trust&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>csvserver_cspolicy_binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>ns-adfs-dep01-cs</td>
</tr>
<tr>
<td>policymame</td>
<td>ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol</td>
</tr>
<tr>
<td>priority</td>
<td>9800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>lbvserver</th>
</tr>
</thead>
<tbody>
<tr>
<td>appflowlog</td>
<td>ENABLED</td>
</tr>
<tr>
<td>authentication</td>
<td>ON</td>
</tr>
<tr>
<td>authenticationhost</td>
<td>ADFS.CITRIX.COM</td>
</tr>
<tr>
<td>authn401</td>
<td>OFF</td>
</tr>
<tr>
<td>authnsvname</td>
<td>ns-adfs-dep01-adfs-ldap-auth-vserver</td>
</tr>
<tr>
<td>downstateflush</td>
<td>ENABLED</td>
</tr>
<tr>
<td>ipv46</td>
<td>192.50.50.50</td>
</tr>
<tr>
<td>lbmethod</td>
<td>LEASTCONNECTION</td>
</tr>
<tr>
<td>name</td>
<td>ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb</td>
</tr>
<tr>
<td>port</td>
<td>446</td>
</tr>
<tr>
<td>servicetype</td>
<td>SSL</td>
</tr>
</tbody>
</table>
**Type : servicegroup**

*servicegroupname*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svgrp  
*servicetype*: SSL

---

**Type : lbvserver_servicegroup_binding**

*name*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb  
*servicegroupname*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svgrp

---

**Type : servicegroup_servicegroupmember_binding**

*ip*: 192.30.30.30  
*port*: 443  
*servicegroupname*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svgrp

---

**Type : sslvserver_sslcertkey_binding**

*certkeyname*: adfs-certificate  
*vservenname*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

---

**Type : csaction**

*name*: ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction  
*targetlbvserver*: ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

---

**Type : cspolicy**

*action*: ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction  
*policynname*: ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol  
*rule*: HTTPREQUURLCONTAINS("/adfs/ls/auth/integrated") | | HTTPREQUURLCONTAINS("/adfs/ls/wia")

---

**Type : csvserver_cspolicy_binding**

*name*: ns-adfs-dep01-cs  
*policynname*: ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol  
*priority*: 9900
Type: cspolicy

action: ns-adfs-dep01-cs-adfs-dep01-adfs-active-csaction
policyname: ns-adfs-dep01-cs-adfs-dep01-adfs-active-cspol
rule: true

Type: csvserver_cspolicy_binding

name: ns-adfs-dep01-cs
policyname: ns-adfs-dep01-cs-adfs-dep01-adfs-active-cspol
priority: 10000

Type: sslvserver_sslcertkey_binding

certkeyname: adfs-certificate
vservername: ns-adfs-dep01-cs

Type: rewritepolicylabel

labelname: ns-adfs-dep01-request-rewritepolicylabel
transform: HTTP_REQ

Type: rewritepolicylabel

labelname: ns-adfs-dep01-response-rewritepolicylabel
transform: HTTP_RES

Type: rewriteaction

name: ns-adfs-dep01-HTTPREQ.URL-rewrite-action
stringbuilderexpr: "/adfs/services/trust/proxmex"
target: HTTPREQ.URL
type: REPLACE

Type: rewritepolicy

action: ns-adfs-dep01-HTTPREQ.URL-rewrite-action
name: ns-adfs-dep01-HTTPREQ.URL-rewrite-policy
rule: HTTPREQ.URL CONTAINS("/adfs/services/trust") &

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Oracle e-business Stylebook

August 1, 2019

Oracle E-Business Suite is the most comprehensive suite of integrated, global business applications. This suite enables organizations to make better decisions, reduce costs, and increase performance and consists of the following applications.

- Enterprise resource planning (ERP)
- Customer relationship management (CRM)
- Supply-chain management (SCM)

These computer applications are either developed or acquired by Oracle. The Oracle E-Business Suite 12.2 StyleBook allows you to deploy the configuration on the selected Citrix ADC instances.

This StyleBook creates a load balancing configuration that comprises a load balancing virtual server, a service group, and a list of services. It also binds the services to the service group and binds the service group to the virtual server. You can choose encrypted communication by selecting SSL and providing the SSL files and key files from your local system.
To create a configuration for Oracle E-Business Suite 12.2

1. In Citrix Application Delivery Management (ADM), navigate to Applications > Configuration > StyleBooks. The StyleBooks page displays all the StyleBooks that are available in your Citrix ADM. Scroll down and select Oracle E-Business Suite 12.2. You can also use the search option to search the StyleBook.

2. Click Create Configuration in the StyleBook panel.

3. Type the name of the load balancer application and the virtual IP address in the load balancer settings section.

4. Select the required protocol. You have two options here - HTTP and HTTPS/SSL. You can also type the port number.

5. Type the IP addresses of all the Oracle E-Business Suite application servers in the network that are to be load balanced. Click + to add more server IP addresses.

6. In SSL Certificates Settings section, select the respective files from your local storage. You can also enable Advanced Certificate Settings check box. Here, you can configure more details such as certificate expiry notification period. You can also enable or disable the certificate expiry monitor.

Select the target Citrix ADC instance on which the configuration must be created, and click Create.
You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window. The refresh icon is currently available only on Citrix ADM.

Create and use custom StyleBooks

August 1, 2019

You can write your own StyleBook for your deployment, import it to Citrix Application Delivery Management (ADM), and create configuration objects. You can also use API to create configurations from your StyleBooks.

This document includes the following information:

Before you begin

Before you begin creating StyleBooks, make sure you have knowledge of the following:

- NITRO API. For more information, see Nitro API documentation
- YAML

StyleBook files use the YAML format. For information about the YAML format, see YAML Syntax.

The following is a list of YAML guidelines you must be aware of while creating StyleBooks:

- YAML is case sensitive.
- YAML requires proper indentation
- Use `<spacebar>` key to create proper indentation. Do not use `<tab>` key. Using `<tab>` key creates compilation error while importing your StyleBook to MA Service.
- Do not use strings within quotation marks. Include the string within quotation marks only if a string contains punctuation marks (dashes, colons, and so on.) If you want to interpret a number as a string, either include the number within quotation marks or use the `str()` built-in function of StyleBooks.
- Literals like YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/ON/OFF/Off/off, and TRUE/falsey/-FALSE/FALSE/False/false/falsely are considered Booleans, and are equivalent to true and false respectively. To interpret them as strings, include them within quotation marks. For example:
  - “YES”
  - “No”
- “True”
- “False” and so on.

**Note**
Before importing your StyleBook file into Citrix ADM, it is recommended that you validate if your file is compliant with the YAML format. Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

While configuring StyleBooks, you can only use Nitro Configuration resources that support the **Create** and **Delete** operations (POST and DELETE HTTP methods). For more information, see the [Nitro APIs documentation](#).

**Anatomy of a StyleBook**

Writing StyleBooks requires that you understand the grammar, syntax, and structure of StyleBooks. A typical StyleBook has the following sections:

- **Header**: This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.

- **Import StyleBooks**: This section lets you declare which other StyleBook you want to refer to from your current StyleBook. Importing Citrix ADC NITRO configuration StyleBooks or other StyleBooks is required to write a StyleBook. This is a mandatory section.

- **Parameters**: This section lets you define the parameters you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. This is an optional section.

- **Components**: This section lets you define the entities (configuration objects) that are created by the StyleBook for a specific configuration. This section is considered as the core of a StyleBook. Components generally use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section.

A StyleBook may have a parameters section, or a components section, or both. A StyleBook with only the parameters section is useful to define a list of parameters that can be used by other StyleBooks. This promotes reusability of parameter groups across a set of StyleBooks. A StyleBook with only a components section may be used when you want to specify the values for attributes in the StyleBook instead of defining parameters to take user input.

- **Outputs**: While the parameters section defines the inputs of the StyleBook, this optional section defines its outputs. In this optional outputs section, you can specify the components that you want to expose to users creating a configuration from this StyleBook and to other StyleBooks that import this StyleBook. Users and importing StyleBooks can then reference the properties of the exposed components.
• **Operations**: A StyleBook may contain an optional section to enable Analytics in Citrix ADM on any virtual server that is part of the StyleBook.

The following figure shows a simple outline of a StyleBook.

The following examples help you learn about the grammar and structure of a StyleBook and how to write StyleBooks with increasing levels of complexity.

  - StyleBook to create a load balancing virtual server
  - StyleBook to create a basic load balancing configuration
  - Create a composite StyleBook
  - Customize your StyleBook by using GUI attributes

**StyleBook to create a load balancing virtual server**

August 1, 2019

In this example, you design a basic StyleBook that creates a load balancing virtual server of HTTP protocol type and listening on port 80. The virtual server name, IP address, and load balancing method
parameters accept user-defined values, that is, they are the parameters of the StyleBook.

**Header**

The first six lines of a StyleBook comprise the header section. In this example, the header section is written as follows:

```plaintext
name: lb-vserver
description: This StyleBook defines a load balancing virtual server configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
```

The header section includes the following details:

- **name**: A name for this StyleBook.
- **description**: A description defining what this StyleBook does. This description appears on Citrix ADM.
- **display-name**: A descriptive name for the StyleBook that appears on Citrix ADM.
- **namespace**: A namespace forms part of a unique identifier for a StyleBook to avoid name collisions.
- **schema-version**: Always takes the value “1.0” in this release.
- **version**: The version number of the StyleBook. You can change the version number when you update the StyleBook.

The combination of **name**, **namespace**, and **version** uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in Citrix ADM. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.

**Note**

Consider that you have updated your StyleBook and you have an updated version number. Now if you are referring to (that is, if you are importing) this StyleBook in other StyleBooks, ensure to update the version number in other StyleBooks too, so that they use the correct version of the imported StyleBook.
Import StyleBooks

The section after header is called “import-stylebooks.” In this section, you must declare the namespace and version number of any other StyleBook that you want to refer to in your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook.

In this example, the import-stylebooks section is written as follows:

```
import-stylebooks:
  - namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
```

Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the Citrix ADC NITRO types, such as lbvserver. As software versions 10.5 and later are supported, you can use your StyleBook to create and run configurations on any Citrix ADC instance running release 10.5 and later.

The prefix used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. In this case, ns refers to netscaler.nitro.config of version 10.5. In the later sections of your StyleBook, instead of using the namespace and version to refer to the imported StyleBook, you can use the prefix string chosen, for example, ns, in the example above.

The version used in the StyleBooks is the Citrix ADC NITRO version. A StyleBook that is based on Nitro version X can be used to configure any Citrix ADC that is version X or higher.

Note

To ensure that your StyleBooks can be used to configure any Citrix ADC instance of version 10.5 or later, Citrix recommends that for maximum compatibility you should import the Nitro 10.5 namespace in your StyleBooks that directly use Nitro built-in StyleBooks (namespace: netscaler.nitro.config, version: 10.5).

It is important that a StyleBook that imports other StyleBooks need to be based on a Nitro version that is at the same or higher version than the StyleBooks it imports. For example, a StyleBook that is based on Nitro version 10.5 cannot depend on or use or import a StyleBook that is based on 11.1. But a StyleBook based on version 11.1 can import a StyleBook based on any version less than 11.1.

It is also possible that a StyleBook that doesn’t import the Nitro namespace at all. That means a StyleBook need not directly define Nitro components but can import (depend on) StyleBooks that defines Nitro components. The StyleBook that imports other StyleBooks always acquires the highest Nitro version in the hierarchy of its dependencies and could therefore be used to configure Citrix ADCs that are of that version or higher.
Parameters

The parameters section lets you declare all the parameters that you need in your StyleBook. You, as the StyleBook developer, have to decide what is the input that you want the users of your StyleBook to specify. In this example, you have built your StyleBook in a way that requires its users to provide the name of the virtual server, its IP address, and the load balancing method.

The parameters section would look as follows:

```yaml
parameters:
- name: name
  type: string
  label: Application Name
  description: Name of the application configuration.
  required: true

- name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

- name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for load balancing client request between the application servers.
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
```

Note

If you do not provide the label of a parameter, then Citrix ADM uses the name attribute when displaying this parameter. You must always define a label for your parameters so that you can control how they show up in Citrix ADM.

When using the APIs however, the parameter is designated by its name.

In this section, you have declared three parameters indicated by their name attribute values - name for virtual server name, ip for IP address of the virtual server, and lb-alg for the load balancing method.
• **type.** Type of value these parameters can take. For example, name and lb-alg can take a string value and the ip value has to be of type ip address. Parameters in a StyleBook can be of any of the following built-in types:

• **string.** An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.

• **number.** An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.

• **boolean.** Can be either true or false. Also, note that all the literals are considered by YAML as booleans (for example, Yes or No).

• **ipaddress.** A string that represents a valid IPv4 or IPv6 address.

• **tcp-port.** A number between 0 and 65535 that represents a TCP or UDP port.

• **password.** An opaque/secret string value. When Citrix ADM displays a value for this parameter, it is shown as asterisks (*****).

• **certfile.** Certificate file.

• **keyfile.** Certificate private key file.

• **file.** A parameter of this type requires the user to upload a file, for example, a certificate or key file.

• **object.** Consists of multiple elements and each of these elements is a parameter. This type can be used to group multiple related parameters under one parent parameter.

• **required.** States whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations using this StyleBook. By default, all parameters are optional. In this example, **name** and **ip** are mandatory parameters while **lb-alg** is an optional parameter, the default value of which is “ROUNDROBIN.”

Use the **default** attribute to assign a default value to an optional parameter. While creating a configuration, if a user does not specify a value, the default value is used. For example, for the **lb-alg** parameter, the default value is ROUNDROBIN.

Use the **allowed-values** attribute to define specific values that a user can choose from when creating a configuration. In this example, you have specified two values for the **lb-alg** parameter - ROUNDROBIN and LEASTCONNECTION.

When you import your StyleBook and use it, Citrix ADM displays a form with these three parameters. The fields displayed for name and ip allow string and ipaddress type of value to be entered, and the lb-alg field is displayed as a drop-down list with ROUNDROBIN selected as the default value.
Note
In addition to built-in types, a parameter can have another StyleBook as its type. This is a way of reusing parameters defined in other StyleBooks.

Components

The last section in this StyleBook is called the components section and is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created by the StyleBook.

For this example, you have to write the components section as follows:

```plaintext
components:
  - name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
```

This example contains only one component. The main attributes of a component are name, type, and properties. The type of a component determines what properties this component provides. Components are of two types:

- **Built-in type.** This type is provided by the system and you do not have to define it, for example, the NITRO entity types “lbvserver” or “servicegroup.” In this example, you are using a built-in component type.

- **Composite type.** This type is the StyleBook that you created and imported into Citrix ADM, or the default StyleBook that is shipped with Citrix ADM. You can learn more about composite StyleBooks in Create a Composite StyleBook.

In this example, you have defined a component called **lbvserver-comp.** This component is of type **ns::lbvserver** (a built-in Nitro type), where “ns” is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section, and “lbvserver” is a Nitro resource in this namespace.

The **properties** defined here are the attributes of the “lbvserver” resource. To learn more about all the available Citrix ADC Nitro resources and their attributes, see the Citrix ADC NITRO REST API documentation.
The properties in this section include the mandatory attributes of the “lbvserver” resource and allows you to specify values for these attributes. In this example, you are specifying static values for service-type and port while the name, ipv46, and lbmethod properties get their values from the input parameters. In the rest of the StyleBook, you can refer to the parameter names defined in the parameters section by using $parameters.<parameter-name> expression, for example, $parameters.ip.

Note

By convention, the prefix “ns” is always used to designate a Citrix ADC Nitro namespace in the “import-stylebooks” section. Though it is not mandatory, Citrix recommends to use the same convention in your own StyleBooks for consistency.

Build your StyleBook

Now that you have defined all the required sections of this StyleBook, bring them all together to build your first StyleBook. Copy and paste the StyleBook content to a text editor, and then save the file as lb-vserver.yaml. Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

The full content of the file lb-vserver.yaml is reproduced below:

```yaml
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP virtual server configuration"
schema-version: "1.0"

import-stylebooks:
- namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
- namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
- name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
To start using your StyleBook to create configurations, you have to import it to Citrix ADM and then use it. For more information, see How to Use User-Defined StyleBooks.

You can also import this StyleBook into other StyleBooks (using the import-stylebooks construct.) Or, you can modify this StyleBook to include more parameters and components as described in the next section.

**StyleBook to create a basic load balancing configuration**

August 1, 2019
In the previous example, you have built a basic StyleBook to create a load balancing virtual server. You can save this StyleBook with a different name and then update it to include additional parameters and components for a basic load balancing configuration. Save this StyleBook file as `basic-lb-config.yaml`.

In this section, you will design a new StyleBook that creates a load balancing configuration comprising of load balancing virtual server, a service group, and a list of services. It also binds the services to the service group and binds the service group to the virtual server.

**Header**

To build this StyleBook, you have to start by updating the header section. This section is similar to the one you created for load balancing virtual server StyleBook. In the header section, change the value of `name` to `basic-lb-config`. Also, update `description` and `display-name` to describe this StyleBook appropriately. You do not have to change the `namespace` and `version` values. Because you have changed the name, the combination of name, namespace, and version creates a unique identifier for this StyleBook in the system.

```yaml
name: basic-lb-config
description: This StyleBook defines a simple load balancing configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
```

**Import StyleBooks**

The import-stylebooks section remains the same. It refers to the netscaler.nitro.config namespace to use the Nitro configuration objects.

```yaml
import-stylebooks:
- namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
```

**Parameters**

You have to update the parameters section to add two additional parameters to define the list of services or servers and the port on which the services listen to. The first three parameters, name, ip, and
lb-alg remain the same.

```yaml
parameters:
- name: name
  type: string
  label: Application Name
  description: Name of the application configuration
  required: true

- name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access
  required: true

- name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm used for load balancing client requests between the application servers.
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN

- name: svc-servers
  type: ipaddress
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true

- name: svc-port
  type: tcp-port
  label: Server Port
  description: The TCP port open on the application servers to receive requests.
  default: 80
```

In this example, the parameter `svc-servers` is added to accept a list of IP addresses of the services that represent the backend servers of the application. This is a mandatory parameter as indicated by `required: true`. The second parameter, `svc-port`, denotes the port number on which the servers listen. The default port number is 80 for `svc-port` parameter, if it is not specified by the user.
Components

You have to also update the components section to define additional components such that they use the two new parameters and build the complete load balancing configuration.

For this example, you have to write the components section as follows:

```plaintext
components:
- name: lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg

components:
- name: svcg-comp
type: ns::servicegroup
properties:
  name: $parameters.name + "-svcgrep"
servicetype: HTTP

components:
- name: lbvserver-svg-binding-comp
type: ns::lbvserver\_servicegroup\_binding
properties:
  name: $parent.parent.properties.name
  servicegroupname: $parent.properties.name

- name: members-svcg-comp
type: ns::servicegroup\_servicegroupmember\_binding
repeat: $parameters.svc-servers
repeat-item: srv
properties:
  ip: $srv
  port: str($parameters.svc-port)
  servicegroupname: $parent.properties.name
```

In this example, the original component `lbvserver-comp` (from the previous example) now has a child component called `svcg-comp`. And, the `svcg-comp` component has two child components within it.
Nesting a component within another component allows the nested component to create configuration objects by referring to attributes in the parent component. The nested component can create one or more objects for each object created in the parent component.

The `svcg-comp` component is used to create a service group on the Citrix ADC instance by using the values provided for the attributes of the resource “servicegroup”. In this example, you are specifying static value for servicetype, while name gets its value from the input parameter. You refer to the parameter `name` defined in the parameters section by using `$parameters.name + “-svcgrp”` notation, where `-svcgrp` is appended (concatenated) to the user-defined name.

The component `svcg-comp` has two child components, `lbvserver-svg-binding-comp` and `members-svcg-comp`.

The first child component, `lbvserver-svg-binding-comp`, is used to bind a configuration object between the service group created by its parent component and the load balancing virtual server (lbvserver) created by the parent’s parent component. The `$parent` notation, also called the parent reference, is used to refer to entities in the parent components. For example, `servicegroupname: $parent.properties.name` refers to the service group created by the parent component `svcg-comp`, and `name: $parent.parent.properties.name` refers to the virtual server created by the parent’s parent component `lbvserver-comp`.

The `members-svcg` component is used to bind configuration objects between the list of services to the service group created by the parent component. The creation of multiple binding configuration objects is achieved by using the `repeat` construct of StyleBook to iterate over the list of servers specified in the parameter `svc-servers`. During the iteration, this StyleBook component creates a Nitro configuration object of type `servicegroup_servicegroupmember_binding` for each service (referred to as srv in the `repeat-item` construct) in the service group, and it sets the `ip` attribute in each Nitro configuration object to the IP address of the corresponding server.

Generally, you can use the `repeat` and `repeat-item` constructs in a component to make that component build multiple configuration objects of the same type. You can assign a variable name to the `repeat-item` construct, for example, `srv`, to designate the current value in the iteration. This variable name is referred to in the properties of the same component or in child components as `$<varname>`, for example `$srv`.

In the above example, you have used nesting of components inside each other to easily construct this configuration. In this particular case, nesting of components was not the only way of building the configuration. You could have achieved the same result without nesting, as shown below:

```plaintext
components:
- name: members-svcg-comp
type: ns::servicegroup\_servicegroupmember\_binding
repeat: $parameters.svc-servers
repeat-item: srv
```
Here, all the components are at the same level (that is, they are not nested) but the result achieved (the Citrix ADC configuration generated) is the same as that of the nested components used earlier. Also, the order in which the components are declared in the StyleBook does not impact the order of creation of the configuration objects. In this example, the components `svcg-comp` and `lbvserver-comp`, even though declared last, must be built before building the second component `lbvserver-svg-binding-comp` because there are forward references to these components in the second component.

**Note**

By convention, the names of StyleBooks, parameters, substitutions, components and outputs are in lowercase. When they contain multiple words, they are separated by a “-“ character. For example “lb-bindings”, “app-name”, “rewrite-config”, and so on. Another convention is to suffix component names with “-comp” string.

**Outputs**

The last section you can add to the new StyleBook is the outputs section where you specify what this StyleBook exposes to its users (or in other StyleBooks) after it is used to create a configuration.
For example, you can specify in the outputs section to expose the lbvserver and the servicegroup configuration objects that would be created by this StyleBook.

```yaml
outputs:
- name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver configuration object
- name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup configuration object
```

The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import this StyleBook more flexibility as you can see when creating a composite StyleBook.

**Note**

It is a good practice to expose an entire component of the StyleBook in the outputs section, rather than just a single property of a component (for example, expose the whole $components.lbvserver-comp rather than just the name $components.lbvserver-comp.properties.name). Also add a description to the output explaining what the specific output represents.

**Build your StyleBook**

Now that you have defined all the required sections of this StyleBook, bring them all together to build your second StyleBook. You have already saved this StyleBook file as `basic-lb-config.yaml`. Citrix recommends that you use the built-in YAML validator in StyleBooks page to validate and import the YAML content.

The full content of the file `basic-lb-config.yaml` is reproduced below:

```yaml
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"

display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing configuration.
schema-version: "1.0"
```
import stylebooks:
-
namespace: netscaler.nitro.config
version: "10.5"
prefix: ns
parameters:
-
  name: name
type: string
label: Application Name
description: Give a name to the application configuration.
required: true
-
  name: ip
type: ipaddress
label: Application Virtual IP (VIP)
description: The Application VIP that clients access
required: true
-
  name: lb-alg
type: string
label: LoadBalancing Algorithm
description: Choose the loadbalancing algorithm (method) used for loadbalancing client requests between the application servers.
allowed-values:
  - ROUNDROBIN
  - LEASTCONNECTION
default: ROUNDROBIN
-
  name: svc-servers
type: ipaddress[]
label: Application Server IPs
description: The IP addresses of all the servers of this application
required: true

components:
-
  name: lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg
To start using your StyleBook to create configurations, you have to import it to Citrix ADM and then use it. For more information, see [How to Use User-Defined StyleBooks](#).

You can also import this StyleBook into other StyleBooks and use its properties as described in the next section.
Create a composite StyleBook

August 1, 2019

An important and powerful feature of StyleBooks is that they can be used as building blocks for other StyleBooks. A StyleBook can be imported into another StyleBook and it can be referred to as a type that is used by components of the second StyleBook similar to a Nitro built-in StyleBook.

For example, you can use the basic-lb-config StyleBook that you built in the previous section, to build another StyleBook called composite-example. To use the “basic-lb-config” StyleBook, you have to import it in the new StyleBook in the import-stylebooks section.

Build your StyleBook

The new StyleBook would look as follows:

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
 - namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
 - namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
 - name: name
   type: string
   label: Application Name
   description: Give a name to the application configuration.
   required: true
 - name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
```
<table>
<thead>
<tr>
<th>line</th>
<th>code</th>
<th>description</th>
<th>details</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td></td>
<td>description: The Application VIP that clients access</td>
<td>required: true</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td>- name: svc-servers</td>
<td>type: ipaddress[]</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td>label: Application Server IPs</td>
<td>description: The IP addresses of all the servers of this application</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>- name: response-code</td>
<td>type: string[]</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td>label: List of Response Codes</td>
<td>description: List of Response Codes - Provide a list of response codes in integer.</td>
</tr>
</tbody>
</table>

**components:**

- **name:** basic-lb-comp | type: stlb::basic-lb-config |
  - description: This component’s type is another StyleBook that builds the NetScaler lbvserver, servicegroups and services configuration objects. |
  - properties: name: $parameters.name | ip: $parameters.ip | svc-servers: $parameters.svc-servers |

- **name:** monit-comp | type: ns::lbmonitor |
  - description: This component is a basic Nitro type (a Builtin StyleBook) that builds the NetScaler monitor configuration object. |
  - properties: monitorname: $parameters.name + "-mon" | type: HTTP | respcode: $parameters.response-code |
    - httprequest: "GET /" |
    - lrtm: ENABLED |
    - secure: "YES" |

  **components:**
  - **name:** monit-svcgrp-bind-comp
In the import-stylebooks section, you import the basic-lb-config StyleBook by using its namespace and version, referred to with the prefix “stlb”.

In the components section, two components are defined. The first component is of type stlb::basic-lb-config, where “basic-lb-config” is the name of the StyleBook you created in StyleBook to create a basic load balancing configuration. The properties that are defined for this component correspond to the mandatory parameters declared in the basic-lb-config StyleBook. You can, however, use any parameter of the StyleBook (both required and optional.) Instead of re-building a lbvserver, a service group, and service and service group bindings, you import the StyleBook that does all of this as a component and use it to create these configuration objects in the new StyleBook.

StyleBook adds a second component “monit-comp” that uses the attributes of the Nitro resource “lb-monitor” (a built-in StyleBook) to create a monitor configuration object. It also has a sub-component “monit-svcgrp-bind-comp” to create the binding configuration object that binds the monitor to the servicegroup created in the first component. Because the servicegroup component created in the “basic-lb-config” StyleBook is exposed as an output, this StyleBook can access it using the expression $components.basic-lb-comp.outputs.servicegroup-comp. This is an example of how the outputs section can be used by the importing StyleBooks to have access to components in the imported StyleBooks that they would not have been able to access otherwise.

Next, copy and paste the StyleBook content to a text editor, and then save the file as composite-example.yaml. Ensure to validate the YAML content before you import the file in Citrix ADM. Then, import it to Citrix ADM and create one or several configurations by using this StyleBook.

Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

**Use GUI attributes in a custom StyleBook**

August 1, 2019

You can add GUI attributes in the parameters section of your StyleBook to make the fields intuitive when displayed on Citrix Application Delivery Management (ADM).

**Example.** You can add a descriptive name for the parameter by using the label attribute, and add a tooltip for this parameter by using the description attribute.
Example. If you have a parameter of type object, you can define the layout by using the gui attribute. In this example, the layout is a collapsible object where fields are displayed in two columns.

```plaintext
1 name: svcg-advanced
2 label: Advanced Application Server Settings
3 type: object
4 required: false
5 gui:
6 collapsePane: true
7 columns: 2
```

Example. You can also display a summary view of a parameter of type object[] (list of objects) as a table with the inner parameters representing the columns. To include or exclude an inner parameter from the summary view, you can use the summaryDisplay attribute in the gui section as follows:

```plaintext
1 name: settings
2 label: Settings
3 type: object[]
4 parameters:
5 -
6   name: name
7     label: Name
8     description: Name of this setting
9     type: string
10    gui:
11     summaryDisplay: true
```

Example. Some StyleBooks on Citrix ADM are used only as building blocks for other StyleBooks. And, you might not want users to create configurations directly from these StyleBooks. Because these StyleBooks are to be used as part of other StyleBooks. Mark the StyleBook as private to ensure the StyleBook is not being used directly to create configurations in the Citrix ADM GUI.

```plaintext
1 name: basic-lb-config
2 description: This stylebook defines a simple load balancing configuration.
3 displayName: Load Balancing Configuration
4 namespace: com.example.stylebooks
```
Use custom StyleBooks

August 1, 2019

After you have built your StyleBook, you have to import it to Citrix ADM to use it. Citrix ADM allows you to import a single StyleBook in YAML form or multiple StyleBook YAML files as a bundle in a .zip, .tgz, or .gz form. The Citrix ADM system validates your StyleBooks on import. The Stylebook is now ready to be used for creating configurations.

Citrix ADM also has a built-in YAML editor that you can use to compose the StyleBook YAML contents. The YAML editor allows you to validate your YAML constructs from Citrix ADM GUI itself. You do not need to use a separate tool for these validation checks. The content is validated against YAML standards and any deviation is highlighted. You can then correct the content and attempt to import the StyleBook into Citrix ADM. The built-in YAML editor provides two advantages while writing your own StyleBook.

- **Color coded.** The editor displays the StyleBook content parsed as per YAML guidelines, and the color coding helps you to differentiate easily between the keys and the values defined in YAML content.
- **YAML validation.** The content is validated for any YAML errors as you type in and any deviation is immediately highlighted. This allows you to write text that conforms to YAML guidelines even before you import the StyleBook in Citrix ADM. Currently, the editor validates the content according to YAML guidelines. It does not validate for code correctness and typographical errors.

**Importing your StyleBook**

1. In Citrix ADM, navigate to **Applications > Configuration > StyleBooks**, and then click **Import New StyleBook**.

2. Click one of the three options available for you to import the StyleBook.

   a) **File.** Select the required file or the bundle of files from your local storage.

   Note

   In this example, import the “lb-vserver.yaml” StyleBook that you had created in Style-Book to Create a Load Balancing Virtual Server.
b) **Bundle.** Citrix ADM allows you to import multiple StyleBooks in YAML format. You can import more than one YAML StyleBook file that are compressed in a zip (.zip) format or tarball (.tgz, .gz) format.

```
Choose zip (.zip) or tarball (.tgz, .gz) bundle that includes multiple StyleBook YAML files.
Choose File stylebook-lbvserv-files.zip
```

```Create  Close```

c) **Raw.** Compose the content of your StyleBook in the YAML editor.

**Note**

While composing StyleBook, make sure you have knowledge of the following:

- NITRO API
- YAML

For more information about how to write your own StyleBooks, see [How to Create Your Own StyleBooks](#).
3. Click **Create**.

Citrix ADM now validates your StyleBook for all syntactic and semantic errors according to the StyleBook grammar. Your StyleBook is not imported into Citrix ADM if there are any errors. If there are no errors the StyleBook is successfully imported and is now listed on the StyleBooks page. You can identify the StyleBook by the display name that you had defined in the header section of the StyleBook.

Note

You can also copy and paste the content from a StyleBook YAML file to validate the content.

For more information on StyleBook grammar and syntax of the different constructs and
attributes, see StyleBook Grammar.

4. To create configurations from this StyleBook, click **Create Configuration** link. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

5. Specify the required values for the parameters. In the example below, you can see that **application name** and the **load balancer IP address** fields are displayed as mandatory fields and can accept user values. The **LB Algorithm** has only two values that you can choose from and by default, ROUNDROBIN is selected.

![Application Configuration](image)

6. Under **Target Instances**, click and select the IP address of the Citrix ADC instance where you want to run the configuration. You can also deploy the configuration on more than one Citrix ADC, by specifying as many target instances as needed.

If you want to have a look at the Citrix ADC (Nitro) configuration objects that would be created on your Citrix ADC before actually creating the configuration, click **Dry Run**. If your configuration is valid, the configuration objects that would be created on the basis of the values you have provided are displayed. In this example, only one object of type lbvserver is created by this example StyleBook. This
Ibvserver was the only component that was defined in this basic example StyleBook. You can later click **Create** to actually create the configuration on the selected Citrix ADC instances.

Once the creation completed, the new ConfigPack is listed on the Configurations page.

**Note**

You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.

---

**Search custom StyleBooks**

Citrix ADM now allows you to search for StyleBooks based on their type. That is, you can now search for either default StyleBooks or custom StyleBooks. This option is especially helpful when you have to search for your user-defined StyleBooks amidst a large number of default StyleBooks.

**To search for custom StyleBooks**

1. In Citrix ADM, navigate to **Applications > Configurations > StyleBooks**.
2. Click the search icon at the top right side.
3. In the search bar that appears, select **Type** from the first list, and select **Custom** from the next list of options.
4. Citrix ADM displays only the user-defined StyleBooks.
Create a StyleBook to upload files to Citrix ADM

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) StyleBooks allow you to create Citrix ADC configurations that might include among other things while uploading files of any type from your local filesystem to the Citrix ADC instance, by using the Citrix ADM GUI or the APIs. These files can be the example certificate files or geolocation files. You can also specify the directory to upload these files.

StyleBook configuration

The following is an example StyleBook that describes how to upload a geo-location file on the Citrix ADC instance. The geo files are used typically in GSLB configurations for defining static-proximity based on the geo location:

Build your StyleBook -1

```yaml
1 name: upload-geolocations
2 namespace: com.citrix.adc.stylebooks.samples
3 version: "1.0"
4 display-name: GeoLocation File Upload
5 description: This StyleBook is used to upload a geolocation file to Citrix ADC
6 schema-version: "1.0"
```
**Note**

The parameter used in this example is of a type file. You can import this StyleBook in Citrix ADM and use it to upload geolocation files.

This StyleBook requires the file to be already present in Citrix ADM (for example, you would have already copied it to Citrix ADM using a utility like scp).

If you want to upload a file to Citrix ADCs through Citrix ADM without first copying it to the Citrix ADM filesystem, you can build a StyleBook that has two “string” parameters, one is for specifying the file name to be used on the Citrix ADC and the other to specify the contents of the file, and use these two parameters in the upload-file-comp components. The following is an alternative StyleBook to upload a geo-location file:

**Build your StyleBook - 2**

```python
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
```
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to Citrix ADC
schema-version: "1.0"

import-stylebooks:
- namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns
parameters:
- name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
- name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true
components:
- name: upload-file-comp
  type: ns::systemfile
  properties:
    filename: $parameters.filename
    filelocation: "/var/Citrix ADC/inbuilt_db/"
    filecontent: base64.encode($parameters.filecontents)

Creating configurations to upload files

The following procedure creates a configuration on a selected Citrix ADC instance that would upload a geolocation file using the first StyleBook described above.

To create a configuration for uploading files:

1. In Citrix ADM, navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks that are available in your Citrix ADM. Scroll down and select the StyleBook that you imported.
The StyleBook parameters appear as a user-interface page that allows you to enter the values for all the parameters defined in this StyleBook.

2. Enter the name of the load balancer and the virtual IP address in the basic load balancer settings section.

3. In **Location File** section, enter the name or location of the file.

   **Note**
   Ensure that in Citrix ADM the file is located under the current tenant’s folder only. Use any file transfer protocol to copy the file to Citrix ADM file system.

4. You might be asked to provide your user credentials before you access the target instances.

5. Select the target Citrix ADC instance on which the configuration needs to be created, and click **Create**.

   **Note**
   Citrix recommends that you select **Dry Run** to check the configuration objects that are created on the target instance before you execute the actual configuration on the instance.

When the creation of the configpack is successful, the file is saved on the Citrix ADC instance file system under the location: `/var/netscaler/inbuilt_db/`

**Note**
You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.

**Using the Citrix ADM API to create a configpack**

You can also use the Citrix ADM API to create a configpack that uploads files to the selected Citrix ADC instance. For more information on how to use APIs, see [How to Use API to Create Configurations to Upload Any File Type](#).

**Create a StyleBook to upload SSL certificate and certificate key files to Citrix ADM**

August 1, 2019

When creating a StyleBook configuration that uses the SSL protocol, you must upload the SSL certificate files and certificate key files as required by the StyleBook parameters. StyleBook allows you to
directly upload the SSL files and key files from your local system by using the Citrix ADM GUI. You can also use Citrix ADM APIs to upload certificate files and key files that are already managed by Citrix ADM.

**StyleBook configuration**

This document assists you to create your own StyleBook - **Load Balancing Virtual Server (SSL)** with components to upload SSL certificates and key files. The StyleBook provided here as an example creates a basic load balancing virtual server configuration on the selected Citrix ADC instance. The configuration uses the SSL protocol. To create a configuration using this StyleBook, you must provide the name and IP address of the virtual server, select the load balancing method parameters, and upload the certificate file and the certificate key file for the virtual server, or use a certificate file and certificate key file that are already present in the Citrix ADM. These are specified in the “parameters” section, as shown below:

```json
parameters:

- name: name
type: string
required: true

- name: ip
type: ipaddress
required: true

- name: lb-alg
type: string
allowed-values:
  - ROUNDROBIN
  - LEASTCONNECTION
default: ROUNDROBIN

- name: certificate
label: "SSL Certificate File"
description: "The file name of the SSL certificate file"
type: certfile

- name: key
label: "SSL Certificate Key File"
description: "The file name of the server certificate's private key file"
type: keyfile
```

Two components are then created in the components section of the StyleBook, as shown below. The
“my-lbvserver-comp” component is of type ns::lbvserver, where:

- “ns” is the prefix that refers to the built-in namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section.
- “lbvserver” is a built-in StyleBook in this namespace. It corresponds to the Citrix ADC NITRO load balancing virtual server resource of the same name.

The second component “lbvserver-certificate-comp” is of type stlb::vserver-certs-binds. The prefix “stlb” refers to the namespace “com.citrix.adc.stylebooks” and version 1.0 that is specified in the import-stylebooks section of the StyleBook. If the “com.citrix.adc.stylebooks” namespace can be thought of as a folder, “vserver-certs-binds” is another StyleBook (or a file) in that folder. StyleBooks that are in the namespace “com.citrix.adc.stylebooks” are shipped as part of Citrix ADM.

The “vserver-certs-binds” StyleBook used by user-defined StyleBooks allows you to easily configure the certificates by uploading the certificate and key files to the target Citrix ADC instance, and by configuring the binding of the certificate and key files to the appropriate virtual servers. The properties for this component are - the name of the lb virtual server and the names of the SSL certificates that you provide while creating the configpack.

```
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: SSL
      ipv46: $parameters.ip
      port: 443
      lbmethod: $parameters.lb-alg
    -
      name: lbvserver-certificate-comp
      type: stlb::vserver-certs-binds
      description: Binds lbvserver with server certificate
      properties:
        vserver-name: $components.my-lbvserver-comp.properties.name
        certificates:
          -
            cert-name: $parameters.name + ”-lb-cert”
            cert-file: $parameters.certificate
            ssl-inform: PEM
            key-name: $parameters.name + ”-key”
            key-file: $parameters.key
```

When you use the API to create a configuration from such a StyleBook, use just the file names (not the full file path). These files are expected to be already available in the certificate and
key file folders on Citrix ADM. The uploaded SSL certificate file is stored on Citrix ADM in the /var/mps/tenants/…/ns_ssl_certs directory, and the SSL certificate key file is stored in /var/mps/tenants/…/ns_ssl_keys directory in Citrix ADM.

Creating configurations to upload SSL files

The following procedure creates a basic load balancing virtual server configuration on a selected Citrix ADC instance using the SSL protocol from the StyleBook specified above. You can use this procedure to upload the SSL certificate files and the certificate keys files in Citrix ADM.

To create a configuration for uploading files

1. In Citrix ADM, navigate to Applications > Configuration > StyleBooks. The StyleBooks page displays all the StyleBooks that are available in your Citrix ADM.
2. Scroll down and select Load Balancing Virtual Server (SSL) or type Load Balancing Virtual Server (SSL) in the search field and press the Enter key.
3. Click Create Configuration link in the StyleBook panel.
   The StyleBook parameters appear as a user-interface page that allows you to enter the values for all the parameters defined in this StyleBook.
4. Enter the name of the load balancer and the virtual IP address in the basic load balancer settings section.
5. In SSL Certificates Settings section, select the respective files from your local storage folder. Alternatively, you can select the files present on the Citrix ADM itself.
6. Select the target Citrix ADC instance on which the configuration needs to be created, and click Create.

   Note
   You can also click the refresh icon to add recently discovered Citrix ADC instances in Citrix ADM to the available list of instances in this window.
**Note**

In Citrix ADM, the following default StyleBooks, which are shipped as part of Citrix ADM, enable you to create SSL support by uploading the SSL certificates and keys.

- HTTP/SSL LoadBalancing StyleBook (lb)
- HTTP/SSL LoadBalancing (with Monitors) StyleBook (lb-mon)
- HTTP/SSL Content Switched Application with Monitors (cs-lb-mon)
• Sample Application StyleBook using CS, LB and SSL features (sample-cs-app)

You can also create your own StyleBooks that make use of SSL certificates in the same way as described in the above StyleBook

Build your StyleBook

The full content of the file lb-vserver-ssl.yaml is shown below:

```yaml
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"

parameters:
  -
    name: name
type: string
required: true

  -
    name: ip
type: ipaddress
required: true

  -
    name: lb-alg
type: string
allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
default: ROUNDROBIN

  -
    name: certificate
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
```yaml
label: "SSL Certificate File"
description: "The file name of the SSL certificate file"
type: certfile

- name: key
  label: "SSL Certificate Key File"
description: "The file name of the server certificate's private key file"
type: keyfile

components:
- name: my-lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name
  servicetype: SSL
  ipv46: $parameters.ip
  port: 443
  lbmethod: $parameters.lb-alg

- name: lbvserver-certificate-comp
type: stlb::vserver-certs-binds
description: Binds lbvserver with server certificate
properties:
  vserver-name: $components.my-lbvserver-comp.properties.name
certificates:
- cert-name: $parameters.name + "-lb-cert"
cert-file: $parameters.certificate
  ssl-inform: PEM
  key-name: $parameters.name + "-key"
  key-file: $parameters.key
```

Using the Citrix ADM API to create a configuration pack

You can also use the Citrix ADM API to create a configpack that uploads Cert and Key files to the selected Citrix ADC instance. For more information on how to use APIs, see How to Use API to Create Configurations to Upload Cert and Key Files.
After the StyleBook configuration pack (configpack) is created on Citrix ADM, click **View objects created** to display all the Citrix ADC objects created on the target Citrix ADC instance.
Enable analytics and configure alarms on a virtual server defined in a StyleBook

August 1, 2019

You can use the operations construct to configure Citrix ADM analytics to collect appflow records on all or some of the traffic transactions handled by any virtual server component that is part of a StyleBook. You can also use this construct to configure alarms to get insight into the traffic managed by the virtual server.

The following example shows an operations section of a StyleBook:

```plaintext
operations:
  analytics:
    name: lbvserver-ops
    properties:
      target: $components.basic-lb-comp.outputs.lbvserver
      filter: HTTP.REQ.URL.CONTAINS("catalog")
    alarms:
      name: lbvserver-alarm
      properties:
        target: $outputs.lbvserver
        email-profile: $parameters.emailprofile
        sms-profile: "NetScalerSMS"
      rules:
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: $parameters.period
        metric: "total_bytes"
        operator: "lessthan"
        value: 60
        period-unit: "day"
```

The attributes in the analytics section are used to instruct Citrix ADM analytics feature to collect appflow records on a virtual server component identified by the target property. You can also optionally specify a filter property that accepts a Citrix ADC policy expression to filter requests for
which appflow records are collected on the virtual server.

When a configpack is created from this StyleBook, the Citrix ADM analytics feature is configured to collect appflow records on the virtual servers that were specified when these are created in the process of creating a configpack.

The attributes in the alarms section are used to set thresholds to generate alarms and send notifications on the virtual server identified by the target property. In the above example, the email-profile and sms-profile properties are used to specify where the notifications should be sent. The rules section defines the thresholds. For example, if the total requests handled by the virtual server are greater than 25 and for a period defined by the user, an alarm is set and notification is sent. The “period-unit” specifies how frequently an alarm is triggered. It can take the value of the day, hour, or weekly.

You can use the following operators when comparing the metric value to the threshold value:

- “greaterthan” for “>”
- “lessthan” for “<”
- “greaterthanequal” for “>=”
- “lessthanequal” for “<=”

Note that StyleBooks use API names for the metrics and not the names displayed on the Citrix ADM analytics GUI.

To learn how to view and analyze data collected on virtual servers that were created as part of a configpack, see the Citrix ADM analytics documentation.

**Instance roles**

August 1, 2019

In Citrix Application Delivery Management (ADM), there might be a scenario where you have to configure multiple Citrix ADC instances for a single application, but also where each ADC instance requires a different configuration to be deployed on them. An example of such a case is the default Microsoft Skype for Business StyleBook.

StyleBooks currently support the ability to create a configpack and apply the same configuration on multiple Citrix ADC instances. Such a scenario where the configuration is identical on all ADC instances, can be referred to as a symmetric configuration.

Now, with the “instance roles” feature of StyleBooks, you can create an asymmetrical configuration, that is, a configpack that can be applied on multiple ADC instances, but with different configurations on different ADC instances.
When a StyleBook with instance roles feature is used to create a configpack, each ADC instance in a configpack can be assigned a different role. This role determines the configuration objects of the configpack that the ADC instance will receive.

**Points to note:**

- The set of instance roles in a StyleBook are defined while creating the StyleBook.
- The roles are assigned to a specific ADC instance when creating or updating the configpack.

### Target-roles section

A new section in a StyleBook called “target-roles” is introduced, where all the roles supported by the StyleBook are declared.

This section is typically placed after the “import-StyleBooks” section of a StyleBook, and before the parameters section.

In the following StyleBook example, two roles are defined in within the “target-roles” section - A and B.

```plaintext
1 target-roles:
2   -
3     name: A
4     name: B
5     min-targets: 2
6     max-targets: 5
```

You can see that role B also defines two optional sub-properties, min-targets and max-targets. Though these two sub-properties are optional, min-targets specify the minimum mandatory number of ADC instances that should be assigned this role when creating a configpack from this StyleBook, and max-targets specify the maximum number of ADC instances that can be assigned this role when creating a configpack from this StyleBook.

If these sub-properties are not specified, then there is no limit on the number of ADC instances that can be configured for that role. If min-targets = 0, the configuration associated with that role is optional and if min-targets = 1, then that configuration is mandatory and at least one ADC instance needs to be configured for that role.

### Role “default”

In addition to explicitly defined roles, there is an implicit role that all StyleBooks have, and that role is called as a default role. This role can be used like any other role in a StyleBook. When creating a configpack, if an ADC instance is not assigned with a specific role, the instance gets implicitly assigned to
the “default” role. The instance will now receive any configuration objects generated by components that have the “default” role.

**Components with roles**

After the roles that a StyleBook can support (including the role “default”) are defined, the roles can be used in the components section of a StyleBook. If you want a component to be deployed only on ADC instances that play a certain role, then you can specify the roles attribute as part of the component, as illustrated in the following example of a component:

```plaintext
- name: C1
type: ns::lbvserver
roles:
  - A
properties:
    name: lb1
    servicetype: HTTP
    ipv46: 1.1.1.1
    port: 80
```

In the above example, the component generates an “lbvserver” that will be deployed on instances playing the role A. Note that the roles attribute of a component is a list, and a component can be assigned multiple roles. These roles would have been declared in the “target-roles” section of the StyleBook.

Note: If a component in a StyleBook doesn’t specify a role attribute, then configuration objects generated by the component are created on all Citrix ADC instances regardless of their role. You can use this feature effectively to create configuration objects that can be applied to all instances of a configpack.

Let’s assume that there is a StyleBook with two roles defined - A and B, and which contains four components.

- Component C1 has the roles A and B
- Component C2 has the role B
- Component C3 doesn’t have any roles defined
- Component C4 has the role “default”

The components section of this StyleBook is reproduced below:

```plaintext
components:
- name: C1
type: ns::lbvserver
```
roles:
  - A
  - B

properties:
  name: lb1
  servicetype: HTTP
  ipv46: 1.1.1.1
  port: 80

- name: C2
  type: ns::lbvserver
  roles:
  - B
  properties:
    name: lb2
    servicetype: HTTP
    port: 80

- name: C3
  type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    port: 80

- name: C4
  type: ns::lbvserver
  roles:
  - default
  properties:
    name: lb4
    servicetype: HTTP
    port: 80

Note that the component C3 doesn’t have a role defined, which means the component is deployed on all instances regardless of their role. On the other hand, component C4 has the role “default”, which means it is applied to any instance that doesn’t have an explicit role assigned to it.

Now, consider that you want to create a configpack using this StyleBook, and deploy it on five ADC instances. At this stage, you can assign the roles to the instances in the following manner:

- Role A is assigned to Instances T1, T2, T3 and T4
• Role B is assigned to Instances T2, T3 and T4
• Instance T5 is not assigned any role

The following image summarizes the role assignments, and shows the resulting configuration that each ADC instance will receive:

Note that component C3 is deployed on all instances regardless of role, since this component had no roles attribute.

The following image shows assignment of roles while creating a sample configpack:
You can also use the “Dry Run” feature when creating a configpack to view and verify the correct assignment of roles and the configuration objects that will be created on each ADC instance.

Build your StyleBook

The full content of the StyleBook “demo-target-roles” is provided below:

```yaml
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
```
- name: A
- name: B
  min-targets: 2
  max-targets: 5
components:
- name: C1
type: ns::lbvserver
  roles:
  - A
  - B
  properties:
    name: lb1
    servicetype: HTTP
    ipv46: 1.1.1.1
    port: 80
- name: C2
type: ns::lbvserver
  roles:
  - B
  properties:
    name: lb2
    servicetype: HTTP
    port: 80
- name: C3
type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    port: 80
- name: C4
type: ns::lbvserver
  roles:
  - default
  properties:
    name: lb4
    servicetype: HTTP
The following image shows the objects created for a sample configpack:
<table>
<thead>
<tr>
<th>Objects created (9)</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Instance: 10.102.102.136</td>
</tr>
<tr>
<td><strong>Type: lbserver</strong></td>
</tr>
<tr>
<td>ip: 1.1.1.1</td>
</tr>
<tr>
<td>name: B1</td>
</tr>
<tr>
<td>port: 80</td>
</tr>
<tr>
<td>service-type: HTTP</td>
</tr>
</tbody>
</table>

| **Type: lbserver** |
| ip: 123.123.123.123 |
| name: B2 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 133.133.133.133 |
| name: B3 |
| port: 80 |
| service-type: HTTP |

| **Instance: 10.102.102.135 | Roles: B | Count: 3** |
| **Type: lbserver** |
| ip: 1.1.1.1 |
| name: B1 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 123.123.123.123 |
| name: B2 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 133.133.133.133 |
| name: B3 |
| port: 80 |
| service-type: HTTP |

| **Instance: 10.102.102.62 | Roles: A, default | Count: 3** |
| **Type: lbserver** |
| ip: 1.1.1.1 |
| name: B1 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 123.123.123.123 |
| name: B2 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 133.133.133.133 |
| name: B3 |
| port: 80 |
| service-type: HTTP |

| **Type: lbserver** |
| ip: 141.141.141.141 |
| name: B4 |
| port: 80 |
| service-type: HTTP |
Using APIs

When using the REST API, you can specify roles for each ADC instance when creating or updating the configpack as follows. In the “targets” block, specify the UUID of the specific Citrix ADC instance on which you want to deploy the individual components.

```json
"targets": [
  {
    "id": "<ADC-UUID>",
    "roles": ["A"
  }
]
```

A complete sample REST API is provided for your reference.

```
POST /<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks
```

```json
{
  "configpack": {
    "parameters": {
      "appname": "app1"
    },
    "targets": [
      {
        "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"
      }
    },
    {
      "id": "c08aa1c-1011-48aa-b8c7-9aed1cd38ed0",
      "roles": ["A", "B"]
    },
    {
      "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
```
Create a Stylebook to perform non-CRUD operations

August 1, 2019

StyleBooks manage Citrix ADC configurations by computing the necessary configuration objects on the Citrix ADC instances. These objects are added, updated or removed from the instance each time you create or update a ConfigPack. That is when you specify the “desired state.”

However, some Citrix ADC configuration objects support a few operations other than create, update or delete (CRUD operations). For example, a load balancer object (lbvserver) or a Citrix ADC feature object (nsfeature) can support the “enable” or “disable” operation. Similarly, Citrix ADC certkeys support the “link” and “unlink” operation to link or unlink a certificate to another certificate. These operations on Citrix ADC objects are called as non-CRUD operations. This section describes how to perform non-CRUD operations on configuration objects that support them using StyleBooks.

Note

The binding between configuration objects (for example, bind a certkey to a lbvserver) is not considered a non-CRUD operation. This is because Nitro bindings are represented as configuration objects in their own right. These objects are created and deleted like any other Citrix ADC configuration object.
Supporting the non-CRUD operations

A new construct called “meta-properties” is added in the component at the same level as the “properties” construct. The only attribute supported in this construct currently is called “action.” This attribute can take values like “enable” or “disable” that are supported by that configuration object.

```plaintext
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    meta-properties
    action: enable
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
```

In the above example, the “my-lbvserver-comp” component is of type “ns::lbvserver.” The “ns” is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section. The “lbvserver” is a NITRO resource in this namespace. As an implicit action, the lbvserver is first created by the StyleBook; then the “enable” operation is performed on it.

The action specified in the meta-properties is performed on the configuration object only during the creation of the ConfigPack. Updates to the ConfigPack do not perform non-CRUD actions.

Note

The value of the action attribute cannot be a StyleBook expression that is evaluated dynamically.

Use API to create configurations from StyleBooks

August 1, 2019

After you have built your StyleBook, you have to import it to Citrix Application Delivery Management (ADM) to use it either by using the Citrix ADM or by using Citrix ADM APIs. Citrix ADM validates your StyleBook when you import it, and if the validation is successful, your StyleBook appears on the Citrix ADM catalog of StyleBooks, ready to be used for creating configurations.

You can now use the StyleBook APIs to create configurations based on this StyleBook. You can use any tool such as the curl command line tool or the Postman chrome browser extension to send HTTP requests to Citrix ADM.
Example 1

Consider the “lb-vserver” StyleBook you have created in StyleBook to Create a Load Balancing Virtual Server. Use REST API to create a configpack from this StyleBook as follows:

```plaintext
POST https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks

Content-Type: application/json
Accept: application/json

{

  "configpack": {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
    },

    "target_devices": [

      {

        "id": "deecee30-f478-4446-9741-a85041903410"
      }

    ]

  }

}
```

In this HTTP request, the id (for example, “deecee30-f478-4446-9741-a85041903410”) is the instance ID of the Citrix ADC instance on which the load balancing virtual server lb1 with IP address 10.102.117.31 is created. The instance ID of the Citrix ADC instance is retrieved from Citrix ADM.

To obtain the ID of an instance managed by Citrix ADM, you can use Citrix ADM APIs. For example, to retrieve the instance ID os a Citrix ADC instance whose IP address is 192.168.153.160, you can use the following API:

```plaintext
```
The response contains the ID in the payload:

```json
200
OK
Content-Type: application/json
{

"errorcode": 0,
"message": "Done",
"operation": "get",
"resourceType": "ns",
"username": "nsroot",
"tenant_name": "Owner",
"resourceName": "",
"ns": [

  {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    ...
    "id": "deecee30-f478-4446-9741-a85041903410",
    ...
  }

}
```

If the configuration (configpack) is successfully created, you receive the following HTTP response:

```json
200 OK
Content-Type: application/json
{

"configpack":
{

"config_id": "1460806080"

}
```
You have created your first configuration (configpack) that is uniquely identified by using the ID 1460806080. You can use this ID to query, update, or delete the configuration.

**Example 2**

You can use the same StyleBook to create another configuration or configpack and execute it on the same or different Citrix ADC instances. In this example, create another configuration and provide a different name and IP address for the virtual server and also specify LEASTCONNECTION as the load balancing method. Deploy this configuration on two Citrix ADC instances.

The HTTP request is as follows:

```plaintext
POST https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks

Content-Type: application/json
Accept: application/json

{  
  "configpack": {
    "parameters": {
      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
    },
    "target_devices": [
      {
        "id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "id": "debecc60-d589-4557-8632-a74032802412"
      }
    ]
  }
}
In this HTTP request, the load balancing virtual server lb2 with IP address 10.102.117.32 is created on the two Citrix ADC instances represented by the ids “deecce30-f478-4446-9741-a85041903410” and “debecc60-d589-4557-8632-a74032802412”.

On successful creation of the configpack, the following HTTP response is received:

```
200 OK
Content-Type: application/json
{
  "configpack": {
    "config_id": "1657696292"
  }
}
```

This new configpack has a different id 1657696292. You can update or remove this configuration by using this id.

**Example 3**

Consider the “basic-lb-config” StyleBook you have created in **StyleBook to Create a Basic Load balancing Configuration**. Use REST API to create a configpack from this StyleBook as follows:

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/basic-lb-config/configpacks

Content-Type: application/json
Accept: application/json
{
  "configpack": {
    "parameters": {
    }
  }
}
```
In this HTTP request, the load balancing configuration is executed on two Citrix ADC instances. You can log on to these Citrix ADC instances to verify whether a virtual server and a service group with two services bound are created.

Example 4

Consider the composite StyleBook `composite-example` you created in Create a Composite StyleBook. Use REST API to create a configpack from this StyleBook as follows:

```json
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpack

Content-Type: application/json
Accept: application/json

"configpack":
```
In this HTTP request, the configuration is created on two Citrix ADC instances represented by their IDs. If you log on to the Citrix ADC instances, you can view the configuration objects created by the “basic-lb-config” StyleBook that was imported into the “composite-example” StyleBook. You can also see a new HTTP monitor called “myapp-mon” that was part of the “composite-example” StyleBook.

On successful creation of the configpack, the following HTTP response is received:

```
200 OK
Content-Type: application/json{
  "configpack": {
    "config_id": "4917276817"
  }
}
```
Updating a configuration

To update this configuration, for example, by adding a new backend server with IP address 10.102.29.54 to the load balancing virtual server myapp, use the API for updating a configpack as follows:

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```json
Content-Type: application/json
Accept: application/json
{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
    }

    ,
    "target_devices": [
    
    { "id": "deec30-f478-4446-9741-a85041903410"
    }

    ,
    { "id": "debecc60-d589-4557-8632-a74032802412"
    }

    ]

  }
}
```

On successful update of the configpack, the following HTTP response is received:

```
200 OK
Content-Type: application/json
{

```
Deleting a configuration

To delete this configuration (from all the Citrix ADC instances), you can use the API for deleting a configpack as follows:

```plaintext
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817

Accept: application/json
```

On successful deletion of the configpack, the following HTTP response is received:

```plaintext
200 OK
Content-Type: application/json
{
  "configpack": {
    "config_id": "4917276817"
  }
}
```

You can log on to the Citrix ADC instance and verify that all the configuration objects that are part of this configpack have been removed.

If you want to remove the configuration from specific Citrix ADC instances instead of from all, use the update configpack operation described above and change the “target_devices” attribute in the JSON payload to remove the specific Citrix ADC instance IDs.

Use API to create configurations to upload certificate and key files

August 8, 2019
Use the StyleBook APIs to create configurations based on this StyleBook. You can use any tool such as the curl command line tool or the Postman chrome browser extension to send HTTP requests to Citrix Application Delivery Management (ADM).

Consider the StyleBook example you created to upload the certificate and key files in How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to Citrix ADM. Use REST API to create a configpack from this StyleBook as follows:

```
POST
https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async

Content-Type: application/json
Accept: application/json

"configpack": {
  "parameters": {
    "lb-appname": "lbmon",
    "lb-virtual-ip": "13.1.11.10",
    "lb-virtual-port": "80",
    "lb-service-type": "HTTP",
    "svc-service-type": "HTTP",
    "svc-servers": [
      {
        "ip": "14.1.1.15",
        "port": "80"
      }
    ],
    "certificates": [
      {
        "cert-name": "server_cert",
        "cert-file": "server_cert.pem",
        "ssl-inform": "PEM",
        "key-name": "server_key",
        "key-file": "server_key.pem",
        "cert-password": "secret",
        "cert-advanced": {
          "is-ca-cert": false,
          "skip-ca-name": false
        }
      }
    ]
  }
}
```
This configpack is uniquely identified by using the id 8c158e7a-0087-423f-91b0-0ccf16de552a. You can
use this ID to query, update, or delete the configuration. On successful update of the configpack, the certificate and key files are uploaded to Citrix ADM file system.

**Use API to create configurations to upload any file type**

August 8, 2019

You can also use the Citrix Application Delivery Management (ADM) API to create a configpack that uploads files to the selected Citrix ADC instance.

Consider the StyleBook example you created to upload files of any type in *How to Create a StyleBook to Upload Files to Citrix ADC MA Service*. As in the example in the above topic, create a configpack and specify the value of the parameter “locationfile” as the file path of the location file on Citrix ADM. Use REST API to create a configpack from this StyleBook as follows:

```plaintext
POST
https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks.samples/1.0/upload-geolocations/configpacks

Content-Type: application/json
Accept: application/json

{
  "configpack": {
    "parameters": {
      "locationfile": "/var/mps/tenants/root/files/custom_geolocations.csv"
    },
    "targets": [{
      "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
    ]}
}
```
Use API to import custom StyleBooks

August 1, 2019

You can now use the StyleBook APIs to import custom StyleBooks into Citrix Application Delivery Management (ADM). Use REST API to create a configpack from this StyleBook as follows in any tool such as the curl command line tool or the Postman chrome browser extension. For example, you can import a StyleBook named example-lb that can be used to create a load balancer configuration on a Citrix ADC instance.

```plaintext
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
  Content-Type: application/json
  Accept: application/json
RequestBody:

{
  "stylebook":
    {
      "file_name": "example-lb.yaml",
      "source": "<base64-contents>",
      "encoding": "base64"
    }
}
```

where, the “source” attribute’s value, is the base64 encoding of the contents of your StyleBook file. You can paste the YAML contents of your StyleBook file in an online tool, for example, https://www.browserling.com/tools/file-to-base64 to obtain the base64 string that you can then use as a value for the “source” attribute above.

Using this API call, you can also upload a compressed tarball file (.tgz file) containing multiple StyleBook files in one API operation. To do this, simply change the file_name attribute to the .tgz filename and the value for the source attribute to the base64 encoding of the contents of your .tgz file.

After the API is run successfully in the tool you get the following response that indicates that the StyleBook has been imported into Citrix ADM.
Use API to download custom StyleBooks

August 1, 2019

You can download a custom StyleBook by providing the following StyleBooks REST API:

```
GET
https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/</VERSION>/</NAME>/actions/download
```

You can run the API in any tool such as the curl command line tool or the Postman chrome browser extension after making modifications to the IP address, name, version, and namespace fields.

```
GET
https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download
```

The StyleBook in the .yaml format is downloaded.
Use API to delete custom StyleBooks

August 1, 2019

You can delete the custom StyleBook by providing the following StyleBooks REST API:

```
1. DELETE
```

If the dependencies query parameter in the URL is not provided or its value is set to false, then the StyleBook dependencies are not deleted (only the StyleBook itself is deleted).

When you receive an HTTP response status code of 200, that means the custom StyleBook (and its dependencies) is successfully removed from Citrix ADM.

**Note**

You cannot delete a custom StyleBook that has other StyleBooks in MA Service that depend on it.

For example, assume that you had created a StyleBook named “lb-virtual-ssl-extended” in Citrix ADM. You later decided to delete that StyleBook.

You can run the API in any tool such as the curl command line tool or the Postman chrome browser extension after making modifications to the IP address, name, version, and namespace fields.

```
DELETE https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false
```

The StyleBook gets deleted from Citrix ADM.
You can design your own StyleBooks, import them to Citrix Application Delivery Management (ADM), and then use them to create configurations either by using Citrix ADM GUI or by using APIs. To be able to create your own StyleBooks, you must first understand the grammar and syntax of the different constructs and attributes you can use.

This document describes the different constructs and references you can use while creating StyleBooks.

Click a section, construct, or reference name in the table below to view the details.

<table>
<thead>
<tr>
<th>Header</th>
<th>Import StyleBooks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Parameters-default-sources construct</td>
</tr>
<tr>
<td>Substitutions</td>
<td>Components</td>
</tr>
<tr>
<td>Optional properties</td>
<td>Helper components</td>
</tr>
<tr>
<td>Properties default sources</td>
<td>Nested components</td>
</tr>
<tr>
<td>Condition construct</td>
<td>Repeat construct</td>
</tr>
<tr>
<td>Repeat-condition construct</td>
<td>Outputs</td>
</tr>
<tr>
<td>Nested repeats</td>
<td>Parent reference</td>
</tr>
<tr>
<td>Parameter reference</td>
<td>Substitutions reference</td>
</tr>
<tr>
<td>Components reference</td>
<td>Operations</td>
</tr>
<tr>
<td>Variable reference</td>
<td>Alarms</td>
</tr>
<tr>
<td>Analytics</td>
<td>Built-in functions</td>
</tr>
<tr>
<td>Expressions</td>
<td>Dependency detection</td>
</tr>
<tr>
<td>In-place interpolations</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

While defining repeat-item, repeat-index, or arguments to substitution functions, do not use the following reserved words to name a user-defined variable, $<var-name>$:

- stylebook, parameters, substitutions, components, properties, outputs, parent, self, oper-
Header

August 1, 2019

The first six lines of a StyleBook comprise the header section. This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.

The following table describes the attributes of the header section:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A name to identify the StyleBook. This attribute is mandatory.</td>
</tr>
<tr>
<td>description</td>
<td>A description defining what a StyleBook does. This description appears on the Citrix ADM GUI. This is an optional attribute.</td>
</tr>
<tr>
<td>display-name</td>
<td>A descriptive name for the StyleBook. This name appears on the Citrix ADM GUI. This is an optional attribute.</td>
</tr>
<tr>
<td>author</td>
<td>The author person or organization who creates the StyleBook. This is an optional attribute.</td>
</tr>
<tr>
<td>namespace</td>
<td>A namespace forms part of a unique identifier for a StyleBook to avoid name collisions. A namespace can be any string, but a good practice is to use it for naming the company, department, or unit that created or owns a set of StyleBooks. For example, you can use the following format: `&lt;company&gt;..&lt;department&gt;..&lt;unit&gt;.stylebooks. This is a mandatory attribute.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>version</td>
<td>The version number of the StyleBook. You can change the version number when you update a StyleBook. StyleBooks of different versions can co-exist together. This is a mandatory attribute.</td>
</tr>
<tr>
<td>schema-version</td>
<td>The version of the StyleBooks schema. It takes the value “1.0” in the current release of Citrix ADM. This is a mandatory attribute.</td>
</tr>
<tr>
<td>private</td>
<td>If this attribute is set to true, the StyleBook is not displayed on the Citrix ADM GUI. This is a useful setting for StyleBooks that are building blocks for other StyleBooks and are not intended to be used by users directly. This is an optional attribute. Its default value is false.</td>
</tr>
</tbody>
</table>

**Example:**

```yaml
1   name: lb
2   description: "This stylebook defines a sample load balancing configuration."
3   display-name: "Load Balancing StyleBook (HTTP)"
4   author: Mike Smith (ACME Infra team)
5   namespace: com.example.stylebooks
6   schema-version: "1.0"
7   version: "0.1"
```

The combination of name, namespace, and version uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in Citrix ADM. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.

**Import StyleBooks**

August 1, 2019
This is the second section of your StyleBook and lets you declare which other StyleBook you want to refer to from your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook. This is a mandatory section.

You must declare the namespace and version number of the StyleBook(s) that you want to refer to in your current StyleBook. Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the Citrix ADC NITRO types, such as lbvserver service or monitor. StyleBooks for Citrix ADC versions 10.5 and later are supported, which means that you can use your StyleBook to create and run configurations on any Citrix ADC instance running release 10.5 or later.

The prefix attribute used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. For example, the “ns” prefix can be used to refer to the namespace netscaler.nitro.config with version 10.5. In the later sections of your StyleBook, instead of using the namespace and version each time you want to refer to a StyleBook with this namespace and version, you can simply use the prefix string chosen together with the name of the StyleBook to uniquely identify it.

Example:

```plaintext
import-stylebooks:
  - namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
  - namespace: com.acme.stylebooks
    version: "0.1"
    prefix: stlb
```

In the above example, the first prefix defined is called ns and refers to the namespace netscaler.nitro.config and version 10.5. The second prefix that is defined is called stlb, and refers to the namespace com.acme.stylebooks and version 0.1.

After you define a prefix, everytime you want to refer to a type or a StyleBook that belongs to a certain namespace and version, you can use the notation `<namespace-shorthand>::<typename>`. For example, `ns::lbvserver` refers to the type lbvserver that is defined in the namespace netscaler.nitro.config, version 10.5.

Similarly, if you want to refer to a StyleBook with version “0.1” in the com.acme.stylebooks namespace, you can use the notation `stlb::<stylebook-name>`.

Note

By convention, the prefix “ns” is used to refer to the NITRO namespace of Citrix ADC.
Parameters

August 1, 2019

This section lets you define all the parameters that you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. Although this is an optional section, most StyleBooks might need one. You can consider the parameters section to define the questions you want users to answer when they use the StyleBook to create a configuration on a Citrix ADC instance.

When you import your StyleBook into Citrix ADM and use it to create a configuration, the GUI uses this section of the StyleBook to display a form that takes input for values of the parameters you have defined.

The following section describes the attributes that you need to specify for each parameter in this section:

name

The name of the parameter you want to define. You can specify an alphanumeric name.

The name must begin with an alphabet, and can include additional alphabets, numbers, hyphen (-), or underscore (_).

Note that when writing a StyleBook, you can use this “name” attribute to refer to the parameter in other sections by using the notation $parameters.<name>.

Mandatory? Yes

label

A string that is displayed in the ADM GUI as the name of this parameter.

Mandatory? No

description

A help string that describes what the parameter is used for. The ADM GUI displays this text when the user clicks the help icon for this parameter.

Mandatory? No
**type**

The type of value these parameters can take. Parameters can be of any of the following built-in types:

- **string**: An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.

- **number**: An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.

- **boolean**: Can be either true or false. Also, note that all the literals are considered by YAML as booleans (for example, Yes or No).

- **ipaddress**: A string that represents a valid IPv4 or IPv6 address.

- **tcp-port**: A number between 0 and 65535 that represents a TCP or UDP port.

- **password**: Represents an opaque/secret string value. When Citrix ADM GUI displays a value for this parameter, it is shown as asterisks (****).

- **certfile**: Represents a certificate file. This allows you to upload the files directly from your local system when you are creating a StyleBook configuration using the ADM GUI. The uploaded certificate file is stored in the directory /var/mps/tenants/ns_ssl_certs in ADM.

  The certificate file will be added to the list of certificates managed by ADM.

- **keyfile**: Represents a certificate key file. This allows you to upload the file directly from your local system when you are creating a StyleBook configuration using the Citrix ADM GUI. The uploaded certificate file is stored in the directory /var/mps/tenants/ns_ssl_keys in Citrix ADM.

  The certificate key file will be added to the list of certificate keys managed by Citrix ADM.

- **file**: Represents a file.

- **object**: This type is used when you want to group several related parameters under a parent element. You have to specify the parent parameter the type as “object”. A parameter of type “object” can have a nested “parameters” section to describe the parameters it contains.

- **another StyleBook**: When you use this type of parameter, then this parameter expects its value to be in the form of the parameters defined in the StyleBook denoting its type.

A parameter can also have a type that is a list of any of the types listed above, by adding “[]” to the end of the type. For example, if the type attribute is string[], this parameter takes a list of strings as input. You can provide one, two, or several strings for this parameter when creating a configuration from this StyleBook.

**Mandatory?** Yes
key

Specify true or false to indicate if this parameter is a key parameter for the StyleBook. A StyleBook can have only one parameter defined as the “key” parameter. When you create different configurations from the same StyleBook (on the same or different Citrix ADC instances), each configuration has a different/unique value for this parameter.

Default value is false.

Mandatory? No

required

Specify true or false to indicate whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations. The Citrix ADM GUI forces the user to provide a valid value for this parameter.

Default value is false.

Mandatory? No

allowed-values

Use this attribute to define a list of valid values for a parameter, when the type is set to “string.” When creating a configuration from the Citrix ADM GUI, the user is prompted to select a parameter value from this list.

Example 1:

name: ipaddress
type: string
allowed-values:
  • SOURCEIP
  • DEST IP
  • NONE

Example 2:

name: TCP Port
type: tcp-port

 allowed-values:

  • 80
  • 81
  • 8080

Example 3:
(list of tcp-ports, where each element of the list can only have values
specified in allowed-values)

 name: tcpports
 type: tcp-port[]
 allowed-values:

  • 80
  • 81
  • 8080
  • 8081

Mandatory? No

default

Use this attribute to assign a default value to an optional parameter. While creating a
configuration, if a user does not specify a value, the default value is used.

When creating the configuration from the Citrix ADM GUI, if a user does not
provide a value for a parameter that does not have a default value, then no value is set
for that parameter.

Example 1:

 name: timeout
 type: number
 default: 20

Example 2:
(where, the default value of the parameter is a list of values):

 name: protocols
 type: string[]
 default:
- TCP
- UDP
- IP

**Example 3:**
name: timeout
type: number
default: 20

**Example 4:**
name: tcpport
type: tcp-port
default: 20

*Mandatory? No*

**pattern**

Use this attribute to define a pattern (regular expression) for the valid values of this parameter, when the type of the parameter is “string.”

**Example:**
name: appname
type: string
pattern: “[a-z]+”

*Mandatory? No*

**min-value**

Use this attribute to define the minimum value for parameters of type “number” or “tcp-port.”

**Example:**
name: audio-port
type: tcp-port
min-value: 5000

The min-value of numbers can be negative, but the min-value for tcp-port should not be negative.

*Mandatory? No*
**max-value**

Use this attribute to define the maximum value for parameters of type “number” or “tcp-port.”

The maximum value should be greater than the minimum value, if defined.

**Example:**

name: audio-port  
type: tcp-port  
min-value: 5000  
max-value: 15000  

**Mandatory?** No

**min-length**

Use this attribute to define the minimum length of values accepted for a parameter of type “string.”

Minimum length of the characters defined as values should be greater or equal to zero.

**Example:**

name: appname  
type: string  
min-length: 3  

**Mandatory?** No

**max-length**

Use this attribute to define the maximum length of values accepted for a parameter of type “string.”

Maximum length of the values should be greater or equal to the length of the characters defined in min-length.

**Example:**

name: appname  
type: string
max-length: 64

Mandatory? No

**min-items**

Use this attribute to define the minimum number of items in a parameter that is a list.

The minimum number of items should be greater or equal to zero.

**Example:**

name: server-ips
type: ipaddress[]
min-items: 2

Mandatory? No

**max-items**

Use this attribute to define the maximum number of items in a parameter that is a list.

The maximum number of items should be greater than the minimum number of items if defined.

**Example:**

name: server-ips
type: ipaddress[]
min-items: 2
max-items: 250

Mandatory? No

**gui**

Use this attribute to customize the layout of the parameter of type “object” in the Citrix ADM GUI.

Mandatory? No
columns

This is a sub-attribute of the gui attribute. Use this to define the number of columns to display in the Citrix ADM GUI.

Mandatory? No

updatable

This is a sub-attribute of the gui attribute. Use this to specify whether the parameter can be updated after the configuration is created.

If the value is set to false, the parameter field is greyed out when you update the configuration.

Mandatory? No

collapse_pane

This is a sub-attribute of the gui attribute. Use this to specify whether the pane defining the layout of this object parameter is collapsible.

If the value is set to true, the user can expand or collapse the child parameters under this parent parameter.

Example:

```
  gui:
    collapse_pane: true
    columns: 2
    updatable: false
```

Example of a complete parameters section:

```
  parameters:
    name: name
    label: Name
    description: Name of the application
```
type: string

required: true

- 
  name: ip
  label: IP Address
  description: The virtual IP address used for this application
  type: ipaddress
  required: true

- 
  name: svc-servers
  label: Servers
  type: object[]
  required: true
  parameters:
    - 
      name: svc-ip
      label: Server IP
      description: The IP address of the server
      type: ipaddress
      required: true

    - 
      name: svc-port
The following is an example that defines all the attributes of a list and the values explained in earlier sections:

```
- label: Server Port
description: The TCP port of the server
type: tcp-port
default: 80

- name: lb-alg
  label: LoadBalancing Algorithm
type: string
  allowed-values:
  - ROUNDROBIN
  - LEASTCONNECTION
  default: ROUNDROBIN

- name: enable-healthcheck
  label: Enable HealthCheck?
type: boolean
default: true
```

```
""YAML
  name: features-list
type: string[]**
min-length: 1
max-length: 3
min-items: 1
```
Parameters-default-sources construct

August 1, 2019

You can use this construct to reuse parameter definitions from other StyleBooks.

Consider a scenario where a parameter or a group of parameters is used repeatedly in multiple StyleBooks. To avoid redefining these parameters, each time you want to create a new StyleBook, you can define them once, and then import their definitions into the StyleBooks that need these parameters by using the parameters-default-sources construct.

For example, if many of your StyleBooks need to configure a virtual IP, you might have to define the same parameters related to virtual IPs in each new StyleBook you create. Instead, you can create a separate StyleBook called, for example, “vip-params” where you define all the parameters related to it as shown in the following example:

```
- name: vip-params
  namespace: com.acme.common types
  version: "1.0"
  description: This StyleBook defines a typical virtual IP config.
  private: true
  schema-version: "1.0"
  parameters:
    - name: lb-appname
      label: Load Balanced Application Name
      description: Name of the Load Balanced application
      type: string
      required: true
```
name: lb-virtual-ip  
label: Load Balanced App Virtual IP address  
description: Virtual IP address representing the Load Balanced application  
type: ipaddress  
required: true

-  
name: lb-virtual-port  
label: Load Balanced App Virtual Port  
description: TCP port representing the Load Balanced application  
type: tcp-port  
default: 80

-  
name: lb-service-type  
label: Load Balanced App Protocol  
description: Protocol used for the Load Balanced application  
type: string  
default: HTTP  
required: true  
allowed-values:
- HTTP
- SSL
- TCP

Then, you can create other StyleBooks that make use of these parameters. Following is an example of such a StyleBook.

name: acme-biz-app  
namespace: com.acme.stylebooks  
version: "1.0"  
description: This stylebook defines the Citrix ADC configuration for Biz App  
schema-version: "1.0"  
import-stylebooks:
-  
  namespace: com.acme.commonetypes  
  prefix: cmtypes  
  version: "1.0"  
parameters-default-sources:  
  - cmtypes::vip-params  
parameters:
In the StyleBook, acme-biz-app, first, the namespace and version of the vip-params StyleBook is imported by using the “import-stylebooks” section. Then the `parameters-default-sources` construct is added, and the StyleBook name, that is, vip-params is specified. This has the same effect as defining the parameters of the vip-params StyleBook directly in this StyleBook.

You can include parameters from multiple StyleBooks because the parameters-default-sources is a list, and each item in the list is expected to be a StyleBook.

In addition to including parameters from other StyleBooks, you can also define your own parameters by using the parameters section. The complete list of parameters of the StyleBook is the combination of parameters included from other StyleBooks and parameters defined in this StyleBook. Therefore, the expression `$parameters` refers to this combination of parameters.

Note that if a parameter is defined both in an imported StyleBook as well as in the current StyleBook, the definition in the current StyleBook overrides the definition imported from another StyleBook. You can use this effectively by customizing a few of the imported parameters if required, while using the rest of the imported parameters as they are.

The parameters-default-sources construct can also be used in nested parameters as shown:

```yaml
parameters:
  - name: monitorname
    label: Monitor Name
    description: Name of the monitor
    type: string
    required: true
  - name: type
    label: Monitor Type
    description: Type of the monitor
    type: string
    required: true
    allowed-values:
      - PING
      - TCP
      - HTTP
      - HTTP-ECV
      - TCP-ECV
      - HTTP INLINE
```

In the StyleBook, acme-biz-app, first, the namespace and version of the vip-params StyleBook is imported by using the “import-stylebooks” section. Then the `parameters-default-sources` construct is added, and the StyleBook name, that is, vip-params is specified. This has the same effect as defining the parameters of the vip-params StyleBook directly in this StyleBook.

You can include parameters from multiple StyleBooks because the parameters-default-sources is a list, and each item in the list is expected to be a StyleBook.

In addition to including parameters from other StyleBooks, you can also define your own parameters by using the parameters section. The complete list of parameters of the StyleBook is the combination of parameters included from other StyleBooks and parameters defined in this StyleBook. Therefore, the expression `$parameters` refers to this combination of parameters.

Note that if a parameter is defined both in an imported StyleBook as well as in the current StyleBook, the definition in the current StyleBook overrides the definition imported from another StyleBook. You can use this effectively by customizing a few of the imported parameters if required, while using the rest of the imported parameters as they are.

The parameters-default-sources construct can also be used in nested parameters as shown:

```yaml
parameters:
  - name: vip-details
    label: Virtual IP details
    description: Details of the Virtual IP
    type: object
```
This is similar to having the parameters of the StyleBook vip-params added directly as child parameters of the vip-details parameter in this StyleBook.

**Substitutions**

August 1, 2019

The substitutions section is used to define shorthand names for complex expressions that can be used in the rest of the StyleBook to make reading the StyleBook easier. They are also useful when the same expression or value is repeated more than once in the StyleBook, for example, a constant value. Using a substitution name for this value allows you to update only the substitution value when this value needs to be changed rather than updating it at every location it appears in the StyleBook, which could be prone to error.

Substitutions are also used for defining mappings between values as described in examples later in this document.

Each substitution in the list is made up of a key and a value. The value can be a simple value, an expression, a function, or a map.

In the following example, two substitutions are defined. The first one is “http-port” that can be used as a shorthand for 8181. By using a substitution, you can refer to this in the rest of the StyleBook as $substitutions.http-port instead of 8181.

**substitutions:**

http-port: 8181

This allows you to specify a mnemonic name to a port number as well as define this port number in one place in the StyleBook, irrespective of the number of times it is used. If you want to modify the port number to 8080, you can modify it in the substitution section, and the change will take effect wherever the mnemonic name http-port is used. The following example shows how a substitution is used in a component.

```
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name + "-lb"
```
A substitution can also be a complex expression. The following example shows how two substitutions use expressions.

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
```

A substitution expression can also use existing substitution expressions as shown in the following example.

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-port) + str("-app")
```

Another useful feature of substitutions is maps, where you can map keys to values. The following is an example of a map substitution.

```
substitutions:
  secure-port:
    true: int("443")
    false: int("80")
  secure-protocol:
    true: SSL
    false: HTTP
```

The following example shows how to use the maps secure-port and secure-protocol.

```
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name + "-lb"
      servicetype: **$substitutions.secure-protocol\[$parameters.is-secure\]**
      ipv46: $parameters.ip
      port: **$substitutions.secure-port\[$parameters.is-secure\]**
      lbmethod: $parameters.lb-alg
```
This implies that if the user of the StyleBook specifies the Boolean value “true” to the parameter insecure, or selects the checkbox corresponding to this parameter in the Citrix ADM GUI, the servicetype property of this component is assigned the value SSL and the port property is assigned the value 443. However, if the user specifies “false” for this parameter or clears the corresponding checkbox in the Citrix ADM GUI, the servicetype property is assigned the value HTTP and the port is assigned the value 80.

The following example shows how to use substitutions as a function. A substitution function can take one or more arguments. Arguments should be of simple type for example, string, number, ipaddress, boolean, and other types.

**substitutions:**

form-lb-name(name): $name + “-lb”

In this example, we define a substitution function “form-lb-name” that takes a string argument called “name” ** and uses it to create a new string that suffixes “-lb” to the string in the name argument. An expression using this substitution function can be written as:

$substitutions.form-lb-name(“my”)

which returns “my-lb”

Consider another example:

**substitutions:**

cspol-priority(priority): 10100 - 100 * $priority

The substitution cspol-priority is a function that takes an argument called priority and uses it to calculate a value. In the rest of the StyleBook, this substitution can be used as shown in the following example:

```
1 components:
2   -
3     name: cspolicy-binding-comp
4     type: ns::csvserver_cspolicy_binding
5     condition: not $parameters.is-default
6     properties:
7         name: $parameters.csvserver-name
8         policymap: $components.cspolicy-comp.properties.policynamer
9         priority: $substitutions.cspol-priority($parameters.pool.priority)
```

Substitution can also be made up of a key and a value. The value can be a simple value, an expression, a function, a map, a list, or a dictionary.

The following is an example of a substitution called ‘slist’ whose value is a list:
The value of a substitution can also be a dictionary of key-value pairs as seen in the following example of a substitution called ‘sdict’ below:

```
substitutions:
sdict:
a: 1
b: 2
c: 3
```

You can create more complex attributes by combining the lists and dictionaries. For example, a substitution called “slistofdict” returns a list of key-value pairs.

```
slistofdict:
a: $parameters.cs1.lb1.port
b: $parameters.cs1.lb2.port
-
a: $parameters.cs2.lb1.port
b: $parameters.cs2.lb2.port
```

But, in the following example, a substitution “sdictoflist” returns a key-value pair, where the value itself is another list.

```
sdictoflist:
a:
  - 1
  - 2
b:
  - 3
  - 4
```

In components, these substitutions may be used in condition, properties, repeat, repeat-condition constructs.

The following example of a component shows how a substitution can be used to when specify the properties:

```
properties:
```
A use case for defining a substitution whose value is a list or a dictionary is when you are configuring a content switching virtual server and multiple load balancing virtual servers. Since all lb virtual servers tied to the same cs virtual server might have an identical configuration, you can use substitution list and dictionary to build this configuration to avoid repeating that configuration for each lb virtual server.

The following example shows the substitution and the component in the cs-lb-mon StyleBooks to create a content switching virtual server configuration. While constructing the properties of cs-lb-mon StyleBooks, the complex substitution “lb-properties” specify the properties of the lb virtual servers associated with the cs virtual server. The “lb-properties” substitution is a function that takes the name, service type, virtual IP address, port, and servers as parameters and generates a key-value pair as the value. In “cs-pools” component, we assign the value of this substitution to lb-pool parameter for each pool.

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
  components:
    -
      name: cs-pools
      type: stlb::cs-lb-mon
      description: Updates the cs-lb-mon configuration with the different pools provided. Each pool with rule result in a dummy LB vserver, cs action, cs policy, and csvector_cspolicy_binding
```
configuration.
condition: $parameters.server-pools
repeat: $parameters.server-pools
repeat-item: pool
repeat-condition: $pool.rule
repeat-index: ndx
properties:
  appname: $parameters.appname + "-cs"
  cs-virtual-ip: $parameters.vip
  cs-virtual-port: $substitutions.cs-port($parameters.protocol == "HTTP")
  cs-service-type: $parameters.protocol
  pools:
    -
      lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP", "0.0.0.0", 0, $pool.servers)
      rule: $pool.rule
      priority: $ndx + 1

Substitution Map:

You can create substitutions that map keys to values. For example, consider a scenario where you want to define the default port (value) to be used for each protocol (key). For this task, write a substitution map as follows.

```plaintext
substitutions:
  port:
    HTTP: 80
    DNS: 53
    SSL: 443
```

In this example, HTTP is mapped to 80, DNS is mapped to 53, and SSL is mapped to 443. To retrieve the port of a certain protocol that is given as a parameter, use the expression

```plaintext
$substitutions.port[$parameters.protocol]
```

The expression returns a value based on the protocol specified by the user.

- If the key is HTTP, the expression returns 80
- If the key is DNS, the expression returns 53
- If the key is SSL, the expression returns 443
- If the key is not present in the map, the expression does not return any value
Components

August 1, 2019

The Components construct in a StyleBook is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created. Using this construct, you can build one or multiple configuration objects of the same type.

The components construct can use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section, although most StyleBooks have a components section.

The following table describes the main attributes of a component.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the component. You can specify an alphanumeric name. The name must begin with an alphabet, and can include additional alphabets, numbers, hyphen (-), or underscore (_).</td>
</tr>
<tr>
<td>description</td>
<td>A description of the role of this component in the StyleBook.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>type</td>
<td>The type determines what properties this component provides. Components have two kind of types: <strong>Built-in type</strong>: This type is provided by the system and you do not have to define it, for example, the NITRO entity types “lbvserver” or “servicegroup.” When a component has a built-in type attribute, it creates a configuration object of that type on the Citrix ADC. For example, if a component refers to the built-in type “lbvserver,” this component creates a load balancing virtual server on the Citrix ADC instance that is the target of the configuration. <strong>Composite type</strong>: This type refers to an existing StyleBook that you created and imported into Citrix ADM. When a component has a composite type attribute, it creates all the configuration objects, which are specified in the referenced StyleBook, on the Citrix ADC instance that is the target of the configuration. This enables you to combine multiple StyleBooks where each StyleBook creates a part of the final configuration. For more information about composite StyleBooks, see <a href="#">Create a Composite StyleBook</a>.</td>
</tr>
<tr>
<td>properties</td>
<td>The sub-attributes that can be used for a component type attribute. The properties that are valid for a component are dictated by its type. For a built-in type, these are the properties or attributes of the corresponding Nitro object. For a component whose type is another StyleBook, that is, a composite type, the properties correspond to the parameters defined in that StyleBook.</td>
</tr>
</tbody>
</table>
Example:

```plaintext
components:
  - name: my-lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg
```

In this example, you have defined a component called my-lbvserver-comp. This component is of type ns::lbvserver (a built-in type), where “ns” is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section, and “lbvserver” is a NITRO resource in this namespace.

The properties in this section include four mandatory and one optional attribute (lbmethod) of the “lbvserver” resource and allows you to specify values for these attributes. In this example, you are specifying static values for servicetype and port while the name, ipv46, and lbmethod properties get their values from the input parameters. You refer to the parameter names defined in the parameters section by using $parameters.<name> notation, for example, $parameters.ip.

**Note**

You have to use lower case for the attribute names of NITRO resource types (its component properties). Otherwise, the import of a StyleBook will fail.

**Helper components**

August 1, 2019

The primary use of components section in a StyleBook is to generate configuration objects through Nitro built-in types or another StyleBook that creates the actual configuration objects. The helper components do not build configuration objects by themselves. Helper components take the inputs from other sections like parameter objects, properties of other components, or outputs of other components and transform them into other forms. This can be later used by other components to generate the actual configuration objects. A helper component can be of two types: object type or another StyleBook that does not contain a component section.

The following example shows a snippet of a StyleBook that is used to create a load balancing server with monitor (lb-mon-comp) on a Citrix ADC instance.
The parameters section allows you to enter the name of the application and the IP addresses of the load balancing servers. In the lb-mon-comp component section, the svc-servers parameter of lb-mon StyleBook expects a list of objects where each item has two sub-parameters: ip and port.

However, the parameters section of this StyleBook only accepts the server IPs through $parameters.ips. The StyleBook assumes that all servers are running on port 80. To create the load balancing configuration using lb-mon StyleBook, you must transform the $parameters.ips to a list of objects. This is achieved using the helper component, help-comp in the above example. The help-comp component is of type server-ip-port-params StyleBook. This StyleBook does not have any components. As a result, it does not create any configuration objects. The help-comp creates a repeat list over $parameters.ips and constructs an object which consists of ip and port (that is set to a static 80) for
each item of $parameters.ips. Thus, help-comp transforms a list of IP addresses into a list of objects that can be later used in lb-mon-comp to assign svc-servers property. The result of the help-comp is assigned to the svc-servers property of lb-mon-comp.

Optional properties

August 1, 2019

In some cases, a property of a component takes its value from an expression, which can be a simple expression such as a parameter reference, or a more complex one. Setting this property value is optional in the component. You can choose to set the property value only if the expression returns an actual value, else you can choose not to set this property.

For example, consider that one of the properties you want to set is the lbmethod (loadbalancing algorithm) of a component whose type is ns::lbvserver. The value of the property lbmethod is taken from a parameter value provided by the user, as shown below:

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
      lbmethod: $parameters.lb-advanced.algorithm
```

Now, consider that the parameter `lb-advanced.algorithm` is an optional parameter. And, if the user does not provide a value for this parameter because it is optional, the expression `$parameters.lb-advanced.algorithm` evaluates to blank value. Therefore, an invalid value is passed for the lbmethod property. In order to avoid such a situation, you can annotate the property as optional by suffixing its name with "?" as follows:

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
```
The use of “?” omits the property if the expression on the right evaluates to nothing, which would be equivalent, in this case, to a component defined as follows:

```plaintext
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
```

Because `lbmethod` is optional, omitting it still makes this a valid component. Note that `lbmethod` might take its default value if one is defined in its type “ns::lbvserver.”

**Properties-default-sources construct**

August 1, 2019

The properties-default-sources construct is analogous to the parameters-default-sources construct. While the parameters-default-sources construct allows the reuse of existing parameters (from other StyleBooks) in a StyleBook, properties-default-sources construct allows the user to specify properties of a component based on existing sources.

The properties of a component may be distributed across various sections of the StyleBook. For example, the properties may come from object parameters, substitutions that return an object, properties of other components, or outputs of other components. In such cases, you need to redefine the properties that occur in other sections of the StyleBook in the definition of the component. Clearly, this is redundant and can lead to errors. To deal with this problem, properties-default-sources construct can be used. The properties-default-sources construct is a list where each item identifies a source for some properties of the component.

For example, consider a component that creates an lbvserver configuration. This component should define the properties of the lbvserver as follows.

```plaintext
parameters:
  -
    name: lb
```
In the above example, observe that the values for all properties defined in the components section are taken from $parameters.lb object. Though they are taken from a single source, the properties are again defined in the StyleBook. In addition, if a new sub-parameter to $parameters.lb object that is relevant to the configuration of the lbvserver is added, you need to update the lb-comp component to add the new property that corresponds to the new sub-parameter.

To avoid redefining properties and to fetch all relevant properties of a component without explicitly list them in the properties section, properties-default-sources construct can be used. The above example can be written as follows.

In the above example, the use of properties-default-sources construct leads to a reduction in the size of the component definition, and this allows you to concisely define a component. In addition, each time the source of the properties of the component changes, the changes are reflected automatically. For example, when a new property, say “persistencetype,” is added in the $parameters.lb object, this property is added to the configuration of lb-comp by default since persistencetype is a property of lbvserver. Thus, properties-default-sources construct provides a dynamic interface to define the components without worrying about changes happening to the sources of the properties of the component.
Computation of the Properties of the Component

This section discusses on how the properties are fetched if properties-default-sources construct is used in a component. First, the StyleBooks compiler identifies the list of properties for a component based on its type (in the above example, lbvserver.) Next, the compiler fetches these properties from the multiple sources in the order that they are defined (in properties-default-sources section of the component). If a property exists in multiple sources then the property appearing in the last source takes precedence over others. Finally, a property fetched by using properties-default-sources construct can be overridden in the properties section of the component. It is important to note that the definition of a component section should at least have a properties-default-sources section or a properties section. It may have both.

Nested components

August 1, 2019

Nesting a component within another component allows the nested component to create its configuration objects by referring to configuration objects or the context created by the parent component. The nested component can create one or more objects for each object created in the parent component. Nesting a component within another component does not indicate any relationship between the configuration objects created. Nesting is a way to facilitate the task of components to construct configuration objects within an existing context of the parent components.

Example:

```plaintext
components:
 -
  name: my-lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg
components:
 -
  name: my-svcg-comp
type: ns::servicegroup
properties:
  name: $parameters.name + "-svcgrp"
servicetype: HTTP
```
In this example, multi-level nesting is used. The component my-lbvserver-comp has a child component called my-svcg-comp. And, the my-svcg-comp component has two child components within it. The my-svcg-comp component is used to create a service group configuration object on the Citrix ADC instance by providing values to the attributes of the built-in NITRO resource type “servicegroup.” The first child component of the my-svcg component, lbvserver-svg-binding-comp, is used to bind the service group created by its parent component to the load balancing virtual server (lbvserver) created by the parent’s parent component. The $parent notation, also called the parent reference, is used to refer to entities in the parent components. The second child component, members-svcg-comp, is used to bind the list of services to the service group created by the parent component. The binding is achieved by using the repeat construct of StyleBook to iterate over the list of services specified for the parameter svc-servers. For information on repeat constructs, see Repeat Construct.

You can also create the same configuration objects without using nesting of components. For more information and examples, see StyleBook to Create a Basic Load Balancing Configuration.

**Condition construct**

August 1, 2019

You can make a component conditional by using a condition construct. The value of a conditional construct is a boolean expression that evaluates to true or false. If the condition is true, the component is used to build its configuration objects. If the condition is false, the component is skipped, and no
configuration objects are created through it. The boolean expression is often based on parameter values.

**Example:**

```plaintext
components:
  -
    name: servicegroup-comp
    type: ns::servicegroup
    condition: $parameters.svc-server-ips
    properties:
      name: $parameters.name + ",svcgrp"
      servicetype: HTTP
```

In this example, if the user specifies a value for the optional parameter svc-server-ips, then the component, servicegroup-comp, is processed by the StyleBook engine. If the condition is false, that is, if the user does not provide a value to this parameter, a null value is assigned to this parameter and evaluates to false, then the StyleBook engine ignores the presence of this component, and no servicegroup is created.

Note that the boolean expression can be based on any valid expression supported in StyleBooks (for example, whether another component is present, or whether a parameter has a certain value).

The following example builds the configuration object of NITRO type ns::systemfile if the condition is evaluated to true.

**Example:**

```plaintext
components
  -
    name: pem_key_files
    type: ns::systemfile
    condition: "$components.der-certificate-files-comp or $components.pem-certificate-files-comp"
    properties:
      filecontent: $certificate.keyfile.contents
      fileencoding: "BASE64"
      filelocation: "/nsconfig/ssl"
      filename: $certificate.keyfile.filename
```

In this example, the condition is a complex “OR” expression, where you want this configuration object to be created by the StyleBook only if two other components in the StyleBook have been processed (not skipped), therefore, creating a dependency between components.
Repeat construct

August 1, 2019

You can use the **repeat** construct of a component to build multiple configuration objects of the same type.

In the following example, the **members-svcg-comp** component is used to bind the list of services to the service group created by the parent component. In order to create a configuration object that binds each server to the service group, use the **repeat** construct to iterate over the list of services specified for the parameter **svc-servers**. During the iteration, the component creates a NITRO object of type **servicegroup_servicegroupmember_binding** for each service (referred to as **srv** in the **repeat-item** construct) in the service group, and it sets the **ip** attribute in each NITRO object to the IP address of the corresponding service.

**Example:**

```yaml
components:
  - name: my-lbvserver-comp
type: ns::lbvserver
  properties:
    name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg
  components:
    - name: my-svcg-comp
type: ns::servicegroup
  properties:
    name: $parameters.name + "-svcgrp"
servicetype: HTTP
  components:
    - name: lbvserver-svg-binding-comp
type: ns::lbvserver\servicegroup\binding
  properties:
    name: $parent.parent.properties.name
    servicegroupname: $parent.properties.
    name
  - name: members-svcg-comp
```
The `repeat` is an object by itself, and `repeat-list` and `repeat-item` are attributes for the repeat object.

- `repeat-list` is a mandatory attribute that identifies the list that the component iterates on.
- `repeat-item` is optional, and is used to give a friendly name to the current item in the iteration.

If not specified, the current item can be accessed using the expression `$repeat-item`. The last component in the above example can also be written as follows:

```plaintext
name: members-svcg-comp
type: ns::servicegroup_servicegroupmember_binding
repeat:
  repeat-list: $parameters.svc-servers
  repeat-item: srv
  properties:
    ip: $srv
    port: $parameters.svc-port
    servicegroupname: $parent.properties.name
```

In addition to being able to refer to the current item while iterating over a list, it is also possible to refer to the current index of the item in the list using `repeat-index`. In the following example, `repeat-index` is used to calculate a port number based on the current index:

```plaintext
name: services
type: ns::service
repeat:
  repeat-list: $parameters.app-services
  repeat-item: srv
  properties:
    ip: $parameters.app-ip
    port: $parameters.base-port + repeat-index
    servicegroupname: $parent.properties.name
```

Similar to the `repeat-item` construct, you can assign a different variable name to refer to the current index of the iteration. The previous example is equivalent to the following example:
Repeat-condition construct

August 1, 2019

The repeat-condition construct is evaluated in each iteration of a repeat construct and the result determines whether to build the configuration object in that iteration or to move to the next iteration. The following example shows the use of the repeat-condition construct:

Example:

```plaintext
| components
|   -
|      name: der-key-files-comp
|      type: ns::systemfile
|      repeat:
|          repeat-list: $parameters.certificate
|          repeat-item: certificate
|          repeat-condition: $certificate.ssl-inform == DER
|          properties:
|              filecontent: base64($certificate.keyfile.contents)
|              fileencoding: BASE64
|              filelocation: /nsconfig/ssl
|              filename: $certificate.keyfile.file
```

In this example, the der-key-files-comp component iterates over all the certificates given by the user but it only builds configuration objects that correspond to certificates with DER encoding. In each iteration, the repeat-condition expression is evaluated to test whether the certificate encoding is of type DER. If it is not of type DER, no configuration object is built in the current iteration, and the iteration moves to the next certificate in the list.
Nested repeats

August 1, 2019

With the nested repeat construct you can have more than one repeat construct in each component depending on the definition of the component. Consider a nested repeat of two levels. For each element in the outer list (first repeat-list), you can create a repeat list for all elements of the inner list (second repeat-list). The StyleBook compiler supports up to three nested repeats. Each repeat level has repeat-item and repeat-index attributes associated with it. Both repeat-item and repeat-index attributes are optional. In addition, each repeat can also specify a repeat-condition.

Example:

```plaintext
parameters:
- name: vips
type: ipaddress[]
-
name: vip-ports
type: tcp-port[]
components:
-
name: lbvservers-comp
type: ns::lbvserver
repeat:
  repeat-list: $parameters.vips
  repeat-item: ip
  repeat:
    repeat-list: $parameters.vip-ports
    repeat-item: port
  properties:
    name: str("lb-") + str($ip) + '-' + str($port)
servicetype: HTTP
ipv46: $ip
port: $port
```

In the above example, for each item in $parameters.vips, we iterate over all items of $parameters.vip-ports. Thus, for each ipaddress specified in $parameters.vips, we create lbvserver configuration objects for all ports specified in $parameters.vip-ports. The properties section define the name of the object with “lb” as a prefix for the combination of the IP address and the port. Therefore, for each iteration, $ip + $port defines a unique combination of the IP address and the port number.

If repeat-item attribute is not provided, the compiler generates a default value for it. The default values for repeat-item are: $repeat-item, $repeat-item-1, $repeat-item-2 respectively for each repeat level.
Similarly, if repeat-index attribute is not provided, the compiler generates a default value for it. The default values for repeat-index are: $repeat-index, $repeat-index-1, and $repeat-index-2 respectively for each repeat level.

The following example describes the naming convention in the absence of repeat-item and repeat-index attributes in a nested repeat object.

**Example:**

```plaintext
components:
  - name: lbvservers-comp
    type: ns::lbvserver
    repeat:
      repeat-list: $parameters.vips
      repeat:
        repeat-list: $parameters.vip-ports
        properties:
          name: str("lb") + str($repeat-item) + '-' + str($repeat-item -1)
          servicetype: HTTP
          ipv46: $repeat-item
          port: $repeat-item-1
```

**Outputs**

August 1, 2019

In the outputs section, you specify what a StyleBook exposes to its users after it has completed creating all the configuration objects successfully. The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import it more flexibility as you can see when creating a composite StyleBook.

The following table describes the attributes used in the outputs section.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the output corresponding to the configuration object you want to expose.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Mandatory</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>description</td>
<td>A text string describing the output.</td>
<td>No</td>
</tr>
<tr>
<td>value</td>
<td>This attribute specifies how to extract the value that is returned by a StyleBook.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
outputs:
- name: lbvserver
description: LBVServer component
value: $components.my-lbvserver-comp

- name: svc-grp
description: ServiceGroup name
value: $components.my-svcg.properties.name
```

In this example, you expose the `lbvserver` component and the servicegroup `name` that would be created by the StyleBook. The value of the output called `lbvserver` is the component `my-lbvserver-comp`. Similarly, the value of the output called `svc-grp` is the name of the servicegroup created by the component `my-svcg`.

**Parameter reference**

August 1, 2019

In the components construct, you refer to the parameters defined in the parameters section by using `$parameters.<parametername>` notation. If `<parametername>` itself contains parameters (when type is object), then you must use the notation `$parameters.<parametername>.<sub-parametername>`, and so on.

**Example:**

```plaintext
parameters:
- name: name
  label: Name
  type: string
```
required: true
-
  name: vip
  label: Virtual IP and Port
  type: object
  required: true
  parameters:
    -
      name: ip
      label: Virtual IP
      description: The Virtual IP Address
      type: ipaddress
      required: true
      -
        name: port
        label: The Virtual Port
        description: The TCP port for the Virtual IP
        type: tcp-port
        default: 80

components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.vip.ip
      port: $parameters.vip.port

Parent reference

August 1, 2019

If you are using nested components, you can refer to the parent component using the $parent notation. If the parent component builds multiple configuration objects using the repeat construct, and within each iteration, child components build other configuration objects, then the $parent notation always refers to the current iteration of the parent component. For example, $parent.properties.name refers to the name property of the configuration object built in the current iteration by the parent.

Example:
You can also navigate upward through the hierarchy of components by accessing the properties of the parents of parents all the way to top-level components. For example, the property name of the component **lbvserver-svg-binding-comp** takes its value from the property name of the parent of its parent, the **my-lbvserver-comp** component, by using the `$parent.parent` notation.
Components reference

August 1, 2019

In the components construct, you refer to top-level component in the StyleBook by using the $components.<componentname> notation. If there are nested components within a top-level component, then the notation used is $components.<componentname>.components.<component-name> to refer to them, and so on.

Example:

```plaintext
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
    -
      name: my-svcg-comp
      type: ns::servicegroup
      properties:
        name: $parameters.name + "-svcgrp"
        servicetype: HTTP
    -
      name: members-svcg-comp
      type: ns::servicegroup_servicegroupmember_binding
      repeat: $parameters.svc-servers
      repeat-item: srv
      properties:
        ip: $srv
        port: str($parameters.svc-port)
        servicegroupname: $components.my-svcg-comp.properties.name
    -
      name: lbvserver-svg-binding-comp
      type: ns::lbvserver_servicegroup_binding
      properties:
        name: $components.my-lbvserver-comp.properties.name
        servicegroupname: $components.my-svcg-comp.properties.name
```

In this example, the components my-svcg-comp and my-lbvserver-comp have to be built before
building the last component `lbvserver-svg-binding-comp` because there are references to these components in this last component. These references are provided by using the components references denoted by `$components.<componentname>`.

**Substitutions reference**

August 1, 2019

In the components section or operations section, you refer to substitutions defined in the substitutions section by using the `$substitutions.<substitution-name>` notation. For example, `$substitutions.http-port`.

If a substitution is a map, you can refer to an element in the map as `$substitutions.<substitution-name>[<map-key>]`. For example, `$substitutions.protocol-map[$parameters.port]`.

**Variable reference**

August 1, 2019

When you use the repeat and repeat-item constructs in components to build multiple configuration objects, you can assign a variable name to the repeat-item construct. This variable can be then referenced in the properties of that component or in child components by using the notation `$<varname>`. Note that when the repeat construct is used without the repeat-item construct in a component, a default variable called $repeat-item can be used to access the iteration items.

**Example:**

```plaintext
components:
  -
    name: server-members-comp
type: ns::server
condition: $parameters.svc-server-domain-names
repeat: $parameters.svc-server-domain-names
repeat-item: server-name
properties:
  name: $server-name + "-server"
domain: $server-name
components:
  -
```
In the above example, a variable name, server-name, is assigned to the repeat-item construct. This variable name is referred to in the properties of the same component as well as in the child components $\langle\text{varname}\rangle$.

**Operations**

August 1, 2019

Operations is an optional section in a StyleBook. In this section, you can configure Citrix Application Delivery Management (ADM) analytics to collect AppFlow records on all or some of the traffic transactions. The virtual server created on a Citrix ADC instance by using the StyleBook handles these traffic transactions. In this section, you can also configure Citrix ADM to trigger alarms when certain traffic conditions are met on a virtual server.

You can configure Citrix ADM through StyleBooks to collect traffic statistics from various Citrix ADM Insights that are listed as follows:

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway Insight.

The virtual servers supported are load balancing, content switching, and VPN virtual servers.

Enable both Web Insight and Security Insight or one of them for analytics on a load balancing or content switching virtual server. For VPN virtual servers, however, you must enable both HDX Insight and Citrix Gateway Insight or one of them.

Any Citrix ADM Insight enabled on Citrix ADC instances through StyleBooks uses IPFIX protocol (AppFlow) to send the data from the instances to Citrix ADC.

Also, when you enable Web Insight, “Client-Side Measurements” is enabled on the load balancing and the content switching virtual servers.

**Example 1:**

```plaintext
name: service-members-comp
type: ns::service
properties:
  name: $server-name + "-service"
  servername: $parent.properties.name
  servicetype: $parameters.svc-service-type
  port: $parameters.svc-server-port
```
The following example shows how to write the operations section in a StyleBook to enable both HDX Insight and Citrix Gateway Insight on a VPN virtual server:

```plaintext
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on a VPN vserver
import-stylebooks:
    - namespace: netscaler.nitro.config
      version: "10.5"
      prefix: ns
      components:
        - name: vpnvserver-comp
          type: ns::vpnvserver
          properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
          operations:
            analytics:
              - name: comp-ops
                properties:
                  target: $components.vpnvserver-comp
                  filter: "true"
                  insights:
                    type: hdxinsight
                    type: gatewayinsight
                  outputs:
                    - name: myvpns
                      value: $components.vpnvserver-comp
```

**Example 2:**

The following example shows how to write the operations section in a StyleBook to enable both Web Insight and Security Insight on a load balancing virtual server:
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on LB vserver

import-stylebooks:
- namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
components:
- name: lbvserver-comp
  type: ns::lbvserver
  properties:
    name: str("lb-") + str($current-target.ip)
    servicetype: HTTP
    ipv46: 1.1.21.37
    port: 80
operations:
analytics:
- name: comp-ops
  properties:
    target: $components.lbvserver-comp
    filter: "true"
    insights:
    - type: webinsight
    - type: securityinsight
outputs:
- name: mylbs
  value: $components.lbvserver-comp

Analytics

August 1, 2019

The analytics sub-section of the operations section has a structure similar to the components section.
Each element in the analytics section is used to configure the Citrix ADM Analytics feature for one or more virtual servers created by the StyleBook.

An element in the analytics section has the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the analytics element.</td>
<td>Yes</td>
</tr>
<tr>
<td>description</td>
<td>A text string describing what this element is.</td>
<td>No</td>
</tr>
<tr>
<td>condition</td>
<td>A boolean expression. When this condition evaluates to false, the entire analytics element is skipped.</td>
<td>No</td>
</tr>
<tr>
<td>repeat</td>
<td>Iterates over a list.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-condition</td>
<td>A boolean expression. If the expression evaluates to false, the current iteration is skipped.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-item</td>
<td>Name of the item in the current iteration.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-index</td>
<td>Name of the index value of the current iteration.</td>
<td>No</td>
</tr>
<tr>
<td>properties</td>
<td>The list of properties of analytics.</td>
<td>Yes</td>
</tr>
<tr>
<td>target</td>
<td>One of the properties in the list. The target expression is the name of a virtual server, configured on the Citrix ADC, for which analytics will be collected.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Mandatory</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>filter</td>
<td>One of the properties in the list. The value of this attribute is a Citrix ADC advanced policy expression that is used to filter the requests on the virtual server for which analytics will be collected. By default, the analytics data is collected on all the traffic passing through the virtual server.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
operations:
  analytics:
    name: lbvserver-ops-comp
    properties:
      target: $components-basic-lb-comp.outputs.lbvserver-name
    filter: HTTP.REQ.URL.CONTAINS("catalog")
```

Each attribute in the analytics section is used to instruct the Citrix ADM Analytics feature to configure the Citrix ADC instances to collect appflow records on the virtual server identified by the target property.

**Alarms**

August 1, 2019

The alarms sub-section of the operations section has a similar structure and the same attributes as in the analytics sub-section. The only difference is in the properties attribute. For a list of all the
attributes (other than the properties attribute), see Analytics.

The following properties are available in an alarms sub-section:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>An expression that evaluates to the name of a virtual server, configured on the Citrix ADC, for which alarms are configured.</td>
<td>Yes</td>
</tr>
<tr>
<td>email-profile</td>
<td>Name of an email profile that is defined in the Citrix ADM Analytics feature and contains a list of email addresses that you want to notify when the alarm is triggered.</td>
<td>No (either an email-profile or an sms-profile must be defined)</td>
</tr>
<tr>
<td>sms-profile</td>
<td>Name of an SMS profile that is defined in the Citrix ADM Analytics feature and contains a list of phone numbers that you want to notify when the alarm is triggered.</td>
<td>No (either an email-profile or an sms-profile must be defined)</td>
</tr>
<tr>
<td>rules</td>
<td>A list of rules that define the conditions that would trigger an alarm for the virtual server defined by the target property.</td>
<td>Yes</td>
</tr>
<tr>
<td>metric</td>
<td>An attribute of rule. The name of a metric you want to track pertaining to the Citrix ADC virtual server.</td>
<td>Yes</td>
</tr>
<tr>
<td>operator</td>
<td>An attribute of rule. The operator to use to compare the metric to the value. Valid operators are “greaterthan” and “lessthan.”</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Attribute Description Mandatory

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong></td>
<td>An attribute of rule. The threshold value that the metric is compared to by using the operator. If the metric value exceeds this threshold, the associated alarms are triggered.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>period-unit</strong></td>
<td>An attribute of a rule. The frequency at which to alert users if the alarm rule is met. This can contain the value day, hour, or weekly. This means that if the rule is met, an alarm will be sent once a period-unit (for example, once a day).</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following table provides a list of metrics that are tracked pertaining to the Citrix ADC virtual server.

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
<th>Detailed Description</th>
<th>Citrix ADM Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>total_requests</strong></td>
<td>Total VPN Session Launch Count</td>
<td>Total number of active sessions on this VPN virtual server started during a time interval specified by the user.</td>
<td>Monotonically increasing counter, incremented on each new session launch</td>
</tr>
<tr>
<td>Counters</td>
<td>Description</td>
<td>Detailed Description</td>
<td>Citrix ADM Calculation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>app_count</td>
<td>VPN App Launch Count</td>
<td>Total number of unique VPN applications on this VPN virtual server launched during a time interval specified by the user.</td>
<td>Monotonically increasing counter on each new application launch</td>
</tr>
<tr>
<td>app_launch_duration</td>
<td>VPN App Launch Duration</td>
<td>Average time taken to launch an application (in milliseconds)</td>
<td>Average value calculated across the launch time durations of all VPN applications launched on this VPN virtual server</td>
</tr>
<tr>
<td>total_requests</td>
<td>Number of requests</td>
<td>Number of client requests on this virtual server since the last appliance reboot, or since the creation of the virtual server, whichever is more recent.</td>
<td>Monotonically increasing counter, incremented on each new request to this virtual server.</td>
</tr>
</tbody>
</table>
### Detailed Description

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
<th>Detailed Description</th>
<th>Citrix ADM Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>total_bytes</td>
<td>Bytes</td>
<td>Total bytes transferred from the virtual server to Citrix ADM over the specified time interval.</td>
<td>Monotonically increasing counter to account for the total number of bytes served by this virtual server.</td>
</tr>
<tr>
<td>application_response_time</td>
<td>Response Time</td>
<td>Average response time of the virtual server.</td>
<td>The average value of the response times of all requests received by this virtual server since the last reboot of the appliance (or since the creation of the virtual server), whichever is last.</td>
</tr>
</tbody>
</table>

**Example of an alarms section in a StyleBook:**

```plaintext
operations:
alarms:
  - name: lbvserver_alarm
    properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"
    rules:
      - metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
```
Expressions

August 1, 2019

One of the most powerful features of StyleBook is the use of expressions. You can use StyleBooks expressions in various scenarios to compute dynamic values. The example below shows an expression to concatenate a parameter value with a literal string.

Example:

```bash
$parameters.appname + "-mon"
```

This expression retrieves the parameter named appname, and concatenates it with the string “-mon”.

The following types of expressions are supported:

Arithmetic Expressions

- Addition (+)
- Substraction (-)
- Multiplication (*)
- Division (/)
- Modulo (%)

Examples:

- Adding two numbers: $parameters.a + $parameters.b
- Multiplying two numbers: $parameters.a * 10
- Finding the remainder after division of one number by another:

15 % 10 results in 5

String Expressions

- Concatenate two strings (+)
Example:

Concatenate two strings: `str("app-") + $parameters.appname`

List Expressions

Merges two lists (+)

Example:

- Concatenate two lists: `$parameters.external-servers + $parameters.internal-servers`
- If `$parameters.ports-1` is `[80, 81]` and `$parameters.port-2` is `[81, 82]`, then `$parameters.ports-1 + $parameters.ports-2` results as a list `[80, 81, 81, 82]`

Relational Expressions

- `==`: Tests if two operands are equal and returns true if they are equal, else returns false.
- `!=`: Tests if two operands are different and returns true if they are different, else returns false.
- `>  `: Returns true if the first operand is greater than the second operand, else returns false.
- `>=`: Returns true if the first operand is greater than or equal to the second operand, else returns false.
- `< `: Returns true if the first operand is lesser than the second operand, else returns false.
- `<=`: Returns true if the first operand is lesser than or equal to the second operand, else returns false.

Example:

- Use of Equality operator: `$parameters.name == "abcd"$
- Use of Inequality operator: `$parameters.name != "default"$
- Examples for other relational operators
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

Logical (Boolean) Expressions

- `and`: The logical ‘and’ operator. If both operands are true, the result is true, else it is false.
• or: The logical ‘or’ operator. If one of the operands is true, the result is true, else it is false.
• not: The unary operator. If the operand is true, the result is false, and vice-versa.
• in: Tests whether the first argument is a substring of the second argument
• in: Tests if an item is part of a list

Note
You can type cast expressions where strings can be converted into numbers and numbers can be converted to strings. Similarly, a tcp-port can be cast to a number, and an IP address can be cast to a string.

You must use a delimiter before and after any operator. You can use the following delimiters:

- Before an operator: space, tab, comma, (,), [, ]
- After an operator: space, tab, (, [
  - For example:
    - abc + def
    - 100 % 10
    - 10 > 9

Expression Type Validation

StyleBook engine now allows for stronger type checking during compile time, that is, the expressions used while writing the StyleBook are validated during the import of StyleBook itself rather than while creating the configuration pack.

All references to parameters, substitutions, components, properties of components, outputs of components, user-defined variables (repeat-item, repeat-index, arguments to substitution functions,) and so on are all validated for their existence and types.

Example of Type Checks:

In the following example, the expected type of port property of lbvserver StyleBook is tcp-port. In Citrix Application Delivery Management (ADM) earlier releases, the StyleBook compiler computed the value as a string and the StyleBook was imported and executed. Now, type validations happen at compile-time (import-time). The compiler finds that string and tcp-port are not compatible types and therefore, the StyleBook compiler throws an error and fails import or migration of the StyleBook.

```plaintext
components:
- name: lbvserver-comp
type: ns::lbvserver
```
Example of Flagging Invalid Expressions:

In earlier releases, when an invalid expression was assigned to a property name, the compiler did not detect invalid expressions and allowed the StyleBooks to be imported into Citrix ADM. Now if this StyleBook is imported to Citrix ADM, the compiler will identify such invalid expressions and flag it. As a result, the StyleBook will not be imported to Citrix ADM.

In this example, the expression assigned to name property in lb-sg-binding-comp component is: `$components.lbvserver-comp.properties.lbvservername`. However, there is no property called `lbvservername` in component `lbvserver-comp`. In earlier Citrix ADM releases, the compiler would have allowed this expression and successfully imported it. The actual failure would happen when a user wants to create a configuration pack using this StyleBook. However now, this kind of error is identified during import and the StyleBook is not imported to Citrix ADM. You must manually correct such errors and import the StyleBooks.
**Indexing Lists**

Items of a list can be accessed now by indexing them directly:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$components.test-lbs[0]</td>
<td>Refers to the first item in test-lbs component</td>
</tr>
<tr>
<td>$components.test-lbs[0].properties.p1</td>
<td>Refers to property p1 of the first item in test-lbs component</td>
</tr>
<tr>
<td>$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname</td>
<td>Refers to property servicegroupname of the second item in servicegroups component, which is an output from the first item of lbcomps component</td>
</tr>
</tbody>
</table>

**In-place interpolations**

August 1, 2019

It is now possible to replace part(s) of a string using a StyleBook expression(s). When these string expressions are evaluated by the StyleBook compiler, the part of the string that uses a StyleBook expression will be replaced by value of the expression. To include StyleBook expressions in a string, we use the following notation:

```
...%{...}%...
```

where the characters enclosed between “%{ “ and “}%” form a StyleBook expression. These expressions are known as “in-place interpolations.”

For example, the string “lb-%{$parameters.appname}%-svc” is a string expression with in-place interpolation of a StyleBook expression. The value of string expression depends on the value of the interpolation expression. Consider that $parameters.appname is assigned with “app1.” Then, the
string expression evaluates to \texttt{lb-app1-svc}. This allows the values to be not hard-coded in string expressions, but rather be evaluated based on the user-defined values.

A practical use case of in-place interpolations is to parameterize policy expressions in StyleBooks. Consider a scenario where you want to write a policy expression that checks if the HTTP URL contains a specific word, say, \texttt{“jpeg”}.

For this, you write a policy expression as follows: \texttt{“HTTP.REQ.URL.CONTAINS(“jpeg”)”}.

Now, if you want to parameterize the object in the HTTP URL, you can add a string parameter in the StyleBook, say, \$parameters.url-object. The policy expression should be written based on this parameter. To do that, you use string concatenation to achieve the result. The expression would look like:

\begin{verbatim}
str(“HTTP.REQ.URL.CONTAINS(“ + $parameters.url-object + “”)”)
\end{verbatim}

If \$parameters.url-object is assigned \texttt{“csv”}, the above expression will evaluate to \texttt{“HTTP.REQ.URL.CONTAINS(“csv”)”}. However, this expression is not easy to read. To make this parameterization easy to read and understand, you can use in-place interpolations.

The expression with in-place interpolation is now:

\begin{verbatim}
str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)
\end{verbatim}

In the above expression, you used an interpolation expression that adds the inner-quotes around the value of the \$parameters.url-object. The result of this expression is same as the above, but, it looks more intuitive and closer to the actual result.

\textbf{Allowed Types Inside Interpolations}

You can use expressions that generates value of following types inside interpolations: boolean, number, tcp-port, ipaddress, and string. The generated value is automatically transformed to a string when the interpolations are replaced with the result.

String expressions can have 0, 1, or more interpolations. In a sequential interpolation, different parts of the string expression can be replaced by different StyleBook expressions. For example, the string \texttt{“lb-%(parameters.appname)-%(parameters.vip)”} returns \texttt{“lb-app1-1.1.1”}, if \$parameters.appname is “app1” and \$parameters.vip is “1.1.1”

String expressions also supports nested interpolations. That is, an interpolation expression can be nested inside another interpolation expression so that the value of one expression can become an input to the second expression.

For example, consider a string \texttt{“%(lb-%(parameters.port + 1)%)”}

The internal string, \texttt{“%(parameters.port + 1)”} returns “lb-81” if \$parameters.port is 80. Here this expression is nested inside another interpolation expression.
The following table describes the different types of interpolations with examples and corresponding results. The value of the parameters used in the examples are:

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

### Simple interpolations

<table>
<thead>
<tr>
<th>Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb-%{$parameters.appname}%def</td>
<td>lb-lb1-def</td>
</tr>
</tbody>
</table>

### Automatic type conversions

<table>
<thead>
<tr>
<th>Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb-%{1}%</td>
<td>lb-1</td>
</tr>
<tr>
<td>lb-%{$parameters.vip}%%</td>
<td>lb-1.1.1.1</td>
</tr>
<tr>
<td>lb-%{true}%%</td>
<td>lb-True</td>
</tr>
</tbody>
</table>

### Sequential interpolations

<table>
<thead>
<tr>
<th>Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{$parameters.appname}%-%str($parameters.appname)%%</td>
<td>lb1-lb1</td>
</tr>
<tr>
<td>lb-%{1}%-%{2}%</td>
<td>lb-1-2</td>
</tr>
</tbody>
</table>

### Nested interpolations
Interpolations with quotewrap

<table>
<thead>
<tr>
<th>Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>str(&quot;%{quotewrap(abcd)}%&quot;)</td>
<td>&quot;abcd&quot;</td>
</tr>
<tr>
<td>str(&quot;%{quotewrap(https://)} %+HTTP.REQ &lt;https://&quot;+HTTP.REQ.HOST+&quot;NAME+HTTP.REQ.URL&quot;')</td>
<td>&quot;&lt;https://&quot;+HTTP.REQ.HOST+&quot;NAME+HTTP.REQ.URL&quot;')</td>
</tr>
</tbody>
</table>

Escape Characters in Interpolations

If the characters "%{“ or “}%" are part of the string, you must provide “\” as an escape character so that the StyleBook compiler does not evaluate these as interpolation tags.

Example:

str("%({str($parameters.vip) + })%") returns "%(1.1.1.1)%" if $parameters.vip is 1.1.1.1

The following table describes a few more expressions and their results:

<table>
<thead>
<tr>
<th>Category</th>
<th>Expression</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escaping interpolations</td>
<td>str(&quot;%{str($parameters.n1) + }{]%}%&quot;)</td>
<td>1)%%</td>
</tr>
<tr>
<td></td>
<td>lb-%{str($parameters.n1) + }{]%}%</td>
<td>lb-1)%%</td>
</tr>
<tr>
<td></td>
<td>&quot;%{str($parameters.n1) + &quot;}{]'&quot;]&quot;]%&quot;</td>
<td>1)%%</td>
</tr>
</tbody>
</table>
Built-in functions

Expressions in StyleBooks can make use of built-in functions.
For example, you can use the built-in function, str() to transform a number to a string.
str($parameters.order)
Or, you can use the built-in function, int() to transform a string into an integer.
int($parameters.priority)
The following is the list of built-in functions supported in StyleBook expressions with examples of how they can be used:

str()
The str() function transforms the input argument to a string value.
Allowed argument types:
- string
- number
- TCP-port
- boolean
- IP address
Examples:
- “set-“ + str(10) returns “set-10”
- str(10) returns “10”
- str(1.1.1.1) returns “1.1.1.1”
- str(True) returns “True”
- str(mas) returns “mas”

int()
The int() function takes a string, number, or tcpport as an argument and returns an integer.
Examples:
- int(“10”) returns 10
- int(10) returns 10
bool()

The bool() function takes any type as an argument. If the argument value is false, empty, or non-existent, this function returns false. Otherwise, it returns true.

Examples:

• bool(true) returns “true”
• bool(false) returns “false”
• bool($parameters.a) returns false if the
  $parameters.a is false, empty, or not present.

len()

The len() function takes a string or a list as an argument, and returns the number of characters in a string or the number of items in a list.

Example 1:
If you define a substitution as follows:
items: [“123”, “abc”, “xyz”]
len($substitutions.items) returns 3

Example 2:
len(“netscaler mas”) returns 13

Example 3:
len($parameters.vips) returns 3 if $parameters.vip is
assigned a value [‘1.1.1.1’, ‘1.1.1.2’, ‘1.1.1.3’]

min()

The min() function takes either a list or a series of numbers or tcp-ports as arguments, and returns the smallest item.

Examples with a series of numbers/tcp-ports:

• min(80, 100, 1000) returns 80
• min(-20, 100, 400) returns -20
• min(-80, -20, -10) returns -80
• min(0, 100, -400) returns -400
Examples with a list of numbers/tcp-ports:

- Support $parameters.ports is a list of tcp-ports and has value: [80, 81, 8080].
  
  min($parameters.ports) returns 80.

max()

The max() function takes either a list or a series of numbers or tcp-ports as arguments, and returns the largest item.

Examples with a series of numbers/tcp-ports:

- max(80, 100, 1000) returns 1000
- max(-20, 100, 400) returns 400
- max(-80, -20, -10) returns -10
- max(0, 100, -400) returns 100

Examples with a list of numbers/tcp-ports:

- Support $parameters.ports is list of tcp-ports and has value: [80, 81, 8080].
  
  max($parameters.ports) returns 8080.

bin()

The bin() function takes a number as an argument, and returns a string that represents the number in binary format.

Examples of expressions:

bin(100) returns “0b1100100”

oct()

The oct() function takes a number as an argument, and returns a string that represents the number in octal format.

Examples of expressions:

oct(100) returns “0144”

hex()

The hex() function takes a number as an argument, and returns a lowercase string that represents the number in hexadecimal format.
Examples of expressions:

hex(100) returns “0x64”

lower()  
The lower() function takes a string as an argument and returns the same string in lowercase.  
Example:  
lower(“MAS”) returns “mas”

upper()  
The upper() function takes a string as an argument and returns the same string in uppercase.  
Example:  
upper(“netscaler_mas”) returns “NET SCALER_MAS”

sum()  
The sum() function takes a list of numbers or tcpports as arguments and returns the sum of the numbers in the list.  
Example 1:  
If you define a substitution as follows:  
substitutions:  
• list-of-numbers:  
  – 11  
  – 22  
  – 55  
  sum($substitutions.list-of-numbers) returns 88  
Example 2:  
If $parameters.ports is [80, 81, 82], sum($parameters.ports) returns 243

pow()  
The pow() function takes two numbers as arguments and returns a number that represents the first argument raised to the power of the second one.
Example:
pow(3,2) returns 9

ip()

The ip function takes a string or an ipaddress as argument returns the IP address based on the input value.

Examples:
- ip("2.1.1.1") returns “2.1.1.1”
- ip(3.1.1.1) returns “3.1.1.1”

base64.encode()

The base64.encode() function takes a string argument and returns the base64 encoded string.

Example:
base64.encode(“abcd”) returns “YWJjZA==”

base64.decode()

The base64.decode function takes base64 encoded string as an argument and returns the decoded string.

Example:
base64.decode(“YWJjZA==”) returns “abcd”

exists()

The exists function takes an argument of any type and returns a Boolean. The return value is True if the input has any value. The return value is False if the input argument does not have a value (that is, no value).

Consider that the $parameters.monitor is an optional parameter. If you provide a value to this parameter when creating a configpack, exists($parameters.monitor) returns True. Otherwise, it returns False.
filter()

The filter() function takes two arguments.

Argument 1: a substitution function that takes one argument and returns a Boolean value.

Argument 2: a list.

The function returns a subset of the original list where each element evaluates to “True” when passed to the substitution function in the first argument.

Example:

Suppose we have defined a substitution function as follows.

substitutions:

```
1 x (a) : $a != 81
```

This function returns True if the input value is not equal to 81. Otherwise, it returns False.

Suppose,$parameters.ports is [81, 80, 81, 89]

filter($substitutions.x, $parameters.ports) returns [80, 89] by removing all occurrences of 81 from the list.

if-then-else()

The function if-then-else() takes three arguments.

Argument 1: Boolean expression

Argument 2: Any expression

Argument 3: Any expression (optional)

If the expression in argument 1 evaluates to True, the function returns the value of the expression provided as argument 2.

Otherwise, if argument 3 is provided, the function returns the value of the expression in argument 3.

If argument 3 is not provided, the function returns no value.

Example 1:

if-then-else($parameters.servicetype == HTTP , 80, 443) returns “80” if $parameters.servicetype has value “HTTP.” Otherwise, the function returns “443”.
Example 2:

if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport) returns the value of “$parameters.hport” if $parameters.servicetype has value “HTTP.” Otherwise, the function returns the value of “$parameters.sport.”

Example 3:

if-then-else($parameters.servicetype == HTTP, 80) returns “80” if $parameters.servicetype has value “HTTP.” Otherwise, the function does not return any value.

join()

The join() function takes two arguments:

Argument 1: list of numbers, tcp-ports, strings, or ipaddresses

Argument 2: delimiter string (optional)

The function joins the elements of the list provided as argument one into a string, where each element is separated by the delimiter string provided as argument two. If argument two is not provided, then elements in the list are joined together as one string.

Example:

- $parameters.ports is [81, 82, 83].
  - With delimiter argument:
    join($parameters.ports, '-') returns “81-82-83”
  - Without delimiter argument:
    join($parameters.ports) returns “818283”

map()

The map function takes two arguments;

Argument 1: Any function

Argument 2: A list of elements.

The function returns a list where each element in the list is the result of applying the map function (argument one) to the corresponding element in argument two.

Allowed functions in argument 1:
• Built-in functions that take one argument:
  base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode

• Substitution functions that take at least one argument.

Example:
Suppose $parameters.nums is [81, 82, 83].

• Map using a built-in function, str
  map(str, $parameters.nums) returns [“81”, “82”, “83”]
  The result of the map function is the list of strings where each element is string is computed by applying the str function on the corresponding element in the input list ($parameters.nums).

• Map using a substitution function
  – Substitutions:
    add-10(port): $port + 10
  – Expression:
    map($substitutions.add-10, $parameters.nums) returns a list of numbers:
    [ 91, 92, 93 ]
  The result of this map function is a list of numbers, each element is computed by applying the substitution function $substitutions.add-10 on the corresponding element in the input list ($parameters.nums).

quotewrap()

The quotewrap function takes a string as argument and returns a string after adding double quote character before and after the input value.

Example:
quotewrap(“mas”) returns “”mas””

replace()

The replace function takes three arguments:
Argument 1: string
Argument 2: string
Argument 3: string (optional)

The function replaces all the occurrences of argument two with argument three in argument one.

If argument three is not provided, all occurrences of argument two are removed from argument one (in other words, replaced with empty string).

Replace a substring with another substring:

- replace('abcdef', 'def', 'xyz') returns “abcxyz”.
- All occurrences of “def” are replaced by “xyz”.
- replace('abcdefabc', 'def') returns “abcabc”.
- As there is no third argument, “def” is removed from the resulting string.

trim()

The trim function returns a string where the leading and trailing whitespaces are stripped from the input string.

Example:
trim(' abc ') returns “abc”

truncate()

The truncate function takes two arguments:

Argument 1: string
Argument 2: number

The function returns a string where the input string in argument one is truncated to the length specified by argument two.

Example:
truncate('netscaler mas', 9) returns “netscaler”

url.encode

The url.encode function returns a string where characters are transformed using ASCII character set according to RFC 3986.

Example:
url.encode(“a/b/c”) returns “a%2Fb%2Fc”
**url.decode**

The `url.decode` function returns a string where the URL encoded argument is decoded into a regular string according to RFC 3986.

**Example:**

`url.decode("a%2Fb%2Fc")` returns “a/b/c”

**is_ipv4()**

The `is_ipv4()` function takes an IP address as an argument and returns “true” if the IP address is of the IPv4 format.

`is_ipv4(10.10.10.10)` returns “True”

**is_ipv6()**

The `is_ipv6()` function takes an IP address as an argument and returns “true” if the IP address is of the IPv6 format.

`is_ipv6(2001:DB8::)` returns “True”

**Dependency detection**

August 1, 2019

Components in a StyleBook can refer to properties or sections of other components in the same StyleBook. Components are complete blocks by themselves and they may not be written in the same order that they have to be executed. The StyleBook compiler checks the order in which the components are written and then executes them in a logical order.

**Example:**

```
components:
- name: lbvserver-comp
type: ns::lbvserver
properties:
  name: mylb
  ipv46: 10.102.190.15
  port: 80
```
In the above example, there are three components defined - `lbvserver-comp`, `lb-sg-binding-comp`, and `sg-comp`. When this StyleBook is executed, the lbvserver-comp is first created. The lb-sg-binding-comp refers to lbvserver-comp properties, but it cannot be created next though it is the second component defined in the StyleBook. This is because the lb-sg-binding-comp also has a dependency on the sg-comp which is yet to be created. As a result, the compiler reorders the components so that the dependencies of a component are resolved by the time a component is created, and executes this reordered list of components. The order of execution of the above StyleBook is: lbvserver-comp, sg-comp, and lb-sg-binding-comp.

Thus, the author of a StyleBook need not worry about the correct order of the components. The components may appear in any order. The compiler computes the correct order of execution of the components based on how the components refer each other. Note that this dependency detection and reordering also works for substitutions and outputs sections as well.

### Cyclic Dependencies

Since a component may refer another component, it is possible that cycle of dependencies may be introduced in the definition of the StyleBook. For example, if component A refers to a property defined in component B, which again refers to a property defined in component A. This kind of dependency is called cyclic dependencies. Cyclic dependencies cannot be resolved automatically. The author of the StyleBook should manually correct the StyleBook definition to eliminate such cyclic dependencies. The compiler will be able to identify cyclic dependencies - if they exist, and report it.

The following example shows a cyclic dependency of components:

```plaintext
components:
- name: lbvserver-comp
```
In the above example, there are three components: `lbvserver-comp`, `lb-sg-binding-comp`, and `sg-comp`. Lbvserver-comp depends on lb-sg-binding-comp, lb-sg-binding comp depends on sg-comp and sg-comp depends on lbvserver-comp. Here, a cycle of dependencies among these components is formed and this cannot be resolved automatically. As a result, this StyleBook cannot be executed. The StyleBook compiler detects this and prevents the StyleBook from being imported into Citrix ADM.

**Instance management**

August 1, 2019

Instances are Citrix Application Delivery Controller (ADC) appliances that you can manage, monitor, and troubleshoot using Citrix Application Delivery Management (ADM). You must add instances to Citrix ADM to monitor them. Instances can be added when you set up Citrix ADM or at a later time 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 so on. A private IP-block groups your instances based on their geographical locations.
Add an instance

You can add instances either while setting up the Citrix ADM server for the first time or at a later time. 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 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 Networks > Dashboard and click All Instances. On the Instances page, select the instance you want to delete and click Remove.

How to use the instance dashboard

The per-instance dashboard in 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 Networks > Instances. From the summary, choose the instance type and then, select the instance you want to view and click Dashboard.

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:
• **Overview.** The overview tab displays the CPU and memory usage of the chosen instance. You can also view events generated by the instance and the throughput data. Instance-specific information such as the IP address, its hardware and LOM versions, the profile details, serial number, contact person, and so on is also displayed here. By scrolling down further, the licensed features that are available on your chosen instance along with the modes configured on it.

• **SSL dashboard.** You can use the SSL tab on the per-instance dashboard to view or monitor the details of your chosen instance’s SSL certificates, SSL virtual servers, and SSL protocols. You can click the “numbers” in the graphs to display further details.

• **Configuration Audit.** You can use the configuration audit tab to view all the configuration changes that have occurred on your chosen instance. The NetScaler config saved status and NetScaler config drift charts on the dashboard display high-level details about configuration changes in saved against unsaved configurations.

• **Network Functions.** Using the network functions dashboard, you can monitor the state of the entities configured on your selected Citrix ADC instance. You can view graphs for your virtual servers that displays 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 on the “plus” icon at the bottom right-corner of the screen to add additional performance report.
Monitor globally distributed sites

August 1, 2019

As a network administrator, you might have to monitor and manage network instances deployed across geographical locations. However, it is not easy to gauge the requirements of the network when managing network instances in geographically distributed data centers.

Geomaps in Citrix Application Delivery Management (ADM) provides you with a graphical representation of your sites and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

The following section explains how you can monitor data centers in Citrix ADM.

Citrix ADM site is a logical grouping of Citrix Application Delivery Controller (ADC) instances in a specific geographical location. For example, while one site is assigned to Amazon Web Services (AWS) and another site might be assigned to Azure™. Still another site is hosted on the premises of the tenant. 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 navigate to Networks > Dashboard page for a visual representation of the sites created on the world map.

Use case

A leading mobile carrier company, ExampleCompany, was relying on private service providers for hosting their resources and applications. The company already had two sites - one at Minneapolis in the United States and another in Alice Springs in Australia. In this image, you can see that two markers represent the two existing sites.
The markers also display a number, which shows the number of applications in each site. You can click these markers for more information about each site.

Click the tabs to view more information:

- **Instances** tab: View the following in this tab:
  - IP address of each network instance
  - Type of the instance
  - Number of critical events on them
  - Significant events and all events raised on a 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.
Configuring Geomaps

ExampleCompany decided to create a third site in Bangalore, India. The company wanted to test the cloud by offloading some of their less-critical, internal IT applications to the Bangalore office. The company decided to use the AWS cloud computing services.

As an administrator, you must first create a site, and next add the Citrix ADC instances in Citrix 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.

Navigate to Networks > Sites, and then click Add.

1. In the Create Site page, specify the following information:
   a) Site Type: Select Data Center.
b) **Type**: Select AWS as the cloud provider from the list.

Note

Check the **Use existing VPC as a site** box accordingly.

c) **Site Name**: Type the name of the site.

d) **City**: Type the city.

e) **Zip Code**: Type the Zip Code.

f) **Region**: Type the Region.

g) **Country**: Type the Country

h) **Latitude**: Type the latitude of the location.
   
   For south latitude, specify negative values. Example: −77.5946.

i) **Longitude**: Type the longitude of the location.
   
   For west longitude, specify negative values. Example: −12.9716.

2. Click **Create**.

   ![Create Site]

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.

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 **Networks > Instances**.

2. Select the type of instance you want to create, 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 + sign next to **Site** field to create a site or click the edit icon to change the details of the default site.

5. Click the right arrow and select the agent from the list that displays.

6. After choosing the agent, you must associate the agent with the site. This step allows the agent to be bound to the site. Select the agent and click **Attach Site**.

1. Select the site from the list and click **Save**.
1. Click OK.

You can also attach an agent to a site by navigating to Networks > Agents.

To associate a Citrix ADM agent with the site:

1. In Citrix ADM, navigate to Networks > Agents.
2. Select the agent, and click Attach Site.

1. You can associate the site and click Save.

Citrix ADM starts monitoring the Citrix ADC instances added in Bangalore site along with the instances at the other two sites as well.

How to create tags and assign to instances

August 1, 2019

Citrix Application Delivery Management (ADM) now allows you to associate your Citrix Application Delivery Controller (ADC) instances with tags. A tag is a keyword or a one-word term that you can assign to an instance. The tags add some additional information about the instance. The tags can be thought of as metadata that helps describe an instance. Tags allow you to classify and search for instances based on these specific keywords. You can also assign multiple tags to a single instance.

The following use cases help you to understand how tagging of instances 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 value as “UK.” This tag helps you to search and monitor all those instances that are located in 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 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 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 **Networks > Instances > Citrix ADC**.
2. Select the **Citrix ADC VPX** tab.
3. Select the required Citrix VPX.
4. Click **Tags**.
5. Create tags and click **OK**.

The **Tags** window that appears allows you to create your own “key-value” pairs by assigning values to every keyword that you create.

For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.
You can also add multiple tags by clicking “+.” Adding multiple and meaningful tags allows you to very efficiently search for the instances.

You can add multiple values to a keyword by separating them with commas.

For example, you are assigning admin role to another coworker, Greg T. You can add his name separated by a comma. Adding multiple names helps you to search by either of the names or by both names. 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.

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**

August 1, 2019

There might be a situation where Citrix Application Delivery Management (ADM) is managing a large number of 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 hostname, 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 **Networks > Instances > Citrix ADC > VPX tab.**

2. Click the search field. You can create a search expression by using Tags or Properties or by combining both.

   The following examples show how you can use the search expression efficiently to search for the instance.

   a) Select **Tags** option and select **Owner.** Select “David T.”
Citrix ADM supports regular expressions and wildcard characters in the search expressions.

b) You can use regular expressions to further expand the search criteria. For example, you want to search instances owned by either David or Stephen. In such a case, you can type the values by separating the values with a “|” expression.

c) You can also use wildcard characters to replace or represent one or more characters. For example, you can type “Dav*” to search for all instances owned by David T and Dave P.
Manage admin partitions of Citrix ADC instances

August 1, 2019

You can configure admin partitions on your Citrix Application Delivery Controller (ADC) instances so that different groups in your organization are assigned different partitions on the same Citrix ADC instance. A network administrator can be assigned to manage multiple partitions on multiple Citrix ADC instances.

Citrix Application Delivery Management (ADM) provides a seamless way of managing all partitions owned by an administrator from a single console. You can manage these partitions without disrupting other partition configurations.

To allow multiple users to manage different admin partitions, you have to create groups and then, assign users and partitions to those groups. Each user can view and manage only the partitions in the group to which the user belongs. Each admin partition is considered as an instance in Citrix ADM. When you discover a Citrix ADC instance, the admin partitions configured on that Citrix ADC instance get added to the system automatically.

Consider that you have two Citrix VPX instances with two partitions configured on each instance. For example, Citrix ADC instance 10.102.216.49 has Partition_1, Partition_2, and Partition_3, and Citrix ADC instance 10.102.29.120 has p1 and p2 as shown in the following image.

To view the partitions, navigate to Networks > Instances > Citrix ADC > VPX, and then click Partitions.
You can assign user-p1 the following partitions: 10.102.29.120-p1 and 10.102.216.49-Partition_1. And, you can assign user-p2 to manage partitions 10.102.29.80-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3.

Then, you have to create the two users, user-p1 and user-p2, and you have to assign the users to the groups that you created for them.

First, you have to create two groups with appropriate permissions (example: admin permissions) and include the required admin partition instances in each group. For example, create system group partition1-admin and add Citrix ADC admin partitions 10.102.29.120-p1 and 10.102.216.49-Partition_1 to this group. Also create system group partition2-admin and add Citrix ADC admin partitions 10.102.29.120-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3 and to this group.

After you have created the admin partition, you can also use the revision history difference feature and the audit template for admin partition feature for auditing purposes.

**Revision history difference** for admin partition allows you to view the difference between the five latest configuration files for a partitioned Citrix ADC instance. You can compare the configurations files against each other (example Configuration Revision - 1 with Configuration Revision -2) or against the current running/saved configuration with Configuration Revision. Along with the differences in configuration, the correction configurations are also shown. You can export all the corrective commands to your local folder and correct the configurations.

To view the revision history difference:

1. Navigate to Networks > Configuration Audit. Click inside the donut chart that represents the instance config status. In the Audit Reports page that opens, click the partitioned Citrix ADC instance.

2. From the Action menu, click Revision History Diff.
3. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision -1 and then, click **Show configuration difference**.

4. You can then view the difference between the five latest configuration files for the selected partitioned Citrix ADC instance as shown below. You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be executed on the base file in order to get the configuration to the desired state (configuration file that is being used for comparison).

**Audit templates for partition** allow you to create a custom configuration template and associate it with a partition instance. Any variation in the running configuration of the instance with the audit template is shown in the **Template vs Running diff** column of the **Audit Reports** page. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.
To view the template vs running difference:

1. From the Audit Reports page, click the partitioned Citrix ADC instance.

2. 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 create groups:

1. Navigate to System > User Administration > Groups, and then click Add.

2. In the Create System User page, specify the following:
   - **Group Settings** tab: Enter the group name and role permissions. To allow access to specific instances, clear the All Instances check box, and then choose your instances on the Select Instances page.
   - **Applications and Templates** tab: You can choose to use this group across all applications and configuration templates.
   - **Select Users** tab: Select users that you’d like to add to this group. You can click on the New link in the Available table to create new users. Optionally, configure the session timeout, where you can configure the time period for how long a user can remain active.

3. Click Finish.
To create users:

1. Navigate to **System > User Administration > Users**, and then click **Add**.
2. On the **Create System User** page, specify the user name and password. Optionally, you can enable external authentication and configure the session timeout.
3. Assign the user to a group by adding the group name from the **Available** list to the **Configured** list.
4. Click **Create**.

Now log out and log on with user-p1 credentials. You can view and manage only the admin partitions assigned to you to manage and monitor.

**Back up and restore Citrix ADC instances**

August 21, 2019

You can back up the current state of a Citrix ADC instance and later use the backed-up files to restore it to the same state. You must always back up an instance before you upgrade it or for just 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 and CLI. You can also 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 backs up and restores the following types of Citrix ADC instances:

- Citrix SDX
- Citrix VPX
- Citrix MPX

Citrix ADM creates a full backup for the Citrix VPX instance. 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 /var/ns_sys_backup/ directory. To avoid issues due to non-availability of disk space, you can save a maximum of 50 backup files in this directory. You can use the “rm system backup” command to delete existing backup files so that you can create more backups.

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 back up of the configuration files in these instances. If necessary, you can also restore the Citrix ADC instances by using these backed up files.

Configure instance backup settings

The Instance Backup Settings page allows you to configure settings on Citrix ADM to back up a selected Citrix ADC instance or multiple instances:

In Citrix ADM, navigate to System > System Administration. In the right-hand pane, under Instance Settings, select Instance Backup Settings, and specify the following:

1. Enable Instance Backups: By default, Citrix ADM is enabled for taking backups of Citrix ADC instances. Clear this option if you do not want to create backup files for the instances.
2. **Password Protect File**: (optional) Select password protect option to encrypt the backup file. Encrypting the backup file ensures that all the sensitive information inside the backup file is secure.

   **Note**
   
   You can download the encrypted backup file to your local machine, but you cannot open the file either with Citrix ADM GUI or with any text editor. The file can be retrieved and used by Citrix ADM alone. You are prompted to provide the password when restoring the encrypted backup file. You can, however, open an unencrypted backup file on your system.

3. **Number of Backup Files to retain**: Specify the number of backup files to retain in Citrix ADM. You can retain up to 50 backup files of the current state of a Citrix ADC instance. The default is three backup files.

   **Note**
   
   Each backup file accounts for some storage requirement. Citrix recommends that you store an optimal number of Citrix ADC backup files on Citrix ADM as per your requirement.

4. **Backup scheduling settings**: (optional) There are two options available for creating backup files, though you can use only one option at a time:

   a) The default backup scheduling option is “interval-based.” A backup file is created in Citrix ADM after the specified interval elapses. The default backup interval is 12 hours.

   b) You can also change the type of scheduled backups to “time-based.” In this option you specify the time in “hours:minutes” format at which the backup should happen. Citrix ADM allows a maximum of four daily backups to happen on the instances.
5. **Citrix ADC settings**: (optional) 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 new 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.

6. **Geodatabase files**: (optional) By default, Citrix ADM does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.

7. **External Transfer**: (optional) Citrix ADM allows you to transfer the Citrix ADC instance backup files to an external location:
   a) Specify the IP address of the location.
   b) Specify the user name and the password of the external server to which you want to transfer the backup files.
   c) Specify the transfer protocol and the port number.
   d) You can specify the directory path where the file needs to be stored.
You also have the option to delete the backup file from Citrix ADM after transferring it to the external server.

Note
Citrix ADM sends an SNMP trap or a Syslog notification to itself when there is a backup failure for any of the selected Citrix ADC instances.

Create a back up 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 Networks > Instances. Under Instances, select the type of instances (for example, Citrix VPX) to display on the screen.

2. Select the instance that you want to back up, and then click Backup/Restore.


4. You can specify whether to encrypt your backup file for additional security. You can either enter your password or use the global password that you previously specified on the Instance Backup Settings page.

5. Click Continue.
Restore a 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 from STAYSECONDARY to ENABLED mode and becomes part of the HA pair again. You can expect a possible downtime on the primary instance until the restore process gets completed.

Perform this task to restore a Citrix ADC instance by using the backup file that you had created earlier:

1. Navigate to Networks > Instances, select the instance that you want to restore.
2. From the Selection Action menu, select Backup/Restore.
3. On the Backup Files page, select the backup file containing the settings that you want to restore, and then click Restore.
Important

1. For a Citrix SDX appliance, Citrix ADM backs up only 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 config files of devices present on SDX
   - Citrix build images
   - Citrix XVA images
   - SDX Single Bundle Image (SVM+XS)
   - Third Party instance images (if provisioned)

1. You must restore your Citrix SDX appliance to the configuration available in the backup file. During appliance restore, the entire current configuration is deleted.

2. If you are restoring the Citrix SDX appliance by using a backup of a different Citrix SDX appliance, ensure 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.

3. Make sure that the Citrix SDX platform variant that was backed up was taken in same as the one on which you are trying to restore. You cannot restore from a different platform variant.

Force a failover to the secondary Citrix ADC instance

August 1, 2019

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix Application Delivery Controller (ADC) instance. You can force failover from either the primary instance or the secondary instance. When you force a failover on the primary instance, the primary becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the instance.

A forced failover fails in any of the following circumstances:
   - You force failover on a standalone system.
• The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.

• The secondary instance is configured to remain secondary.

The 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 Application Delivery Management (ADM), navigate to Networks > Instances > Citrix ADC > VPX tab, and then select an instance.

2. Select instances in an HA setup from the instances listed under the selected instance type.

3. From the Action menu, select Force Failover.

4. Click Yes to confirm the force failover action.

**Force a secondary Citrix ADC instance to stay secondary**

August 1, 2019

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want
the secondary node to take over; you want it to remain the secondary node even if it detects a failure in the primary node.

When you force the secondary node to stay secondary, it will remain 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.

Forcing the node to stay secondary works on both standalone and secondary nodes. On a standalone node, you must use this option before you can add a node to create an HA pair. When you add the new node, the existing node continues to function as the primary node, and the new node becomes the secondary node.

**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 Application Delivery Management (ADM), navigate to **Networks > Instances > Citrix ADC > VPX** tab, and then select an instance.
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the “Stay Secondary” action.

Create instance groups

August 1, 2019
To create an instance group, you must first add all your Citrix Application Delivery Controller (ADC) instances to Citrix Application Delivery Management (ADM). After you have added the instances successfully, create instance groups based on their device family. By creating a group of instances, you can simultaneously perform actions such as upgrade, backup, and restore on all instances that have been grouped, instead of performing them on each instance separately.

**To create an instance group using Citrix ADM:**

1. In Citrix ADM, navigate to **Networks > Instance Groups**, and then click **Add**.
2. Give a name to your instance group and select the instance family from the list.
3. Select the instance type from the **Instance Family** menu.
4. Click **Select Instances** and select the instances from the window that slides in.
5. Click **Create**.

### Rediscover multiple Citrix VPX instances

August 1, 2019

You can now rediscover multiple Citrix VPX instances in your Citrix Application Delivery Management (ADM) setup. Previously, you could rediscover only single Citrix VPX instances. You can rediscover multiple Citrix VPX instances when you want to view the latest states and configurations of those instances. The Citrix ADM server rediscovers all the Citrix VPX instances and checks whether the Citrix Application Delivery Controller (ADC) instances are reachable.

**To rediscover multiple Citrix VPX instances:**

1. In a web browser, type the IP address of the Citrix ADM server (for example, [http://192.168.100.1](http://192.168.100.1)).
2. In the **User Name** and **Password** fields, enter the administrator credentials. The default administrator credentials are nsroot and nsroot.
3. Navigate to **Networks > Instances > Citrix ADC > VPX** tab and select the instances you want to rediscover.
4. In the **Select Action** menu, click **Rediscover**.
5. When the confirmation message for running the Rediscover utility appears, Click **Yes**.

The screen reports the progress of rediscovery of each of the Citrix VPX instances.
Unmanage an instance

If you want to stop the exchange of information between Citrix Application Delivery Management (ADM) and the instances in your network, you can unmanage the instances.

To unmanage an instance:

Navigate to Networks > Instances > Citrix ADC > VPX tab. In the list of instances, either right-click an instance and then select Unmanage, or select the instance and from the Select Action list, select Unmanage.

The status of the selected instance changes to Out of Service as shown in the following figure.

Trace the route to an instance

By tracing the route of a packet from the Citrix Application Delivery Management (ADM) to an instance, you can find information such as the number of hops necessary in order to reach the instance. Traceroute traces the path of the packet from source to destination. It displays the list of network hops along with the host name and IP address of each entity in the route.

Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, traceroute shows where the problem exists.

To trace the route of an instance:

1. In Citrix ADM, navigate to Networks > Instances > Citrix ADC > VPX tab.
2. In the list of instances, either right-click an instance and then select **TraceRoute** or select the instance and from the **Select Action** menu, click **TraceRoute**.

The TraceRoute message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.

**Events**

August 1, 2019

When the IP address of a Citrix Application Delivery Controller (ADC) instance is added to Citrix Application Delivery Management (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 (**Networks > Events**), and all active events are displayed in the Event Messages page (**Networks > 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 may require immediate attention. For example, system failure could be categorized as a “Critical” event severity and would need to be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of 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 executed. 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 additional measure, you may customize your email with a specific subject line, user message, and upload an attachment.

**Use events dashboard**

August 1, 2019
As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your Citrix Application Delivery Controller (ADC) instances, along with events and their severity on specific instances. You can use the Citrix Application Delivery Management (ADM)’s events dashboard 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 **Networks > 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 on 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 (**Networks > Events > Reports > NetScaler/ NetScaler SDX/ NetScaler SD-WAN WO**) 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
Set event age for events

August 1, 2019

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 will receive an email notification with details such as entity name, status change, and time.
To set event age in Citrix ADM:

1. In Citrix ADM, navigate to Networks > Events > Rules, and click Add.
2. On the Create Rule page, set the rule parameters.
3. Specify the event age in seconds.

Ensure to set all the co-related traps in the Category section and also set the respective severity in the Severity section when you set event age. In the above example, select the entityup, entitydown, and entityofs traps.

Schedule an event filter

August 1, 2019

After creating a filter for your rule, if you do not want the Citrix Application Delivery Management (ADM) server to send a notification every time the event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals such as daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends a large number of email notifications when 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 Networks > 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 checkbox to enable the scheduled event rule.
   - **Recurrence** - Interval at which to schedule the rule. Select either a specific day of the week or a specific date in a month.
   - **Days**: Select the day of the week to run the rule. You can select multiple days.
   - **Dates**: Type in the dates. You can type multiple dates as comma-separated values.
   - **Scheduled Time Interval (Hours)** – Hour(s), at which to schedule the rule (use the 24-hour format).

4. Click Schedule.

**Set repeated email notifications for events**

August 1, 2019

To ensure that all critical events are addressed and no important email notifications are missed, you can opt to send repeated email notifications for event rules that meet the criteria you’ve selected. For example, if you’ve created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

**Note**

Events can only be cleared automatically if there is an equivalent “clear” trap set and sent from your Citrix Application Delivery Controller (ADC) instance.

To clear an event manually, you can do the following:

- Navigate to Networks > Events > Event Summary, choose a Category and select an event in the category and click Clear.
- Or, navigate to Networks > Events > Event Messages. Choose an instance type and then, select an event from the grid below and click Clear.

**To set repeated email notifications from Citrix ADM:**

1. In Citrix Application Delivery Management (ADM), navigate to Networks > 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**: abc-mails
- **Email Subject**: Critical event
- **Attachment**: Choose File
- **Message**: Disk failures to be resolved
- **Repeat Email Notification until the event is cleared**
- **Time Interval (minutes)**: 5
Suppress events

August 1, 2019

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 suppress events by using Citrix ADM:**

1. In Citrix Application Delivery Management (ADM), navigate to **Networks > Events > Rules**. Click **Add**.
2. Specify all the parameters required to create a rule.
3. Under **Event Rule Actions**, click **Add Action** to assign notification actions for the event.
4. On the **Add Event Action** page, select **Suppress Action** from the **Action Type** drop-down and specify the time period, in minutes, for which an event needs to be suppressed.
5. Click **OK**.

Create event rules

August 1, 2019

May 24, 2018

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of events generated across your Citrix Application Delivery Controller (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 executed. The conditions for which you can create filters are: severity, 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.
- **Send SMS Action**: Send a Short Message Service (SMS) message for each event that matches the filter criteria.
- **Run Command Action**: Run a command when an incoming event meets the configured rule.
- **Execute Job Action**: Execute a job is for events that match the filter criteria that you’ve specified.
- **Suppress Action**: Suppresses drop an event for a specific time period.

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/or attachment.

For example, as an administrator you might want to monitor “high CPU usage” events for specific Citrix ADC instances if those events could lead to an outage of your Citrix ADC instances. You could create a rule to monitor the instances, and specify an action that sends you an email notification when an event in the “high CPU usage” category occurs. You could schedule the rule to run at a specific time, such as between 11 AM to 11 PM, so that you are not notified every time there is an event generated.
Configuring an event rule involves the following tasks:

1. Define the rule
2. Choose the severity of the event that the rule detects
3. Specify the category of the event
4. Specify Citrix ADC instances to which the rule applies
5. Specify failure objects
6. Specify any additional filters
7. Specify actions to be taken when the rule detects an event

**Step 1 - Define an event rule**

Navigate to **Networks > Events > Rules**, and click **Add**. If you want enable your rule, select the **Enable Rule** checkbox.

You can set the **Event Age** option to specify the time interval (in seconds) after which Citrix Application Delivery Management (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 a period of 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 will receive an email notification with details of the event.

You can also filter event rules by **Device Family** to track the Citrix ADC instance from which Citrix ADM receives an event.
**Step 2 - Choose the severity of the event**

You can create event rules that use the default severity settings. Severity specifies the current severity of the events you which you want to add the event rule.

You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.

![Severity levels](image)

**Note**

You can configure severity for both generic and enterprise-specific events. To modify event severity for Citrix ADC instances managed on Citrix ADM, navigate to **Networks > 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 - Specifying 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 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 will need to 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.

Step 5 - Select failure objects

You can either select a failure object from the drop-down list provided or add a failure object for which an event has been generated. Failure objects are entity instances or counters for which an event has been generated.

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. For example, if a user has login issues, then the failure object here is the username or password, such as “nsroot”.

This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events, and so on.
Step 6 - Specify additional filters

You can further filter an event rule by:

- **Configuration Commands** - You can specify the complete configuration command, or specify the description pattern within asterisk (*) to filter the events. In addition to the command, you can choose to 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 the description pattern within asterisk (*) to filter the events.
  For example, for a NetscalerConfigChange event, type *ns_client_ipaddress :10.102.126.250*.
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 e-mail Action
- Send Trap Action
- Send SMS Action
- Run Command Action
- Execute Job Action
- Suppress Action

To set e-mail Event Rule Action:

When you choose the Send e-mail Action event action type, an email is triggered when the events meet the defined filter criteria. You will need to 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.

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.

Using this option, 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 checkbox 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 listeners when events meet the defined filter criteria.

**To set SMS Event Rule Action:**

When you choose the **Send SMS Action** event action type, a **Short Message Service** (SMS) message for each event that matches the filter criteria. You will need to either create an SMS distribution list by providing the SMS server or SMS profile details or you can select an SMS distribution list that you’ve previously created.

**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 executed on Citrix ADM for events matching a particular filter criterion. For example, if an event of “Critical” severity is raised when there is a configuration change on a managed instance, you can run a command script.

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>$source</td>
<td>This parameter corresponds to the source IP address of the received event.</td>
</tr>
<tr>
<td>$category</td>
<td>This parameter corresponds to the type of traps defined under category of the filter</td>
</tr>
<tr>
<td>$entity</td>
<td>This parameter corresponds to the entity instances or counters for which an event has been generated. It can include the counter names for all threshold-related events, entity names for all entity-related events, and certificate names for all certificate-related events.</td>
</tr>
<tr>
<td>$severity</td>
<td>This parameter corresponds to the severity of the event.</td>
</tr>
<tr>
<td>$failureobj</td>
<td>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.</td>
</tr>
</tbody>
</table>
To configure the “Run Command Action” event action on Citrix ADM:

1. Under Event Rule Actions, click Add Action and select Run Command Action from the Action Type drop-down.

2. On the Create Command Distribution List page, specify a profile name and the command to be run. This command will be executed when the events meet the defined filter criteria.

   ![Create Command Distribution List](image)

   **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 will discard 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 executed as a built-in job or a custom job for Citrix ADC, Citrix SDX, and Citrix SD-WAN WO 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 menu.

2. Create a profile with a job you want 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.

![Create Job](image)

**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.

![Add Event Action](image)

Your event rule is now created with appropriate filters and well defined event rule actions.

**Modify the reported severity of events that occur on Citrix ADC instances**

August 1, 2019

You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on a particular instance and view reports on the basis of event
severity. You can create event rules that use the default severity settings, and you can change the severity settings. You can configure severity for both generic and enterprise-specific events.

You can define the following levels of severity: Critical, Major, Minor, Warning, and Clear.

To modify event severity:

1. Navigate to Networks > Events > Event Settings.
2. Click the tab for the Citrix Application Delivery Controller (ADC) instance type that you want to modify. Then, select the category from the list and click Configure Severity.
3. In Configure Event Severity, select the severity level from the drop-down list.
4. Click OK.

View events summary

August 1, 2019

You can now view an Events Summary page to monitor the events and traps received on your Citrix Application Delivery Management (ADM) server. Navigate to Networks > 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 (ADC) instance goes down and stops sending information to the Citrix ADM server. During the event, a notification is sent to an administrator, explaining the reason why the instance is down, the time for which it had been down, and so on. The event is then recorded on the Events Summary page, on which you can view a summary and access the details of the event.

• **Number of traps received for each category.** The number of traps received, categorized by severity. By default, each trap sent from 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 on 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 Citrix ADC instance's IP address and host name, date on which the trap was received, category, failure objects, configuration command run, and the message notification.

### Display event severities and SNMP trap details

August 1, 2019

When you create an event and its settings in Citrix Application Delivery Management (ADM), you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all Citrix Application Delivery Controller (ADC) instances added to your 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 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 VPX instance on the Dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of
service. By clicking on the graph, you are taken to that instance's page, where the out of service filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and so on. You can also select the instance and see that particular Citrix instance's 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 **Networks > Dashboard**.
   
   Or,

   Navigate to **Networks > Events > Reports**.
3. From the menu in the upper-right corner of the page, select the duration for which you want to see events by severity.
4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.
5. You can click each section on the donut chart to display the corresponding **Severity based events** page, which shows the following details for the selected severity for the selected duration:
   
   • Instance Source
   
   • Data of the event
   
   • Category of events generated by the 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 more easily view and monitor your chosen severity.

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 server on the Event Settings page. Navigate to Networks > 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 to.
- **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.”

Export syslog messages

August 1, 2019

You can now view syslog messages without logging into Citrix Application Delivery Management (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 (ADC) instances in PDF,
CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses at various intervals.

**Note**
For more information about configuring a syslog server, the syslog data and time format, and how to view syslog messages on Citrix ADM, see [View Auditing Information](#).

To view syslog messages, navigate to Networks > Events > Syslog Messages. In the right pane, under Syslog Viewer, you can filter the syslog messages you want to view by module, event type, severity, and source IP address. Click **Apply** to generate the syslog messages.

**To export a syslog messages report by using Citrix ADM:**

1. Navigate to Networks > Events > Syslog Messages.
2. In the right pane, click on the export button at the top right corner of the Syslog Messages page.
3. Under the **Export Now** tab, select the required format, and then click **Export**.

![Export Now](image)

**To schedule the export of syslog messages report by using Citrix ADM:**

1. Navigate to Networks > Events > Syslog Messages.
2. On the Syslog Messages page, in the right pane, click on **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 drop-down list provided. An email is triggered when the report...
Citrix Application Delivery Management 12.1

is generated and meets the scheduled time criteria. If you want to create a new email distribution list, click + and provide mail server and mail profile details.

How to Configure Events Prune Settings by Using Citrix ADM

To limit the amount of event messages data being stored in your Citrix ADM server’s database, you can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

Navigate to System > System Administration. Under Instance Settings, click Events Prune Settings. Enter the time interval, in days, for which you want to retain data on the Citrix ADM server and click OK.
Suppress syslog messages

When configured as a syslog server, Citrix Application Delivery Management (ADM) receives all syslog messages sent to it by the configured Citrix Application Delivery Controller (ADC) instances. There might be a large number of messages that you might not want to see. For example, you might not be interested in seeing all informational level messages. You can now discard some of the syslog messages that you are not interested in. You can suppress some of the syslog messages coming into Citrix ADM by setting up some filters. Citrix ADM drops all messages that matches 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 matches 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 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 Networks > Events > Syslog Messages > Suppress Filter.

2. On Create Suppress Filter page, update the following information:
   a) Name - type a name for the filter.
   
   Note
   
   If different users have different access to multiple Citrix ADC instances, different filters must be created for different instances as users can see only those filters in which they have access to all the instances.

   b) Severity - Select and add the log levels for which you must suppress the messages. For example, if you do not want to view any informational messages coming in, you can select Informational to suppress those messages.
c) **Instances** - Select the Citrix ADC instances on which the syslog messages have been configured.

![Create Suppress Filter](image)

**d) Facilities** - Select the facility to suppress messages on the basis of the source that generates them.

**e) Message Pattern** - You can also type a text pattern surrounded by asterisk (*) to suppress the messages. The messages are searched for the text pattern string and those messages that contain this pattern are suppressed.
Disabling the filter

To allow the messages to be viewed on Citrix ADM, you must disable the filter.

1. Navigate to Networks > Events > Syslog Messages > Suppress Filter, and on Suppress Filter page, select the filter and click Edit.

2. On Configure Suppress Filter page, clear Enable Filter check box to disable the filter.

Configure prune settings for instance events

August 1, 2019

Citrix Application Delivery Controller (ADC) instances managed by your Citrix Application Delivery Management (ADM) server send event messages data continuously to be stored on Citrix ADM. You can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

Note

The value you can specify cannot exceed 40 days or be less than 1 day.

To configure prune settings for instance events:

1. Navigate to System > System Administration.

2. Under Prune Settings, click Instance Events Prune Settings.
3. Enter the time interval, in days, for which you want to retain data on the Citrix ADM server and click **OK**.

---

**SSL Dashboard**

August 1, 2019

Citrix Application Delivery Management (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 keep track of your SSL certificates.

An Secure Socket Layer (SSL) certificate, which is an integral part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the Citrix Application Delivery Controller (ADC) appliance, is used to complete asymmetric key (or public key) encryption and decryption.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as VeriSign
- By generating a new SSL certificate and key on the 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 keep track of 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 then create Citrix ADM.

You can link a Citrix ADC instance’s certificate(s) to a CA certificate. However, make sure that all of the certificate(s) that you link to the same CA certificate have the same source and the same issuer. After you have linked the certificate(s) to a CA certificate, you can unlink them.

**Use the SSL Dashboard**

August 1, 2019

You can use the SSL certificate dashboard in Citrix Application Delivery Management (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

**To monitor SSL certificates**

You may use the SSL dashboard on Citrix ADM to monitor your certificates if your company has SSL Policy where you have defined certain SSL certificate requirements such as all certificates must have minimum key strengths of 2048 bits and a trusted CA authority must authorize it.

In another example, you 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 on 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 **Networks > 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 Networks > SSL Dashboard and click Poll Now. The Poll Now page pops up, presenting the option to poll all Citrix Application Delivery Controller (ADC) instances in the network or poll selected instances.

You can use the Citrix ADM SSL dashboard to view or monitor the details of Citrix ADC 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 52 under “Self signed vs. CA signed” in the above figure, a new window appears, showing details of the 52 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. 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 on 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 on the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.

**To view audit trails for SSL certificates**

You can now view log details of SSL certificates on 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 trail information is useful while monitoring SSL certificate changes done on an application with multiple owners.

To view an audit log for a particular operation performed on Citrix ADM using SSL certificates, navigate to Networks > SSL Dashboard > SSL Audit Trails.
For a particular operation performed using SSL certificate you can view its status, start time, and end time. Furthermore, you can view the instance on which the operation was performed and the commands executed on that instance.

To exclude default Citrix ADC certificates on the SSL Dashboard

Citrix ADM allows you to show or hide default Citrix ADC 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 **Networks > SSL Dashboard** in the Citrix ADM GUI.
2. On SSL Dashboard page, click Settings.


4. Type the number of days when the certificate expires to receive notification about certificate expiry.

5. Select the method of notification and create the respective profiles.

6. In the Certificate Filter section, clear the Show Default Certificates check box and click Save and Exit.

Set up notifications for SSL certificate expiry

August 1, 2019

As a security administrator, you can set up notifications to inform you when certificates are about to expire and to include information about which Citrix Application Delivery Controller (ADC) instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

For example, you can set an email notification to be sent an email distribution list 30 days before your certificate is due to expire.

To set up notifications from Citrix ADM:

1. In Citrix Application Delivery Management (ADM), navigate to Networks > SSL Dashboard.

2. On the SSL Dashboard page, click Settings.

3. On the SSL Settings page, click the Edit icon.

4. In the Notification Settings section, specify when you want to send the notification in terms of number of days prior to the expiration date.

5. Choose the type of notification you want to send. Select the notification type and the distribution list from the drop-down menu. The notification types are as follows:

   - Email – Specify a mail server and profile details. An email is triggered when your certificates are about to expire.

   - SMS – Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your certificates are about to expire.

   - Slack - Specify Slack profile details.

6. Click Save and Exit.

Citrix ADM now sends SSL certificate expiry trap to external trap destination server when your SSL certificates are due for expiry. Citrix ADM sends a trap when the following two conditions are satisfied:
- You have configured the number of days for the certificate expire in SSL dashboard settings page.
- You have added the trap destination.

You can set trap destinations by navigating to System > SNMP > Trap Destinations. Type the IP address of the destination SNMP server where the traps are sent. Enter the port number and type “public” (without quotes) as the community string.

**Update an installed certificate**

August 1, 2019

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from Citrix Application Delivery Management (ADM) without needing to log on to individual Citrix Application Delivery Controller (ADC) instances.

**To update an SSL certificate, key, or both from Citrix ADM:**

1. In Citrix ADM, navigate to Networks > 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.
Before installing SSL certificates on Citrix Application Delivery Controller (ADC) instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed with secure signature algorithms.

To install an SSL certificate from another Citrix ADC Instance:

You can also import a certificate from a chosen Citrix ADC instance and apply it to other targeted Citrix ADC instances from the Citrix Application Delivery Management (ADM) GUI.

1. Navigate to **Networks > SSL Dashboard**.
2. In the upper-right corner of the SSL dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:
   
   a) **Certificate Source**
   
   Select the option to **Import from Instance**.
   
   • Choose the **Instance** that you want to import the certificate from.
   
   • Choose the **Certificate** from the list of all SSL certificate files on the instance.

   b) **Certificate Details**
   
   • **Certificate Name**. Specify a name for the certificate key.
   
   • **Password**. Password to encrypt the private key. You can use this option to upload encrypted private keys.

4. Click **Select Instances** to select the 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 **Networks > SSL Dashboard**.

2. In the upper-right corner of the dashboard, click **Install**.

3. On the **Install SSL Certificate on NetScaler Instance** page, select **Upload Certificates File** and specify the following parameters:
   
   • **Certificate File** - Upload an SSL certificate file by selecting either **Local** (your local machine) or **Appliance** (the certificate file must be present on the 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 ADM instances on which you want to install your certificates.

4. To save the configuration for future use, select the **Save Configuration** check box.

5. Click **OK**.

### Install SSL Certificate on Citrix ADC Instances

<table>
<thead>
<tr>
<th>Certificate Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import from Instance</strong></td>
</tr>
<tr>
<td><strong>Certificate File</strong></td>
</tr>
<tr>
<td>Choose File</td>
</tr>
<tr>
<td>Choose File</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certificate Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td>[ ]</td>
</tr>
<tr>
<td>[ ]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.29.200</td>
<td>--</td>
</tr>
<tr>
<td>10.102.29.160</td>
<td>NS</td>
</tr>
</tbody>
</table>

**Create a Certificate Signing Request (CSR)**

August 1, 2019
A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate will be used. It contains information that will be included in the certificate such as the name of your organization, common name (domain name), locality, and country.

**To create a CSR using Citrix ADM:**

1. In Citrix Application Delivery Management (ADM), navigate to **Networks > SSL Dashboard**.
2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select **Create CSR** from the **Select Action** list.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:
   - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the Citrix ADM virtual instance).
   - **Create a key** - Select the **I do not have a Key** option, and then specify the following parameters:

<table>
<thead>
<tr>
<th>Encryption Algorithm</th>
<th>Type of key. For example, RSA.</th>
</tr>
</thead>
<tbody>
<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 (<strong>DES</strong> or <strong>DES3</strong>) that you want to use to encrypt the generated RSA key. If you select this algorithm, you’ll need to 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 additional details. If you want to create the CSR without changing the defaults, click **Continue**.

**Note**

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.

Most CAs accept certificate submissions by email. The CA will return a valid certificate to the email address from which you submit the CSR.

---

**Link and unlink SSL certificates**

August 1, 2019

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 Application Delivery Management (ADM), navigate to **Networks > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select **Link** from the **Action** drop-down list.
4. From the list of matched certificates, select the certificate to which you want to link, and then click **OK**.

**Note**

If a matching certificate is not found, the following message is displayed: No certificate found to link.

**To unlink an SSL certificate using Citrix ADM:**

1. In Citrix ADM, navigate to **Networks > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select **Unlink** from the **Action** drop-down list.
4. Click **OK**.
Configure an enterprise policy

August 1, 2019

You can configure an enterprise policy and add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificate keys in Citrix Application Delivery Management (ADM). If any of the certificates installed on your Citrix Application Delivery Controller (ADC) instance have not been added to the enterprise policy, the SSL certificate dashboard displays the issuer of those certificates as Not Recommended. Also, if the certificate key strength does not match the recommended key strength in the enterprise policy, the SSL certificate dashboard displays the strengths of those keys as Not Recommended.

To configure an enterprise policy on Citrix ADM:

1. In Citrix ADM, navigate to Infrastructure > SSL Dashboard, and then click Settings.
2. On the SSL Settings page, click the Edit icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys.
3. Click Save to save your enterprise policy.

Poll SSL certificates from Citrix ADC instances

August 1, 2019

Citrix Application Delivery Management (ADM) automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix Application Delivery Controller (ADC) instances. Polling all the 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 Networks > 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.
   a) To poll the SLL certificates of all the Citrix ADC instances, select the All Instances tab and click Start Polling.
   b) To poll specific instances, select the Select Instances tab, select the instances from the list, and click Poll Now.

Configuration jobs

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple Citrix Application Delivery Controller (ADC) instances in the network.

Citrix ADM allows you to create configuration jobs that will 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 execute a configuration job.

1. Configuration Template
2. Instance
3. File
4. Record and Play

**Configuration Template**

You can create configuration templates while creating a new 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. 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 execute the job immediately or schedule the job to be executed at a later stage.

**Instance**

You can perform a single-bundle upgrade of your Citrix 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 executing the commands on another Citrix ADC instance of the same type. This allows you to replicate the configuration of one instance on the other.

**File**

You can upload a configuration file from your local machine and create jobs.

Advantages of using a file

- You can use any text file to create a reusable source of configuration commands.
- Any kind of formatting is not required.
- The file can be saved on your local machine.

You can either create and save a new file or import an existing file, and run the commands.
Record and Play

Using Create job you can either enter your own CLI commands, or you can use 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.

Related Articles

- How to Use SCP (put) Command in Configuration Jobs
- How to Use Variables in Configuration Jobs
- How to Create Configuration Jobs from Corrective Commands
- How to Use Configuration Templates to Create Audit Templates
- How to Use Record-and-Play to Create Configuration Jobs
- How to Use the Master Configuration Template on Citrix ADM

Create a configuration job

August 1, 2019

A job is a set of configuration commands that you can create and run on one or more multiple managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the Citrix Application Delivery Management (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 Networks > 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 drop-down list.
4. In the Configuration Source drop-down 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 drop-down list, select the different templates and then drag and drop the templates in 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 and then add a template of different type, then the whole job template will be of Master Configuration type.

5. 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 at a later time while editing the configuration job.

6. You can define variables that enable you to assign different values for these parameters or execute 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 on the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

7. In the **Select Instances** tab, select the instances you want to run the configuration audit on and click **Next**.

8. 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

9. Click **Next**.

10. You can evaluate and verify the commands to be run on each instance on the **Job Preview** tab. To evaluate rollback commands, select the **Preview Rollback Commands** checkbox

11. In the **Execute** tab, choose to either execute your job now or schedule to execute the job at a later time. Also, you must also select what action Citrix ADM should take if the command fails.

**To send email notification for a job:**

An email notification is now sent every time a job is executed or scheduled. The notification will cover details such as the success or failure of the job along with the relevant details.

After creating a job, in the Execute tab, select the **Email** checkbox under the Receive Execution Report Through section. Choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the + icon and specifying email server details.
To view execution summary details:

Navigate to **Networks > Configuration Jobs**. Select a job and click **Details**. Click **Execution Summary** to see the status of the instance on that executed the job, the commands executed on the job, the start and end time of the job, and the instance user’s name.

**Use record-and-play to create configuration jobs**

August 1, 2019
If you are accustomed to using the NetScaler GUI to configure a NetScaler instance, at times, you might find it difficult to recall the exact CLI commands to create a configuration task and run it on multiple NetScaler instances.

Citrix ADM enables you to record the configuration tasks performed using the GUI of a NetScaler instance and convert it into CLI commands. You can then create a configuration task from these CLI commands and run this task on multiple instances.

To record the GUI configuration and convert it into a configuration task

1. Navigate to Networks > Configuration Jobs, and then click Create Job.
2. Specify the job name and the type of instance.
3. From the Configuration Source list, select Record and Play, and then select the source instance from which you want to record the configuration. Click Record.
4. The NetScaler GUI opens. Configure the features and settings that you want the configuration task to contain. Then, close the NetScaler GUI window and click Stop in the Configuration Editor. The commands appear as a link in the left pane. Drag and drop the commands to the right pane, and then click Next.

You can then rearrange and reorder the commands in the configuration editor as appropriate. 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.
5. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.

6. Do one of the following to view all the variables in a single consolidated view:

   • While creating a configuration job, navigate to **Networks > Configuration Jobs**, select **Create Job**. On the **Create Job** page, you can review all the variables that you have added while creating the configuration job.

   • While editing a configuration job, navigate to **Network > Configuration Jobs**, select the **Job Name** and click **Edit**. On the **Configure Job** page, you can review all the variables that were added while creating the configuration job.

7. You can then click on the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

   ![Image showing the Preview Variables tab](image)

8. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the **Done** button after you have edited or modified any of the parameters.

   ![Image showing the Preview Variables table](image)

9. Click **Add Instances** and select the instances on which you want to run the configuration job. Click **OK**, and then click **Next**.
10. If you have specified variables in the commands, on the **Specify Variable Values** tab, select one of the following options to specify variables for your instances:

- **Upload input file for variables values**: Click **Download Input Key** File to download an input file. In the input file, enter values for the variables that you have defined in your commands, and then upload the file to the Citrix ADM server.

- **Common variable values for all instances**: Enter values for the variables. The variables vary depending on the selected template.

The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

To view the executed configuration jobs while creating a configuration job, navigate to **Network > Configuration Jobs**, and click **Create Job**. In the **Create Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already executed configuration jobs while editing a configuration job, navigate to **Network > Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

11. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

12. On the **Execute** tab, you can choose to execute your job now or schedule it to be executed at a
later time. You can also choose what action Citrix ADM should take if the command fails.

You can also choose to allow authorized users to execute jobs on your managed instances, and you can choose whether to send an email notification regarding the success or failure of the job, along with other details.

13. On the Jobs page, you can then view the progress of your configuration task execution on all the instances.
Use configuration jobs to replicate configuration from one instance to multiple instances

August 1, 2019

You can use the Configuration Jobs feature of Citrix ADM to extract a particular configuration from a NetScaler instance and replicate it on multiple instances.

For example, you might have configured both load balancing and front-end optimization (FEO) on a NetScaler instance for your deployment. However, now you want to replicate only the FEO configuration to other NetScaler instances.

To retrieve and replicate configuration from one instance to other NetScaler Instances:

1. Navigate to Networks > Configuration Jobs, and then click Create Job.

2. Specify the job name and the type of instance.

3. Select Instance as the Configuration Source and select the source instance whose configuration you want to replicate. Select the type of configuration that you want to extract. If you select the “Configuration by time duration,” set the time period when you had run this configuration, and then click Extract.

The number of commands executed on that instance in the time duration you selected is displayed on the screen as highlighted in the image below.
Job Name*  
replicate-job

Configuration Editor

Configuration Source
Instance

Source Instance
10.102.29.120

- Running Configuration
- Saved Configuration
- Configuration by time duration

Duration
Today

Extract

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name.

10 commands from 10.102.29.120
4. Drag and drop the commands to the **Commands** field in the right pane.

Retain only the commands related to FEO and manually delete the commands related to load balancing, or commands related to any other configuration, and then click **Next**.

5. Click **Add Instances** and add the instances on which you want to apply the FEO configuration. Click **OK**, and then click **Next**.

6. If you have specified variables in the commands, on the Specify Variable Values tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to Citrix ADM.

7. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

8. On the **Execute** tab, click **Finish** to execute the job on the selected NetScaler instances.
Use variables in configuration jobs

August 1, 2019

A configuration job is a set of configuration commands that you can execute on one or more managed instances. When you execute the same configuration on multiple instances, you might want to use different values for the parameters used in your configuration. You can define variables that enable you to assign different values for these parameters or execute a job across multiple instances.

For example, consider a basic load balancing configuration where you add a load balancing virtual server, add two services, and bind the services to the virtual server. Now, you might want to have the same configuration on two instances but with different values for the virtual server and services names and IP addresses. You can use the configuration jobs feature to achieve this by using variables to define the names and IP addresses of the virtual server and services.

In this example, the following commands and variables are used:

add lb vserver servername HTTP ipaddress portnumber
add service servicename1 ipaddress1 HTTP 80
add service servicename2 ipaddress2 HTTP 80
bind lb vserver servername servicename1
bind lb vserver servername servicename2

To create a configuration job by defining variables in Citrix ADM:

1. Navigate to Networks > Configuration Jobs.
2. Click Create Job.
3. On the Create Job page, select the custom job parameters such as the name of the job, the instance type, and the configuration type.
4. In the Configuration Editor, type in the commands to add a load balancing virtual server, two services, and bind the services to the virtual server. Double click to select the values that you want to convert to a variable, and then click Convert to Variable. For example, select the IP address of the load balancing server ipaddress, and click Convert to Variable as shown in the image below.
5. Once you see dollar signs enclose the variable's value, click on the variable to further specify the details of the variable such as name, display name, and type. You can also click the Advanced option if you want to further specify a default value for your variable. Click Save and then, click Next.

Type in the rest of your commands and define all the variables.

6. You can review all the variables that you have defined while creating or editing a configuration.
job in a single consolidated view.

7. Do one of the following to view all the variables in a single consolidated view:
   - While creating a configuration job, navigate to Networks > Configuration Jobs, select Create Job. On the Create Job page, you can review all the variables that you have added while creating the configuration job.
   - While editing a configuration job, navigate to Network > Configuration Jobs, select the Job Name and click Edit. On the Configure Job page, you can review all the variables that were added while creating the configuration job.

8. You can then click on the Preview Variables tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

9. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the Done button after you have edited or modified any of the parameters.

10. You can then rearrange and reorder the commands in the configuration editor as appropriate. 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.
11. Select the instances you want to run the configuration job on.

12. In the Specify Variable Values tab, select the Upload input file for variable values option and then click Download Input Key File. In our example, you will need to specify the server name on each instance, the IP addresses of the server and services, port numbers, and the service names. Save the file and upload it. If your values aren’t defined accurately, the system might throw an error.

13. The input key file is downloaded to your local system and you can edit it by specifying the variable values for each NetScaler instance you’ve selected previously and click Upload to upload the input key file to Citrix ADM. Click Next. The input key file downloads to your local system and you can edit it by specifying the variable values for each NetScaler instance that you have selected previously.

   **Note** In the input key file, the variables are defined at three levels:
   - Global level
   - Instance-group level
   - Instance level

Global variables are variable values that are applied across all instances. Instance group level variable values are applied to all instances that are defined in a group. Instance level variable values are only applied to a specific instance.

Citrix ADM gives first priority to instance level values. If there are no values provided to the variables for individual instances, Citrix ADM uses the value provided at the group level. If there are no values provided at group level, Citrix ADM uses the variable value provided at the global level. If you provide an input for a variable across all three levels, Citrix ADM uses the instance level value as the default value.

14. Click Upload to upload the input key file to Citrix ADM. Click Next.
**Important**

When you upload a CSV file from a Mac, Mac stores the CSV file with semicolons instead of commas. This will cause the configuration to fail when you upload the input file and run the job. If you are using a Mac, use a text editor to make the necessary changes and then upload the file.

15. You can also give common variable values across all instances and click **Upload** to upload the input key file to Citrix ADM.

The key input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

To view the executed configuration jobs while creating a configuration job, navigate to **Network > Configuration Jobs**, and click **Create Job**. In the **Create Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already executed configuration jobs while editing a configuration job, navigate to **Network > Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

16. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

17. In the **Execute** tab, you can choose to execute your job now or schedule it to be executed at a later time. You can also choose what action Citrix ADM should take if the command fails and if you’d like to send an Email notification regarding the success or failure of the job along with other details.
After configuring your jobs and executing it, you can see the job details by navigating to Networks > Configuration Jobs and select the job you just configured. Click on Details and then, click on Variable Details to see the list of variables added to your job.

Note

The values that you have provided for the variables in STEP 5 are retained by Citrix ADM when you save the job and exit, or when you schedule a job to be run at a later point of time.
Create configuration jobs from corrective commands

August 1, 2019

You can use the audit template feature in Citrix Application Delivery Management (ADM) to monitor configuration changes across managed Citrix ADC instances and troubleshoot configuration errors.

The typical work flow for auditing configuration changes using audit templates consists of the following steps:

1. Create audit template with a set of valid/expected Citrix ADC commands for auditing instance configurations.
2. Select the Citrix ADC instances against which you want to run the audit template to check for any differences between the running configuration and the expected configurations.
3. Understand the differential/corrective commands and utilize the “Create Job” functionality to get the instance's configurations to the desired state.

Consider a scenario where multiple administrators are managing five Citrix ADC instances. All these administrators make updates to the existing instance configuration as and when there are any changes needed. The super administrator wants to ensure that a certain set of important configuration remains untouched irrespective of the changes being made by other administrators. For this use case, the super administrator creates a template of the configuration that is expected to be present on the Citrix ADC instances and runs it against the instances. Citrix ADM compares the audit template configuration with the running configuration and reports any mismatch on the Configuration Audit dashboard.

If you notice that there is a change in the configuration of some instances, you can use the Citrix ADM corrective commands feature to create a configuration job with the modified and corrected configuration commands for specific Citrix ADC instances.

If any difference exists between the audit template configuration and the running configuration, a Diff Exists status message appears on the Audit Report page. Clicking the Diff Exits link takes you to the Configuration Diff page, where you can view the corrective command. You can also use these corrective commands to create a configuration job and execute that on the specific Citrix ADC instances to get them back to the desired configuration.

To create a configuration job from corrective commands on Citrix ADM:

1. Navigate to Networks > Configuration Audit.
2. On the Configuration Audit page, click inside any of the two donut charts to access the Audit Reports page.
3. Click the **Diff Exists** link (under the **Saved vs Running Diff** column in the table) for the instance for which you want to correct the configuration commands. The **Configuration Diff** page appears, listing the differences between the Saved Configuration, Running Configuration, and Correction Configuration for that instance.

4. Click **Create Job** to go to the **Create Job** page, on which the corrective commands are populated. For instructions on how to create a configuration job, see [How to Create a Configuration Job on Citrix ADM](#).

---

### Replicate running and saved configuration from one NetScaler instance to another

August 1, 2019

May 24, 2018

You can now replicate a NetScaler instance's configuration on other instances. When you configure a
job in Citrix ADM, select an instance as the Configuration Source and choose the selected instance's running or saved configuration.

For example, when you select Running Configuration and click Extract, Citrix ADM sends a request to the selected NetScaler instance to locate the running configuration, and displays it as a template. You can drag and drop the template into the Commands field in the right-hand pane. You can modify commands, parameters, and the instances.

To replicate running and saved configuration commands of one instance to another instance on Citrix ADM:

1. Navigate to Networks > Configuration Jobs, and click Create Job.
2. Specify the job name and the type of instance. For example, specify NetScaler Running Config1 as your job's name and the instance type as NetScaler.
3. Select Instance as the Configuration Source, select the source instance whose configuration you want to replicate on other instances.
4. You will see the following three options:
   - Running Configuration
   - Saved Configuration
   - Configuration by time duration
5. Choose Running Configuration, and click Extract. The number of running configuration commands executed on that instance is displayed.
6. Drag and drop the commands in the Commands field in the right pane.
7. You can edit the commands in the Commands field. For example, if the commands extracted are to set up a NetScaler instance. This may include adding partitions, setting up load balancing,
binding the load balancing server to services, and so on. You may want to edit your commands, to set up your new NetScaler instances without partitions. So, to remove partitions, manually delete commands related to the creation of partitions and click **Next**.

8. Click **Add Instances** and add the instances on which you want to apply the running configuration commands. Click OK and then, click **Next**.

9. If you have specified variables in the commands, on the **Specify Variable Values** tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to Citrix ADM.

10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

11. In the **Execute** tab, you can choose to execute your job now or schedule it to be executed at a later time. You can also choose what action Citrix ADM should take it the command fails and if you’d like to send an Email notification regarding the success or failure of the job along with other details.

### Reuse executed configuration jobs

August 1, 2019

Configuration jobs allow you to create a set of configuration commands that you can run on one or more managed instances. You can also run the same set of saved configuration jobs after modifying the commands, the parameters, the configuration source, and instances in the job. This is useful when the same sets of commands have to be executed on a different instance, or when the job encounters an error and stops further execution.

Citrix Application Delivery Management (ADM) provides a function to execute the completed jobs again. With this function, jobs that are executed completely can be run again without changing the job name.

**Note** You can re-execute only those jobs that are executed when the mode of execution is “Now.”

**To edit completed jobs:**

1. From Citrix ADM home page, navigate to **Networks > Configuration Jobs**.

2. In **Jobs** page, select a job that shows the Execution Summary as Completed, and click **Edit**. You can also edit a scheduled configuration job.

3. In **Configure Job** page, you can see that the Job Name and the Instance type are non-editable. You can modify other fields like configuration source, add instances, edit variable values, and set execution settings.
4. Click **Finish** to run the configuration job again.

![Image of the Jobs screen with a job named "ns-config-syslog" showing its execution summary, instance type, instances, and commands.]

**Note**

You can also select the job and click **Execute** again to run the job without modifying any source, instance, and commands. This is useful when you have to run the same set of commands on same instances. Sometimes, the job might encounter a transient error from the server side, and you might have to run the job again.

**Schedule jobs created by using built in templates**

August 1, 2019

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, use the built-in template option to schedule a job to configure syslog servers. You can also choose to execute the job immediately, or schedule the job to be executed at a later stage.

**To schedule a job by using built-in templates in Citrix Application Delivery Management (ADM)**

1. In Citrix ADM, navigate to **Networks > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, on the **Select Configuration** tab, specify the **Job Name** and select the **Instance Type** from the drop-down list.
3. Select **Inbuilt Template** from the **Configuration Source** drop-down list. Drag and drop the *NSConfigureSyslogServer* command to the right pane, and then click **Next**.

4. On the **Select Instances** tab, click **Add Instances**, select the instances on which you want to run the job, and then click **OK**.

5. Click **Next**. On the **Specify Variable Values** tab, select one of the following options to specify variables for your instances:
   - **Variable values from an input file** - Download an input file to enter values for the variables that you have defined in your commands. Then, upload the file to the Citrix ADM server.
   - **Common variable values for all instances** – Specify the syslog server IP address and port.

6. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

7. Click **Next**.

8. On the **Execute** tab, set the following conditions:
   - **On Command Failure** - If a command fails, you can either choose to ignore the errors and continue to execute the job or stop further execution of the job. Choose the action that you want to execute from the drop-down list.
   - **Execution Mode** - You can either execute the job now or schedule to execute the job later. If you want to schedule the job later, you must specify the execution frequency settings for that job. Choose the schedule you want the job to follow from the drop-down list.

9. You can also execute a job on a set of instances sequentially or in parallel by selecting the required method under **Execution Settings**. If a job execution fails on any instance, it does not continue on the remaining instances.

   You can choose to allow authorized users to execute jobs on your managed instances. An email notification can also be sent regarding the success or failure of the job, along with other details.
10. Click **Finish**.

   ![Citrix ADM Configuration Jobs](image)

   **Use maintenance jobs to upgrade NetScaler SDX instances**

   August 1, 2019

   You can perform a single-bundle upgrade of your NetScaler SDX instances running NetScaler release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in Citrix ADM. With this built-in task, you can upgrade the NetScaler SDX Management Service, Citrix Hypervisor, and the supplemental packs and hotfixes for Citrix Hypervisor.

   **To upgrade NetScaler SDX instances using Citrix ADM:**

   1. Navigate to **Networks > Configuration Jobs > Maintenance Jobs**.

   2. Click **Create Job**. In the Create Job page, select the **Upgrade NetScaler SDX** built-in task to upgrade your NetScaler SDX instances. Click **Proceed**.

   3. On one or more Upgrade NetScaler Appliances page, in the **Instance Selection** tab, specify the **Job Name** and click **Add Instances**.

   4. Select the target instances or instance groups that you want to upgrade.

   5. After you have added the NetScaler instances or instance groups, click **Next** to start the pre-upgrade validation on the selected instances. The screen reports the progress of pre-validation of each of the NetScaler instances.
6. On the **Modify Upgrade NetScaler Appliance(s)** page, select the **Upgrade** tab. From the **Software Image** drop-down menu, select either **Local** (your local machine) or **Appliance** (the build file must be present on Citrix ADM).

7. You can also see if any instances have pre-validation upgrade errors. These errors are shown in the form of message. The messages show the errors related to disk space, hard disk drive, and user customization. If you do not want to proceed with instances that have failed the pre-validation upgrade check, you can remove the instances. To remove the instances, select the instances and click **Delete**.

8. On the **Schedule Task** tab, you can also set execution details where you can perform the upgrade process now or schedule it for a later date. You can also choose to backup your NetScaler SDX instance, receive an execution report through email, or perform a two-stage upgrade for nodes in HA.

The two-stage upgrade for nodes in HA gives you the option to can either perform the upgrade immediately or schedule a time for the nodes to be updated one after another. Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.

### Create configuration jobs for Citrix SD-WAN WANOP instances

**August 1, 2019**

A job is a set of configuration commands that you can create and schedule on one or more managed instances. For Citrix SD-WAN WANOP instances, you can use the following options to create jobs:

- **Configuration Template**: 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.

- **File**: You can upload a configuration file from your local machine and create jobs.

Once a job is created, you can choose to execute the job immediately or schedule the job to be executed later. You can also set the execution frequency

<table>
<thead>
<tr>
<th>Inbuilt Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableCloudBridgeWANOpt</td>
<td>Enables traffic through the Citrix SD-WAN WANOP appliance.</td>
</tr>
<tr>
<td>Inbuilt Template</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DisableCloudBridgeWANOpt</td>
<td>Disables the traffic through Citrix SD-WAN WANOP appliance.</td>
</tr>
<tr>
<td>RestartCloudBridgeWANOpt</td>
<td>Restarts Citrix SD-WAN WANOP appliance.</td>
</tr>
<tr>
<td>RestoreConfig</td>
<td>Restores the configuration of Citrix SD-WAN WANOP appliance.</td>
</tr>
<tr>
<td>AddLink</td>
<td>Creating or defining links enable the SD-WAN WANOP appliance to prevent congestion and loss on the links and to perform traffic shaping. You can define the maximum bandwidth sent or received over the link and also specify it is LAN side or WAN side traffic.</td>
</tr>
<tr>
<td>ConfigureBandwidth</td>
<td>Sets the bandwidth limits and other bandwidth management settings.</td>
</tr>
<tr>
<td>AddUser</td>
<td>Adds a new user, for whom you can assign privileges.</td>
</tr>
<tr>
<td>AddUserAdvancedPlatform</td>
<td>Adds a new user enables you to assign privileges not available in the AddUser template.</td>
</tr>
<tr>
<td>AddService-class</td>
<td>Creates a service class for Citrix SD-WAN WANOP appliance with one or more service class filters and enables it.</td>
</tr>
<tr>
<td>SetApplication</td>
<td>Sets the application classifier definition.</td>
</tr>
<tr>
<td>AddorRemoveVideoCachingPorts</td>
<td>Adds or removes the port number at which the video source can send or receive data. The default port is 80.</td>
</tr>
<tr>
<td>RemoveVideoCachingSource</td>
<td>Removes one or more video caching source. Specify the video source IP address or domain name.</td>
</tr>
<tr>
<td>RemoveAllVideoCaching</td>
<td>Removes all the available video caching sources.</td>
</tr>
<tr>
<td>VideoCachingState</td>
<td>Enables or disables the video caching feature on Citrix SD-WAN WANOP appliances.</td>
</tr>
<tr>
<td>ClearVideoCaching</td>
<td>Clears either the video cache or the video caching statistics.</td>
</tr>
<tr>
<td>Inbuilt Template</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SetVideoCaching</td>
<td>Sets the maximum size for cached objects. An object larger than this limit is not cached. By default, the maximum caching object size is 100 MB.</td>
</tr>
<tr>
<td>AddVideoCachingSource</td>
<td>Adds the IP address or the domain name of the video source. Includes options to enable or disable video caching for that source.</td>
</tr>
<tr>
<td>ConfigureRemoteLicenseServer</td>
<td>Configures the centralized license server. Specify the license server model, IP address and port number.</td>
</tr>
<tr>
<td>ConfigureLocalLicenseServer</td>
<td>Sets the license server location as local.</td>
</tr>
<tr>
<td>InstallCACert</td>
<td>Installs CA certificates on Citrix SD-WAN WANOP appliance. Specify the certificate name, file name and the keystore password.</td>
</tr>
<tr>
<td>InstallCombinedCerKey</td>
<td>Installs a combined SSL certificate-key pair file.</td>
</tr>
<tr>
<td>InstallSeperateCertKey</td>
<td>Installs SSL certificate and key as separate files.</td>
</tr>
<tr>
<td>EnableWCCP</td>
<td>Enables WCCP deployment mode.</td>
</tr>
<tr>
<td>AddWCCPServiceGroup</td>
<td>Adds a new WCCP service-group definition for Citrix SD-WAN WANOP appliance.</td>
</tr>
<tr>
<td>DisableWCCP</td>
<td>Disables the WCCP deployment mode.</td>
</tr>
<tr>
<td>AddTrafficShapingPolicy</td>
<td>Creates a traffic shaping policy for the Citrix SD-WAN appliance. The policy controls the network bandwidth.</td>
</tr>
<tr>
<td>SetTrafficShapingPolicy</td>
<td>Modifies the traffic shaping policy for Citrix SD-WAN WANOP appliance. The policy controls the network bandwidth.</td>
</tr>
<tr>
<td>AddVideoPrePopulation</td>
<td>Creates a video pre-population entry, which enables you to download and cache a video in advance. You can also specify when to cache a video.</td>
</tr>
<tr>
<td>UpdateVideoPrePopulation</td>
<td>Modifies a video prepopulation entry, which specifies when to cache a video.</td>
</tr>
</tbody>
</table>
Inbuilt Template Description

<table>
<thead>
<tr>
<th>Inbuilt Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddVideoPrePopulationNow</td>
<td>Configures video prepopulation, enabling you to download and cache a video immediately. You can control how you want to download and cache videos from the URL(s).</td>
</tr>
<tr>
<td>VideoPrePopulationState</td>
<td>Changes, starts, updates, or removes video pre-population.</td>
</tr>
<tr>
<td>ConfigureSyslogServer</td>
<td>Sets the IP address and the port number of the syslog server.</td>
</tr>
<tr>
<td>ConfigureAlert</td>
<td>Configures alert level.</td>
</tr>
</tbody>
</table>

To create a configuration job for Citrix SD-WAN WANOP instances:

1. In Citrix ADM, navigate to **Networks > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, under the **Select Configuration** tab, specify the **Job Name**.
3. In the **Instance Type** field, select **Citrix SD-WAN WO**.
4. In the **Configuration Source** drop-down list, select an option to create a job.

   **Note**
   
   Select **Save as Configuration Template** and specify a name to save the configuration as a template and reuse it.

5. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
6. Do one of the following to view all the variables in a single consolidated view:
While creating a configuration job, navigate to Networks > Configuration Jobs, select Create Job. On the Create Job page, you can review all the variables that you have added while creating the configuration job.

While editing a configuration job, navigate to Network > Configuration Jobs, select the Job Name and click Edit. On the Configure Job page, you can review all the variables that were added while creating the configuration job.

7. You can then click on the Preview Variables tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

8. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the Done button after you have edited or modified any of the parameters.

9. Click Next, and then on the Select Instances tab, click Add Instances. Select the instances on which you want to run the job, and then click OK.

10. Click Next, and then on the Specify Variable Values tab, select one of the following options to specify variables for your instances:

   - **Upload input file for variables values:** Click Download Input Key File to download an input file. In the input file, enter values for the variables that you have defined in your commands, and then upload the file to the Citrix ADM server.

   - **Common variable values for all instances:** Enter values for the variables. The variables vary depending on the selected template.
The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

To view the executed configuration jobs while creating a configuration job, navigate to **Network > Configuration Jobs**, and click **Create Job**. In the **Create Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already executed configuration jobs while editing a configuration job, navigate to **Network > Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

11. Click **Next**, on the **Job Preview** tab, you can evaluate and verify the commands to be executed as a job.

12. Click **Next**, on the **Execute** tab, set the following conditions:
   - **On Command Failure**: What to do if a command fails: ignore the errors and continue the job, or stop further execution of the job. Choose an action from the drop-down list.
   - **Execution Mode**: Execute the job immediately, or schedule execution for a later time. If you schedule execution for a later time, you must specify the execution frequency settings for the job. Choose the schedule you want the job to follow from the **Execution Frequency** drop-down list.
13. Under **Execution Settings**, select to execute the job sequentially (one after the other), or in parallel (at the same time).

14. To have a job execution report emailed to a list of recipients, select the **Email** checkbox in the **Receive Execution Report Through** section. From the drop-down list that appears, choose an email distribution list. To create an email distribution list, click the + icon and enter the email addresses of the recipients, and email server details.

15. Click **Finish**.

**Use the master configuration template**

**August 1, 2019**

Using a master configuration template is a flexible option for creating and deploying a master configuration on multiple Citrix ADC instances.

As an administrator, you might want to make configuration changes and save licenses, certificates, and other files on the ADC instance. You can save the new configuration as a master configuration template (.conf file).

To save your master configuration template from a an ADC instance, you can do one of the following:

- At the command prompt, enter `save ns config`. The configuration is saved in the instance’s FLASH memory in the /nsconfig/ns.conf file.
- From the instance’s GUI, navigate to **Diagnostics > View Configuration**. Choose the kind of configuration you’d like to save. For example, if you want to save the saved configuration of your
instance, select **Saved configuration**. Click the **Save text to a file** link to save the ‘ns.conf’ file to your local machine.

When you deploy the master configuration template by using the ‘DeployMasterConfiguration’ configuration template while creating a new job, you can customize it further for each specific ADC instance by adding additional commands, modifying existing commands, and providing different variable values in the input file.

For example, as an administrator you may want to upload certificate keys to your ADC instances in addition ns.conf file and deploy the master configuration on them as well.

**Important**

You cannot execute a configuration job using the DeployMasterConfiguration template on Citrix ADC CPX instances, instances configured in a cluster, or on partitioned ADC instances.

**To create a configuration job using the Master Config configuration template on Citrix ADM:**

1. In Citrix ADM, navigate to **Networks > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, on the **Select Configuration** tab, specify the **Job Name** and select the **Instance Type** from the drop-down list.
3. Select **Master Configuration** from the **Configuration Source** drop-down list. Drag and drop the DeployMasterConfiguration template’s commands to the right pane. You can add, modify, or delete commands in the right pane as well. Click **Next**.

**Note**

You can add `put` commands to add input files to your template. In our example, we will need to upload certificate and key files in addition to the configuration template file and variable input files.

4. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
5. Do one of the following to view all the variables in a single consolidated view:
• While creating a configuration job, navigate to **Networks > Configuration Jobs**, select **Create Job**. On the **Create Job** page, you can review all the variables that you have added while creating the configuration job.

• While editing a configuration job, navigate to **Network > Configuration Jobs**, select the Job Name and click **Edit**. On the **Configure Job** page, you can review all the variables that were added while creating the configuration job.

6. You can then click on the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

7. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the **Done** button after you have edited or modified any of the parameters.

8. Select the instances on which you want to run the configuration job, and then click **Next**.

9. On the **Specify Variable Values** tab, upload the following:
   - **Configuration Template File (.conf)** - Upload the .conf file that you extracted from an ADC instance.
   - **Upload the Input File (.xml/csv)** - Upload the input file with values for the variables you have defined in your commands.
A sample xml file is provided here for your usage. Ensure that the xml files contain the details corresponding to the ADC instances that you are using.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<properties>
<!--
Provide inputs for all the parameters defined in the master config file.

- global. This tag contains all the common parameters and value.
- devicegroup. This tag contains all the instance group specific parameters and values.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence over the instance group. The instance group specific parameters value will take precedence over global parameters in the execution.

- name. This attribute represents the name of the instance group.
- device. This tag contains all the instance specific parameters and value.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence in the execution.

- name. This attribute represents the IP Address of the instance. Host name is not supported for the attribute.

HA pair should be represented as <primaryip>-<secondaryip>. Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within the dollar sign, Example: $NSIP$, $CC_Trap_Dest$ and parameters names are case sensitive.
-->
<global>
```
The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

To view the executed configuration jobs while creating a configuration job, navigate to Network > Configuration Jobs, and click Create Job. In the Create Job page. On the Specify Variable Values tab, select the Common Variable Values for all Instances option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already executed configuration jobs while editing a configuration job, navigate to Network > Configuration Jobs, select the Job Name and click Edit. In the Configure Job page, on the Specify Variable Values tab, select the Common Variable Values for all Instances option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

1. On the Job Preview tab, you can evaluate and verify the commands to be run on each instance.
or instance group, and then click **Next**.

2. **On the Execute** tab, you can choose to execute your job now or schedule it to be executed at a later time. You can also choose what action Citrix ADM should take if the command fails.

You can also choose to allow authorized users to execute jobs on your managed instances, and you can choose whether to send an email notification regarding the success or failure of the job, along with other details.
After executing your job, you can see the job details by navigating to Networks > Configuration Jobs and select the job you just configured. Click on Details and then, click on Execution Summary to see the details of your job. Click on the instance to see the Command Logs to see the commands executed on the job.

Use jobs to upgrade Citrix ADC instances

August 1, 2019

You can use Citrix Application Delivery Management (ADM) to upgrade one or more Citrix ADC instances. Before upgrading an instance, ensure you have uploaded the correct build and documentation files to the Citrix ADC instances. You must know the licensing framework and types of licenses...
before you upgrade an instance.

When you upgrade your Citrix ADC instance by creating a maintenance task, you can do the following:

- Perform a pre-validation check on the instances that are being upgraded. The pre-validation check consists of the following checks:
  1. Check for any existing customizations on Citrix ADC instances and delete the customizations. You can reapply all the customizations after the upgrade process is completed.
  2. Check the disk usage of Citrix ADC instances. If the disk usage is more than 80%, clean up the disk space.
  3. Check for disk hardware issues of Citrix ADC instances.

- Perform the Citrix ADC HA pair upgrade in two stages.
  1. Perform the upgrade task on a node immediately or you can even schedule that for later.
  2. Schedule the upgrade for the other node later. It must be scheduled after the initial node is upgraded.

When you upgrade a Citrix ADC HA pair, note the following:

- Currently, the second node of the HA pair is upgraded first, and then, the upgrade for the first node is scheduled to be done later.

- Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.

- After the upgrade of both nodes, you will see an error message in execution history (that indicates that HA Sync is not enabled) if your nodes in the HA pair are on different builds or versions.

To create a maintenance task to upgrade your Citrix ADC instance:

1. Navigate to Networks > Configuration Jobs > Maintenance Jobs.
2. In the Maintenance Jobs page, click Create Job.
3. In the Create Maintenance Job page, select Upgrade Citrix ADC/Upgrade Citrix ADC HA and click Proceed.
4. On one or more Upgrade Citrix ADC Appliance(s) page, in the **Instance Selection** tab, specify the **Job Name** and click **Add Instances**.

5. Select the target instances or instance groups that you want to upgrade.

   **Note**
   - To upgrade Citrix ADC instances in high availability mode, you have to select IP ad-
addresses of either the primary or secondary instances. However, always using the primary node for the upgrade is recommended.

- To upgrade Citrix ADC instances in cluster mode, select the cluster IP address.

6. After you have added the Citrix ADC instances or instance groups, click Next to start the pre-upgrade validation on the selected instances. The screen reports the progress of pre-validation of each of the Citrix ADC instances.

7. On the Upgrade Citrix ADC Appliance(s) page, select the Upgrade tab. From the Software Image drop-down menu, select either Local (your local machine) or Appliance (the build file must be present on Citrix ADM).

8. You can also see if any instances have pre-validation upgrade errors. These errors are shown in the form of message. The messages show the errors related to disk space, hard disk drive, and user customization.

If you do not want to proceed with instances that have failed the pre-validation upgrade check, you can remove the instances. To remove the instances, select the instances and click Delete.

1. Click Next.

Note

It is highly recommended to proceed the upgrade process, only if the pre-upgrade validation check passes for the Citrix ADC instances.

2. On the Schedule Task tab, you can also set execution details where you can perform the upgrade process now or schedule it for a later date.

3. You can enable email notification to receive the execution report of upgrading Citrix ADC instances. Click the Receive Execution Report Through Email checkbox to enable the email notification. To create an email distribution list:

   - Select the + icon to Create the Email Distribution List.

   - On the Create Email Distribution List page, specify a Name for the Email Distribution List. Add the SMTP mail server to use for sending email notifications to the Email Server. In the From box, add the Email address from which to send messages. In the To box, add Email address or addresses to which to send messages. You can also add an Email address or addresses to which to send message copies and copies without displaying these addresses in the messages or the copies. Click Create. After creating the email distribution list, click Finish to complete the configuring process.

4. On the Schedule Task tab, you can also perform the two-stage upgrade for nodes in HA. You can either perform the upgrade immediately or schedule a time for the nodes to be updated one after another. Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.
You can now use configuration commands that were previously saved as configuration templates to create Audit Templates that can be applied to specific NetScaler instances. While creating an audit...
template, you can drag and drop previously saved configuration templates into the Commands field, and edit the template to suit your requirements. You can then apply the audit template to specific NetScaler instances. Citrix ADM compares these instances with the audit template and reports any mismatch. This process helps you identify errors and rectify them in a timely manner.

You can create configuration templates while creating a new 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 example, consider a basic load balancing configuration for which you add a load balancing virtual server, add two services, and bind the services to the virtual server.

This example uses the following commands:

- `add lb vserver servername HTTP ipaddress portnumber`
- `add service servicename1 ipaddress1 HTTP 80`
- `add service servicename2 ipaddress2 HTTP 80`
- `bind lb vserver servername servicename1`
- `bind lb vserver servername servicename2`

To save a configuration template in Citrix ADM:

1. Navigate to Networks > Configuration Jobs, and click Create Job.
2. On the Create Job page, specify the job name and the instance type.
3. Choose Configuration Template as the Configuration Source and, in the Commands field, enter commands such as those in the above example.
4. Select the Save as Configuration Template checkbox and specify a name for your template. You can choose to overwrite other templates that exist with the same name.
5. Click Save.
To use a configuration template to create an audit template in Citrix ADM:

1. Navigate to **Networks > Configuration Audit > Audit Templates**, and click **Add**.

2. On the **Create Template** page, specify a name for the template name, and enter a description.

3. From the **Configuration Source** list, select **Configuration Template**, and then drag and drop the template into the Commands field in the right pane. You can also edit the configuration and save the template with a different name. Click **Next**.

4. On the **Select Instances** tab, click **Add Instances** and add the instances on which you want to run the configuration. Click **OK**.

5. Click **Finish**.
The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances.

**Use SCP (put) command in configuration jobs**

August 1, 2019

You can use the Configuration Jobs feature of Citrix ADM to create configuration jobs, send email notifications, and check execution logs of the jobs created. A job is a set of configuration commands that you can create and run on a single managed instance or on multiple managed instances. For example, you can use configuration jobs for device upgrades.

Configuration jobs in Citrix ADM use Secure Shell (SSH) commands to configure instances, and you can configure a configuration job to use secure copy (SCP) to securely transfer files. SCP is based on the SSH protocol. One of the SCP commands that you can include in a configuration job is the “put”
You can use the “put” command in configuration jobs to upload or transfer one or more files stored in a local directory on your system to Citrix ADM and then to a directory on the NetScaler instance or instances.

Note The file is uploaded to Citrix ADM and it is later copied (put) to the selected NetScaler instances. The uploaded file is stored in Citrix ADM and is deleted only when the job is deleted. This is necessary for jobs scheduled to execute at a later time.

The command has the following syntax:

```
put <local_filename> <remote_path/remote_filename>
```

where,

- `<local_filename>` is the name of the local file to be uploaded.
- `<remote_path / remote_filename>` is the path to a remote directory, and the name to assign to the file when it is copied to that directory.

While creating the configuration job, you can convert the local and remote file name parameters into variables. This lets you assign different files to these parameters for the same set of NetScaler instances every time you execute the job. Also, when you use a file at multiple places in a job and if you want to rename the file, you can redefine the variable instead of changing the file name at all places.

To use the put command to upload files in a configuration job:

1. Navigate to Networks > Configuration Jobs.
2. On the Jobs page, click Create Job.
3. On the Create Job page, enter the name of the job in the Job name field, and in the Configuration Editor pane, enter the “put” command.

   For example, if you want to create a configuration job that copies a SSL certificate file saved on your local system to multiple NetScaler instances, you can add a “put” command that uses a variable instead of the name of a particular file, and define the variable type as “file”.

```
put ssl-file /nsconfig/ssl-file
```

   In this example,
   - `ssl-file` - This is the name of the file that needs to be uploaded in the NetScaler instance.
   - `/nsconfig/ssl-file` - This is the destination folder on the instance where the ssl-file will be put after the execution of the task.

4. In the command that you just entered, select the file name that you want to convert to a variable, and then click Convert to Variable, as shown in the following figure.
5. Verify that the file name has been enclosed by dollar signs (indicating that it is now a variable), and then click the variable.

6. Specify the details of the variable, such as name, display name, and type.

7. From the **Type** drop-down list, select **File**. Click **Save**. Declaring the variable as a “File” type allows you to upload files to Citrix ADM.

8. Click **Next** and select the NetScaler instances to which to copy the files.

9. On the **Specify Variable Values** tab, select **Common Variables Values for all Instances** section, select the file from the local storage on your system, click **Upload** to upload the file to Citrix ADM, and click **Next**.
10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

11. On the **Execute** tab, you can execute the job now or schedule it to be executed at a later time. You can also choose what action Citrix ADM should take if the command fails. You can also create an Email notification to receive notification about the success or failure of the job, and other details. Click **Finish**.

12. You can see the job details by navigating to **Networks > Configuration Jobs**, and selecting the job that you just configured. Click **Details**, and then click **Variable Details** to list the variables added to your job.

---

**Reschedule jobs configured by using built in templates**

August 1, 2019
You can reschedule a job that you scheduled by using built-in templates in Citrix Application Delivery Management (ADM). For example, you can change the action that Citrix ADM must take if a command fails. If you had previously opted to ignore an error and continue, you can change it to roll back all successful commands if a command fails.

To reschedule a job that was configured by using built-in templates in Citrix ADM

1. In Citrix ADM, navigate to Networks > Configuration Jobs.
2. Select the job you want to edit, add or remove instances, specify variable values, and then change execution actions and settings.
3. Click Finish to reschedule the job.

Note
You can also select the job and click Execute Again to run the job without modifying any source, instance, and commands. This is useful when you have to run the same set of commands on same instances. Sometimes, the job may encounter a transient error from the server side, and you may have to run the job again.

Reuse configuration audit templates in configuration jobs

August 1, 2019

As an admin, you can now save configuration commands as a set of reusable configuration templates when you create a job and run a configuration audit. The configuration template created and saved in Configuration Jobs is available in Configuration Audit to create an audit template that can be applied to specific Citrix ADC instances. Similarly, the audit template created in Configuration Audit module is available in Configuration Jobs so that you can run the template as a configuration job. Any change made in the template is now visible in both Configuration Jobs and Configuration Audit modules.

Earlier the configuration job and configuration audit templates had to be created separately for the same configuration and saved as different files. This caused a duplication of effort in creating and maintaining the templates.

Citrix Application Delivery Management (ADM) allows you to save this template in the system so that the audit template is available in Configuration Jobs also. Now the audit templates can be used to create configuration jobs. This way the templates can be used interchangeably between configuration jobs and configuration audits.

For example, consider a basic load balancing configuration for which you add a load balancing virtual server, add two services, and bind the services to the virtual server.
This example uses the following commands:

```
1     add lb vserver servername HTTP ipaddress portnumber
2     add service servicename1 ipaddress1 HTTP 80
3     add service servicename2 ipaddress2 HTTP 80
4     bind lb vserver servername servicename1
5     bind lb vserver servername servicename2
```

Creating a Template in Configuration Audits and Reusing it in Configuration Jobs

Perform the following task to create a template on configuration audit module and reuse the same in configuration jobs module.

**To create an audit template:**

1. In Citrix ADM, navigate to **Networks > Configuration Audit > Audit Template**, and click **Add**.
2. On the **Create Template** page, specify the template name. You can also add more information about the template in the **Description** field.
3. In the **Commands** pane, enter commands from the example.
4. Select the **Save as Configuration Template** checkbox and specify a name for your template, for example, you can name this template as “LBVariablesTemplate.” You can choose to overwrite other templates that exist with the same name.
   
   **Note** The audit template name can be same as the configuration template name.
5. Click **Save** and click **Next**.
6. Click Next.

7. In Select Instances tab, select the Citrix ADC instances on which you want to run these configuration commands and click Finish. The new template is now visible in the list of audit templates.
8. When you want to run these configuration commands, navigate to Networks > Configuration Jobs, and click Create Job. The audit template that you created earlier is listed as a configuration template.

To reuse the audit template in configuration jobs:

1. Enter a name for the job and select the instance type, and drag and drop the template to the commands pane.

   While creating the configuration job, you can convert the local and remote file name parameters into variables. This lets you assign different files to these parameters for the same set of Citrix ADC instances every time you execute the job.

2. In the command that you entered, select the file name that you want to convert to a variable, and then click Convert to Variable.

3. In Select Instances tab, select the instances on which you want to run these commands.

---

**Audit Templates**

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBVariablesTemplate</td>
<td>Basic load balancing configuration to add a load balancing virtual server</td>
</tr>
<tr>
<td>config-template2</td>
<td>abc</td>
</tr>
<tr>
<td>abc</td>
<td></td>
</tr>
</tbody>
</table>
4. If you have specified any variables in the commands, in Specify Variable Values tab, select one of the following options to specify variables for your instances:

- Variable values from an input file - Download an input file to enter values for the variables that you have defined in your commands, and then upload the file to the Citrix ADM server.
- Common variable values for all instances – Specify the syslog server IP address and port.

5. In the Job Preview tab, you can evaluate and verify the commands to be run on each instance or instance group and click Next.

6. In the Execute tab, click Finish to run the configuration job. Now if you want to add another service to this load balancing server and bind the service to the server, you can edit the commands in the command page and save them.
7. Navigate to **Audit Templates** and click **Add**.

8. Drag and drop the "LBVariablesTemplate" template to the commands pane. You can see that the template has been updated with the new commands.

The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances. You can now create templates and reuse them between configuration jobs and configuration audit modules.

**Import and export configuration templates**

August 1, 2019

You can export the configuration templates from any Citrix Application Delivery Management (ADM). You can also import the file to the same or another Citrix ADM at any time in future. The configuration templates data (like configuration commands, variable definitions, and parameters) are not lost.

You can export the configuration templates to a .json file format and save it in the local folder. You can import configuration template .json files into Citrix ADM. This file might be new or the one that you have exported from the same or other Citrix ADM.

**To export the configuration templates:**
1. Navigate to **Networks > Configuration Jobs > Configuration Templates**.

2. Click on the **Add** button to create the configuration template.

3. On the **Create Configuration Template** page, specify the configuration template name, and choose the instance type. Under **Configuration Editor**, select configuration source as Configuration Template from the drop-down menu. You can drag and drop the existing configuration templates to the configuration editor. Click **Create**.

4. Navigate to **Networks > Configuration Jobs > Configuration Templates** to view the templates created in the list of Configuration Templates.
5. Select the newly created configuration template and click the Export button.

The corresponding configuration template gets downloaded on your local system in .json format.

To import the configuration templates:

1. Navigate to Networks > Configuration Jobs > Configuration Templates and click the Import button. Select the path where you have the .json files of the configuration template and upload the .json files. It is highly recommended to upload the .json files that you have exported already.

2. You can also import the configuration template using File option on Configuration Editor.

3. Select File from the drop-down menu in the Configuration Editor.

4. Select Choose File (.json files) from your local system and upload the configuration template .json files.
Every new imported template is stored with a new id string.

You can import the configuration templates only if the file is saved in the .json format. If you import the configuration templates other than .json files, from your local system, it shows an error and fails the import of the files.

Maintenance jobs

August 1, 2019

You can create the following maintenance jobs using Citrix ADM. You can then schedule the maintenance jobs at a specific date and time.

- Upgrade Citrix ADC instances
- Upgrade Citrix SD WAN-WO instances
- Upgrade Citrix ADC SDX instances
- Configure HA pair of Citrix ADC instances
- Convert HA pair of instances to 2-node Cluster

Schedule upgrading of Citrix ADC instances

1. Navigate to Networks > Configuration Jobs > Maintenance Jobs. Click Create Job button.
2. On the Create Maintenance Task page, select Upgrade Citrix ADC/Upgrade Citrix ADC HA and click Proceed.
Create Maintenance Job

Select a task to create Maintenance Job*

- Upgrade Citrix ADC/Upgrade Citrix ADC HA
- Upgrade Citrix SD-WAN WO
- Upgrade Citrix ADC SDX
- Configure HA Pair of Citrix ADC Instances
- Convert HA Pair of Instances to 2 Node Cluster

Proceed  Close

3. On the Upgrade Citrix ADC Appliance(s) page, in the **Instance Selection** tab, add the Citrix ADC instances on which you want to run the upgrade process. Click **Next** to start the pre-upgrade validation on the selected instances.
4. On the **Upgrade** tab, 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).

5. You can enable email notification to receive the execution report of upgrading Citrix ADC instances. Click the **Receive Execution Report Through Email** checkbox to enable the email notification.

6. Select the + icon to Create the Email Distribution List.

7. To upgrade Citrix ADC instance now, select **Now** from the Execution Mode list.

8. To upgrade Citrix ADC instance at a later time, select **Later** from the Execution Mode list. You can then choose the Execution Date and the Start Time for upgrading the Citrix ADC instances.
9. On the **Create Email Distribution List** page, specify a name for the Email Distribution List. Add the SMTP mail server to use for sending email notifications to the Email Server. In the **From** box, add the Email address from which to send messages. In the **To** box, add Email address or addresses to which to send messages. You can also add an Email address or addresses to which to send message copies and copies without displaying these addresses in the messages or the copies. Click Create. After creating the email distribution list, click **Finish** to complete the configuring process.
Schedule upgrading of Citrix SD-WAN WO instances

1. In Citrix ADM, navigate to Networks > Configuration Jobs > Maintenance Jobs. Click Create Job button.

2. On the Create Maintenance Job page, select Upgrade Citrix SD-WAN WO and click Proceed.
3. On the **Upgrade Citrix SD-WAN WO** page, in the **Instance Selection** tab, add a **Task Name**. From the Software Image list, select either Local (your local machine) or Appliance (the build file must be present on the Citrix MAS virtual appliance). Add the Citrix SD-WAN WO instances on which you want to run the upgrade process. Click **Next**.

4. To upgrade Citrix SD-WAN WO instance now, select **Now** from the **Execution Mode** list. Click **Finish**.

5. To upgrade Citrix SD-WAN WO instance at a later time, select **Later** from the **Execution Mode** list. You can then choose the execution date and the start time for upgrading the Citrix SD-WAN WO instance.

6. You can enable email notification to receive the execution report of upgrading Citrix SD-WAN WO instance. Click the **Receive Execution Report Through Email** checkbox to enable the email notification.

7. Select the + icon to create the email distribution list.

8. On the **Create Email Distribution List** page, specify a name for the email distribution list. Add the SMTP mail server to use for sending email notifications to the email server. In the **From** box, add the Email address from which to send messages. In the **To** box, add email address or addresses to which to send messages. You can also add an email address or addresses to
which to send message copies and copies without displaying these addresses in the messages or the copies. Click Create. After creating the email distribution list, click Finish to complete the configuring process.

**Schedule upgrading of Citrix ADC SDX instances**

1. In Citrix ADM, navigate to Networks > Configuration Jobs > Maintenance Jobs. Click Create Job button.
2. On the Create Maintenance Job page, select Upgrade Citrix ADC SDX and click Proceed.
3. On the Upgrade Citrix ADC SDX appliance(s) page, in the Instance Selection tab, add a Task Name. 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). Add the Citrix ADC SDX instances on which you want to run the upgrade process. Click Next.
4. You can enable email notification to receive the execution report of upgrading Citrix ADC SDX instance. Click the Receive Execution Report Through Email checkbox to enable the email notification.
5. Select the + icon to create the email distribution list.
6. To upgrade Citrix ADC SDX instance now, select Now from the Execution Mode list. Click Finish.
7. To upgrade Citrix ADC SDX instance at a later time, select Later from the Execution Mode list. You can then choose the execution date and the start time for upgrading the Citrix ADC SDX instance.
8. On the Create Email Distribution List page, specify a name for the email distribution list. Add the SMTP mail server to use for sending email notifications to the email server. In the From box, add the Email address from which to send messages. In the To box, add email address or addresses to which to send messages. You can also add an email address or addresses to
which to send message copies and copies without displaying these addresses in the messages or the copies. Click Create. After creating the email distribution list, click Finish to complete the configuring process.

**Schedule configuring HA pair of Citrix ADC Instances**

1. Navigate to Networks > Configuration Jobs > Maintenance Jobs. Click Create Job button.
2. On the Create Maintenance Job page, select Configure HA Pair of Citrix ADC Instances and click Proceed.
3. On the Citrix ADC HA Pair page, in the Instance Selection tab, add a Task Name. Enter the primary IP address and the secondary address and Click Next.
4. On the Schedule Task tab, you can either choose to configure the Citrix ADC HA pair now or later.
5. To configure the Citrix ADC HA pair now, select **Now** from the **Execution Mode** list. You can enable email notification to receive the execution report of Citrix ADC HA pair. Click the **Receive Execution Report Through Email** checkbox to enable the email notification.

6. To configure the Citrix ADC HA pair at a later time, select **Later** from the **Execution Mode** list. You can then choose the execution date and the start time. You can enable email notification to receive the execution report of Citrix ADC HA pair. Click the **Receive Execution Report Through Email** checkbox to enable the email notification.

7. Select the + icon to create the email distribution list.

8. On the **Create Email Distribution List** page, specify a **Name** for the email distribution list. Add the SMTP mail server to use for sending email notifications to the email server. In the **From** box, add the email address from which to send messages. In the **To** box, add email address or addresses to which to send messages. You can also add an email address or addresses to which to send message copies and copies without displaying these addresses in the messages or the copies. Click **Create**. After creating the email distribution list, click **Finish** to complete the configuring process.

**Schedule converting HA pair of instances to Cluster**

1. Navigate to **Networks > Configuration Jobs > Maintenance Jobs**. Click **Create Job** button.

2. On the **Create Maintenance Job** page, select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.

3. On the **Migrate Citrix ADC HA to Cluster** page, in the **Instance Selection** tab, add a **Task Name**. Specify the primary IP address, secondary address, primary node ID, secondary node ID, cluster IP address, cluster ID, and backplane. Click **Next**.
4. On the **Schedule Task** tab, you can either choose to migrate the Citrix ADC HA to Cluster now or later.

5. To configure the Citrix ADC HA pair at a later time, select **Later** from the **Execution Mode** list. You can then choose the execution date and the start time. You can enable email notification to receive the execution report of Citrix ADC HA pair. Click the **Receive Execution Report Through Email** checkbox to enable the email notification.

6. Select the + icon to create the email distribution list.

7. On the **Create Email Distribution List** page, specify a name for the email distribution list. Add the SMTP mail server to use for sending email notifications to the email server. In the From box, add the email address from which to send messages. In the To box, add email address or addresses to which to send messages. You can also add an email address or addresses to which to send message copies and copies without displaying these addresses in the messages or the copies. Click Create. After creating the email distribution list, click **Finish** to complete the configuring process.
Configuration audit

August 1, 2019

This document includes:

- Creating Audit Templates
- Viewing Audit Reports
- Audit Configuration Changes Across Instances
- Get Configuration Advice on Network Configuration
- How to Poll Configuration Audit of NetScaler Instances

Create audit templates

August 1, 2019

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed Citrix Application Delivery Controller (ADC) instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown. You can create audit templates with specific configurations you want to audit on certain instances. Citrix Application Delivery Management (Citrix ADM) compares these instances with the audit template and reports if there is a mismatch in the configuration. Whenever there is a configuration mismatch, Citrix ADM generates a configuration diff report, which enables you to troubleshoot, and rectify unwanted configuration changes.

You can automate the running of the audit template by

- Scheduling the time at which the template should be run
- Setting the frequency at which Citrix ADM should run the template. You can run the template daily, on a specific day in a week, or on a specific date in a month.

Also, you have an option to send the diff report generated by Citrix ADM to specified email addresses that you can configure. By this option, your user can receive the report as a mail attachment and there is no need for the user to log on to Citrix ADM to export the reports manually.

To create audit templates:

1. Navigate to Networks > Configuration Audit > Audit Templates, and click Add.
2. On the Create Template page, and in the Audit Commands tab, specify the template name and its description.
3. In the **Configuration Editor** page, type in your commands and save the commands as a configuration template. You can also drag an existing template from the left pane to the editor.

4. Select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server "ipaddress1," and click **Convert to Variable**. The variable is now enclosed with "$" as shown in the image below.

In the **Define Variable** window, set the properties for this variable - name, display name, and the type of the variable. Click the **Advanced** option if you want to further specify a default value for your variable.
You can also save the commands as a configuration template.

5. Click **Save** and then, click **Next**.

6. In the **Select Instances** tab, select the instances you want to run the configuration audit on and click **Next**.
7. 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

8. Click **Next**.

9. In the **Template Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group. Click **Next**.
10. In the **Schedule Template** tab, you have the following options to schedule the running of the template and configuring the mail address to send the diff report.

   - **Use global polling interval.** Select this option to run the template on the instances at a time configured globally on Citrix ADM.

     **Note**

     To configure global polling interval in Citrix ADM, navigate to **Networks > Configuration Audit > Audit Templates**, and click **Global Polling Interval**. In the **Poll Interval** field, enter the minutes at which Citrix ADM should globally poll the instances.

   - **Customize template schedule.** Use this option to configure the time and the frequency at which the templates need to be run

   - **Send report through email.** Use this option to configure the mail profile to which the diff report should be sent as a mail attachment.

11. Click **Finish**.
The audit template appears in the **Audit Templates** list and is run at the scheduled time against the configurations in the specified instances.

**View audit reports**

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) allows you to view and download the configuration audit diff report in configuration audit section. The configuration audit section enables you to export the summary report across all instances and per instance, and also allows you to export granular diff report for each instance-template pair.

The audit templates that appear in the Audit Templates list are run at the scheduled time against the configurations in the specified instances. The **NetScaler Config Drift** chart on the **Configuration Audit** dashboard displays high-level details about configuration changes in saved against unsaved configurations. When you click **NetScaler Config Drift** chart, the ensuing **Audit Reports** page displays a list of instances that shows both “Diff Exists” and No Diff.” You can download the diff reports displayed by Citrix ADM.

Citrix ADM also provides an option to schedule automatic export of diff report as a mail attachment. For more information on how to schedule export of reports, see **Creating Audit Templates**.

**To export configuration audit reports:**

1. In Citrix ADM, navigate to Networks > Configuration Audit.
2. On the **Configuration Audit** page, click inside the **NetScaler Config Drift** chart.

3. The **Audit Reports** page lists instances that have a difference. The page also displays a list of instances that does not have any difference in their running configurations.

In the image you can see that for some instances a diff is present only in **Saved Vs Running Diff** and for some instances, a diff is present only in **Template vs Running Diff**. For some instances, differences exist in both **Saved Vs Running Diff** and **Template vs Running Diff**.

### Saved Vs Running Diff

You can view a report of the diff between the configuration saved on the instance and the configuration currently running on that instance. For example, click **Diff Exists** for an instance under **Saved Vs Running Diff**.

Here, you can see a report for saved configuration against running configuration diff for that instance.

Click **Export diff report** to download a .csv file of the diff report. You can also click Export corrective commands to export the commands to a .txt file. You can then run the commands on the associated Citrix ADM instance from configuration jobs to correct the configuration in that instance.
Template vs Running Diff

The Template vs Running Diff includes all templates other than Saved Vs Running Diff which is the default template. You can view the difference that exists between the template and running configuration. For example, click Diff Exists for one of the instances under Template vs Running Diff.

Now you can see that two templates show diff and the Citrix ADM instance has a different configuration from what the template is looking for.

Click Diff Exists again. The following image shows the configuration that the template is looking for and the running configuration that is blank, because no such commands has been configured or has been removed. You can also see the correction configurations or the commands to run to correct the configuration.

Click Export diff report to download a .csv file of the diff report. You can also click Export corrective commands to export the commands to a .txt file. You can then run the commands in CLI to correct the configuration in that instance.

The following image shows an example .csv diff file that is downloaded to your system:
Audit configuration changes across instances

August 1, 2019

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed Citrix Application Delivery Controller (ADC) instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown. You can create audit templates with specific configurations you want running on certain instances. The Citrix Application Delivery Management (Citrix ADM) compares these instances with the audit template and reports if there is a mismatch in configuration. This enables you to troubleshoot and rectify the errors.

You can automate the running of the audit template by scheduling the time at which the template should be run. You can also set the frequency at which Citrix ADM should run the template. You can run the template daily, on a specific day in a week, or on a specific date in a month. You also have the option to send the diff report generated by Citrix ADM to specified email addresses that you can configure. By this option, your user receives the report as a mail attachment and there is no need for the user to log on to Citrix ADM to check the reports manually.

To create audit templates:

1. Navigate to **Networks > Configuration Audit > Audit Templates**, and click **Add**.
2. On the **Create Template** page, and in the **Audit Commands** tab, specify the template name and its description.
3. In the **Configuration Editor**, type in your commands and save the commands as a configuration template. You can also drag and drop an existing template from the left pane on the editor.
4. Select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server "ipaddress," and click **Convert to Variable** as shown in the image below.
Click the **Advanced** option if you want to further specify a default value for your variable.

You can also save the commands as a configuration template.

5. Click **Save** and then, click **Next**.

6. In the **Select Instances** tab, select the instances you want to run the configuration audit on.

7. 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

8. Click **Next**.
9. In the **Template Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group. Click **Next**.

10. In the **Schedule Template** tab, you have three options to automate the running of the template and the mail address to send the diff report.

   - **Use global polling interval.** Select this option to run the template on the instances at a time configured globally on Citrix ADM
   - **Customize template schedule.** Use this option to configure the time and the frequency at which the templates need to be run
   - **Send report through email.** use this option to configure the mail profile to which the diff report should be sent as a mail attachment.

11. Click **Finish**.
The audit template appears in the Audit Templates list and is run at the scheduled time against the configurations in the specified instances.

**Viewing Details of Configuration Changes**

You can also use the Configuration Audit dashboard to view high-level details about configuration changes such as the top ten instances by configuration change or the number of saved and unsaved configurations.

Citrix ADM also allows you to poll configuration audits manually and adds all the configuration audits of the instances immediately to the Citrix ADM. To do so, navigate to Networks > Configuration Audit,
click **Poll Now**, the pop-up page *Poll Now* provides you an option to poll all Citrix ADC instances in the network, or poll the selected instances.

You can also force an audit on an instance. To do so, click the **NetScaler Config Saved Status** chart or **NetScaler Config Drift** chart. On the *Audit Reports* page, select the instance and, in the *Action* list, select *Poll Now*.

### To set configuration audit notifications:

1. Navigate to *Networks > Configuration Audit*.
2. On the *Configuration Audit* page, click *Settings*.
3. On the *Notification Settings* page, click the *Edit* icon, to enable the notification settings.
4. Select the *Enabled* check box and then, choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the + icon and specifying email server details.

### Get configuration advice on network configuration

August 1, 2019

You set up your Citrix Application Delivery Controller (ADC) instances with optimal configurations so that you can achieve optimal performance on your applications. However, it may happen that some configurations might not be standard configurations and this might affect the performance of your applications.

To help you optimize your application performance, Citrix Application Delivery Management (Citrix ADM) analyzes the Citrix ADC instance configuration and provides you with recommendations. You can apply the recommended configurations from Citrix ADM.

### To analyze the Citrix ADC instance:

1. Navigate to *Networks > Configuration Audit > Configuration Advice*.
2. Do one of the following:
   - Click **Upload Configuration File** and upload the configuration file of your network instance.
   - Click **Select Device** and select the Citrix ADC instance that you want to analyze.
Citrix ADM analyzes the configuration on your instance and provides a list of configuration recommendations as shown in the image below. Click the check box next to a configuration advice to view the corrective commands.

If you want to update your configuration, specify the values for the variables in the corrective commands and click **Apply Now** as shown in the image below.

**Note**

The commands listed here are only recommendations. A user with read and write access might be able to edit any command using this feature. Ensure that you grant a limited privileged access to users whom you think should not edit the commands.

When the command is successfully run on the network instance, the check box next to the advice disappears.
If you want to view the details of the commands run on your network instance, navigate to **Networks > Instances > `<Instance_Type>`**, select the IP address of the instance, and then click **Events** from the **Actions** drop-down list.

On the **Events** page, you can view the details of the configuration change.

### Poll configuration audit of Citrix ADC instances

**August 1, 2019**

Citrix Application Delivery Management (Citrix ADM) automatically polls the configuration audits every 10 hours to look for configuration changes that occur on Citrix Application Delivery Controller (ADC) instances. You can also manually poll the configuration audits to discover recent changes, but polling all the Citrix ADC instances configuration places a heavy load on the network.

Instead of polling the entire Citrix ADC instances configuration audit, you can manually poll only the configuration audits of a selected instance or instances.

**To poll configuration audits of Citrix ADC instances:**
1. In Citrix ADM, navigate to **Networks > Configuration Audit**.

2. On **Configuration Audit** 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.
   a) To poll all Citrix ADC instances, select the **All Instances** tab and click **Start Polling**.
   
   ![Poll Now all instances](image1.png)
   
   ![Poll Now start polling](image2.png)
   
   b) To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.
   
   ![Poll Now select instances](image3.png)
Generate configuration audit diff for ConfigChange SNMP Traps

August 1, 2019

Whenever there is a configuration change in a Citrix Application Delivery Controller (ADC) instance in the network, the configuration file is updated. The instance sends a ConfigChange SNMP trap to Citrix Application Delivery Management (Citrix ADM). You can enable Citrix ADM to perform a configuration audit on that instance when the instance sends a ConfigChange SNMP trap.

If any difference exists between the audit template configuration and the running configuration, a Diff Exists status message appears on the Audit Report page. Clicking the Diff Exits link takes you to the Configuration Diff page, where you can view the corrective command. You can use these corrective commands to create a configuration job and execute that on the specific Citrix ADC instances. When you run the configuration job, the instances are brought back to the desired configuration. For more information on how to create configuration job from corrective commands, see How to Create Configuration Jobs from Corrective Commands on Citrix ADM.

To run configuration audit templates on receiving ConfigChange SNMP trap:

Citrix ADM allows you to enable the option to run the configuration audit template in Citrix ADM.

1. In Citrix ADM, navigate to Networks > Configuration Audit.
2. Click Settings on the Configuration Audit page.
3. Click the edit icon in the Configuration Change Audit Settings section.
4. Select the Do Configuration Audit when netScalerConfigChange event is received check box.

Note
This is a global setting for all instances. Citrix ADM performs a configuration audit for every instance that it receives the netScalerConfigChange SNMP traps in the future.

1. In the Time delay to run the Audit Template (in minutes) field, type the minutes. Citrix ADM runs the configuration audit template on the Citrix ADC instance after this time delay when it receives the ConfigChange SNMP trap by that instance.

Network functions

August 1, 2019

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix Application Delivery Controller (ADC) instances. You can view statistics such as trans-
action details, connection details, and throughput of a load balancing virtual server. You can also enable or disable the entities when you plan a maintenance.

The Network Functions dashboard provides you with the following graphs:

- Top 5 virtual servers with highest client connections
- Top 5 virtual servers with highest server connections
- Top 5 virtual servers with maximum throughput (MB/sec)
- Bottom 5 virtual servers with lowest throughput (MB/sec)
- Top 5 instances with most virtual servers
- State of the virtual servers
- Health of the load balancing virtual servers
- Protocols

**Generate reports for load balancing entities**

August 1, 2019

Citrix Application Delivery Management (ADM) allows you to view the reports of Citrix Application Delivery Controller (ADC) instance entities at all levels. There are two types of reports that you can download in 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.

![Example of a summarized report](image)

The consolidated report is in a CSV format. The entries in each column are described as follows:
- **NetScaler IP Address**: IP address of the Citrix ADC instance is displayed in the report.
- **NetScaler HostName**: Host name is displayed in the report.
- **Partition**: IP address of the administrative partition is displayed.
- **Virtual Server**: `<name_of_the_virtual_server>#virtual_IP_address:port_number`
- **Services**: `<name_of_the_service>#service-IP_address:port_number`
- **Service Groups**: `<name_of_service_group>#server_member1_IP_address:port,server_member2_IP_address:port,server_member3_IP_address:port,………..,server_membern_IP_address:port`

**Note**
- If there is no host name available, the corresponding IP address is displayed.
- Blank columns indicate that the respective entities are not configured for that 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 **Networks > Network Functions > Load Balancing**.
2. On **Load Balancing** page, click .
3. On the **Export** page that opens, you have two options to view the report:
   a) Select **Export Now** tab and click **OK**. The consolidated report downloads to your system.
   b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.
      i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.
      ii. **Recurrence time** - Enter the time as Hour:Minute in 24-hour format.
      iii. **Email Profile** - Select a profile from the drop-down list box, or click + to create an email profile.
Note

If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.

Note

If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.
Generate an individual load balancing entity report

You can generate and export an individual report for a particular type of entity associated with the instances. For example, consider a scenario where you want to see a list of all load balancing services in the network.

1. In Citrix ADM, navigate to Networks > Network Functions > Load Balancing > Services.
2. On Services page, click the Export button at the top right-hand corner.
a) Select **Export Now** tab if you want to generate and view the report at this instant.

b) Select **Schedule Export** to schedule generating and exporting of the report at regular intervals.

**Note**

You can only download the reports or export the reports as mail attachments. You cannot view the reports on the Citrix ADM GUI.

**Export or schedule export of network functions reports**

August 1, 2019

You can generate a comprehensive report for selected network functions such as Load Balancing, Content Switching, Cache Redirection, Global Server Load Balancing (GSLB), Authentication, and Citrix Gateway in Citrix Application Delivery Management (ADM). This report allows you to have a high-level view of mapping between the Citrix ADC instances, partitions, and the corresponding bound entities (virtual servers, service groups, and services) that are present in the network. You can export these reports in .csv file format.

The report displays the following virtual server data:

- NetScaler IP address
- Host name
- Partition data
- Virtual Server name
- Type of virtual server
- Virtual server
- Target LB virtual server

**Note**

For Content Switching and Cache Redirection virtual servers, the Target LB virtual server column lists all the LB servers, that is, both default servers and policy-based servers.

- Service name
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.
- You cannot generate a network functions report for HAProxy.

**To export and schedule network functions reports:**

1. Navigate to Networks > 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.
b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

   i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.
   
   ii. **Recurrence time** - Enter the time as Hour: Minute in 24-hour format.
   
   iii. **Email Profile** - Select a profile from the drop-down list box, or click + to create an email profile.

Click **Enable Schedule** to schedule your report and then, click **OK**. By clicking the **Enable Schedule** checkbox, you can generate the selected reports.
You can optimize resource usage by monitoring your network reporting on Citrix Application Delivery Management (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 (ADC) instances to load balance, content switch, or compress the traffic. Network performance can impact the application performance. To continue to maintain performance of your applications, you must regularly monitor your network performance and make sure all resources are used optimally.

Citrix ADM now allows you to generate reports not only for instances at a global level but also for entities such as the virtual servers and network interfaces. The instance family comprises both Citrix ADC and SD-WAN instances. The virtual servers for which you can generate reports are as follows:

- Load balancing servers
• Content switching servers
• Cache redirection
• Global service load balancing (GSLB)
• Authentication
• Citrix Gateway

The network reporting dashboard in Citrix ADM is a highly customizable. You can now create multiple dashboards for various instances, virtual servers, and other entities.

**Network reporting dashboard**

The following image calls out the various features in the dashboard:

- The left side panel lists all the custom dashboards that are created in Citrix ADM. You can click on 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 a variety of 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.
Citrix Application Delivery Management 12.1

• You can remove a report by clicking “X”. You can also export the report as a .pdf, .jpeg, .png, or .csv format to your system. You can also schedule a time and recurrence of when the report should be generated. You can also configure an email distribution list to which the reports should be sent.

• The Instances section at the top of the dashboard lists the IP addresses of all the instances for which the report is generated.

• You can either remove instances by clicking “X” or add more instances to the reports. But, currently Citrix ADM allows you to view reports for ten 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 **Networks > Network Reporting**.
2. In the Select Reports tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click Next.

3. To view the existing dashboards, click View Dashboard. The Network Reporting Dashboard page opens where you can view all your dashboards and report widgets.

4. To create a dashboard, click Create Dashboard.

5. The Create Dashboard page opens.

6. 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 SD-WAN
   c) Type. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.
   d) Description. Type a meaningful description for the dashboard.
e) Click **Next**.

7. In the **Select Entities** tab, click **Add**.

8. In the **Choose LB Virtual Servers** window that slides in, select any number of virtual servers that you want to monitor.

   ![Choose LB Virtual Servers](image)

   **Note**

   Depending on the entity type that you have selected in Basic Settings tab, the Entities tab is populated with corresponding entities. For example, if you select global, you can add instances.

9. Click **Create**.

   The **TCP and SSL** dashboard is created and displays all the reports that you have selected.

   **Note**

   Currently, any changes that you make to legends or filters cannot be saved.
Exporting network reports

While you can export widget reports in .pdf, .png, .jpeg, or .csv formats, you can export the entire dashboards in only .pdf, .jpeg, or .png formats.

Note

You cannot export reports in 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 Networks > 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.

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 will have 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 dashboard reports:

1. Navigate to Networks > 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**. **

   ![Network Reporting Dashboard](image)

To export widget reports:

1. Navigate to **Networks** > **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 **TCP and SSL**.

4. Select a widget. For example, select **Front-end RSA vs. DH Key Exchange**.

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 Networks > 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 Networks > Network Reporting > Thresholds. Under Thresholds, click Add.

   1. On the Create Threshold page, specify the following details:
      
      • Threshold Name. Name of the threshold.
      
      • Instance Type. Choose Citrix ADC or Citrix SD-WAN WO.
      
      • Report Name. Name of the performance report that provides information about this threshold.

   2. 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 Networks > 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.

   3. Choose the IP address of the instance or instances for which you want set the threshold.

   4. You can additionally 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.
5. Select **Enable** to enable the threshold to generate alarms.

6. Optionally, you can configure **Actions** such as email and/or SMS notifications.

7. Click **Create**.

**Set Performance Polling Interval for Network Reports**

By default, every 5 minutes, NITRO calls collect performance data for network reporting. This retrieves instance statistics such as counter information and aggregates them on the basis of 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 **Networks > Network Reporting and click Configure Polling Interval**. Your polling interval cannot be less than 5 minutes or more than 60 minutes.

![Welcome to Network Reporting](Image)

**Configure Polling Interval**

![Configure Polling Interval](Image)

**Configuring Network Reporting Prune Settings**

You can configure the purge interval of network reporting data in Citrix ADM. This limits the amount of network reporting data being stored in the Citrix ADM server’s database. By default, pruning happens every 24 hours (at 01.00 hours) for the network reporting historical data.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Note
The value you can specify cannot exceed 90 days or be less than 1 days.

To configure network reporting prune settings:


2. In the Configure Network Reporting Prune Settings page, specify the number of days for which to retain data, and click OK.

All the network reporting performance data are persisted in the Citrix ADM database for the number of days selected.
Analytics

August 1, 2019

Citrix ADM Analytics feature provides an easy and scalable way to look into various Citrix ADC insights to analyze and improve application performance. You can use one or more analytics features simultaneously on Citrix ADM.

The following table describes various analytics features that are supported on Citrix ADM:

<table>
<thead>
<tr>
<th>Analytics Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Insight</td>
<td>Web Insight enables visibility into enterprise web applications and allows you to monitor all web applications in Citrix ADC. As an administrator, you can see integrated and real-time monitoring of applications.</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>HDX Insight provides end-to-end visibility for ICA traffic passing through Citrix ADC. HDX Insight enables you to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues.</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>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.</td>
</tr>
<tr>
<td>Security Insight</td>
<td>Security Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.</td>
</tr>
<tr>
<td>SSL Insight</td>
<td>SSL Insight provides visibility into secure web transactions (HTTPS) and allows you to monitor all the secure web applications in Citrix ADC. As an administrator, you can see integrated and real-time, and historic monitoring of secure web transactions.</td>
</tr>
</tbody>
</table>
TCP Insight provides an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in Citrix ADC instances to avoid network congestion in data transmission.

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.

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

License requirements

August 1, 2019

The licensing requirements needed on the Citrix ADC instances to view the various analytics reports on Citrix Application Delivery Management (ADM) are described in the following table:

<table>
<thead>
<tr>
<th>Citrix ADM Analytics Features</th>
<th>Citrix ADC license Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Insight</td>
<td>Web Insight report on Citrix ADM is supported on all Citrix ADC license editions (Standard/Enterprise/Platinum).</td>
</tr>
<tr>
<td>Citrix ADM Analytics Features</td>
<td>Citrix ADC license Requirement</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>HDX Insight report on Citrix ADM is supported on any of the following Citrix ADC licenses: Enterprise Edition (for reporting &lt; 1 hour) or Platinum Edition (for unlimited reporting). <strong>Note</strong> Standard license edition is not supported.</td>
</tr>
<tr>
<td>Security Insight</td>
<td>Security Insight report on Citrix ADM is supported on all Citrix ADC license editions (Standard/Enterprise/Platinum). Platinum Edition or Enterprise Edition with App Firewall license. <strong>Note</strong> Standard license edition and Standalone App Firewall license is not supported.</td>
</tr>
<tr>
<td>SSL Insight</td>
<td>SSL Insight report on Citrix ADM is supported on all Citrix ADC license editions (Standard/Enterprise/Platinum).</td>
</tr>
<tr>
<td>Gateway Insight</td>
<td>Gateway Insight report on Citrix ADM is supported on any of the following Citrix ADC licenses: Enterprise Edition (for reporting &lt; 1 hour) or Platinum Edition (for unlimited reporting). <strong>Note</strong> Standard license edition is not supported.</td>
</tr>
<tr>
<td>TCP Insight</td>
<td>TCP Insight report is supported on all Citrix ADC license editions (Standard/Enterprise/Platinum).</td>
</tr>
<tr>
<td>Video Insight</td>
<td>Video Insight report on Citrix ADM is supported on Citrix ADC Premium (VPX-T 1000 series, VPX-T) edition.</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>WAN Insight report on Citrix ADM is supported on Citrix SD-WAN WO Edition (WAN Optimization Edition).</td>
</tr>
</tbody>
</table>

**Logstream overview**

August 8, 2019
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 an 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 should 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 or earlier, then ensure you have installed Citrix ADM 12.1 Build 50.39.

**To use Logstream as the communication mode while enabling analytics on Citrix ADM:**

1. Navigate to **Networks > Instances > Citrix ADC**, and select the Citrix ADC instance on which you want to enable analytics.

2. From the **Select Action** list, select **Configure Analytics**.

3. On the **Configure Insight** page:
a) Select the **Application List** for either Load Balancing or Content Switching.

b) Select the virtual server and click **Enable AppFlow**.

4. In the Enable AppFlow dialog box:
   - Enter **true** in the text box
   - Select **Logstream** as the transport mode

   **Note**
   Citrix recommends you to select Logstream as the transport mode.
   - Select the insight type and 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>
<tr>
<td>SSL Insight</td>
<td>Not supported</td>
<td>•</td>
</tr>
<tr>
<td>CR Insight</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IP Reputation</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>AppFirewall</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Client Side Measurement</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Syslog/Auditlog</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
Disable URL data collection

August 1, 2019

You can disable URL data collection if you do not want URL reports to be displayed on the Web Insight node of the dashboard in Citrix Application Delivery Management (ADM).

To disable URL data collection from Citrix ADM

1. In Citrix ADM, navigate to Analytics > Settings, and then click Configure Analytics Data Record Logs.
2. In the Web Insight URL Data Collection Settings section, if the Enable URL Data Collection option is checked, clear the check box.
3. Click OK.

Create thresholds and alerts

August 1, 2019

You can set thresholds and alerts to monitor the state of a Citrix ADC instance. You can set thresholds on counters and monitor instances and entities on managed instances.
When the value of a counter exceeds the threshold, Citrix Application Delivery Management (ADM) generates an event to signify a performance-related issue. When the counter value matches the clear value specified in the threshold, the event is cleared, which means that the particular threshold has returned to its normal state.

You can also associate an action with the threshold. Actions include sending an alert, email, or SMS notification. When the threshold is breached, Citrix ADM performs the action you define is taken automatically like enabling an alert and sending an email or SMS notification.

To create a threshold and alert using Citrix ADM

1. In Citrix ADM, navigate to Analytics > Settings > Thresholds. Under Thresholds, click Add.
2. On the Create Thresholds page, specify the following details:
   - **Name** – Name for configuring the threshold.
   - **Traffic Type** – Type of traffic for which you want to configure the threshold.
   - **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.
   - **Configure Rule** – Rule for the metric for which you want to configure the threshold.
   - **Notification Settings** - Enable threshold and receive notifications through various channels like email, slack, or sms when threshold exceeds.
3. Click Create.

For HDX insight, you can also set multiple thresholds for which an alert is generated only if all the entities in the configured threshold are breached.

Configure adaptive thresholds

August 1, 2019

The adaptive threshold functionality sets the threshold value for the maximum number of hits on each URL. If the maximum number of hits on a URL is greater than the threshold value set for the URL, a syslog message is sent to an external syslog server. The threshold value interval can be in either days or weeks.

The threshold value is calculated as follows:
Threshold value = Max hits * Threshold multiplier

Where:

- Max hits is the maximum number of hits on a URL.
- Threshold multiplier is an integer value that you define (default: 2).

To create an adaptive threshold using Citrix ADM

1. In Citrix ADM, navigate to Analytics > Settings > Adaptive Thresholds, and then click Add.
2. On the Adaptive Thresholds page, specify the following parameters:
   - Name - Threshold name
   - Entity - URL
   - Duration - Duration of the threshold (day or week)
   - Threshold Multiplier - A user-defined integer that is multiplied with the maximum hit count of the specified URL to obtain the adaptive threshold for the URL.

Configure database persistence

August 1, 2019

Configure database persistence in Citrix Application Delivery Management (ADM) allows you to customize the duration for you want to store the historical data of your Citrix ADC analytics data. You can choose the following database persistence types for your analytics’ historical data:

- Hours to persist minutely data
- Days to persist hourly data
- Days to persist daily data

To Configure Database Persistence

1. Navigate to > Analytics > Settings > Database Persistence.
2. Click on the Insight type you want to configure the database persistence.
3. Specify the duration for which you want to retain Insight data on Citrix ADM. For example, for Gateway Insight, you can store your analytics’ minutely historical data for 2 hours, or hourly data for 1 day.

Self-service diagnostics for Analytics

August 1, 2019

Citrix Application Delivery Management (ADM) performs self-service diagnostics to identify the license and configuration issues on the managed instances for the following analytics features:

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- Secure Web Gateway Analytics

The self-service diagnostics runs every 12 hours and generates a diagnostic report if issues are found for each of the specified analytics features. The diagnostic report provides the sources of the issues, the types of issues, and the corrective actions to resolve the issues. The self-service diagnostics helps you to identify and troubleshoot the issues faster.

For example, if AppFlow policy is not bound on a virtual server or a virtual server is not licensed, Citrix ADM does not get the desired data for Web Insight monitoring. The self-service diagnostics identifies the issues and generates a diagnostic report. You can view the diagnostic report to check the issues and perform the corrective actions.

View the diagnostic report

To view the diagnostic reports for the specified analytics features, you need to go to the respective analytics node in the dashboard of Citrix ADM.

For example, to view the diagnostic report for Web Insight, navigate to Analytics > Web Insight. On the Web Insight page, select the Show Diagnostics icon.

You can also run an instant diagnostic if you want to check for issues. Click Run diagnostics. Choose the instances and select Run Diagnostics.
Analyse the diagnostic report

The self-service diagnostics displays the diagnostic report in either orange or blue background according to criticality of issues.

Diagnostic report in the orange background signifies a higher criticality than the blue background.

For example, there are five virtual servers configured on your Citrix ADC instance. If you have not enabled the AppFlow parameters on any virtual servers, Citrix ADM does not receive the Web Insight and Security Insight traffic for analysis. The self-service diagnostics identifies the configuration issues as critical. You see the diagnostic reports in orange background in the Web Insight and the Security Insight feature.

If you have enabled AppFlow on one of the virtual servers, Citrix ADM receives data for analytics. You see the diagnostic report in blue background because at least one virtual server is sending traffic for analysis.

**IMPORTANT**: The self-service diagnostics does not check for traffic flow. It only checks for license or configuration issues that are associated with the specified analytics features on the managed instances. Sometimes, you do not see any analytics data because there is no active traffic flowing through virtual servers.

The Diagnostic report has a summary page and a detailed information page.

The summary page provides an overview about the types of issues - license or configuration. The page might contain hyperlinks that direct you to the relevant configuration pages.
For example, if there are no load balancing virtual servers licensed on your Citrix ADM, the summary page provides a hyperlink that directs you to the System Licenses page.

To view the detailed information about the issues, click See more on the summary page.

The detailed information page provides the complete information about the issues and recommends action that you need to perform. You can click the hyperlink against each issue to configure the managed instance or the virtual server.

You can also search the issues based on the action, host name, IP address, and issue type and so on.
After resolving the issues, you need to run an instant diagnostic to generate the latest diagnostic report.

**Web Insight**

August 1, 2019

Web Insight enables visibility to the administrators to monitor all web applications served by Citrix ADC instances. As an administrator, you can get an integrated and real-time monitoring of the applications from Citrix ADC instances. Web Insight provides critical information such as client network latency and server response time, ensuring to monitor and improve application performance. The data used for analytics is captured from each HTTP, HTTPS transactions that are processed by the Citrix ADC instance. The analytics data enables you to analyze the performance of Citrix ADC instances, application, URL, client, and server in your environment.

The following are some of the use cases you can view the data using Web Insight:

- The list of clients that are experiencing high latency while accessing an application like SharePoint
- The top application which had the most hits within an hour
- The list of applications and URLs accessed from clients
- The operating system and browser used by a particular client
- The applications or servers that send the most error-related responses
• Accessibility issues with one particular client
• Accessibility issues across few or all application from a particular client
• Few pages of an application are slow from a particular client and from backend server
• Application is slow when accessed from a particular client and from backend server

You can enable Web Insight for a specific virtual server on a selected instance to monitor the traffic on your web application. The Web Insight feature then provides statistics for the virtual server in Citrix ADM. To enable the Web Insight:

1. Log on to Citrix ADM with administrator credentials.
2. Navigate to Networks > Instances > Citrix ADC, and select the Citrix ADC instance on which you want to enable analytics.
3. From the Select Action list, select Configure Analytics.

4. On the Configure Insight page:
   a) Select the Application List for either Load Balancing or Content Switching.
   b) Select the virtual server and click Enable AppFlow.
5. In the Enable AppFlow dialog box:

- Enter **true** in the text box
- Select **Logstream** as the transport mode
  
  Note Citrix recommends you to select Logstream as the transport mode
- Select **Web Insight** and click **OK**.
Analyze web application issues

One of the common issues that an administrator needs to identify is the latency issues. As an administrator, you need to find if the latency issue is from the server network, client network, or server response time. Using Citrix ADM, you can identify this information by navigating to Analytics > Web Insight.

When you navigate to Analytics > Web Insight, it displays the Citrix ADC instances that are enabled with Web Insight. You can view the detailed information for the instances such as IP address, hostname, total number of hits, and bandwidth.

Using the list, you can select the time duration to view the insights for the instances.
You can also use the slider to customize the time duration and click **Go** to display the results.

When you click on the graph or the IP address of the instance, the detailed information about the instance is displayed. You can view insights for the following:

- **Total number of hits**

- **Bandwidth**
• Applications

• Domains

• URLs

• HTTP Request Methods
• HTTP Response Status

HTTP Response Status

○ 200 (654)

• Clients
• **Servers**

• **Operating Systems**
You can also select Web Insight entities for which you want to view reports on the GUI.

1. Navigate to Analytics > Web Insight > Settings.
2. Click Configure Analytics Data Record Logs.
3. Under **Web Insight Report Settings**, select the entities that you want to view reports on the GUI.

4. Click **OK**.

To drill-down for further analysis, you can click each insight category under Web Insight in the GUI. For example, if you want to check issues for the configured servers:

1. Navigate to **Analytics > Web Insight > Servers**.

2. The Servers page is displayed with all configured servers.

3. Click the IP address from the graph. You can also click the IP address from the table.
The detailed insight view for the selected server is displayed. From this view, you can check for multiple insights such as:

- Total number of hits received by the server
- Bandwidth
- Server processing time
- Server network latency
- Virtual servers configured for the server
- Total number of clients accessing the server
- Total number of response codes provided by the server

**Use case 1 - Internal server error**

Consider a scenario that your users are experiencing inaccessibility error 500 for your web application. The error 500 (Not Found) is HTTP response status error that indicates an issue on the web server, but the server does not state the issue explicitly. To identify and drill-down to the actual issue:

1. Navigate to Analytics > Web Insight > Response Status.

   The dashboard page is displayed. The dashboard provides you the metrics that you can use to analyze the success and failure of the HTTP transactions that are processed.

2. Click **Not Found** on the graph.
3. Scroll down to view the Servers graph, and from the Filter By list, select Server Network Latency.

The graph indicates that every application server had an issue in retrieving the web application and hence the response time for web server is increased. The issue can be with the web server not responding for any request from any server.

**Use case 2 - User experiencing slowness in accessing the web application**

Consider a scenario that your web application is hosted through 10 different web servers. When the application gets accessed by multiple users at the same time, one or more users may experience application slowness. As an administrator, you have to analyze the following scenarios to understand the root cause of the issue:

**Scenario 1 - Server Processing Time:**

When multiple requests hit the 10 web servers at a same time, the time taken to load the request differs based on:

- Number of requests in the queue.
- The bandwidth consumed by each request to process the HTTP transaction.

The server graph can help you understand the processing time of each server for the request processed by the servers. Similarly, the application graph displays the hits, response time, and
the bandwidth consumed by each HTTP transaction.

1. Navigate to Analytics > Web Insight > Servers.

2. Select the server from the graph.

3. Click Server Processing Time to analyze the processing time of the server.

Scenario 2 - Client Latency:

The response time and the total number of hits for the application can be the reason for application access slowness. You can check the client network latency and analyze the metrics for the client network latency. To analyze the root cause:

1. Navigate to Analytics > Web Insight > Clients.

2. Select the client from the graph.

3. Click Client Network Latency to analyze the high latency.

In this example, as an administrator, you can see the issue root cause is from the client network because the client network latency indicates high.
Use case 3 - Slowness in accessing the web application

Consider a scenario that you have web servers for Windows users and web servers for Mac users, and your users are reporting slowness in accessing the web application. As an administrator, you are aware that you have:

• Configured a content switching virtual server for Windows users.
• Configured a content switching virtual server for Mac users.
• Configured associated services bound to the virtual servers to redirect requests based on Windows and Mac users.

To analyze the root cause of the web application slowness issue:

1. Navigate to **Analytics > Web Insight > Applications**
2. Select the content switching virtual server.
   For example, the “CSTOLBTarget” application in the image is a content switching virtual server that is bound to other load balancing virtual servers.

3. Click the content switching virtual server to view the other load balancing virtual server. You can also click the application name in the table.
You can further click the bound load balancing servers to view the Web Insight details of those applications.
Analyse insights for browsers and operating systems

You can use Web Insight to help you segregate L7 latency issues and understand mobile device usage uptake. As an administrator, the insight can help you to understand different operating system uptakes across your user base.

Navigate to Analytics > Web Insight > Operating system to see why there is slowness in user access and if it is due to incompatibility across certain browsers. You can also see which operating systems are being used across certain clients, and the browsers being accessed. You can compare the rendered time across the different browsers and further drill-down to particular a browser to identify which application pages are associated with the highest rendering time for that browser.

For example, you can select Google Chrome and see the corresponding rendering times for the different URL pages for a particular application.

Citrix ADC instances deployed in high availability mode

Citrix ADM provides reports for ADC instances that are deployed in high availability mode. Aggregated reports for instances in high availability mode are supported in all analytics.
You can click on the name of the instances that are in high availability to view more details.
Citrix ADC instances deployed in cluster mode

Citrix ADM provides reports for ADC instances that are deployed in cluster mode. Aggregated reports for instances in cluster mode are supported in all analytics.

You can also click the CLIP host name to view all details about the ADC instances that are deployed in a cluster mode.
Note

- All data previously collected before you upgraded to Citrix ADM 12.1 build 503.x continues to be displayed as independent reports for the period until the data persists.
- For ADC instances deployed in cluster mode, Observation Domain ID/Observation Domain Names are replaced by CLIP host name and CLIP. All data previously collected continues to report Observation Domain ID/Observation Domain Name.

Web Insight geomap configuration

Geomaps feature in Citrix ADM displays the usage of web applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage and for capacity planning.

Geomap 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.

Geomaps provide 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 provides you an option to configure geomaps for private IP addresses or public IP addresses.

Configure geomaps for private IP addresses

To view the web application traffic originating from private IP addresses on the geomap, you must first create private IP address blocks and then enable geo data collection.

To enable the Geo Data Collection:

1. Navigate to Networks > Instances > Citrix ADC, and select the Citrix ADC instance.
2. From the Select Action list, select Configure Analytics.
3. On the **Configure Insight** page, select **Enable Geo data collection for Web and HDX 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 **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 location of a client 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.

**Configure thresholds**

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 **Analytics > Settings > Thresholds**.
2. On the **Thresholds** page, click **Add**.
   
   The **Create Threshold** page is displayed.
3. Specify the following details:
   
   a) **Name** - Specify a name for creating an event.
   
   b) **Traffic Type** - From the list, select WEB.
   
   c) **Entity** - From the list, select the category or the resource type. By default, “applications” is selected as the entity.
   
   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 duration.
f) In the **Configure Rule** section, create a rule by choosing the metric, a required comparator, and provide a threshold value.

![Configure Rule](image)

- **Metric**: Server Network Latency
- **Comparator**: >
- **Value**: 200

g) In the **Notifications Settings** section, select **Enable Threshold** and the alert mode for which you want to get the alerts.

![Notifications Settings](image)

- **Enable Threshold**: Check box
- **Notify through Email**: Check box
- **Server Admin Distro**: Drop-down menu
- **Notify through SMS**: Check box
- **SMS Distribution List**: Drop-down menu
- **Notify through Slack**: Check box

4. Click **Create**.
HDX Insight

August 1, 2019

HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktops passing through Citrix ADC. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables Citrix Application Delivery Management (ADM) to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your Citrix Gateway virtual server(s). 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 on 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 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 Citrix 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 username and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.
4. On the **Current Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.

5. On the **Current Sessions** table, click the hop diagram symbol to display information about the connection between the client and the server, including latency values.
Summary

In this example, the DC Latency is 751 milliseconds, the WAN latency is 52 milliseconds and Host Delays is 6 seconds. This indicates that the user is experiencing delay due to average latency caused by the server network.

Scenario 2

User is experiencing delay while launching an application on Citrix Virtual 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. On the Analytics tab, navigate to HDX Insight > Users.
2. Scroll down and click on the user name.
3. In the graphical representation, note the WAN Latency, DC Latency and RTT values for the particular session.
4. In the **Current Sessions** table, note that the host delay is high.

<table>
<thead>
<tr>
<th>Diagram</th>
<th>Session ID</th>
<th>Session Type</th>
<th>ICA RTT</th>
<th>Host Delay</th>
<th>Start Time</th>
<th>Up Time</th>
<th>Client IP Address</th>
<th>Server IP Address</th>
<th>NetScaler IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>784 ms</td>
<td>517.00 ms</td>
<td>10/29/2016</td>
<td>5:20:20 PM</td>
<td>0 h 2 m 50 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>780 ms</td>
<td>297.00 ms</td>
<td>10/29/2016</td>
<td>5:20:20 PM</td>
<td>0 h 2 m 35 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>760 ms</td>
<td>351.00 ms</td>
<td>10/29/2016</td>
<td>5:17:40 PM</td>
<td>0 h 5 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>625 ms</td>
<td>608.00 ms</td>
<td>10/29/2016</td>
<td>6:17:20 PM</td>
<td>0 h 5 m 51 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>625 ms</td>
<td>107.00 ms</td>
<td>10/29/2016</td>
<td>6:17:20 PM</td>
<td>0 h 8 m</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>275 ms</td>
<td>615.00 ms</td>
<td>10/29/2016</td>
<td>6:14:20 PM</td>
<td>0 h 8 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>509 ms</td>
<td>86.00 ms</td>
<td>10/29/2016</td>
<td>6:11:20 PM</td>
<td>0 h 11 m 51 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>796 ms</td>
<td>191.00 ms</td>
<td>10/29/2016</td>
<td>6:11:20 PM</td>
<td>0 h 11 m 51 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>777 ms</td>
<td>93.00 ms</td>
<td>10/29/2016</td>
<td>6:08:13 PM</td>
<td>0 h 14 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>625 ms</td>
<td>622.00 ms</td>
<td>10/29/2016</td>
<td>6:08:13 PM</td>
<td>0 h 14 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>777 ms</td>
<td>67.00 ms</td>
<td>10/29/2016</td>
<td>6:05:13 PM</td>
<td>0 h 17 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>805 ms</td>
<td>652.00 ms</td>
<td>10/29/2016</td>
<td>6:05:13 PM</td>
<td>0 h 17 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>875 ms</td>
<td>628.00 ms</td>
<td>10/29/2016</td>
<td>6:02:13 PM</td>
<td>0 h 20 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>787 ms</td>
<td>55.00 ms</td>
<td>10/29/2016</td>
<td>6:02:13 PM</td>
<td>0 h 20 m 52 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>780 ms</td>
<td>634.00 ms</td>
<td>10/29/2016</td>
<td>5:59:19 PM</td>
<td>0 h 23 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>830 ms</td>
<td>52.00 ms</td>
<td>10/29/2016</td>
<td>5:59:19 PM</td>
<td>0 h 23 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>866 ms</td>
<td>369.00 ms</td>
<td>10/29/2016</td>
<td>5:56:10 PM</td>
<td>0 h 26 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
<tr>
<td></td>
<td>0000-000001</td>
<td>Application</td>
<td>739 ms</td>
<td>48.00 ms</td>
<td>10/29/2016</td>
<td>5:56:10 PM</td>
<td>0 h 26 m 53 s</td>
<td>190.104.96.33</td>
<td>10.102.60.51</td>
</tr>
</tbody>
</table>

**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 additional user metrics, such as WAN jitter and Server Side Re-transmits if you are using Citrix ADM running software 11.1 build 51.21 or later. To view these metrics, navigate to **Analytics > HDX Insight > Users**, and select a user name. The user metrics appear in the table next to the graph.
Citrix Application Delivery Management 12.1

Geomaps for HDX Insight

The Citrix ADM geomaps functionality displays the usage of applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage across various geographical locations.

You can configure Citrix ADM to display the geomaps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

You can also view the historical and active users' details from the geo location maps in HDX Insight. Navigate to Analytics > HDX Insight, and in the World section of the map, click the country or region for which you want to see the details. You can further drill down to view information by city and state.

To configure a geomap for data centers:

On the Analytics tab, navigate to Settings > IP Blocks to configure geomaps for a particular location.

Use Case

Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.
The Santa Clara users use the Citrix Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the Citrix 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 Citrix Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

A Citrix ADC administrator analyzing the traffic can use the geomap functionality to show the traffic in Santa Clara office. The map shows that the response time in the Santa Clara office is very high, because the Santa Clara office has only one Citrix Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another Citrix Gateway, so that users have two local Citrix Gateway appliances through which to access the VPN.

Limitations

If Citrix ADC instances have Enterprise license, thresholds set on Citrix ADM for HDX Insight will not be triggered since analytical data is collected for only 1 hour.
Create thresholds and configure alerts for HDX Insight

August 1, 2019

HDX Insight on Citrix Application Delivery Management (ADM) allows you to monitor the HDX traffic passing through 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 a number of 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 case of 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) should be <= 100 ms
- Threshold rule2: WAN Latency (metric) for users (entity) should be <= 100 ms

An example of threshold group can be: {Threshold rule 1 + Threshold rule 2}

To create a rule, you should first select the entity that you want to monitor. Then choose a metric while creating a rule. For example, you can select applications entity and then select Total Session Launch count or App Launch Count. You can create one rule for every combination of an entity and a metric.

Use the comparators provided (> , < , >= , and <=) and type a threshold value for each metric.

Note

If you do not want to monitor multiple entities in a single group, you must create a separate threshold rule group for each entity.
When the value of a counter exceeds the value of a threshold, Citrix 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 and/or receive the alert as an email or as an SMS on your mobile device. For the last two actions, you must configure the email server or the SMS server on 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 Citrix Gateway and Citrix GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc. wants to track the user experience for all their offices in order 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 datacenter, while a few are located at further away from the datacenter. 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 e-mail or SMS for breaches per area. Eric is also able to combine tracking of more than one metric within a threshold rule group and narrow down the root cause to capacity issues if any. Eric is now able to proactively track any deviation without having to worry about the complexity of manually looking through all Citrix Virtual Apps and Desktops portfolio metrics.

**To create a threshold rule group and configure alerts for HDX Insight using Citrix ADM:**

1. In Citrix ADM, navigate to **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 drop-down list box, select HDX.
   c) **Entity.** From the drop-down list box, select the category or the resource type. The entities differ for each traffic type that you have selected earlier.
d) **Reference Key.** A reference key is automatically generated based on the traffic type and entity that you have selected.

e) **Duration.** From the drop-down list box, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.

![Create Threshold](image)

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](image)
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 notifications and SMS notifications.

7. Click Create to create a threshold rule group.
Viewing HDX Insight reports and metrics

August 1, 2019

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 etc. within the specified time interval.
- **Instances**: Displays the reports on the Citrix 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.

**Note**

The Licenses value does not apply to Citrix SD-WAN appliances.

User View reports and metrics

Nov 06, 2017

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktops users.

**To navigate to the Users view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Users**
User view reports and metrics consists of the following sections:

- **Summary View**
- **Per User View**
- **Per User Session View**

### Summary View

The summary view displays the reports for all the users that have logged in during the selected time-line. All the metrics/reports in this view displays the values corresponding to them for the selected time period unless specified otherwise.

**To change the selected time period:**

1. Use the time period drop-down or the time slider to set the desired time interval.
2. Click **Go**.

### Line chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual App sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
User Summary report
Following are the metrics that are specific to this report.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual App sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Total App Launch Count</td>
<td>Total Apps launched by the user during the selected time period.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Active Desktops</td>
<td>Total number of active Citrix Virtual Desktops during a given time interval.</td>
</tr>
</tbody>
</table>
Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.
User Agents

User agents represent the overall bandwidth/total bytes consumed by each receiver client in the form of a doughnut chart. Each colored segment in the chart represents one receiver client. The length of the segment depends on the number of users launching their applications on that receiver client. You can also sort the metrics by bandwidth, or total bytes.

Click on each segment to view the details of the users using that receiver client.

Thresholds Breach count

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period.

World Map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
• Bandwidth
• Total Bytes

Per User view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Users**.

3. Select a particular user from the Users summary report.

**Line chart**

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

**Current/Terminated sessions report**

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the Citrix ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual App server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive -Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
</tbody>
</table>
### Metrics Description

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
</tbody>
</table>

**Support for EDT in HDX Insight**

Citrix Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol. EDT support for Citrix Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Receiver.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they will appear as “NA”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.
### Note

EDT in HDX Insight is supported on Citrix ADM from release 12.1 build 50.28 and is available on ADC instances from release 12.1 build 49.23.

**HDX Insight metrics available from Citrix ADM 12.0 and later:**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>L7 Client-side Latency</strong></td>
<td>The average L7 latency observed between the ICA client and the Citrix ADC instance. This metric is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td><strong>L7 Server-side Latency</strong></td>
<td>The average L7 latency observed between the Citrix ADC device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td><strong>Maximum Breach Latency</strong></td>
<td>The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.</td>
</tr>
<tr>
<td><strong>Average Breach Latency</strong></td>
<td>The average value of L7 latency when the system is in a “L7 latency breached” state.</td>
</tr>
<tr>
<td><strong>L7 Threshold Breach Count</strong></td>
<td>The number of times a L7 threshold breach has occurred.</td>
</tr>
</tbody>
</table>
Desktop users

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>

Applications

A bar graph representing apps sorted by Active, total session launch count, total app launch count and launch duration.
Instances

A bar graph representing Citrix ADC instances sorted by Active and total apps.

Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.
User Agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

Per User Session view

The per user session view provides reporting for a particular selected user’s session.

To view the metrics for a selected user’s session:

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Users.
3. Select a particular user from the User Summary Report section.
4. Select a session from Current Sessions or Terminated Sessions column.
## Timeline chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
### Metrics

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>

---

**Active Application**

The Active Applications section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.

---

**Related Sessions**

The related Sessions section displays the related sessions of the selected user’s sessions. The relationship can be selected as common servers or common Citrix ADC.
Citrix Application Delivery Management 12.1

Application View reports and metrics

The reports and metrics in this view are focussed on the Citrix Virtual Apps.

To navigate to the Application view:

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Applications.

Summary view

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Sessions</td>
<td>Total number of sessions during a given time interval.</td>
</tr>
<tr>
<td>Launch duration</td>
<td>Average time taken to launch an application.</td>
</tr>
</tbody>
</table>
Applications Summary report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Apps.</td>
</tr>
<tr>
<td>Total Session Launch count</td>
<td>Total number of active Citrix Virtual Apps sessions during the given time interval.</td>
</tr>
<tr>
<td>Total App Launch Count</td>
<td>Total number of Citrix Virtual Apps launched during the given time interval.</td>
</tr>
<tr>
<td>Launch Duration</td>
<td>Average time taken to launch the Citrix Virtual App.</td>
</tr>
</tbody>
</table>

Active Application report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual App.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the application: Green-Active, Red-Inactive</td>
</tr>
</tbody>
</table>
# Active Sessions
Number of active user sessions using this app during a given time interval.

# Active Apps
Number of active sessions for this application.

**Active Applications**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th># Active Sessions</th>
<th># Active Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicator</td>
<td></td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Fidelity</td>
<td></td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>GoToMeeting</td>
<td></td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

**Threshold report**
The Threshold Report represent the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds.

**Line chart**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td>Launch duration</td>
<td>Average time taken to launch an application.</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
## Current Sessions report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the Citrix ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual Apps server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td><strong>Metrics</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive -Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
</tbody>
</table>
### Metrics Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name of the user accessing this particular Citrix Virtual App.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Unique identifier for the Citrix Virtual Apps session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Will be “Application”.</td>
</tr>
<tr>
<td>State</td>
<td>Session state: Green for active, Red for inactive.</td>
</tr>
<tr>
<td>Maximum Breach Latency</td>
<td>The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.</td>
</tr>
<tr>
<td>Average Breach Latency</td>
<td>The average value of L7 latency when the system is in a “L7 latency breached” state.</td>
</tr>
<tr>
<td>L7 Threshold Breach Count</td>
<td>The number of times a L7 threshold breach has occurred.</td>
</tr>
<tr>
<td>L7 Client-side Latency</td>
<td>The average L7 latency observed between the ICA client and the Citrix ADC instance. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td>L7 Server-side Latency</td>
<td>The average L7 latency observed between the Citrix ADC device and the Citrix Virtual Apps. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
</tbody>
</table>
**Per Application Session view**

The per application session view displays reports for a particular selected application session.

**To view the Session reports:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Applications**.
3. Select a particular user from the Application Summary Report.
4. Select a session from current sessions report.

**Line chart**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
</tbody>
</table>
### Metrics Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>

### User Bar graph

The User’s bar graph represents the users logged into this particular app.
Desktop View reports and metrics

The reports and metrics in this view are focussed on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Desktop.

Summary view

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
Desktop Summary report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Sessions</td>
<td>Total number of active Citrix Virtual Desktops sessions during a given time interval.</td>
</tr>
<tr>
<td>Active Desktops</td>
<td>Total number of active Citrix Virtual Desktops during a given time interval.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
</tbody>
</table>
### Metrics Description

| Total Bytes | Total Bytes consumed by the user during the selected time period. |

#### Threshold report

The threshold report represents the count of thresholds breached where the entity is selected as Desktop in the selected period. For more information, see how to create thresholds.

#### Per Desktop view

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

**To navigate to the particular Desktop view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Desktop.
3. Select a particular Desktop from the Desktop Summary Report.

#### Line chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>
## Metrics Description

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td></td>
<td>A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
### Desktop Users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>
User Desktops Active/Inactive report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the Citrix ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual Apps server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive - Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
</tbody>
</table>
## Metrics Description

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>VDI Image Name</td>
<td>Name of the Citrix Virtual Desktop to which the user is connected</td>
</tr>
</tbody>
</table>

### Diagram

Per Desktop Session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

**To navigate to the Desktop session view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.
3. Select a particular desktop from the **Desktop Summary Report**.
4. Select a session from current sessions report.
**Timeline chart**

The per user session view provides reporting for a particular selected user’s session.

**To view the metrics for a selected user’s session:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Users.
3. Select a particular user from the User Summary Report section.
4. Select a session from Current Sessions or Terminated Sessions column.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
</tbody>
</table>
**Metrics Description**

**Server side fast RTO**
Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.

**Bandwidth per Interval**
The bandwidth consumed by the session during that particular interval of time.

**Server side Zero Window size event**
This counter indicates the number of times the server advertised a zero TCP window.

**Client side Zero Window size event**
This counter indicates the number of times the client advertised a zero TCP window.

---

**Related Desktop Sessions report**
These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the Citrix ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/Citrix Virtual Apps server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive -Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between Citrix ADC and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between Citrix ADC and the end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
**Metrics Description**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between Citrix ADC and backend server.</td>
</tr>
</tbody>
</table>

**Instance View reports and metrics**

The reports and metrics in the instance view are focussed on the Citrix ADC instance(s).

**To navigate to the Instance view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Instances.

Instance view reports and metrics consists of the following sections:

- Instance Summary View
- Per Instance View

**Instance Summary view**

This view is called the summary view as it shows the reports for all the Citrix ADC instances that are added to Citrix ADM.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

**Instance Bar graph**

This graph displays the instance vs the Total Session Launch count

Total Apps which can be selected from the dropdown on the top right on the graph canvas.
## Instance/Active Instances Summary report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Host name of the Citrix ADC instance.</td>
</tr>
<tr>
<td>IP Address</td>
<td>NetScaler IP address.</td>
</tr>
<tr>
<td>Total Session Launch count</td>
<td>Total number of unique user sessions created during a given time interval.</td>
</tr>
<tr>
<td>Total Apps</td>
<td>Total number of unique applications launched during a given time interval.</td>
</tr>
<tr>
<td>Type</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instances</th>
<th>IP Address</th>
<th>Total Session Launch count</th>
<th>Total Apps</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangalore_Oynam(10.102.216.219)</td>
<td>10.102.216.219</td>
<td>2.65 K</td>
<td>2.12 K</td>
<td>-NA-</td>
</tr>
<tr>
<td>NetScaler_VPX_1(10.102.216.177)</td>
<td>10.102.216.177</td>
<td>1.59 K</td>
<td>1.24 K</td>
<td>-NA-</td>
</tr>
</tbody>
</table>

### Active Instances

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th># Active Sessions</th>
<th># Active Apps</th>
<th># Active Desktops</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler_VPX_1(10.102.216.177)</td>
<td>10.102.216.177</td>
<td>538</td>
<td>417</td>
<td>320</td>
<td>-NA-</td>
</tr>
<tr>
<td>Bangalore_Oynam(10.102.216.219)</td>
<td>10.102.216.219</td>
<td>900</td>
<td>720</td>
<td>180</td>
<td>-NA-</td>
</tr>
</tbody>
</table>

## Threshold report

Threshold report represents the count of thresholds breached where the entity is selected as Instance in the selected period. For more information, see [how to create thresholds](#).
Skipped Flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of receiver or receiver type etc. This table shows the IP address and the skipped flow count. These receivers may not be part of whitelisted receivers; hence these sessions are skipped from monitoring.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Skipped Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.105.2.341</td>
<td>1</td>
</tr>
<tr>
<td>10.105.2.342</td>
<td>1</td>
</tr>
</tbody>
</table>

World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes
**Per Instance view**

Per instance view provides detailed end user experience reporting for a particular selected Citrix ADC instance.

**To navigate to the Instance view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Instances**.
3. Select a particular Instance from the *Instance Summary Report*.

**Line chart**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>This represents the NetScaler IP address of the selected instance.</td>
</tr>
<tr>
<td>Total session launch count</td>
<td>Total number of active Citrix Virtual Apps sessions during the given time interval.</td>
</tr>
<tr>
<td>Total Apps</td>
<td>Total number of unique applications launched during a given time interval.</td>
</tr>
</tbody>
</table>

**Applications bar graph**

Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count or launch duration.
The Users bar graph displays top 5 users based on the following criteria:

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management 12.1

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from Citrix ADC to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from Citrix ADC to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>

**World view**

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes
License View reports and metrics

The license view gives details on the Citrix Gateway license information.

To navigate to the License view:

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Licenses.
**Line chart**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses in use</td>
<td>The Citrix Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.</td>
</tr>
<tr>
<td>Total licenses</td>
<td>Total number of Citrix Gateway CCU licenses available for the customer to utilize.</td>
</tr>
</tbody>
</table>

**Threshold report**

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see [how to create thresholds](#).

**Application View Reports and Metrics**

August 1, 2019

The reports and metrics in this view are focussed on the Citrix Virtual Apps.

**To navigate to the Application view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Applications.

Summary View

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line Chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Sessions</td>
<td>Total number of sessions during a given time interval.</td>
</tr>
<tr>
<td>Launch duration</td>
<td>Average time taken to launch an application.</td>
</tr>
</tbody>
</table>

Applications Summary Report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual App.</td>
</tr>
<tr>
<td>Total Session Launch count</td>
<td>Total number of active Citrix Virtual App sessions during the given time interval.</td>
</tr>
</tbody>
</table>
Metrics Description

Total App Launch Count Total number of Citrix Virtual Apps launched during the given time interval.

Launch Duration Average time taken to launch the Citrix Virtual Apps.

<table>
<thead>
<tr>
<th>Applications</th>
<th>Total App Launch Count</th>
<th>Launch Duration</th>
<th>Total Session Launch Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Outlook</td>
<td>531</td>
<td>514.00 ms</td>
<td>531</td>
</tr>
<tr>
<td>Microsoft Visio</td>
<td>354</td>
<td>555.00 ms</td>
<td>354</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>354</td>
<td>557.00 ms</td>
<td>354</td>
</tr>
<tr>
<td>Microsoft Excel</td>
<td>354</td>
<td>555.00 ms</td>
<td>354</td>
</tr>
</tbody>
</table>

**Active Application Report**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual App.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the application: Green-Active, Red-Inactive</td>
</tr>
<tr>
<td>#Active Sessions</td>
<td>Number of active user sessions using this app during a given time interval.</td>
</tr>
<tr>
<td>#Active Apps</td>
<td>Number of active sessions for this application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Applications</th>
<th>State</th>
<th># Active Sessions</th>
<th># Active Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicator</td>
<td>✔️</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Fidelity</td>
<td>✔️</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>GoToMeeting</td>
<td>✔️</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

**Threshold Report**

The Threshold Report represent the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds and alerts.

**Line Chart**
Citrix Application Delivery Management 12.1

**# Active Sessions**
This number indicates the count of active Citrix Virtual Apps and Desktops sessions.

**Launch duration**
Average time taken to launch an application.

---

**Current Sessions Report**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual App server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive -Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td><strong>Metrics</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>WAN latency</strong></td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td><strong>DC latency</strong></td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td><strong>Total Bytes</strong></td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td><strong>Server Side Retransmits</strong></td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td><strong>Client Side Retransmits</strong></td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td><strong>Client side Zero Window size event</strong></td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td><strong>Client side fast RTO</strong></td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td><strong>Server side Zero Window size event</strong></td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td><strong>Server side fast RTO</strong></td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>The user name of the user accessing this particular Citrix Virtual Apps.</td>
</tr>
<tr>
<td><strong>Session ID</strong></td>
<td>Unique identifier for the Citrix Virtual App session.</td>
</tr>
<tr>
<td><strong>Session Type</strong></td>
<td>Will be “Application”.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Session state: Green for active, Red for in-active.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Breach Latency</td>
<td>The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.</td>
</tr>
<tr>
<td>Average Breach Latency</td>
<td>The average value of L7 latency when the system is in a “L7 latency breached” state.</td>
</tr>
<tr>
<td>L7 Threshold Breach Count</td>
<td>The number of times a L7 threshold breach has occurred.</td>
</tr>
<tr>
<td>L7 Client-side Latency</td>
<td>The average L7 latency observed between the ICA client and the NetScaler instance. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td>L7 Server-side Latency</td>
<td>The average L7 latency observed between the NetScaler device and the Citrix Virtual Apps. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
</tbody>
</table>

**Per Application Session View**

The per application session view displays reports for a particular selected application session.

**To view the Session reports:**

1. Navigate to Analytics > HDX Insight > Applications.
2. Select a particular user from the Application Summary Report.
3. Selected a session from current sessions report.

**Line Chart**
<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
</tbody>
</table>
Metrics Description

Client side Zero Window size event This counter indicates the number of times the client advertised a zero TCP window.

User Bar Graph

The User’s bar graph represents the users logged into this particular app.

Desktop View Reports and Metrics

August 1, 2019

The reports and metrics in this view are focussed on the Citrix Virtual Desktops.

To navigate to the Desktop view:
1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.

### Summary View

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

### Line Chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual App sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
</tbody>
</table>
## Metrics Description

**Client Side Retransmits**
The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

**Client side fast RTO**
Number of times the retransmission timeout occurred on the connection between NetScaler and the end user.

**Server side fast RTO**
Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

**Client side Zero Window size event**
This counter indicates the number of times the client advertised a zero TCP window.

**Server side Zero Window size event**
This counter indicates the number of times the server advertised a zero TCP window.

---

**Desktop Summary Report**
### Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Sessions</td>
<td>Total number of active Citrix Virtual Desktop sessions during a given time interval.</td>
</tr>
<tr>
<td>Active Desktops</td>
<td>Total number of active Citrix Virtual Desktops during a given time interval.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
</tbody>
</table>

### Threshold Report

The threshold report represents the count of thresholds breached where the entity is selected as Desktop in the selected period. For more information, see how to create thresholds and alerts.

### Per Desktop View

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

To navigate to the particular Desktop view:
1. Navigate to Analytics > HDX Insight > Desktop.
2. Select a particular Desktop from the Desktop Summary Report.

**Line Chart**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
</tbody>
</table>
## Server side fast RTO
Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

## Client side Zero Window size event
This counter indicates the number of times the client advertised a zero TCP window.

## Server side Zero Window size event
This counter indicates the number of times the server advertised a zero TCP window.

### Desktop Users Report
This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
</tbody>
</table>
### Metrics Description

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>

**User Desktops Active/Inactive Report**

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
</tbody>
</table>
## Citrix Application Delivery Management 12.1

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual App server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive -Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. i.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>VDI Image Name</td>
<td>Name of the Citrix Virtual Desktop to which the user is connected.</td>
</tr>
</tbody>
</table>
Per Desktop Session View

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Navigate to Analytics > HDX Insight > Desktop.
2. Select a particular desktop from the Desktop Summary Report.
3. Select a session from current sessions report.

Timeline Chart

The per user session view provides reporting for a particular selected user’s session.

To view the metrics for a selected user’s session:

1. Navigate to Analytics > HDX Insight > Users.
2. Select a particular user from the User Summary Report section.
3. Select a session from Current Sessions or Terminated Sessions column.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
</tbody>
</table>
### Metrics Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>

![Graph showing network metrics](image_url)
## Related Desktop Sessions Report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual App server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive - Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
User View Reports and Metrics

August 1, 2019

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktops users.

**To navigate to the Users view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Users**

**Summary view**

The summary view displays the reports for all the users that have logged in during the selected timeline. All the metrics/reports in this view displays the values corresponding to them for the selected time period unless specified otherwise.

**To change the selected time period:**

1. Use the time period drop-down or the time slider to set the desired time interval.
2. Click **Go.**
# Line Chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual Apps sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>
Citrix Application Delivery Management 12.1

## Metrics Description

### Server side Zero Window size event
This counter indicates the number of times the server advertised a zero TCP window.

### User Summary Report
Following are the metrics that are specific to this report.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Active Sessions</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td># Active Apps</td>
<td>This number indicates the count of active Citrix Virtual App sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Total App Launch Count</td>
<td>Total Apps launched by the user during the selected time period.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Active Desktops</td>
<td>Total number of active Citrix Virtual Desktops during a given time interval.</td>
</tr>
</tbody>
</table>
Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.
User Agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

Thresholds Breach Count

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period. For more information, see how to create thresholds and alerts.

World Map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes
Per User View

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user’s metrics:

1. Navigate to Analytics > HDX Insight > Users.
2. Select a particular user from the Users summary report.
Line Chart

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated Sessions Report

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identity for an ICA session.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Application/Desktop.</td>
</tr>
<tr>
<td>State</td>
<td>Green/Red for active/Inactive sessions.</td>
</tr>
<tr>
<td>Host Delay</td>
<td>Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Bytes per Interval</td>
<td>Number of bytes consumed by the session during that particular interval of time.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Session duration.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>End user IP.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Backend/ Citrix Virtual App server IP.</td>
</tr>
<tr>
<td>NetScaler IP Address</td>
<td>NetScaler Management IP (NSIP).</td>
</tr>
<tr>
<td>Client Type</td>
<td>Receiver type- Citrix Windows Client etc.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Receiver version.</td>
</tr>
<tr>
<td>MSI</td>
<td>Boolean (Yes/No). Indicates if the session is multi-stream ICA.</td>
</tr>
<tr>
<td>Session Reconnects</td>
<td>Number of times the session reconnected.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>Total number of times a client automatically reconnects users to disconnected sessions.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Access Type</td>
<td>Displays the mode of access of the ICA session. For example, Citrix Gateway user/transparent mode.</td>
</tr>
<tr>
<td>Country</td>
<td>Country from which the session was established.</td>
</tr>
<tr>
<td>Region</td>
<td>Region from which the session was established.</td>
</tr>
<tr>
<td>City</td>
<td>City from which the session was established.</td>
</tr>
<tr>
<td>USB Status</td>
<td>Active/Inactive - Green/Red.</td>
</tr>
<tr>
<td>Number of USB Instances Accepted</td>
<td>The count of USB instances accepted.</td>
</tr>
<tr>
<td>Number of USB Instances Rejected</td>
<td>The count of USB instances rejected.</td>
</tr>
<tr>
<td>Number of USB Instances Stopped</td>
<td>The count of USB instances stopped.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The host name of the client.</td>
</tr>
<tr>
<td>HA Failover Count</td>
<td>Number of times HA failover occurred.</td>
</tr>
<tr>
<td>Reason for termination</td>
<td>Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>Total Bytes consumed by the user during the selected time period.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
</tbody>
</table>

**Support for EDT in HDX Insight**

Citrix Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol. EDT support for Citrix Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Receiver.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they will appear as “NA”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.
HDX Insight metrics available from Citrix ADM 12.0 and later:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L7 Client-side Latency</td>
<td>The average L7 latency observed between the ICA client and the NetScaler instance. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td>L7 Server-side Latency</td>
<td>The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metrics is useful in case of non-Citrix devices being present in the delivery path.</td>
</tr>
<tr>
<td>Maximum Breach Latency</td>
<td>The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.</td>
</tr>
<tr>
<td>Average Breach Latency</td>
<td>The average value of L7 latency when the system is in a “L7 latency breached” state.</td>
</tr>
<tr>
<td>L7 Threshold Breach Count</td>
<td>The number of times a L7 threshold breach has occurred.</td>
</tr>
</tbody>
</table>
**Desktop Users**

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>

![Desktop Users](image.png)

**Applications**

A bar graph representing apps sorted by Active, total session launch count, total app launch count and launch duration.
Instances

A bar graph representing NetScaler Instances sorted by Active and total apps

Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.
User Agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

Per User Session View

The per user session view provides reporting for a particular selected user’s session.

To view the metrics for a selected user’s session:

1. Navigate to Analytics > HDX Insight > Users.
2. Select a particular user from the User Summary Report section.
3. Select a session from Current Sessions or Terminated Sessions column.
### Timeline chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Reconnects</td>
<td>This number indicates the count of active Citrix Virtual Apps and Desktops sessions.</td>
</tr>
<tr>
<td>ACR Counts</td>
<td>This number indicates the count of active Citrix Virtual App sessions.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>Session Bandwidth</td>
<td>The bandwidth consumed by the session irrespective of the interval of time.</td>
</tr>
<tr>
<td>Server Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Client Side Retransmits</td>
<td>The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.</td>
</tr>
<tr>
<td>Client side fast RTO</td>
<td>Number of times the retransmission timeout occurred the connection between NetScaler and the end user.</td>
</tr>
<tr>
<td>Server side fast RTO</td>
<td>Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.</td>
</tr>
<tr>
<td>Bandwidth per Interval</td>
<td>The bandwidth consumed by the session during that particular interval of time.</td>
</tr>
</tbody>
</table>
## Metrics

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server side Zero Window size event</td>
<td>This counter indicates the number of times the server advertised a zero TCP window.</td>
</tr>
<tr>
<td>Client side Zero Window size event</td>
<td>This counter indicates the number of times the client advertised a zero TCP window.</td>
</tr>
</tbody>
</table>

### Active Application

The Active Applications section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.

### Related Sessions

The related Sessions section displays the related sessions of the selected user’s sessions. The relationship can be selected as common servers or common NetScaler.
Instance View Reports and Metrics

August 1, 2019

The reports and metrics in the instance view are focused on the NetScaler instance(s).

**To navigate to the Instance view:**

1. Log on to your Citrix ADM using a supported web browser.
2. Navigate to Analytics > HDX Insight > Instances.

**Instance Summary View**

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to Citrix ADM.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

**Instance Bar Graph**

This graph displays the instance vs the Total Session Launch count and Total Apps which can be selected from the dropdown on the top right on the graph canvas.
Instance/Active Instances Summary Report

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Host name of the NetScaler instance.</td>
</tr>
<tr>
<td>IP Address</td>
<td>NetScaler IP address.</td>
</tr>
<tr>
<td>Total Session Launch count</td>
<td>Total number of unique user sessions created during a given time interval.</td>
</tr>
<tr>
<td>Total Apps</td>
<td>Total number of unique applications launched during a given time interval.</td>
</tr>
<tr>
<td>Type</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instances</th>
<th>IP Address</th>
<th>Total Session Launch count</th>
<th>Total Apps</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangalore_Dynamics(10.102.216.219)</td>
<td>10.102.216.219</td>
<td>2.65 K</td>
<td>2.12 K</td>
<td>N/A</td>
</tr>
<tr>
<td>NetScaler_VPX_1(10.102.216.177)</td>
<td>10.102.216.177</td>
<td>1.59 K</td>
<td>1.24 K</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Instances</th>
<th>IP Address</th>
<th># Active Sessions</th>
<th># Active Apps</th>
<th># Active Desktops</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler_VPX_1(10.102.216.177)</td>
<td>10.102.216.177</td>
<td>538</td>
<td>417</td>
<td>120</td>
<td>N/A</td>
</tr>
<tr>
<td>Bangalore_Dynamics(10.102.216.219)</td>
<td>10.102.216.219</td>
<td>900</td>
<td>720</td>
<td>180</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Threshold Report

Threshold report represents the count of thresholds breached where the entity is selected as Instance in the selected period. For more information, see how to create thresholds and alerts.

Skipped Flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of receiver or receiver type etc. This table shows the IP address and the skipped flow count. These receivers may not be part of whitelisted receivers; hence these sessions are skipped from monitoring.

Please visit Error! Hyperlink reference not valid. for more details on issues related to ICA parsing.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Skipped Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.105.2.343</td>
<td>1</td>
</tr>
<tr>
<td>10.105.2.342</td>
<td>1</td>
</tr>
</tbody>
</table>

World View

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes
Per Instance View

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

To navigate to the Instance view:

1. Navigate to Analytics > HDX Insight > Instances.
2. Select a particular Instance from the Instance Summary Report.
Line Chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>This represents the NetScaler IP address of the selected instance.</td>
</tr>
<tr>
<td>Total session launch count</td>
<td>Total number of active Citrix Virtual Apps sessions during the given time interval.</td>
</tr>
<tr>
<td>Total Apps</td>
<td>Total number of unique applications launched during a given time interval.</td>
</tr>
</tbody>
</table>

Applications Bar Graph

Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count or launch duration.
**Users Bar Graph**

The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT

![Users Bar Graph](image)

**Desktop Users Report**

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Citrix Virtual Desktop.</td>
</tr>
<tr>
<td>Desktop Launch Count</td>
<td>Number of times the desktop has launched.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Total bytes per second taken for end to end communication during the selected time interval.</td>
</tr>
<tr>
<td>DC latency</td>
<td>Latency caused by the server side of the network. I.e. from NetScaler to backend servers.</td>
</tr>
<tr>
<td>WAN latency</td>
<td>Latency caused by the client side of the network. I.e. from NetScaler to end user.</td>
</tr>
<tr>
<td>ICA RTT</td>
<td>ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.</td>
</tr>
</tbody>
</table>
World View

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking on the region. The administrators can further drill-down to view information by city and state. From Citrix ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metrics is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes
License View Reports and Metrics

August 1, 2019

The license view gives details on the Citrix Gateway license information.

To navigate to the License view:

1. Log on to your NetScaler MA Service using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Licenses**.

### Line Chart

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses in use</td>
<td>The Citrix Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.</td>
</tr>
<tr>
<td>Total licenses</td>
<td>Total number of Citrix Gateway CCU licenses available for the customer to utilize.</td>
</tr>
</tbody>
</table>

### Threshold Report

The threshold report represents the count of thresholds breached where the `entity` is selected as License in the selected period. For more information, see how to create thresholds and alerts.

### Enabling HDX Insight data collection

August 1, 2019

HDX Insight enables IT to deliver an exceptional user experience by providing unprecedented end-to-end visibility into the ICA traffic that passes through the Citrix ADC instances or Citrix SD-WAN appliances, and is a part of Citrix Application Delivery Management (ADM) Analytics. HDX Insight delivers compelling and powerful business intelligence and failure analysis capabilities for the network, virtual desktops, applications and application fabric. HDX Insight can both instantly triage on user issues, collects data about virtual desktop connections, and generates AppFlow records and presents them as visual reports.

The configuration to enable data collection in the Citrix ADC differs with the position of the appliance in the deployment topology.

### Enabling data collection for monitoring Citrix ADCs deployed in LAN user mode

External users who access Citrix Virtual Apps and Desktops applications must authenticate themselves on the Citrix Gateway. Internal users, however, might not require to be redirected to the Citrix Gate-
way. 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 Citrix ADC appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the Citrix Gateway appliance.

Note Citrix ADM and Citrix Gateway appliance reside in the same subnet.

To monitor Citrix ADC appliances deployed in this mode, first add the Citrix ADC appliance to the NetScaler 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

- On an ADC instance, you can navigate to System > AppFlow > Collectors, to check if the collector (that is, Citrix ADM) is up or not. Citrix ADC instance sends AppFlow records to Citrix ADM using NSIP. But the instance uses its SNIP to verify connectivity with Citrix ADM. So, ensure that the SNIP is configured on the instance.
- You cannot enable data collection on a Citrix ADC deployed in LAN User mode by using the Citrix ADM configuration utility.
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. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

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

   Example
   ```
   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 Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

   ```
   add vpn trafficAction <name> <qual> [-HDX (ON or OFF)]
   add vpn trafficPolicy <name> <rule> <action>
   ```

   Example
   ```
   1 add vpn trafficAction act1 tcp -HDX ON
   2 add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   ```

3. Add Citrix ADM as an appflow collector on the Citrix ADC appliance.

   ```
   add appflow collector <name> -IPAddress <ip_addr>
   ```

   Example:
   ```
   add appflow collector MyInsight -IPAddress 192.168.1.101
   ```

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

   ```
   add appflow action <name> -collectors <string> ...
   ```

   Example:
   ```
   add appflow action act -collectors MyInsight
   ```
5. Create an appflow policy to specify the rule for generating the traffic.

   **add appflow policy** <policyname> <rule> <action>

   Example:

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

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

   **bind appflow global** <policyname> <priority> -type <type>

   Example:

   ```
   bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
   ```

   **Note** The value of type should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for Appflow to 60 seconds.

   **set appflow param** -flowRecordInterval 60

   Example:

   ```
   set appflow param -flowRecordInterval 60
   ```

8. Save the configuration. Type: `save ns config`

**Enabling data collection for Citrix Gateway appliances deployed in Single-Hop mode**

When you deploy Citrix Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization.

In single-hop mode, users access the Citrix ADC appliances through a virtual private network (VPN).

To start collecting the reports, you must add the Citrix Gateway appliance to the Citrix Application Delivery Management (ADM) inventory and enable AppFlow on ADM.
To enable the AppFlow feature from Citrix ADM:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Networks > Instances, and select the Citrix ADC instance you want to enable analytics.
4. From the Select Action drop-down, select Configure Analytics.
5. Select the VPN virtual servers, and click Enable AppFlow.
6. In the Enable AppFlow field, type true, and select ICA.
7. Click OK.
Note: The following commands are executed in the background when you enable AppFlow in single-hop mode. These commands are explicitly specified here for troubleshooting purposes.

- add appflow collector <name> -IPAddress <ip_addr>
- add appflow action <name> -collectors <string>
- set appflow param -flowRecordInterval <secs>
- disable ns feature AppFlow
- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> -priority <positive_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config

EU EM virtual channel data is part of HDX Insight data that the Citrix ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on Citrix ADM.

**Enabling data collection for Citrix Gateway appliances deployed in Double-Hop mode**

The Citrix Gateway double-hop mode provides additional protection to an organization's internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (Citrix Gateway appliances) through which the ICA connections pass, and also the details about the latency
on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install Citrix ADM so that the Citrix Gateway appliances report these vital statistics.

The Citrix Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This Citrix Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The Citrix Gateway in the second DMZ serves as a Citrix Gateway proxy device. This Citrix 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 Gateway appliance in the first DMZ or the subnet belonging to the Citrix Gateway appliance second DMZ. In the above image, the Citrix ADM and Citrix Gateway in the first DMZ are deployed in the same subnet.

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 Gateway appliances to the Citrix ADM inventory and enable data collection, each of the appliances 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 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 Gateway appliances and generates the reports.
To monitor Citrix Gateway appliances deployed in this mode, you must first add the Citrix 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. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first Citrix Gateway appliance, and then enable AppFlow for TCP on the second appliance. By doing so, one of the appliances export 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. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In **UserName** and **Password**, enter the administrator credentials.
3. Navigate to **Networks > Instances**, and select the Citrix ADC instance you want to enable analytics.
4. From the **Select Action** drop-down, select **Configure Analytics**.
5. Select the VPN virtual servers, and click **Enable AppFlow**.
6. In the **Enable AppFlow** field, type **true**, and select **ICA/TCP** for ICA traffic and TCP traffic respectively.
   
   **Note** If AppFlow logging is not enabled for the respective services or service groups on the Citrix ADC appliance, the Citrix ADM dashboard does not display the records, even if the Insight column shows Enabled.
7. Click **OK**.
Configuring Citrix Gateway appliances to export data

After you install the Citrix Gateway appliances, you must configure the following settings on the Citrix Gateway appliances to export the reports to Citrix ADM:

- Configure virtual servers of the Citrix Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the Citrix Gateway virtual server in the second DMZ to the Citrix Gateway virtual server in the first DMZ.
- Enable double hop on the Citrix Gateway in the second DMZ.
- Disable authentication on the Citrix Gateway virtual server in the second DMZ.
- Enable one of the Citrix Gateway appliances to export ICA records.
- Enable the other Citrix Gateway appliance to export TCP records.
- Enable connection chaining on both the Citrix Gateway appliances.

**Configuring Citrix Gateway Using the Command Line Interface:**

1. Configure the Citrix Gateway virtual server in the first DMZ to communicate with the Citrix Gateway virtual server in the second DMZ.

   ```
   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON or OFF)] [-imgGifToPng] ...
   ```

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. Bind the Citrix Gateway virtual server in the second DMZ to the Citrix Gateway virtual server in the first DMZ. Run the following command on the Citrix Gateway in the first DMZ:
bind vpn vserver <name> -nextHopServer <name>
bind vpn vserver vs1 -nextHopServer nh1

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

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

set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED

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

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

set vpn vserver vs -authentication OFF

5. Enable one of the Citrix Gateway appliances to export TCP records.

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

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type OTHERTCP_REQUEST

6. Enable the other Citrix Gateway appliance to export ICA records:

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

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA_REQUEST

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

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]
```

set appflow param -connectionChaining ENABLED

**Configuring Citrix Gateway using Configuration Utility:**

1. Configure the Citrix Gateway in the first DMZ to communicate with the Citrix Gateway in the second DMZ and bind the Citrix Gateway in the second DMZ to the Citrix Gateway in the first DMZ.

   a) On the **Configuration** tab expand **Citrix 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 Gateway appliance.

2. Enable double hop on the Citrix Gateway in the second DMZ.

   a) On the **Configuration** tab expand **Citrix 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 Gateway in the second DMZ.
   a) On the Configuration tab expand Citrix 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 uncheck Enable Authentication.

4. Enable one of the Citrix Gateway appliance to export TCP records.
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
   e) Add a policy binding, and click Close.

5. Enable the other Citrix Gateway appliance to export ICA records:
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
   e) Add a policy binding, and click Close.

6. Enable connection chaining on both the Citrix Gateway appliances.
   a) On the Configuration tab, navigate to System > Appflow.
   b) In the right Pane, in the Settings group, click on Change Appflow Settings.
   c) Select Connection Chaining and Click OK.

7. Configure the Citrix Gateway in the first DMZ to communicate with the Citrix Gateway in the second DMZ and bind the Citrix Gateway in the second DMZ to the Citrix Gateway in the first DMZ.
   a) On the Configuration tab expand Citrix 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 Gateway appliance.

8. Enable double hop on the Citrix Gateway in the second DMZ.
   a) On the Configuration tab expand Citrix Gateway and click Virtual Servers.
   b) In the right pane, double-click the virtual server, and in the Basic Settings group, click the edit icon.
   c) Expand More, select Double Hop and click OK.

9. Disable authentication on the virtual server on the Citrix Gateway in the second DMZ.
   a) On the Configuration tab expand Citrix 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 uncheck Enable Authentication.

10. Enable one of the Citrix Gateway appliance to export TCP records.
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
   e) Add a policy binding, and click Close.

11. Enable the other Citrix Gateway appliance to export ICA records.
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
   e) Add a policy binding, and click Close.

12. Enable connection chaining on both the Citrix Gateway appliances.
Enabling data collection for monitoring Citrix ADCs deployed in transparent mode

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 Desktop 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 figure 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.

```
  set ns param --icaPorts <port>...
```
Example:

```bash
set ns param -icaPorts 2598 1494
```

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.

Example:

```bash
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

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

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.

Example:

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

add appflow action act -collectors MyInsight

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

Example:

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

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

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

Example:

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

```bash
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

Note The value of `type` should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.
7. Set the value of the \texttt{flowRecordInterval} parameter for Appflow to 60 seconds.

\begin{verbatim}
set appflow param -flowRecordInterval 60
\end{verbatim}

\textbf{Example:}

\begin{verbatim}
set appflow param -flowRecordInterval 60
\end{verbatim}

8. Save the configuration. Type: \texttt{save ns config}

\section*{Enable data collection for Citrix Gateway appliances deployed in single-hop mode}

August 1, 2019

When you deploy Citrix Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization.

In single-hop mode, users access the Citrix ADC appliances through a virtual private network (VPN).

To start collecting the reports, you must add the Citrix Gateway appliance to the Citrix Application Delivery Management (ADM) inventory and enable AppFlow on ADM.
To enable the AppFlow feature from ADM:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable analytics.
4. From the Action drop-down, select Enable/Disable Insight.
5. Select the VPN virtual servers, and click Enable AppFlow.
6. In the Enable AppFlow field, type true, and select ICA.
7. Click OK.
The following commands are executed in the background when you enable AppFlow in single-hop mode. These commands are explicitly specified here for troubleshooting purposes.

- `add appflow collector <name> -IPAddress <ip_addr>`
- `add appflow action <name> -collectors <string>`
- `set appflow param -flowRecordInterval <secs>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy <name> <rule> <expression>`
- `set appflow policy <name> -rule <expression>`
- `bind vpn vserver <vsname> -policy <string> -type <type> >-priority <positive_integer>`
- `set vpn vserver <name> -appflowLog ENABLED`
- `save ns config`

EUEM virtual channel data is part of HDX Insight data that the Citrix ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on Citrix ADM.

**Enable data collection to monitor NetScaler ADCs deployed in transparent mode**

August 1, 2019
When a NetScaler ADC is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a Citrix Virtual Apps and 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 NetScaler appliance, and you must configure an Appflow policy to collect all or specific ICA traffic that flows through the appliance.

**Note**
- You cannot enable data collection on a NetScaler 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 figure shows the network deployment of a Citrix ADM when a NetScaler ADC is deployed in a transparent mode:

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

```bash
set ns param --icaPorts \<port\>...
```

**Example:**
1. set ns param -icaPorts 2598 1494

Note
- You can specify up to 10 ports with this command.
- The default port number is 2598. You can modify the port number as required.

3. Add NetScaler Insight Center as an appflow collector on the NetScaler appliance.

   1 add appflow collector <name> -IPAddress <ip_addr>

   Example:

   1 add appflow collector MyInsight -IPAddress 192.168.1.101

   Note To view the appflow collectors configured on the NetScaler appliance, use the show appflow collector command.

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

   1 add appflow action <name> -collectors <string> ...

   Example:

   1 add appflow action act -collectors MyInsight

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

   1 add appflow policy <policyname> <rule> <action>

   Example:

   1 add appflow policy pol true act

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

   1 bind appflow global <policyname> <priority> -type <type>

   Example:

   1 bind appflow global pol 1 -type ICA_REQ_DEFAULT

   Note The value of type should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for Appflow to 60 seconds.
Enable data collection for Citrix Gateway appliances deployed in double-hop mode

August 1, 2019

The Citrix Gateway double-hop mode provides additional protection to an organization’s internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (Citrix Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install Citrix ADM so that the Citrix Gateway appliances report these vital statistics.

Figure 3. Citrix ADM deployed in double-hop mode

The Citrix Gateway in the first DMZ handles user connections and performs the security functions of an
SSL VPN. This Citrix Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The Citrix Gateway in the second DMZ serves as a Citrix Gateway proxy device. This Citrix 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 Gateway appliance in the first DMZ or the subnet belonging to the Citrix Gateway appliance second DMZ. In the above image, the Citrix ADM and Citrix Gateway in the first DMZ are deployed in the same subnet.

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 Gateway appliances to the Citrix ADM inventory and enable data collection, each of the appliances 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 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 Gateway appliances and generates the reports.

To monitor Citrix Gateway appliances deployed in this mode, you must first add the Citrix 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. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first Citrix Gateway appliance, and then enable AppFlow for TCP on the second appliance. By doing so, one of the appliances export 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 NetScaler instance you want to enable analytics.
2. From the **Action** drop-down, select **Enable/Disable Insight**.
3. Select the VPN virtual servers, and click **Enable AppFlow**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA/TCP** for ICA traffic an TCP traffic respectively.
**Note** If AppFlow logging is not enabled for the respective services or service groups on the NetScaler appliance, the Citrix ADM dashboard does not display the records, even if the Insight column shows Enabled.

5. Click **OK**.

---

**Configuring Citrix Gateway appliances to export data**

After you install the Citrix Gateway appliances, you must configure the following settings on the Citrix Gateway appliances to export the reports to Citrix ADM:

- Configure virtual servers of the Citrix Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the Citrix Gateway virtual server in the second DMZ to the Citrix Gateway virtual server in the first DMZ.
- Enable double hop on the Citrix Gateway in the second DMZ.
- Disable authentication on the Citrix Gateway virtual server in the second DMZ.
- Enable one of the Citrix Gateway appliances to export ICA records
- Enable the other Citrix Gateway appliance to export TCP records:
- Enable connection chaining on both the Citrix Gateway appliances.

**Configuring Citrix Gateway using the command line interface:**

1. Configure the Citrix Gateway virtual server in the first DMZ to communicate with the Citrix Gateway virtual server in the second DMZ.
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON/OFF)] [-imgGifToPng] ...

1. add vpn nextHopServer nh1 10.102.2.33 8443 - secure ON

2. Bind the Citrix Gateway virtual server in the second DMZ to the Citrix Gateway virtual server in the first DMZ. Run the following command on the Citrix Gateway in the first DMZ:

   bind vpn vserver <name> -nextHopServer <name>

   1. bind vpn vserver vs1 -nextHopServer nh1

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

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

   1. set vpn vserver vsnahop2 -doubleHop ENABLED -appFlowLog ENABLED

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

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

   1. set vpn vserver vs -authentication OFF

5. Enable one of the Citrix Gateway appliances to export TCP records.

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

   1. bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type OTHERTCP\_REQUEST

6. Enable the other Citrix Gateway appliance to export ICA records:

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

   1. bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA\_REQUEST

7. Enable connection chaining on both the Citrix Gateway appliances:
Configuring Citrix Gateway using configuration utility:

1. Configure the Citrix Gateway in the first DMZ to communicate with the Citrix Gateway in the second DMZ and bind the Citrix Gateway in the second DMZ to the Citrix Gateway in the first DMZ.
   a) On the Configuration tab expand Citrix 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 Gateway appliance.

2. Enable double hop on the Citrix Gateway in the second DMZ.
   a) On the Configuration tab expand Citrix 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 Gateway in the second DMZ.
   a) On the Configuration tab expand Citrix 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 uncheck Enable Authentication.

4. Enable one of the Citrix Gateway appliance to export TCP records.
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
   e) Add a policy binding, and click Close.

5. Enable the other Citrix Gateway appliance to export ICA records:
   a) On the Configuration tab expand Citrix 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 in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   d) Click Continue.
e) Add a policy binding, and click Close.
6. Enable connection chaining on both the Citrix Gateway appliances.
   a) On the Configuration tab, navigate to System > Appflow.
   b) In the right Pane, in the Settings group, click on Change Appflow Settings.
   c) Select Connection Chaining and Click OK.

Enable data collection to monitor NetScaler ADCs deployed in LAN user mode

August 1, 2019

External users who access Citrix Virtual Apps and Desktops applications must authenticate themselves on the Citrix Gateway. Internal users, however, might not require to be redirected to the Citrix Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual Apps and Desktops applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the Citrix Gateway appliance.

Figure 4. Citrix ADM deployed in LAN User Mode
Note

Citrix ADM and Citrix Gateway appliance reside in the same subnet.

To monitor Citrix appliances deployed in this mode, first add the Citrix appliance to the NetScaler Insight inventory, enable AppFlow and then view the reports on the dashboard.

After you add the Citrix appliance to the Citrix ADM inventory, you must enable AppFlow for data collection.

Note

- You cannot enable data collection on a NetScaler ADC deployed in LAN User 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.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.

2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.
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 Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

1 add vpn trafficAction ** <name> <qual> [ [-HDX ( ON | OFF )] ]
2 add vpn trafficPolicy ** <name> <rule> <action>

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.

1 add appflow collector ** <name> **-IPAddress ** <ip_addr>

Example:

1 add appflow collector MyInsight -IPAddress 192.168.1.101

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

1 add appflow action ** <name> **-collectors ** <string> ... 

Example:

1 add appflow action act -collectors MyInsight

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

1 add appflow policy ** <policyname> <rule> <action>

Example:

1 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 1 -type ICA\_REQ\_DEFAULT
```

**Note** The value of `type` should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for Appflow to 60 seconds.

```bash
set appflow param -flowRecordInterval 60
```

**Example:**

```bash
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

```bash
save ns config
```

---

**Gateway Insight**

August 1, 2019

In a Citrix Gateway deployment, visibility into a user's access details 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 a Citrix 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 Citrix ADC instances with Enterprise license. A Platinum license is needed 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 Citrix 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.

**Enabling Gateway Insight**

To enable Gateway Insight for your Citrix Gateway appliance, you must first add the Citrix 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 Devices.
To view end-point analysis (EPA) failures in Citrix ADM, you must enable AppFlow AAA Username logging on the Citrix Gateway appliance.

To enable AppFlow for a virtual server in Citrix ADM

1. Log on to Citrix ADM.
2. Navigate to Networks > Instances, and select the instance for which you want to enable AppFlow.
3. From the Select Action list, select Configure Analytics.
4. In the Configure Insight page, under Configure Analytics, select Citrix Gateway.
5. Select the virtual server for which you want to enable AppFlow, and click Enable AppFlow.
6. On the Enable AppFlow screen, in the Select Expression list, click true.
7. Next to Transport Mode, select the Logstream check box.

8. Click OK.
To enable AppFlow AAA Username logging on a Citrix Gateway appliance by using the GUI

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

Viewing Gateway Insight reports

In Citrix ADM, you can view reports for all users, applications, and gateways associated with the Citrix Gateway appliances, and you can view details for a particular user, application, or gateway. In the Overview section, you can view the EPA, SSO, Authentication, and Application Launch failures. You can also view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.

To view EPA, SSO, authentication, authorization and application launch failures

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

To view a summary of session modes, clients, and the number of users

In Citrix ADM, navigate to Analytics > Gateway Insight, scroll down to view the reports.
Viewing Gateway Insight reports for users

You can view reports for all users associated with the Citrix Gateway appliances. You can view the EPA, authentication, SSO, and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

To view user details

1. In Citrix ADM, navigate to Analytics > 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 now view the number of active users, number of active sessions, bytes and licenses used by all users during the time period.
Scroll down to view a list of available users and active users.

On the Users or Active Users tab, you can click on a user in the Username column to display the EPA, authentication, SSO, and application launch failures and other details for that user.

**Viewing Gateway Insight reports for 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.

**To view application details**

1. In Citrix ADM, navigate to Analytics > 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.

<table>
<thead>
<tr>
<th>Applications Launched</th>
<th># Sessions</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>24031</td>
<td>10472</td>
<td>7.75 MB</td>
</tr>
</tbody>
</table>

On the Other Applications tab, you can click an application in the Name column to display details of that application.

**Viewing Gateway Insight reports for gateways**

You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a Citrix Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

**To view gateway details**

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

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

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

**Exporting reports**

You can save the Gateway Insight reports with all the details shown in the GUI in PDF, JPEG, PNG, or CSV format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.
Note

- Users with read only access cannot export reports.
- Geo map reports are exported only if the Citrix ADM has internet connectivity.

To export a report

1. On the Dashboard tab, in the right pane, click the export button.
2. Under Export Now, select the required format, and then click Export.

To schedule export:

1. On the Dashboard tab, in the right pane, click the export button.
2. Under Schedule Export, specify the details and click Schedule.

To add an email server or an email distribution list:

1. On the Configuration tab, navigate to 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 Citrix Gateway appliances.

A user is not able to log in to the Citrix Gateway appliance or to the internal web servers

You are a Citrix Gateway administrator monitoring Citrix 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 Analytics > 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.

To view the authentication failure details:

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

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

3. Click the Authentication tab. You can view the number of authentication errors at any given time in the Failures graph.

Scroll down to view details of each authentication error such as Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address, and more from the table on the same tab. The Error Description column in the table displays the reason for the logon failure, and the State column displays at what stage of a two-stage authentication the failure occurred.
You can click on 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 downward arrow as indicated in the following screen shot.

### EPA failures

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

**To view EPA failure details:**

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

Scroll down to view details of each EPA error such as **Username**, **NetScaler IP Address**, **Gateway IP Address**, **VPN**, **Error Time**, **Policy Name**, **Gateway Domain Name** and more from the table on the same tab. The **Error Description** column in the table displays the reason for the EPA failure, and the **Policy Name** column displays the policy that resulted in the failure.

You can click on a user in the **Username** column to display the EPA errors and other details for that user.

You can customize the table to add or delete columns by using the downward arrow as indicated in the following screen shot.
Note
Citrix Gateway doesn’t report the EPA failures when the “clientSecurity” expression is configured as a VPN session policy rule.

SSO failures
You can view the all the SSO failures at any stage for a user accessing any applications through the Citrix Gateway appliance.

To view the SSO failure details:

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

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

3. Click the SSO (Single Sign On) tab. You can view the number of SSO errors at any given time in the Failures graph.

Scroll down to view details of each SSO error such as Username, NetScaler IP Address, Error Time, Error Description, Resource Name and more from the table on the same tab.
You can click on a user in the **Username** column to display the SSO errors and other details for that user.

You can customize the table to add or delete columns by using the downward arrow as indicated in the following screen shot.

<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>Error Time</th>
<th>Error Description</th>
<th>Error Count</th>
<th>SSO Method</th>
<th>Gateway Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>10.102.61.201</td>
<td>10.102.61.210</td>
<td>10.144.2.35</td>
<td>attest</td>
<td>2/22/2016, 1:00:04 PM</td>
<td>Single Sign-On failed</td>
<td>1</td>
<td>AG Basic</td>
<td>attest.citrix.com</td>
</tr>
<tr>
<td>user3</td>
<td>10.102.61.201</td>
<td>10.102.61.210</td>
<td>10.252.241.48</td>
<td>attest</td>
<td>2/22/2016, 12:30:04 PM</td>
<td>Single Sign-On failed</td>
<td>1</td>
<td>Basic</td>
<td>attest.citrix.com</td>
</tr>
<tr>
<td>user4</td>
<td>10.102.61.201</td>
<td>10.102.61.210</td>
<td>10.252.241.48</td>
<td>attest</td>
<td>2/22/2016, 1:30:04 PM</td>
<td>Single Sign-On failed</td>
<td>1</td>
<td>AG Basic</td>
<td>attest.citrix.com</td>
</tr>
</tbody>
</table>

**After successfully logging on to Citrix 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 Apps server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

**To view the application launch failure details:**

1. In Citrix ADM, navigate to **Analytics > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.

3. Click the **Application Launch** tab. You can view the number of application launch failures at any given time in the **Failures** graph.
Scroll down to view details of each application launch error, such as **NetScaler IP Address**, **Error Time**, **Error Description**, **Resource Name**, and **Gateway Domain Name**, and more, from the table on the same tab. The **Error Description** column in the table displays the IP address of the STA server and the **Resource Name** column displays the details of the resource for which the STA validation has failed.

You can click on a user in the **Username** column to display the application launch errors and other details for that user.

You can customize the table to add or delete columns by using the downward arrow as indicated in the following screen shot.

**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.

**To view total bytes and bandwidth consumed by an application:**

In Citrix ADM, navigate to **Analytics > 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.

A user has logged on to Citrix Gateway successfully, but is unable to access certain network resources in the internal network.

With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

To view user access for resources:

1. In Citrix ADM, navigate to Analytics > 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.
Different users might be using different Citrix Gateway deployments or might log on to Citrix Gateway through different access modes. The administrator should 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 Citrix Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

To view the summary of session modes, type of clients, and number of users logged on:

1. In Citrix ADM, navigate to Analytics > 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.
Web and web service applications that are exposed to the Internet have become increasingly vulnerable to attacks. To protect applications from attack, you need visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures. Security Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

Note

Security Insight is supported on Citrix Application Delivery Management (ADM) with Citrix ADC appliances running on version 11.0 Build 65.31 and later.

How Security Insight works

Security Insight is an intuitive dashboard-based security analytics solution that gives you full visibility into the threat environment associated with your applications. Security insight is included in Citrix ADM, and it periodically generates reports based on your Application Firewall and Citrix ADC system security configurations. 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, regardless if the application is protected or not protected by a Citrix ADC appliance. The more critical the attacks on an application, the higher the threat index for that application. 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 you insight into the attacks on the
application. Violation information is sent to Citrix ADM only when a violation or attack occurs. A large number of breaches and vulnerabilities lead to a high threat index value.

- **Safety index.** A single-digit rating system that indicates how securely you have configured the Citrix ADC instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. 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, have not been adopted, applications are assigned a low safety index value.

- **Actionable Information.** Information that you need for lowering the threat index and increasing the safety index, which significantly improves application security. For example, you can review information about violations, existing and missing security configurations for application firewall and other security features, the rate at which the applications are being attacked, and so on.

### Configure Security Insight

Citrix ADM supports Security Insight from all Citrix ADC instances that have application firewall configured on them.

To configure security insight on an ADC instance, first configure an application firewall profile and an application firewall policy. Though you can then bind the application firewall policy globally, Citrix recommends that the policy is bound to the virtual server.

To view the analytics on Citrix ADM, enable the AppFlow feature on the instance, configure an AppFlow collector, action, and policy, and bind the policy globally. Here also though you can then bind the application firewall policy globally, Citrix recommends that the policy is bound to the virtual server. Citrix also recommends that you use Citrix ADM to deploy AppFlow configurations on the ADC instances. 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 security insight on a Citrix ADC instance:**

1. Run the following commands to configure an application firewall profile and policy, and bind the application firewall policy globally or to the load balancing virtual server.

```plaintext
add appfw profile <name> [-defaults ( basic advanced )]

set appfw profile <name> [-startURLAction <startURLAction> …]
```
add appfw policy <name> <rule> <profileName>
bind appfw global <policyName> <priority>

or,
bind lb vserver <lb vserver> -policyName <policy> -priority <priority>

1 add appfw profile pr_appfw -defaults advanced
2 set appfw profile pr_appfw -startURLaction log stats learn
3 add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS" pr_appfw
4 bind appfw global pr_appfw_pol 1
5 or,
6 bind lb vserver outlook -policyName pr_appfw_pol -priority "20"

2. Run the following commands to enable the AppFlow feature, configure an AppFlow collector, action, and policy, and bind the policy globally or to the load balancing virtual server:

add appflow collector <name> -IPAddress <ipaddress>

set appflow param disabled
[-SecurityInsightRecordInterval <secs>]
[-SecurityInsightTraffic { ENABLED DISABLED }]

add appflow action <name> -collectors <string>
add appflow policy <name> <rule> <action>
bind appflow global <policyName> <priority> [ <gotoPriorityExpression> ] [-type <type>]

or,
bind lb vserver <vserver> -policyName <policy> -priority <priority>

1 add appflow collector col -IPAddress 10.102.63.85
2 set appflow param -SecurityInsightRecordInterval 600 -SecurityInsightTraffic ENABLED
3 add appflow action act1 -collectors col
4 add appflow policy pol1 true act1
5 add appflow policy pol2 true act1
6 add appflow policy pol3 true act1
7 bind appflow global pol1 1 END -type REQ_DEFAULT
8 or,
9 bind lb vserver Sap -policyName af_action_Sap_10.102.63.85 -priority "20"
To enable AppFlow from Citrix ADM:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Networks > Instances, and select the Citrix ADC instance you want to enable AppFlow.
4. From the Select Action list, select Configure Analytics.
5. Select the virtual servers, and click Enable AppFlow.
6. In the Enable AppFlow field, type true, and select Security Insight.
7. Click Ok.

View geo locations for Security Insight reports

Security Insight reports include the exact geographic locations from which client requests originate. You can view the geographic locations in Citrix ADM. The geo database file that is inbuilt in Citrix ADC contains most of the public IP addresses. The file is available at the location /var/netscaler/in-built_db in Citrix ADC.

To enable geo locations:
Run the following commands to enable geo-location logging and logging in the CEF format:

- **add locationFile** &lt;Complete path with the DB filename&gt;
- **set appfw settings -geoLocationLoggingON**
- **set appfw settings -CEFLogging ON**

If any IP address is not available in the geo database file, you can add the IP address for the geographic location. Along with the IP address, you can also add city/state/country name and the latitude and longitude coordinates of each location.

Open the geo database file with a text editor, such as vi editor, and add an entry for every location. The entry must be in the following format:

```plaintext
<start IP>,<end IP>,,<country>,,<state>,,<city>,,longitude,latitude
```

For example,

```plaintext
4.17.142.224,4.17.142.239,,US,New York,,,Harrison,,,73.7304,41.0568
```

**IP Reputation**

You can use NetScaler Insight Center to monitor and manage your incoming traffic's IP Reputation. You can configure policies to add more IPs as malicious, and create a customized block list.

To know about configuring and using IP Reputation, see [IP Reputation](#).

**Monitor IP Reputation**

The IP Reputation feature provides attack-related information about malicious IP addresses. For example, it reports IP Reputation Score, IP Reputation category, IP Reputation attack time, Device IP, and details about the Client IP address.

IP Reputation score indicates risk associated with an IP address. The score has the following are the ranges:

<table>
<thead>
<tr>
<th>IP Reputation score</th>
<th>Level of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-20</td>
<td>High Risk</td>
</tr>
<tr>
<td>21 – 40</td>
<td>Suspicious</td>
</tr>
<tr>
<td>41 – 60</td>
<td>Moderate Risk</td>
</tr>
<tr>
<td>61 – 80</td>
<td>Low Risk</td>
</tr>
</tbody>
</table>
To monitor IP Reputation:

1. Navigate to Analytics > Security Insight, and select the application you want to monitor.

2. In the Threat Index tab, select IP Reputation.

3. Select a severity to display more details of the attacks that were at that level. You can click on the bar graph or in the table under the graph.

4. Select the time period for which you want to view the details. You can use the time slider to further customize the selected period. Then, click Go.

5. To customize the display, click the settings button.
Thresholds

You can set and view thresholds on safety index and threat index of applications in Security Insight.

To set a threshold:

1. Navigate to Analytics > Settings > Thresholds, and select Add.
2. Select the traffic type as Security in the Traffic Type field, and enter required information in the other appropriate fields such as Name, Duration, and entity.
3. In the Configure Rule section, use the Metric, Comparator, and Value fields to set a threshold. For example, “Threat Index” “>” “5”
4. In the Notification Settings, select the notification type.
5. Click Create.

To view the threshold breaches:

1. Navigate to Analytics > Security Insight > Devices, and select the Citrix ADC instance.
2. In the Application section, you can view the number of threshold breaches occurred for each virtual server in the Threshold Breach column.

Security Insight use cases

The following use cases describe how you can use security insight to assess the threat exposure of applications and improve security measures.
Obtain an overview of the threat environment

In this use case, you have a set of applications that are exposed to attacks, and you have configured Citrix ADM to monitor the threat environment. You need to frequently review the threat index, safety index, and the type and severity of any attacks that the applications might have experienced, so that you can focus first on the applications that need the most attention. The security insight dashboard provides a summary of the threats experienced by your applications over a time period of your choosing, and for a selected Citrix ADC device. It displays the list of applications, their threat and safety indexes, and the total number of attacks for the chosen time period.

For example, you might be monitoring Microsoft Outlook, Microsoft Lync, SharePoint, and a SAP application, and you might want to review a summary of the threat environment for these applications.

To obtain a summary of the threat environment, log on to Citrix ADM, and then navigate to Analytics > Security Insight.

Key information is displayed for each application. The default time period is 1 hour.

To view information for a different time period, from the list at the top-left, select a time period.
To view a summary for a different Citrix ADC instance, under **Devices**, click the IP address of the Citrix ADC instance. To sort the application list by a given column, click the column header.

**Determine the threat exposure of an application**

To identify the applications that have a high threat index and a low safety index on the Security Insight dashboard, you want to determine the threat exposure before deciding to secure them. That is, you want to determine the type and severity of the attacks that have degraded their index values. You can determine the threat exposure of an application by reviewing the application summary.

In this example, Microsoft Outlook has a threat index value of 6, and you want to know what factors are contributing to this high threat index.

To determine the threat exposure of Microsoft Outlook, on the **Security Insight** dashboard, click **Outlook**. The application summary includes a map that identifies the geographic location of the server.
Click **Threat Index > Security Check Violations** and review the violation information that appears.

Click **Signature Violations** and review the violation information that appears.
Determine existing and missing security configuration for an application

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’s safety index summary.

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

- **Application Firewall Configuration.** Shows how many signature and security entities are not configured.
- **NetScaler System Security.** Shows how many system security settings are not configured.

In the previous use case, you reviewed the threat exposure of Microsoft Outlook, which has a threat index value of 6. Now, you want to know what security configurations are in place for Outlook and what configurations can be added to improve its threat index.
On the **Security Insight** dashboard, click **Outlook**, and then click the **Safety Index** tab. Review the information provided in the **Safety Index Summary** area.

![Safety Index Summary](image1)

On the **Application Firewall Configuration** node, click **Outlook_Profile** and review the security check and signature violation information in the pie charts.

![Application Firewall Configuration](image2)

Review the configuration status of each protection type in the application firewall summary table. To sort the table on a column, click the column header.
Click the **NetScaler System Security** node and review the system security settings and Citrix recommendations to improve the application safety index.

**Identify applications that require immediate attention**

The applications that need immediate attention are those having a high threat index and a low safety index.

In this example, both Microsoft Outlook and Microsoft Lync have a high threat index value of 6, but Lync has the lower of the two safety indexes. Therefore, you might have to focus your attention on Lync before improving the threat environment for Outlook.

![Security Insight](image)

**Determine the number of attacks in a given period of time**

You might want to determine how many attacks occurred on a given application at a given point in time, or you might want to study the attack rate for a specific time period.

On Security Insight page, click any application and in the Application Summary, click the number of violations. The Total Violations page displays the attacks in a graphical manner for one hour, one day, one week, and one month.
The Application Summary table provides the details about the attacks. Some of them are as follows:

- Attack time
- IP address of the client from which the attack happened
- Severity
- Category of violation
- URL from which the attack originated, and other details.

While you can always view the time of attack in an hourly report as seen in the image, now you can view attack time range for aggregated reports even for daily or weekly report. If you select “1 Day” from the time-period list, the Security Insight report displays all attacks that are aggregated and the attack time is displayed in one-hour range. If you choose “1 Week” or “1 Month,” all attacks are aggregated and the attack time is displayed in one-day range.
Obtain detailed information about security breaches

You might want to view a list of the attacks on an application and gain insights into the type and severity of attacks, actions taken by the Citrix ADC instance, resources requested, and the source of the attacks.

For example, you might want to determine how many attacks on Microsoft Lync were blocked, what resources were requested, and the IP addresses of the sources.

On the Security Insight dashboard, click Lync > Total Violations. In the table, click the filter icon in the Action Taken column header, and then select Blocked.
View log expression details

Citrix ADC instances use log expressions configured with the Application Firewall profile to take action for the attacks on an application in your enterprise. In Security Insight, you can view the values returned for the log expressions used by the Citrix ADC instance. These values include request header, request body, and so on. Apart from the log expression values, you can also view the log expression name and the comment for the log expression defined in the Application Firewall profile that the Citrix ADC instance used to take action for the attack.

Prerequisites

Ensure that you:

- Configure log expressions in the Application Firewall profile. For more information, see Application Firewall.

- Enable log expression based Security Insights setting in Citrix ADM. Do the following:
  1. Navigate to Analytics > Settings, and click Enable Features for Analytics.
  2. In the Enable Feature for Analytics page, select Enable Security Insight under the Log Expression Based Security Insight Setting section and click OK.
For example, you might want to view the values of the log expression returned by the Citrix ADC instance for the action it took for an attack on the Microsoft Lync in your enterprise.

On the Security Insight dashboard, navigate to **Lync > Total Violations**. In the **Application Summary Table**, click the URL to view the complete details of the violation in the **Violation Information** page including the log expression name, comment, and the values returned by the Citrix ADC instance for the action.
Determine the Safety Index before deploying the configuration

Security breaches occur after you deploy the security configuration on a Citrix ADC instance, but you might want to assess the effectiveness of the security configuration before you deploy it.

For example, you might want to assess the safety index of the configuration for the SAP application on the Citrix ADC instance with IP address 10.102.60.27.

On the Security Insight dashboard, under Devices, click the IP address of the Citrix ADC instance that you configured. You can see that both the threat index and the total number of attacks are 0. Threat index is a direct reflection of the number and type of attacks on the application. Zero attacks indicate that the application is not under any threat.
Click **Sap > Safety Index > SAP_Profile** and assess the safety index information that appears.

In the application firewall summary, you can view the configuration status of different protection settings. If a setting is set to log or if a setting is not configured, the application is assigned a lower safety index.
SSL Insight

August 1, 2019

SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the Citrix ADC by providing integrated and real-time and historic monitoring of secure web transactions. With this visibility the administrator can assess following:

- **Determine Configuration Change Impact on Customer Usage**: The administrator can understand the impact on clients for making a configuration change like turning off SSLv3 or removing a cipher like RC4-MD5. This can be done by assessing the historic transaction data on this protocol and cipher.

- **Quantify client performance**: Administrator can understand the impact on Application Response Time based on the SSL ciphers/protocol used or the certificates negotiated.

- **Application Security**: Assess if any of the applications have transactions running on low security protocols, ciphers, or weak key strength.

When SSL Analytics is enabled on a Citrix ADC instance, SSL statistics are recorded and logged for every SSL transaction. The statistics show the details of the SSL flow. Also, every successful connection is logged and displayed by Citrix Application Delivery Management (ADM) Analytics.

SSL Insight provides the following critical information, which is displayed by Citrix ADM Analytics:

- SSL Protocol version negotiated
- Cipher negotiated, and the cipher strength
• Signature Hash algorithm of the certificate used
• Certificate Type & Size
• SSL Frontend and Backend errors

Note
For successful SSL connections, SSL AppFlow logging happens at the end of every transaction.

Prerequisites

• The Citrix ADC instance on which you intend to configure SSL Insight must be running Citrix ADC software release 11.1 51.21 and higher. Run the following commands on the ADC instance running 11.1 51.21 to enable Logstream as a transport type for SSL Insight.

1. enable ns mode ulfd
2. add ulfd server <IP Address of the ADM>

For ADC instances running version 12.0 and above, select Logstream as the transport type while enabling AppFlow from ADM.

• The Citrix ADM version and build must be equal to or higher than the Citrix ADC version and build. For example, if you have installed Citrix ADM 11.1 build 61.7, then ensure you have installed Citrix ADC 11.1 build 60.14 or earlier.

Configuring SSL Insight

SSL Insight Metrics are included in Web Insight reports if you enable the following elements:

• Enable AppFlow for Web Insight on each Citrix ADC instance.
• Enable ULFD mode on each Citrix ADC instance.
• Enable required AppFlow parameters on each Citrix ADC instance.

Enabling the AppFlow feature

Note
You can enable the AppFlow feature either from Citrix ADM or from each Citrix ADC instance.

To enable the AppFlow feature from Citrix ADM:

1. Navigate to Networks > Instances, and select the Citrix ADC instance on which you want to enable analytics.
2. From the Select Action list, select Configure Analytics.
3. Select the virtual servers, and click **Enable AppFlow**.

4. In the Enable AppFlow field, type **true**, and select **Web Insight**.

5. Repeat steps 3 through 6 on each Citrix ADC instance.

6. Click **OK**.

**Note**

You cannot enable data collection on a virtual server if the operational state of the virtual server is other than UP.

**To enable the AppFlow feature by using the Citrix ADC GUI:**

In a Citrix ADC instance’s GUI, navigate to **Configuration > System > Settings**, click **Configure Advanced Features**, and select **AppFlow**.

**Enabling SSL Insight parameters**

On each Citrix ADC instance, you have to enable some HTTP parameters to display SSL Insight records in Citrix ADM.

**To enable SSL Insight parameters from the Citrix ADC configuration utility:**

1. Navigate to **Configuration > System > AppFlow**, and click **Change AppFlow Settings**.
2. Select the following check boxes: HTTP Domain, HTTP Host, HTTP Method, HTTP URL, HTTP User-Agent, HTTP Content-Type.

3. Click OK.

Viewing the SSL Insight metrics

SSL Insight metrics in Citrix ADM provide a detailed view of the performance of the SSL transactions served by the Citrix ADC instances. You can view the SSL Insight metrics at the client, server, or application level, and the SSL success and failure transactions’ metrics. With the help of these metrics, you can analyze and optimize your Citrix ADC HTTPS settings and SSL-certificate settings, and track performance issues.

To monitor SSL Insight Metrics in Citrix ADM:

1. On the Analytics tab, navigate to Web Insight and click the Client, Server, or Application node to display the metrics about clients, the server, or the applications, respectively.

2. In the top-left pane, from the period list, select the time frame whose metrics you want to display. You can customize the time frame by using the time-frame slider. Click Go.

3. The SSL Insight metrics appear as pie charts, which you can click for more details.

Note

The pie charts display the metrics of all the applications, clients, or servers.
4. To display details for a specific application, client, or server, click the corresponding value on the bar graph.
5. To View the Failed SSL transactions, on the SSL section, select the radio button on the SSL section.

**Use case: Obtain an overview of the SSL transactions of applications, clients, or servers**

The following use case describes how you can use SSL Insight to assess the usage of various SSL Parameters in applications, clients and servers, and improve security measures.

Consider that you have a set of applications that are using SSL transactions (HTTPS) for communication, and you have configured Citrix ADM to monitor the SSL components. You might need to frequently review the applications so that you can focus first on the applications that need the most attention. The SSL insight dashboard provides a summary of various SSL parameters used by your applications over a time period of your choosing, and for a selected Citrix ADC device. They are:

- SSL Certificates
- SSL Protocols
- SSL Cipher Negotiated
- SSL Key Strength
- SSL Failure – Frontend
- SSL Failure – Backend
In the following example, you can see list of clients (identified by their IP addresses) and the SSL hits per client. Also, at the right, you can view the SSL Parameters for all the clients.
To display SSL details for a client, select the client on the bar graph or in the table below the graph. In the following example, the selected client’s transactions use an SHA1 SSL certificate and four major protocols: TSLv1.2, TSLv1.1, TSLv1, and SSLv3. You can also see that ciphers of various strengths were negotiated. The color code indicates the strength of the SSL protocol, which gives you information about weak ciphers and strong ciphers.
Similarly, to view the information about the failed SSL transactions, select the radio button on the SSL section. SSL front end and back-end failures are displayed separately in two pie charts. In the following example, you can view that the major back-end SSL errors are Handshake failures and major front-end SSL errors are Illegal parameters.
The TCP Insight feature of Citrix Application Delivery Management (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 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 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.

*Note* Citrix recommends that you use 500 GB for better performance.
Enabling TCP Insight

Before you can view the TCP Insight metrics, you must enable the feature on Citrix ADM.

To Enable TCP Insight:

1. Log on to Citrix ADM using the administrator credentials.
2. Navigate to Analytics > Settings, and click Enable Features for Analytics.
3. On the Enable Features for Analytics page, select Enable TCP Insight.
4. In the confirmation window, click OK.

Viewing 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 Analytics > 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 from 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.
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 datacenter and the branch sites. WAN Insight analytics enable administrators to easily monitor the accelerated and unaccelerated WAN traffic that flows between the datacenter 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 datacenter WAN optimization appliance enables the Citrix Application Delivery Management (ADM) to collect data and provide reports and statistics for the datacenter and the branch WAN optimization appliances.
To enable analytics on the WAN optimization appliance:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).

2. In the **UserName** and **Password** fields, enter the administrator credentials.

3. Navigate to **Networks > Instances > Citrix SD-WAN**, and select the SD-WAN WO instance.

4. From the **Select Action** drop-down, select **Configure Analytics**.

5. Select the following parameters as required:
   - **Geo data collection for HDX Insight**: Shares client IP address with the Google Geo API.
   - **AppFlow**: Starts collecting data from WAN optimization instances.
     - **TCP and WANOpt**: Provides TCP and WANOpt Insight reports.
     - **HDX**: Provides HDX Insight reports.
TCP only for HDX: Provides TCP only for HDX Insight reports.

Configure Insight

Enable data collection on the load balancer SD-WAN WO instance, so that the performance of applications can be monitored.

<table>
<thead>
<tr>
<th>Type of traffic</th>
<th>Type of Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppFlow</td>
<td>HDX</td>
</tr>
<tr>
<td>TCP and WANOpt</td>
<td>HDX</td>
</tr>
<tr>
<td>TCP only for HDX</td>
<td>HDX</td>
</tr>
</tbody>
</table>

6. Click OK.

To view WAN Insight reports:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. Navigate to Analytics > 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 datacenter 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>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>
The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by Citrix ADC appliances to improve customer experience and operational efficiency, providing benefits such as:

- Manage the network during congestion in peak hours.
- Improve video play consistency and reduce video stalling.
- Enable new video service offerings (for example, Binge-on video services).
- Enable customers to select the best sustainable video quality.
- Provide a consistent user experience for the subscriber.

While optimizing the video traffic, the Citrix ADC appliance uses a special mechanism to dynamically pace the video bit-rate and a random sampling technique to estimate the savings from the optimization technique. For more information about the Citrix ADC Video Optimization feature, see Video Optimization. When you integrate Citrix ADC appliance with Citrix Application Delivery Management (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 coll -IPAddress 10.106.76.15 -port 5557 -Transport logstream
2 set appflow param -videoInsight ENABLED
3 add appflow action act1 -collectors coll -videoAnalytics ENABLED
4 add appflow policy appol true act1
5 bind appflow global appol 1
6 enable ns mode ulfd
7 enable feature appflow
```

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:

1. In a web browser, type the IP address of the Citrix ADM virtual appliance (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.

3. Navigate to **Analytics > Video Insight**.

**Note**

The values provided by the legend **OTHER** in the charts represents 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**

August 1, 2019

For a given time frame, Citrix Application Delivery Management (ADM) provides a graph that shows the ratio of optimized to unoptimized video sessions in the time frame. It also displays the percentage of bandwidth saved by optimization. The percentage of bandwidth saved is calculated with the following formula:

\[
\text{Percentage of bandwidth saved} = \frac{\text{Average optimized ABR video Data Volume}}{\text{Average of unoptimized ABR Video Data Volume}}.
\]

To see the percentage of bandwidth saved by optimization, log on to Citrix ADM, navigate to **Analytics > Video Insight**, and click **ABR Video**. Then, in the right pane, select a time frame from the drop-down
Compare the data volume used by optimized and unoptimized ABR videos

August 1, 2019

For a given time frame, Citrix Application Delivery Management (ADM) shows the data volume used by optimized and unoptimized ABR videos, so that you can compare the two volumes.

To see the data volume used by ABR videos, log on to Citrix ADM, navigate to **Analytics > Video Insight** and click **ABR Video**. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click **Go** and select the **Data Volume** tab.

You can use the **Filters** drop-down 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

August 1, 2019

The Citrix ADC appliance detects the encrypted or unencrypted video traffic in your network and the type of video streaming (PD or ABR). Citrix Application Delivery Management (ADM) displays these metrics and the data volume consumed by the video traffic for a defined time frame.

To see the types of videos and the consumed data volume, log on to Citrix ADM, navigate to Analytics > Video Insight and click Video Classification. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click Go.

You can use the Filters drop-down list to select the HTTP, HTTPS, or QUIC traffic.
The **Data Volume** tab provides a line graph and pie chart showing the types of video traffic streaming from your network and the data volume consumed by your network. You can hover your mouse pointer on the line graph to view the data consumed during a particular time frame:
Also, you can hover your mouse pointer on the pie chart to view the percentage of data volume consumed by a particular type of video traffic.
Compare optimized and unoptimized play time of ABR videos

August 1, 2019

For a given time frame, Citrix Application Delivery Management (ADM) provides the play time of ABR videos and also enables you to compare the play time of optimized and un-optimized ABR videos in your network.

To view the play time, log on to Citrix ADM, navigate to Analytics > Video Insight and click ABR Video. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click Go and select Play Time tab.

You can use the Filters drop-down list to select the HTTP, HTTPS, or QUIC ABR videos.
For the selected time frame, the **Play Time** tab provides a line graph and pie chart describing the:

- Total play time of ABR videos from your network
- Total play time of optimized and unoptimized plays of ABR videos from your network for the selected time frame.
- Total play time of encrypted and unencrypted ABR videos.
- Average play time of ABR videos
- Average play time of optimized and unoptimized plays of ABR videos
- Average play time of encrypted and unencrypted ABR videos
- Play time distribution between optimized and unoptimized ABR videos
Compare bandwidth consumption of optimized and unoptimized ABR videos

August 1, 2019

For a given time frame, Citrix Application Delivery Management (ADM) provides the bandwidth consumed by optimized and un-optimized of ABR videos and also enables you to compare the bandwidth consumed by optimized and un-optimized ABR videos in your network based on:

- Play Time
- Data Volume

To view the bandwidth consumption, log on to Citrix ADM, navigate to Analytics > Video Insight and click ABR Video Analytics. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click Go and select Bandwidth tab.

You can use the Filters drop-down 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

August 1, 2019

For a given time frame, Citrix Application Delivery Management (ADM) shows the number of plays
of ABR videos and enables you to compare the number of optimized and unoptimized plays in your network.

To see the number of plays, log on to Citrix ADM, navigate to Analytics > Video Insight, and click ABR Video Analytics. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click Go and select # of Plays tab.

You can use the Filters drop-down 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

August 1, 2019

Citrix Application Delivery Management (ADM) shows you the peak throughput or data rate of the video traffic in your network.

To see the peak data rate of the video traffic, log on to Citrix ADM, navigate to Analytics > Video Insight, and click Video Classification. Then, in the right pane, select a time frame from the drop-down list. You can further customize the time frame by using the time-frame slider. Click Go and select Peak Data Rate tab.

You can use the Filters drop-down 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.
Secure Web Gateway Analytics

August 1, 2019

A Citrix Secure Web Gateway (SWG) appliance at the edge of the enterprise network acts as an internet proxy. The appliance can operate in transparent proxy mode or explicit proxy mode and offers controls to intercept internet traffic, including HTTPS. A decision to intercept, bypass, or block any requests is made based on the policies configured on the appliance. A user is authenticated before logging on to the enterprise network. All requests and responses are tagged to the user and the user activities are logged in the appliance. For more information, see Citrix Secure Web Gateway.

When you integrate the Citrix Application Delivery Management (ADM) with a Citrix SWG appliance, the logged user activity and the subsequent records on the appliance are exported to Citrix ADM by using logstream. Citrix ADM collates and presents information on the activities of users, such as, websites
visited and the bandwidth spent. It also reports bandwidth use and detected threats, such as malware and phishing sites. You can use these key metrics to monitor your network and take corrective actions with the Citrix SWG appliance.

**To integrate a Citrix SWG appliance with Citrix ADM:**

1. On the Citrix SWG Appliance, while configuring the Secure Web Gateway, enable **Analytics** and provide the details of the Citrix ADM instance that you want to use for analytics.
2. In Citrix ADM, add the Citrix SWG appliance as an instance to Citrix ADM. For more information see, [Add Instances to Citrix ADM](#).

**Dashboards**

August 1, 2019

May 24, 2018

Citrix Application Delivery Management (ADM) provides two dashboards, the **Outbound Traffic Dashboard** and **User Dashboard**. These dashboards display multiple charts that summarize the websites or applications accessed from the enterprise network and also the activities performed by the users in your network.

**Outbound Traffic Dashboard**

The **Outbound Traffic Dashboard** provides a summary of the URLs or Domains accessed from your network. It provides a holistic view of the all the URLs or Domains by number of transactions or data volume consumed by the URLs or Domains.

It also provides details such as the following:

1. Amount of bandwidth consumed by the URLs or domains accessed from your network.
2. Number of transactions that occurred while accessing the URLs and domains from your network.
3. Number of SSL connections intercepted by the Citrix SWG appliance during the transactions.
4. Number of SSL connections not intercepted by Citrix SWG appliance during the transactions.
5. Number of SSL connections reset by the Citrix SWG appliance during the transactions.
6. Amount of web traffic transmitted, based on the port used to transmit the traffic, the protocol used by the web traffic, and the client operating systems used to transmit the traffic.
To access the Outbound Traffic Dashboard, navigate to Applications > Outbound Traffic Dashboard.

View the Outbound Traffic from the Network

The Outbound Traffic Dashboard includes an Outbound Traffic Overview pane. In the Outbound Traffic Overview pane, Citrix ADM groups the accessed URLs or domains into categories, such as Shopping, News, Social Networking, and so on. The Outbound Traffic Overview pane displays the URLs or domains accessed from your network as nodes in the URL categories. The nodes are sized according to the data volume consumed by accessing the URL or domain. The color of the node indicates the number of transactions that occurred while accessing the URL or domain.
You can click on a category to filter the charts to display details related to the category for the specified time frame.

**User Dashboard**

The **User Dashboard** displays a summary of the activities performed by the users in your enterprise. It provides key metrics that you can use to determine the following:

1. Browsing behavior of users in your enterprise.
2. URL categories accessed by the users in your enterprise.
3. Top five users, based on their risk scores and the bandwidth they consume. For more information about risk score, see Risk Score.
4. Browsers used to access the URLs or domains.
5. Amount web traffic generated by the users, based on the traffic reputation score.

To access the **User Dashboard**, navigate to **Users > Dashboard**.
You can click on a user in the **Top Users** pane to filter the charts to display details of the web activity performed by the user in the specified time frame.

**User Activity Investigator**

The **User Dashboard** includes a **User Activity Investigator** pane displaying various web activities performed by the users. It shows the URL categories accessed by the users during the selected time frame, and various events triggered per URL category. You can click on the events to get the transaction level details.

The **User Activity Investigator** displays key information such as browsing behavior of the user, high risk activity by the user, and triggered events, per URL category. The events are shown as rectangular legends on the chart. Each of the legends is aggregated at one-minute intervals if the selected duration is one hour, and at one-hour intervals if the selected duration is one day.
These legends are aggregated, and are color coded according to the number of events that have occurred. You can hover your mouse pointer on a legend to show details such as time and the number of events aggregated for the selected legend. You can customize the time period of the graph by selecting a time from the time-period drop down.

You can click on the events to further drill down for the details of the transactions.

**User Transactions**

The User Transactions page displays the details of the user transactions in your network. It provides transaction-level details such as:

1. Time at which the transaction occurred
2. Protocol used for the transaction
3. User name
4. Domain that was accessed by the user
5. URL category

6. Proxy server used to intercept the transaction

7. Client port details

8. Bytes In

9. Bytes Out

**Summary panel**

The **Summary Panel** displays all the metrics of the transactions that are visible in the **Transaction Details** pane. This panel enables you to sort and view the transactions in the **Transaction Details** pane by selecting or deselecting the metrics. The **Summary Panel** displays the following metrics:

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>Protocols used in the transactions</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports used for the transactions</td>
</tr>
<tr>
<td>URL Reputation</td>
<td>URL reputation score</td>
</tr>
<tr>
<td>Browsers</td>
<td>Browsers used for the transactions</td>
</tr>
<tr>
<td>Operation System</td>
<td>Operating system used for the transactions</td>
</tr>
<tr>
<td>Bytes In</td>
<td>Amount of data received through the Citrix SWG Appliance.</td>
</tr>
</tbody>
</table>
Bytes Out

Amount of data sent through the Citrix SWG Appliance.

**Risk Score**

Risk Score is a scoring system used in Citrix ADM to determine the risks associated with users in your enterprise. Citrix ADM assigns a risk score based on the URL reputation score assigned by the Citrix SWG appliance for the URLs accessed by the users in your network. For information on URL reputation score, see [URL Reputation Score](#). The following table describes the Risk Scores assigned by Citrix ADM.

<table>
<thead>
<tr>
<th>Risk Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The web activity of the user has no perceived threat or is not abnormal.</td>
</tr>
<tr>
<td>2</td>
<td>The web activity of the user has no perceived threat or is not abnormal, but the user is accessing “Unknown Sites,” which do not have URL reputation scores.</td>
</tr>
<tr>
<td>3</td>
<td>No threat is detected in the web activity of the user, but the user has attempted to access sites that are potentially vulnerable or affiliated with sites that are potentially vulnerable.</td>
</tr>
<tr>
<td>4</td>
<td>Potentially compromised user.</td>
</tr>
<tr>
<td>5</td>
<td>The web activity of the user is abnormal and the user has accessed known malicious sites.</td>
</tr>
</tbody>
</table>

**Use cases**

August 1, 2019
Monitoring the SSL Interceptions

A Citrix SWG appliance enables you to inspect your encrypted outbound traffic. You can intercept, bypass, or block any HTTPS requests on the basis of policies configured on the appliance. Citrix Application Delivery Management (ADM) provides the following details about the SSL connections in the Outbound Traffic Dashboard for a selected time frame:

- Number of SSL connections that are intercepted, not intercepted, and reset by the Citrix SWG appliance
- Transaction details of the SSL connections

Using these details, you can further fine tune the policies on your Citrix SWG appliance to efficiently inspect the encrypted outbound traffic. For more information, see Citrix Secure Web Gateway.

To display the number of SSL connections that have been intercepted, not intercepted, and reset:

Navigate to Applications > Outbound Traffic Dashboard. The Outboard Traffic Dashboard displays the number of SSL connections that are intercepted, not intercepted, and reset.

To display the transaction details of the SSL connections that have been intercepted:

1. Navigate to Applications > Outbound Traffic Dashboard.
2. On the Outboard Traffic Dashboard, click the total count in the SSL INTERCEPTS section.
The transaction details of the SSL connections that were intercepted during the selected time frame are displayed on the **Transaction Details** page.

You can further filter the transactions details by user and URL category.

**To view the transaction details of the SSL connections on which traffic was not intercepted:**

1. Navigate to **Applications > Outbound Traffic Dashboard**.
2. In the **Outbound Traffic Dashboard**, click the total count in the **Not-intercepted SSL Connections** section.
The transaction details of the SSL connections on which traffic was not intercepted during the selected time frame appear in the **Transaction Details** page.

You can further filter the transactions details by user and URL category.

**To display the transaction details of the SSL connections that are reset:**

1. Navigate to **Applications > Outbound Traffic Dashboard**.

2. On the **Outboard Traffic Dashboard**, click the total count in the **Reset SSL Connections** section.
The transaction details of the SSL connections on which traffic was not intercepted during the selected time frame appear on the Transaction Details page.

You can further filter the transactions details by the user and URL category.

**Inspecting Endpoints**

The policies you have configured on a Citrix SWG appliance specify how the appliance logs all the user activities performed in your enterprise. Citrix ADM provides key metrics that you can use to determine:

1. Browsing behavior of users in your enterprise.
2. URL categories accessed by the users in your enterprise.
3. Top five users, based on their risk scores and the bandwidth they consume. For more information about risk scores, see Risk Score.
4. Browsers used to access the URLs or domains.

5. Amount web traffic generated by the users, based on the traffic reputation score.

For example, if a user with user id testuser3 constantly accesses malware related sites in your enterprise, Citrix ADM identifies the user as high-risk activity user and assigns a higher risk score. The testuser3 information is displayed in the Top Users section of the User Dashboard.

![Top Users Table]

You can click on testuser3 to filter the User Dashboard to display all the key metrics related to testuser3.
In the User Activity Investigation pane, the high-risk activity of testuser3 is displayed as events in the respective URL categories.
You can hover over the events to display the number of events, and you can click on events to investigate the transactions that occurred during the events.
With this information, you can determine whether the user’s system is infected by malware, or you can understand the bandwidth consumption pattern of the user and fine-tune your Citrix SWG policies. For more information, see Citrix Secure Web Gateway Documentation.

**Reporting Bandwidth Consumption**

The **Outbound Traffic Dashboard** and the **User Dashboard** provide multiple charts that summarize the websites or applications accessed from the enterprise network, and the activities performed by the users in your network.

The **Outbound Traffic Dashboard** provides the details of data-volume consumption by the URLs or domains that were accessed from your network. Navigate to **Applications > Outbound Traffic Dashboard**, where the data volume details are shown in the **Data Volume** section.
In the Outbound Traffic Overview pane, you can click on a domain or URL to display the details of the data volume consumed by the domain or URL.

The User Dashboard provides details about the bandwidth consumed by the users in your network. Navigate to Users > Dashboard to display the details of the bandwidth consumed by users in the DATA...
**VOLUME** section in the User Dashboard.

You can view the details of the bandwidth consumed by a user by selecting the user from the **Top Users** section. The **DATA VOLUME** section and other key metrics in the chart are filtered for the selected user.

Using these details, you can understand the bandwidth consumption and the reason for the consumption. For example, if a user is accessing social networking websites and this has caused a lot of bandwidth consumption, the administrator can access the Citrix SWG appliance and configure a URL List...
feature to control access to the websites. For more information, see Use Case: URL Filtering by using Custom URL Set topic.

**Viewing Outbound Traffic Distribution**

The Citrix SWG appliance provides URL categorization and filtering features that you can use to categorize the URLs that are accessed from your network. In Citrix ADM, the Outbound Traffic Dashboard includes an Outbound Traffic Overview pane. In the Outbound Traffic Overview pane, Citrix ADM groups the accessed URLs or domains into categories, such as Shopping, News, Mobile, and so on to show the outbound traffic distribution in your network. For a selected time frame, you can click on the URL, to understand the:

1. Bandwidth consumed by accessing the URL
2. Transactions that occurred while accessing the URL
3. Number of SSL connections that were intercepted, not intercepted, and reset while accessing the URL

With this information, you can understand the outbound traffic pattern and make corrective decisions, such as whether to block certain URLs.

**To view Outbound Traffic Distribution:**

Navigate to Applications > Outbound Traffic Dashboard. The Outboard Traffic Dashboard displays the URLs in the Outbound Traffic Overview pane:
If you want to view the details of a particular URL, select the URL.

Using this information, you can understand the outbound traffic pattern and control your network traffic using a URL Filter configured on your SWG appliance. For more information, see URL Filtering.

Orchestration

August 1, 2019

In Software Defined Networking (SDN), a software application controller manages a network and its activities instead of hardware that supports the network. That is, SDN allows the network administrators to virtualize a physical network connectivity into a logical network connectivity and manage network services using a software based centralized management tool. SDN allows network engineers and administrators to respond to rapidly changing business requirements.

While the better known advantages of SDN are traffic programmability, greater agility, the ability to create policy driven network supervision, and implementing network automation, some of the specific advantages of SDN are listed below:

- Centralized network provisioning
- Increased network security at granular level
- Reduced operating costs
Citrix Application Delivery Management (ADM) supports SDN in enterprises network by integrating with SDN controllers of different vendors. Citrix ADM supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

**VMware NSX Manager**

Citrix ADM integrates with VMware network virtualization platform to automate the deployment, configuration, and management of Citrix ADC services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter administrators to programmatically deploy Citrix ADC services faster.

VMware NSX Manager exposes logical firewalls, switches, routers, ports, and other networking elements to allow virtual networking among diverse hypervisors, cloud management systems, and associated network hardware. It also supports external networking, and security services.

The Cloud Orchestration feature of Citrix ADM enables the integration of Citrix ADC products with VMware NSX, and provides the following capabilities:

- Ability to allocate a pre-provisioned VPX on-demand to a certain Edge gateway as part of service insertion.
- Ability to configure advanced features of Citrix ADC such as SSL and CS along with basic load balancing through application templates on the instances that are running inside NSX environment.
- Ability to de-allocate a VPX from a certain Edge gateway as part of service deletion and re-allocate the same VPX for another Edge gateway.
- Ability to rapidly deploy Citrix ADC functions from the vCenter console as part of the deployment workflow of all the infrastructure required for an application.

**Benefits:**

- Automated, on-demand allocation of new ADC services as part of an application deployment workflow
- Simplified configuration of application specific, advanced ADC functionality through application templates
- Multi-tenant separation-of-duties and a self-service consumption model while providing cloud administrators a single point of control
- Easier integration with Citrix ADM API’s, which help to support unanticipated future uses.
For more information on how to configure VMware NSX Manager on Citrix ADM, see Integrating Citrix ADC Appliances with VMware NSX Manager.

Cisco ACI Hybrid Mode

Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to Citrix ADM, which acts as a Device Manager in the APIC.

The Citrix ADC Hybrid Mode solution is supported by a hybrid mode device package and Citrix ADM. You need to upload the hybrid mode device package in the APIC. For more information, see Citrix ADC Automation Using Citrix ADM in Cisco ACI's Hybrid Mode.

OpenStack: Integrate Citrix ADC instances

August 1, 2019

The Cloud Orchestration feature of Citrix Application Delivery Management (ADM) enables integration of Citrix Citrix ADC products with OpenStack platform. By using this feature with OpenStack platform, the OpenStack users are able to avail the load balancing feature (LBaaS) of the Citrix ADC. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in Citrix ADC instance. The following sections provide a brief description of the features in Citrix ADM and OpenStack integration workflow.

Citrix ADC Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plugin includes a Citrix ADC driver that enables OpenStack to communicate with the Citrix ADM. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the Citrix ADM, which creates the load balancer configuration on the desired Citrix ADC instances. OpenStack also uses the driver to call Citrix ADM at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the Citrix ADCs. Citrix ADC driver software for OpenStack platform is bundled along with the Citrix ADM. To download and install the drivers, you have to first install Citrix ADM and launch the application.

Register Citrix ADM and OpenStack with each other

You have to first register OpenStack information on the Citrix ADM. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack Citrix ADC driver user
credentials. You can later specify the same login credentials in the Citrix ADC_driver section of the
Neutron configuration file (neutron.conf) so that Citrix ADC driver in OpenStack can connect to Citrix
ADM during LB configurations.

After OpenStack and Citrix ADM are registered with each other, both can talk to each other. Also, Open-
Stack users can use their existing credentials in OpenStack to log on to the Citrix ADM user interface
to check how their LB configurations are performing in Citrix ADCs.

**Tenants in OpenStack**

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

**Placement policies**

Placement policies provide the flexibility to decide on the Citrix ADC instance that is used in each load balancer configuration created by users. Alternatively, the Citrix ADM also provides an option to assign a Citrix ADC instance based on OpenStack tenants.

**Service packages**

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
- Multiple tenants can be associated with the same service package.
- In a service package that is set for auto-provisioning, virtual Citrix ADC instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

**Features supported on LBaaS V1 and LBaaS V2**

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
Use case scenario

The following use-case scenario explains the workflow of integrating Citrix ADM with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider’s cloud infrastructure. Tom’s organization, Example-SportsOnline.com, requires two servers S1 and S1, and Tom also requires a dedicated Citrix ADC device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and Citrix ADM, and prepare them to work with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.
Steve has to register OpenStack details with Citrix ADM, and configure the Citrix ADC LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, Citrix ADM displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the Citrix ADC LBaaS features and configure Tom to get a dedicated Citrix ADC allotted for his load balancer configurations in Citrix ADM.

For this, Steve can either provision a Citrix ADC VPX instance on the computing layer (Nova) of OpenStack using Citrix ADM user interface or enable MAS to auto-provision a Citrix ADC VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, Citrix ADM manages the VPX instance. For achieving this, Steve creates a service package in Citrix ADM, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the ‘dedicated’ isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many Citrix ADC VPX instances to the service package, and associates Example-SportsOnline, along with other tenants, who require a dedicated Citrix ADC with the service package. As a result, when Tom performs his first load balancer configuration, Citrix ADM allots one of the Citrix ADC VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that Citrix ADC.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and virtual servers on the Citrix ADC instance. Tom can also create health monitors to monitor the servers, and send application traffic to only those servers which are UP at any point of time and reachable from Citrix ADC.

The load balancing configuration created in OpenStack is now implemented on the Citrix ADC instance. Once fully configured, the Citrix ADC VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

**Citrix ADM integration with OpenStack workflow**

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.
Prerequisites

August 1, 2019

Before you integrate the Citrix ADC virtual instance with OpenStack platform, ensure that the following requirements are met:

Citrix ADM and OpenStack Software Requirements

- Citrix ADM 12.1 is installed on a supported hypervisor workstation that meets the minimum hardware requirements system.
- OpenStack components are installed and running.
- Citrix ADM 12.1 supports the following OpenStack versions - Newton, Ocata, and Pike.

Citrix ADM Hardware Requirements

The following table lists the virtual computing resources that you should have on your OpenStack server to install Citrix ADC virtual instances.
### Component Requirement

<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>8</td>
</tr>
<tr>
<td>Storage Space</td>
<td>500 GB</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Note**

The memory and hard disk requirements specified above are for deploying Citrix ADM on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depends on the number of virtual machines running on it.

---

### Pre-configuration tasks in Citrix ADM and OpenStack

August 1, 2019

This section assists you to perform the pre-configuration tasks before you configure Citrix Application Delivery Management (ADM) and OpenStack.

#### Installing Citrix ADM

Install Citrix ADM on a supported hypervisor. For more information on how to download and install Citrix ADM, see Deploying Citrix ADM.

#### Installing the Citrix ADC driver software and registering Citrix ADM on OpenStack

Download the Citrix ADC bundle for OpenStack from the Citrix ADM Downloads page.

**To install Citrix ADC driver on OpenStack platform using Citrix ADM GUI:**

1. In Citrix ADM, click Downloads. The Downloads page in Citrix ADM provides you links to download Citrix ADC bundle for OpenStack software required for Newton, Ocata, and Pike OpenStack versions.
2. Download the latest Citrix ADC bundle tar file to a temporary directory (for example, /tmp) in OpenStack Controller. This bundle includes the LBaaS V2 driver and Heat plug-in for all OpenStack releases.

3. Run the following command to extract the files from the Citrix ADC driver tar file:
   ```shell
tar -xvzf <name_of_tar_file>
```

4. If you have an OpenStack <Release Name> setup, at the prompt, type the following command:
   ```shell
cd <Release Name>
```
   **Example:**
   ```shell
cd Newton
```

5. Run the following command to install the driver and specify the Citrix ADM IP address, the Citrix ADC driver password that you configured when you registered OpenStack with Citrix ADM, and the protocol:
   ```shell
./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
```
   **Example for single node OpenStack setup:**
   ```shell
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
```
   **Example for multinode OpenStack setup:**
   ```shell
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

   **Note**
   Providing the path of the neutron-lbaas directory of the system is optional. Providing the path might assist the script to find the drivers.

   After Citrix ADM is registered successfully on OpenStack, you can log on to Citrix ADM using your OpenStack user credentials also.

   After Citrix ADM is registered successfully on OpenStack, restart the OpenStack Neutron services.

**Registering OpenStack with Citrix ADM**

**To register OpenStack with Citrix ADM using Citrix ADM GUI:**
1. In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > OpenStack**.

2. Click **Configure OpenStack Settings**.

3. In **Configure OpenStack Settings** page, you can set the parameters to configure OpenStack in Citrix ADM. You have two options here - Default and Customized.

   For Newton and Ocata releases of OpenStack, you can use either default or customized deployment type. But for Pike release, you must use customized deployment type to register OpenStack with Citrix ADM.

   - **Default Deployment Type**
     
     Select **Default**, if the OpenStack services are running on default ports. For example, the default portal for Neutron services is 9696, the default portal for Keystone services is 5000.

     1. OpenStack Controller IP Address - IP address of the OpenStack controller (both the KeyStone service and the Neutron service should be reachable on this IP address). For example, enter the IP address 10.102.205.23.
     
     2. OpenStack Admin Username - administrative username of the OpenStack controller. For example, enter admin1.
     
     3. Password - password of the administrative user of the OpenStack controller.
     
     4. OpenStack Admin Tenant - the name of the administrative tenant on OpenStack. For example, enter admin.

     ![OpenStack Details](image)
**Customized Deployment Type**

Select deployment type as **Customized** if the OpenStack services are running on ports different from the default ports. If these services are running on different ports, specify them here. Registering OpenStack Newton and Ocata releases with Citrix ADM is different from registering OpenStack Pike release.

**Newton and Ocata Release of OpenStack:**

1. Specify the port numbers for the various OpenStack services if you are registering Newton release of OpenStack.

2. Specify the OpenStack Admin username, password, and OpenStack Admin Tenant username as you had specified earlier in the **Default** settings.

**Pike Release of OpenStack:**

If you are registering the Pike release of OpenStack enter the details of the OpenStack services
as shown in the following image. You must also specify the OpenStack Admin username, password, and OpenStack Admin Tenant username as in Default settings.

1. In **OpenStack Neutron LBaaS - Credentials Used by Citrix ADC Driver** section, set the Citrix ADC Driver Password for the OpenStack Citrix ADC driver user account. Citrix ADM authenticates the calls from the OpenStack Citrix ADC driver by using these credentials. You must specify the same password when you execute the Citrix ADC driver installation script in the OpenStack controller.

2. Click **OK**.

**Creating a tenant on OpenStack**

Create a project or a tenant on OpenStack, add users to the project or tenant, and assign roles to all of the users. KeyStone, the Identity service in OpenStack provides authentication services for each OpenStack service. The authentication service uses a combination of domains, projects (tenants), users, and roles.

For more information on how to create a project, and to perform other tasks in OpenStack, see the OpenStack documentation at [http://docs.openstack.org/](http://docs.openstack.org/).

**Adding OpenStack tenants**

1. In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > OpenStack > OpenStack Tenants**, and then click **Add**.

2. In **Add OpenStack Tenants** page, click **+Add**, and then select the OpenStack tenant.

3. Click **OK**.

Based on whether you are using pre-provisioned instance or auto-provisioning the instance when you are integrating the OpenStack, follow one of these two tasks:

- Pre-provision the Citrix ADC Devices
- Auto-provision the NetScaler VP X devices on OpenStack

**Provisioning Citrix ADC devices**

Based on whether you are using pre-provisioned instance or auto-provisioning the instance when you are integrating the OpenStack, follow one of these two tasks:

- Pre-provision the Citrix ADC Devices
- Auto-provision the NetScaler VP X devices on OpenStack
Pre-provisioning Citrix ADC devices

Install the Citrix ADC device on any of the hypervisor platforms like Citrix Hypervisor, KVM, or ESX, and add the instance to Citrix ADM. Citrix ADM then manages this device that load balances the traffic in the servers.

To add an existing Citrix ADC VPX instance in Citrix ADM:

1. In Citrix ADM, navigate to Infrastructure > Instances > Citrix ADC VPX, and then click Add.
2. On the Add Citrix ADC VPX page, specify the IP address of the Citrix ADC VPX instance and select an instance profile from the Profile Name list. The instance profile contains the credentials used to logon to the Citrix ADC VPX. You can also create a new instance profile by clicking the + icon. Click OK.

Autoprovisioning Citrix ADC devices

Download the required Citrix ADC instance image from the Citrix download page, and upload it on Glance, the OpenStack Imaging service. Having an image available on Glance allows you to configure a Citrix ADC instance on-demand when assigning the instance to the tenant.

To auto-provision the Citrix ADC VPX devices on OpenStack:

1. In Citrix ADM, navigate to Orchestration > Cloud Orchestration > OpenStack.
2. Click Deployment Settings.
3. Set the following parameters:
   a) Management Network - select the management network on OpenStack, to which the auto-provisioned Citrix ADC VPX is connected.
   b) Profile Name - select the profile from the drop-down list. The Citrix ADM uses the password contained in this profile to configure new auto-provisioned Citrix ADC VPX instances.
   c) Licenses - provide the Citrix ADM license activation codes (LAC) used to license new auto-provisioned Citrix ADC instances. Citrix ADM provisions Citrix ADC instances on OpenStack compute in management network, then triggers license installation on them using the specified license code. The Citrix ADC instance then downloads the license files from Citrix website using the LAC specified here.
   d) Citrix ADC VPX Image in Glance - select the Citrix ADC VPX image available in the OpenStack Glance that is used to create a Citrix ADC VPX instance.
   e) Proxy Settings - provide details of Citrix ADC proxy server for installing licenses. This may be required when Citrix ADC does not have direct access to the Internet through the management network.
4. Click **OK**.

**Deployment Settings**

**Instance Provision Settings**

Application Delivery Management can be configured to create and destroy Citrix ADC instances dynamically through service instances on the fly.

Management Network (Neutron network)*

- public - 2001:db8::/64

**Credentials configured in Citrix ADC instances provisioned by Application Delivery Management**

During creation of new Citrix ADC instances, the default password is changed to the password mentioned below. Application use this password to login to the instance after it is created.

Profile Name*

- ns_vxrooot_profile

**Settings to provision Citrix ADC VPX instances using OpenStack Compute Service (Nova)**

Citrix ADC VPX image in OpenStack Imaging Service (Glance)

- ns_vpx_12.1

**Proxy for License Installation**

Server Name/IP Address

Port

**Network Provision Settings**

- ADM to provision selected instance in appropriate VIP and Pool networks
- Provision both VIP and Pool networks
- Provision only VIP network and route pool traffic through VIP network

**Creating a service package in Citrix ADM**

**To create service packages for a tenant in Citrix ADM:**

1. In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, and then click **Add**.

2. On the **Service Package** page specify the following parameters:
   a) Name - name for the service package. For example, enter SVC-PKG-GOLD.
b) Citrix ADC Instance Allocation - the type of instance allocation defined in the service package based which Citrix ADC instance resources are allocated to a tenant. Select Dedicated. For more information on policies, see Service Package Isolation Policies.

c) Citrix ADC Instance Provisioning - select Existing Instance to allocate an existing Citrix ADC instance to a tenant. If you want to create Citrix ADC instances during the configuration itself, select Create Instance OnDemand.

d) Citrix ADC Instance Type - select Citrix ADC VPX.

Note
Select Citrix ADC VPX to allocate pre-provisioned Citrix ADC instances hosted on SDX platform.

3. Click Continue to associate a tenant with a service package.

Note
Enable Provision pair of Citrix ADC instances for high availability, if you are deploying the Citrix ADC instances in high availability mode.

4. In Assign Instances section, click Add, and then select the Citrix ADC instance that you want to assign to the tenant, and click Continue.

5. In Assign OpenStack Tenants/Placement Policies section, under OpenStack Tenants, click Add, and select the tenant.

6. Click Continue, and then click Done.

Note
If the policy is not found, the fallback mechanism is revived, and the Citrix ADM assigns Citrix ADC instances based on tenants. If the tenant is not part of any service package, the Citrix ADM displays an error message that says: “Tenant <admin> is not part of any Service Package and there is no default Service Package.”

Creating placement policies (optional)

Isolation Policies are not tenant-based only. You can create flexible placement policies, where the policies are not only based on tenant name or id, but on other custom attributes also.

To create placement policies for a tenant in Citrix ADM:

1. In Citrix ADM, navigate to Orchestration > Cloud Orchestration > OpenStack > Placement Policy, and then click Add.

2. On the Add Placement Policy page, set the following parameters:
a) Name - type a name for the placement policy

b) Sample Expressions - select a sample expression from the list. These examples are helpful to construct the placement policy.

c) Expression - a Boolean expression is populated in this field based on the sample expression that you have selected in the earlier field. Edit the field names as required.

3. Click OK.

Enabling traffic from Citrix ADC instances to backend servers through client network

By default, in the OpenStack orchestration workflow, Citrix ADC instances are dynamically bound to the load balancer or client networks and member or server networks.

In certain deployments servers are also reachable through client networks and can be routed through the client gateway. In such cases, the Citrix ADC instances need not be bound to server networks, but they need to be bound only to client networks.

Perform the following setting to configure traffic through client gateway.

Navigate to Orchestration > Cloud Orchestration > OpenStack > Deployment Settings, and then select the Provision only VIP network and route pool traffic through VIP network option.

Citrix ADM then configures the Citrix ADC instance to client networks by adding a SNIP in that network, and will further add a default route to the client network gateway. This enables the instance to reach the servers through the client gateway.

Auto-provisioning Citrix ADC VPX devices deployed on Citrix ADC SDX platform

Add the Citrix ADC SDX platform in Citrix ADM, so that Citrix ADM provisions the instances on this platform on-demand.

To auto-provision Citrix ADC instances deployed on Citrix ADC SDX platform:

1. In Citrix ADM GUI, navigate to Networks > Instances > Citrix ADC SDX, and click Add to add a Citrix ADC SDX platform.

2. Navigate to Orchestration > Cloud Orchestration > OpenStack > Deployment Settings.

3. In Management Network section, select the management network on OpenStack to which the auto-provisioned Citrix ADC SDX is connected.

   a) In Profile Name, select the profile from the drop-down list. The Citrix ADM uses the password contained in this profile to configure new auto-provisioned Citrix ADC VPX instances.

   b) Click OK.
4. To provision the Citrix ADC SDX platform in OpenStack, navigate to **Orchestration > Cloud Orchestration > OpenStack> Service Package**.
   a) Click **Add** to create a new service package.
   b) Enter the name of the service package.
   c) In **Citrix ADC Instance Allocation** field, select **Dedicated**.
   d) In **Citrix ADC Instance Provisioning** field, select **Create Instance OnDemand**, and in **Auto Provision Platform** field, select **Citrix ADC SDX**.
   e) By default, only Citrix ADC VPX instances are provisioned on Citrix ADC SDX platform.
   f) Click **Continue**.
   g) In **Auto Provision Settings** section, set the **Resources** properties.
      i. **Throughput** field. Enter 1000 Mbps.
      ii. **Citrix ADC Version** field. From the list, select the right version of the Citrix ADC VPX image present on the Citrix ADC SDX platform. Configure LBaaS V2 using command line
   h) In **Citrix ADC SDX Platforms** section, click **Add** to add the SDX platform to the service package.
   i) Click **Continue**.
   j) In **Configure OpenStack Tenants** section, click **Add** to add the tenants. You can also add new tenants by clicking **New**.
   k) Click **Done**.

5. LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and execute the configuration tasks. For more information on how to execute configuration commands, see **Configuring LBaaS V2 using Command Line**.

**Configure LBaaS V1 using Horizon**

August 1, 2019

Tom can now log on to the OpenStack Horizon portal and create an LBaaS pool and select a subnet where all the members of this pool are located in. Tom has to add a virtual IP (VIP) address and assign this VIP to the pool that he has created. Tom can also perform this on command line or through APIs. External clients for Tom’s servers can connect to this VIP address, which is hosted on the assigned Citrix ADC, and Citrix ADC distributes all requests to the pool members on the configured ports.
LBaaS pool members are the load balanced servers that are added to the selected pool. Tom can assign a weight and a port to each of these members.

Health monitors are used to watch the health and good functioning of all members of the pool. Tom can create a health monitoring template in OpenStack by specifying delay, timeout, and retry limits, and also specify method, URL path, and expected HTTP codes upon success. After creating a monitor, Tom has to associate the monitor with the pool that was previously created.

For more information on how to create a pools, and other LBaaS configuration tasks in OpenStack, see OpenStack Documentation.

Important
LBaaS V1 is not supported in Liberty release of OpenStack. For more information, see OpenStack Release Notes.

Configure LBaaS V2 using command line

August 1, 2019

LBaaS V2 supports SSL offload with certificates managed by Barbican, certificate bundles (includes intermediary Certification Authorities), SNI support along with the regular load balancing features. LBaaS V2 supports only command line interface to execute configuration tasks. LBaaS V2 API implementations are performed through Neutron LBaaS commands.

Note
Upload certificate and key to Barbican service when you require SSL offloading feature. Perform steps 1, 2, and 3 if SSL offloading is supported, else continue from step 4 to create a load balancer, a listener, a pool and a member.

1. Upload certificate to Barbican service using the following command:

   ```bash
   barbican secret store --payload-content-type <content_type> --name <certificate_name> --payload<certificate_location>
   ```

   **Example:** barbican secret store --payload-content-type='text/plain' --name='hp_server_certificate' --payload=" hp_server/tmp/server_certificate"

© 1999-2019 Citrix Systems, Inc. All rights reserved.
2. Upload key to Barbican service using the following command:

```bash
barbican secret store –payload-content-type <content_type> –name <key_name> –payload <key_location>
```

**Example:** `barbican secret store –payload-content-type='text/plain' –name='shp_server_key' –payload='hp-server/tmp/server_key'

**Note**

When you execute these two Barbican commands to load the certificate and the key, the Secret href fields provide a location or url. This is where the certificate and the key are stored on the system where OpenStack is installed. Copy these links and provide these links as parameters when you create the container on Barbican service in step 3.

3. Create a container in Barbican service to store the certificate and the key using the following command:

```bash
barbican secret container create –name <container_name> –type <container_type> –secret <certificate_url> –secret <key_url>
```

**Example:** `barbican secret container create –name='hp_container' –type='certificate' –secret='http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret='private\_key=hp-server/tmp/server_key'`
Copy the container href value. You have to provide the link to the container when creating the listener in step 6.

4. Set the environment variables in OpenStack. The variables enable the OpenStack client commands to communicate with the OpenStack services.

   **Example:**
   
   ```
   export OS_PASSWORD=hp
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
   export OS_USERNAME=hp_user
   export OS_TENANT_NAME=hp
   export OS_IDENTITY_API_VERSION=2.0
   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
   ```

   **Note**
   
   Set these variables for every SSH session before running other commands. For more information about OpenStack environment variables, see OpenStack environment variables.

5. Create a load balancer using the following command:

   ```
   neutron lbaas-loadbalancer-create --name <loadbalancer-name> <subnet-name> --provider <netscaler>
   ```

   **Example:** neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
The status changes from PENDING_CREATE to ACTIVE after the load balancer is successfully created.

6. Create a listener using the following command:

```bash
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number> --default-tls-container-id <container_url>
```

**Example:**
```
neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
```

**Note**
If you are creating a listener without SSL offload support, execute the following command without providing locations to the container:

```bash
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>
```

---

© 1999-2019 Citrix Systems, Inc. All rights reserved.
7. Create a pool using the following command:

   neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener <listener-name> --protocol <protocol_type> --name <pool-name>

   **Example:** neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener demo-lister --protocol http --name demopool

8. Create a member using the following command:

   neutron lbaas-member-create --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number> <pool-name>

   **Example:** neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool

---

**Monitoring OpenStack Applications in Citrix ADM**

Your tenants can log on to Citrix Application Delivery Management (ADM) using their OpenStack credentials to monitor VIPs and pools created from OpenStack from any browser. The URL should be in the following format:

   `http://\<mas-ip\>/admin\_ui\>/mas/ent/html/cc\_tenant\_main.html`

Where, `<mas-ip-address>`, is the Citrix ADM IP address that is registered with the OpenStack.

**Note**

- OpenStack VIPs correspond to virtual servers in Citrix ADM.
- OpenStack Pools correspond to service groups in Citrix ADM.
Configure layer 7 content switching

August 1, 2019

Citrix Application Delivery Management (ADM) orchestrates with OpenStack to configure the Layer 7 (L7) switching or content-based switching functionalities on Citrix ADC instances. Content switching differs from simple load balancing in that specific types of requests can be directed to specific servers. When the L7 configurations are created in OpenStack with a Citrix ADC instance as the provider, Citrix ADM allots a Citrix ADC instance, and deploys content switching and responder configurations corresponding to the L7 configurations. The Citrix ADC instances can then distribute and load balance user requests on the basis of application-layer characteristics of the requests.

The OpenStack layer 7 (L7) load balancing feature combines load balancing and content switching to provide optimized delivery of specific types of content. This improves the performance of the load balancer by executing only those policies that are applicable to the content. Layer 7 load balancing also facilitates increased efficiency of the application infrastructure. The ability to separate out content according to type, URI, or data allows better allocation of physical resources in the application infrastructure. For example, an end user browsing to http://example-sports.com/about-us should be served by a pool of servers hosting content about the company and the services, while a user browsing to http://example-sports.com/shopping-cart-football should be served by a different pool of servers that allows the users to make online purchases.

In L7 switching, a load balancer is implemented as a content switching virtual server that accepts HTTP requests from users and distributes those requests to the application servers. L7 switching or content switching allows you to have a single-point entry to access a variety of the back-end services (for example, not just web applications, web service portals, web mails, but also mobile management, content in different languages, and so on). That is, you can provide one public IP address for all services you are offering your users.

Unlike lower-level load balancing, Layer 7 switching does not require that all servers in the pool have the same content. A load balancer configuration using L7 switching expects the application or back-end servers from different pools to have different content. L7 switches can direct requests on the basis of URI, host, HTTP headers, or anything else in the application message. The application servers should essentially serve specific types of content. For example, one server could serve only images, another could execute server-side scripting languages, such as PHP and ASP, and another could serve static content such as HTML, CSS, and JavaScript.
L7 Rules

The following attributes are defined in a rule for evaluating the traffic and they are compared against the values defined in the rule:

- **hostname**: The hostname in the HTTP request is compared against the value parameter in the rule. For example, “www.example-sports.com”

- **path**: The path portion of the HTTP URI is compared against the value parameter in the rule. For example, “www.example-sports.com/shopping-cart/football_pump.html”

- **file_type**: The last portion of the URI is compared against the value parameter in the rule. For example, txt, html, jpg, png, xls, and others.

- **header**: The header defined in the key parameter is compared against the value parameter in the rule.

- **cookie**: The cookie named by the key parameter is compared against the value parameter in the rule. The cookie request-header field value contains a name and value pair of information stored for that URL; the general syntax is as follows - Cookie: name=value. For example, a rule that is looking for a cookie named “stores” with the value starting with “football-“ will look like: type = Cookie, compare_type=StartsWith, key = stores value = football-.

Comparison Types

When evaluating the traffic, the L7 policy compares the following expressions against the attributes defined in the rule.

- **regex**: Perl type regular expression matching

- **starts_with**: String start with

- **ends_with**: String ends with

- **contains**: String contains

- **equal_to**: String equals

**Note**

The hostname, path, header, and cookie attributes support all comparison types, but the file_type attribute supports only regex and equal_to.

L7 Policies

An L7 policy processes the incoming HTTP traffic and returns a “true” value when all the rules defined in the policy are matched.
In any L7 policy, all the rules are logically joined with an AND operator. A request must match all the rules so that the policy returns a “true” value. The action taken by the load balancer is based on the value returned by the policy. You can create a second policy with the same action to achieve a logical OR operation between the rules.

For example, you can create one policy where the incoming HTTP request can contain the words “EXAMPLE-SPORTS,” “SPORTS-FOOTBALL,” or “EXAMPLE-FOOTBALL,” so that the load balancer takes the appropriate action of forwarding these requests to the server-pool of the Example-sports ecommerce company to serve the requested content. You can create another policy that takes the same action but matches “example-sports,” “example-sports-football,” or “example-football.” When a user sends an HTTP request with any of these six keywords, the load balancer forwards the request to the Example-Sports server.

Depending on the rules defined in the policy, an L7 policy can take any of the following actions:

- Redirect to pool - Forward the request to the application server pool identified by the rules associated with the L7 policy. That is, you can create an application rule to direct requests to a specific load balancer pool according to domain name. For example, you can create a rule that directs some requests to example-football.com to pool_1, and other requests to example-sports-online_purchase.com to pool_2.

- Redirect to URL - Send the client a redirect HTTP response in which the location response header contains the new location. The browser will update the address bar with the new location and issue a new request. The use cases are many. For example, if a website address has changed, you can redirect requests to the new address instead of dropping. Or, during website maintenance, you can redirect the users to a read-only site.

- Reject - Rejects the request and takes no further action. For example, you can return a 401 Unauthorized response to deny access to the users for restricted web pages.

A content switching configuration consists of a content switching virtual server, a load balancing setup consisting of load balancing virtual servers and services, and content switching policies. After you create your content switching virtual server and policies, you bind each policy to the content switching virtual server. When binding the policy to the content switching virtual server, you specify the target load balancing virtual server. When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. The priority of the policy defines the order in which the policies bound to the content switching virtual server are evaluated.

Any pool that has the listener ID can be assigned as a default pool of virtual servers to which traffic is diverted. The pool is loosely bound with a listener, and becomes associated with a listener only through implementation of an L7 policy. A pool can also be created directly under a load balancer without necessarily being tied to a listener. In such a case, the pool is created in a “pending_create” state. Because the L7 policies are tightly bound with the listeners, an L7 policy containing the pool ID must be created and implemented for the pool to become “active” and start receiving traffic requests.
A pool can be served by multiple L7 policies, but remains in the “active” state if at least one policy is attached to it. When the last policy is removed, the pool goes back into the “pending_create” state until another policy is created and associated with it. If the pool itself is removed, all HTTP requests that it would otherwise have received are redirected to the default pool.

### Mapping Between OpenStack L7 Policies and Citrix ADC Entities

<table>
<thead>
<tr>
<th>OpenStack</th>
<th>Citrix ADC Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L7 policy with action REDIRECT_TO_POOL</td>
<td>Content switching policy &gt; Content switching action</td>
<td>Citrix ADM creates a content switching policy that is bound to the content switching virtual server and associated with a content switching action that specifies the target pool of application servers for content retrieval and presentation to the user.</td>
</tr>
<tr>
<td>L7 policy with action REDIRECT_TO_URL</td>
<td>Responder policy &gt; Responder action</td>
<td>Citrix ADM creates a responder policy that is bound to the content switching virtual server and associated with a responder action that specifies the target URL to be presented to the users.</td>
</tr>
<tr>
<td>L7 policy with action REJECT</td>
<td>Responder policy &gt; Drop the request</td>
<td>Citrix ADM creates a responder policy that is bound to the content switching virtual server and associated with a responder action that drops the request.</td>
</tr>
</tbody>
</table>

If the action of an L7 policy that evaluates to “true” redirects traffic to a pool that is in “create_pending” state, Citrix ADM implements the specified pool along with a load balancing virtual server. Citrix ADM creates a content switching policy out of the L7 policy and uses the corresponding content switching action to redirect the requests to the load balancing virtual server associated with that pool. If a sec-
ond L7 policy redirects to the same pool, Citrix ADM creates a content switching policy and a content switching action to redirect the traffic to the existing load balancing virtual server associated with the pool.

Policy Positioning

Evaluation of L7 policies in OpenStack is determined by their priorities. In OpenStack, by default, the policies are assigned priorities in the order in which they are created. The policy created first is numbered “1,” and subsequently created policies are numbered consecutively. But you can change the priorities of the policies and assign them different priorities. The policies are always evaluated in the order of their priorities. The first policy that matches a specific request is always executed first.

When creating policies, note the following points:

- If you assign a new policy the same priority as an existing policy, the new policy takes that priority. The existing policy’s priority is lowered. If necessary, the priorities of other policies are also lowered to retain the order in which the policies are evaluated.

- If you create a new policy without specifying a position, the new policy will just be appended to the list.

- If you create a new policy and assign it a position that is greater than the number of policies already in the list, the new policy will be appended to the list, that is, the new policy always takes the next available priority. For example, if there are three policies A, B, and C with priorities 1, 2, and 3, and if you create a policy and assign a priority of 8, the new policy’s priority becomes 4.

- If you add a policy to the list or delete a policy from the list, the policy position values are reordered from 1 without skipping numbers. For example, if policy A, B, C, and D have position values of 1, 2, 3, and 4, and if you delete policy B from the list, policy C now takes the second position, and policy D takes the third position.

In Citrix ADM, there is always a default policy associated with a csvserver with a priority of 1. This default policy specifies the number of TCP connections that an lbvserver should process at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in Citrix ADC, they are always assigned a priority 1 greater than the priority of the corresponding L7 policy. For example, when an L7 policy with a priority of 1 is evaluated and a content switching policy is created with a priority of 2. Similarly, when an L7 policy with a priority of 2 is evaluated and a responder policy is created with a priority of 3.

In OpenStack, the “reject” and/or “redirect_to_url” policies are first evaluated, and then the “redirect_to_pool policy is evaluated. In a Citrix ADC instance, the responder policies are always evaluated first to either drop the request or present the user with a redirected web address, and the content switching policies are evaluated last. This order of evaluation usually does not cause any conflict if the content switching and responder policies are mutually exclusive. That is, two L7 policies should
not have identical expressions. The derived expressions should be added in the responder and content switching policies to avoid such conflicts. For example, write an expression to reject all requests to “sports-football.com” and another expression to allow requests to “example-sports-football.com.” Create the L7 policies so that all the responder policies to reject the request are arranged at the top of the evaluation list, followed by the responder policies for web direct, followed by the content switching policies.

In Citrix ADM, there is always a default policy associated with a csvserver with a priority of 1. This default policy specifies the number of TCP connections that an lbvserver should process at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in Citrix ADC, they are always assigned a priority 1 greater than the priority of the corresponding L7 policy. For example, when an L7 policy with a priority of 1 is evaluated and a content switching policy is created with a priority of 2. Similarly, when an L7 policy with a priority of 2 is evaluated and a responder policy is created with a priority of 3.

In OpenStack, the “reject” and/or “redirect_to_url” policies are first evaluated and then the “redirect_to_pool policy is evaluated. In Citrix ADC, the responder policies are always evaluated first to either drop the request or present the user with a redirected web address, and the content switching policies are evaluated last. This order of evaluation usually does not cause any conflict if the content switching and responder policies are mutually exclusive. That is, no two L7 policies should have similar expressions. Similar derived expressions should be added in the responder and content switching policies to avoid such conflicts. For example, write an expression to reject all requests to “sports-football.com” and another expression to allow requests to “example-sports-football.com.” Create the L7 policies so that all the responder policies to reject the request are arranged at the top of the evaluation list, followed by the responder policies for web direct, followed by the content switching policies.

**Configuration Tasks**

The L7 policy and action implementations are performed through Neutron LBaaS commands.

Set the environment variables in OpenStack and create the load balancer (for example, LB1). After the load balancer is successfully created, create the listener and pools (for example, L1, P1, and P2), and add members and monitors to the pools. For example, P1 is the default pool for L1, while P2 is the pool tied to LB1 and managing the application servers.

For more information on how to configure LBaaS V2 by using the command line, see Configuring LBaaS V2 using Command Line.

The following commands create the policies and define the specific actions:

**Create L7 Policy to Drop Requests**
Example:

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

The above command creates and binds policy11, a responder policy, to the content switching server to reject requests. Because no rule was created for this policy, the policy evaluates to “false” and the request is rejected.

Create L7 Policy to Redirect Requests to Particular URL

Example:

neutron lbaas-l7policy-create –name policy12 –action REDIRECT_TO_URL –listener admin-list1 –redirect-url http://example-sports/about-us.html

The above command creates a responder action to redirect requests to a URL, creates a responder policy with action, and binds this policy to the content switching virtual server.

Create L7 Policy to Redirect Requests to a Pool

Example:

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2
If this is the first L7 policy, the above command implements P2 along with LB1, creates the content switching redirect action and redirects the requests to LB1. If P2 already exists, the command creates the content switching redirect action and redirects the requests to LB1.

**Manual provisioning of Citrix ADC VPX instance on OpenStack**

August 1, 2019

In a few enterprise networks, Citrix ADC VPX instances cannot connect to Citrix license server to automatically download the licenses, for security reasons. In such a scenario, you need to manually deploy Citrix ADC VPX instances on OpenStack platform. Using the License Activation Code (LAC) received by you from Citrix, download the appropriate Citrix ADC VPX license and save it on your local system.

**To Manually Provision Citrix ADC VPX Instance on OpenStack:**

1. **Install the Citrix ADC Driver Software and Register Citrix Application Delivery Management (ADM) on OpenStack**
   a) In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > OpenStack**.
   b) Click **Configure OpenStack Settings**. In **Configure OpenStack Settings** page, you can set the parameters to configure OpenStack in Citrix ADM. You have two options here - **Default** and **Customized**.
   c) Select **Default**, if the OpenStack services are running on default ports.

2. **Navigate to Orchestration > Cloud Orchestration > OpenStack, and click Deployment Settings.**
   a) **Management Network** - select the management network on OpenStack, to which the auto-provisioned Citrix ADC VPX is connected.
   b) **Profile Name** - select the profile from the drop-down list. The Citrix ADM uses the password contained in this profile to configure new auto-provisioned Citrix ADC VPX instances.
   c) **Citrix ADC VPX Image in Glance** - select the Citrix ADC VPX image available in the OpenStack Glance that is used to create a Citrix ADC VPX instance. The drop-down list will display only those images that are present on OpenStack Glance.

3. In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, and then click **Add**.

4. On the **Service Package** page specify the following parameters:
   a) **Name** - name for the service package. For example, enter SVC-PKG-GOLD.
b) **Citrix ADC Instance Allocation** - select **Dedicated** or **Partitioned** as the type of instance allocation defined in the service package.

c) **Citrix ADC Instance Provisioning** - select **Create Instance OnDemand** to create Citrix ADC instances during the configuration itself.

d) **Auto Provision Platform** - select **OpenStack Compute**. By default, Citrix ADC VPX will be selected as the instance type.

e) **Assign OpenStack Tenants/Placement Policies** - section, under OpenStack Tenants, click **Add**, and select the tenant.

f) Click **Continue**, and then click **Done**.

5. Navigate to **System > System Administration > Change System Settings** and select **http** from the drop-down list.

6. Navigate to **Networks > Instances > Citrix ADC VPX**.

7. In **Citrix ADC VPX** page, click **Admin** drop-down list and select **Provision Device**.

   a) On the **Device Provisioning** page, enter the name of the device, and select the service package that you created in the previous step.

   b) Click **OK**.

8. Navigate to **Orchestration > Cloud Orchestration > OpenStack > Requests** tab. Select the request and click **Tasks** to view the tasks. When the status of the task changes to **Finished**, it means that the Citrix ADC VPX is provisioned in Citrix ADM.

9. Navigate to **Networks > Instances > Citrix ADC VPX** to check that the Citrix ADC VPX instance appears in Citrix ADC VPX page.

10. Click the Citrix ADC VPX instance. When the Citrix ADC VPX instance opens in your browser window, log on to the instance. Navigate to **Configuration > System > Licenses**, and manually add the new license. For more information on how to add new license, see **Citrix ADC Licensing Overview**.

11. Restart the Citrix ADC VPX instance.
12. After a few minutes, you can log on to OpenStack and in **System > Instances**, you can see that the Citrix ADC VPX instance is deployed on OpenStack.

13. LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and execute the configuration tasks. For more information on how to execute configuration commands, see *Configuring LBaaS V2 using Command Line*.

**Provisioning of Citrix ADC VPX instance on OpenStack using StyleBook**

August 1, 2019

In the OpenStack orchestration workflow, Citrix Application Delivery Management (ADM) now uses the “os-cs-lb-mon” StyleBook to deploy LBaaS configurations on Citrix ADC instances allotted to the OpenStack tenant. A configuration pack is created for each load balancer created by the OpenStack user.

Using StyleBooks for configuration in OpenStack workflow provides the following benefits:

- Better visualization by viewing all the configuration objects.
- Reliability through rollback.
- Support for various Citrix ADC instance types (Citrix ADC HA, partitions, VPX, CPX, MPX, and others.)
- Customization by using your own Stylebooks to deploy configuration for OpenStack tenants.

As Citrix ADM admin, navigate to **Applications > Configurations** to view the configuration pack deployed on the Citrix ADC instance.

You can perform the following tasks:

- Scroll to view the “os-cs-lb-mon” configuration pack deployed for the load balancer.
- Click **View Definition** on the “os-cs-lb-mon” StyleBook panel to check the configuration that is deployed on the instances.
- Click **View Object** to view the list of Citrix ADC objects or entities deployed on the instances.
Points to note before provisioning instances using StyleBooks

From Citrix ADM 12.1 build 49.23 onwards, the architecture of OpenStack orchestration workflow has been updated. The workflow now uses Citrix ADM StyleBooks to configure Citrix ADC instances. If you are upgrading to Citrix ADM 12.1 build 49.23 from either version 12.0 or from version 12.1 build 48.18, you must run the following migration script:

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

- Running the migration script creates configuration packs of the “os-cs-lb-mon” StyleBook corresponding to the existing OpenStack configurations.
- Running this migration script is mandatory if you had OpenStack configurations deployed from these earlier builds.
- You can deploy new configurations on the instances using the “os-cs-lb-mon” StyleBook only after you run the migration script from version 12.1 build 49.23.
- All configurations attempted from OpenStack will fail until the migration script is run.

**Note**

- Once you run the migration script, you cannot downgrade to the previous build of Citrix ADM.
- Ensure that you have upgraded the Citrix ADC drivers for OpenStack LBaaS V2 to the latest version. Use the Citrix ADC bundle files provided along with the latest Citrix ADM 12.1 build 49.23.

LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and execute the configuration tasks. For more information on how to execute configuration commands, see Configuring LBaaS V2 using Command Line.

VPX check-in and check-out license and pooled license support for OpenStack environment

August 1, 2019

In OpenStack orchestration workflow, Citrix Application Delivery Management (ADM) creates Citrix ADC VPX instances on demand when you select service package with OpenStack Compute. Now, the service package page in the Orchestration feature in Citrix ADM is enhanced to provide the license that is required to be installed on the Citrix ADC VPX instances that are created on demand. The licenses provided can be either VPX check-in and check-out license or pooled license.
To use this feature, you must first upload the licenses in Citrix ADM and then create service packages that use OpenStack compute.

- If it is a check-in and check-out license, then you can choose the license to be installed from the various licenses available.

- If it is a pool license, then you can select both bandwidth and the type of license edition to be installed.
Whenever you deploy your first load balancer with Citrix ADM as a provider, Citrix ADM creates the Citrix ADC VPX instance and installs the license specified in service package to the newly created instance.

Also, when you delete an existing load balancing instance, that instance is no more needed. The instance is decommissioned and the license is returned back to Citrix ADM. This allows for optimal use of licenses available in Citrix ADM.

Note
When Citrix ADM is deployed in high availability mode, consider that the licenses are uploaded to the current active or the primary Citrix ADM, MAS-HA-1. When you deploy the first request and Citrix ADM creates the Citrix ADC VPX instances, the instance checks out the required licenses
from MAS-HA-1. At later point in time, assume the secondary Citrix ADM, MAS-HA-2, which does not have the licenses is active now. The ADC VPX instance cannot check out the license from MAS-HA-2 now and therefore the instance cannot be created for new users.

In such a case, ensure MAS-HA-1 is UP and is now the current primary node. That is, manually failover the Citrix ADM from MAS-HA-2 to MAS-HA-1. After this, you must re-attempt the configuration from OpenStack and the instances will be recreated with proper licenses. For more information on license support in Citrix ADM high availability deployment, see High Availability.

Shared VLAN support for admin partitions

August 1, 2019

For tenants connecting from private networks, the Citrix Application Delivery Management (ADM) supports isolation policy so that each tenant has its own dedicated partition, a dedicated VLAN, and dedicated servers. For tenants connecting from public networks, a dedicated VLAN will require too many IP addresses to be used. A shared VLAN circumvents this problem by creating one virtual IP address on each partition thus creating a single IP subnet.

When an tenant configures a VIP or a listener, an admin partition is created in the Citrix ADC device for that tenant. All load balancer configuration is pushed to that admin partition that is created. If the tenant is using a shared network or an external network to create a load balancer, then the VLAN of that network is added and the sharing feature is enabled. When a different tenant uses the same shared network to create its load balancer, the VLAN is not added to the Citrix ADC again, but the VLAN will be bound to the second partition as well. Thus, any tenant who uses the same shared network gets a partition which is bound to the same VLAN.

The Citrix ADM supports virtual destination MAC address. When tenants share a VLAN, the Citrix ADM assigns different MAC addresses to the partition on the Citrix ADC device. This allows a VLAN to be shared across partitions or across all tenants and all traffic domains.

Configuring Shared VLAN from Citrix ADC Instance

1. In a Citrix ADC instance, navigate to Configuration > System > Network > VLANs, select a VLAN profile, and click Edit to set the partition sharing parameter.

2. On the Configure VLAN page, select the Partitions Sharing check box.

3. Click OK.
Configuring Shared VLAN from OpenStack Orchestration

1. In OpenStack, navigate to **Admin > System > Networks**, and then click **Create Network**.

2. In **Create Network**, set the following parameters:
   a) Name - enter the name of the network
   b) Project - select a project from the drop-down list
   c) Provider Network Type - select VLAN from the drop-down list. This defines that the virtual network is established as VLAN.
   d) Physical Network - the default physical network is selected here. You can edit this.
   e) Admin State - by default, the administrative state of the network is UP
   f) Select **Shared** and **External** Network to define that the VLAN is shared and is using an external network.

3. Click **Create Network**.
Trial licensing workflow

August 1, 2019

During auto-provisioning of the Citrix ADC VPX instance using OpenStack orchestration, the Citrix Application Delivery Management (ADM) uses OpenStack Compute to launch a Citrix ADC VPX instance. The newly provisioned Citrix ADC VPX instance contacts the Citrix licensing portal during the set up, and uses the License Activation Code (LAC) to automatically download and install the license files.

Trial Licenses

Technical support staff use trial licenses when they install Citrix ADM and Citrix ADC VPX devices in field. A trial or evaluation license for Citrix ADC VPX is valid for 90 days. If there is a need to evaluate more than one Citrix ADC or extend the testing after 90 days, a new evaluation license needs to be requested. Instead of automatic installation of trial license files, Citrix ADM provides you an alternate solution. You can manually download the license files and install them on Citrix ADC VPX to complete the installation of the instance.

If the Citrix ADC VPX is unable to connect to the internet, configure the Citrix ADM to act as a proxy server for the Citrix Licensing Portal and install the license files.

Citrix ADC VPX instances that have a trial license can communicate with Citrix ADM on HTTP only. To configure HTTP communication in Citrix ADM, navigate to System > System Administration,
and click **Change System Settings**. Select **http** from the drop-down list to set the communication method, and click **OK**.

### Integrate with OpenStack Heat services

**August 1, 2019**

The OpenStack Neutron LBaaS enables core load balancing services, such as load balancing, SSL offloading, and content switching, for applications. LBaaS is managed through a RESTful API, and the API allows tenants to make REST calls to create, update, and delete LBaaS objects. Because LBaaS provides load balancing services, it does not allow use of the more advanced Citrix ADC features during the orchestration process. The Citrix ADC Heat plug-in overcomes this limitation.

### Heat Orchestration Service

The OpenStack Heat orchestration service allows deployment of complex cloud applications on the basis of templates. The Heat orchestration template (HOT) describes the infrastructure for a cloud application in text files that are readable and writable by humans, and can be managed by version
control tools. YAML, a structured language, is used to write these templates. The HOT template allows you to create most of the OpenStack resource types and specifies the relationships among the resources defined within it. The Citrix ADC Heat plug-in allows you to configure advanced application delivery controller (ADC) functionalities on any Citrix ADC instance.

**Citrix ADC StyleBooks**

Citrix Application Delivery Management (ADM) StyleBooks can be used to create and configure Citrix ADC functionalities. Just like Heat templates, the StyleBooks are also written in YAML. A separate StyleBooks can be created for each functionality, and a single StyleBooks can be used to deploy configurations on multiple Citrix ADC instances.

During Citrix ADC integration with OpenStack, Citrix ADM publishes all Citrix ADM StyleBooks as a resource in the Heat service. This includes both the StyleBooks that are shipped with Citrix ADM and the StyleBooks that are created by the user at a later point of time. The Heat template allows you to configure the advanced features of Citrix ADCs using these StyleBooks resources.

**Workflow to Configure Citrix ADC Instances using Heat**

The following flowchart illustrates the workflow for deploying the Heat stack:

1. Install Citrix ADC bundle for OpenStack
2. Register OpenStack with Citrix ADM
3. Add Citrix ADC instances (optional)
4. Create service packages
   - Add OpenStack tenants
5. Prepare the HOT by using the Citrix ADC Heat resources and ADC Network Resource
6. Deploy the Heat stack

Perform the following tasks as a cloud administrator:

**To configure Heat services in OpenStack:**
1. Download Citrix ADC bundles for OpenStack

Install the Citrix ADC bundles in OpenStack. In Citrix ADM, navigate to Downloads and download the Citrix ADC driver bundles, untar the bundles, and copy the contents of the Heat folder in the bundle to the Heat engine resources directory in OpenStack. The directory path is as follows:

```
/opt/stack/heat/heat/engine/resources/netscaler_resources
```

2. Create a section “netscaler_plugin” in the heat.conf file, and update the following parameters in that section:

   `[netscaler_plugin]`

   a) When the communication is http, the parameters are updated as follows:

   ```
   NMAS_BASE_URI=<http://10.146.103.45:80>
   NMAS_USERNAME=
   NMAS_PASSWORD=
   ```

   b) When the communication is https, the parameters are updated as follows:

   ```
   NMAS_BASE_URI=https://common_name_used_in_certificate
   NMAS_USERNAME=<openstack_driver_username>
   NMAS_PASSWORD=<openstack_driver_password>
   SSL_CERT_VERIFY=<True_or_False>
   CERT_FILE_PATH=<path_of_the_certificate_file>
   ```

   If user sets ssl_cert_verify to be “False,” Citrix ADM sends verify=False in the request calls, which disables the SSL certificate validation. If ssl_cert_verify is set to “True” and cert_file_path entry is present, Citrix ADM sends this path in the verify parameter of request, otherwise Citrix ADM sends verify=True.

   **Note**

   For deploying Citrix ADM in “High Availability” mode, update the following parameters in heat.conf file:

   ```
   NMAS_BASE_URI=<ip address of the front-end virtual server>
   ```

3. Restart the Heat service in OpenStack.

When you restart the Citrix ADC Heat services in OpenStack, all the defined Citrix ADM Style-Books are imported into Heat as resources. Also, the Citrix ADC network resource and the certificate resource are imported into OpenStack as Citrix ADC Heat resources.

4. Register Citrix ADM with OpenStack.
a) In Citrix ADM, navigate to Orchestration > Cloud Orchestration > OpenStack, and click Configure OpenStack Settings.

b) In Configure OpenStack Settings page, you can set the parameters to configure OpenStack. You have two options here: Default and Customized.

c) Select Default if the OpenStack services are running on default ports. Enter the following parameters:
   i. OpenStack Controller IP Address
   ii. Admin Username
   iii. Password
   iv. OpenStack Admin Tenant
   v. Citrix ADC Driver and Heat password

   **Note**
   This is the same password (NMAS_PASSWORD) that you entered in the heat.conf file.

5. Create service packages and define the SLAs with your tenant.

   A tenant is created in Citrix ADM for each user during OpenStack registration, and the tenant information is used by both the LBaaS driver and the Heat plug-in. The Heat plug-in uses this information to contact Citrix ADM to import StyleBooks as Heat resources in OpenStack.

   **Note**
   For more information about creating service packages and other pre-configuration tasks in Citrix ADM and OpenStack, see Integrating Citrix ADM with OpenStack Platform.

6. Observe that all the relevant Stylebooks in Citrix ADM are imported into OpenStack Heat as resources. Also, observe that the Citrix ADC network resource and Citrix ADC certificate resource are imported into OpenStack Heat as resources.

   **Note**
   Currently, you can use only the StyleBooks that are shipped with Citrix ADM.

   Your tenant can now create the Heat template in OpenStack, enter the values of the required Heat parameters, and deploy the Heat stack. When the Heat stack is deployed, the configuration is pushed to Citrix ADM, and the required Citrix ADC instances are configured.

**To prepare Heat template and launch Heat stack:**

1. In OpenStack, the tenant can create a Heat orchestration template (HOT) by using the Heat resources.

2. In OpenStack Horizon, the tenant admin can navigate to Project > Orchestration > Stacks to create the Heat template and launch the Heat Stack. There are two ways to create HOT:
- **File** - Select the updated template from the local directory
- **Direct input** - Copy and paste the YAML contents from the template in the window

**Note**

After successfully deploying the stack, the tenant can update the stack by using the Change Stack Template. But the subnet information and the virtual IP address (VIP) that was provided initially during creation of stack cannot be modified.

After the tenant deploys the stack, navigate to **Orchestration > Cloud Orchestration > OpenStack > Requests** in Citrix ADM to observe the lists of tasks. Also, navigate to **Applications > Configuration** in Citrix ADM to observe that the Citrix ADC instances are successfully configured in the form of StyleBooks configpacks.

**An Example of a Citrix ADM StyleBooks:**

The following image shows an example of how a Citrix ADM StyleBooks is constructed and briefly explains the components. For more information about Citrix ADM StyleBooks and how to use the shipped StyleBooks, see **StyleBooks**.

![An Example of a Citrix ADM StyleBooks](image)

**An Example of a Heat Template:**

The following image shows the structure of a Heat template defined in YAML, and points to the StyleBooks resources and Citrix ADC network resources that are imported as Heat resources.
For more information about Heat services and how to create templates, see OpenStack Heat documentation.

Service package isolation policies

August 1, 2019

Dedicated Isolation Policy

Every tenant associated with the Citrix Application Delivery Management (ADM) service package of a dedicated policy is assigned a Citrix ADC instance from among the instances that are part of this service package. This assigned Citrix ADC instance is not shared with other tenants.

Partition Isolation Policy

Every tenant associated with the service package of partition policy is assigned a dedicated logical admin partition of a Citrix ADC instance that is part of the service package.
**Shared Isolation Policy**

Tenants associated with the service package share the Citrix ADC instances that are part of the service package. All configurations of a tenant are assigned to one Citrix ADC instance. In this mode, configurations from multiple tenants can be hosted on the same Citrix ADC instance. You can select **Citrix ADC VPX** or **Citrix ADC MPX** as device type. You can choose to allot only one Citrix ADC instance or many instances to the service package. That is, multiple tenants can share one or multiple virtual instances of the Citrix ADC device.

**Note**

Add Citrix ADC SDX instances in the service packages as Citrix ADC VPX instances only, as a Citrix ADC SDX has a Citrix ADC VPX provisioned on it.

**Note**

You can also create flexible placement policies, where the policies are not only based on tenant name or ID, but on other custom attributes. For more information on flexible placement policies, see [Flexible Policy-Based Device Allotment](#).

**Flexible policy-based device allotment**

August 1, 2019

Citrix Application Delivery Management (ADM) assigns Citrix ADC virtual instances to tenants, based on the SLAs agreed with the tenants. The assignment of virtual instances to tenants creates a one-to-one relation between the instance and the tenant, where a tenant can be assigned to only one service package in the data center.

In some situations, tenants might require more than one instance, or the assignment of instances might not be based on tenants as a criterion, but on other factors such as network ID, or application. In such cases, Citrix ADM allows you to precisely define placement policies based on user-defined expressions in order to assign a load balancer configuration to one of the managed instances.

Placement policies provide the flexibility to decide on the Citrix ADC instance that is used in each load balancer configuration created by users. Flexible placement policies in Citrix ADM provide an added option to the existing method of assigning Citrix ADC instances based on tenants.

**Note**

You can assign instances to tenants manually or use placement policies to assign instances based
Placement policies are based on Boolean expressions defined over properties of the main LBaaS configuration objects, such as pools and load balancers. The placement policy user interface in Citrix ADM provides pre-defined expressions that you can choose from, to define a customized policy. You can create multiple placement policies for different expressions. So, each tenant can have multiple devices that are defined by the tenant's requirement.

You have to first select an expression to match a root object that has to be configured later. The root object can be a pool object in case of LBaaS V1, and a load balancer object in case of LBaaS V2. So, the Citrix ADM policy based placements are supported for both LBaaS V1 and V2 APIs. These placement policies are then associated with service packages. Once the root object is placed in an instance, the successive objects in the model are added in the instance.

For example, the pool configuration object can have the following properties:

- tenant_id
- name
- description
- protocol
- lb_method
- subnet_id
- subname_name
- admin_state_up
- status
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

The following are examples that show some of the expressions that uses pool properties to define an expression for the policy:

1. Pool Name based policy expression

   ```
   config["pools"]["name"] == "high-end-pool"
   ```
2. Pool Subnet Name based policy expression
   config[“pools”][“subnet_name”] == “us-west-payment-subnet1”

3. Load Balancer Subnet Name based policy expression
   config[“loadbalancers”][“subnet_name”] == “mas-subnet”

**Adding Placement Policy**

1. From the Citrix ADM home page, navigate to Orchestration > Cloud Orchestration > Placement Policy, and then click Add.

2. On the Add Placement Policy page, set the following parameters:
   a) Name - type a name for the placement policy
   b) Frequently Used Expressions - select an expression from the drop-down list.
   c) Expression - a logical (Boolean) expression is populated in this field based on the expression you have selected in the earlier field. Edit the field names as required.

   **Note**
   When creating multiple policies, make sure that the policies are exclusive to one another.

3. Click OK.

4. Navigate to Orchestration > Cloud Orchestration > OpenStack > Service Packages, and then click Add.

5. On the Service Package page, set the following parameters:
   a) Name - type a name for the service package
   b) Isolation Policy - select Shared policy
      In shared isolation policy, the load balancer configuration of a tenant coexists with the load balancer configuration of other tenants in the device allocated to the tenant.
   c) Device Type - select a preprovisioned Citrix ADC VPX or Citrix ADC MPX
      Select Allot one device if you want all the load balancer configurations of a tenant to be tied to one device. Select Allot many devices if you want each load balancer configurations of a tenant to be distributed on several devices based on placement policies.

   **Note**
   Citrix ADC SDX has to be added in the service packages as Citrix ADC VPX instances only, as a Citrix ADC SDX has a Citrix ADC VPX provisioned on it.
d) Placement Method - select **Least Configured**

When Least Configured is selected, the Citrix ADC instance that has the least number of pool members configured at that point in time is chosen as the device for the tenant.

6. Click **Continue**.

7. In **Assign Devices** section, add the available Citrix ADC devices to the configured devices list.

8. Click **Continue**.

9. In **Assign Placement Policies/OpenStack Tenants** section, add the placement policy that you created earlier.
Note

If the policy is not found, the fallback mechanism is revived, and the Citrix ADM assigns Citrix ADC instances based on tenants. If the tenant is not part of any service package, the Citrix ADM displays an error message that says: “Tenant <admin> is not part of any Service Package and there is no default Service Package.”

10. Click **Continue**, and then click **Done**.

### NSX Manager: manual provisioning of Citrix ADC instances

August 1, 2019

Citrix Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of Citrix ADC services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy Citrix ADC services faster.

This article provides you with a list of tasks that you have to perform on both VMware NSX Manager and on Citrix ADM.

**Note**

Ensure that VMware NSX for vSphere 6.2 and above is installed and configured, and the edge gateways, DLR, and virtual machines that have to be load balanced are already created.

**Prerequisites**

- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
- Install Citrix ADM on any of the supported hypervisors.

For tasks to installCitrix ADM build 12.1, on any of the supported hypervisors, see [Deploying Citrix ADM](https://docs.citrix.com/).
VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you require on your VMware ESXi server to install a Citrix ADM virtual appliance.

<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>8</td>
</tr>
<tr>
<td>Storage space</td>
<td>500 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
The memory and hard disk requirements specified above are for deploying Citrix ADM on VMware ESXi server, considering that there are no other virtual machines running on the host. The hardware requirements for VMware ESXi server depends on the number of virtual machines running on it.

Configuring VMware NSX

- Create a pool of Citrix ADC VPX instances of different capacities, which are added to the different service packages.

For example:

- Create five Citrix ADC VPX instances of VPX1000 (1 Gbps). These instances are added to the Gold service package.

- Create five Citrix ADC VPX instances of VPX10 (10 Mbps). These instances are added to the Bronze service package.

1. In vSphere client, navigate to Networking, and create a port group of type VLAN trunking with range, for example, 101-105 (you can even provide the full range, but create port group of type VLAN for only the required VLANs).
2. Create a new interface for each Citrix ADC VPX instance, and attach it to the VLAN range trunk port group that was created above.

3. In vSphere client, navigate to Networking, and create a port group of type VLAN.
For example, if the initial trunked port group was created with range 101-105, create five VLAN port groups one per VLAN, that is a port group with VLAN 101, another with VLAN102, and so on, until VLAN 105.

Adding Citrix ADC VPX Instance in Citrix ADM

Add Citrix ADC VPX instances in Citrix ADM and specify the VLAN range of the trunked group for each device.

1. In Citrix ADM, navigate to Infrastructure > Instances > Citrix ADC VPX, and click Add.

2. On the Add Citrix ADC VPX page, specify either the host names of the instances, the IP address of each instance, or a range of IP addresses, and then select an instance profile from the Profile Name list. You can also create a new instance profile by clicking the + icon.

3. Click OK.

4. Select the newly added Citrix ADC VPX instance from the list on the Citrix ADC VPX page, and click the down arrow button in Action field. Select Configure Interfaces for Orchestration.
5. On the **Interfaces** page, select the management interface, and click **Disable** to disable VLAN from binding to the management interface.

6. On the **Interfaces** page, select the required interface, and click **Configure VLAN Range**.

7. Enter the VLAN range configured in NSX Manager, click **OK**, and then click **Close**.
Registering VMware NSX Manager with Citrix ADM

Register VMware NSX manager with Citrix ADM to create a communication channel between them.

1. In Citrix ADM, navigate to Orchestration > SDN Orchestration > VMware NSX Manager from the drop-down list, and click Configure NSX Manager Settings.

2. On Configure NSX Manager Settings page, set the following parameters:
   a) NSX Manager IP Address - IP address of NSX Manager.
   b) NSX Manager Username - Administrative user name of NSX Manager.
   c) Password - Password of the administrative user of NSX Manager.

3. In Citrix ADM account used by NSX Manager section, set the Citrix ADC Driver Username and Password for the NSX Manager. Citrix ADM authenticates load balancer configuration requests from the NSX Manager by using these logon credentials.

4. Click OK.

5. Navigate to Orchestration > System > Deployment Settings. Provide the VLAN range which was configured in trunked port group.
6. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions > Service Managers**.

You can view Citrix Citrix ADM as one of the service managers. This indicates that the registration is successful and a communication channel is established between the NSX manager and Citrix ADM.

---

### Creating a Service Package in Citrix ADM

1. In Citrix ADM, navigate to **Orchestration > SDN Orchestration > VMware NSX Manager > Service Packages**, and click **Add** to add a new service package.

2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a) Name – type the name of a service package
   b) Isolation Policy – by default, the isolation policy is set to Dedicated
   c) Device Type – by default, the device type is set to Citrix ADC VPX
Note

These values are set by default in this version, and you cannot modify them.

d) Click Continue.

Service Package

3. In Assign Devices section, select the pre-provisioned VPX for this package, and click Continue.

4. In Publish Service Package section, click Continue to publish the service package to VMware NSX, and then click Done.
This procedure configures a service package in the NSX Manager. A service can have multiple devices added to it and multiple edges can use the same service package to offload the Citrix ADC VPX instance to Citrix ADM.

5. Log on to the NSX Manager on vSphere Web Client, and navigate to Service Definitions > Services.

You can see that the Citrix ADM service package is registered.

Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the previously created NSX Edge gateway (offload the load balancing function from NSX LB to Citrix ADC).

1. In NSX Manager, navigate to Home > NSX Edges, and select the edge gateway that you have configured.

2. Click Manage, and on the Load Balancer tab, select Global Configuration, and click Edit.
3. Select Enable Load Balancer, Logging, Enable Service Insertion to enable them.

   a) In Service Definition, select the service package that was created in Citrix ADM and published to NSX Manager.

4. Select the existing runtime NICs and click the Edit icon to edit runtime NICs that have to be connected when Citrix ADC VPX is allocated.

5. Edit the name of the NIC, specify Connectivity Type as Data, and click Change.
6. Select the appropriate web logical switch.

7. In **Primary IP Allocation Mode**, select IP Pool from the drop-down list, and click the down-arrow button on IP Pool field.

8. In the **Select IP Pool** window, select the appropriate IP pool, and click **OK**.
The IP address is acquired and is set as the source net IP address in the Citrix ADC VPX appliance. A L2 gateway is created in the NSX Manager to map the VXLAN to VLAN.

**Note**

All data interfaces are connected as run-time NICs, and they should be part of interfaces for DLR.

9. Refresh the view to see the creation of the run time.
10. After the VM has started, the value of Status changes to **In Service** and that of Install State changes to **Enabled**.

   ![Load Balancer Configuration](image)

   **Note**

   In Citrix ADM, navigate to **Orchestration > Requests** to see progress details of completion of LB service insertion.

### Viewing L2 Gateway on NSX Manager

1. Log on to the NSX Manager on vSphere Web Client, navigate to **NSX Edges**, and select the DLR created.

   ![NSX Manager](image)

2. In the DLR page, navigate to **Manage > Bridging**. You can see the L2 gateway displayed in the list.
Viewing Allotted Citrix ADC

1. Log on to the Citrix ADC VPX instance using the IP address displayed in Citrix ADM. Then, navigate to Configuration > System > Networking. In the right pane, you can see that the two IP address are added. Click the IP address hyperlink to see the details.

   The subnet IP address is same as the IP address of the web interface added in the NSX.

2. Navigate to Configuration > System > Licenses to view the licenses that are applied to this instance.

Configuring Citrix ADC VPX Instance Using Stylebook

1. In Citrix ADM, navigate to Orchestration > SDN Orchestration > Configure NSX Manager > Edge Gateways.

   Make a note of the Citrix ADC instance IP that is allotted to the respective Edge Gateway on which Load Balancing configuration through Stylebooks has to be applied.
2. Create a new Stylebook. Navigate to **Applications > Configuration**, import the stylebook, and select the stylebook from the list.

To create a new stylebook, see **Create Your Own Stylebook**.

3. Specify values for all the required parameters.

4. Specify the Citrix ADC VPX instance on which you want to run these configuration settings.

5. Select the IP instance noted earlier, and click **Select**.

6. Click **Create** to apply the configuration on the selected device.
Viewing Load Balancer Configuration

1. Log on to the Citrix ADC VPX instance, navigate to Configuration > Traffic Management > Load Balancing to view the load balancing virtual server that is created.

2. Select the service group, and click Manage Members. The Configure Service Group Member page displays the members associated with the service group.
Deleting Load Balancer Service

1. In Citrix ADM, navigate to Applications > Configuration, and click X icon to delete the application configuration.

2. Log on to the NSX Manager on vSphere Web Client and navigate to the edge gateway to which the Citrix ADC VPX instance is connected.

3. Navigate to the Manage > Load Balancer > Global Configuration, right-click on the runtime entry, and click Unprovision.

Note

Edge Gateways in NetScaler MAS corresponds to runtime entries in NSX manager.
The Citrix ADC VPX instance is rendered out of service.

4. In Citrix ADM, navigate to **Orchestration > SDN Orchestration > Configure NSX Manager > Edge Gateways**. Verify that the respective mapping of Edge Gateway to the deleted instance is not present.

**NSX Manager: auto provisioning of Citrix ADC instances**

August 1, 2019

**Overview**

Citrix Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of Citrix ADC services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programatically deploy Citrix ADC services faster.
During load-balancing service insertion and deletion on VMware NSX Manager, Citrix ADM dynamically provisions and destroys the Citrix ADC instances. This dynamic provisioning requires the Citrix ADC VPX license assignments to be automated in Citrix ADM. When the Citrix ADC licenses are uploaded to the Citrix ADM, Citrix ADM performs the role of license server.

**Prerequisites**

- Citrix ADM, version 12.1 setup in high availability and installed on ESX.
- Citrix ADC VPX, version 12.1
- Citrix ADC VPX licenses for Citrix ADC VPX instances, version 12.1
- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.

**High-Availability Deployment of Citrix ADM and Citrix ADC Instances**

To provision the Citrix ADM HA setup, install the Citrix ADM image file that you have downloaded from the Citrix download site. For more information on how to provision Citrix ADM HA set up, see Deploying Citrix ADM in High Availability.

**Setting up Citrix ADM HA Endpoint Details**

To integrate VMware NSX manager with Citrix ADM that is deployed in a HA mode, you must first enter the virtual IP address of the load balancing Citrix ADC instance. You must also upload the certificate file that is present on the Citrix ADC load balancing virtual server to the Citrix ADM file system.

**To provide load balancing configuration information in Citrix ADM:**

1. In Citrix ADM HA node, navigate to **System > Deployment**.
2. Click **HA Settings** in the top-right corner, and in **MAS-HA Settings** page, click **MAS-HA Endpoint Details**.
3. On **MAS-HA Endpoint Details** page, upload the same certificate that is already present on the load balancing Citrix ADC instance.

4. Enter the virtual IP address of the load balancing Citrix ADC instance and click **OK**.

### MAS-HA Endpoint Details

You can provide the LB configuration information (VIP and cert) which was configured in the NetScaler for loadbalancing traffic to MAS nodes.

| Certificate file* | server_cert
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP*</td>
<td>10.102.29.192</td>
</tr>
</tbody>
</table>

![MAS-HA Endpoint Details](image)

### Registering VMware NSX Manager with Citrix ADM

When you set up two Citrix ADM servers in high availability, the two server nodes are in active-passive mode. Log on to the primary Citrix ADM server node to register VMware NSX manager with Citrix ADM in HA, to create a communication channel between them.

To register VMware NSX manager with Citrix ADM in HA:

1. In the primary Citrix ADM server node, navigate to **Orchestration > SDN Orchestration > VMware NSX Manager**.

2. Click **Configure NSX Manager Settings**.

3. On **Configure NSX Manager Settings** page, set the following parameters:
   a) NSX Manager IP Address - IP address of NSX Manager.
   b) NSX Manager Username - Administrative user name of NSX Manager.
   c) Password - Password of the administrative user of NSX Manager.

4. In Citrix ADM account used by NSX Manager section, set the Citrix ADC Driver Password for the NSX Manager.

5. Click **OK**.

### Upload Licenses in Citrix ADM

Upload the Citrix ADC VPX licenses to Citrix ADM, so that Citrix ADM can automatically assign licenses to the instances during orchestration with NSX.

To install license files on Citrix ADM:
1. In Citrix ADM, navigate to Networks > Licenses.

2. In License Files section, select one of the following options:
   a) Upload license files from a local computer - If a license file is already present on your local computer, you can upload it to the Citrix ADM. To add license files, click Browse and select the license file (.lic) that you want to add. Then click Finish.
   b) Use License Access Code - Citrix emails the License Access Code (LAC) for the licenses that you purchase. To add license files, enter the LAC in the text box and then click Get Licenses.

   **Note**
   At any time, you can add more licenses to the Citrix ADM from the License Settings.

---

### Upload Citrix ADC VPX Images in Citrix ADM

Add the Citrix ADC images to Citrix ADM, so that the Citrix ADM uses these images as defined in the service package.

**To upload Citrix ADC VPX images in Citrix ADM:**

1. In Citrix ADM, navigate to Orchestration > SDN Orchestration > VMware NSX Manager > ESX NSVPX Images.

2. Click Upload, and select the Citrix ADC VPX zip package from the local storage folder.
Create service packages in Citrix ADM

Create service packages in Citrix ADM to define the set of SLAs, which states how the Citrix ADC resources are allocated.

To create service packages in Citrix ADM:

1. In Citrix ADM, navigate to Orchestrations > SDN Orchestration > VMware NSX Manager > Service Packages, and click Add to add a new service package.

2. On Service Package page, in Basic Settings section, set the following parameters:
   a) Name - name of a service package
   b) Isolation Policy - select Dedicated
   c) Citrix ADC Instance Provisioning - select Create Instance OnDemand
   d) Auto Provision Platform - select CitrixADC SDX
   e) Click Continue

3. In the Auto Provision Settings section, select the recently uploaded Citrix ADC VPX zip package for deploying it on NSX platform, select the corresponding license, and click Continue.

   Note
   In High Availability section, check the box to provision Citrix ADC instances for HA.
4. Click **Continue**.

5. The service package is published to NSX Manager. In NSX Manager, navigate to **Service Definitions > Service Managers**. You can view Citrix Citrix ADM as one of the service managers. This indicates that the registration is successful and bi-directional communication is established between the NSX manager and Citrix ADM.

**Note**

For Citrix ADM in high availability deployment, the licenses are uploaded only in the Citrix
Perform load balancer service insertion for Edge

Perform load balancer service insertion on the existing NSX Edge Gateway, that is, offload the load balancing function from NSX load balancer to Citrix ADC.

To insert load balancing service on NSX Edge Gateway:

1. In NSX Manager, navigate to Home > Networking and Security > NSX Edges, and double-click to select the edge gateway that you have configured.
2. Click Manage, and on the Load Balancer tab, select Global Configuration, and click Edit.
3. Select Enable Load Balancer and Enable Service Insertion to enable them.
4. In Service Definition, select the service package that was published to NSX Manager.
5. Configure one virtual NIC for management interface, and one or more virtual NICs for data interfaces. Select the networks for management and data accordingly.

   Note
   Select IP Pool option in Primary IP Allocation mode. Citrix ADM does not support manual or DHCP allocation of IP addresses.

6. Click the refresh icon to see the creation of the run time.

   Note
   Because you are deploying two Citrix ADC VPX instances in HA deployment, two run times are created in the NSX manager.
   You might have to refresh the screen to view the run times displayed on the screen.

7. Select the run time, click Actions, and select Install from the pop-up menu. For HA, repeat this for the other run time also.

8. When both the virtual machines start, the value of Status changes to “In Service” and that of Install State changes to “Enabled.”

   Note
   You might have to refresh the screen to view the change in status.

9. In Citrix ADM, navigate to Orchestration > Requests to see progress details of completion of service insertion. You can see that a request to create and update the run time has come in to Citrix ADM. When the run time has been updated, select the request and click the Tasks button to view that Citrix ADM has been added in NSX Manager.
For HA, there will be two requests to create and update two run times in Citrix ADM. When both run times have been updated, select both requests and click the Tasks button to view that two Citrix ADM HA nodes have been added in NSX Manager.

10. In Citrix ADM, navigate to Orchestration > SDN Orchestration > VMware NSX Manager > Edge Gateways. In the right-hand side panel, you can view that the Citrix ADC VPX has been added to the NSX Edge Gateway.

For HA, you can see that two Citrix ADC VPX instances in HA mode have been added to the NSX Edge Gateway.

11. In Citrix ADM, navigate to Networks > Licenses > VPX Licenses. Select the Citrix ADC VPX license and the edition that you have installed.

The Citrix ADC VPX instances that are in HA mode consume two licenses and the status is displayed on your screen as below.

When the service insertion is complete, you can use StyleBooks to configure the Citrix ADC instances in one of the following two methods:

- Configure Load Balancing Services on Citrix ADC VPX in VMware NSX Manager GUI
- Configure Load Balancing Services on Citrix ADC VPX in Citrix ADM GUI
Configure Load Balancing Services on Citrix ADC VPX in VMware NSX Manager GUI

Perform the following task to enable configuration of load balancing services on the NSX Edge gateway device using built-in StyleBooks.

In NSX Manager, navigate to Home > Networking and Security > NSX Edges, and double-click to select the edge gateway that you have configured.

Creating pools and pool members

Create a pool of servers and members of different capacities.

1. Click Manage, and on the Load Balancer tab, select Pools, and click “+” icon to add a new pool, and set the following parameters:
   a) Name - Name of the new pool
   b) Algorithm - Select an algorithm from the drop-down list base on which the pool will be selected.
   c) Monitors - Make sure the service monitor is set to default_http_monitor
   d) Members - Click “+” to add members to the pool and enter the required parameters in the New Member window.
      i. Name - Name of the member
      ii. IP Address/ VC Container - Click Select to select the object from the available list or enter the IP address of the object.

2. Click OK.

Add as many members as required.
Create virtual servers

Create a set of virtual servers and assign a pool to each virtual server.

1. Click Manage, and on the Load Balancer tab, select Virtual Servers, and click “+” icon to add a virtual server, and set the following parameters:
   a) Application profile - By default, the service profile that you created in Citrix ADM is displayed.
   b) Name - Name of the virtual server.
   c) IP Address - Click Select to select an existing pool of IP addresses or create a new pool of IP addresses.
   d) Default pool - Select the default pool from the drop-down list.

2. Click OK.

3. In Citrix ADM, navigate to Orchestration > Requests to see progress details of completion of service creation on the selected Citrix ADC instance(s).

4. In Citrix ADM, navigate to Applications > Configuration, and check that the “nsx-lb-mon” config pack has been created.

Configure Load Balancing Services on Citrix ADC VPX in Citrix ADM GUI

Deploy load balancer configurations on the Citrix ADC instance using Citrix ADM StyleBooks. For HA, the configuration is deployed on both Citrix ADC instances that are in HA.

To create configuration packs through StyleBooks:

1. In Citrix ADM, navigate to Applications > Configuration > Create New, and select the HTTP/SSL LoadBalancing (with Monitors) StyleBook from the list. The StyleBook opens as a user interface page on which you enter the values for all the parameters defined in this StyleBook.

2. Specify values for all the required parameters.
3. Select the target Citrix ADC VPX instance that is provisioned in the NSX environment, and click **Create** to apply the configuration on the selected device. For HA deployment, select the instances that are in HA mode.

**Verify Creation of Virtual Servers and Service Groups in Citrix ADC VPX Instances**

You can view that the service groups and virtual servers are created by logging on to the Citrix ADC VPX instance.

**To view the service groups and virtual servers:**

1. Log on to the Citrix ADC VPX instance. For HA deployment, you must log on to both Citrix ADC instances that are in HA.
2. Navigate to **Configuration > System > Networking**. In the right pane, you can view the IP addresses that are added. Click the IP address hyperlink to see the details. You can see that the subnet IP address is same as the IP address of the web interface that was added in NSX.
3. Next, navigate to **Traffic Management > Load Balancing > Virtual Servers** and view the virtual server details.
4. Next, navigate to **Service Groups** and view the service group details.
5. Finally, navigate to **Configuration > System > Licenses** to view the licenses that are applied to this instance.

**Delete load balancing services**

When the load balancing services are no longer required on the Citrix ADC VPX instances deployed on the NSX manager, you can delete the service insertions that were performed earlier.

**To delete configuration and service insertion:**

1. In Citrix ADM, Navigate to **Applications > Configuration**, select the application configuration created, and then delete the configuration by clicking on the “X” icon.
2. In NSX Manager, navigate to the edge gateway to which the Citrix ADC VPX instance is connected. Navigate to **Manage > Load Balancer > Global Configuration**, right-click on the runtime entry, and then click **Unprovision**. The virtual machine is rendered out of service.
3. In Citrix ADM, navigate to **Orchestration > Cloud Orchestration > Edge Gateways**. Verify that the respective mapping of Edge gateway to deleted instance should not be present.
Citrix ADC automation using Citrix ADM in Cisco ACI hybrid mode

August 1, 2019

Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to Citrix Application Delivery Management (ADM), which acts as a Device Manager in the APIC.

The Citrix ADC Hybrid Mode solution is supported by a hybrid mode device package and Citrix ADM. You need to upload the hybrid mode device package in the APIC. This package provides all network L2-L3 configurable entities from Citrix ADC. Application parity is mapped by StyleBook from Citrix ADM to the APIC. In other words, StyleBook acts as reference between L2-L3 and L4-L7 configurations for a given application. You must provide a StyleBook name while configuring the network entities from the APIC for Citrix ADC.

The following illustration provides an overview of Citrix ADC in a hybrid mode solution:

In Hybrid Mode, the Citrix ADC configuration is performed in the following two phases:

1. Network stitching is done from the Cisco APIC
2. Configuration is done from the Citrix ADM

For any given application, a network administrator has to provide network specific details, such as IP addresses, port, VLAN (automated) and so on, as part of the service graph creation and deployment in the Cisco APIC. These configuration details are then pushed to Citrix ADM through the device package, and Citrix ADM internally processes them and configures the Citrix ADC. An application administrator creates the application’s ADC related configuration by using StyleBook in Citrix ADM, and
these configurations are then pushed from Citrix ADM to the Citrix ADC. The Cisco APIC and Citrix ADM communicate with the ADC through the management network.

The following diagram shows a Citrix ADC workflow in the hybrid solution:
Prerequisites

August 1, 2019

Make sure that:

• You have conceptual knowledge of Cisco ACI components and Citrix ADCs.
  – For more information about the Citrix ADCs, see the Citrix ADC product documentation at: http://docs.citrix.com/.

• All the required components of Cisco ACI, including a Cisco APIC in the datacenter, are set up and configured. For more information about Cisco ACI and its components, see the product documentation at: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

• You have installed Citrix ADC 11.1 or later.

• You have configured Citrix ADCs in Cisco ACI so that they can be managed by using the Cisco APIC.

• You have deployed Citrix Application Delivery Management (ADM) in your environment. For more information, see Citrix ADM 12.1.

• Management connectivity from APIC to Citrix ADM and ADC are established.

• Make a note of:
  – The connection interfaces and IP addresses that are used for management and data-path connectivity.
  – Leaf-switch details: Citrix ADC IP addresses, ports, interfaces, and so on.

  Note
  In this release, the hybrid mode solution supports Citrix ADC in a single-context, that is, admin partitions are not supported.

Configure Citrix ADC in hybrid mode using Cisco APIC and Citrix ADM

August 1, 2019
Perform the following tasks to configure a Citrix ADC in Hybrid Mode by using Cisco APIC and Citrix Application Delivery Management (ADM):

1. Add Citrix ADC instances in your fabric to Citrix ADM. For instructions, see Adding an Instance to Citrix ADM.

2. Use Citrix ADM to create a StyleBook for the application. For instructions, see Creating a Style-Book for the Application Using Citrix ADM.

3. Import the Citrix ADC hybrid mode device package into Cisco APIC. For instructions, see Importing the Citrix ADC Hybrid Mode Device Package into Cisco APIC.

4. Add Citrix ADM as a device manager in the Cisco APIC. For instructions, see Adding Citrix ADM as a Device Manager in Cisco APIC.

5. Use Cisco APIC to add a Citrix ADC device in Cisco ACI. For instructions, see Adding the Citrix ADC as a Device in Cisco ACI.

6. Create and deploy a service graph template. For instructions, see Creating and Deploying a Service Graph.

7. Configure L4-L7 parameters by using StyleBook in Citrix ADM. For instructions, see Configure L4-L7 parameter using StyleBook from Citrix ADM.

8. Attach or detach endpoint events from the Cisco APIC. For more information, see Attaching or Detach endpoint events from APIC.

Create a StyleBook for an application using Citrix ADM

August 8, 2019

A StyleBook is a configuration template that you can use to create and manage Citrix ADC configurations for any application. You can create a StyleBook for configuring a specific Citrix ADC feature, such as load balancing, SSL offload, or content switching. You can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Lync. For more information, see StyleBooks.

You can create your own StyleBook for your application or modify and use the APIC-HTTP-LB StyleBook shipped with Citrix Application Delivery Management (ADM).

To create your own StyleBook for your application in Citrix ADM, see How to Create Your Own Style-Books.

While creating the StyleBook, make sure that you follow the the APIC’s service graph model in the StyleBook. In other words, the APIC’s service graph for any application follows consumer and provider
model connected through an ADC function. Consumer and provider are represented as an End-Point Group (EPG) and have a 1:1 relationship. The same model must be followed in StyleBook as well, where the provider EPG must be represented as a servicegroup and each end point as a member of the service group. The ADC function node must be represented by a virtual server (for example, a load balancing virtual server), and there must be a 1:1 relationship between virtual server and servicegroup.

This essentially captures the essence of the service graph and allows you to handle the attach or detach event from the APIC, where an attach event binds the end point to the corresponding servicegroup and a detach event unbinds it. You must make sure that the service graph and StyleBook are in parity for seamless automation from network L2-L3 to ADC-feature L4-L7 configurations.

**Import Citrix ADC hybrid-mode device package into Cisco APIC**

August 8, 2019

The Hybrid Mode device package is a lightweight package compared to a fully managed mode. Only L2-L3 network parameters are available through the Device Model. The Device Model has only one generic ADC function defined in it, and four function profiles based on the Citrix ADC deployment in the fabric (for example, one-arm and two-arm and the same with RHI). The Hybrid Mode Device package name is **Citrix-ADM-1.0**. Download the Hybrid Mode device package from the [Citrix Download Site](https://www.citrix.com) and import the device package to the APIC.

**Note**

The hybrid mode device package can co-exist with a fully managed mode device package.

**To import the hybrid mode device package to the APIC by using the APIC GUI:**

1. On the menu bar, click the **L4-L7 Services** tab and select the **Packages** panel.
2. In the **Navigation** pane, right-click on **L4-L7 Device Types** and select **Import Device Package**.
3. In the **Import Device Package** dialog box, click **Browse** to select the downloaded Citrix ADC hybrid mode device package.
4. Click **Submit**.

   After successfully importing the device package to the APIC, in the **Navigation** pane, you can view the details of the device package by clicking **Citrix-ADM-1.0**.
Important

After you import the device package, make sure that there are no faults in the APIC. You can view the faults by clicking the **Faults** tab in the Device Types window.

Create and deploy a service graph

August 8, 2019

You have to use Cisco APIC service graph templates in APIC to create and deploy the Citrix ADCs. Make sure that you use the ADC function profile while creating and deploying a service graph.

After the graph is configured in the APIC, the APIC automates the device configuration on the basis of the function definitions, device connectivity to the fabric, and the entities configured as part of the graph deployment. The APIC also automates the network configuration, such as VLAN allocation and its binding, as part of the service graph creation, and the configuration is removed once you delete the graph from the APIC.

A service graph is represented as two or more tiers of an application, with the appropriate service function inserted between them. A service graph is inserted between the source and destination EPGs by a contract.

**To create a service graph by using the APIC GUI:**

1. On the menu bar, go to **Tenants > All Tenants**.
2. In the **Work** pane, double-click the tenant’s name.

3. In the **Navigation** pane, select **tenant_name > L4-L7 Services > L4-L7 Service Graph Templates**.

4. In the **Work** pane, select **Actions > Create a L4-L7 Service Graph Template**.

5. In the **Create a L4-L7 Service Graph Template** dialog box, in the Device Clusters section, select a device cluster and do the following:
   a) In the **Graph Name** field, enter the name of the service graph template.
   b) In the **Graph Type** field, select **Create A New One**.
   c) From the **Device Cluster** section, drag the device and drop it between the consumer end-point group and provider end-point group to create a service node.

   ![Create L4-L7 Service Graph Template](image)

   d) In the `<L4-L7device_name information>` section, do the following:
      i. In the **ADC** field, select **One-Arm** or **Two-Arm**, depending on how the Citrix ADC is deployed in the fabric.
      ii. In the **Profile** drop-down list, select the function profile provided in the device package.
iii. Click **SUBMIT**.

6. In the **Navigation** pane, click the service graph template. The screen presents a graphic topology of the service graph template.

**Note**

The Cisco APIC supports the notion of connectors, and these connectors are visible in the ADCCluster node. The connectors define the network traffic direction and the device script that dynamically binds the allocated VLAN to a virtual IP (VIP) or subnet IP (SNIP) address, depending on whether the connection is external or internal. VLANs are also bound to specific interfaces used for inbound and outbound traffic.
Applying the Service Graph Template to Endpoint Groups

After you have created the service graph template, you need to apply the created service graph template by using the APIC GUI.

To apply the service graph template:

1. On the menu bar, go to **Tenants > All Tenants**.
2. In the **Work** pane, double click the tenant’s name.
3. In the Navigation pane, choose **tenant_name > L4-L7 Services > L4-L7 Service Graph Templates**.
4. Right-click on the **template_name** and click **Apply L4-L7 Service Graph Template**.
5. In the **Apply L4-L7 Service Graph Template To EPGs** dialog box, in the **EPG Information** section, complete the following fields:
a) In the **Consumer EPG/External Network** drop-down list, select the consumer endpoint group.

b) In the **Provider EPG/External Network** drop-down list, select the provided endpoint group.

c) In the **Contract Information** section, complete the appropriate fields. The contract information is specific to the Cisco APIC and is configured as part of the security policies associated with the EPGs.

d) Click **Next**.

e) In the **Graph Template** drop-down list, select the service graph template that you created.

f) In the **Connector** section, do the following:

   i. In the **Type** field, select General.

   ii. In the **BD** drop-down list, select the bridge domain. Connector details are part of the bridge domain that is part of the Cisco APIC infrastructure model.

   iii. In the **Cluster Interface** drop-down list, select the appropriate cluster interface for the selected bridge domain.

   The Cisco APIC uses the selected bridge domains for data path traffic between the Citrix ADC device and the fabric as required by the selected service graph template.
iv. Click **Next**.

On the **Parameters** screen, on the **Required Parameters** tab, enter the L2-L3 specific details, such as the IP address that is mandated by the profile. The other key parameter is the StyleBook name. It can be the built-in StyleBook `APIC-HTTP-LB` provided in Citrix Application Delivery Management (ADM), or you can provide the name of the StyleBook that you created in *Creating a StyleBook for the Application Using Citrix ADM*

**Note**

The StyleBook name links the Service Graph details with the L4-L7 configuration created with Citrix ADM for a given application.
The Cisco APIC GUI allows you to filter the parameters on the basis of features (for example, load balancing). You can view and set all the mandatory parameters on the **Required Parameters** tab, and you can view and set all the other parameters related to the feature on the **All Parameters** tab.

**Note**

By default, a built-in one-arm profile requires you to provide SNIP details such as IP address and netmask. You can view other networking parameters by clicking **All Parameters** and expanding the **Configure Network** tree in the Cisco APIC GUI. This lists all the network parameters supported by Citrix ADC. You can instantiate any entity and provide values for the listed attributes from the Cisco APIC GUI.

6. Click **Finish**.

**Important**

After you apply the service graph template, make sure that there are no faults in the deployed graph. You can view the faults by clicking the **Faults** tab in the **Work** pane.
As part of the Service Graph deployment, the Hybrid Mode Device package pushes the configuration details from the Cisco APIC to the Citrix ADM. The Citrix ADM internally processes these configurations to the respective Citrix ADC and returns the response to the APIC. A successful graph deployment will have no fault, and the Citrix ADC is successfully networked with the fabric for the corresponding graph.

The APIC supports different ways to configure and deploy graphs by using APIs, and graph deployment includes various dependencies on some APIC-specific constructs, such as Tenant, contract, VLAN and namespace.

The following sample approach illustrates one of the ways to make use of the APIC’s APIs to create and deploy L4-L7 graphs, with the assumption that APIC specific artifacts are already configured in the APIC.

Important

Make sure that you use these XML payloads as a reference and make appropriate changes to the XML before you use them in your environment.

Following is an example of creating and deploying the service graph by using APIs:

a) Create AppProfile

b) Create service graph details

c) Attach the service graph to a contract

Following is a sample XML payload for creating an AppProfile. The AppProfile contains EPGs, and the provider EPG contains the Citrix ADC specific entities, attributes, and their values. In the following sample XML payload, Citrix ADC-specific network entities such as the NSIP are created with a set of attributes and StyleBook name.
<polUni>
  <fvTenant name="coke">
    <!-- Application Profile -->
    <fvAp dn="uni/tn-coke/ap-sap" name="sap">
      <!-- EPG 1 -->
      <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
        <fvRsBd tnFvBDName="BD_web" />
      </fvAEPg>
      <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name="Network">
        <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">
          <vnsParamInst key="ipaddress" name="ipl" value="110.110.110.2" />
          <vnsParamInst key="netmask" name="netmask1" value="255.255.255.0" />
          <vnsParamInst key="type" name="tye" value="SNIP" />
          <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED" />
          <vnsParamInst key="hostroute" name="hostroute" value="DISABLED" />
        </vnsFolderInst>
        <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip2">
          <vnsParamInst key="ipaddress" name="ip2" value="220.220.220.2" />
          <vnsParamInst key="netmask" name="netmask2" value="255.255.255.0" />
          <vnsParamInst key="type" name="tye" value="SNIP" />
          <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED" />
          <vnsParamInst key="hostroute" name="hostroute" value="DISABLED" />
        </vnsFolderInst>
      </vnsFolderInst>
      <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook" name="stylebook_1">
        <vnsParamInst name="stylebookName" key="name" />  
      </vnsFolderInst>
    </fvAEPg>
  </fvTenant>
</polUni>
value="APIC-HTTP-LB"/>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="internal_network" name="internal_network">
  <vnsCfgRelInst name="internal_network_key" key="internal_network_key" targetName="Network/snip1"/>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="external_network" name="external_network">
  <vnsCfgRelInst name="external_network_key" key="external_network_key" targetName="Network/snip2"/>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook" name="mFCngStylebook">
  <vnsCfgRelInst name="Stylebook_key" key="Stylebook_key" targetName="stylebook_1"/>
</vnsFolderInst>
<!-- ------- END CONFIG PAYLOAD ----------- -->
<fvSubnet ip="110.110.110.110/24" scope="shared"/>
<fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
<fvRsDomAtt tDn="uni/phys-sepg"/>
<fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
</fvAEPg>
<!-- EPG 2 -->
<fvAEPg dn="uni/tn-coke/ap-sap/epg-app" name="app">
  <fvRsCons tnVzBrCPName="Ctrct1"/>
  <fvRsBd tnFvBDName="BD_app"/>
  <fvSubnet ip="220.220.220.220/24" scope="shared"/>
  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
  <fvRsDomAtt tDn="uni/phys-sepg"/>
</fvAEPg>
</fvAp>
</fvTenant>
</polUni>

Following is a sample XML payload for creating service graph details:

```xml
<polUni>
  <fvTenant name="coke">
    <vnsAbsGraph name="Graph1"/>
  </fvTenant>
</polUni>
```
Following is a sample XML payload for attaching the service graph to a contract:

```xml
<polUni>
    <vnsAbsTermNodeProv name = "Input1">
        <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
    </vnsAbsTermNodeProv>
    <vnsAbsNode name="ADC" funcType="GoTo">
        <vnsAbsFuncConn name = "outside" attNotify="true">
            <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name = "inside" attNotify="true">
            <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
        </vnsAbsFuncConn>
        <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction"/>
        <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-ADCOneArmServiceProfileGroup/absFuncProf-A DCOneArmFunctionProfile"/>
        <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/>
    </vnsAbsNode>
    <vnsAbsTermNodeCon name = "Output1">
        <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
    </vnsAbsTermNodeCon>
    <vnsAbsConnection name = "CON1">
        <vnsRsAbsConnectionConns tDn="uni/tn-coke/absGraph-Graph1/absTermNodeCon-Output1/absTConn" />
        <vnsRsAbsConnectionConns tDn="uni/tn-coke/absGraph-Graph1/absNode-ADC/absFConn-outside" />
    </vnsAbsConnection>
    <vnsAbsConnection name = "CON2">
        <vnsRsAbsConnectionConns tDn="uni/tn-coke/absGraph-Graph1/absNode-ADC/absFConn-inside" />
        <vnsRsAbsConnectionConns tDn="uni/tn-coke/absGraph-Graph1/absTermNodeProv-Input1/absTConn" />
    </vnsAbsConnection>
</vnsAbsGraph>
</polUni>
```
Configure L4-L7 parameters from Citrix ADM using StyleBook

August 8, 2019
May 24, 2018

In Citrix Application Delivery Management (ADM), you can view the deployed service graph details on the **Orchestration** tab, under **Cisco ACI**. The tabular view shows the service graph details such as graph name, tenant name, context, StyleBook name, and network configuration status.

Note
If the graph is deleted from the Cisco APIC, the corresponding configuration is removed from the device, including the L4-L7 configuration.

Additionally, the tabular view allows you to sort on any column displayed in the table and filter the data by using the Search option. You can also customize the column details by selecting or unselecting the column names from the drop-down column list:
Also, you can click the **Search** button and use the search options to filter the data. You can select any column from the drop-down box and enter a corresponding value to filter the data displayed in the table.

**Note**

The Search functionality is case-sensitive, and you must provide the exact search criteria.

To deploy L4-L7 configuration by using StyleBook in Citrix ADM:

1. Click the StyleBook name that appears as a URL in the tabular view.
2. In the Configuration window, double-click **StyleBook**.

3. In the Deploy Configuration window, do the following:
   
   a) In the **Application Name** field, enter the name for the ADC feature configuration that corresponds to the application’s service graph in the APIC.

   b) In the Service (ports) Settings section, click +.
c) In the **Settings for EPG & endpoints (ports) defined in the service graph** window, enter values for the parameter populated from the StyleBook and click **Create**.

d) Click **Create**.

The L4-L7 configuration specified in the StyleBook is deployed, in Citrix ADM. You can view the Style-
Boook configuration from the **Application** tab, by navigating to **Application > Configuration**.

**APIC fault reports**

August 1, 2019

When you deploy a Citrix ADC device package in Cisco ACI, the Cisco APIC reports any failures. You can view the fault reports at any level of the APIC (for example, device, tenant, EPGs, or service graph). The screen shot below shows a fault report at the device level. For more information on faults, see [http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html).

Select any APIC entity and click the **Faults** tab to display the faults reported by the APIC for that entity.
Logs generated by Citrix ADM

August 1, 2019

Citrix Application Delivery Management (ADM) provides extensive logging that can help troubleshoot issues. The generated logs (admin.log) are located at: /var/controlcenter/log/

You can log on to Citrix ADM and use the shell to navigate to the Citrix ADM directory structure. Following is a sample snippet of a Citrix ADM log for an APIC's graph deployment.

```
2016-06-29 10:58:33,816 DEBUG APIC Config = {
  (0, '', 5230): {
    'dn': 'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-ctxcktx1',
    'state': 1,
    'transaction': 0,
    'ackedstate': 0,
    'tenant': 'coke_SDX2',
    'ctxName': 'ctxcktx1',
    'value': {
      (10, '', 'ADCHybridMode_1_Consumer_1'): {
        'state': 1,
        'transaction': 0,
        'value': {
          (3, 'ADCFunction', 'N1'): {
            'state': 1,
            'transaction': 0,
            'ackedstate': 0,
            'value': {
            }}}}}}
```
(4, 'mFCngNetwork', 'mFCngnetwork'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
    'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
}
}
,
(4, 'internal_network', 'internal_network'): {
    'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
    'state': 1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate': 0 }
}
}
,
(2, 'external', 'consumer'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
    'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
}
}
,
(4, 'mFCngStylebook', 'mFCngStylebook'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
    'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0 }
}
}
,
(2, 'internal', 'provider'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
    'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
}
}
,
'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
,
(4, 'Network', 'network'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {

© 1999-2019 Citrix Systems, Inc. All rights reserved.
(5, 'type', 'type'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP'}
, (5, 'hostroute', 'hostroute'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED'}
, (5, 'ipaddress', 'ipaddress'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1'}
, (5, 'dynamicrouting', 'dynamicRouting'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED'}
, (5, 'netmask', 'netmask'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0 '}
}
}
}
}
}
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {  
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', 'ackedstate': 0, 'encap': '2129920_32778'}
, (4, 'Stylebook', 'stylebook_1'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {  
(5, 'name', 'stylebookName'): {  
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'}
}
}
}
}
}
, 'txid': 10000}
}
2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'univ/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {  
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]}'}
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790}
2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
2016-06-29 10:58:33,832 DEBUG SUCCESS updated track with new task 2
2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
Details = 10.102.102.62 +++++++++++++++++

2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
2016-06-29 10:58:33,867 DEBUG Host name from device = ADCHybridMode_1

"InProgress","message":null,"replication_status":"","target":
10.102.102.81","operation":"POST","entity_type":"apic",""
entity_id":null
}

2016-06-29 10:58:44,141 DEBUG Save config Response = {
"errorcode": 0, "message": "Done", "severity": "NONE" }

2016-06-29 10:58:44,141 DEBUG ++contextAwareFlag = True
2016-06-29 10:58:44,141 DEBUG +++getTenantName = {
'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
}

2016-06-29 10:58:44,142 DEBUG Service health details = {
collection length = 0
2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
0
2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection = {
((0, ''), (1, ''), (5790), (3, 'ADCFunction', 'N1')):
{ 'faults': [], 'state': 0, 'health': [([0, '', 5230), (1, ''), 5790),
(3, 'ADCFunction', 'N1')], 0) }

2016-06-29 10:58:44,142 DEBUG +++getServiceHealth Fault List =
[]
2016-06-29 10:58:44,142 DEBUG Service HEALTH final response = {
'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
: [([0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0) }

2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
"errorcode": 0, "message": "Done", "severity": "NONE" }
2016-06-29 10:58:44,237 DEBUG +++ Faults respCol = {
'10.102.102.62': 
'10.102.102.62': 

© 1999-2019 Citrix Systems, Inc. All rights reserved.
u'errorcode': 0, u'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': u'add_op'}

, (7, '', '2129920_32778'): {
  'vlan': {
    u'errorcode': 0, u'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': u'add_op'}
  , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')), (2, 'internal', 'provider')), 'nsip'): {
    'vlan_nsip_binding': {
      u'errorcode': 0, u'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': u'bind_op'}
  }
  , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', 'internal_snip')): {
    'nsip': {
      u'errorcode': 0, u'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': u'add_op'}
  }
  , (): {
  }
  , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
    'vlan_interface_binding': {
      u'errorcode': 0, u'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': u'bind_op'}
  }
}

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op
2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op
2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op
2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op
2016-06-29 10:58:44,237 DEBUG +++++++++++++++ ServiceAudit response = {
  'faults': [], 'state': 0, 'health': []
}
2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
  'graphDN': u'unii/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-
Logs generated by hybrid-mode device package

August 1, 2019

The Citrix ADC Hybrid Mode device package generates configuration-related logs and monitoring-related logs. The generated logs are located at /data/devicescript/Citrix.NetScalerMAS.1.0/logs.

Following is a sample snippet of a Cisco APIC’s debug.log:

```
2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62, 24063] Device manager details ip = 10.102.102.81, port = 80
```
Thread DEBUG ++++++

2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62, 24063] ++++++ serviceAudit request ++++++++

2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62, 24063] +++++++ getStyleBookObjects ++++++++

2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62, 24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 = {
5 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6 (5, 'name', 'stylebookName'): {
7 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
8 }
9 }


2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62, 24063] NMAS collection retCol= {
13 'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, ''), 5230), (4, 'Stylebook', 'stylebook_1')) }


17 u'stylebook': {
18 u'uses builtin namespaces': {
19 u'netscaler.config': u'10.5' } , u'name': u'APIC-HTTP-LB', u'used by stylebooks': [], u'namespace': u'
20 com.citrix.adc.stylebooks', u'source': u'---\nnname: APIC-HTTP-LB\nnnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name: "Sample StyleBook for APIC Load Balanced Application"\ndescription: "This is a sample StyleBook for HTTP Load Balanced Application configuration via APIC\nschema-version: "1.0"\nnimport-stylebooks: \n - \n namespace: netscaler.nitro.config\nprefix: ns\nversion: "10.5"\n - \n namespace: com.citrix.adc.stylebooks\nprefix: "stlb"\nversion: "1.1"\nparameters -default-sources: \n - stlb::APIC-ROOT\nsubstitutions: \n lb-name( appname, port): $appname +"-" + str($port) +"-lb"\nsg-name( appname, port): $appname +"-" + str($port) +"-sg"\nhealthmonitor[]:\ntrue: "NO"\nfalse: "YES"\ncomponents: \n - \n name: lbvserver\ntype: ns::lbvserver\nrepeat: $parameters.app-services\nrepeat-item: app\nproperties: \n
n   name: $substitutions.lb-name($parameters.appname, $app.
virtual-port)\n   ipv46: $app.virtual-ip\n   port: $app.
virtual-port\n   servicetype: $app.protocol\n   lbmethod?:
   $app.algorithm\n   persistencetype?: $app.persistence\n   - \n   name: svcgrp\n   type: ns::servicegroup\n   repeat: $parameters.
app-services\n   repeat-item: app\n   properties: \n   name: $substitutions.sg-name($parameters.appname, $app.virtual-port)\n   servicetype: $app.protocol\n   useproxyport?: $app.sg-
advanced.useproxyport\n   usip?: $app.sg-advanced.usip\n   cip?: $app.sg-advanced.cip\n   cipheader?: $app.sg-advanced.
cipheader\n   healthmonitor?: $substitutions.healthmonitor($app.
skip_healthmonitor)\n   components: \n   \n   lbserver-svg-binding\n   type: ns::
   lbserver_servicegroup_binding\n   properties: \n   name: $substitutions.lb-name($parameters.appname, $app.virtual-port)
   servicegroupname: $parent.properties.name\n   - \n   name: svg-members\n   type: ns::
   servicegroup_servicegroupmember_binding\n   condition: $app.
server-ips\n   repeat: $app.server-ips\n   repeat-item:
   serverip\n   properties: \n   ip: $serverip\n   port: $app.server-port\n   servicegroupname: $parent.
properties.name\n   noutputs: \n   \n   name: lbservers\n   value: $components.lbserver\n   - \n   name: servicegroups\n   value: $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
   u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
   ': u'APIC-ROOT' }
}]
}

2016-06-28 03:06:54.359221 DEBUG Thread=20 18732 [10.102.102.62, 24063] ++++ Response from Device Mgr serviceAudit = {
"APIC"[:]
}
2016-06-28 03:06:54.359266 DEBUG Thread=20 18733 [10.102.102.62, 24063] ++++++++++++++ serviceAudit response = {
"APIC"[:]
}
2016-06-28 03:06:54.359306 DEBUG Thread=20 18734 [10.102.102.62, 24063] ++++++++++++++ serviceAudit response headers content type = application/json; charset=utf-8
2016-06-28 03:06:54.359394 DEBUG Thread=20 18735 [10.102.102.62, 24063] ++++++++++++++ serviceAudit response headers = {
'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding': 'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016 10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': 'application/json; charset=utf-8'}


2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62, 24063] ++++++++++++++ pollingStatus = True, pollingTime = 0

2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62, 24063] ++++++++++++++ pollingResponse json = {

u'journalcontext': {

u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name': u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin', u'start_time': u'2016-06-29T00:58:33.760565', u'is_default': u'false', u'end_time': None, u'target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'replication_status': u''}

2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62, 24063] ++++++++++++++ pollingStatus = True, pollingTime = 1

2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62, 24063] ++++++++++++++ pollingResponse json = {

u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name': u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin', u'start_time': u'2016-06-29T00:58:33.760565', u'is_default': u'false', u'end_time': None, u'target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'replication_status': u''}


u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin', u'start_time': u'2016-06-29T00:58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'}
2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62, 24063] Cluster ("uni/tn-coke_SDX2/1DevVip-ADCHybridMode_1", (0, '', 5230)), transaction: 0
   'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False, 'devs': {
      'ADCHybridMode_1_Device_1': {
         'state': 0, 'virtual': False, 'manager': {
            'hosts': {
               '10.102.102.81': {
                  'port': 80 }
            }
          }
       },
       'name': 'NMAS_1', 'creds': {
          'username': 'nsroot', 'password': '<hidden>' }
    }
   }
   'manager': {
      'hosts': {
         '10.102.102.81': {
            'port': 80 }
      }
   }
   'contextaware': True, 'port': 80, 'creds': {
      'username': 'nsroot', 'password': '<hidden>' }
}
is 0
2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62, 24063] Deleting ("uni/tn-coke_SDX2/1DevVip-ADCHybridMode_1", (0, '', 5230))
Citrix ADC device package in Cisco ACI’s cloud orchestrator mode

August 1, 2019

With Application Policy Infrastructure Controller (APIC) version 3.1 Citrix Citrix ADC, and Cisco ACI expand the joint integration portfolio to provide a new solution addressing customer’s needs. The new integration mode, ACI Cloud Orchestrator Mode, simplifies L4-L7 integrations by abstracting configuration complexity through standardized parameters. The solution works seamlessly to automate L4-L7 services, achieving the goals of agile application deployments, operational flexibility, and simplicity.

The Cisco ACI cloud orchestrator mode by using Citrix ADC solution provides the following benefits:

- Automation of L4-L7 services reduces the human error.
- The pre-built integration of Cisco ACI solution helps you in reducing the deployment time, and increases the performance of applications, such as web applications, virtual machines, and SQL.
- Fully integrated visibility into the health of applications such as web applications, virtual machines, and SQL across physical and virtual network components.

The ACI cloud orchestrator mode now gives you more choices to utilize the new simplified APIC GUI directly or by selecting any cloud orchestrator, such as Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize, or any other based on your preference. This new change is achieved by exposing a set of ADC attributes as ADC schema. These attributes are mapped in the device packages function profiles. You can provide values for these attributes while provisioning the ADC service by the cloud orchestrator (Cisco Cloud Center or Wireless Application Protocol (WAP)).

The following illustration provides an overview of Citrix ADC in a cloud orchestration solution:
The cloud orchestrator mode solution using Microsoft Azure Pack involves many integration points, such as Azure Pack to Cisco APIC, Cisco APIC to System Central virtual machine Manager (SCVMM), and Cisco APIC to Citrix ADC. As a tenant in the private cloud, you can enable NAT, provision network services, and can add a load balancer.

Azure Pack supports tenant and administrator portals, and each of them has their own set of operations that can be performed.

- As an administrator, you can perform administrative tasks such as ACI registration, VIP range, Citrix ADC device association with virtual machine cloud, and tenant user account creation.
- As a tenant, you can perform tasks such as log on to the Azure Pack tenant Portal and configure the network, bridge domains, and Virtual Routing and Forwarding (VRFs), and can use the Citrix ADC load balancing and RNAT features.

The following illustration provides an overview of Azure Pack in a cloud mode solution:
**Important**

- Cloud administrator can facilitate with L4-L7 schema supported by APIC and any additional changes can be done by APIC administrator directly in the APIC. This allows you to configure and deploy Citrix ADC at par with the supported feature set.

- Tenants can deploy multiple VIP addresses with different ports for the same network. You must ensure that the IP and port combination is unique.

- The Citrix ADC device package supports only single-context deployment. Each tenant gets a dedicated Citrix ADC instance.

- Wireless Application Protocol (WAP) supports Citrix ADC MPX appliances and Citrix ADC VPX appliances (includes Citrix ADC VPX instances deployed on the Citrix ADC SDX platform).

The cloud orchestrator mode device package supports both fully managed mode and service manager mode. The fully managed mode package supports a wide variety of function profiles, such as simple...
load balancing, content switching, SSL offload, and other profiles. These function profiles cover a complete feature set and deployment mode of the Citrix ADC. Similarly, service manager mode device package supports one-arm and two-arm configuration and deployment of Citrix ADC using APIC. The Citrix Application Delivery Management (ADM) acts as service manager for APIC and you can use Citrix ADM to configure Citrix ADC L4-L7 parameters.

**Note**

In service manager mode (hybrid mode), you cannot reuse or reassign the same server IP address, which is already present in the Citrix ADC appliance.

Cloud orchestrator mode function profile has a set of parameters mapped to APICs ADC schema and the orchestrator uses these parameters. The cloud orchestrator provides the values for ADC parameters (VIP, while provisioning the Citrix ADC through APIC). The orchestrator communicates with APIC’s APIs and passes the ADC specific details as part of the payload for a specific function profile. Internally, APIC extracts the values and passes them to the device package which configures the Citrix ADC internally.

For more information on the complete list of ADC schema’s, which are supported by Cisco APICs, see Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.1(i).

The fully managed mode device package supports the following function profiles:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
The service manage mode device package supports the following cloud mode function profiles:

1. ADCOneArmFunctionProfileCM
2. ADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

Citrix ADC supports the above-mentioned function profiles. The APIC supports a subset of these parameters in the ADC schema. If there are any unsupported attributes by Cisco ACI present in the function profile, you have to clone the cloud orchestrator mode function profile and provide the values for all unsupported attributes by APIC and must save the attributes. Later, the orchestrator can use the newly cloned function profile.

Citrix Cloud Mode Device Package supports Citrix ADC 12.0 and service manager mode uses Citrix ADM 12.0 as well. Device package has changed the model version from 1.0 to 2.0 and can be used as a new install. Cloud orchestrator Mode Device package cannot be upgraded from previous device package versions since the model version is changed.

Cloud orchestrator Mode device packages can be used in regular deployment as well. The package does not mandate user to provision Citrix ADC through any cloud orchestrator. The device package is compatible with just APIC and APIC with cloud orchestrator.
Licenses for Citrix ADM License server in high availability

August 1, 2019

License files - ADM VIP licenses, CICO licenses, and pooled capacity licenses - issued to Citrix ADM server are bound to the host ID of the server to which they are issued and cannot be assigned to other servers. Citrix ADM servers that are configured as license servers and deployed in high availability need to have the same license files installed on both servers. Because of this limitation of the license files, Citrix ADM license servers could not be deployed in high availability mode.

Citrix ADM now allows you to assign the same license to both Citrix ADM license servers that are deployed in high availability.

Whenever a failover occurs, the secondary server now assumes the role of the primary server. The real host ID of the old primary server is configured as the virtual host ID of the new primary server. The license files recognizes that the host ID of the new primary server is same as that of the old primary server. The license files are now assigned to the new primary server as well.

**Note**
While upgrading the ADM servers in high availability, the license files are automatically copied to both the servers.

**Definitions used in the document**

- **Real Host ID.** This is the Host ID is generated from MAC Address of MAS server. MAS standalone server will have a unique Host ID generated for each deployment.

- **Virtual Host ID.** This is the virtual Host ID used for ADM deployment in high availability. Real Host ID of ADM primary server in high availability is used as virtual Host ID. The virtual Host ID is auto generated in during HA deployment. This virtual Host ID is stored in ADM database in encrypted format and cannot be changed by the customer. Virtual Host ID will have preference over real Host ID.

**Architecture of ADM servers in high availability**

**Workflow during Citrix ADM server deployment in high availability mode**

Assume that Node1 is the current primary server and Node2 is the current secondary server.

The virtual Host ID of Node1 is synced with Node2.

1. License files available in Node1 will be synced to Node2.
2. Any new license files (node locked to virtual Hoss ID) also will be synced to Node2 periodically.

3. ADM ensures that the License Server is running only on Node1 to avoid doubling of license capacity.

4. Citrix ADC instances will check-out licenses from Node1 using floating IP address.

**Citrix ADC pooled capacity**

August 1, 2019

Citrix ADC pooled capacity 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 Citrix 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, consequently, 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.

This licensing framework maximizes bandwidth utilization by ensuring that instances are not allocated bandwidth in excess of their requirement. The ability of Citrix 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 Citrix ADC licenses in the pool from one instance to another.

**How Citrix ADC pooled capacity licensing works**

Citrix ADC pooled capacity has the following components:

- Citrix ADC instances, which can be categorized into:
  - Zero-capacity hardware
  - Standalone VPX instances or CPX instances
- Bandwidth pool
- Instance pool
- Citrix ADC license server
Zero-capacity hardware

When managed through Citrix ADC pooled capacity, MPX and SDX instances are referred to as “zero-capacity hardware” because these instances cannot function until they check resources out of the bandwidth and instance pools. Accordingly, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware require a platform license to be able to check out bandwidth and an instance license from the common pool. However, you cannot use Citrix ADC pooled capacity to manage and install platform licenses. You must install a platform license manually, by using the hardware serial number or the license access code. After a platform license is installed, it is locked to the hardware and cannot be shared across Citrix ADC hardware instances on demand. However, you can manually move the platform license to another Citrix ADC hardware instance.

Zero-capacity hardware, running the NetScaler software release 11.1 Build 54.14 or later, support NetScaler pooled capacity. For more information, see table 1 below.

Standalone Citrix ADC VPX instances

Citrix ADC VPX instances running Citrix ADC software release 11.1 Build 54.14 and later on the following hypervisors supports pooled-capacity:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Citrix ADC VPX instances running Citrix ADC software release 12.0 Build 51.24 and later on the following hypervisors and cloud platforms supports pooled-capacity
• Microsoft Hyper-V
• Amazon AWS
• Microsoft Azure

**Note**

To enable communication between Citrix ADM and Microsoft Azure or AWS, an IPSEC tunnel has to be configured. For more info, see Add Citrix ADC VPX Instances Deployed in Cloud to Citrix ADM. Unlike zero-capacity hardware, VPX does not require platform license. To process traffic, it must check out bandwidth and an instance license from the pool.

**Standalone Citrix ADC CPX instances**

Citrix ADC CPX instances deployed on a Docker host supports pooled-capacity. Unlike zero-capacity hardware, CPX does not require platform license. To process traffic, it must check out an instance license from the pool.

**Bandwidth Pool**

The bandwidth pool is the total bandwidth that can be shared by Citrix ADC instances, both physical and virtual. The bandwidth pool comprises separate pools for each software edition (Standard, Enterprise, and Platinum). A given Citrix ADC instance cannot have bandwidth from different pools checked out concurrently. The bandwidth pool from which it can check out bandwidth depends on its software edition for which it is licensed.

**Instance pool**

The instance pool defines the number of VPX instances or CPX instances that can be managed through Citrix ADC pooled capacity or the number of VPX instances in an SDX-Z instance.

When checked out from the pool, a license unlocks the MPX-Z, SDX-Z, VPX, and CPX instance’s resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

**Note**

The Management Service of an SDX-Z does not consume an instance.

**Citrix ADC license server**

Citrix ADC license server is a component in Citrix Application Delivery Management (ADM). Citrix ADC pooled capacity uses Citrix ADC license server to manage pooled capacity licenses: bandwidth pool li-
censes and instance pool licenses. You can use Citrix ADM to manage pooled capacity licenses without a MAS license.

When checking out licenses from bandwidth and instance pool, Citrix ADC form factor and hardware model number on a zero-capacity hardware determines

- The minimum bandwidth and the number of instance that a Citrix ADC instance must check-out before being functional.
- The maximum bandwidth and the number of instances that a Citrix ADC can check-out.
- The minimum bandwidth unit for each bandwidth check-out. Minimum bandwidth unit is the smallest unit of bandwidth that a Citrix ADC has to check-out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if minimum bandwidth unit of a Citrix ADC is 1 Gbps, 100 Gbps can be checked out, but not 200 Mbps or 150.5 Gbps. Minimum bandwidth unit is different from the minimum bandwidth requirement. A Citrix ADC instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check-out additional bandwidth with minimum bandwidth unit.

Tables 1, 2, and 3 summarize the maximum bandwidth/instances, minimum bandwidth/instances, and minimum bandwidth unit for all supported NetScaler instances. Table 4 summarizes the license requirement for different form factors for all supported Citrix ADC instances:

Table 1. For MPX and SDX

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum bandwidth (Gbps)</th>
<th>Minimum bandwidth (Gbps)</th>
<th>Minimum instances</th>
<th>Maximum instances</th>
<th>Minimum bandwidth unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPX 8900Z</td>
<td>33</td>
<td>5</td>
<td>NA</td>
<td>NA</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>MPX-14000Z</td>
<td>100</td>
<td>20</td>
<td>NA</td>
<td>NA</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>series</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPX-15000Z</td>
<td>100</td>
<td>20</td>
<td>NA</td>
<td>NA</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>series</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPX-25000Z-40G</td>
<td>200</td>
<td>100</td>
<td>NA</td>
<td>NA</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX-84XX</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>series</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDX 89XX</td>
<td>30</td>
<td>10</td>
<td>2</td>
<td>7</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>series</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Citrix Application Delivery Management 12.1

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Bandwidth (Gbps)</th>
<th>Minimum Bandwidth (Gbps)</th>
<th>Minimum Instances</th>
<th>Maximum Instances</th>
<th>Minimum Bandwidth Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDX-115XX series</td>
<td>42</td>
<td>8</td>
<td>5</td>
<td>20</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX-14000Z series</td>
<td>100</td>
<td>20</td>
<td>5</td>
<td>25</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX 15000Z-50G</td>
<td>100</td>
<td>20</td>
<td>5</td>
<td>55</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX-175XX series</td>
<td>20</td>
<td>20</td>
<td>10</td>
<td>40</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX-22XXX series</td>
<td>40</td>
<td>40</td>
<td>20</td>
<td>80</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX-25000Z-40G</td>
<td>200</td>
<td>100</td>
<td>20</td>
<td>115</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>SDX 26000Z-100G</td>
<td>200</td>
<td>100</td>
<td>20</td>
<td>115</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Table 2. For CPX**

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Bandwidth (Gbps)</th>
<th>Minimum Bandwidth (Gbps)</th>
<th>Minimum Instances</th>
<th>Maximum Instances</th>
<th>Minimum Bandwidth Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPX</td>
<td>1</td>
<td>NA</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

**Table 3. For Citrix ADC VPX on Hypervisors and Cloud services**

<table>
<thead>
<tr>
<th>Hypervisor/Cloud Service</th>
<th>Maximum Bandwidth (Gbps)</th>
<th>Minimum Bandwidth (Mbps)</th>
<th>Minimum Instances</th>
<th>Maximum Instances</th>
<th>Minimum Bandwidth Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Hypervisor</td>
<td>40 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>100 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Linux KVM</td>
<td>100 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Hypervisor/Cloud Service</td>
<td>Maximum bandwidth (Gbps)</td>
<td>Minimum bandwidth (Mbps)</td>
<td>Minimum instances</td>
<td>Maximum instances</td>
<td>Minimum bandwidth unit</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>3 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>AWS</td>
<td>5 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Azure</td>
<td>3 Gbps</td>
<td>10 Mbps</td>
<td>1</td>
<td>1</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

The following table summarizes the license requirement for different form factors:

<table>
<thead>
<tr>
<th>Zero Capacity Hardware Purchase</th>
<th>Bandwidth &amp; Edition Subscription</th>
<th>Instance Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPX</td>
<td>License required</td>
<td>License required</td>
</tr>
<tr>
<td>SDX</td>
<td>License required</td>
<td>License required</td>
</tr>
<tr>
<td>VPX</td>
<td>License required</td>
<td>License required</td>
</tr>
<tr>
<td>CPX</td>
<td>License required</td>
<td></td>
</tr>
</tbody>
</table>

**Configure Citrix ADC pooled capacity**

August 1, 2019

Citrix Application Delivery Management (ADM) is the license server for all Citrix ADC instances added to ADM. You can upload the pooled capacity license files (Bandwidth Pool or Instance Pool) to the license server. You can allocate licenses in the license pool to Citrix ADC instances on demand. You can allocate the licenses from Citrix ADM, or you can check-out the licenses from Citrix ADC instances (MPX-Z /SDX-Z/VPX/CPX) according to the minimum and maximum capacity of the instance.
Supported hardware and software versions

<table>
<thead>
<tr>
<th>Citrix ADC Software Version</th>
<th>Citrix ADC MPX Zero-Capacity Hardware</th>
<th>Citrix ADC SDX Zero-Capacity Hardware</th>
<th>Supported Hypervisors for Citrix ADC VPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0 Build 51.24 and later</td>
<td></td>
<td></td>
<td>Microsoft Hyper-V, Amazon AWS, Microsoft Azure</td>
</tr>
</tbody>
</table>

Configuring Citrix ADM as license server

You can configure Citrix ADM as a license server for the Citrix ADC pooled capacity. There are two ways for a Citrix ADC instance to get bandwidth and or instance license:

- A Citrix ADC instance can initiate the check-out request to Citrix ADM to obtain its bandwidth and/or instance licenses.
- The licenses can be allocated to a Citrix ADC instance through Citrix ADM.

**Note**

Pooled Capacity is displayed on Citrix ADM only if pooled licenses are added to the Citrix ADM.

Following are the operating modes of the Citrix ADC instances that are using the Citrix ADC Pooled Capacity:

- **Optimum** – Instance is running with proper license capacity.
- **Capacity mismatch** – instance is running with a capacity less than user configured.
- **Grace** - Instance is running on grace license.
- **Grace & Mismatch** – Instance is running on grace but with a capacity less than user configured.
- **Not available** – Instance is not registered with Citrix ADM for management or Nitro communication from Citrix ADM to Instance is not working.
- **Not allocated** – License is not allocated in instance.

**To install license files on Citrix ADM:**

1. In a web browser, type the IP address of the **Citrix ADM** (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Networks > Licenses**.
4. In the **License Files** section, select one of the following options:
   - **Upload license files from a local computer** – If a license file is already present on your local computer, you can upload it to the Citrix ADM. To add license files, click **Browse** and select the license file (.lic) that you want add. Then click **Finish**.
     
     **Note**
     
     If the uploaded license files does not add the licenses in the Citrix ADC Pooled capacity, you can select the license files and click **Apply Licenses** to add the licenses to the pool.
   - **Use license access code** – Citrix emails the License Access Code (LAC) for the licenses that you purchase. To add license files, enter the LAC in the text box and then click **Get Licenses**.
     
     **Note**
     
     At any time, you can add more licenses to Citrix ADM from the License Settings.

**To allocate Citrix ADC Pooled Capacity licenses from Citrix ADM:**

**Note**

If you have not registered the Citrix ADC instance with Citrix ADM, you can check-out licenses from Citrix ADM, but cannot allocate from Citrix ADM to the Citrix ADC pooled capacity enabled instance.

Ensure that the following prerequisite is met before you allocate pooled capacity licenses to the ADC instances.

**Prerequisite**

Before you can manage your instance’s pool licenses through Citrix ADM, you must register the Citrix ADC instance with the Citrix ADM. In the Citrix ADC GUI, navigate to **System > Licenses > Manage Licenses** and select the **Register with Citrix ADM for manageability** check box when adding the Citrix ADM IP.
In the Username and Password fields on the above screen, enter Citrix ADM credentials.

After the instance is registered with the license server, allocate the licenses as follows:

1. In a web browser, type the IP address of Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. On the Configuration tab, navigate to Networks > Licenses > Pooled Capacity.
4. Click on the license pool that you want to manage.
5. Select a Citrix ADC instance from the list of available instances by clicking on the > button.
6. If you want to change or release a license allocation, click **Change allocation** or **Release allocation**.

![Change License Allocation](image)

7. If you click **Change allocation**, a pop-up window with the available licenses in the license server appears.

8. You can choose the bandwidth or instance allocation to the Citrix ADC instance by setting the **Allocate** drop-down options. After making your selections, click **Allocate**.

9. You can also change the allocated license edition from the drop-down options in the Change License Allocation window.

### Configuring Citrix ADC Pooled Capacity on MPX-Z

MPX-Z is the Citrix ADC pooled-capacity enabled Citrix ADC MPX appliance. MPX-Z supports bandwidth pooling for Platinum, Enterprise, or Standard edition licenses.

MPX-Z require its platform licenses before it can connect to the license server. You can install the MPX-Z platform license by either uploading the license file from a local computer or using the instance's hardware serial number, or the License Access Code from **System > Licenses** section of the Citrix ADC Instance’s GUI. If you remove the MPX-Z platform license, the pooled-capacity feature is disabled and all the checked-out licenses are checked in to the license server.

You can dynamically modify the Bandwidth of a MPX-Z instance without a restart. A restart is required only if you want to change the license edition.
When you restart the instance, it automatically checks out the pooled licenses required for its configured capacity.

**Configuring Citrix ADC Pooled Capacity on a Citrix ADC VPX Instance**

A pooled-capacity enabled Citrix ADC VPX instance can check-out licenses from a bandwidth pool (Platinum/Enterprise/Standard editions). You can use the Citrix ADC GUI to check-out licenses from the license server.

You can dynamically modify the Bandwidth of a VPX instance without a restart. A restart is required only if you want to change the license edition.

When you restart the instance, it will automatically check-out the pooled licenses required for its configured capacity.

**Allocating Pool Licenses to a Citrix ADC MPX-Z or Citrix ADC VPX Instance**

To allocate your licenses:

1. In a web browser, type the IP address of the Citrix ADC instance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the Configuration tab, navigate to **System > Licenses > Manage Licenses**, click **Add New License** and select **Use Pooled Licensing**.
4. Enter the details of the license server in the Server Name/IP Address field.

5. If you want to manage your instance’s pool licenses through Citrix ADM, select the Register with Citrix ADM for manageability check box and enter ADM credentials.


7. You can change or release the license allocation by selecting Change allocation or Release allocation.
8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

   **Note**
   A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.

   ![Allocate licenses](image)

   **Allocate licenses**

<table>
<thead>
<tr>
<th>Pool</th>
<th>Total</th>
<th>Available</th>
<th>Allocate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>200</td>
<td>197</td>
<td>1</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>500 Gbps</td>
<td>489.9 Gbps</td>
<td>0 (Mbps)</td>
</tr>
</tbody>
</table>

   [Get Licenses] [Cancel]

9. You can allocate bandwidth or instances to the Citrix ADC instance from the **Allocate** drop-down list. Then click **Get Licenses**.

10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

   **Note**
   Bandwidth allocation should be a multiple of the minimum bandwidth unit.

**Configuring Citrix ADC Pooled Capacity on SDX-Z**

An SDX-Z instance is a pooled-capacity enabled instance of Citrix ADC SDX. SDX-Z supports bandwidth pooling for Platinum, Enterprise, and Standard editions, and instance pooling. After you apply the
SDX-Z platform license, the Management Service provides options for checking licenses out from and back into the licensing server, and for allocating bandwidth capacity to the Citrix ADC instances running on the SDX-Z platform.

**Note**

Citrix ADC VPX instances running on SDX-Z cannot directly check licenses out from or in to the license server. This can be done by the Management Service in SDX.

You can install the SDX-Z platform license by either uploading the license file from the local computer or using the instance's hardware serial number, or the License Access Code.

If you remove the SDX-Z platform license, the pooled-capacity feature is disabled and all the licenses are checked back into the licensing server.

**Note**

If you reboot the instance, it checks-out the pooled licenses required for its configured capacity.

**Pool Capacity on Citrix ADC SDX**

**Instance Pool:**

An SDX appliance can provision same number of instances that are available in the instance pool of the SDX appliance.

**Bandwidth Pool:**

During Citrix ADC instance provisioning, bandwidth is allocated to the instance. You can select the edition and required bandwidth to provision a Virtual Citrix ADC instance. The Management Service allows the provisioning to continue only if the instance has sufficient bandwidth for the requested edition. You are notified if the bandwidth is insufficient.

**Note**

Bandwidth modification does not require an instance restart.

**Allocating Pool Licenses to a Citrix ADC SDX-Z Instance**

**To allocate your licenses:**

1. In a web browser, type the IP address of your Citrix ADC SDX-Z instance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the Configuration tab, navigate to **System > Licenses**, and go to **Pooled Capacity**.
4. Enter the details of the license server in the **Server Name/IP Address** field.

5. If you want to manage your instance's pool licenses through Citrix ADM, select the **Register with Citrix ADM** check box and enter the ADM credentials.

6. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.

**Note**

The checked out licenses are stored in a separate pool by the ADM.
7. To change the license allocation for a specific VPX instance in the SDX-Z instance, select the instance from the Instances section, and click Change allocation. A new window displays the available licenses.

8. You can change the bandwidth edition of the instance from the Feature License drop-down list, and the required bandwidth in the Throughput (mbps) field. Then click Done.

   **Note**
   
   Bandwidth allocation should be an integer multiple of the minimum bandwidth unit of the corresponding form factor.

**Configuring Citrix ADC Pooled Capacity on a Citrix ADC CPX Instance**

While provisioning the Citrix ADC CPX instance, you can configure the Citrix ADC CPX instance to use Citrix ADC Pooled Capacity. In the docker run command, you need to provide the Citrix ADC Licensing Server details. The Citrix ADC CPX instance checks-out licenses from the Instance pool.

   **Note**
   
   By default, Citrix ADC CPX instance checks-out an instance license from the instance pool and the throughput is automatically set to 1000 Mbps. You cannot modify the 1000 Mbps bandwidth allocated to the instance.

You can download Citrix ADC CPX from the Docker App Store. On the Docker host, to download Citrix ADC CPX, run the following command:

```
docker pull store/citrix/netscalercpx: <version>
```

**To configure Citrix ADC Pooled Capacity while provisioning the Citrix ADC CPX Instance:**
While provisioning a Citrix ADC CPX instance, define the Citrix Licensing Server as an environmental variable in the `docker run` command as shown below:

```
1  docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --cap-add=NET_ADMIN <REPOSITORY>:<TAG>
```

Where:

- `<LS_IPADDRESS>` is the IP address of the Citrix Licensing Server.
- `<LS_PORT>` is the port of the Citrix Licensing Server. By default, the port is 27000.

**Upgrade a Perpetual License in Citrix ADC MPX to Citrix ADC Pooled Capacity**

August 1, 2019

Citrix ADC MPX appliance with perpetual license can be upgraded to Citrix ADC Pooled Capacity license. Upgrading to Citrix ADC Pooled Capacity license enables you to allocate licenses from the license pool to Citrix ADC appliances on demand. You can also configure Citrix ADC Pooled Capacity license for Citrix ADC instances configured in high availability mode. To configure Citrix ADC Pooled Capacity license for Citrix ADC MPX instances in high availability mode, see Upgrade the Perpetual License in Citrix ADC MPX High Availability Pair to Citrix ADC Pooled Capacity.

**Important**

For upgrading Citrix ADC MPX appliance to Citrix ADC Pooled Capacity license, you need to upload the MPX-Z license to the appliance.

**To upgrade to Citrix ADC Pooled Capacity:**

1. In a Web browser, type the IP address of the Citrix ADC appliance, such as `http://192.168.100.1`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the Configuration tab, navigate to **System > Licenses**.
5. In the details pane, click **Manage Licenses**, click Add **New License**.
6. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.
7. After the license is uploaded, click **Reboot** to reboot the appliance.

Ensure there are no configurations saved before rebooting the appliance.

**Warning**

After applying the MPX-Z license, the features including SSL offloading on the appliance become unlicensed. The appliance stops processing HTTPS requests.

If the **Secure Access Only** option is enabled on the appliance before the upgrade, you cannot connect to the appliance through Citrix ADM GUI using HTTPS.

8. On the **Confirm** page, click **Yes**.

9. After the appliance reboots, logon to the appliance.
10. **On the Welcome page, click on the Licenses section.**

11. **In the License Server section, do the following:**
a) In the **Server Name/IP Address** field, enter the license server details.

b) In the **License Port** field, enter the licence server port. Default value: 27000.

c) If you want to manage your instance’s pool licenses through Citrix ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

d) Click **Continue**.

12. In the Allocate licenses window, do the following:

   a) Select the license edition from the drop-down list.
b) Allocate the bandwidth to the Citrix ADC appliance from the Allocate menu and click Get Licenses.

![Allocate Licenses](image)

b) Allocate the bandwidth to the Citrix ADC appliance from the Allocate menu and click Get Licenses.

![Allocate Licenses](image)

c) When prompted, click Reboot to reboot the appliance.

13. Once the Citrix ADC MPX appliance reboots, logon to the Citrix ADC MPX appliance. On the Welcome page, click Continue.

![Welcome](image)

The Licenses page lists all the licensed features.
14. Navigate to **System > Licenses** and click **Manage Licenses**.

On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated bandwidth.
Upgrade the Perpetual License in Citrix ADC MPX High Availability Pair to Citrix ADC Pooled Capacity

For Citrix ADC MPX Appliances configured in high availability mode, you have to configure Citrix ADC Pooled Capacity on both the primary and secondary Citrix ADC instances in the HA pair. You need to allocate licenses of the same capacity to both the primary and secondary Citrix ADC instances in the HA pair. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need to allocate 2 Gbps capacity from the common pool so that you can allocate 1 Gbps capacity each to the primary and secondary Citrix ADC instances in the HA pair.

Important
For upgrading Citrix ADC MPX appliance to use Citrix ADC Pooled Capacity license, you need to upload the MPX-Z to the appliance.

Prerequisites

Make sure that you upload the MPX-Z license to both the primary and secondary instances in the HA pair.

To upload the MPX-Z license to the Citrix ADC MPX instances in the HA pair:

1. In a Web browser, type the IP address of the appliance, such as http://192.168.100.1.
2. In User Name and Password fields, type the administrator credentials.
3. On the Welcome page, click Continue.

5. In the details pane, click Manage Licenses, click Add New License.

6. In Licenses page, select Upload license files and click Browse to select the zero capacity license from your local machine.

Once the license is uploaded you are prompted to reboot the appliance.

7. Click Reboot to reboot the appliance.

8. On the Confirm page, click Yes.
To upgrade an existing HA setup to Citrix ADC Pooled Capacity:

1. Log on to the secondary Citrix ADC MPX Instance. In a Web browser, type the IP address of the Citrix ADC appliance, such as http://192.168.100.1.

2. In **User Name** and **Password** fields, type the administrator credentials.

3. On the **Welcome** page, click on the **Licenses** section.

4. In the **License Server** section, do the following:
In the `Server Name/IP Address` field, enter the license server details.

b) In the `License Port` field, enter the licence server port. Default value: 27000.

c) If you want to manage your instance’s pool licenses through Citrix ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

d) Click **Continue**.

5. In the **Allocate licenses** window, do the following:

a) Select the license edition from the drop-down list.
b) Allocate the bandwidth to the Citrix ADC appliance from the Allocate menu and click Get Licenses.

![Allocate Licenses](image)

- **Type**: Total | Available | Allocate
- **Instance**: 200 | 197 | 1
- **Bandwidth**: 200 Gbps | 178.95 Gbps | 50

   - Get Licenses
   - Cancel

   c) When prompted, click Reboot to reboot the appliance.

   After the secondary Citrix ADC MPX appliance reboots, it becomes the primary Citrix ADC MPX appliance in the HA pair.

6. Log on to the existing primary Citrix ADC MPX appliance and reboot the appliance. Perform the following:
   a) In a Web browser, type the IP address of the Citrix ADC appliance, such as `http://192.168.100.1`.
   b) In **User Name** and **Password** fields, type the administrator credentials.
   c) On the **Welcome** page, click **Continue**.
   d) On the **Configuration** tab, click **System**.
   e) On the **System** page, click **Reboot**.

   ![Configuration Tab](image)

   f) On the **Reboot** page, select **Warm reboot** and click **OK**.
After the primary Citrix ADC MPX appliance reboots, it becomes the secondary Citrix ADC MPX appliance in the HA pair. If required, you can change the primary and secondary instance in the HA pair to your original HA pair configuration by using the following command on any instance in the HA pair:

```
1 > force ha failover
```

**Upgrade a perpetual license in Citrix ADC SDX to Citrix ADC pooled capacity**

**August 1, 2019**

Citrix ADC SDX appliance with perpetual license can be upgraded to Citrix ADC Pooled Capacity license. Upgrading to Citrix ADC Pooled Capacity license enables you to allocate licenses from the license pool to Citrix ADC appliances on demand. You can also configure Citrix ADC Pooled Capacity license for Citrix ADC instances configured in high availability mode.

**Important**

For upgrading SDX appliance to Citrix ADC Pooled Capacity license, you need to upload the SDX-Z license to the appliance.

**To upgrade to Citrix ADC pooled capacity:**

1. In a Web browser, type the IP address of the Citrix ADC appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero-capacity license. On the Configuration tab, navigate to **System > Licenses**.
5. Navigate to **System > Licenses**.
6. In the **Licenses** page, click **Manage Licenses** and then click **Add New License**.

7. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero-capacity license from your local machine. Then, click **Finish**.

Once the zero-capacity license is applied successfully, **Pooled Licenses** section appears on the **Licenses** page.

8. In the **Pooled licenses** section, do the following:
a) In the **Licensing Server Name or IP Address** field, enter the license server details.

b) In the **Port Number** field, enter the license server port. Default value: 27000.

c) If you want to manage your instance’s pool licenses through Citrix ADM, select the **Register with Citrix ADM** check box and enter the ADM credentials.

d) Click **Get Licenses**.

9. In the **Allocate Licenses** window, specify the required instances and bandwidth and click **Allocate**.

On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated instances and bandwidth from the pool.
Citrix ADC pooled capacity on Citrix ADC instances in cluster mode

August 1, 2019

You can configure Citrix ADC pooled capacity on the Citrix ADC instances configured as a cluster. Following are the prerequisites for configuring pooled capacity on Citrix ADC instances in cluster mode:

- Instances should be individually running in a pooled-capacity license mode to form the cluster.
- All the instances should be running with same bandwidth.
- All the instances should check out the pooled capacity from the same Citrix Application Delivery Management (ADM).
- New instances cannot be added to an existing Citrix ADC cluster unless their capacity and Citrix ADM configurations are same as those of the existing instances in the cluster.

Any capacity check-out from the Citrix ADC cluster will assign same capacity to all the cluster nodes and the checkout Bandwidth = Bandwidth provided * number of nodes.
For example, if you check-out 50 Mbps of bandwidth from the Citrix ADC cluster, and the cluster includes 12 instances, each instance automatically receives 50 Mbps; and 600 mbps is checked out from the pool.

Note

If one or more instances in the cluster become unresponsive, the cluster continues to work with the capacity of the remaining instances.

To allocate Citrix ADC Pooled capacity on Citrix ADC instances in cluster mode:

1. In a web browser, type the IP address of the Cluster IP (CLIP) address (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses > Manage Licenses, click Add New License, and select Use Pooled Licensing.
4. Enter the name or address of the license server in the Server Name/IP Address field.
5. If you want to manage your instance’s pool licenses through Citrix ADM, select the Register with Citrix ADM for manageability check box and enter the ADM credentials.
6. Select the license edition and the required bandwidth, and click Get Licenses.

7. You can change or release the license allocation by selecting Change allocation or Release allocation.
8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

**Note**

Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.

9. You can allocate bandwidth or instances to the Citrix ADC instance from the **Allocate** drop-down list. Then click **Get Licenses**.

10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

**Note**

A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.
Health monitoring

August 1, 2019

The license server continuously monitors the health of the Citrix ADC pooled-capacity enabled instance. The instances communicate through periodical messages to the license server. If few consecutive messages are not received, the license server reports that connectivity has been lost.

You can create custom notifications to supplement the default alarms.

Grace Period

When a Citrix ADC pooled-capacity enabled instance is in a healthy state and the license server stops responding, the instance continues to operate with the current capacity for 30 days. If the connectivity to the license server is not restored after 30 days, the instance loses its capacity and stops processing traffic.

Notifications and Alarms

Notifications can be enabled from Citrix Application Delivery Management (ADM) for any action performed on the instance. Apart from the custom notification settings, some alarms are configured by default. For example: To configure an alarm for replenishing a pool that has depleted a certain percentage of its capacity, navigate to Infrastructure > License > Settings > Notification Settings and click the edit button.
Expected behaviors when issues arise

August 1, 2019

Following are the expected behaviors of the license servers and Citrix ADC instances when they experience the issues described:

License Server stops responding

Warning

The license Server is not responding. Citrix ADC will continue to operate with the current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the Citrix ADC will loses its current capacity and stops processing traffic.

If the license server stops responding, the Citrix ADC instance enters the Grace Period until connectivity is restored.

Citrix ADC pooled-capacity enabled instance stops responding

If the Citrix ADC pooled-capacity enabled instance stops responding and the license server is in a healthy state, the license server checks in all the Citrix ADC instance’s licenses after 10 minutes. When the instance reboots, it sends a request to check-out all the licenses from the licensing server.

Both license server and Citrix ADC pooled-capacity enabled instance stop responding

If both the license server and the Citrix ADC pooled-capacity enabled instance restarts and reestablishes the connection, the license server checks-in all its licenses after 10 minutes, and the Citrix ADC pooled capacity enabled instances automatically check-out the licenses after the reboot is completed.

The Citrix ADC pooled-capacity enabled instance shuts down gracefully

During a graceful shutdown, you can choose to check the licenses in or keep the licenses that were allocated before the graceful shutdown. If you choose to check the licenses in, the Citrix ADC pooled-capacity enabled instance is unlicensed after the it restarts. If you choose to keep the licenses, they are checked in to the licensing server when the instance shuts down. After the instance restarts, it reestablishes the connection with the licensing server and checks out the licenses as specified in the saved configuration.
If system reboots and the check-out fails due to no capacity available in the pool, the Citrix ADC will check the inventory of Citrix Application Delivery Management (ADM) pool licenses and will check-out any available capacity. An SNMP alarm is raised to notify this condition to the user if Citrix ADC is not running with full capacity as per configuration. If no capacity is available in the bandwidth pool, the pool capacity enabled instance will become unlicensed.

**Network loses connectivity**

*Error message (syslog)*

License Server is not responding.

If the license server and Citrix ADC pooled-capacity enabled instances are in healthy states but network connectivity is lost, the instances continue to operate with their current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the instances lose their capacity and stop processing traffic, and the license server checks-in all its licenses. After the license server reestablishes connectivity with the Citrix ADC instances, the instances check the licenses out again.

**Configure expiry checks for pooled capacity licenses**

August 1, 2019

You can now configure license expiry threshold for Citrix ADC pooled capacity licenses. By setting thresholds, Citrix Application Delivery Management (ADM) sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification is also sent when the license has expired on Citrix ADM.

An event is generated when a license expiry notification is sent and this event can be viewed on Citrix ADM.

**To configure license expiry checks:**

1. Navigate to **Networks > Licenses**.

2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
   - **Feature**: Type of license that is going to expire.
   - **Count**: Number of virtual servers or instances that will be affected.
   - **Days to expiry**: Number of days before license expiry.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.

4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
   
   a) **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.

   b) **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.

5. Then, specify when you want to send the notification in terms of number of days before license expiry.

6. Click **Save**.

**Note**

When you add new licenses to the pool, the Citrix ADC instances use the new licenses on expiry of their existing licenses.
Citrix ADC VPX check-in and check-out licensing

August 1, 2019

You can allocate VPX licenses to Citrix ADC VPX instances on demand from Citrix Application Delivery Management (ADM). The Licenses are stored and managed by Citrix ADM, which has a licensing framework that provides scalable and automated license provisioning. 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.

Prerequisites

Make sure that the following prerequisites are met:

- You are using a Citrix ADC VPX image running software version 12.0. For example: NSVPX-ESX-12.0-xx.xx_nc.zip
- You have installed Citrix ADM running version 12.0. For example: MAS-ESX-12.0-xx.xx.zip

Note

To manage existing VPX licenses by Citrix ADM, you need to rehost the licenses to Citrix ADM.

Installing Licenses in Citrix ADM

Note

Before installing licenses, restart the Citrix ADM virtual appliance if you have changed the software edition or bandwidth.

To install license files on Citrix ADM:

1. In a web browser, type the IP address of the Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Networks > Licenses.
4. In the License Files section, select one of the following options:
   - Upload license files from a local computer - If a license file is already present on your local computer, you can upload it to the Citrix ADM.
     To add license files, click Browse and select the license file (.lic) that you want add. Then click Finish.
Use license access code - Citrix emails the License Access Code (LAC) for the licenses that you purchase.
To add license files, enter the LAC in the text box and then click Get Licenses.

Note
Make sure you are connected to internet before using LAC code for installing the licenses.

At any time, you can add more licenses to the Citrix ADM from the License Settings.

Verification

You can view the available and allocated licenses in the Citrix ADM GUI.

To display the licenses:

1. In a web browser, type the IP address of Citrix ADM (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. On the Configuration tab, navigate to Networks > Licenses > VPX Licenses.

4. You can view the allocated licenses in the table under the available licenses section.
Allocating VPX Licenses to a Citrix ADC VPX Instance by using the Citrix ADC GUI

1. In a web browser, type the IP address of the Citrix ADC instance (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses > Manage Licenses, click Add New License and select Use Remote Licensing.
4. Enter the details of the license server in the Server Name/IP Address field.
5. If you want to manage your instance’s VPX licenses through the Citrix ADM, select the Register with Citrix ADM check box and enter the Citrix ADM credentials.
6. Select the license edition with the required bandwidth, click Get Licenses.
7. Click **Reboot**, your Citrix ADC VPX instance will reboot.

8. You can change or release the license allocation by navigating to **System > Licenses > Manage Licenses**, and selecting **Change allocation** or **Release allocation**.

9. If you click **Change allocation**, a pop-up window shows the licenses available on the license server. Select the required license, click **Get Licenses**.

Allocating VPX Licenses to a Citrix ADC VPX Instance by using the Citrix ADC CLI

1. In a SSH client, enter the IP address of the Citrix ADC instance, and log on by using administrator credentials.

2. To add a licensing server, enter the following command:

   ```
   add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number>]
   ```

   ```
   > add ns licenseserver 10.102.29.97 -port 27000
   ```

   ```
   Done
   ```

3. To show the available licenses on the licensing server, enter the following command:

   ```
   sh licenseserverpool
   ```
4. To assign a license to the Citrix ADC VPX appliance, enter the following command:

```bash
set capacity -platform V\[S/E/P\]\[Bandwidth\]
```

```
set capacity -platform VE8000
```

*Warning: The configuration changes will not take effect until the system is rebooted*

### Allocating VPX Licenses to a Citrix ADC VPX Instance by using API

In a web browser or an API client, log on to the Citrix ADC VPX instance by using the administrator credentials.

**To add a licensing server:**

1. Set the request type to **Post**.
2. Set the path to `/nitro/v1/config/nslicensingserver`.
3. Set the payload as follows:

```json
content-type: application/x-www-form-urlencoded

object= {
  "params" :{
    "warning" : "yes" 
  },
  "nslicensing server" :{
    "servername" : "<Citrix ADM IP>", "port" : "27000" 
  }
}
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix ADM responds to the request. The following sample response shows success.

```json
RESPONSE: **************
HTTP/1.1 201 Created
Date: Fri, 06 Jan 2017 19:03:21 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 57
Content-Type: application/json; charset=utf-8

{
  "errorcode": 0,
  "message": "Done",
  "severity": "NONE"
}
```

To view the available licenses on the licensing server:

1. Set the request type to **Get**.

2. Set the path to `/nitro/v1/config/nslicenseserverpool`

Citrix ADM responds to the request. The following sample response shows success, and the list of available licenses on the license server.
To assign a license to the Citrix ADC VPX appliance:

1. Set the request type to **Post**.

2. Set the path to `/nitro/v1/config/nscapacity`.

3. Set the payload as follows:

   ```
   content-type: application/x-www-form-urlencoded
   
   "nscapacity": {
     "platform": "VE8000"
   }
   ```

   Citrix ADM responds to the request. The following sample response shows success.

```json
{
  "nscapacity": {
    "platform": "VE8000"
  }
}
```
Configure Expiry Checks for Citrix ADC VPX Check-In/ Check-Out Licenses

You can now configure license expiry threshold for Citrix ADC VPX licenses. By setting thresholds, Citrix ADM sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification is also sent when the license has expired on Citrix ADM.

An event is generated when a license expiry notification is sent and this event can be viewed on Citrix ADM.

To configure license expiry checks:

1. Navigate to Networks > Licenses.

2. In the License Settings page, under the License Expiry Information section, you can find the details of the licenses that are going to expire:

   - Feature: Type of license that is going to expire.
   - Count: Number of virtual servers or instances that will be affected.
   - Days to expiry: Number of days before license expiry.

3. In the Notification Settings section, click the Edit icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.

4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
a) **Email Profile:** Specify a mail server and profile details. An email is triggered when your licenses are about to expire.

b) **SMS Profile:** Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.

5. Then, specify when you want to send the notification in terms of number of days before license expiry.

6. Click **Save.**

---

### Citrix ADC virtual CPU licensing

August 1, 2019

Data center administrators like you are moving to newer technologies that simplify network functions while offering lower costs and greater scalability. Newer data center architecture must include the following features in the least:

- Software-defined networking (SDN)
- Network functions virtualization (NFV)
- Network virtualization (NV)
- Micro-services

Such a movement also necessitates that the software requirements to be dynamic, flexible, and agile to meet the ever-changing business needs. Licenses are also expected to be managed by a central management tool with full visibility into the usage.
Virtual CPU licensing for Citrix ADC VPX

Earlier, Citrix ADC VPX licenses were allocated based on the bandwidth consumption by the instances. A Citrix ADC VPX is restricted to use a specific bandwidth and other performance metrics based on the license edition that it is bound to. To increase the available bandwidth, you must upgrade to a license edition that provides more bandwidth. In certain scenarios, the bandwidth requirement might be less, but the requirement is more for other L7 performance such as SSL TPS, compression throughput, and so on. Upgrading the Citrix ADC VPX license might not be suitable in such cases. But you might still have to buy a license with large bandwidth to unlock the system resources required for CPU-intense processing. Citrix ADM now supports allocating licenses to Citrix ADC instance based on the virtual CPU requirements.

In the virtual CPU-usage-based licensing feature, the license specifies the number of CPUs that a particular Citrix ADC VPX is entitled to. So, the Citrix ADC VPX can check-out licenses for only the number of virtual CPUs running on it from the license server. Citrix ADC VPX checks out licenses depending on the number of CPUs running in the system. Citrix ADC VPX does not consider the idle CPUs while checking out the licenses.

Similar to pooled license capacity and CICO licensing functionalities, the Citrix ADM license server manages a separate set of virtual CPU licenses. Here also, the three editions managed for virtual CPU licenses are standard, enterprise, and platinum. These editions unlock the same set of features as those unlocked by the editions for bandwidth licenses.

There might be a change in the number of virtual CPUs or when there is a change in the license edition. In such a case, you must always shut down the instance before you initiate a request for a new set of licenses. You must restart the Citrix ADC VPX after checking out the licenses.

To configure licensing server in Citrix ADC VPX using GUI:

1. In Citrix ADC VPX, navigate to System > Licenses and click Manage Licenses.
2. On the License page, click Add New License.
3. On the Licenses page, select the Use remote licensing option.
4. Select CPU licensing from the Remote Licensing Mode list.
5. Type the IP address of the license server and the port number.
6. Click Continue.
7. In the **Allocate licenses** window, select the type of license. The window displays the total and the available virtual CPUs and also the CPUs that can be allocated. Click **Get Licenses**.

8. Click **Reboot** on the next page to apply for the licenses.
Note
You can also release the current license and check out from a different edition. For example, you are already running Standard edition license on your instance. You can release that license and then check out from Enterprise edition.

Configuring licensing server in Citrix ADC VPX license using CLI

In the Citrix ADC VPX console, type the following commands for the following two tasks:

1. To add the licensing server to the Citrix ADC VPX:

   ```
   add licenseserver <IP address of the license server>
   ```

2. To apply for the licenses:

   ```
   set capacity -vcpu - edition platinum
   ```

   When prompted, reboot the instance by typing the following command:

   ```
   reboot -w
   ```

Managing virtual CPU licenses on Citrix ADM

1. In Citrix ADM, navigate to Networks > Licenses > Virtual CPU Licenses.

2. The page displays the licenses allocated for each type of license edition.

3. Click on the number within each donut to view the Citrix ADC instances that are using this license.

Virtual CPU licensing for Citrix ADC CPX

While provisioning the Citrix ADC CPX instance, you can configure the Citrix ADC CPX instance to check out licenses from the license server depending on the CPU usage on the instance.
Citrix ADC CPX relies on the license server, running on Citrix ADM, to manage the licenses. Citrix ADC CPX checks out the licenses from the license server when it is starting up. The licenses are checked back in to the license server when the Citrix ADC CPX shuts down.

You can download Citrix ADC CPX from the Docker App Store. On the Docker host, to download Citrix ADC CPX, run the following command:

```bash
docker pull store/citrix/netscalercpx:<version>
```

There are three license types available for CPX licensing:

1. Virtual CPU subscription licenses supported for CPX and VPX
2. Pooled Capacity licenses
3. CP1000 licenses that support single to multiple vCPUs for CPX only

**To configure vCPU subscription licenses while provisioning the Citrix ADC CPX instance:**

You need to specify the number of vCPU licenses that the Citrix ADC CPX instance uses.

- This value is entered as an environment variable through Docker, Kubernetes, or Mesos/Marathon.
- The target variable is “CPX_CORES.” The CPX can support from 1 to 7 cores.

To specify 2 cores, you can perform the docker run command as follows:

```bash
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2
```

While provisioning a Citrix ADC CPX instance, define the Citrix ADC Licensing Server as an environmental variable in the `docker run` command as shown below:

```bash
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> cpx:11.1
```

Where,

- `<LS_IP_ADDRESS>` is the IP address of the Citrix ADC Licensing Server.
- `<LS_PORT>` is the port of the Citrix ADC Licensing Server. By default, the port is 27000.

**Note**

By default, the Citrix ADC CPX instance checks out the license from the vCPU subscription pool. The CPX instance checks out “n” number of licenses if the instance is running with “n” CPUs.

**To configure Citrix ADC Pooled Capacity or CP1000 licenses while provisioning the Citrix ADC CPX instance:**
If you want to check out licenses for the CPX instance using the pooled licensing (bandwidth-based) or the CPX private pool (CP1000 or private-pool-based), you must provide the environment variables accordingly.

For example,

```bash
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
  -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e PLATFORM=CP1000 cpx:11.1
```

**CP1000.** This command triggers the checkout from CP1000 pool (CPX private pool). The Citrix ADC CPX instance then retrieves “n” number of instances for “n” number of cores specified for CPX_CORES. The most common use case is to specify n = 1 for a checkout of a single instance. Multicore CPX use cases checks out “n” vCPUs (where “n” is from 1 to 7).

```bash
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
  -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e BANDWIDTH=2000 cpx:11.1
```

**Pooled capacity.** This command checks out one license from the instance pool and consumes 1000 Mbps of bandwidth from the platinum bandwidth pool yet enables CPX to run up to 2000 Mbps. In Pooled Licensing, the first 1000 Mbps is not charged.

### Note

Specify the corresponding number of vCPUs for the desired target bandwidth when checking out from the bandwidth pool as detailed in the following table:

<table>
<thead>
<tr>
<th>Number of cores (vCPU)</th>
<th>Maximum bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td>2</td>
<td>2000 Mbps</td>
</tr>
<tr>
<td>3</td>
<td>3500 Mbps</td>
</tr>
<tr>
<td>4</td>
<td>5000 Mbps</td>
</tr>
<tr>
<td>5</td>
<td>6500 Mbps</td>
</tr>
<tr>
<td>6</td>
<td>8000 Mbps</td>
</tr>
<tr>
<td>7</td>
<td>9300 Mbps</td>
</tr>
</tbody>
</table>
Manage Citrix SD-WAN instances

August 1, 2019

Citrix ADM allows you to monitor, manage, and view analytics of the Citrix SD-WAN appliances in your Network. The following interoperability table provides information on which features of Citrix ADM are currently supported in each of the Citrix SD-WAN platform editions.

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

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>Discovery</th>
<th>Configuration Monitoring</th>
<th>Reporting (Network Reports)</th>
<th>Event Management</th>
<th>HDX Insight</th>
<th>WAN 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>
<td>Yes</td>
</tr>
<tr>
<td>Citrix SD-WAN SE</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Citrix SD-WAN EE</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Citrix SD-WAN versions supported by Citrix ADM**

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>Citrix SD-WAN Version</th>
<th>Citrix ADM Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix SD-WAN WANOP</td>
<td>Citrix CloudBridge 7.4 and later</td>
<td>Citrix ADM 11.0 and later</td>
</tr>
<tr>
<td>Citrix SD-WAN SE</td>
<td>Citrix SD-WAN 9.3.0 and later</td>
<td>Citrix ADM 12.0.53.8 and later</td>
</tr>
<tr>
<td>Citrix SD-WAN EE</td>
<td>Citrix SD-WAN 9.3.0 and later</td>
<td>Citrix ADM 12.0.53.8 and later</td>
</tr>
</tbody>
</table>

You can add a Citrix SD-WAN WANOP appliance as a managed instance on Citrix ADM. For more information see, Add Instances to Citrix ADM. You can view the WAN insight, HDX insight, Network reports, and Event reports for Citrix SD-WAN WANOP instances.
Citrix ADM allows Citrix SD-WAN Standard Edition (SE) and Enterprise Edition (EE) appliances to register themselves as managed instances on Citrix ADM.

To add a Citrix SD-WAN SE/EE appliance to Citrix ADM, configure Citrix ADM as an AppFlow collector on the Citrix SD-WAN SE/EE appliances. The Citrix SD-WAN SE/EE appliance adds itself as a managed instance on Citrix ADM. The SD-WAN SE/EE appliance then sends the analytics data to Citrix ADM.

You can set Citrix ADM as an AppFlow collector on each SD-WAN SE/EE device individually, or use the Citrix SD-WAN Center to export the configuration to the managed appliances.

For more information, see Adding Citrix SD-WAN SE/EE Instances in Citrix ADM.

For a Citrix SD-WAN EE appliance, you can view HDX data records or multi-hop data, depending on the AppFlow configuration. A Citrix SD-WAN SE appliance provides multi-hop data only. For more information see, Viewing HDX Insight Reports and Metrics and Viewing Analytics Data for Multi-hop Deployment.

This page provides quick access links to the topics that you can refer to set up Citrix ADM and to manage your SD-WAN WANOP appliances using Citrix ADM.

**Citrix ADM Overview**

- About Citrix ADM
- Architecture
- How Citrix ADM Discovers Instances
- How Citrix ADM Communicates with Managed Instances

**Citrix ADM Deployment**

- Deploy Citrix ADM with Citrix Hypervisor
- Deploy Citrix ADM with Microsoft Hyper-V
- Deploy Citrix ADM with VMWare ESXi
- Deploy Citrix ADM with Linux KVM Server
- Deploy Citrix ADM in High Availability Mode
- Migrate from NetScaler Insight Center to Citrix ADM
- Integrate Citrix ADM with Director
Instance Management

How to Add Instances to Citrix ADM
How to Create Instance Groups on Citrix ADM
How to Back Up and Restore an Instance using Citrix ADM

Configuration Management

How to Create Configuration Jobs from Corrective Commands on 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
How to Reuse Executed Configuration Jobs

Analytics

WAN Insight
HDX Insight
How to View Network Reports for Citrix SD-WAN WANOP Instances
How to Configure Adaptive Thresholds
How to Configure Database Summarization for Analytics
How to Create Thresholds and Alerts Using Citrix ADM

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 View Event Reports for Citrix SD-WAN WANOP instances
How to Modify the Reported Severity of Events that Occur on NetScaler Instances
How to View the Events Summary in Citrix ADM
How to Display Event Severities and Skews of SNMP Traps on the Infrastructure Dashboard of Citrix ADM

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Authentication

How to Cascade External Authentication Servers
How to Add RADIUS Authentication Servers
How to Add LDAP Authentication Servers
How to Add TACACS Authentication Servers
How to Extract Authentication Server Group in Citrix ADM
How to Enable Fallback Local Authentication

Citrix ADM System

Managing Citrix ADM System
How to Upgrade Citrix ADM
How to Generate a Tech Support File for Citrix ADM
How to Back up and Restore your Citrix ADM Server in a Single-Server Deployment
How to Back Up and Restore a Citrix ADM Configuration in an HA Pair
How to Enable Shell Access for Non-Default Users in Citrix ADM
How to Configure NTP Server on Citrix ADM
How to Configure SSL Settings for Citrix ADM
How to Configure Syslog Purging Interval for Citrix ADM
How to View Auditing Information of Citrix ADM
How to Configure System Notification Settings of Citrix ADM
How to Monitor CPU, Memory, and Disk Usage of Citrix ADM
How to Configure a Cipher Group for Citrix ADM
How to Create SNMP Traps, Managers, and Users on Citrix ADM
How to Assign a Host Name to a Citrix ADM Server
How to Configure System Prune Settings for Citrix ADM
How to Configure System Backup Settings by Using Citrix ADM
How to Configure and View System Alarms on Citrix ADM
Add Citrix SD-WAN SE/PE instances

August 1, 2019

Configure Citrix ADM as the AppFlow collector on the Citrix SD-WAN SE/PE appliance to add these instances in Citrix ADM. The Citrix SD-WAN SE/PE appliances are registered as managed instances on Citrix ADM, and their AppFlow records are collected. For a Citrix SD-WAN PE appliance, you can enable either the **TCP only for HDX** template or the **HDX** template. The **TCP only for HDX** template provides multi-hop data. The **HDX** template provides HDX data, it should be enabled on the Data Center appliance only.

You can configure Citrix ADM as an AppFlow collector on the individual SD-WAN SE/PE appliance, or you can configure Citrix ADM as the AppFlow collector using SD-WAN Center and export the configuration to the appliances managed by it.

To configure Citrix ADM as an AppFlow collector on an Citrix SD-WAN SE/PE appliance:

1. In the SD-WAN SE/PE web interface, navigate to Configuration > AppFlow/IPFIX
2. Choose **Enable**.
3. In the **Data Update Interval** field, specify the time interval, in minutes, at which the AppFlow reports are exported to AppFlow collector.

   **Note**
   
   If Citrix ADM is the AppFlow collector, the data update interval should be 1 minute.

4. Do one of the following:

   - Choose **HDX**, to send HDX insight data to the AppFlow collector. This should be enabled on the branch appliances.
   - Choose **TCP only for HDX**, to send multi-hop data to the AppFlow collector.

   **Note**
   
   HDX template option is available for Citrix SD-WAN PE appliance only, it should be enabled on the Data Center appliance.

5. In the **IPAddress** field, type the IP Address of the external AppFlow collector system (Citrix ADM Server).

6. In the **Port** field, type the port number on which the external AppFlow collector system listens. The default value is 4739.

7. Choose the **Citrix ADM** check box, to specify that Citrix ADM is the AppFlow collector.

   **Note**
   
   - Citrix ADM currently does not support IPFIX collection.
   - You can add up to four AppFlow collectors. Either Citrix ADM or any AppFlow collector that supports the IPFIX protocol.

8. Enter the credentials for the Citrix ADM server.

9. Click **Apply Settings**.

The Citrix SD-WAN SE/PE appliances are discovered and listed on Citrix ADM. The Citrix SD-WAN SE/PE appliances send the analytics data to Citrix ADM. For more information, see [AppFlow and IPFIX](#).

**To configure Citrix ADM as an AppFlow collector by using Citrix SD-WAN Center:**

1. In Citrix SD-WAN Center management UI, navigate to **Configuration > Appliance Settings**.

2. Navigate to the **AppFlow / IPFIX** section and choose **Include in File**.

3. Select **Enable IPFIX / AppFlow Collection**.
4. In the **Data Update Interval** field, specify the time interval, in minutes, at which the AppFlow reports are exported to the AppFlow collector.

   **Note**
   
   If Citrix ADM is the AppFlow collector, the data update interval should be 1 minute.

5. Do one of the following:

   - Choose **HDX**, to send HDX insight data to the AppFlow collector.
   - Choose **TCP for HDX**, to send multi-hop insight data to the AppFlow collector. This should be enabled on the branch appliances.

   **Note**
   
   **HDX** template option is available for Citrix SD-WAN PE appliance only, it should be enabled on the Data Center appliance.

6. In the **IPFIX / AppFlow Collector** field, type the IP Address of the external AppFlow collector system (Citrix ADM Server).

7. In the **Port** field, type the port number on which the external AppFlow collector system listens. The default value is 4739.

8. Choose the **Citrix ADM** check box to specify that Citrix ADM is the AppFlow collector.

9. Enter the credentials for the Citrix ADM server.

   **Note**
   
   You can add up to four AppFlow collectors. Either Citrix ADM or any AppFlow collector that supports the IPFIX protocol.

10. Save and Export the configuration to the managed appliances.

   For more information, see [How to Configure and Export Appliance Settings to Managed Appliances](#).
For more information about configuring Citrix ADM as an AppFlow collector by using Citrix SD-WAN Center, AppFlow and IPFIX.

The Citrix SD-WAN SE/PE appliances are discovered and listed by Citrix ADM. The Citrix SD-WAN SE/PE appliances are discovered and listed in Citrix ADM. To view the discovered Citrix SD-WAN SE/PE appliances, in the Citrix ADM web interface, navigate to Networks > Instances > Citrix SD-WAN and select SD-WAN SE/PE.

You can view the IP address, name, current state, software edition, and version of the discovered appliances. You can also see if the appliance is a master controller node (MCN) or not.

You can perform the following actions:

- View and remove instance profiles.
- Remove instances from Citrix ADM.
- Rediscover instances.

For a Citrix SD-WAN PE appliance, you can view HDX data records or multi-hop data, depending on the AppFlow configuration. A Citrix SD-WAN SE appliance provides multi-hop data only. For more information see, Viewing HDX Insight Reports and Metrics and Viewing Citrix SD-WAN Analytics Data for Multi-hop Deployment.

**View Citrix SD-WAN analytics data for multi-hop deployment**

August 1, 2019

A multi-hop network deployment has multiple devices between the client and the server, as shown in the following figure. In this type of deployment, the Citrix SD-WAN SE appliances and the Citrix Gateway are added to Citrix ADM, and AppFlow is enabled.
Citrix ADM identifies the appliance from which it receives the data, based on the hop count and connection chain ID. The hop count represents the number of appliances through which the traffic flows from the client to the server. The connection chain ID represents the end-to-end connections between the client and the server.

Citrix ADM uses the hop count and connection chain ID to correlate the data from the appliances, and generates the reports.

For Citrix SD-WAN SE appliances to send the analytics data to Citrix ADM, you should configure the Virtual IP address of Citrix Gateway as the DPI ICA IP and set the DPI ICA port number to 443.

**To configure ICA DPI settings:**

1. In the Citrix SD-WAN SE appliance UI, navigate to *Configuration Editor > Advanced > Global > Applications > Settings*

2. Select *Enable Deep Packet Inspection > Enable Deep Packet Inspection for Citrix ICA Applications > Enable Multi-Stream ICA*
3. In the **DPI ICA IP-1** field, enter the Citrix Gateway Virtual IP address and prefix.

4. In the **DPI ICA Port-1** field, enter the port number 443.

5. Click **Apply** and export the configuration to the appliance using the change management process.

In Citrix ADM, for every active ICA session, you can view a session diagram in HDX Insight. The session diagrams provide details about the devices in the connection path. They also provide insight into the client-side / server-side latency between a network device and its immediate next hop. This information enables you to identify the root cause of delay and troubleshoot performance issues.

Citrix SD-WAN SE does not send HDX data records. It provides TCP for HDX information only. The HDX insight data is provided by the HDX insight enabled devices in your network (for example, Citrix ADC or Citrix Gateway).

The Citrix SD-WAN EE appliance can send TCP for HDX data or HDX insight data, depending on the AppFlow configuration of the appliance. HDX template should be enabled on the Data Center appliance.
**Note**

In a multi-hop deployment, ensure that only one of the network devices sends HDX insight data. The rest of the network devices can send TCP for HDX data.

**To view multi-hop data:**

In Citrix ADM web interface, navigate to **HDX Insight > Users > Current Sessions** or **HDX Insight > Applications > Current Sessions** and click the **Diagram** icon.

The network topology diagram appears.

Click any network element to display more information.

**Note**

The information displayed depends on the selected network element.

The following parameters appear for Citrix appliances:
Citrix Application Delivery Management 12.1

- **Name**: Name of the Citrix appliance.
- **IPAddress**: IP address of the appliance.
- **WAN Latency**: Latency caused by the client side of the network. That is, from Citrix appliance to end-user.
- **DC Latency**: Latency caused by the server side of the network. That is, from Citrix appliance to back-end servers.
- **State**: Device reachability status.

**View event reports for Citrix SD-WAN WANOP Instances**

August 1, 2019

You can view the events of the Top 10 SD-WAN WANOP instances as a graphical representation by navigating to **Networks > Events > Reports** and select **Citrix SD-WAN WO**.

The events are displayed based on their severity for each instance, you can click each severity to know more information on the number of events, when it occurred and what category it belongs to.

**View network reports for Citrix SD-WAN WANOP Instances**

August 1, 2019

You can view WAN optimization network related reports in Citrix ADM, using this data you can troubleshoot network issues or analyze the behavior of your Citrix SD-WAN WAN WANOP devices. You can view the reports of network statistics of your WAN optimization devices for the past one hour, one day, one week or one month.
You can view the following reports:

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceleration</td>
<td>Use this report to analyze the pattern of accelerated traffic (KBPS by service class) and the number of accelerated TCP connections passing through the WAN optimization appliance. This includes the number of TCP connections passing through the WAN optimization device that undergo acceleration, the number of open and half-closed connections that have been selected for acceleration, and the number of half-open connections that are candidates for acceleration.</td>
</tr>
<tr>
<td>Pass through Connection</td>
<td>Use this report to view the non-accelerated connections for the WAN optimization device.</td>
</tr>
<tr>
<td>Service Class</td>
<td>Use this report to view the sent and receive bandwidth savings based on the service class type defined for the WAN optimization device.</td>
</tr>
<tr>
<td>Application</td>
<td>Use this report to view the sent and received data volume in bits-per-second for the applications running on the WAN optimization device.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Use this report to view the CPU utilization of the WAN optimization device as a percentage.</td>
</tr>
<tr>
<td>Capacity Increase</td>
<td>Use this report to view the cumulative send compression ratio for the WAN optimization device.</td>
</tr>
<tr>
<td>Data reduction</td>
<td>Use this report to view the transmit and receive bandwidth savings as a percentage. You can also analyze the transmit bandwidth and receive bandwidth saving values separately for the WAN optimization device.</td>
</tr>
<tr>
<td>Link Utilization</td>
<td>Use this report to view the transmit link utilization and receive link utilization for the WAN optimization as a percentage.</td>
</tr>
</tbody>
</table>
Reports Description

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Usage</td>
<td>Use this report to view the number of plugins connected to the WAN optimization device.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Use this report to view the link dropped sent packets and link dropped received packets for the links defined in the WAN optimization device.</td>
</tr>
<tr>
<td>Throughput</td>
<td>Use this report to view the link sent volume and link received volume in bits-per-second for the WAN optimization device.</td>
</tr>
<tr>
<td>QoS</td>
<td>Use this report to view the QOS Sent and QOS Receive volume in bits-per-sec for the WAN optimization device.</td>
</tr>
</tbody>
</table>

**To view Citrix SD-WAN WANOP network reports:**

1. In Citrix ADM, navigate to Networks > Network Reporting > Citrix SD-WAN WO.
2. From the Report Name drop-down list select a report that you want to view.
3. From the Instances drop-down list, select the Citrix SD-WAN WANOP instance for which you want to view the report.
4. From the Duration drop-down list, select the time interval.
5. Click Run.

**Back up Citrix SD-WAN WANOP instances**

August 1, 2019

You can back up the current state of an instance and later use the backed-up files to restore the instance to the same state. It is a good practice to back up an instance before you upgrade the instance or for precautionary reasons. A backup of a stable system enables you to restore the system to a stable point in case it becomes unstable. There are multiple ways to perform backups and restores on a Citrix SD-WAN WANOP instance. You can manually backup and restore instances using the GUI, CLI, or use Citrix ADM to perform backups. Citrix ADM backs up the current state of your managed Citrix SD-WAN WANOP instances using NITRO calls, Secure Shell (SSH) protocol, and Secure Copy (SCP) protocol.
Configuring Instance Backup Settings

Before you take a backup of the Citrix SD-WAN WANOP instance in Citrix ADM, you have to configure the instance backup settings on Citrix ADM.

To configure instance backup settings:

1. In Citrix ADM, navigate to System > System Administration. In the right-hand pane, under Backup Settings, select Instance Backup Settings.

2. Select Enable Instance Backups. This option is enabled by default.

3. Select Password Protect File to encrypt the backup file. Encrypting the backup file ensures that the sensitive information in the backup file is secure.

4. In the Number of Backup Files to retain field, specify the number of backup files to retain in Citrix ADM. You can retain up to 50 backup files.

   **Note**

   Each backup file requires some storage requirement. Citrix recommends that you store an optimal number of backup files on Citrix ADM as per your requirement.

5. Set the Backup Scheduling settings. Choose one of the following options:
   - **Interval Based** - A backup file is created in Citrix ADM after the specified interval elapses. The default backup interval is 12 hours.
   - **Time Based** - You can specify the time in “hours:minutes” format at which the backup should happen. Citrix ADM allows up to four daily backups to happen on the instances.
6. Select **Enable External Transfer** to transfer the instance backup files to an external location. Enter the values for the following fields:

- **Server**: IP address of the external server.
- **User Name**: User name of the external server
- **Password**: Password of the external server.
- **Port**: Port number used to communicate with the external server.
- **Transfer Protocol**: Protocol to be used for transferring the backup files from Citrix ADM to the external server.

You can also delete the backup file from Citrix ADM after transferring it to the external server.
7. Click OK.

Note
Citrix ADM sends an SNMP trap or a Syslog notification to itself when there is a backup failure for any of the selected Citrix SD-WAN WANOP instances.

**Creating a Backup of Citrix SD-WAN WANOP Instance**

The procedure to create a backup for Citrix SD-WAN WANOP instance is applicable for an admin user, using the default nsroot profile.

For information on how a custom user can take back up of a Citrix SD-WAN WANOP instance see, Creating a Backup of Citrix SD-WAN WANOP Instance for Custom Users section in this topic.

Ensure that a Citrix SD-WAN WANOP instance is added to Citrix ADM for more information see, Adding Instance to Citrix ADM.
To create a backup for Citrix SD-WAN WANOP Instance:

1. In Citrix ADM, navigate to Networks > Instances > Citrix SD-WAN.

2. In SD-WAN WO, select the Citrix SD-WAN WANOP instance that you want to back up, and then click Backup/Restore.


4. Encrypt your backup file by using any one of the following options:
   - Select Password Protected file, and enter a password to encrypt the backup files.
   - Select Use Global Password to use the global password that you specified on the instance backup settings page.

5. Click Create Backup

Creating a Backup of Citrix SD-WAN WANOP Instance for Custom Users

If you have created a custom user with admin privileges in Citrix SD-WAN WANOP instance, use the following procedure to add an instance and take back up of that instance using Citrix ADM.

Backup operation by custom users is not supported on 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100 SD-WAN WANOP platforms.

*Note*

Citrix recommends you to use the default nsroot profile, while creating backup of Citrix SD-WAN advanced platforms in Citrix ADM.

To add a Citrix SD-WAN WANOP Instance and take a backup for a custom user:

1. In Citrix ADM, navigate to Networks > Instances > Citrix SD-WAN and select SD WAN WO.

2. Click Add.

3. In the IP Address field, enter the IP address of the Citrix SD-WAN WANOP instance.
4. Click Add next to Profile Name field to create a new profile. The Create Citrix SD-WAN WO Profile window appears.

![Create NetScaler SD-WAN WO Profile](image)

5. In the Profile Name field, enter a name for the profile.
6. In the User Name field, enter the username of the custom user that you create on the SD-WAN WANOP instance.
7. In the Password field, enter the password that you set for the custom user in the SD-WAN WANOP instance.
8. In the Community field, enter the SNMP communication string configured on the SD-WAN WANOP appliance. (for example: public)
9. Click Create.
10. In the Profile Name field, select the newly created profile and click OK.
11. Navigate to **Networks > Instances > Citrix SD-WAN**.

12. In **SD-WAN WO**, select the Citrix SD-WAN WANOP instance that you just added, and then click **Backup/Restore**.

13. On the **Backup Files** page, click **Back Up**.

14. Encrypt your backup file by using any one of the following options:
   - Select **Password Protected file**, and enter a password to encrypt the backup files.
   - Select **Use Global Password** to use the global password that you specified on the instance backup settings page.

   **Note**
   
   You can download the encrypted backup file to your local machine, but you cannot view its contents. Only Citrix ADM can use these backup file for restore purpose. Restoring encrypted backup will prompt for password.

15. Click **Create Backup**.

   **Important**
   a) For a Citrix SD-WAN WANOP VPX appliance, Citrix ADM backs up only the CB broker
b) For an advanced Citrix SD-WAN WANOP platform, Citrix ADM backs up the following:

- CB broker configuration file
- NTP configuration file
- DNS
- SNMPD configuration file
- Syslog configuration file
- SSL certificate, keys and policies
- SVM Database file
- Components (in XML format)
- Resources (in XML format)

The files that are backed up in the respective folders are listed in the following table. Note that if a folder name is followed by a “*”, all files in that folder are backed up.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Sub-Directory or Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>/br_broker/</td>
<td>CB-6bbb660a/ ws.conf</td>
</tr>
<tr>
<td>/etc/</td>
<td>resolv.conf</td>
</tr>
<tr>
<td>/mps/</td>
<td>mps_devices.xml</td>
</tr>
<tr>
<td>/mpsconfig/</td>
<td>ssl/*, ntp.conf, snmpd.conf, syslog.conf</td>
</tr>
<tr>
<td>/mpsdb/</td>
<td>mpsdb_dump.sql</td>
</tr>
<tr>
<td>/ns/</td>
<td>NS-6cb660a/*</td>
</tr>
<tr>
<td>/var/</td>
<td>mps/policy/<em>, mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/</em></td>
</tr>
</tbody>
</table>

Manage HAProxy instances

August 1, 2019

HAProxy is an open-source load balancer that can load balance any TCP or HTTP service. For more information about HAProxy, see [http://www.haproxy.org/](http://www.haproxy.org/).

The Citrix Application Delivery Management (Citrix ADM) supports HAProxy version 1.4.24 or later. When you add a host on which you have provisioned the HAProxy instances to Citrix ADM, Citrix ADM discovers the HAProxy instances on the host and enables you to monitor them. It shows you the following types of information about the HAProxy configuration on the instances:
• Frontend – How requests should be forwarded to the back end.
• Backend – The set of servers that receive the forwarded requests.
• Servers – The servers among which HAProxy load balances the traffic.

For more information, see http://www.haproxy.org/download/1.7/doc/configuration.txt.

Also, Citrix ADM provides an HAProxy App Dashboard on which you can monitor the frontends in real-time. For more information, see HAProxy App Dashboard.

Add HAProxy instances to Citrix ADM

August 1, 2019

In Citrix Application Delivery Management (Citrix ADM), you need to manually add the details of the host on which you have provisioned the HAProxy instance. After you add those details, Citrix ADM automatically discovers the HAProxy instances provisioned on the host and adds them to Citrix ADM Inventory. It also discovers all the frontends, backends, and servers configured on the HAProxy instances, and treats the frontends as discovered applications.

Prerequisites

Make sure that you have:

• Deployed an HAProxy instance on a host in your deployment. For more information, see http://www.haproxy.org/#docs.
• Identified and decided on the number of frontends for which you want to view the application statistics on the HAProxy App Dashboard. By default, the HAProxy App Dashboard displays the statistics for 30 discovered applications. For more information about HAProxy App Dashboard, see HAProxy App Dashboard. If you want to view the statistics of more than 30 discovered applications, you need to purchase a separate license. For more information, see Third-Party Licensing.

Important

Citrix ADM requires access to the host in order to discover the HAProxy instances in it. You can provide access to Citrix ADM by either providing the SSH key pair of the host or by using the host password. If you want to provide access using the SSH key pair, make sure that you generate the SSH private and public key pair in the host and add the public key to the authorized keys on the host. Also, the SSH user account must have superuser permissions.

To add an HAProxy instance to Citrix ADM:
1. In a web browser, type the IP address of the Citrix Application Delivery Management (for example, http://192.168.100.1).

2. In the User Name and Password fields, enter the administrator credentials. The default administrator credentials are “nsroot” and “nsroot”.

3. Navigate to Networks > Instances. Under Instances, select HAProxy and click Add.

4. In the Add HAProxy Host dialog box, do the following:

   - In the IP Address field, enter the IP address of the host on which you have provisioned the HAProxy instances.
   - a) In the HAProxy Profile menu, select an existing HAProxy profile or create and select a new HAProxy profile. To create an HAProxy profile, click Add.
      - i. In the Add HAProxy Profile dialog box, do the following:
In the **Profile Name** field, enter the profile name.

ii. In the **UserName** and **Password** fields, enter the user credentials of the host.

iii. Click **Create**.

2. From the **Site** menu, select a HAProxy site. To create and add a new site to the menu, click **Add**.

3. From the **Agent** menu, select an Agent.

4. In the Tags fields, enter values appropriately.

5. Click **OK**.

Citrix ADM discovers the HAProxy instances provisioned on the host, and you can view all the HAProxy instances on the **Instances** tab.

### Viewing the configuration of an HAProxy instance

To view the configuration of an HAProxy instance in Citrix ADM, navigate to **Networks > Instances > HAProxy** and, on the, **Instances** tab, select the HAProxy instance and click **View Configuration**.
The Application Dashboard provides real-time statistics of all the HAProxy frontends monitored by Citrix Application Delivery Management (Citrix ADM). It lists the frontends as discrete applications and provides transactions, throughput, and sessions information about the applications.

Important

Make sure that you enable `stats` in the HAProxy instance configuration file. To enable `stats`, edit your HAProxy configuration file and, after the defaults section, add an entry similar to the one in the following sample:

```
1  listen stats :9000  # Listen on localhost:9000
2  mode http
3  stats enable    # Enable stats page
4  stats hide-version  # Hide HAProxy version
5  stats realm Haproxy\ Statistics  # Title text for popup window
```
To access the HAProxy application on the Application Dashboard in Citrix ADM, after you have added the HAProxy instances to Citrix ADM, navigate Applications > Dashboard. You can filter the dashboard to display only the HAProxy application, to filter the dashboard, select HAPROXY displayed under Application Family section in the App Summary Info Panel.

View key Metrics of HAProxy Application

The App Info panel is at the first level when you drill down on an HAProxy application. It displays the key metrics and components of the application, along with its state. For example, for any selected HAProxy application, the App Info panel shows the total number of HAProxy frontends, total number of HAProxy backends, data volume, trend of the client connections, and the transactions. To view the key metrics of the HAProxy application, click on the HAProxy application tile on the application dashboard. The App Info panel then replaces the App Summary panel.
View the real-time performance of HAProxy application

Citrix ADM enables you to view the real-time performance of your HAProxy applications. It provides the following real-time details of the selected HAProxy application:

- **Transactions.** Transactions performed by the application.
- **Throughput.** Throughput of the application.
- **Sessions.** Number of sessions established by the application.

To view real-time performance of your HAProxy application, on the Application Dashboard, double-click the HAProxy application tile.
By default, the **Transactions** tab is selected and the real-time transactions performed by the application is displayed.

To view the real-time throughput of the application, click the **Throughput** tab.
You can click the **Sessions** tab to view the number of sessions established by the application in real-time.
Third-party licensing

August 1, 2019

After you add the hosts to Citrix Application Delivery Management (Citrix ADM), Citrix ADM automatically discovers the HAProxy instances provisioned on the hosts and adds them to Citrix ADM Inventory. It also discovers all the frontends, backends, and servers configured on the HAProxy instances and considers the frontends as discovered applications.

You can manage and monitor all the discovered applications but, by default, the HAProxy App Dashboard displays the application statistics for 30 discovered applications. For more information about HAProxy App Dashboard, see HAProxy App Dashboard. If you want to view the application statistics of more than 30 discovered applications, you need to purchase a separate license.

![Managed Third Party licensed Virtual Servers](image)

Licenses for additional frontends are available in virtual server packs of 100. You can obtain a valid license and install the license by using the Citrix ADM GUI.

Installing the third-party licenses

You can install a license on Citrix ADM to view the application statistics of more than 30 discovered applications.

To install a license:

1. In a web browser, type the IP address of the [NetScaler Management and Analytics System](http://192.168.100.1) (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Networks > Licenses.
4. In the License Files section, select one of the following options:
• **Upload license files from a local computer.** If a license is already present on your local computer, click Browse and select the license file (.lic) that you want to use to allocate your licenses. Click **Finish**.

• **Use License Activation Code** - Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box and then click **Get Licenses**.

**Note**

If you select this option, the NetScaler Management and Analytics System must be connected to the Internet, or a proxy server must be available.

You can verify the licenses installed on your Citrix ADM by navigating to **Networks > Licenses > Third Party Licenses**.
Managing the third-party licenses

The Citrix ADM randomly selects the discovered applications in the HAProxy instances and automatically licenses them. If you want to change the selected discovered applications, you need to manually unlicense the licensed discovered applications and then allocate the licenses to the discovered applications that you want to license.

To manage the third-party licenses:

1. Navigate to Networks > Licenses > Third Party licenses and click Modify Third party licensed Virtual Servers. The dashboard displays the managed frontends.

2. Select the frontends from the list, Mark Unlicensed, and click Finish to free up the licenses.

3. After you free up the licenses, or if you already have licenses available, click Add HAProxy Frontends.
4. In the **Choose HAPoxy Frontend** dialog box, select the unlicensed frontends from the list and click **Select**.

5. Click **Finish Now**.

**Role-based access control for HAPoxy instances**

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) uses fine-grained, role-based access control (RBAC) to control access to configuration objects. For example, you can create users and give them access to particular instances of HAPoxy, and you can specify view/read-only permission for HAPoxy App dashboard. For more information, see [Role Based Access Control in Citrix ADM](#).

**Monitor HAPoxy instances**

August 1, 2019
The HAProxy dashboard in Citrix Application Delivery Management (Citrix ADM) displays graphs that help you keep track of CPU and memory usage of an HAProxy instance. The dashboard also displays graphs that indicate the following:

- Percentage of CPU used by the HAProxy instance on the host.
- Percentage of CPU used by other entities on the host.
- Percentage of CPU remaining on the host.
- Percentage of memory used by the HAProxy instance on the host.
- Percentage of memory used by other entities on the host.
- Percentage of memory remaining on the host.

To monitor an HAProxy instance in Citrix ADM, navigate to the **Networks > Instances > HAProxy > Instances** tab, select the HAProxy instance, and click **Dashboard**.

View the details of frontends configured on HAProxy instances

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) reports the following details of the frontend configured on an HAProxy instance:

- **Host IP Address.** IP address of the host
**Configuration Path.** Absolute configuration path of the HAProxy instance on the host.

**Name.** Name of the frontend that handles the incoming traffic.

**Bind Host.** IP address to which the frontend is bound.

**Bind Port.** Port to which the frontend is bound.

**To view the frontend configured on the HAProxy instances:**

In Citrix ADM, navigate to **Networks > Network Functions > HAProxy > Frontends.**

---

**View the details of backends configured on HAProxy instances**

**August 1, 2019**

Citrix Application Delivery Management (Citrix ADM) reports the following details of a backend application configured on an HAProxy instance:

- **Host IP Address.** IP address of the host.
- **Configuration Path.** HAProxy instance path on the host.
- **Name.** Name of the backend to which the traffic is forwarded.
- **Algorithm.** Load balancing algorithm used to balance the traffic.

**To view the backend configured on the HAProxy instances:**
In Citrix ADM, navigate to **Networks > Network Functions > HAProx > Backends**.

### Backends

<table>
<thead>
<tr>
<th>Host IPAddress</th>
<th>Configuration Path</th>
<th>Backend Name</th>
<th>Name</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal3.cfg</td>
<td>api_backend2</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal1.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal4.cfg</td>
<td>api_backend2</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal2.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal4.cfg</td>
<td>api_backend2</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal1.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal2.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>roundrobin</td>
</tr>
</tbody>
</table>

**View the details of servers configured on HAProx instances**

August 1, 2019

Citrix Application Delivery Management (Citrix ADM) reports the following details of servers configured on an HAProx instance:

- **Host IP Address**. Name of the host.
- **Configuration Path**. Absolute path of the HAProx instance configuration file on the host.
- **Backend Name**. Name of the backend in the HAProx configuration.
- **Name**. Name of the Server in the HAProx configuration.
- **Server Address**. IP address of the server.
- **Server Port**. Port used by the server.

To view the servers configured on the HAProx instances:

In Citrix ADM, navigate to **Networks > Network Functions > HAProx > Servers**.

### Servers

<table>
<thead>
<tr>
<th>Host IPAddress</th>
<th>Configuration Path</th>
<th>Backend Name</th>
<th>Name</th>
<th>Server Address</th>
<th>Server Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.205.179</td>
<td>lb_testportal3.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>10.102.213.219</td>
<td>80</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal1.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>10.102.213.219</td>
<td>80</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal4.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>10.102.213.219</td>
<td>80</td>
</tr>
<tr>
<td>10.102.205.59</td>
<td>lb_testportal2.cfg</td>
<td>api_backend1</td>
<td>api_machine1</td>
<td>10.102.213.219</td>
<td>80</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
View the HAProxy instances with the highest number of frontends or servers

August 1, 2019

On the Application Dashboard, Citrix Application Delivery Management (Citrix ADM) displays the number of HAProxy instances that it discovers, and it lists the top five HAProxy instances that are configured with highest number of frontends or servers.

To view the Application Dashboard, in Citrix ADM, navigate to Applications > Dashboard.

The number of HAProxy instances discovered by Citrix ADM is displayed in the top row, as shown below:

To view the list of top five HAProxy instances that are configured with highest number of frontends or the highest number of servers, scroll down the dashboard:
To restart a HAProxy instance from the Citrix Application Delivery Management (Citrix ADM) GUI, you can select either hard restart or soft restart.

**Hard restart**

Hard restart terminates the HAProxy process on the instance and closes all the established connections. After the restart a new haproxy process is created and the subsequent new connections are processed by the new HAProxy process.

**Soft restart**

Soft restart unbinds the HAProxy process from the listening port, but the HAProxy process continues to process existing connections until they close. A new HAProxy process is created to process new connections.

**To restart an HAProxy instance, do the following:**

1. Navigate to **Networks > Instances > HAProxy** and click the **Instance** tab.
2. On the **Instance** tab, select the HAProxy instance that you want to restart.
3. Click **Hard Restart** to hard restart the HAProxy instance or click **Soft Restart** to soft restart the HAProxy instance.
You can back up the current state of a HAProxy instance in an HAProxy configuration file. If the instance becomes unstable, you can use the backedup file to restore the instance to the stable state.

To back up an HAProxy instance by using Citrix ADM:

1. In Citrix Application Delivery Management (Citrix ADM), navigate to Networks > Instances > HAProxy.
2. In the HAProxy page, click the Instances tab.
3. Select the HAProxy instance that you want to back up, and then click View Backup.
5. You can choose to encrypt your backup file for additional security.
6. Click **Continue**.

**To restore an instance by using Citrix ADM:**

1. Navigate to **Networks > Instances > HAProxy**.
2. On the **HAProxy** page, click the **Instances** tab.
3. Select the instance that you want to restore, and then click **View Backup**.

4. On the **Backup Files** page, select the backup file that you want to restore, and then click **Restore**.

**Note**

When you restore an instance, Citrix ADM soft restarts the HAProxy instance.

**Edit the HAProxy configuration file**

August 1, 2019

You can update the frontend, backend, server and other settings in the existing HAProxy configuration file. To edit the HAProxy configuration file:
- Back up the HAProxy configuration file.
- Download the backup HAProxy configuration file and edit it offline.
- Upload the updated HAProxy configuration file to Citrix Application Delivery Management (Citrix ADM).
- Restore the HAProxy instance with the updated backup file.

To edit the HAProxy configuration file by using Citrix ADM:

1. In Citrix ADM, navigate to **Networks > Instances > HAProxy**.
2. On the **HAProxy** page, click the **Instances** tab.
3. Select the HAProxy instance that you want to back up, and then click **View Backup**.
4. On the **Backup Files** page, click **Back Up**.
5. Click **Continue**.
6. On the **Backup Files** page, select the backup file and click **Download**.

**Note**
Do not encrypt the backup file.
7. Using a text editor, edit the HAProxy configuration file.

8. On the **Backup Files** page, click **Upload** to browse and select the updated HAProxy configuration file.

After the updated HAProxy configuration file is uploaded, it is listed on the **Backup Files** page.

9. Select the updated HAProxy configuration file and click **Restore**.

---

**Manage system settings**

August 1, 2019

The following table describes how to configure the system settings on your Citrix ADM.

<table>
<thead>
<tr>
<th>If you want to …</th>
<th>Do this …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure message of the day</td>
<td>You can now create a welcome message in Citrix ADM. You can use this feature to set reminder messages for yourself or the user who logs on to Citrix ADM. Navigate to <strong>System &gt; System Settings</strong> and click <strong>Configure message of the day</strong>. Click <strong>Enable Message</strong>, type the message in the message box, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Shut down Citrix ADM</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. You can click on <strong>Shut Down Citrix ADM</strong> to completely shut down Citrix ADM. <strong>Note</strong> Once you shut down Citrix ADM, you can start Citrix ADM again only from the hypervisor where you have installed it.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure the setup wizard settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up Citrix ADM</strong>, select <strong>Setup Wizard Settings</strong>. You can select the <strong>Citrix ADM Network</strong> option to modify network settings, such as IP address of Citrix ADM, and its password. You can click <strong>System Settings</strong> to modify the hostname, mode of communication with the instance(s), or local time zone.</td>
</tr>
<tr>
<td>Configure the network settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up Citrix ADM</strong>, select <strong>Network Configuration</strong>. The GUI displays the SSL certificates and keys installed on the Citrix ADM.</td>
</tr>
<tr>
<td>View SSL certificate</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up Citrix ADM</strong>, select <strong>View SSL Certificate</strong>. The GUI displays the SSL certificates and keys installed on the Citrix ADM.</td>
</tr>
<tr>
<td>Change Time Zone</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Change Time Zone</strong>. From the <strong>Time Zone drop-down</strong> list, select the time zone for your Citrix ADM appliance’s clock.</td>
</tr>
<tr>
<td>Change Hostname</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Change Hostname</strong>. Enter a hostname that will be used to identify your Citrix ADM, so that when you generate the universal license for Citrix ADM Gateway, the hostname is displayed in the license.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change the system settings</td>
<td>Navigate to System &gt; System Administration. Under System Settings, select Change System Settings. Then, select or clear check boxes to enable or disable the following features- Secure Access Only, Enable Session Timeout, Allow Basic Authentication, Enable nsrecover Login, Enable Certificate Download, Enable Shell access for non-nsroot User, Prompt for user credentials for instance login</td>
</tr>
<tr>
<td>Configure the SSL settings</td>
<td>Navigate to System &gt; System Administration. Under System Settings, select Configure SSL Settings to display the current protocol settings and the applied cipher suites. If you want to modify any of the settings, under Edit Settings, select Protocol Settings or Cipher Suites.</td>
</tr>
<tr>
<td>Enable the user experience improvement settings feature</td>
<td>Navigate to System &gt; System Administration. Under System Settings, select Configure User Experience Improvement Settings, and then select the Enable CUXIP check box. If you select this check box, usage statistics are collected for the sole purpose of improving the graphical user interface. The received data is used only by Citrix engineers and is not shared with anyone.</td>
</tr>
<tr>
<td>Upgrade Citrix ADM</td>
<td>Navigate to System &gt; System Administration. Under the System Administration subheading, select Upgrade Citrix ADM, and then select the new image file. You can select a file that is already on the Citrix ADM virtual appliance, or you can upload a file from your local computer.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restart Citrix ADM</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under the <strong>System Administration</strong> subheading, select <strong>Reboot Citrix ADM</strong>. A dialog box appears, asking you to confirm your action. Click <strong>Yes</strong>.</td>
</tr>
<tr>
<td>Configure the system prune settings (for pruning old data)</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Prune Settings</strong>, select <strong>System Prune Settings</strong>. In the Data to keep (days) field, enter the number of days for which to retain data in the system.</td>
</tr>
<tr>
<td>Configure the system backup settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Backup Settings</strong>, select <strong>System Backup Settings</strong>, and then enter the number of system backups to retain on the Citrix ADM appliance. You can also elect to encrypt the backup files, and you can specify an external location to which to transfer them. Transferred backup files can be retained on or deleted from the system.</td>
</tr>
<tr>
<td>Configure the instance backup settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Backup Settings</strong>, select <strong>Instance Backup Settings</strong>, and enter the time interval (in hours) at which to create a backup file backing up all the instances managed by the Citrix ADM. You can specify the number of backup files to retain, and whether to encrypt them so that they cannot be accessed without a password.</td>
</tr>
<tr>
<td>View the system statistics</td>
<td>Navigate to <strong>System &gt; Statistics</strong>. A line graph displays information such as CPU usage, memory usage, and disk usage.</td>
</tr>
<tr>
<td>View and manage sessions</td>
<td>Navigate to <strong>System &gt; Sessions</strong>. You can then see all the active sessions, with details. To terminate a session, select its check box and click <strong>Cancel Session</strong>.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add or modify a tenant</td>
<td>Navigate to <strong>System &gt; Tenants</strong>, and add a new tenant or edit the settings for an existing tenant. You can provide additional information, such as an organizational unit name, department, and URL for the tenant.</td>
</tr>
<tr>
<td>Change the user lockout policy</td>
<td>Navigate to <strong>System &gt; User Administration</strong>. Under <strong>User Configuration</strong>, select <strong>User Lockout Configuration</strong>, and then select the <strong>Enable User Lockout</strong> check box. You can specify the number of invalid attempts a user can make before their account is disabled, and for how long the user-lockout policy is active.</td>
</tr>
<tr>
<td>Change the password complexity</td>
<td>Navigate to <strong>System &gt; User Administration</strong>. Under <strong>User Configuration</strong>, select <strong>Password Policy</strong>, and then select the <strong>Enable Password Complexity</strong> check box. In the <strong>Minimum Password Length</strong> field, enter the minimum number of characters required for a password on the Citrix ADM.</td>
</tr>
<tr>
<td>Add or modify a user</td>
<td>Navigate to <strong>System &gt; User Administration &gt; Users</strong>. Under Users, add a new user or edit the settings for an existing user. When adding a user, you can enable options such as external authentication, session timeout, and assigning the user to specific groups.</td>
</tr>
<tr>
<td>Add or modify a user group</td>
<td>Navigate to <strong>System &gt; User Administration &gt; Groups</strong>. Under Groups, add a new group or edit the settings for an existing group. When adding a group, you can enable options such as assigning permissions for the group, configuring a session timeout, assigning users to the group, and allowing access to particular or all applications on the Citrix ADM.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>Change the authentication configuration</strong></td>
<td>Navigate to <strong>System &gt; Authentication &gt; Authentication</strong>. Under <strong>Authentication</strong>, select <strong>Authentication Configuration</strong>, and select the type of authentication server.</td>
</tr>
<tr>
<td><strong>Add or modify a RADIUS server</strong></td>
<td>Navigate to <strong>System &gt; Authentication &gt; RADIUS</strong>. Under <strong>RADIUS</strong>, add a new RADIUS server or edit the settings for an existing RADIUS server by entering or modifying the network parameters.</td>
</tr>
<tr>
<td><strong>Add or modify an LDAP server</strong></td>
<td>Navigate to <strong>System &gt; Authentication &gt; LDAP</strong>. Under <strong>LDAP</strong>, add a new LDAP server or edit the settings for an existing LDAP server by entering or modifying the network parameters.</td>
</tr>
<tr>
<td><strong>Add or modify a TACACS server</strong></td>
<td>Navigate to <strong>System &gt; Authentication &gt; TACACS</strong>. Under <strong>TACACS</strong>, add a new TACACS server or edit the settings for an existing TACACS server by entering or modifying the network parameters.</td>
</tr>
<tr>
<td><strong>Add or modify a syslog server</strong></td>
<td>Navigate to <strong>System &gt; Auditing &gt; Syslog Servers</strong>. Under <strong>Syslog Servers</strong>, add a new syslog server or edit the settings for an existing syslog server by entering or modifying the network parameters. You can provide additional information by selecting the kind of log levels you want to monitor.</td>
</tr>
<tr>
<td><strong>Read syslog messages</strong></td>
<td>Navigate to <strong>System &gt; Auditing</strong>. Under <strong>Audit Messages</strong>, select <strong>Syslog Messages</strong>. Summaries of all system log files are displayed in the Syslog Viewer. You can select the syslog file you want to view from the File drop-down option. Additionally, syslog files can be further filtered by module, event type, and severity.</td>
</tr>
<tr>
<td><strong>Configure the syslog purge settings</strong></td>
<td>Navigate to <strong>System &gt; Auditing</strong>. Under <strong>Settings</strong>, select <strong>Syslog Purge Settings</strong>, and then enter the number of days to retain syslog data before it is deleted from the Citrix ADM.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>View system events</td>
<td>Navigate to <strong>System &gt; Events</strong>. You can then see all the current events, with details.</td>
</tr>
<tr>
<td>Add or modify an NTP server</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong>. Add a new NTP server or edit the settings for an existing NTP server.</td>
</tr>
<tr>
<td>Configure NTP parameters</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong>. Click <strong>NTP Parameters</strong> and enter the server’s configuration details in given fields provided.</td>
</tr>
<tr>
<td>Enable NTP synchronization</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong>. To synchronize the time displayed on the NTP server with your local clock, select the <strong>Enable NTP Synchronization</strong> check box.</td>
</tr>
<tr>
<td>Add or modify cipher groups</td>
<td>Navigate to <strong>System &gt; Cipher Groups</strong> to add a new cipher group or edit the settings of an existing cipher group. You must enter a description of your cipher group and assign it to a cipher suite.</td>
</tr>
<tr>
<td>Configure notification settings</td>
<td>Navigate to <strong>System &gt; Notifications</strong>. Under <strong>Settings</strong>, select <strong>Change Notification Settings</strong>. Choose the actions for which you want to send the notifications, and select <strong>Email</strong>, <strong>SMS</strong>, or both.</td>
</tr>
<tr>
<td>Configure event digest settings</td>
<td>Navigate to <strong>System &gt; Notifications</strong>. Under <strong>Settings</strong>, select <strong>Configure Event Digest Settings</strong>. After clearing the <strong>Disable Event Digest</strong> check box, you can set a recurrence period and choose an email distribution list for sending event digest notifications.</td>
</tr>
<tr>
<td>Add or modify email servers</td>
<td>Navigate to <strong>System &gt; Notifications &gt; Email</strong>. Under <strong>Email</strong>, select the <strong>Email Servers</strong> tab to add a new email server or edit the settings for an existing email server. You can enable additional checks to ensure that authentication is required for access to the email server or to specify that your email server supports SSL authentication.</td>
</tr>
<tr>
<td>If you want to ...</td>
<td>Do this ...</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Add or modify email distribution lists</td>
<td>Navigate to <strong>System &gt; Notifications &gt; Email.</strong> Under Email, select the <strong>Email Distribution List</strong> tab to add a new email distribution list or edit the settings for an existing email distribution list.</td>
</tr>
<tr>
<td>Add or modify SMS servers</td>
<td>Navigate to <strong>System &gt; Notifications &gt; SMS.</strong> Under SMS, select the <strong>SMS Server</strong> tab to add a new SMS server or edit the settings for an existing SMS server.</td>
</tr>
<tr>
<td>Add or modify SMS distribution lists</td>
<td>Navigate to <strong>System &gt; Notifications &gt; SMS.</strong> Under SMS, select the <strong>SMS Distribution List</strong> tab to add a new SMS distribution list or edit the settings for an existing SMS distribution list.</td>
</tr>
<tr>
<td>Configure SNMP Engine ID</td>
<td>Navigate to <strong>System &gt; SNMP.</strong> Under <strong>Settings</strong>, select <strong>Configure Engine ID</strong> and specify the Engine ID.</td>
</tr>
<tr>
<td>Configure SNMP MIB</td>
<td>Navigate to <strong>System &gt; SNMP.</strong> Under <strong>Settings</strong>, select <strong>Configure SNMP MIB</strong>, and enter the SNMP MIB details.</td>
</tr>
<tr>
<td>Configure SNMP Traps</td>
<td>Navigate to <strong>System &gt; SNMP &gt; Trap Destinations.</strong> Under <strong>SNMP Traps</strong>, add a new SNMP trap destination or edit the settings for an existing SNMP trap destination.</td>
</tr>
<tr>
<td>Add or modify an SNMP manager</td>
<td>Navigate to <strong>System &gt; SNMP &gt; Managers.</strong> Under <strong>SNMP Manager</strong>, add a new SNMP manager or edit the settings for an existing SNMP manager.</td>
</tr>
<tr>
<td>Add or modify an SNMP user</td>
<td>Navigate to <strong>System &gt; SNMP &gt; Users.</strong> Under <strong>SNMP User</strong>, add a new SNMP user or edit the settings for an existing SNMP user.</td>
</tr>
<tr>
<td>Add or modify SNMP views</td>
<td>Navigate to <strong>System &gt; SNMP &gt; Views.</strong> Under <strong>SNMP View</strong>, add a new SNMP view or edit the settings for an existing SNMP view.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modify alarms</td>
<td>Navigate to <strong>System &gt; Alarms</strong> and select the alarm whose settings you want to modify. Alarms help you monitor the health of your Citrix ADM server.</td>
</tr>
<tr>
<td>View the task log</td>
<td>Navigate to <strong>System &gt; Diagnostics &gt; Task Logs</strong>. You can then see all the task logs, with details. You can view additional information by selecting a task log and viewing its Device Log, and then view the Command Log for the selected device log.</td>
</tr>
<tr>
<td>Generate the technical support file</td>
<td>Navigate to <strong>System &gt; Diagnostics &gt; Technical Support</strong>. Under <strong>Technical Support</strong>, click <strong>Generate Technical Support File</strong> to generate an archive (TAR file) of the Citrix ADM data and statistics, which you can send to Citrix Support for help with debugging an issue.</td>
</tr>
<tr>
<td>Configure Dashboard reporting timezone settings</td>
<td>Navigate to <strong>System &gt; Analytics Settings</strong>. Under <strong>Analytics Settings</strong>, select <strong>Configure Dashboard Reporting Time Zone Settings</strong> to set your local time or GMT zone as the default for the reports displayed on your dashboard.</td>
</tr>
<tr>
<td>Configure ICA session timeout</td>
<td>Navigate to <strong>System &gt; Analytics Settings</strong>. Under <strong>Analytics Settings</strong>, select <strong>Configure ICA Session Timeout</strong> and enter the amount of time for which an ICA session can remain in an idle state before being terminated.</td>
</tr>
<tr>
<td>If you want to …</td>
<td>Do this …</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Configure analytics features</td>
<td>Navigate to <strong>System &gt; Analytics Settings</strong>. Under <strong>Analytics Settings</strong>, select <strong>Configure Features</strong> to enable multihop settings and adaptive threshold settings. If you select the <strong>Enable Multihop</strong> check box, Citrix ADM collects and correlates the AppFlow records from all appliances deployed with more than one Citrix ADC instance between a client and a server. If you select the <strong>Enable Adaptive Threshold</strong> check box, a syslog message is sent to the syslog server whenever the number of hits on a URL is higher than it's threshold value.</td>
</tr>
<tr>
<td>Configure database settings</td>
<td>Navigate to <strong>System &gt; Analytics Settings</strong>. Under <strong>Analytics Settings</strong>, select <strong>Configure Features</strong> to enable database index settings and database cleanup settings. By selecting the <strong>Enable Database Indexing</strong> check box, you can facilitate efficient querying of the Citrix ADM database. If you select the <strong>Enable Database Cleanup</strong> check box, an attempt to clean up the database is repeated if a heavy load on the Citrix ADM prevents cleanup at its regularly scheduled time.</td>
</tr>
<tr>
<td>Configure database cache settings</td>
<td>Navigate to <strong>System &gt; Analytics Settings</strong>. Under <strong>Analytics Settings</strong>, select <strong>Configure Database Cache Settings</strong> to locally store the database content in the cache, so that you can view this content without needing access to the database server.</td>
</tr>
<tr>
<td>Configure data record settings</td>
<td>In <strong>Analytics Settings</strong>, select <strong>Configure Data Record Settings</strong>. You can enable features for the following settings- Data Record Log Settings, Data Duration Persistency Settings, Web Insight Report Settings, Web Insight SLA Data Collection Settings, Web Insight URL Data Collection Settings, URL Parameter Settings</td>
</tr>
</tbody>
</table>
If you want to … | Do this …
---|---
Configure SLA Management for specific Citrix ADC IP addresses | Navigate to **System > Analytics Settings > SLA Management**. From the list displayed, select the Citrix ADC IP address of an appliance on which you want to manage SLA over server response time, hits/second, and bandwidth usage.

Configure the duration for which to retain database records for each Insight summarization level | Navigate to **System > Analytics Settings > Database Summarization**. Specify the duration for which you want to retain Insight data on Citrix ADM. You can choose to store this data either hourly, daily, and once every minute.

Add or modify adaptive thresholds | Navigate to **System > Analytics Settings > Adaptive Thresholds**. Under **Adaptive Thresholds**, add a new adaptive threshold or edit the settings for an existing adaptive threshold. The adaptive threshold functionality sets the threshold value for the maximum number of hits on each URL. If the maximum number of hits on a URL is higher than the threshold value set for the URL, a syslog message is sent to an external syslog server. The threshold value interval can be either days or weeks.

Add or modify threshold and alerts | Navigate to **System > Analytics Settings > Thresholds**. Under **Thresholds**, add a new limit or edit the settings for an existing threshold. You can provide additional action items while creating or modifying a threshold, such as enabling it, sending notifications by email or SMS, or configuring a rule for the threshold.
<table>
<thead>
<tr>
<th>If you want to …</th>
<th>Do this …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload SSL certificate files and SSL keys</td>
<td>Navigate to System &gt; Advanced Settings &gt; SSL Certificate Files. Under SSL Certificate Files, select the SSL Certificates tab to upload a new SSL certificate. Similarly, under SSL Certificate Files, select the SSL Keys tab to upload a new SSL key.</td>
</tr>
<tr>
<td>View or edit report export schedule/s</td>
<td>Navigate to System &gt; Advanced Settings &gt; Export Schedules. You can then see all the export schedules, with details. You can edit any export schedule from the list displayed here.</td>
</tr>
<tr>
<td>Schedule a report export</td>
<td>Navigate to System &gt; Advanced Settings &gt; Export Schedules. To add a new schedule, click the button on the extreme right, and select the Schedule Export tab. Specify the details and click Schedule.</td>
</tr>
<tr>
<td>Use the backup and restore features</td>
<td>Navigate to System &gt; Advanced Settings &gt; Backup Files to create a backup of the current settings of the Citrix ADM. You can later use these backed up files to restore the Citrix ADM to the state that you backed up. Citrix recommends using this feature before performing an upgrade, and in general as a precautionary measure.</td>
</tr>
<tr>
<td>Install an SSL certificate</td>
<td>Navigate to System &gt; System Administration. Under Set Up Citrix ADM, select Install SSL Certificate. You can select a certificate file and SSL key file that are already on the Citrix ADM virtual appliance, or you can upload the files from your local computer. You must enter the Citrix ADM password in the Password field to successfully install the SSL certificate.</td>
</tr>
<tr>
<td>Prompt Credentials for Instance Login</td>
<td>Navigate to System &gt; Change System Settings. Enable Prompt Credentials for Instance Login to prompt users for their instance credentials in any configuration operation on Citrix ADC instances.</td>
</tr>
</tbody>
</table>
Enable Automatic Data Purge

Navigate to **System > System Administration**. Under **Prune Settings**, select **System Prune Settings**. Select **Enable Automatic Data Purge** check box to allow Citrix ADM to purge the data when the disk usage reaches the set threshold value. When this feature is enabled, Citrix ADM purges data related to events, syslogs, perf reporting, and analytics until disk usage comes below the set threshold value. Click the edit icon to modify the threshold value for disk usage.

---

**Configure system backup settings**

August 1, 2019

You should set your initial System Backup Settings before you need to back up and restore the Citrix Application Delivery Management (ADM) system.

1. Navigate to **System > System Administration**. Under **Backup Settings**, click **System Backup Settings**.

2. On the **Configure System Backup Settings** page, specify the following:
   - Number of backups to retain. You can only retain up to 10 backups.
   - Encrypt the backup file.
   - Enable external transfer. You can transfer a copy of 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 file to the Citrix ADM server and then perform the restore operation. Specify the server, user name and password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see Transferring a Citrix ADM Backup File to an External System.

3. Click **OK**.
Configure a NTP server

August 1, 2019

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

To configure an NTP server on Citrix ADM:

1. Navigate to System > NTP Servers, and then click Add.
2. On the Create NTP Server page, enter the following details:
   - Server Name/IP Address – Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - Minimum Poll Interval – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as $2^6$, enter 6.
   - Maximum Poll Interval – Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as $2^8$, enter 8.
   - Key Identifier - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.
   - Autokey - Select Autokey if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
• **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

To enable NTP synchronization on Citrix ADM:

1. Navigate to **System > NTP Servers**.

2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** checkbox.

3. Click **OK**.

---

**Upgrade Citrix ADM**

August 1, 2019

Each Citrix Application Delivery Management (ADM) release offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read the release notes before you upgrade the software. It is important to understand the licensing framework and types of licenses before you start to upgrade.

To upgrade Citrix ADM:

1. Navigate to **System > System Administrations**. Under the **System Administration** sub-heading, click **Upgrade Citrix ADM**.
2. On the Upgrade Citrix ADM page, upload a new image file by selecting either **Local** (your local machine) or **Appliance** (the certificate file must be present on the Citrix ADM virtual appliance). By default, the software image is cleaned up after a successful upgrade.

3. Click **OK**.

![Upgrade Citrix ADM](image)

---

**How to reset the password for Citrix ADM**

August 1, 2019

The procedure to reset the password for Citrix ADM might differ on hypervisors where it is hosted. If you have changed your default password and want to reset to default password, you can reset the password by rebooting the Citrix ADM node.

**Citrix Hypervisor using XenCenter:**

1. Log on to Citrix Hypervisor using XenCenter.
2. Select the Citrix ADM node, right-click, and select **Reboot**.
3. On the **Console** tab, press **CTRL + C** to interrupt the boot sequence.
4. Run `boot -s` command at the OK prompt.

Citrix ADM reboots and displays the following message:
5. Press **Enter** to get the /u@ prompt.

6. Mount the flash partition using the following command:

```
mount dev/ad0s1a /flash
```
7. Create a new file using the following command:

   touch /flash/mpsconfig/.recover

   The password is now reset to default password.

8. Run the Reboot command to reboot Citrix ADM.

9. Access the Citrix ADM GUI and wait until the reboot is complete.
You can now use nsroot/nsroot credentials to log on from GUI and nsrecover/nsroot to log on from hypervisor.

**Esx using vSphere:**

1. Log on to ESX using vSphere.
2. Select the Citrix ADM node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.
4. Run **boot -s** command in the OK prompt.

   The Citrix ADM reboots.
5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

   ```bash
   mount dev/da0s1a /flash
   ```
7. Create a new file using the following command:

   ```bash
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.
8. Run the **Reboot** command to reboot Citrix ADM.

9. Access the Citrix ADM GUI and wait until the reboot is complete.

You can now use `nsroot/nsroot` credentials to log on from GUI and `nsrecover/nsroot` to log on from ESX server.

**Hyper-v using Hyper-v manager:**

1. Log on to hyper-v using hyper-v manager.

2. Select the Citrix ADM node, right-click, and then select **Reboot**.

3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.

4. Run the **boot -s** command at the OK prompt.

   The Citrix ADM reboots.

5. Press **Enter** to get the `/u@` prompt.

6. Mount the flash partition using the following command:

   ```bash
   mount dev/ad0s1a /flash
   ```
7. Create a new file using the following command:

```
touch /flash/mpsconfig/.recover
```

The password is now reset to default password.

8. Run the **Reboot** command to reboot Citrix ADM.

9. Access the Citrix ADM GUI and wait until the reboot is complete.

You can now use **nsroot/nsroot** credentials to log on from GUI and **nsrecover/nsroot** to log on from hyper-v manager.

**Linux KVM server (SSH to KVM Server by using any SSH client):**

1. Log on to Citrix ADM using an SSH client to the KVM server.

2. Reboot Citrix ADM.

3. Press **CTL + C** to interrupt the boot sequence shortly after the **Loading /boot/default-s/loader.conf** message is displayed.

4. At the OK prompt, execute the following command:

```
set console="comconsole,vidconsole"
```

5. Run the **boot -s** command to reboot Citrix ADM.

6. After the **Enter full path of shell or RETURN for /bin/sh:** message is displayed, press **Enter** to get the /u@ prompt.

7. Mount the flash partition using the following command:

```
mount dev/vtbd0s1a /flash
```

8. Create a new file using the following command:

```
touch /flash/mpsconfig/.recover
```

The password is now reset to default password.

9. Run the **Reboot** command to reboot Citrix ADM.
10. Access the Citrix ADM GUI and wait until the reboot is complete.

You can now use nsroot/nsroot credentials to log on from GUI and nsrecover/nsroot to log on from the SSH console.

**Configure syslog purging interval**

August 1, 2019

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the Citrix Application Delivery Controller (ADC) instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the Citrix ADC instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the following syslog data will be deleted from Citrix Application Delivery Management (ADM):

- Generic Syslog Data
- AppFirewall Data
- Citrix Gateway Data

You can also configure the Citrix Gateway purge interval by syslog type. This purge interval takes precedence over the purge interval configured to retain Citrix Gateway data.

**To configure syslog purge interval settings for Citrix ADM:**

1. Navigate to **System > System Administration**. Under **Prune Settings**, click **Instance Syslog Prune Settings**.
2. In **Configure Instance Syslog Purge Settings** page, specify **Retain Syslog Generic Data**. Type the number of days for which Citrix ADM retains generic syslog messages.

![Configure Instance Syslog Prune Settings](image)

**Configure system prune settings**

August 1, 2019

To limit the amount of reporting data being stored in your Citrix Application Delivery Management (ADM) software’s database, you can prune it. You can specify the interval for which you want Citrix ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

**Note**

The value you specify cannot exceed 30 days or be less than 15 days.

**To configure system prune settings for performance reports using Citrix ADM:**

1. Navigate to **System > System Administration**. Under **Prune Settings**, click **System Prune Settings**.

2. In the **Configure System Prune Settings** page, specify the number of days for which to retain data, and click **OK**.
You can enable automatic purging by selecting the **Enable Automatic Data Purge** check box. An alarm is triggered when disk usage breaches the configured **Data Purge Threshold Value**.

You can configure and enable the **diskUtilizationHigh** alarm (by default) and specify the following:

- **Severity**, such as, Critical.
- **Alarm Threshold**. Type the value for which the event severity is calculated.
- **Time**. Time length (in minutes) after which you want to trigger the alarm.
Enable shell access for non-default users

August 1, 2019

You can enable shell access for non-default users in Citrix Application Delivery Management (ADM). You can use this feature to enable and set up communication mode with instances.

Note
By default, shell access is disabled for non-default users.

To enable shell access for non-default users in Citrix ADM:

1. In Citrix ADM, navigate to System > System Administration.
2. In System Settings, click Change System Settings.
3. On the Modify System Settings page, configure the following parameters:
Communication with instances - Select the communication protocol.
Secure Access - Enable secure access for Citrix ADM.
Enable Session Timeout - Specify the time period for which to retain an inactive session.
Allow Basic Authentication - Allow Management Service to accept credentials given using Basic Authentication Protocol.
Enable nsrecover Login - Enable nsrecover login on Management Service.
Enable Certificate Download - Enables you to download certificates from the added Citrix ADC.
Enable Shell access for non-nsroot User - Enable shell access for non-default users in Citrix ADM.
Prompt user credentials for instance login - Allow users to enter their user credentials while logging on to instances from Citrix ADM.

4. Click OK.

Recover inaccessible Citrix ADM servers

August 19, 2019

Citrix Application Delivery Management (ADM) now provides a database maintenance tool to perform cleanup of the system database. You can now launch the Citrix ADM utility tool to connect to the file system, delete a few components, and make the database accessible. Citrix ADM recovery script is a tool that helps to recover space in the file system by clearing old or unused database tables and files. The tool assists you to navigate through the database tables and files in successive steps and shows the current space occupied on the filesystem by respective items. Once you have selected the database tables and files to be deleted, the tool deletes those from the filesystem after confirmation.

How to Use Citrix ADM Database Recovery Script for a Citrix ADM Standalone Deployment

Use the following procedure in a single server Citrix ADM deployment to connect to the file system, delete a few components, and make the database accessible, and then perform the recovery operations.

1. Using an SSH client or your hypervisor’s console, logon to Citrix ADM and type the following command:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. When the screen displays a caution message for stopping a few Citrix ADM processes, type “y” and press the Enter key.
The following screen appears while the system determines which components of the database you can delete without affecting the system’s core files.

3. The screen displays the list of files in the database. Type “y” and press the Enter key to begin the cleanup process.

4. You can select the specific database component that needs to be cleaned and type the corresponding number. Press the Enter key.

   For example, to perform System Catalog cleanup, select option 8 in the DB component selec-
tion menu and type “y” and press the Enter key to continue with the system catalog clean up.

Note

Citrix ADM includes user tables known as system catalog. The system catalog is a location in the Citrix ADM database where a relational database management system stores schema metadata, such as information about tables and columns and internal records. The tables in the system catalog are like regular tables that can accumulate inflated and dead rows over time and therefore, need periodic cleanup for optimal performance. It is a good practice to regularly maintain these tables. The activity not only frees up disk space but also improves the overall performance of the database and therefore of the Citrix ADM.

The cleanup utility gives you an option to clean database components and file components. You can select any file component by typing a number between “1” and “9,” or type “11” and press the Enter key to clean the database component.

Note

The number “11” indicates that you have not selected any file component to be cleaned and you are going ahead with cleaning up the earlier database component that you had earlier selected. In this example, it is “system catalog.”
5. Type “y” and press the Enter key again in the final confirmation screen.

The System Catalog is cleaned up, which may take time depending on the size of the table in the System Catalog. After the process is complete, a summary screen is shown.
6. Type “y” and press the Enter key to restart Citrix ADM.

   Ensure you restart Citrix ADM after system clean up. Wait for about 30 minutes for internal database operations to complete after Citrix ADM has restarted. You must then be able to connect to Citrix ADM database. If not, run the recovery script again to free up more space. When Citrix ADM is up and running, it must work as expected.

   Note

   The current size of the system catalog table is never equal to Zero after clean up. This is because only empty rows are removed from the table and the table might have some valid entries even after they are cleaned up.

   How to use Citrix ADM database recovery script for a Citrix ADM high availability deployment

   The database system for Citrix ADM servers in a high availability deployment is in continuous synchronization mode. While using the new database recovery tool, you do not need to replicate the procedure on both the Citrix ADM servers.

   1. Using an SSH client or hypervisor’s console, log on to the primary node.

   2. Run the following command:

      `/mps/mas_recovery/mas_recovery.py`

   3. Follow the procedure from step 2 available for Citrix ADM Standalone Deployment Recovery Script
Assign a host name to a Citrix ADM server

August 1, 2019

To identify a Citrix Application Delivery Management (ADM) server, you can assign the server a host name. The host name is displayed on the Universal license for Citrix ADM.

**To assign a host name to a Citrix ADM server:**

1. In Citrix ADM, navigate to **System > System Administration**.
2. Under **System Settings**, click **Change Hostname**.
3. On the **Configure Hostname** page, enter a host name and click **OK**.

Back up and restore your Citrix ADM server in a single-server deployment

August 1, 2019

In a Citrix Application Delivery Management (ADM) single-server deployment, you can take periodic backups of your Citrix ADM server. You can either take a partial backup of the server that includes the configuration files, instance details, system data, and so on, or you can take a complete backup of the entire Citrix ADM server. If your Citrix ADM becomes unstable, you can use these backed up files to restore your server to a stable state. Citrix recommends that you back up your Citrix ADM server's configuration before performing an upgrade or for precautionary reasons.

**How to take a partial backup of your Citrix ADM server and restore it**

In a partial backup process, you can back up the following components of your Citrix ADM server:
• Citrix ADM Configuration Files:
  – SNMP
  – Syslog server configuration files
  – NTP files
  – SSL certificates
  – Control Center files

• Backups of Citrix ADC instances being managed by the Citrix ADM server.

• Configuration audit templates.

• System data stored on the database:
  – List of tenants and users created.
  – External authentication server configuration (LDAP, RADIUS, and others).
  – Configuration jobs and job templates created.

• Infrastructure and application data stored on the database:
  – Data from added and managed Citrix ADC instances.
  – Instance profile details, version details, instance group details, and so on.
  – A static application (group of virtual servers) created by the administrator.

• SNMP settings.

In this backup process, you cannot back up analytics data, events, and syslog messages.

**Back up the Citrix ADM configuration**

By default, the Citrix ADM server backs up the configuration every 24 hours (at 00.30 hours). You can also take a backup at a time of your choosing. You can further move a copy of the backed up file to another system.

The backup is stored as a compressed TAR file that can also be encrypted. By default, three backup files are retained in the server. To avoid issues due to non-availability of disk space, you can store a maximum of 10 backup files on your Citrix ADM server. However, Citrix recommends that you store some copies of your backup files on the server or transfer the files to another system.

**To back up a Citrix ADM configuration:**

1. Navigate to **System > Advanced Settings > Backup Files**, and then click **Back Up**.
2. To encrypt the backup file, select the **Password Protect file** checkbox, and then provide a password to encrypt the file.

![Password Protection](image)

**Note**
You can also set a backup file for encryption by navigating to **System > System Backup Settings**, and then selecting **Encrypt Backup File**.

---

**Transfer a Citrix ADM backup file to an external system**

You can transfer a copy of the backup file to another system as a precautionary measure. When you want to restore the configuration, you have to first upload the file to the Citrix ADM server and then perform the restore operation.

**To transfer a Citrix ADM backup file:**

1. Navigate to **System > Advanced Settings > Backup Files**.
2. Select the backup file that you want to move to another system, and then click **Transfer**.
3. On the **Backup Files** page, specify the following parameters:
   - **Server** - IP address of the system where you want to transfer the backed-up file.
   - **User Name and Password** - User credentials of the new system where the backed-up files are being copied.
   - **Port** - Port number of the system the files are being transferred to.
   - **Transfer Protocol** - Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the backed-up file.
   - **Directory Path** - The location where the backed-up file is being transferred to on the new system.

   Alternatively, you can also set the external systems detail by navigating to **System > System Backup Settings**.

4. You can delete the backup file from Citrix ADM after transfer by selecting the **Delete file from Application Delivery Management after transfer** checkbox.
5. Click **OK** to make the transfer.

**Note**
To save a copy of the backup file in your local system, navigate to **System > Advanced Settings > Backup Files**, select the file you want to copy, and then click **Download**.

**Restore the Citrix ADM configuration from a backup file**

When you restore the Citrix ADM configuration from a previously backed up file, the restore operation untars the backup file and then restores the configuration. The restore operation deletes the existing configuration and replaces it with the configuration in the backup file.

**Note**
The restore operation will not succeed if your backup file has been renamed or if the contents within the backup file have been modified.

**To restore a Citrix ADM configuration from a backup file:**

1. Navigate to **System > Advanced Settings > Backup Files**.
2. Select the backup file that you want to restore, and then click **Restore**.
3. On the confirmation dialog box, click **Yes**.
**Note**

To restore the configuration from a backup file stored in an external system, you have to upload the backup file to the Citrix ADM server before performing the restore operation. To upload the file, navigate to **System > Advanced Settings > Backup Files**, and then click **Upload**.

---

**View auditing information**

August 1, 2019

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the Citrix Application Delivery Controller (ADC) instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the Citrix ADC instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

You can monitor the syslog messages that a Citrix ADC device generates if you configure the device to redirect syslog messages to Citrix Application Delivery Management (ADM). You can schedule a job to create syslog servers that generate different kinds of syslog data using the built-in templates feature in Citrix ADM.

First, configure a syslog server to which the instance can send log information. Then, specify the date and time format for recording log messages.

**To configure a syslog server on Citrix ADM:**

1. Navigate to **System > Auditing**. Under **Configuration Summary**, select **Syslog Servers**. Or you can navigate to **System > Auditing > Syslog Servers**.
2. In the **Syslog Server** page, click **Add**.
3. On the **Create Syslog Server** page, enter the following values:
   - **Name** - Name for the syslog server.
   - **IP Address** - IP address of the syslog server.
   - **Port** - Syslog server port.
4. Choose the log levels (All, None, or Custom). Accordingly, select the severity levels.
5. Click **Create**.

**To configure the syslog date and time format on Citrix ADM:**

1. Navigate to **System > Auditing**. Under **Configuration Summary**, select **Syslog Servers**.
2. In the **Syslog Server** page, select a syslog server, and then, click **Syslog Parameters**.

3. On the **Configure Syslog Parameters** page, specify the date and time format.

4. Click **OK**.

**To view syslog messages on Citrix ADM:**

You can now view all your syslog messages generated on your managed Citrix ADC instances if you have configured your instance to redirect the syslog messages to the Citrix ADM server. The syslog messages are stored in the Citrix ADM server’s database centrally and will make them available on the Syslog Viewer for auditing purposes. You can consolidate this logging information and derive reports for analytics from the collected data.

You can filter this information by module, event type, and severity. You can also configure syslog to log different types of events.

**To view the** **Syslog Viewer**, navigate to **System > Auditing**. In the **Auditing** page, under **Audit Messages**, select **Syslog Messages**. Choose the appropriate filters, to view your system log messages.

**Configure SSL settings**

August 1, 2019

SSL (Secure Socket layer) and TLS (Transport Layer Security) are commonly used security networking protocols that provide encrypted communication between users and servers. You can configure SSL
settings on Citrix Application Delivery Management (ADM) and specify the type of clients that connect to the system.

To configure SSL settings for Citrix ADM:

1. Navigate to **System > System Administration**. Under **System Settings**, click **Configure SSL Settings**.
2. On the **SSL Settings** page, review the current protocol settings and the cipher suites applied to the system.
3. To modify the protocol settings, navigate to **Edit Settings > Protocol Settings** and make the changes that you want.
4. To modify the applied cipher suites, navigate to **Edit Settings > Cipher Suites** and make the changes that you want.
5. Click **OK**, and then click **Close**.

**Monitor CPU, memory, and disk usage**

August 1, 2019

You can use the information maintained in logs and statistics. This information is also displayed in reports that helps you to configure and maintain Citrix Application Delivery Management (ADM).

To monitor CPU, memory, and disk usage,

- **Standalone deployment.** Navigate to **System > Statistics**. You can view real-time CPU, memory, and disk utilization charts.

  ![Statistics](image)

- **High availability deployment.** Navigate to **System > Deployment**. The statistics for memory, CPU, disk space, and managed instances are displayed numerically as shown in the following figure:
Configure system notification settings

August 1, 2019

You can send notifications to select groups of users for a number of system-related functions. These system functions are organized into event categories such as SystemReboot, StatusPoll, SystemState, and so on. You can configure Citrix Application Delivery Management (ADM) to send you notifications either through email or SMS. You have to configure an email server and/or Short Message Service (SMS) gateway server to send email and text notifications to users. This ensures that you are notified of any system-level activities such as user logon or system restart.

For example, you might want to send an email notification to two users when someone attempts to log on to Citrix ADM by using the CLI and the logon attempt fails. You have to configure system notification by selecting the UserLogin category and either create an email notification server or choose an existing email distribution list to send the notification to.

To configure system notification settings on Citrix ADM:


2. On the Configure System Notification Settings page, under Category, select a category such as UserLogin.
3. Select **Send Email**, and either select an email distribution from the drop-down list or click the “+” icon to create a new email distribution list as shown in the figure below. If you want to send text notifications, select **Send SMS (Text Message)** and create an SMS distribution list by clicking the “+” icon and specifying SMS server details.
Create Email Distribution List

Name*
System-Notifications

Email Servers*
10.9.164.57

From
admin@example.com

To*
john@example.com;
chris@example.com

Cc
Email Address(s) to be included in Cc list

Bcc
Email Address(s) to be included in Bcc list

Create  Close
After the notifications are set for certain event categories, whenever an event pertaining to that category occurs, a notification is sent to the recipients either by using email or SMS. In this example, you can see email notification when a user fails to log on to Citrix ADM by using the CLI.

System notifications are sent for the following events:

<table>
<thead>
<tr>
<th>Category</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupFailure</td>
<td>The system backup fails</td>
</tr>
<tr>
<td>DataStorageExceeded</td>
<td>The database storage crosses the limit specified in license</td>
</tr>
<tr>
<td>DeviceBackupFailure</td>
<td>The instance backup fails</td>
</tr>
<tr>
<td>HAMonitoring</td>
<td>The system HA failover occurs, no heartbeats from peer node, and database sync failure occurs</td>
</tr>
<tr>
<td>HealthMonitoring</td>
<td>The CPU, RAM, or Disk utilization crosses threshold value</td>
</tr>
<tr>
<td>LicensePool</td>
<td>The license pool crosses the threshold value</td>
</tr>
<tr>
<td>Licenses</td>
<td>License fails when applied</td>
</tr>
<tr>
<td>PasswordRecovery</td>
<td>Password recovery fails or succeeds</td>
</tr>
<tr>
<td>PerfCounterThresholdHigh</td>
<td>The performance counter value exceeds the limit</td>
</tr>
<tr>
<td>PerfCounterThresholdNormal</td>
<td>The value of the performance counter is normal</td>
</tr>
<tr>
<td>PolicyFailed</td>
<td>Any of the system policies fails</td>
</tr>
<tr>
<td>RemoteDeviceBackupFailure</td>
<td>The remote instance backup fails</td>
</tr>
<tr>
<td>RemoteSystemBackupFailure</td>
<td>The remote system backup fails</td>
</tr>
<tr>
<td>RemoteSystemBackupNormal</td>
<td>The remote system backup succeeds</td>
</tr>
<tr>
<td>SSLCertThreshold</td>
<td>The threshold for a certificate is breached</td>
</tr>
<tr>
<td>StatusPoll</td>
<td>Any change in the state of an instance</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
### Generate a tech support file

August 1, 2019

Citrix recommends that you generate an archive of Citrix Application Delivery Management (ADM) data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

**Note**

For Citrix ADM servers in a high availability mode, you can generate a technical support file from either of the servers. Citrix advises you to not use the load balancing virtual server IP address to generate the technical support file.

**To configure and send a technical support file from Citrix ADM:**

1. Navigate to **System > Diagnostics > Technical Support**, and then click **Generate Technical Support File**.

2. On the **Generate Support File** page, select the following options:

   - **Collect Debug Logs** – Select this option to collect afdecoder logs.

   - **Duration** – Enter the duration for which debug logs should be collected. You will only see this option, if you enable the **Collect Debug Logs** option.

   - **Collect Data Distribution** – Select this option to collect distinct and diverse logs from the database.

```
1 The archive file is created as a TAR file.
2 For example, the archive file that is created might be named as follows: Citrix_ADM_<ADM_IP_address>_DDMMYY_<time_stamp>.tar.gz
```
1. You can send the technical support files to the support team in two ways:
   a) You can download the file from the ADM GUI to your local storage and then use a web browser to upload to CIS.
   b) You can also upload the technical support files to Citrix Insight Services (CIS) website by running a script on the ADM console.
      i. Using SSH, log on to the ADM console.
      ii. Switch to Shell prompt and type:

```
/mps/collector_upload.pl
```

The full command is given below with the attributes you need to provide:

```
```

The advantage of running the Perl script is that you don’t have to download the technical support file from ADM to your local system and then upload it to CIS. As an option, you can upload the file to CIS directly by using a proxy from ADM console.

Ensure that you have an account on CIS. You can use your Citrix account credentials to upload files to CIS.

What if you don’t have a proxy server? Or what if you are facing some issues with SSL forward proxies? (This can happen if the Perl script does not trust the proxy server’s root certificate.) You can still upload the file directly from ADM shell to CIS.

Note

You can still download the file and email them to the Citrix technical support team in a situation where ADM fails to upload the file to CIS from the console. Or, you can download the file from ADM to your local storage and then use a web browser to upload to CIS.

**Diagnose and troubleshoot Citrix ADC instances**

August 1, 2019

Applications deployed in an enterprise network runs on thousands of backend servers in a large infrastructure, and the traffic sent to these servers pass through the virtual servers configured in the Citrix Application Delivery Controller (ADC) instances and are monitored by using virtual servers. Also, each
of the virtual servers are bound to multiple services representing the backend servers. As the infrastructure size gets larger, it becomes difficult to track the problems associated with the huge amount of traffic received on the servers and narrow down on the required troubleshooting.

With **Citrix ADM Diagnostics and Troubleshooting**, you can diagnose Citrix ADC instances with the problem associated to the virtual servers configured such as the state of the virtual servers, state of the services, AppFlow configuration.

**Note**

Citrix SD WAN and Citrix Gateway instances are not supported.

**To diagnose a Citrix ADC instance:**

1. Login to Citrix ADM using administrator credentials.
2. Navigate to **System > Diagnostics > Troubleshooting**.
3. In the **Select Citrix ADC** field, select the Citrix ADC instance from the available instances, and click **Select**.

   **Note**

   You can also use the search option to search for a Citrix ADC instance discovered in Citrix ADM.

4. Click **Diagnose**.

   AppFlow Configuration on Citrix ADC are listed down. Also, virtual servers are grouped according to their type, and corresponding issues regarding them are displayed.
You can further drill-down to see the problems related to the virtual servers.
Back up and restore a Citrix ADM configuration in an HA pair

August 1, 2019

You can back up the current configuration of a Citrix Application Delivery Management (ADM). In an HA deployment of Citrix ADM, you can back up and restore the Citrix ADM configuration from either one of the servers. If you are using a load balancing virtual server IP address to take the backup, the backup file can be stored on either server and must be checked manually.

If you restore when only one node is active, or when restoring if a fail over happens, the restore process fails to complete.

**To back up a Citrix ADM configuration:**

1. Navigate to System > Advanced Settings > Backup Files, and then click **Back Up**.
2. To encrypt the backup file, select the **Password Protect file** checkbox.

**To restore a Citrix ADM configuration from a backup file:**

1. Navigate to System > Advanced Settings > Backup Files.
2. Select the backup file that you want to restore, and then click **Restore**.

**To configure system backup settings:**

1. Navigate to System > System Administration. Under **Backup Settings**, click **System Backup Settings**.
2. On the **Configure System Backup Settings** page, specify the following:
   - Number of backups to retain. You can only retain up to 10 backups.
   - Encrypt the backup file.
   - Enable external transfer. 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 file to the Citrix ADM server and then perform the restore operation. Specify the server, username, password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see **Transfer a Citrix ADM Backup File to an External System**.
3. Click **OK**.
Configure a cipher group

August 1, 2019

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the Citrix Application Delivery Controller (ADC) instance. A cipher suite comprises a protocol, a key exchange (Kx) algorithm, an authentication (Au) algorithm, an encryption (Enc) algorithm, and a message authentication code (Mac) algorithm.

To add a cipher group on Citrix ADM:

1. Navigate to System > Cipher Groups, and then click Add.
2. On the Create Cipher Group page, enter the following details:
   - Group Name - Name for the cipher group.
   - Cipher Group Description – Provide a description for your cipher group.
   - Cipher Suites – Click Add to select cipher suites from the Available list, and then move the selected (or all) cipher suites to the Configured list.
3. Click Create.
Whenever an abnormal condition occurs on the Citrix ADM, an SNMP trap is generated. The traps are then sent to a remote device called a trap destination server or the SNMP trap destination. You can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

To create an SNMP trap destination on Citrix ADM:

1. Navigate to System > SNMP > Trap Destinations.
2. Under SNMP Traps, click Add to create an SNMP trap, and then specify the following details:
   - Version. Select the SNMP version to use.
   - Destination Server. Name or IP address of the trap destination.
   - Port. Enter the trap destination's port. The port is set to 162 by default.
   - Community. Specify the community string to use when sending a trap to the trap listener.
3. Click Create.

Note
If you are creating an SNMP v3 trap destination, specify the SNMP user credentials to which
you want to bind the trap. To add an SNMP user credential, click Insert and then add the user from the list of SNMP users available.

**To create an SNMP manager community:**

1. Navigate to System > SNMP > Managers.
2. Under SNMP Manager, click Add to create an SNMP manager community, and then specify the following details:
   - **SNMP Manager.** Enter the name or IP address of the SNMP manager.
   - **Community.** Specify the community string to use when sending traps to the trap listener.
3. Optionally, you can select the Enable Management Network check box to specify the Netmask which is the subnet mask of the SNMP manager network.
4. Click Create.

**To create an SNMP user:**

1. Navigate to System > SNMP > Users.
2. Under SNMP User, click Add.
3. Enter the user name and assign a security level to the user from the menu.
4. Based on the security level you’ve assigned to the user, provide extra authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.

### Configure and view system alarms

**August 1, 2019**

You can enable and configure a set of Alarms to monitor the health of your Citrix Application Delivery Management (ADM) servers. You should configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, loginFailure), a message is recorded in the system and you can view the message as syslog message. You can further set notifications to receive an email or SMS corresponding to your alarm settings.

You can assign or modify the severity of an alarm. The severity levels that you can assign are Critical, Major, Minor, Warning, and Informational.
Consider a scenario where you want to monitor whenever there is a failed back up attempt. You can enable the backupFailed alarm and assign a severity, such as Major, to it. Whenever Citrix ADM attempts to back up the system files and when the attempt fails, an alarm is triggered. You can view the message on the Citrix ADM or get notifications through email or SMS.

To configure the alarm, you must select the backupFailed alarm and specify the severity level as Major. The alarm is enabled by default.

**To configure and view a system alarm by using Citrix ADM:**

1. Navigate to **System > Alarms**.

2. Select the alarm you want to configure (for example, backupFailed) and click **Edit** to modify its settings.

3. The alarm is enabled by default. Assign a severity level (example: Major), and then click **OK**.

**Note**

For a few alarms, you cannot set a threshold.

When the alarm is triggered, you can view the generated event as a syslog message.

**To view the event generated by the backupFailed alarm by using Citrix ADM:**

1. Navigate to **System > Auditing**.

2. In the **Auditing** page, under **Audit Messages**, select **Syslog Messages**.

3. In the search field, type in the name of the alarm.

   In this example, you can see that an event was generated for a failed back up attempt.

You can also set notifications to send you either an email or an SMS (Short Message Service) text when an alarm is triggered. For information about how to configure system notifications, see
Citrix ADM as an API proxy server

August 1, 2019

In addition to being able to receive NITRO REST API requests for its own management and analytics functionality, Citrix Application Delivery Management (Citrix ADM) can function as a REST API proxy server for its managed instances. Instead of sending API requests directly to the managed instances, REST API clients can send the API requests to Citrix ADM. Citrix ADM can differentiate between the API requests to which it must respond and the API requests that it must forward unchanged to a managed instance.

As an API proxy server, Citrix ADM provides you with the following benefits:

- **Validation of API requests.** Citrix ADM validates all API requests against configured security and role-based access control (RBAC) policies. Citrix ADM is also tenant-aware and ensures that API activity does not cross tenant boundaries.
- **Centralized auditing.** Citrix ADM maintains an audit log of all API activity related to its managed instances.
- **Session management.** Citrix ADM frees API clients from the task of having to maintain sessions with managed instances.

**How Citrix ADM Works as an API Proxy Server**

When you want Citrix ADM to forward a request to a managed instance, you configure the API client to include any one of the following HTTP headers in the API request:

- `_MPS_API_PROXY_MANAGED_INSTANCE_NAME`. Name of the managed instance.
- `_MPS_API_PROXY_MANAGED_INSTANCE_IP`. IP address of the managed instance.
- `_MPS_API_PROXY_MANAGED_INSTANCE_ID`. ID of the managed instance.

The presence of any of these HTTP headers helps Citrix ADM identify an API request as one that it must forward to a managed instance. The value of the header helps Citrix ADM identify the managed instance to which it must forward the request.

This flow is depicted in the following figure:
As shown in the above figure, when one of these HTTP headers appears in a request, Citrix ADM processes the request as follows:

1. Without modifying the request, Citrix ADM forwards the request to the instance API proxy engine.
2. The instance API proxy engine forwards the API request to a validator and logs the details of the API request in the audit log.
3. The validator ensures that the request does not violate configured security policies, RBAC policies, tenancy boundaries, and so on. It performs additional checks, such as a check to determine whether the managed instance is available.

If the API request is valid and can be forwarded to the managed instance, Citrix ADM identifies a session that is maintained by the instance session manager and then sends the request to the managed instance.

**How to Use Citrix ADM as an API Proxy Server**

The following examples show REST API requests that an API client sends to a Citrix ADM server that has an IP address of 192.0.2.5. Citrix ADM is required to forward the requests, unchanged, to a managed instance with IP address 192.0.2.10. All examples use the _MPS_API_PROXY_MANAGED_INSTANCE_IP header.

Before sending Citrix ADM the API requests, the API client must log in to Citrix ADM, obtain a session ID, and include the session ID in subsequent API requests. The logon API request is of the following
form:

```plaintext
POST /nitro/v1/config/login HTTP/1.1
Host: 192.0.2.5
Cache-Control: no-cache

{  
  "login": 
    {  
      "username": "nsroot",
      "password": "nsroot"
    }
}
```

Citrix ADM responds to the logon request with a response that includes the session ID. The following sample response body shows a session ID:

```plaintext
{  
  "errorcode": 0,
  "message": "Done",
  "operation": "add",
  "resourceType": "login",
  "username": "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*",
  "tenant\_name": "Owner",
  "resourceName": "nsroot",
  "login": [  
    {  
      "tenant\_name": "Owner",
      "permission": "superuser",
    }
  ]
}
```
Example 1: Retrieve Load Balancing Virtual Server Statistics

The client must send Citrix ADM an API request of the following form:

```
GET /nitro/v1/stat/lbvserver HTTP/1.1
Host: 192.0.2.5
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: #
    D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
Content-type: application/json
Cache-Control: no-cache
```
Example 2: Create a Load Balancing Virtual Server

The client must send Citrix ADM an API request of the following form:

```plaintext
POST /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
Host: 192.0.2.5
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
Content-type: application/vnd.com.citrix.netscaler.lbvserver+json
Accept-type: application/vnd.com.citrix.netscaler.lbvserver+json
Cache-Control: no-cache
{
   "lbvserver":{
      "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","port":80
   }
}
```

Example 3: Modify a Load Balancing Virtual Server

The client must send Citrix ADM an API request of the following form:

```plaintext
PUT /nitro/v1/config/lbvserver HTTP/1.1
Host: 192.0.2.5
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
Content-type: application/vnd.com.citrix.netscaler.lbvserver+json
Accept-type: application/vnd.com.citrix.netscaler.lbvserver+json
Cache-Control: no-cache
{
   "lbvserver":{
      "name":"sample_lbvserver","appflowlog":"DISABLED"
   }
}
```

Example 4: Delete a Load Balancing Virtual Server

The client must send Citrix ADM an API request of the following form:

```plaintext
DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
Host: 192.0.2.5
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Autoscaling of Citrix ADC in AWS using Citrix ADM

August 1, 2019

Efficient hosting of applications in a cloud involves easy and cost-effective management of resources depending on the application demand. For example, consider that you have an e-commerce web portal running on AWS. This portal sometimes offers enormous discounts during which there is a spike in the application traffic. When application traffic increases during these offers, the applications must be scaled out dynamically and accordingly network resources might also need to be increased.

The Citrix ADM autoscaling feature supports provisioning and autoscaling of Citrix ADC instances in AWS. The Citrix ADM autoscaling feature constantly monitors the threshold parameters such as memory usage, CPU usage, and throughput. You can select one of these parameters or more than one parameter for monitoring. These parameter values are then compared to the user configured values. If the parameter values breach the limits, then scale-out or scale-in is triggered accordingly.

The Citrix ADM autoscale feature architecture is designed in such a way that you can configure the minimum and maximum number of instances for each of the autoscale group. Pre-setting these numbers ensures that your application is always up and running.

Benefits of autoscaling

High availability of applications. Autoscaling ensures that your application always has the right number of Citrix ADC VPX instances to handle the traffic demands. This is to ensure that your application is up and running all the time irrespective of traffic demands.

Smart scaling decisions and zero touch configuration. Autoscaling continuously monitors your application and adds or removes Citrix ADC instances dynamically depending on the demand. When demand spikes upward, the instances are automatically added. When the demand spikes downward, the instances are automatically removed. The addition and removal of Citrix ADC instances happens automatically making it a zero-touch manual configuration.

Automatic DNS management. The Citrix ADM autoscale feature offers automatic DNS management. Whenever new Citrix ADC instances are added, the domain names are updated automatically.

Graceful connection termination. During a scale-in, the Citrix ADC instances are gracefully removed avoiding the loss of client connections.
**Better cost management.** Autoscaling dynamically increases or decreases Citrix ADC instances as needed. This enables you to optimize the costs involved. You save money by launching instances only when they are needed and terminate them when they are not needed. Thus, you pay only for the resources you use.

**Observability.** Observability is key to application dev-ops or IT personnel to monitor the health of the application. The Citrix ADM’s autoscale dashboard enables you to visualize the threshold parameter values, autoscale trigger time stamps, events, and the instances participating in autoscale.

**Supportability**

Currently, autoscale feature is supported only for AWS deployments.

**Licensing requirements**

- Citrix ADCs provisioned by Citrix ADM use AWS subscription licenses.
- Enterprise or Platinum ADC licenses are used for licensing Citrix ADC instances created as part of Citrix autoscale group. Citrix ADC clustering feature is part of Enterprise or Platinum ADC licenses.

**AWS terminology**

The following table provides a brief description of some of the autoscaling terms used in this document.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS auto scaling group</td>
<td>AWS auto scaling group is a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management.</td>
</tr>
<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>Terminology</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elastic IP (EIP) addresses</td>
<td>An Elastic IP address is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with any instance or network interface for any VPC in your account.</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>
<tr>
<td>Instance type</td>
<td>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.</td>
</tr>
<tr>
<td>Identity and Access Management (IAM) role</td>
<td>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.</td>
</tr>
<tr>
<td>IAM-instance-profile</td>
<td>An identity provided to the Citrix ADC instances provisioned in a cluster in AWS. The profile allows the instances to access AWS services when it starts to load balance the client requests.</td>
</tr>
<tr>
<td>Listener</td>
<td>A listener is a process that checks for connection requests, using the protocol and port that you configure. The rules that you define for a listener determine how the load balancer routes requests to the targets in one or more target groups.</td>
</tr>
<tr>
<td>NLB</td>
<td>Network load balancer. NLB is an L4 load balancer available in the AWS environment.</td>
</tr>
<tr>
<td>Route 53</td>
<td>Route 53 is Amazon's highly available and scalable cloud domain name system (DNS) web service.</td>
</tr>
</tbody>
</table>
### Terminology Description

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security groups</td>
<td>A named set of allowed inbound network connections for an instance.</td>
</tr>
<tr>
<td>Subnets</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Citrix ADC VPX autoscale terminology

The following table provides a brief description of some of the Citrix ADC VPX autoscaling terms used in this document.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoscale groups</td>
<td>Autoscale group is a group of Citrix ADC instances that load balance applications as a single entity and trigger autoscaling when the threshold parameters breach the limits. Citrix ADC instances scale-out or scale-in dynamically based on the autoscale groups configuration. <strong>Note</strong> Citrix autoscale group is called autoscale group throughout this document whereas the AWS autoscale group is explicitly called AWS autoscale group.</td>
</tr>
<tr>
<td>Citrix ADC clusters</td>
<td>A Citrix ADC cluster is a group of Citrix ADC VPX instances and each instance is called a node. The client traffic is distributed across the nodes to provide high availability, high throughput, and scalability.</td>
</tr>
</tbody>
</table>
### Terminology Description

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drain connection timeout</td>
<td>During scale-in, once an instance is selected for deprovisioning, Citrix ADM removes the instance from processing new connections to autoscale group and waits until the specified drain connection timeout period expires before deprovisioning. This allows existing connections to this instance be drained out before it gets deprovisioned. If the connections are drained before the drain connection timeout expires, even then the Citrix ADM waits for the drain connection timeout period to expire before starting a new evaluation. <strong>Note</strong> If the connections are not drained even after the drain connection timeout expires, the Citrix ADM removes the instances which might impact the application. Default value is 5 minutes and is configurable.</td>
</tr>
<tr>
<td>Cooldown period</td>
<td>After a scale-out, cooldown period is the time for which evaluation of the statistics has to be stopped. This ensures organic growing of an autoscale group by allowing current traffic to stabilize and average out on the current set of instances before the next scaling decision is made. Default cooldown period value is 10 minutes and is configurable. <strong>Note</strong> Default value is determined based on the time required for the system to stabilize after a scale-out (approximately 4 minutes) plus Citrix ADC configuration and DNS advertisement time.</td>
</tr>
</tbody>
</table>
## Terminology Description

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tags</strong></td>
<td>Each autoscale group is assigned a tag which is a key and value pair. You can apply tags to the resources that enable you to organize and identify resources easily. The tags are applied to both AWS and Citrix ADM. <strong>Example:</strong> Key= name, Value = webserver. It is recommended to use a consistent set of tags to easily track the autoscale groups that might belong to various groups such as development, production, testing.</td>
</tr>
<tr>
<td><strong>Threshold parameters</strong></td>
<td>Parameters that are monitored for triggering scale-out or scale-in. The parameters are CPU usage, memory usage, and throughput. You can select one parameter or more than one parameter for monitoring.</td>
</tr>
<tr>
<td><strong>Time to Live (TTL)</strong></td>
<td>Specifies the time interval that the DNS resource record may be cached before the source of the information should again be consulted. Default TTL value is 30 seconds and is configurable.</td>
</tr>
<tr>
<td><strong>Watch time</strong></td>
<td>The time for which the scale parameter's threshold has to stay breached for a scaling to happen. If the threshold is breached on all the samples collected in this specified time then a scaling happens. If the threshold parameters remain at a value higher than the maximum threshold value throughout this duration, a scale-out is triggered. If the threshold parameters operate at a value lower than the minimum threshold value, a scale-in is triggered. Default value is 3 minutes and is configurable.</td>
</tr>
</tbody>
</table>
Architecture

August 1, 2019

The following diagram illustrates the architecture of the autoscaling feature with DNS as the traffic distributor.

The following diagram illustrates the architecture of the autoscaling feature with NLB as the traffic distributor.

Citrix Application Delivery Management (ADM)

Citrix Application Delivery Management is a web-based solution for managing all Citrix ADC deployments that are deployed on-premises or on the cloud.

You can use this cloud solution to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified, and centralized cloud-based console. Citrix Application Delivery Management (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.

The autoscale groups are created in Citrix ADM and the Citrix ADC VPX instances are provisioned from Citrix ADM. The application is then deployed through StyleBooks in Citrix ADM.

Traffic distributors (NLB or DNS/Route53)

NLB or DNS/Route53 is used to distribute traffic across all the nodes in an autoscale group. See Autoscale traffic distribution modes for more information.

The Citrix ADM communicates with the traffic distributor to update the application domain and IP addresses of the load balancing virtual servers that frontend the application.

Citrix ADM autoscale group

Autoscale group is a group of Citrix ADC instances that load balance applications as a single entity and trigger autoscaling based on the configured threshold parameter values.

Citrix ADC clusters

A Citrix ADC cluster is a group of Citrix ADC VPX instances and each instance is called a node. The client traffic is distributed across the nodes to provide high availability, high throughput, and scalability.
Note

- Autoscaling decisions are made at the cluster level and not at the node level.
- Independent clusters are hosted in different availability zones and therefore support for some of the shared state features are limited.

Persistence sessions such as source IP persistence and others except cookie based persistence cannot be shared across clusters. However, all the stateless features like load balancing methods work as expected across the multiple availability zones.

AWS auto scaling groups

AWS auto scaling group is a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management.

AWS availability zones

AWS availability zone is an isolated location inside a region. Each region is made up of several availability zones. Each availability zone belongs to a single region.

Traffic distribution modes

As you move your application deployment to cloud, autoscaling becomes a part of the infrastructure. As the applications scale-out or scale-in using autoscaling, these changes must be propagated to the client. This propagation is achieved using DNS based or NLB based autoscaling.

NLB based autoscaling

In NLB-based deployment mode, the distribution tier to the cluster nodes is the AWS network load balancer.

In NLB based autoscaling, only one static IP address is offered per availability zone. This is the public IP address that is added to route53 and the backend IP addresses can be private. With this public IP address, any new Citrix ADC instance provisioned during autoscaling operates using private IP addresses and does not require additional public IP addresses.

NLB supports only TCP-based load balancing. If you want to support UDP traffic, you can choose DNS based autoscaling.
DNS based autoscaling

In DNS based autoscaling, DNS acts as the distribution layer to the Citrix ADC cluster nodes. The scaling changes are propagated to the client by updating the domain name corresponding to the application. Currently, the DNS provider is AWS Route53.

**Note**

In DNS based autoscaling, each Citrix ADC instance requires a public IP address.

How autoscaling works

The following flowchart illustrates the autoscaling workflow.

The Citrix ADM collects statistics (CPU usage, memory usage, throughput) from the autoscale provisioned clusters at a time interval of one minute.

The statistics are evaluated against the configuration thresholds. Depending on whether the statistics exceed the maximum threshold or are operating below the minimum threshold, scale-out or scale-in is triggered respectively.

- If a scale-out is triggered;
  - New nodes are provisioned.
  - The nodes are attached to the cluster and the configuration is synchronized from the cluster to the new node.
  - The nodes are registered with Citrix ADM.
  - The new node IP addresses are updated in DNS/NLB.

When the application is deployed, IPset is created on clusters in each availability zone and the domain and the instance IP addresses are registered with DNS/NLB.

- If a scale-in is triggered;
  - The IP addresses of the nodes identified for removal are removed.
  - The nodes are detached from the cluster, deprovisioned and then deregistered from Citrix ADM.

When the application is removed, the domain and the instance IP addresses are deregistered from DNS/NLB and the IPset is deleted.

Example

Consider that you have created an autoscale group named asg_arn in a single availability zone with the following configuration.

- Threshold parameter – Memory usage
Citrix Application Delivery Management 12.1

- Minimum limit: 40
- Maximum limit: 85
- Watch time – 3 minutes
- Cooldown period – 10 minutes
- Drain connection timeout – 10 minutes
- TTL timeout – 60 seconds

After the autoscale group is created, statistics are collected from the autoscale group. The autoscale policy also evaluates if any an autoscale event is in progress and if an autoscaling is in progress, waits for that event to complete before collecting the statistics.

**Sequence of events:**

- **T1 and T2:** Memory usage exceeds the maximum threshold limit.
- **T3:** Memory usage is below the maximum threshold limits.
- **T6, T5, T4:** Memory usage has breached the maximum threshold limit consecutively for three watch time durations.
  - A scale-out is triggered.
  - Provisioning of nodes occur.
  - Cooldown period is in effect.
- **T7 – T16:** Autoscale evaluation is skipped for this availability zone from T7 through T16 as the cooldown period is in effect.
- **T18, T19, T20:** Memory usage has breached the minimum threshold limit consecutively for three watch time durations.
  - Scale-in is triggered.
  - Drain connection timeout is in effect.
  - IP addresses are relieved from the DNS/NLB.
- **T21 – T30:** Autoscale evaluation is skipped for this availability zone from T21 through T30 as the drain connection timeout is in effect.
- **T31**
  - For DNS based autoscaling, TTL is in effect.
  - For NLB based autoscaling, deprovisioning of the instances occurs.
- **T32**
  - For NLB based autoscaling, evaluation of the statistics starts.
  - For DNS based autoscaling, deprovisioning of the instances occurs.
- **T33:** For DNS based autoscaling, evaluation of the statistics starts.
Autoscale configuration

August 1, 2019

To start autoscaling of Citrix ADC VPX instances in AWS, you must complete the following steps:

1. Complete all the pre-requisites on AWS
2. Complete all the pre-requisites on Citrix ADM
3. Create autoscale groups
   a) Initialize autoscale configuration
   b) Configure autoscale parameters
   c) Configure provision parameters
4. Deploy the application

Pre-requisites for AWS

You must ensure that you have completed all the pre-requisites on the AWS to use the autoscale feature. This document assumes that you already possess an AWS account.

The next few sections assist you in performing all the necessary tasks in AWS before you create autoscale groups in Citrix ADM. The tasks that you must complete are as follows:

1. Subscribe to the required Citrix ADC VPX instance on AWS.
2. Create the required VPC or select an existing VPC.
3. Define the corresponding subnets and security groups.
4. Create two IAM roles, one for Citrix ADM and one for Citrix ADC VPX instance.
5. Create a user for Citrix ADM and assign the role created for Citrix ADM to the user.
6. Generate the Access Key ID and Secure Access Key for the user.

For more information on how to create VPC, subnet and security groups, refer AWS documentation.

Subscribe to Citrix ADC VPX license in AWS

1. Go to aws marketplace.
2. Log on with your credentials.
3. Search for Citrix ADC VPX platinum or enterprise edition.
Create subnets

Create three subnets in your VPC - one each for the management, client, and server connections. 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 each of the availability zones where servers are present.

- **Management.** Existing subnet in your Virtual Private Cloud (VPC) dedicated for management. Citrix ADC needs to contact AWS services and requires internet access. Configure a NAT gateway and add a route table entry to allow internet access from this subnet.

- **Client.** Existing subnet in your Virtual Private Cloud (VPC) dedicated for client side. Typically, Citrix ADC receives client traffic for the application via a public subnet from the internet. Associate the client subnet with a route table which has a route to an Internet gateway. This will allow Citrix ADC to receive application traffic from the internet.

- **Server.** A server subnet where the application servers are provisioned. All your application servers will be present in this subnet and will be receiving application traffic from the Citrix ADC through this subnet.

Create security groups

Create a security group to control inbound and outbound traffic in the Citrix ADC VPX instance. Create rules for both incoming and outgoing traffic that you want to control in the Citrix autoscale groups. You can add as many rules as you want.

- **Management.** Existing security group in your account dedicated for management of Citrix ADC VPX. Inbound rules should be allowed on the following TCP and UDP ports.
  - TCP: 80, 22, 443, 3008-3011, 4001
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000
  Ensure that the security group allows the Citrix ADM agent to be able to access the VPX.

- **Client.** Existing security group in your account dedicated for client side communication of Citrix ADC VPX instances. Typically, inbound rules are allowed on the TCP ports 80, 22, and 443.

- **Server.** Existing security group in your account dedicated for server-side communication of Citrix ADC VPX.

Create IAM roles

Along with creating an IAM role and defining a policy, you must also create an instance profile in AWS. IAM roles allow Citrix ADM to provision Citrix ADC instance, create or delete Route53 entries.
While roles define “what can I do?” they do not define “who am I?” AWS EC2 uses an instance profile as a container for an IAM role. An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts.

When you create an IAM role using the console, the console creates an instance profile automatically and gives it the same name as the role it corresponds to. Roles provide a mechanism to define a collection of permissions. An IAM user represents a person and an instance profile represents the EC2 instances. If a user has role “A,” and an instance has an instance profile attached to “A,” these two principals can access the same resources in the same way.

**Note**

Ensure that the role names start with “Citrix-ADM-” and the instance profile name starts with “Citrix-ADC-.”

**To create an IAM role for Citrix ADM**

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.

3. 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.

4. Click **Permissions**.

5. In **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 for Citrix ADM is provided in the following box:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:UnmonitorInstances"
            ]
        }
    ]
}
```
“ec2:MonitorInstances”,
“ec2:CreateKeyPair”,
“ec2:ResetInstanceAttribute”,
“ec2:ReportInstanceStatus”,
“ec2:DescribeVolumeStatus”,
“ec2:StartInstances”,
“ec2:DescribeVolumes”,
“ec2:UnassignPrivateIpAddresses”,
“ec2:DescribeKeyPairs”,
“ec2:CreateTags”,
“ec2:ResetNetworkInterfaceAttribute”,
“ec2:ModifyNetworkInterfaceAttribute”,
“ec2:DeleteNetworkInterface”,
“ec2:RunInstances”,
“ec2:StopInstances”,
“ec2:AssignPrivateIpAddresses”,
“ec2:DescribeVolumeAttribute”,
“ec2:DescribeInstanceCreditSpecifications”,
“ec2:CreateNetworkInterface”,
“ec2:DescribeImageAttribute”,
“ec2:AssociateAddress”,
“ec2:DescribeSubnets”,
“ec2:DeleteKeyPair”,
“ec2:DisassociateAddress”,
“ec2:DescribeAddresses”,
“ec2:DeleteTags”,
“ec2:RunScheduledInstances”,
“ec2:DescribeInstanceAttribute”,
“ec2:DescribeRegions”,
“ec2:DescribeDhcpOptions”,
“ec2:GetConsoleOutput”,
“ec2:DescribeNetworkInterfaces”,
“ec2:DescribeAvailabilityZones”,
“ec2:DescribeNetworkInterfaceAttribute”,
“ec2:ModifyInstanceAttribute”,
“ec2:DescribeInstanceStatus”,
“ec2:ReleaseAddress”,
“ec2:RebootInstances”,
“ec2:TerminateInstances”,

© 1999-2019 Citrix Systems, Inc. All rights reserved.
“ec2:DetachNetworkInterface”，
“ec2:DescribeIamInstanceProfileAssociations”，
“ec2:DescribeTags”，
“ec2:AllocateAddress”，
“ec2:DescribeSecurityGroups”，
“ec2:DescribeHosts”，
“ec2:DescribeImages”，
“ec2:DescribeVpcs”，
“ec2:AttachNetworkInterface”，
“ec2:AssociateIamInstanceProfile"
],
“Resource”: “”
},
{
“Sid”: “VisualEditor1”,
“Effect”: “Allow”,
“Action”: [
“iam:GetRole”,
“iam:PassRole”
],
“Resource”: “”
},
{
“Sid”: “VisualEditor2”,
“Effect”: “Allow”,
“Action”: [
“route53:CreateHostedZone”,
“route53:CreateHealthCheck”,
“route53:GetHostedZone”,
“route53:ChangeResourceRecordSets”,
“route53:ChangeTagsForResource”,
“route53:DeleteHostedZone”,
“route53:DeleteHealthCheck”,
“route53:ListHostedZonesByName”,
“route53:GetHealthCheckCount”
],
“Resource”: “”
}
"Sid": "VisualEditor3",
"Effect": "Allow",
"Action": [  
  "iam:ListInstanceProfiles",
  "iam:ListAttachedRolePolicies",
  "iam:SimulatePrincipalPolicy"
],
"Resource": "*"
],
{
"Sid": "VisualEditor4",
"Effect": "Allow",
"Action": [  
  "ec2:ReleaseAddress",
  "elasticloadbalancing:DeleteLoadBalancer",
  "ec2:DescribeAddresses",
  "elasticloadbalancing:CreateListener",
  "elasticloadbalancing:CreateLoadBalancer",
  "elasticloadbalancing:RegisterTargets",
  "elasticloadbalancing:CreateTargetGroup",
  "elasticloadbalancing:DeregisterTargets",
  "ec2:DescribeSubnets",
  "elasticloadbalancing:DeleteTargetGroup",
  "elasticloadbalancing:ModifyTargetGroupAttributes",
  "ec2:AllocateAddress"
],
"Resource": "*
]}

1. Copy and paste the list of permissions in the JSON tab and click **Review policy**.

2. In **Review policy** page, type a name for the policy, enter a description, and click **Create policy**.

   **Note**

   Ensure that the name starts with “Citrix-ADM-.”

3. In the **Create Role** page, enter the name of the role.
Note
Ensure that the role name starts with “Citrix-ADM-.”

4. Click Create Role.

To create an IAM role for Citrix ADC instances

Similarly, create an IAM role for Citrix ADC. The Citrix ADC can then login to your AWS account and perform the following actions:

- re-assigning management IP address during node failures
- listen to AWS autoscale events of backend servers, and so on.

Attach the policy with permissions provided by Citrix for AWS to access the Citrix ADC instances.

1. In AWS, click Services. In the left side navigation pane, select IAM > Roles, and click Create role.

2. Ensure that you select AWS service > EC2, and then click Permissions to create an instance profile.

3. Click Permissions.

4. In Attach permissions policies page, click Create policy.

5. You can create and edit a policy in the visual editor or by using JSON.

The list of permissions from Citrix for Citrix ADC instances is provided in the following box:

```json
{"Version": "2012-10-17",
 "Statement": [
  {
    "Sid": "VisualEditor0",
    "Effect": "Allow",
```
Register the DNS domain

You must also ensure that you have registered the DNS domain for hosting your applications.

Assess the number of elastics IPs (EIP) required in your network.

The number of EIPs required varies based on whether you are deploying DNS based autoscaling or NLB based autoscaling. To increase the number of EIPs, create a case with AWS.

- For DNS based autoscaling, the number of EIPs required per availability zone is equal to the number of applications multiplied by the maximum number of VPX instances you want to configure in the autoscale groups.
- For NLB based autoscaling, the number of EIPs required is equal to the number of applications multiplied by the number of availability zones in which the applications are getting deployed.

Assess the instance limit requirements

When assessing instance limits, ensure that you consider space requirements for Citrix ADC instances also.

Install Citrix ADM agent on AWS

The Citrix ADM agent works as an intermediary between the Citrix ADM and the discovered instances in the data center or on the cloud. Ensure that you have installed Citrix ADM agent in AWS. Add a route in AWS ADM agent so that ADM can reach the agent after you establish the layer 3 connectivity.

Follow these steps to add a route in the agent installed in AWS:

1. Access the console of the ADM agent installed on AWS.
2. Execute the following command at the prompt:
   
   ```
   route add -net <DMZ network> <gateway to ADM agent>
   ```
   
   For example, “route add -net 10.x.x.0/24 21.1.1.10”
The route is removed after the agent restarts. This behavior is specific to AWS/Azure agent images where network settings are skipped.

For details on how to install the Citrix ADM agent on AWS, see Installing Citrix ADM agent on AWS

Prerequisites for Citrix ADM

You must ensure that you have completed all the pre-requisites on the Citrix ADM to use the autoscale feature.

Create a site

Create a site in Citrix ADM and add the details of the VPC associated with your AWS role.

1. In Citrix ADM, navigate to Networks > 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 Access Key ID that is associated with the role that you have created in AWS.
   c) Type the Secret access Key generated while creating an IAM role for Citrix ADM in AWS.
      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.
   d) Click Create.
6. Again click Create to create the site.

Configure NTP server

Ensure to configure NTP server on Citrix ADM, so that the Citrix ADM clock has the same date and time settings as the Citrix ADCs deployed on AWS.

For more information on how to configure NTP servers, see Configure NTP server.

Configure domain name server

The Citrix ADM requires internet connectivity to connect to the ADC instances deployed on the AWS.

Configure DNS IP address on ADM to allow internet connectivity.
1. In Citrix ADM, navigate to **System > Set Up Citrix ADM**, and select **Network Configuration**.

2. In **Network Configuration** page, enter the IP address of the DNS configured in your network.

3. Click **OK**.

**Configure Layer 3 connectivity**

You need to establish Layer 3 connectivity between Citrix ADM and the ADC VPX instances deployed on the public cloud. To establish the Layer 3 connectivity, you can use solutions such as Citrix Cloud-Bridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN in Azure, or third-party connectors such as Equinix and so on.

For more information on how to create Layer 3 connectivity, see [Add VPX Instances deployed in cloud to Citrix ADM](#).

**Install Citrix ADM agent on AWS**

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

For details on install the Citrix ADM agent on AWS, see [Installing Citrix ADM agent on AWS](#).

**Create autoscale groups**

**Initialize autoscale configuration**

1. In Citrix ADM, navigate to **Networks > AutoScale Groups**.

2. Click **Add** to create autoscale groups. The **Create AutoScale Group** page appears.

3. Enter the following details.

   - **Name**: Type a name for the autoscale group.
   - **Site**: Select the site that you have created to provision the Citrix ADC VPX instances on AWS.
   - **Agent**: Select the Citrix ADM agent that manages the provisioned instances.
   - **Cloud Access Profile**: Select the cloud access profile.

**Note**

If the cloud access profile does not exist in the field, click **Add** to create a profile.

   - Type the ARN associated with the role that you have created in AWS.
   - Type the external ID that you provided while creating an Identity and Access Manage-
ment (IAM) role in AWS. Depending on the cloud access profile that you select, the availability zones are populated.

- **Device Profile.** Select the device profile from the list. The device profile will be used by Citrix ADM whenever it needs to log on to the instance.

- **Traffic Distribution Mode.** The **Load Balancing using NLB** option is selected as default traffic distribution mode. If applications are using UDP traffic, then select **DNS using AWS route53**.

  **Note** After the autoscale configuration is set up, new availability zones cannot be added or existing availability zones cannot be removed.

- **Enable AutoScale Group.** Enable or disable the status of the ASG groups. This option is enabled, by default. If this option is disabled, autoscaling is not triggered.

- **Availability Zones.** Select the zones in which you want to create the autoscale groups. Depending on the cloud access profile that you have selected, availability zones specific to that profile are populated.

- **Tags.** Type the key-value pair for the autoscale group tags. A tag consists of a case-sensitive key-value pair. These tags enable you to organize and identify the autoscale groups easily. The tags are applied to both AWS and Citrix ADM.

4. Click **Next**.

**Configuring autoscale parameters**

1. In the **AutoScale Parameters** tab, enter the following details.
2. Select one or more than one of the following threshold parameters whose values must be monitored to trigger a scale-out or a scale-in.

   - **Enable CPU Usage Threshold:** Monitor the metrics based on the CPU usage.
   - **Enable Memory Usage Threshold:** Monitor the metrics based on the memory usage.
   - **Enable Throughput Threshold:** Monitor the metrics based on the throughput.

   **Note**
   - Default minimum threshold limit is 30 and maximum threshold limit is 70. However, you change modify the limits.
   - Minimum threshold limit must be equal or less than half of the maximum threshold limit.
   - More than one threshold parameters can be selected for monitoring. In such cases, a scale-in is triggered if at least one of the threshold parameters is above the maximum threshold. However, a scale-in is triggered only if all the threshold parameters are operating below their normal thresholds.
- **Minimum Instances.** Select the minimum number of instances that need to be provisioned for this autoscale group.
  - By default, the minimum number of instances is equal to the number of zones selected. You can increment the minimum instances by multiples of number of zones.
  - For example, if the number of availability zones is 4, the minimum instances is 4 by default. You can increase the minimum instances by 8, 12, 16.
- **Maximum Instances.** Select the maximum number of instances that need to be provisioned for this autoscale group.
  - The maximum number of instances must be greater than or equal to the minimum instances value. The maximum number of instances that can be configured is equal to number of availability zones multiplied by 32.
  - Maximum number of instances = number of availability zones * 32
- **Drain Connection Timeout (minutes).** Select the drain connection timeout period. During scale-in, once an instance is selected for deprovisioning, Citrix ADM removes the instance from processing new connections to autoscale group and waits until the specified time expires before deprovisioning. This allows existing connections to this instance to be drained out before it gets deprovisioned.
- **Cooldown period (minutes).** Select the cooldown period. During scale-out, cooldown period is the time for which evaluation of the statistics has to be stopped after a scale-out occurs. This ensures organic growing of instances of an autoscale group by allowing current traffic to stabilize and average out on the current set of instances before the next scaling decision is made.
- **DNS Time To Live(seconds).** Select the amount of time (in seconds) that a packet is set to exist inside a network before being discarded by a router. This parameter is applicable only when the traffic distribution mode is DNS using AWS route53.
- **Watch-Time (minutes).** Select the watch-time duration. The time for which the scale parameter’s threshold has to stay breached for a scaling to happen. If the threshold is breached on all the samples collected in this specified time then a scaling happens.

3. Click **Next**.
Configure provision parameters

1. In the **Provision Parameters** tab, enter the following details.

   - **IAM Role**: Select the IAM role that you have created in AWS. An IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.
   - **Product**: Select the Citrix ADC product version that you want to provision.
   - **Version**: Select the Citrix ADC product release version and build number. The release versions and build numbers are auto-populated based on the product that you have selected.
   - **AWS AMI ID**: Enter the AMI ID specific to the region that you have selected.
   - **Instance Type**: Select the EC2 instance type.

   **Note**
   
   The recommended instance type for the selected product is auto-populated, by default.

   - **Security Groups**: Security groups control the inbound and outbound traffic in the Citrix ADC VPX instance. You create rules for both incoming and outgoing traffic that you want to control. Select appropriate values for the following subnets:

     - group in your account dedicated for management of Citrix ADC VPX instances. Inbound rules should be allowed on the following TCP and UDP ports:

       |   | TCP:     | UDP:  |
       |---|---------|-------|
       | 1 | 80, 22, 443, 3008–3011, 4001 |
       | 2 | 67, 123, 161, 500, 3003, 4500, 7000 |

     Ensure that the security group allows the Citrix ADM agent to be able to access the VPX.

   - **Client**: Existing security group in your account dedicated for client side communication of Citrix ADC VPX instances. Typically, inbound rules are allowed on the TCP ports 80, 22, and 443.

   - **Server**: Existing security group in your account dedicated for server side communication of Citrix ADC VPX.

   - **IP’s in server subnet per node**: Select the number of IP addresses in server subnet per node for the security group.

   - **Zone**: The number of zones that are populated is equal to the number of availability zones that you have selected. For each zone, select the appropriate values for the following subnets:

   - **Management**: Existing subnet in your Virtual Private Cloud (VPC) dedicated for management. Citrix ADC needs to contact AWS services and requires internet access. Configure a NAT gateway and add a route table entry to allow internet access from this subnet.
• **Client.** Existing subnet in your Virtual Private Cloud (VPC) dedicated for client side. Typically, Citrix ADC receives client traffic for the application via a public subnet from the internet. Associate the client subnet with a route table which has a route to an Internet gateway. This will allow Citrix ADC to receive application traffic from the internet.

• **Server.** Application servers are provisioned in a server subnet. All your application servers will be present in this subnet and will be receiving application traffic from the Citrix ADC via this subnet.

2. Click **Finish.**

   A progress window with the status for creating autoscale group appears. It might take several minutes for creation and provisioning of autoscale groups.

### Configure application using Stylebooks

1. In Citrix ADM, navigate to **Networks > Autoscale Groups.**
2. Select the autoscale group that you created and click **Configure.**
3. The **Choose StyleBook** page displays all the StyleBooks available for your use to deploy configurations in the autoscale clusters.
   - Select the appropriate StyleBook. For example, you can use the **HTTP/SSL Loadbalancing StyleBook.** You can also import new StyleBooks.
   - Click on the StyleBook to create the required configuration.
     The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
   - Enter values for all the parameters.
   - If you are creating backend servers in AWS, select Backend Server Configuration. Further select **AWS EC2 Autoscaling > Cloud** and enter the values for all the parameters.
   - There might be a few optional configurations required depending on the StyleBook that you have chosen. For example, you might have to create monitors, provide SSL certificate settings, and so on.
   - Click **Create** to deploy the configuration on the Citrix ADC cluster.

### Note

- The FQDN of application or the virtual server cannot be modified after it is configured and deployed.

  The FQDN of the application is resolved to the IP address using DNS. As this DNS record might be cached across various name servers, changing the FQDN might cause the traffic to be blackholed.

- SSL session sharing work as expected within an availability zone but across availability
zones, requires reauthentication.

SSL sessions are synchronized within the cluster. As the autoscale group spanning across availability zones has separate clusters in each zone, SSL sessions cannot be synchronized across zones.

- Shared limits such as max client and spill-over are set statically based on number of availability zones. This limit has to be set after calculating it manually. Limit = \( \frac{\text{Limit required}}{\text{number of Zones}} \).

Shared limits are distributed automatically across nodes within a cluster. As the autoscale group spanning across availability zones has separate clusters in each zone, these limits have to be calculated manually.

**Upgrade Citrix ADC clusters**

You must manually upgrade the cluster nodes. You first upgrade the image of existing nodes and then update AMI from the Citrix ADM.

**Important**

Ensure the following during an upgrade:

- No scale-in or scale-out is triggered.
- No configuration changes must be performed on the cluster in the autoscale group.
- You keep a backup of ns.conf file of the previous version. In case an upgrade fails, you can fall back to the previous version.

Perform the following steps to upgrade the Citrix ADC cluster nodes.

1. Disable the autoscale group on the MAS ASG portal.
2. Select one of the clusters within the autoscale groups for upgrade.
3. Follow the steps documented in the topic Upgrading or downgrading the Citrix ADC cluster.

**Note**

- Upgrade one node in the cluster.
- Monitor the application traffic for any failures.
- If you encounter any issues or failures, downgrade the node that was previously upgraded. Else, continue with the upgrade of all nodes.

4. Continue upgrading the nodes in all the clusters in the autoscale group.

**Note**

If the upgrade for any cluster fails, downgrade all the clusters in the autoscale group to the
previous version. Follow the steps documented in the topic *Upgrading or downgrading the Citrix ADC cluster*.

5. After successful upgrade of all clusters, update AMI on MAS ASG Portal. AMI must be of the same version as the image used for the upgrade.

6. Edit the autoscale group and type the AMI that corresponds to the upgraded version.

7. Enable the autoscale group on the ADM portal.

**Modify autoscale groups configuration**

- You can modify an autoscale group configuration or delete an autoscale group. You can modify only the following autoscale group parameters.
  - Traffic distribution mode
  - Maximum and minimum limits of the threshold parameters
  - Minimum and maximum instance values
  - Drain connection period value
  - Cooldown period value
  - Time to live value – If the traffic distribution mode is DNS
  - Watch duration value

- You can also delete the autoscale groups after they are created.

  When you delete an autoscale group, all the domains and IP addresses are deregistered from DNS/NLB and the cluster nodes are deprovisioned.

**Dashboard**

**August 1, 2019**

1. In Citrix ADM, navigate to *Networks > Autoscale Groups*.

2. Select the autoscale group and click *Dashboard*.

   You can view the graph for the selected monitoring parameters. The right-side panel displays the events that trigger the autoscaling. The left-side panel displays the active nodes in the cluster per zone and the events.

   The following figure displays a sample dashboard.

The following figure displays a portion of the autoscale dashboard.
FAQs

August 1, 2019

This section provides the FAQ on the following Citrix Application Delivery Management (Citrix ADM) features. Click a feature name in the following table to view the list of FAQs for that feature.

<table>
<thead>
<tr>
<th>Analytics</th>
<th>Authentication</th>
<th>Configuration Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Management</td>
<td>Deployment</td>
<td>Deployment (Disaster recovery)</td>
</tr>
<tr>
<td>Event Management</td>
<td>Instance Management</td>
<td>Stylebooks</td>
</tr>
<tr>
<td>System Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Analytics**

**Should I enable EUEM virtual channel on Citrix Gateway instances deployed in single-hop mode?**

EUEM virtual channel data is part of HDX Insight data that the Citrix ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on Citrix ADM.

EUEM virtual channel is a default service running on Citrix Virtual Desktop applications (VDA). If it is not running, start the “Citrix End User Experience Monitoring” process in VDA services.

**How do I enable Citrix ADM to monitor web-application and virtual-desktop traffic?**

1. Navigate to **Infrastructure > Instances**, and select the Citrix Application Delivery Controller (Citrix ADC) instance on which you want to enable analytics.
2. Select **Enable/Disable Insight** from the **Action** drop-down list.
3. In the **Configure Insight** page that opens, select all the virtual servers on which you want to enable analytics, and click **Enable AppFlow**. For more details, see How to Enable Analytics on Instances.

**Note**

For Citrix ADC instances of 11.0 release, 65.30 build and later, there is no option on Citrix ADM to enable Security Insight explicitly. Ensure that you configure the AppFlow parameters on the
Citrix ADC instances, so that Citrix ADM starts receiving the Security Insight traffic along with the Web Insight traffic. For more information on how to set the AppFlow parameters on Citrix ADC instances, see To set the AppFlow parameters by using the configuration utility.

After I add the Citrix ADC instances, does Citrix ADM automatically start collecting analytical information?

No. You must first enable analytics on the virtual servers hosted in Citrix ADC instances that are managed by Citrix ADM. For more details, see How to Enable Analytics on Instances.

Should I access the individual Citrix ADC appliance for enabling analytics?

No. All configuration is done from the Citrix ADM user interface, which lists the virtual servers hosted on the specific Citrix ADC instance. For more details, see How to Enable Analytics on Instances.

What are the types of virtual servers that can be listed on a Citrix ADC instance to enable analytics?

Currently, the Citrix ADM user interface lists the following virtual servers for enabling analytics:

- Load balancing virtual server
- Content switching virtual server
- VPN virtual server
- Cache redirection virtual server

How do I attach an additional disk to Citrix ADM?

To attach an additional disk to Citrix ADM:

1. Shut down the Citrix ADM virtual machine.
2. In the hypervisor, attach an additional disk of the required disk size to Citrix ADM virtual machine.

   For example, Let us consider that you want to increase the disk space to 200 GB, in a Citrix ADM virtual machine of 120 GB. In this scenario, you need to attach a disk space of 200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, Citrix ADM log files. The existing 120 GB disk space will be used to store core files, Operating system log files, and so on.
3. Start the Citrix ADM virtual machine.
What do you mean by collectors are not configured on Citrix ADC instances?

A collector receives AppFlow records generated by the Citrix ADC appliance. Citrix ADM receives Security Insight and Web Insight traffic from the Citrix ADC instances when the AppFlow feature is enabled. When you enable the AppFlow feature on a Citrix ADC instance, you must specify at least one collector to which the AppFlow records are sent. If the collectors are not configured on the Citrix ADC instances, Citrix ADM does not receive the traffic from the instances.

For example, five Citrix ADC instances are added to Citrix ADM. If collectors are not specified for two instances, no traffic flows to Citrix ADM. Self-service diagnostics detects the issue and displays the issue as “Collectors are not configured on 2 instances.”

For more information about how to configure the AppFlow Feature, see Configuring the AppFlow Feature.

Authentication

What is load balancing of authentication requests?

The authentication-server load balancing feature enables Citrix ADM to load balance the authentication requests that are directed to the external authentication servers. Load balancing the authentication servers ensures that the authentication load is split across multiple authentication servers and thus avoid an authentication server from being overloaded. You can create an authentication service to connect with and get user information from your existing external authentication server using the authentication protocols like LDAP, RADIUS, or TACACS.

Why do we need to cascade external authentication servers?

Cascaded external authentication servers provide uninterrupted authentication processing, allowing access to legitimate users if an authentication server fails. There is no limitation on which types of authentication servers you can cascade. You can have all RADIUS servers, or all LDAP servers, or a combination of RADIUS and LDAP servers.

How many external authentication servers can I cascade?

You can cascade up to 32 external authentication servers in Citrix ADM.
Do I have an alternative when external authentication fails?

There can be a situation when external authentication completely fails, even when you have cascaded a number of servers. For example, the external servers could become unreachable, or a new user’s credentials might not have been entered in any of the external authentication servers. To prevent locking users out in such a situation, you can enable fallback local authentication. For more details, see Fallback Local Authentication.

What is fallback local authentication?

Fallback local authentication is an option to authenticate your users locally when external authentication fails. If external authentication fails, Citrix ADM accesses the local user database to authenticate your users.

In Citrix ADM, navigate to System > Authentication > Authentication Configuration. On this page, you can add multiple external authentication servers in a cascade, and you can select the Enable fallback local authentication option.

What is extraction of external user groups?

If you have added external servers for authenticating the users, you can import (extract) existing user groups into Citrix ADM. You have to import user groups once and provide a group permission to a user group rather than importing individual users and giving them individual permissions. You do not have to recreate the users on Citrix ADM.

Why do we need to assign group permissions?

When you are using the load balancing feature of Citrix ADC, you can integrate Citrix ADM with external authentication servers, and import user group information from the authentication servers. Log in to Citrix ADM and manually create same group information in Citrix ADM and assign permission to those groups. The user and user group permission is managed in Citrix ADM and not in the external server. The users have different role-based access permissions on the external servers. Configure the same permissions for the users in Citrix ADM also. Instead of configuring permissions individually for each user, you can configure a group-level permission so that the user-group members can access specific services on the load balanced virtual servers. The typical permissions that you can assign are permissions to manage Citrix ADC instances, Citrix SDX instances, virtual servers, and so on, so that the users of that group can manage only those instances or virtual servers. You can later edit the permissions given to the users at the group level. You can even remove one or more user groups; other group users still function on Citrix ADM.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 1162
Configuration Management

Can I perform configuration across multiple Citrix ADC instances simultaneously using Citrix ADM?

Yes, you can use configuration jobs to perform configuration across multiple Citrix ADC instances.

What are configuration jobs on Citrix ADM?

A job is a set of configuration commands that you can create and run on one or more managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the Citrix ADM GUI. You can also convert the recorded tasks 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.

Can I schedule jobs using built-in templates in Citrix ADM?

Yes! You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can choose to execute the job immediately, or schedule the job to be executed later.

You can save the configuration of a job that was previously created, and run the job again after modifying the commands, the parameters, the configuration source, and targeted instances. This is useful when the same set of commands has to be executed on a different instance, or when the job encounters an error and stops further execution.

Certificate Management

Does the deletion of SSL certificates from Citrix ADM lead to deletion of certificates from Citrix ADC instances?

No
Deployment

What is the default user name and password?

- After you complete the initial network configuration, you can log on to Citrix ADM from the hypervisor or SSH console, using the default user name and password (nsrecover/nsroot).
- The default user name and password to log on from the GUI is nsroot/nsroot.

How to change the default password?

To change the password:

1. In Citrix ADM, navigate to System > User Administration > Users.
   The Users page is displayed.
2. Select the user name nsroot and click Edit.
   The Configure System User page is displayed.
3. Select Change Password and create a password of your choice.
4. Click OK.
   You can now use the new password to log on from GUI and hypervisor or SSH console.

Note
You cannot modify the user name.
How to reset the password?

You can see this documentation to reset the password.

In a HA pair, if the password is changed in the primary node and if Break HA pair option is selected later, what is the behavior?

You can log on to both standalone nodes using your new password.

If two standalone servers have different passwords, what is the impact in deploying these two servers in HA pair?

It is recommended to have default password for both servers when you deploy two standalone servers to HA pair.

The HA configuration is complete, but the primary node GUI is not accessible. What can be the reason?

It takes a few minutes for the configuration to take effect. You can try accessing again after a few minutes.

The HA configuration is complete, but the floating IP address GUI is not accessible. What can be the reason?

After the HA configuration, you need to first access the primary node GUI and complete the deployment. For more information, see Deploy the primary and secondary node as a high availability pair. After the deployment is complete, the server reboots and gets ready for high availability deployment. You can then access the floating IP address GUI.

What DB is supported in Citrix ADM standalone and Citrix ADM HA?

Both Citrix ADM standalone and Citrix ADM HA support PostgreSQL.

What is the potential data loss to the secondary node?

The secondary node listens to the heartbeat messages that the primary node sends through the Citrix ADM database. If the secondary node does not receive the heartbeats for more than 180 seconds,
then the secondary node performs an SSH-based check on the primary node. If the heartbeat and SSH-based check fail, the primary node is considered to be down.

In this scenario, the secondary node takes over as the primary node and the 180 seconds timeframe can be considered as the possible data loss to the secondary node.

**What happens if the primary node is down?**

The secondary node takes over and becomes the primary node.

**How to reinstall the failed node?**

It is recommended to install a fresh VM build. To reinstall:

1. Break the HA pair. Navigate to System > Deployment
   The deployment page is displayed. Click Break HA
2. Delete the failed node from the hypervisor.
3. Import the .xva image file to the hypervisor.
4. From the Console tab, configure Citrix ADM with the initial network configurations. For more information, see Register and deploy the first server (primary node) and Register and deploy the second server (secondary node).
5. Redeploy the HA pair.

**Does Citrix ADM support SAN Storage?**

Citrix recommends you to host the Citrix ADM VHD on a local storage. When hosted on storage devices in a storage area network (SAN), Citrix ADM might not work as expected.

**Does Citrix ADM support additional disk?**

Yes. A new installation of Citrix ADM HA pair allocates 120 GB of storage by default. For more than 120 GB storage, you can add one additional disk for a maximum of 3 TB storage. Adding more than one additional disk is not supported.

**After disabling the HA pair, what happens to the floating IP address configured?**

The floating IP address will be no longer accessible and you need to redeploy the high availability pair.
Can I give a different floating IP address while redeploy?

Yes. You can configure a new floating IP address.

Why is secondary node GUI not accessible?

Secondary node is only a read-replica server and acts as a primary node only if the primary node is down for any reason. Citrix recommends to access either the primary node GUI or the floating IP address GUI.

If the primary node is down for a long duration, can the configurations still be done using the floating IP address GUI?

Yes. You can still continue to do configurations and the configurations get saved in the secondary node. After the primary node is back, all the configurations are synchronized.

If there is a necessity to change the primary node IP address or secondary node IP address or floating IP address in the future (for example, changing it to IPv6), what are the recommended solutions to follow?

Changing the IP addresses in HA pair is not supported without breaking the HA pair.

To update the primary node or the secondary node IP address:


   The Deployment page is displayed. Click Break HA

   a) Log on to the primary node using an SSH client or from the hypervisor.
   b) Use nsrecover as the user name and enter the password that you have set.
   c) Enter networkconfig. Perform the procedure from step 3 available at Register and deploy the first server (primary node).

   During the initial network configuration, you can provide a different IP address.
   d) Perform the same procedure for secondary node and continue with the procedure from step 3 available at Register and deploy the second server (secondary node).

To update the floating IP address:

1. Navigate to System > Deployment.

   The Deployment page is displayed.
   a) Click HA Settings.
b) Click **Configure Floating IP Address for High Availability Mode**.

c) Enter the floating IP address and click **OK**.

**Deployment (Disaster Recovery)**

**How frequent does the replication happens between the primary site and disaster recovery site?**

The replication between the primary site and the disaster recovery site is real time.

**After initiating the backup script at the DR site, does the DR site becomes the temporary primary site, until the primary site is recovered and fully operational?**

No. The DR site will now become the primary site.

**If the Break HA pair option is selected, both nodes operate as a standalone server. Since DR support is not applicable for standalone server, what happens to the DR site if Break HA pair is selected?**

If you select Break HA pair option, the replication between the primary site and the DR site is terminated. You need to reconfigure the DR site as part of redeploying HA pair.

**Event Management**

**How can I keep track of all the events that have been generated on my managed Citrix ADC instances using Citrix ADM?**

As a network administrator, you can view details such as configuration changes, log on conditions, hardware failures, threshold violations, and entity state changes on your Citrix ADC instances, along with events and their severity on specific instances. You can use the Citrix ADM events dashboard to view reports generated for critical event severity details on all your Citrix ADC instances.

**What are event rules?**

Using Citrix ADM, you can configure rules to monitor specific events. Event Rules make it easier to monitor a large number of events generated across your Citrix ADM infrastructure.
You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is executed.

The conditions for which you can create filters are severity, Citrix ADC instances, category, and failure objects. The actions you can assign to the events are sending an email notifications, forwarding SNMP traps from managed Citrix ADC instances to the Citrix ADM, and sending an SMS notification.

**Instance Management**

**What are data centers in Citrix ADM?**

A Citrix ADM data center is a logical grouping of the Citrix ADC instances in a specific geographical location. Each server can monitor and manage several Citrix ADC instances within a data center. You can use the Citrix ADM server to manage data such as syslog, application traffic flow, and SNMP traps from the managed instances. For more details on configuring data centers, see How to Configure Data Centers for Geomaps in Citrix ADM.

**What are the different Citrix Appliances that are supported by Citrix ADM?**

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

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN EE

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

**What is an instance profile?**

An instance profile is used by Citrix ADM to access a particular instance.

An instance profile contains the user name and password for access to one or more instances. A default profile is available for each instance type. For example, the ns-root-profile is the default profile for Citrix ADC instances. It contains the default Citrix ADC administrator credentials. When you change
the credentials required for access to instances, you can define custom instance profiles for those instances.

**Can we add unlimited SD-WAN instances in Citrix ADM? Can Citrix ADM handle all scalar and vector counters for SD-WAN?**

Currently, there is no license limit on SD-WAN instances that can be added to Citrix ADM. Citrix ADM has a set of built-in reports that internally polls both scalar and vector counters.

**Can I rediscover multiple Citrix VPX instances in Citrix ADM?**

Yes, you can rediscover multiple Citrix VPX instances in Citrix ADM to learn the latest states and configurations of the instances.

Navigate to **Networks > Instances > NetScaler VPX**, select the instances that you want to rediscover, and in the **Action** drop-down list click **Rediscover**. For more information, see **How to Rediscover Multiple VPX Instances**.

**Can Citrix ADM be installed on Citrix SDX?**

No

**Stylebooks**

**Can stylebooks be used to configure different Citrix ADC instances running on different versions of the Citrix ADC software?**

Yes, you can use stylebooks to configure different Citrix ADC instances running on different versions if there is no discrepancy between the commands across different versions.

**When a stylebook is used to configure multiple Citrix ADC instances at the same time, and configuration of one Citrix ADC instance fails, what happens?**

If applying the configuration to a Citrix ADC instance fails, the configuration is not applied to any more instances, and already-applied configurations are rolled back.

**Do Citrix ADC backups made through Citrix ADC include configurations applied through Stylebooks?**

Yes
**System Management**

**Can I assign a host name to my Citrix ADC server?**

Yes, you can assign a host name to identify your Citrix ADM server. To assign a host name, navigate to **System > System Administration > System Settings**, and click **Change Hostname**.

The host name is displayed on the Universal license for Citrix ADM. For more information, see [How to Assign a Host Name to a Citrix ADM Server](#).

**Can I back up and restore my Citrix ADM configuration?**

Yes, you can back up configuration files (NTP files and SSL certificates), system data, infrastructure and application data, and all your SNMP settings. If your Citrix ADM ever becomes unstable, you can use the backed up files to restore your Citrix ADM to a stable state.

To back up and restore your Citrix ADM’s configuration, navigate to **System > Advanced Settings > Backup Files**, and click **Back Up** or **Restore** as the case may be. For more information, see [How to Back Up and Restore Configuration on Citrix ADM](#).

Citrix recommends that you use this feature before performing an upgrade or for precautionary reasons.

**What are Thresholds and Alerts on Citrix ADM?**

You can set thresholds and alerts to monitor the state of a Citrix ADC instance and monitor entities on managed instances.

When the value of a counter exceeds the threshold, Citrix ADM generates an alert to signify a performance-related issue. When the counter value returns to the clear value specified in the threshold, the event is cleared.

**Can I generate a technical support file for Citrix ADM?**

Yes. Citrix recommends that you generate an archive of Citrix ADM data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

You can generate a technical support file that contains debug logs, duration for which debug logs were collected, and distinct and diverse logs from the Citrix ADM database.

To configure and send a technical support file, navigate to **System > Diagnostics > Technical Support**, and then, click Generate Technical Support File. For more information, see [How to Generate a Tech Support File for Citrix ADM](#).
What is syslog purging?

Syslog is a standard protocol for logging. Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which all Generic Syslog data, AppFirewall data, and Citrix Gateway data will be deleted from Citrix ADM.

Can I configure NTP server on Citrix ADM?

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

To configure an NTP server, navigate to System > NTP Servers, and then click Add. For more information, see How to Configure NTP Server on Citrix ADM.

From which version is the Citrix ADM active-passive HA deployment supported?

The Citrix ADM active-passive HA deployment mode is supported from Citrix ADM version 12.0 build 51.24.

I had a Citrix ADM active-active HA setup and had configured a Citrix ADC appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration?

After you upgrade the Citrix ADM HA pair to active-passive mode, you have to run the following command on the Citrix ADC appliance to update the load balancing configuration:

```
add lb monitor MAS_Monitor TCP-ECV -send “GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r
” -recv “{"statuscode":0, \n"is_passive":0}” -LRTM DISABLED
```

Can I configure load balancing of the Citrix ADM HA pair on a Citrix ADC Instance using port 443?

No, you cannot configure load balancing of the Citrix ADM HA pair on a Citrix ADC Instance using port 443.

When you configure the http-ecv and https-ecv monitors on Citrix ADC, it does not monitor the Citrix ADM HA nodes correctly.
Can a Citrix ADM server backup file be used to restore the configuration of another Citrix ADM server?

Yes

After Citrix ADM backs up a Citrix ADC instance, can that backup file be used to restore the configuration of another Citrix ADC instance through Citrix ADM?

Yes. Download the Citrix ADM backup file, upload it into another Citrix ADC instance’s backup repository, and restore that instance. Make sure that the network information and authentication information do not conflict. For example, check for IP-address or port conflicts, mismatched password profiles. Also make sure that the restored VPX instance has the same NSIP address and Citrix ADC license as the one that was backed up.

Before restoring an instance in a high availability pair, make sure the IP addresses and state (primary or secondary) stored in the backup file match those of the original HA configuration. Also verify that the new primary and secondary have the same type of Citrix ADC license.

Can we force Citrix ADM to use a SNIP address to communicate with the Citrix ADC instances, instead of using the NSIP address of the Citrix ADM server?

Yes, you can add a SNIP address (with management enabled) in Citrix ADM for communication with Citrix ADC instances.

When I back up Citrix ADC Instances in Citrix ADM, is the result a full back-up or a basic back-up?

Backups of Citrix ADC instances by Citrix ADM are full backups.

Is there a troubleshooting guide for Citrix ADM?

Yes. See https://support.citrix.com/article/CTX224502.

How are Citrix ADC instances managed when a Citrix ADM HA failover occurs?

If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node. All the Citrix ADC instances are updated with the latest primary node details as their SNMP trap destination by default.
The new primary (active) Citrix ADM node checks to determine whether the previously active node was configured as AppFlow collector or syslog server, if it was, the new primary adds the AppFlow collector or syslog server details to the information sent to the instances.

For syslog it replaces the old server details.

**What happens when the Citrix ADM HA node that went down comes back up?**

After returning to service, the Citrix ADM node remains passive unless the active node fails over.

**How are Citrix ADC instances distributed across Citrix ADM HA nodes?**

All the Citrix ADC instances are managed by the primary Citrix ADM node.

**How are virtual server licenses managed in case of Citrix ADM HA failover?**

If the Citrix ADM primary node on which vServer licenses are applied goes down, the new primary node manages the vServer licenses for a grace period of 30 days. The licenses have to be reapplied on the new primary by the end of the grace period. For alternatives, contact Citrix support.

**Is a load balancer mandatory for a Citrix ADM HA setup?**

No, but if there is no load balancer, Citrix ADM nodes must be accessed through their own IP addresses. The passive node is marked with the tag “Passive,” and Citrix recommends not to create any configurations on the passive node.

**Does Citrix ADM support an external database?**

No

**Can a Citrix ADC instance that is being managed by Citrix ADM be used as a Load balancer for Citrix ADM HA?**

Yes
What data is synchronized between Citrix ADM HA nodes?

Complete Citrix ADM database is synchronized, and the following folders are synchronized:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/
Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).