NetScaler Application Delivery Management 13.1

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Release notes 58

Migrate on-premises NetScaler ADM to Citrix Cloud™ 61

Configure the ADM service agent 61

Get the client and secret CSV file from Citrix Cloud 62

Validate the ADM service licenses 62

Migrate using a script 63

Roll back to onpremises ADM 68

Prerequisites 68

Use the rollback script 68

FAQs 70

ADM service 70

Is ADM service agent optional similar to on-premises NetScaler agent? 70

Why ADM service? 70

What happens after migration if on-premises NetScaler ADM is an HA pair? 70

What happens if the agent goes down for any reason? 71

Is instance backup also migrated? 71

Is historical data also migrated? 71

Are on-premises licenses also migrated? 71

What is not migrated from on-premises NetScaler ADM? 71

On-premises NetScaler ADM is integrated with Citrix Director. What happens to the integration? 71

After migration, is it again required to license the instance or to enable analytics? 72

Migration tool 72

After running the migration script, error messages are displayed. What can be the issue? 72

The ADC instances have lower versions than the mentioned limitation for pooled licensing. What happens if the option ‘Y’ is selected to change the license server? 72

What happens if the migration script has failed configuration regarding ADC instances? 72

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What happens if a few of the ADC instances fail to move to ADM service. Will rerunning the migration script help? 72

Is there a log file to check the migration status? 73

What happens if the session gets terminated while running the migration script? 73

What happens if ADM service has lesser licenses than the on-premises NetScaler ADM and the migration script is initiated? 73

What happens when on-premises NetScaler ADM is migrated to the ADM service Express Account? 73

What happens if a Citrix Cloud invited user (other than Admin User who created Citrix Cloud account) tries to migrate on-premises ADM setup? 74

Rollback script 74

What happens if rollback script is used in on-premises ADM HA pair? 74

What happens to Disaster Recovery node after using the rollback script? 74

Troubleshooting 74

Manual profile added to ADM service 75

NetScaler device added to ADM service 75

StyleBook custom templates import to ADM service 75

Configuration Jobs added to ADM service 76

IP blocks added to ADM service 76

Network dashboard report addition status 76

All how to articles 77

Instance management 77

Configuration management 78

Certificate management 79

StyleBooks 79

Analytics 80

Event management 80

Authentication 81

NetScaler ADM system 81

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network functions 82
Overview 83
Features and solutions 83
Application Analytics and Management 83
Networks 84
Analytics 85
Orchestration 86
Architecture 86
How NetScaler® ADM discovers instances 87
Polling overview 90
How NetScaler® ADM polls managed instances and entities 90
Different ways of polling instances 94
Global polling of instances 95
Manual polling of instances 95
Manual polling of entities 96
NetScaler® telemetry program 98
Data governance 104
Licensing 107
High Availability 111
How licenses are synchronized between ADM high-availability nodes? 111
Orchestration 112
Upgrade the virtual server licenses 113
Verification 114
Manage virtual servers 114
Disable auto-licensing virtual servers 114
Select third-party virtual servers for licensing 115
Apply virtual server licenses manually 116
Configure policy based virtual server licensing 116

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View the licensed virtual servers 117

Configure auto license support for non-addressable virtual servers 118

Expiry Checks for virtual server licenses 118

System requirements 120

Requirements for NetScaler ADM 120

Requirements for NetScaler ADM on-prem agent 121

Minimum NetScaler version required for NetScaler ADM features 121

Requirements for NetScaler ADM analytics 123

Minimum Citrix Virtual Apps and Desktops versions required for NetScaler ADM features 123

Thin clients supported for HDX™ insight 123

NetScaler instance license required for HDX insight 124

Supported hypervisors 124

Supported operating systems and Workspace versions 125

Supported browsers 125

Supported ports 126

Ports for the ADM server 127

Ports for the ADM agent 129

Ports for ADC instances 130

Ports for ADC built-in agent 132

Ports for external servers 132

Limitations 133

Getting started 135

Step 1 - Review the system requirements 135

Step 2 - Deploy NetScaler ADM 136

Step 3 - Add instances to NetScaler ADM 136

Step 4 - Enable analytics on virtual servers 137

Step 5 - Configure NTP server on NetScaler ADM 137

Step 6 - Configure system settings for optimal NetScaler ADM performance 137

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's next 139

Deploy 140

Prerequisites for installing NetScaler® ADM 141

General requirements for NetScaler ADM 141

NetScaler ADM on Citrix Hypervisor™ 142

Prerequisites 142

XenCenter system requirements 143

Install NetScaler Application Delivery Management 143

Verification 145

NetScaler® ADM on Microsoft Hyper-V 145

Prerequisites 145

Microsoft Hyper-V system requirements 145

Installing NetScaler Application Delivery Management 146

Verification 150

NetScaler® ADM on VMware ESXi 151

Prerequisites 151

To install NetScaler ADM 151

Verification 157

Automate deployment of NetScaler agent on VMware ESXi 157

Configure the NetScaler agent 157

Register the NetScaler agent and change the default password 158

Prerequisites 158

How to configure and register a NetScaler agent 158

Download and edit the .OVF file 159

Install NetScaler ADM virtual appliance on VMware ESXi 163

Verify 172

NetScaler® ADM on Kubernetes cluster 172

Prerequisites 172

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kubernetes cluster 172
NFS share 173
NetScaler appliance 173
Install ADM on Kubernetes cluster 173
NetScaler® ADM on Linux KVM server 175
Prerequisites 176
Hardware requirements 176
Software requirements 177
Network requirements 177
Download NetScaler ADM setup files 177
Install the NetScaler Application Delivery Management on Linux-KVM 177
Configure the NetScaler Application Delivery Management 180
Configure high availability deployment 182
Deployment scenario 183
Components of high availability architecture 185
Monitoring tool 186
Primary node 186
Secondary node 186
Physical streaming replication 186
Heartbeat messages 186
Floating IP address 187
Key points to note 187
Prerequisites 188
To set up NetScaler ADM in high availability mode 190
Register and deploy the first server (primary node) 190
Register and deploy the second server (secondary node) 193
Deploy the primary and secondary node as a high availability pair 195
Disable high availability 196

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Redeploy high availability 197
High availability failover scenarios 197
View Database Synchronization Log messages 197
Split-brain scenario 198
Configure disaster recovery for high availability 199
Disaster recovery workflow 200
Initial setup before disaster 200
Prerequisites 201
First time disaster recovery setup 202
Deploy NetScaler ADM in high availability mode 202
Deploy and register the NetScaler ADM disaster recovery node using DR console 203
Deploy the disaster recovery node using NetScaler ADM GUI 205
Workflow after the disaster 206
Post disaster recovery 207
Revert configurations to the original primary site 208
Configure on-prem agents for multisite deployment 209
Architecture 211
Get started 211
Install the agent in a data center 212
Ports 212
Register the agent 214
Attach an agent to a site 215
Agent actions 216
Add NetScaler instances 216
Attach an existing instance to the agent 217
Access the GUI of an instance to validate events 217
NetScaler agent failover 218
Configure agent unreachable threshold and notification 218

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install an ADM agent as a microservice on a Kubernetes cluster 219
Get started 219
Install NetScaler agent in Kubernetes cluster 220
Migrate NetScaler® ADM single-server deployment to a high availability deployment 221
Modify the existing NetScaler ADM server node 221
Provision the second server node 222
Deploy the two servers in a high availability mode 224
Migrate from NetScaler® Insight Center to NetScaler ADM 225
Prerequisites 225
Hardware requirement 226
Installation procedure 227
Integrate NetScaler® ADM with Citrix Director 227
Prerequisites 228
Hardware requirements for HDX Insight to NetScaler ADM Migration 228
Minimal requirements 228
Software requirements 228
Limitations 229
Attach an extra disk to NetScaler® ADM 229
Attach an extra disk in a standalone NetScaler ADM 230
NetScaler ADM disk partition tool 231
Launch the disk partition tool 231
Create partitions in the new additional disk 232
Resize the partitions in the existing additional disk 234
Remove the partitions in the additional disk 236
Restart the virtual machine 237
Create a backup file of the disk data 237
Additional commands 238
Attach additional disks to NetScaler ADM deployed in high availability 241

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure 243

Add instances to NetScaler® ADM 244

How to create a NetScaler profile 244

Add ADC instances to NetScaler ADM 247

Add NetScaler CPX instances to NetScaler ADM 249

Add a standalone NetScaler BLX instance in NetScaler ADM 250

Add high-availability NetScaler BLX instances in NetScaler ADM 252

Access an instance GUI from the NetScaler ADM 254

Add NetScaler VPX instances deployed in cloud to NetScaler ADM 255

Manage licensing and enable analytics on virtual servers 257

Manage licensing on virtual servers 258

Enable analytics 259

Edit analytics 262

Disable analytics 262

A unified process to enable analytics on virtual servers 263

Prerequisites 264

Enable analytics 264

Configure NTP server 266

Configure system settings 267

Configure system alarms 267

Configure system notifications 268

Configure system prune settings 268

Configure instance syslog prune settings 269

Configure instance event prune settings 269

Configure system backup settings 269

Configure instance backup settings 270

Enable or disable ADM features 270

Integrate NetScaler® ADM with the ServiceNow instance 271

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites 272
How to integrate ADM with ServiceNow? 272
Step 1 - Subscribe to ITSM Adapter service in Citrix Cloud 272
Step 2 - Create an endpoint access in the ServiceNow instance 273
Step 3 - Add a ServiceNow instance 274
Step 4 - Test auto-generation of ServiceNow tickets in ADM 274
Set ServiceNow notifications in ADM 275
Export or schedule export reports 276
Export a report 276
Schedule export report 277
View and edit the scheduled export reports 278
Upgrade 279
Before you upgrade 279
Important points to note before upgrading to 13.1-xx.xx and later 280
Upgrade a single NetScaler ADM server to 13.1-12.x 281
Upgrade a single NetScaler ADM server to 13.1-4.x or 13.1-9.x 284
Troubleshooting database migration issues 286
Upgrade a high availability pair from 12.1 release to 13.1 release 287
Upgrade NetScaler ADM disaster recovery deployment 287
Upgrade the NetScaler ADM disaster recovery node 288
Upgrade on-prem agents for multisite deployment 288
Upgrade the on-prem agent 288
Add an extra disk to the NetScaler ADM server 289
Provision NetScaler instances in OpenStack using StyleBooks 289
Authentication 291
External authentication servers 291
Authenticate users in NetScaler ADM 292
Configure external authentication servers in NetScaler® ADM 293

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add LDAP authentication server 293
Add RADIUS authentication server 295
Add TACACS authentication server 297
Users in NetScaler® ADM 299
User Groups in NetScaler ADM 299
Extract an authentication server group 300
Enable external authentication servers and fallback options 300
Configure fallback and cascade external servers 301
Access Control 303
Role-based access control 303
Limitations 305
Configure access policies 306
Grant StyleBook permissions to users 309
Configure groups 310
Create a user group 310
Manage user access across multiple network function entities 318
How user access changes based on the authorization scope 320
Mapping of RBAC when upgrading NetScaler ADM from 12.0 to later releases 321
Configure roles 321
Configure users 323
View recommendations and manage your ADCs and applications efficiently 325
How to use the Guide me workflow and complete the task? 329
FAQs 330
Applications 332
Prerequisites 332
Application overview 332
Discrete applications 333
Custom applications 333

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Points to note 333

Microservices applications 333

Application management and application dashboard 334

Manage applications 334

Application dashboard 334

Updates in the new dashboard behavior compared to the earlier dashboard 335

Manage applications 335

View application details 336

Add an application 337

Create an application using the StyleBook 339

Edit or delete an application 340

Export reports of app dashboard and security dashboard 340

View applications 341

Configure and associate an application to multiple custom applications 342

Application dashboard overview 344

Search and filter results using the search bar 347

Application details 348

Select App Score components and set thresholds 352

Application details for microservices applications 356

Intelligent App Analytics 360

Configure Intelligent App Analytics 361

Performance indicators for application analytics 362

Response Time 362

Active Services 363

Average CPU Usage 364

Memory Usage 365

Service Flaps 366

Unstable Server 367

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Buildup 369
Low Session Reuse 369
Surge Queue Buildup 370
Unusually large HTTP packets 371
Improper Persistence Type 372
TCP reassemble queue limit hits 373
SSL Real Time Traffic 374
Troubleshoot App Dashboard 375
Troubleshooting scenario 376
Application is licensed 377
Metrics collector is enabled 377
NetScaler instance earlier builds 378
NetScaler instance later builds 379
Application usage and anomalies 383
Application usage analytics 386
View metrics details in graphical format 393
Troubleshoot Web Insight issues 396
Web Insight dashboard 397
Integrated cache requests 400
Troubleshoot Web Insight issues 401
Service Graph 402
Service graph for applications across all NetScaler instances 402
Service graph for Kubernetes applications 403
Service graph for 3-tier Web applications 404
Service graph for Kubernetes apps 405
Setting up service graph 406
Software requirements 406
Before you begin 407

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single tier or Unified ingress topology 407
Dual tier or Service Mesh Lite topology 407
Service mesh topology 408
View details in service graph 409
Service graph dashboard 410
View key metrics trends using the tabular view 413
View client metrics 413
Create a private IP block 414
Public IP blocks 416
View ingress metrics 416
View TCP and SSL metrics 417
TCP metrics 417
SSL metrics 418
View service details 419
Apply filters 419
Using the settings option 421
Analyze the errors 421
View HTTP transaction details 422
Configure thresholds in service graph 424
Single threshold 426
Double threshold 426
View service details 427
Metrics details 429
View backend pod details 429
Use the Poll Now option to get the pod status 430
View ingress details for troubleshooting issues 430
Distributed tracing 436
Prerequisites 436

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View service trace details 441

View the transaction details 442

View diagnostic details for partial or no data in service graph 445

Diagnostics for no data 446

Diagnostics for partial data 446

Troubleshooting 447

Service graph for applications 447

Application view 448

Network functions view 449

Service graph view for no active transactions 450

Analyze metrics 451

Client metrics 451

Network function metrics 451

Service metrics 452

NetScaler metrics (only for GSLB applications) 453

Holistic view of all applications in service graph 454

View client metrics 455

View NetScaler details 456

View discrete applications 458

View microservice applications 460

Search bar to filter results 462

StyleBooks 464

StyleBook categories 466

Default and custom StyleBooks 466

Public and private StyleBooks 466

Example of a StyleBook marked as private 467

View StyleBooks 467

Download custom StyleBooks 469

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delete custom StyleBooks 470
View StyleBook dependencies 471
To view StyleBook dependencies 471
Forward dependencies 471
Reverse dependencies 472
Audit ADC configuration against configuration pack 472
Create a tag for the StyleBook 473
To configure a StyleBook using CLI commands 476
Import and synchronize StyleBooks from GitHub repository 476
Add a repository and import StyleBooks from GitHub repository 477
Use default StyleBooks 479
To create a configuration from a default StyleBook 479
Web application firewall StyleBook 482
Deploying application firewall configurations 482
Create WAF and BOT profiles using StyleBook 492
Create a WAF profile using the StyleBook 492
Create a BOT profile using the StyleBook 493
Hide all default StyleBooks 493
Migrate NetScaler application configuration using StyleBooks Configuration Builder 495
Supported NetScaler Features 496
Create a StyleBook to migrate the NetScaler application configuration 496
Limitations 499
Business application StyleBooks 499
SSO Google Apps StyleBook 500
To deploy SSO Google apps StyleBook 501
SSO Office 365 StyleBook 504
To deploy SSO Microsoft Office 365 StyleBook 505
Microsoft Skype for Business StyleBook 513

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Primary components 513
Front-end servers 513
Edge servers 514
Director servers 514
Configuring NetScaler instances in an enterprise 515
To configure front-end servers 515
Microsoft Exchange StyleBook 521
NetScaler features configured by using Microsoft Exchange StyleBook 521
Prerequisites 522
Configuring a Microsoft Exchange StyleBook 522
To configure a Microsoft Exchange application in NetScaler® ADM 522
Microsoft SharePoint StyleBook 524
Prerequisites 525
NetScaler features configured by the Microsoft SharePoint 2016 StyleBook 525
Load balancing 525
Content switching 526
Responder 526
Rewrite 526
Compression 526
Integrated caching 527
Deploying SharePoint StyleBook configurations 527
Viewing the objects defined on the NetScaler instance 533
Microsoft ADFS proxy StyleBook 535
Benefits of using NetScaler as ADFS proxy 535
Configuration details 536
Deploying Microsoft ADFS proxy StyleBook configurations from NetScaler® ADM 537
To deploy Microsoft ADFS proxy StyleBook 537
Objects created 542

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Oracle e-business StyleBook 553
To create a configuration for Oracle E-Business Suite 12.2 553
Citrix StoreFront™ StyleBooks 555
Create configuration for Citrix StoreFront applications 555
Create and use custom StyleBooks 557
Before you begin 558
Anatomy of a StyleBook 559
StyleBook to create a load balancing virtual server 560
Header 560
Import StyleBooks 562
Parameters 563
Components 566
Build your StyleBook 567
StyleBook to create a basic load balancing configuration 570
Header 570
Import StyleBooks 571
Parameters 571
Components 573
Outputs 578
Build your StyleBook 579
Create a composite StyleBook 583
Build your StyleBook 583
Use GUI attributes in a custom StyleBook 587
Import custom StyleBooks 589
To import your StyleBook 590
Search custom StyleBooks 595
To search for custom StyleBooks 595
Create and edit a configuration pack 595

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a configuration pack 595
Change the StyleBook of a configuration pack 596
Change the StyleBook that has multiple configuration packs 600
Export or import configuration packs 601
Export configuration 601
Import configuration 602
Detach a target instance from a configuration pack 604
Build your StyleBooks 605
Create a StyleBook to upload files to NetScaler® ADM 609
StyleBook configuration 609
Build your StyleBook -1 609
Build your StyleBook - 2 611
Creating configurations to upload files 613
Using the NetScaler ADM API to create a configuration pack 614
Create a StyleBook to upload SSL certificate and certificate key files to NetScaler ADM 614
StyleBook configuration 614
Creating configurations to upload SSL files 617
To create a configuration for uploading files 618
Build your StyleBook 618
Using the NetScaler ADM API to create a configuration pack 622
Viewing the objects defined on the NetScaler instance 622
Enable analytics and configure alarms on a virtual server defined in a StyleBook 623
Instance roles 626
Target-roles section 626
Role “default” 627
Components with roles 627
Build your StyleBook 631
Using APIs 636

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a StyleBook to perform non-CRUD operations 638

Supporting the non-CRUD operations 638

Migrate configuration pack of a StyleBook to another StyleBook 639

Migrate configuration pack 640

To migrate a configuration pack created using example-lb StyleBook to example-lb-mon StyleBook 640

Build your StyleBooks 644

Use API to create configurations from StyleBooks 648

Example 1 649

Example 2 652

Example 3 654

Example 4 655

Updating a configuration 657

Deleting a configuration 659

Use API to create configurations to upload certificate and key files 660

Use API to create configurations to upload any file type 663

Use API to import custom StyleBooks 664

Use API to download custom StyleBooks 666

Use API to delete custom StyleBooks 667

StyleBooks grammar 669

Header 670

Import StyleBooks 672

Parameters 673

'name' 674

'label' 674

'description' 674

'type' 674

'network' 677

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'dynamic-allocation' 678
'key' 678
'required' 679
'allowed-values' 679
'default' 680
'pattern' 682
'min-value' 682
'max-value' 683
'min-length' 683
'max-length' 684
'min-items' 684
'max-items' 685
'gui' 685
'columns' 685
'updatable' 685
'collapse_pane' 686
'layout' 691
'dependent-parameters' 692
Parameters-default-sources construct 694
Substitutions 699
Substitution map 707
Iterate through substitution lists 707
Components 710
Helper components 713
Optional properties 715
Properties-default-sources construct 717
Computation of the Properties of the Component 719
Nested components 719

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Condition construct 722
Repeat construct 723
Repeat-condition construct 727
Nested repeats 728
Outputs 731
Parameter reference 732
Parent reference 734
Components reference 736
Substitutions reference 737
Variable reference 738
Operations 739
Analytics 743
Alarms 747
Expressions 751
Arithmetic expressions 751
String expressions 751
List expressions 751
Relational expressions 752
Logical expressions - boolean 752
Verbatim string expressions 753
Target expressions 754
Expression Type Validation 754
Indexing Lists 757
In-place interpolations 757
Allowed Types Inside Interpolations 758
Simple interpolations 759
Automatic type conversions 759
Sequential interpolations 759

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nested interpolations 760
Interpolations with quotewrap 760
Escape Characters in Interpolations 760
Built-in functions 760
str() 761
int() 761
bool() 762
len() 762
min() 762
max() 763
bin() 763
oct() 763
hex() 764
lower() 764
upper() 764
sum() 764
pow() 765
ip() 765
base64.encode() 766
base64.decode() 766
exists() 766
filter() 766
if-then-else() 767
join() 768
split() 768
map() 769
quotewrap() 770
replace() 770

© 1997–2026 Citrix Systems, Inc. All rights reserved.

trim() 771
truncate() 771
distinct() 771
url.encode() 771
url.decode() 771
is-ipv4() 772
is-ipv6() 772
startswith() 772
endswith() 772
contains() 773
substring() 773
Dependency detection 774
Cyclic Dependencies 776
Security 778
Application Security Dashboard 778
Threat index details 779
Safety index details 780
View application security violation details 781
Prerequisite 782
Integration with Splunk 782
Configure Splunk to receive data from NetScaler ADM 782
Setup the Splunk HTTP event collector endpoint and generate a token 783
Install the Splunk Common Information Model 784
Prepare a sample dashboard in Splunk 785
Configure NetScaler ADM to export data to Splunk 788
View dashboards in Splunk 791
Integration with New Relic 793
Prerequisites 794

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add the key details in NetScaler ADM 794

New Relic dashboard 796

Gateway 799

Gateway Insight 799

Points to note 800

Limitations 800

Enable Gateway Insight 801

For NetScaler ADM version **13.0 Build 41.x or later** 802

Enable AppFlow authentication, authorization, and auditing user name logging on a NetScaler Gateway appliance by using the GUI 802

Viewing Gateway Insight reports 802

To view EPA, SSO, authentication, authorization, and application launch failures 803

To view a summary of session modes, clients, and the number of users 803

Viewing Gateway Insight reports for users 804

To view user details 804

Viewing Gateway Insight reports for applications 807

To view application details 807

Viewing Gateway Insight reports for gateways 808

To view gateway details 808

Exporting reports 809

To export a report 810

Gateway Insight use cases 810

A user is not able to log in to the NetScaler Gateway appliance or to the internal web servers 810

Authentication failures 811

EPA failures 812

SSO failures 814

After successfully logging on to NetScaler Gateway, a user is not able to launch any virtual application 815

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application 817

A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network 818

Different users might be using different NetScaler Gateway deployments or might log on to NetScaler Gateway through different access modes. The administrator must be able to view details about the deployment types and access modes 818

Troubleshoot Gateway Insight issues 819

Gateway Insight configuration checklist 819

Connectivity between NetScaler and NetScaler ADM checklist 820

Record generation in NetScaler checklist 820

Validation of records in NetScaler ADM 821

Validation of Logstream logs in NetScaler ADM 821

Gateway Insight counters 821

AppFlow records in NetScaler log 822

Sample logs 822

Contact Citrix technical support 823

Known Issues 824

HDX™ Insight 824

Identifying the root cause of slow performance issues 825

Scenario 1 825

Summary 827

Scenario 2 827

Summary 828

Geomaps for HDX Insight 829

Use case 829

Limitations 830

Enabling HDX™ Insight data collection 831

Enabling data collection for monitoring NetScalers deployed in LAN user mode 831

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling data collection for NetScaler Gateway appliances deployed in single-hop mode 835
Enabling data collection for NetScaler Gateway appliances deployed in double-hop mode 837
Configure HDX Insight on virtual servers used for Optimal Gateway 838
Enable data collection on NetScaler ADM 839
Configuring NetScaler Gateway appliances to export data 839
Enable data collection for monitoring NetScalers deployed in transparent mode 844
Enable data collection for NetScaler Gateway appliances deployed in single-hop mode 847
Enable data collection to monitor NetScalers deployed in transparent mode 849
Enable data collection for NetScaler Gateway appliances deployed in double-hop mode 852
Enable data collection on NetScaler ADM 854
Configure NetScaler Gateway appliances to export data 854
Enable data collection to monitor NetScalers deployed in LAN user mode 858
Create thresholds and configure alerts for HDX™ Insight 861
Example Use cases 862
Viewing HDX™ Insight reports and metrics 865
User view reports and metrics 866
Summary view 867
Line chart 867
User summary report 869
Channels 871
User agents 871
Thresholds breach count 872
World map 872
Per User view 873
Line chart 874
Current/Terminated sessions report 874
Support for EDT in HDX insight 876
Desktop users 879

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications 879
Instances 880
Channels 880
User agents 881
Per User session view 881
Timeline chart 882
Active application 883
Related sessions 883
Application view reports and metrics 884
Summary view 884
Line chart 884
Applications summary report 885
Active application report 885
Threshold report 886
Line chart 886
Current sessions report 887
Per application session view 890
Line chart 891
User bar graph 892
Desktop view reports and metrics 892
Summary view 893
Line chart 893
Desktop summary report 894
Threshold report 895
Per Desktop view 895
Line chart 896
Desktop Users report 897
User Desktops Active/Inactive report 898

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Per Desktop session view 901
Timeline chart 901
Related Desktop sessions report 903
Instance view reports and metrics 906
Instance summary view 907
Instance bar graph 907
Instance/Active instances summary report 907
Threshold report 908
Skipped flows 908
World view 908
Per instance view 909
Line chart 910
Applications bar graph 910
Users bar graph 911
Desktop Users report 911
World view 912
License view reports and metrics 913
Line chart 914
Threshold report 914
- Application View Reports and Metrics 914
- Summary view 914
- Line chart 915
- Applications summary report 915
- Active application report 916
- Threshold report 916
- Line chart 916
- Current sessions report 917
- Per Application session view 920

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart 921
User bar graph 922
Desktop View Reports and Metrics 923
Summary view 923
Line chart 923
Desktop summary report 925
Threshold report 925
Per desktop view 925
Line chart 926
Desktop users report 927
User desktops active/inactive report 928
Per desktop session view 931
Timeline chart 931
Related desktop sessions report 933
User View Reports and Metrics 936
Summary view 937
Line chart 937
User summary report 939
Channels 941
User agents 942
Thresholds breach count 942
World map 942
Per user view 943
Line chart 944
Current/Terminated sessions report 944
Support for EDT in HDX insight 946
Desktop Users 949
Applications 949

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instances 950
Channels 950
User agents 951
Per User session view 951
Timeline chart 952
Active application 953
Related sessions 953
Instance View Reports and Metrics 954
Instance summary view 954
Instance bar graph 954
Instance/Active instances summary report 955
Threshold report 955
Skipped flows 955
World view 956
Per instance view 957
Line chart 958
Applications bar graph 958
Users bar graph 959
Desktop users report 959
World view 960
License View Reports and Metrics 961
Line chart 962
Threshold report 962
Troubleshoot HDX™ Insight issues 962
HDX Insight configuration checklist 963
Connectivity between NetScaler and NetScaler ADM checklist 963
Record generation for HDX/ICA traffic in NetScaler checklist 964
Error counters 972

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nstrace validation 976

Population of records in NetScaler ADM checklist 976

Before contacting Citrix technical support 977

Known Issues 977

Infrastructure 978

Infrastructure Analytics 978

Infrastructure analytics 979

Instance score 979

Health indicators 979

View ADC Capacity issues 981

Value of health indicators 982

Infrastructure analytics dashboard 984

Circle pack view 984

Instance circles 985

Grouped instance circles 987

Clustered instance circles 988

How to use Circle Pack 991

Tabular view 993

How to use the summary Panel 995

Instance info 998

Traffic profile 999

How to use the settings panel 1000

View 1000

Score thresholds 1001

How to visualize data on the dashboard 1003

View instance details in Infrastructure Analytics 1003

View the capacity issues in an ADC instance 1011

View recommended actions to solve capacity issues 1012

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced Infrastructure Analytics with new indicators 1013
Tabular view 1015
View details of an anomaly 1016
Instance management 1017
Add an instance 1017
How to use the instance dashboard 1018
Monitor globally distributed sites 1020
Use case 1021
Configuring Geomaps 1022
How to create tags and assign to instances 1026
How to search instances using values of tags and properties 1029
To search for NetScaler VPX instances 1030
Manage admin partitions of NetScaler instances 1032
Create a NetScaler high-availability pair 1037
Back up and restore NetScaler instances 1040
Configure instance backup settings 1041
Create a backup for a selected NetScaler instance by using NetScaler ADM 1044
Restore a NetScaler instance by using NetScaler ADM 1045
Restore a NetScaler SDX appliance using NetScaler ADM 1046
Force a failover to the secondary NetScaler instance 1047
Force a secondary NetScaler instance to stay secondary 1049
Create instance groups 1050
To create an instance group using NetScaler® ADM 1050
Provision NetScaler VPX instances on SDX using ADM 1051
Step 1 - Add a VPX instance 1051
Step 2 - Allocate licenses 1052
Step 3 - Allocate resources 1053
Step 4 - Add instance administration 1056

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5 - Specify network settings 1057
Step 6 - Specify Management VLAN settings 1059
View the provisioned VPX instance 1060
Provision NetScaler VPX instances on VMware ESX 1061
Prerequisites 1061
Convert NetScaler VPX files into templates 1061
Create a site in ADM 1062
Provision an instance on VMware ESX 1064
Rediscover multiple NetScaler VPX instances 1068
Unmanage an instance 1069
Trace the route to an instance 1069
Replicate configurations from one NetScaler instance to another 1070
To replicate configurations from one instance to other NetScaler instances 1071
SSL certificate management 1072
Enterprise SSL policy settings 1072
How the NetScaler ADM certificate works 1073
SSL certificate management use cases 1074
Install SSL certificates 1074
Notification settings for certificate expiry 1074
Renewal of certificates 1075
Update the existing certificate 1075
Create certificate signing request 1076
Link and unlink SSL certificates 1078
Audit logs 1078
Use the SSL Dashboard 1079
To monitor SSL certificates 1079
To view audit trails for SSL certificates 1081
To exclude default NetScaler certificates on the SSL Dashboard 1082

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View, upload, and download SSL files 1083
Set up notifications for SSL certificate expiry 1084
Update an installed certificate 1086
Install SSL certificates on a NetScaler instance 1086
Create a Certificate Signing Request (CSR) 1088
Link and unlink SSL certificates 1091
Configure an enterprise policy 1091
Poll SSL certificates from NetScaler instances 1092
Events 1093
Use events dashboard 1094
Set event age for events 1096
Schedule an event filter 1098
Set repeated email notifications for events 1100
Suppress events 1101
Create event rules 1102
Step 1 - Define an event rule 1104
Step 2 - Choose the severity of the event 1105
Step 3 - Specify the event category 1106
Step 4 - Specify NetScaler instances 1106
Step 5 - Select failure objects 1107
Step 6 - Specify advanced filters 1107
Step 7 - Add event rule actions 1108
To set email Event Rule Action 1109
To set Trap Event Rule Action 1110
To set the Run Command Action 1110
To set the `Execute` Job Action 1113
To set the Suppress Action 1114
To set Slack notifications from NetScaler ADM 1115

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set PagerDuty notifications from NetScaler ADM 1116
To auto-generate ServiceNow incidents from NetScaler ADM 1117
Modify the reported severity of events that occur on NetScaler instances 1117
View events summary 1118
Display event severities and SNMP trap details 1119
View and export NetScaler syslog messages 1122
Configure ADM as a syslog server 1122
View and search syslog messages 1123
Export and schedule syslog messages 1124
Suppress syslog messages 1126
Suppressing syslog messages by creating filters 1127
Disabling the filter 1129
Configure prune settings for instance events 1129
Network functions 1130
Generate reports for load balancing entities 1130
Generate a combined load balancing report 1132
Generate an individual load balancing entity report 1133
Export or schedule export of network functions reports 1134
Network reporting 1137
Network reporting dashboard 1138
Exporting network reports 1142
View network reporting data by applying aggregations 1143
How to manage Thresholds for Network Reports on NetScaler ADM 1145
Set Performance Polling Interval for Network Reports 1148
Configuring Network Reporting Prune Settings 1148
Configuration jobs 1148
Configuration Template 1149
Instance 1150

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File 1150

Record and Play 1150

Related Articles 1150

Create a configuration job 1151

Use record-and-play to create configuration jobs 1154

To record the GUI configuration and convert it into a configuration task 1155

Use configuration jobs to replicate configuration from one instance to multiple instances 1159

Use variables in configuration jobs 1161

Create configuration jobs from corrective commands 1168

To create a configuration job from corrective commands on NetScaler® ADM 1169

Replicate running and saved configuration from one NetScaler instance to another 1170

Reuse run configuration jobs 1171

Use SCP (put) command in configuration jobs 1173

Use configuration templates 1176

Use the master configuration template 1176

Schedule jobs created by using built in templates 1184

To schedule a job by using built-in templates in NetScaler® Application Delivery Management (ADM) 1185

Use configuration templates to create audit templates 1186

Reschedule jobs configured by using built in templates 1189

To reschedule a job that was configured by using built-in templates in NetScaler ADM 1189

Reuse configuration audit templates in configuration jobs 1190

Creating a Template in Configuration Audits and Reusing it in Configuration Jobs 1191

Import and export configuration templates 1194

Configuration audit 1196

Create audit templates 1196

View audit reports 1201

Saved Vs Running Diff 1202

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Template vs Running Diff 1203
View the file status audit reports 1204
Audit configuration changes across instances 1206
Viewing details of configuration changes 1209
Set configuration audit notifications 1210
Get configuration advice on network configuration 1211
Poll configuration audit of NetScaler instances 1213
Generate configuration audit diff for ConfigChange SNMP Traps 1214
Upgrade jobs 1215
Schedule upgrading of NetScaler instances 1216
Schedule upgrading of NetScaler SDX instances 1220
Schedule upgrading of NetScaler BLX instances 1223
Schedule upgrading Autoscale™ group 1228
Schedule configuring HA pair of NetScaler instances 1229
Schedule converting HA pair of instances to cluster 1231
Instance Advisory 1234
Upgrade Advisory (Preview) 1234
View upgrade advisory 1234
Security Advisory (Preview) 1236
View security advisory 1236
Supported CVEs through Security Advisory 1237
Latest supported CVEs 1237
Supported CVEs 1238
Orchestration 1241
VMware NSX Manager 1241
Cisco ACI Hybrid Mode 1242
OpenStack: Integrating NetScaler instances 1243
NetScaler Driver for OpenStack Neutron LBaaS 1243

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registering NetScaler ADM and OpenStack with each other 1243
Tenants in OpenStack 1243
Placement policies 1244
Service packages 1244
Features Supported on LBaaS V1 and LBaaS V2 1244
Use Case Scenario 1245
NetScaler ADM Integration with OpenStack Workflow 1246
OpenStack: Integrating NetScaler instances 1246
NetScaler Driver for OpenStack Neutron LBaaS 1247
Registering NetScaler ADM and OpenStack with each other 1247
Tenants in OpenStack 1247
Placement policies 1247
Service packages 1248
Features Supported on LBaaS V1 and LBaaS V2 1248
Use Case Scenario 1249
NetScaler ADM Integration with OpenStack Workflow 1250
Prerequisites 1250
NetScaler® ADM and OpenStack Software Requirements 1250
NetScaler ADM Hardware Requirements 1251
Pre-configuration tasks in NetScaler® ADM and OpenStack 1251
Installing NetScaler ADM 1251
Installing the NetScaler driver software and registering NetScaler ADM on OpenStack 1251
Registering OpenStack with NetScaler ADM 1253
Creating a tenant on OpenStack 1257
Adding OpenStack tenants 1257
Provisioning NetScaler devices 1257
Pre-provisioning NetScaler devices 1257
Autoprovisioning NetScaler devices 1258

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Creating a service package in NetScaler ADM 1259

Creating placement policies (optional) 1260

Enabling traffic from NetScaler instances to back-end servers through client network 1261

Auto-provisioning NetScaler VPX devices deployed on NetScaler SDX platform 1261

Configure LBaaS V1 using Horizon 1263

Configure LBaaS V2 using command line 1263

Monitoring OpenStack Applications in NetScaler® ADM 1269

Configure layer 7 content switching 1269

L7 Rules 1270

Comparison Types 1271

L7 Policies 1271

Mapping Between OpenStack L7 Policies and NetScaler Entities 1272

Policy Positioning 1273

Configuration Tasks 1275

Create L7 Policy to Drop Requests 1275

Create L7 Policy to Redirect Requests to Particular URL 1276

Create L7 Policy to Redirect Requests to a Pool 1276

Manual provisioning of NetScaler VPX instance on OpenStack 1277

Provisioning of NetScaler VPX instance on OpenStack using StyleBook 1279

Points to note before provisioning instances using StyleBooks 1280

VPX check-in and check-out license and pooled license support for OpenStack environment 1281

Shared VLAN support for admin partitions 1283

Configuring Shared VLAN from NetScaler Instance 1284

Configuring Shared VLAN from OpenStack Orchestration 1285

Trial licensing workflow 1286

Trial Licenses 1286

Integrate with OpenStack Heat services 1287

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Heat Orchestration Service 1287
NetScaler StyleBooks 1287
Workflow to Configure NetScaler Instances using Heat 1288
Service package isolation policies 1293
Dedicated Isolation Policy 1293
Partition Isolation Policy 1294
Shared Isolation Policy 1295
Flexible policy-based device allotment 1296
Adding Placement Policy 1298
NSX Manager: manual provisioning of NetScaler instances 1302
Prerequisites 1302
VMware ESXi Hardware Requirements 1302
Configuring VMware NSX 1303
Adding NetScaler VPX Instance in NetScaler ADM 1306
Registering VMware NSX Manager with NetScaler ADM 1308
Creating a Service Package in NetScaler ADM 1309
Performing Load Balancer Service Insertion for Edge 1312
Viewing L2 Gateway on NSX Manager 1316
Viewing Allotted NetScaler 1316
Configuring NetScaler VPX Instance Using StyleBook 1317
Viewing Load Balancer Configuration 1319
Deleting Load Balancer Service 1320
NSX Manager: auto provisioning of NetScaler instances 1321
Overview 1321
Prerequisites 1322
High-Availability Deployment of NetScaler ADM and NetScaler Instances 1322
Setting up NetScaler® ADM HA Endpoint Details 1322
Registering VMware NSX Manager with NetScaler ADM 1323

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Uploading Licenses in NetScaler ADM 1324
Uploading NetScaler VPX Images in NetScaler ADM 1324
Creating Service Packages in NetScaler ADM 1325
Performing Load Balancer Service Insertion for Edge 1327
Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI 1329
Creating pools and pool members 1329
Creating virtual servers 1330
Configuring Load Balancing Services on NetScaler VPX in NetScaler ADM GUI 1331
Verifying Creation of Virtual Servers and Service Groups in NetScaler VPX Instances 1331
Deleting Load Balancing Services 1332
NetScaler automation using NetScaler ADM in Cisco ACI hybrid mode 1332
Prerequisites 1335
Configure NetScaler in hybrid mode using Cisco APIC and NetScaler ADM 1335
APIC fault reports 1366
Logs generated by NetScaler® ADM 1367
Logs generated by hybrid-mode device package 1371
NetScaler device package in Cisco ACI's cloud orchestrator mode 1375
Manage the Kubernetes Ingress configuration in NetScaler® ADM 1380
Before you begin 1381
Configure the NetScaler ADM with a secret token to manage a Kubernetes cluster 1381
Add the Kubernetes cluster in NetScaler ADM 1382
Video Insight 1384
Configuring Video Insight 1385
Sample 1386
Viewing the Video Insight metrics in NetScaler ADM 1386
View network efficiency 1388
Compare the data volume used by optimized and unoptimized ABR videos 1389
View the type of videos streamed and data volume consumed from your network 1390

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compare optimized and unoptimized play time of ABR videos 1392
Compare bandwidth consumption of optimized and unoptimized ABR videos 1395
Compare optimized and unoptimized number of plays of ABR videos 1396
View peak data rate for a specific time frame 1399
Configure IP address management (IPAM) 1401
Add an external IP address provider 1401
Add a network 1402
View allocated IP addresses 1403
Use ADM audit logs for managing and monitoring your infrastructure 1404
ADC instance related audit logs 1404
Configure the ADM service as a syslog server 1404
ADM related audit logs 1406
Application related audit logs 1406
Manage instance licenses 1407
NetScaler pooled capacity 1407
How NetScaler pooled capacity licensing works 1408
Zero-capacity hardware 1408
Manage and install platform licenses 1409
Standalone NetScaler VPX instances 1409
Standalone NetScaler CPX instances 1410
Standalone NetScaler BLX instances 1411
Bandwidth Pool 1411
Instance pool 1411
NetScaler ADM license server 1411
Table 1. Supported pooled capacity for MPX and SDX instances 1412
Table 2. Supported pooled capacity for CPX instances 1416
Table 3. Supported pooled capacity for VPX instances on Hypervisors and Cloud services 1416
Table 4. Supported pooled capacity for BLX instances 1417

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 5. License requirement for different form factors 1417

Configure NetScaler pooled capacity 1417

Supported hardware and software versions 1418

ADC pooled capacity states 1418

Step 1 - Apply licenses in ADM 1419

Step 2 - Register NetScaler ADM as a license server 1419

Use GUI to register ADM as a license server 1420

Use CLI to add ADM as a license server 1421

Step 3 - Allocate pooled licenses to ADC instances 1423

Configure pooled capacity on ADC instances 1425

NetScaler MPX™ instances 1425

NetScaler VPX instances 1426

NetScaler high-availability pair 1426

Configure an ADM server only as the pooled license server 1427

How to configure an ADM server only as the pooled license server 1428

Upgrade a perpetual license in NetScaler VPX to NetScaler pooled capacity 1429

Prerequisites 1430

Upgrade the Perpetual License in NetScaler VPX high availability pair to NetScaler pooled capacity 1433

Upgrading a Perpetual License in NetScaler MPX to NetScaler Pooled Capacity 1437

Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler pooled capacity 1442

Prerequisites 1442

Upgrade a perpetual license in a NetScaler SDX to NetScaler pooled capacity 1446

NetScaler pooled capacity on NetScaler instances in cluster mode 1449

Allocate ADC Pooled capacity to an ADC cluster 1450

Allocate ADC Pooled capacity to an ADC cluster using CLI 1452

Health monitoring 1453

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Grace Period 1454

Notifications and Alarms 1454

Expected behaviors when issues arise 1456

License Server stops responding 1456

NetScaler pooled-capacity enabled instance stops responding 1457

Both license server and NetScaler pooled-capacity enabled instance stop responding 1457

The NetScaler pooled-capacity enabled instance shuts down gracefully 1457

Network loses connectivity 1457

Configure expiry checks for pooled capacity licenses 1458

Check in and check out NetScaler VPX and BLX licenses 1460

Prerequisites 1460

Installing Licenses in NetScaler ADM 1461

Verification 1462

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler GUI 1462

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler CLI 1465

Allocate VPX and BLX Licenses to an ADC instance by using API 1465

Update a licensing server IP address 1468

Configure Expiry Checks for NetScaler VPX and BLX Check-In and Check-Out Licenses 1469

NetScaler virtual CPU licensing 1470

Virtual CPU licensing for NetScaler VPX 1471

Configuring licensing server in NetScaler VPX license using CLI 1473

Update a licensing server IP address 1473

Managing virtual CPU licenses on NetScaler ADM 1474

Virtual CPU licensing for NetScaler CPX 1474

Manage system settings 1477

Network Configurations 1477

System Configurations 1478

System Maintenance 1479

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data Pruning 1479

Backup 1480

Event Notifications 1481

SSL Settings 1481

Configure Features 1482

Configure system backup settings 1482

Configure an NTP server 1483

Upgrade NetScaler® Application Delivery Management (ADM) 1485

How to reset the password for NetScaler® ADM 1485

Configure a secondary NIC to access NetScaler® ADM 1493

Prerequisites 1494

Configure a second NIC in NetScaler ADM 1494

Configure a secondary NIC to access ADM agent 1495

Modify the IPV4 NIC network addresses using CLI 1496

Configure syslog purging interval 1498

Configure system prune and event prune settings 1499

Configure Events Prune Settings by Using NetScaler® ADM 1500

Enable shell access for non-default users 1501

Recover inaccessible NetScaler® ADM servers 1502

How to Use NetScaler ADM Database Recovery Script for a NetScaler ADM Standalone Deployment 1502

How to use NetScaler ADM database recovery script for a NetScaler ADM high availability deployment 1506

Assign a host name to a NetScaler® ADM server 1507

Back up and restore your NetScaler® ADM server 1508

Back up the NetScaler ADM configuration 1509

Transfer a NetScaler ADM backup file to an external system 1510

Restore the NetScaler ADM configuration from a backup file 1512

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VM snapshots of NetScaler® ADM in high availability deployment 1513
Take a snapshot of NetScaler ADM servers 1513
Restore a snapshot of NetScaler ADM servers 1513
View auditing information 1514
Configure SSL settings 1515
Monitor CPU, memory, and disk usage 1515
Configure notification settings 1516
Create an email distribution list 1517
Create an SMS distribution list 1518
Create a Slack profile 1519
Create a PagerDuty profile 1520
View the ServiceNow profile 1521
Generate a tech support file 1521
Configure a cipher group 1523
Create SNMP trap destination, manager community, and users 1524
Configure and view system alarms 1525
Create SNMP managers and users for NetScaler agent 1527
Add an SNMP v2 manager 1527
Add an SNMP v3 manager 1528
Add an SNMP user 1529
Managing SNMP views 1532
Configure agent settings 1533
Set agent's keep-alive interval 1533
Change agent's password without the current password 1533
NetScaler® ADM as an API proxy server 1535
How NetScaler ADM Works as an API Proxy Server 1535
How to use NetScaler ADM as an API proxy server 1538
Example 1: Retrieve load balancing virtual server statistics 1541

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example 2: Create a load balancing virtual server 1541

Example 3: Modify a load balancing virtual server 1542

Example 4: Delete a load balancing virtual server 1543

Example 5: Download the CLI running config on the ADC 1543

FAQs 1545

Analytics 1545

Is it required to enable EUEM virtual channel on NetScaler Gateway instances deployed in single-hop mode? 1545

How do I enable NetScaler ADM to monitor web-application and virtual-desktop traffic? 1546

After I add the NetScaler instances, does NetScaler ADM automatically start collecting analytical information? 1546

Is it required to access the individual NetScaler appliance for enabling analytics? 1547

What are the types of virtual servers that can be listed on a NetScaler instance to enable analytics? 1547

How do I attach an extra disk to the NetScaler ADM? 1547

What do you mean by collectors are not configured on NetScaler instances? 1548

What does enabling client-side measurements do? 1548

Authentication 1549

What is load balancing of authentication requests? 1549

Why do we need to cascade external authentication servers? 1549

How many external authentication servers can I cascade? 1549

Do I have an alternative when external authentication fails? 1550

What is fallback local authentication? 1550

What is an extraction of external user groups? 1550

Why do we need to assign group permissions? 1551

Configuration Management 1551

Can I perform configuration across multiple NetScaler instances simultaneously using NetScaler ADM? 1551

What are configuration jobs on NetScaler ADM? 1552

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can I schedule jobs using built-in templates in NetScaler ADM? 1552

Certificate Management 1553

Does the deletion of SSL certificates from NetScaler ADM lead to the deletion of certificates from NetScaler instances? 1553

Deployment 1553

What is the default user name and password? 1553

How to change the default password? 1553

How to reset the password? 1554

In a HA pair, if the password is changed in the primary node and if the Break HA pair option is selected later, what is the behavior? 1555

If two standalone servers have different passwords, what is the impact in deploying these two servers in HA pair? 1555

The HA configuration is complete, but the primary node GUI is not accessible. What can be the reason? 1555

The HA configuration is complete, but the floating IP address GUI is not accessible. What can be the reason? 1556

What DB is supported in NetScaler ADM standalone and NetScaler ADM HA? 1556

What is the potential data loss to the secondary node? 1556

What happens if the primary node is down? 1556

How to reinstall the failed node? 1557

Does NetScaler ADM support SAN Storage? 1557

Does NetScaler ADM support an extra disk? 1557

After disabling the HA pair, what happens to the floating IP address configured? 1558

Can I give a different floating IP address while redeploy? 1558

Why is secondary node GUI not accessible? 1558

If the primary node is down for a long duration, can the configurations still be done using the floating IP address GUI? 1558

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? 1559

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Does ADM support AMD processors? 1560

Deployment (Disaster Recovery) 1560

How frequent does the replication happens between the primary site and disaster recovery site? 1560

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? 1560

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? 1561

Event Management 1561

How can I keep track of all the events that have been generated on my managed NetScaler instances using NetScaler ADM? 1561

What are event rules? 1562

Instance Management 1562

What happens if an ADC instance cannot connect to ADM after bandwidth allocation when you use NetScaler pooled capacity licensing? 1562

What are data centers in NetScaler ADM? 1563

What are the different NetScaler ADC appliances that are supported by NetScaler ADM? 1563

What is an instance profile? 1563

Can I rediscover multiple NetScaler VPX instances in NetScaler ADM? 1564

Can NetScaler ADM be installed on NetScaler SDX? 1564

Can I add a NetScaler instance on the ADM software by using a public IP address? 1564

How to register a disaster recovery node if the DR node credentials are changed? 1565

StyleBooks 1566

Can StyleBooks be used to configure different NetScaler instances running on different versions of the NetScaler software? 1566

When a StyleBook is used to configure multiple NetScaler instances at the same time, and configuration of one NetScaler instance fails, what happens? 1566

Do NetScaler backups made through NetScaler include configurations applied through StyleBooks? 1566

System Management 1567

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can I assign a host name to my NetScaler ADM server? 1567

Can I back up and restore my NetScaler ADM configuration? 1567

What are Thresholds and Alerts on NetScaler ADM? 1567

Can I generate a technical support file for NetScaler ADM? 1568

What is syslog purging? 1568

Can I configure NTP server on NetScaler ADM? 1569

From which version is the NetScaler ADM active-passive HA deployment supported? 1569

I had a NetScaler ADM active-active HA setup and had configured a NetScaler appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration? 1569

Can I configure load balancing of the NetScaler ADM HA pair on a NetScaler Instance using port 443? 1570

Can a NetScaler ADM server backup file be used to restore the configuration of another NetScaler ADM server? 1570

After NetScaler ADM backs up a NetScaler instance, can that backup file be used to restore the configuration of another NetScaler instance through NetScaler ADM? 1570

Can we force NetScaler ADM to use a SNIP address to communicate with the NetScaler instances, instead of using the NSIP address of the NetScaler ADM server? 1571

When I back up NetScaler Instances in NetScaler ADM, is the result a full back-up or a basic back-up? 1571

Is there a troubleshooting guide for NetScaler ADM? 1571

How are NetScaler instances managed when a NetScaler ADM HA failover occurs? 1572

What happens when the NetScaler ADM HA node that went down comes back up? 1572

How are NetScaler instances distributed across NetScaler ADM HA nodes? 1572

How are virtual server licenses managed if there is NetScaler ADM HA failover? 1573

Is a load balancer mandatory for a NetScaler ADM HA setup? 1573

Does NetScaler ADM support an external database? 1573

Can a NetScaler instance that is being managed by NetScaler ADM be used as a Load balancer for NetScaler ADM HA? 1573

What data is synchronized between NetScaler ADM HA nodes? 1574

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index 1575

Configure adaptive thresholds 1576

To create an adaptive threshold using NetScaler® ADM 1577

Configure database summarization 1577

To configure database summarization 1577

Configure SLA management 1578

To configure SLA breach for a NetScaler instance 1579

Create thresholds and alerts 1580

To create a threshold and alert using NetScaler ADM 1580

Disable URL data collection 1580

To disable URL data collection from NetScaler ADM 1581

Logstream overview 1581

Enable Logstream as Transport Mode 1582

Dashboards 1584

Outbound traffic dashboard 1585

View the outbound traffic from the network 1585

User dashboard 1586

User activity investigator 1587

User transactions 1588

Summary panel 1589

Risk score 1590

All Violations 1590

Violation categories 1591

Security violations dashboard 1592

Violation details 1593

Application overview 1593

Violation categories 1595

View WAF violation details 1596

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View bot violation details 1599
View events history 1602
Network violation details 1602
HTTP Slow Loris 1602
DNS Slow Loris 1603
HTTP Slow Post 1604
NXDOMAIN Flood Attack 1605
HTTP Desync Attack 1606
Bleichenbacher Attack 1608
Segment Smack Attack 1609
SYN Flood Attack 1610
Small Window Attack 1611
SSL Insight 1612
Prerequisites 1613
Configure SSL Insight 1614
Enable the AppFlow feature 1614
Enable SSL Insight parameters 1617
View the SSL Insight metrics 1618
Use case: Obtain an overview of the SSL transactions 1619
Use case: SSL metrics for clients 1620
TCP Insight 1621
Prerequisites 1621
Enabling TCP Insight 1622
View the TCP Insight metrics in NetScaler ADM 1622
Use cases 1622
Assess benefits of TCP optimization 1623
Tune TCP parameters 1623
Measure impact of TCP optimization on traffic volume 1624

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot Web Insight issues 1625
Diagnostics for no data 1625
Issues related to Web Insight dashboard reports 1625
Configuration issue 1626
Connectivity issue between NetScaler and NetScaler ADM 1626
AppFlow data not received from NetScaler 1627
License issue 1627
Observation point ID issue 1628
Missing AppFlow parameters issue 1628
Troubleshoot using counters 1629
View analytics for Web transactions 1629
Detailed web transactions 1630
View events 1632
Add columns in the event list 1636
Advanced search 1637
Save search 1640
Export data 1641
Detailed procedures to setup dual tier or service mesh lite topology 1641
Software requirements 1641
Before you begin 1641
Software requirements 1642
Before you begin 1643
Configure static routes in NetScaler ADM 1643
Download the sample deployment files from GitHub 1645
Add parameters in CPX YAML file 1645
Add VPX or SDX or MPX or BLX instance in NetScaler ADM 1647
Add Kubernetes cluster in NetScaler ADM 1647
Deploy a sample microservice application 1650

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy CPX and register CPX in ADM 1651

Enable auto select virtual servers for licensing 1651

Enable Web Transaction and TCP Transaction settings 1652

Send traffic to microservices 1652

Detailed procedures to set up service mesh topology 1653

Configure static routes in NetScaler® ADM 1653

Configure the required parameters 1654

Deploy a sample application 1656

Add Kubernetes cluster in NetScaler ADM 1658

Enable auto select virtual servers for licensing 1661

Enable Web Transaction and TCP Transaction settings 1662

Send traffic to microservices 1663

Detailed procedures to set up single tier or unified ingress topology 1664

Add VPX or SDX or MPX or BLX instance in NetScaler® ADM 1664

Add Kubernetes cluster in NetScaler ADM 1664

Optional telemetry data for NetScaler® telemetry program 1667

NetScaler Console feature usage 1667

Required telemetry data for NetScaler® telemetry program 1674

Licensing 1675

NetScaler Gateway feature usage 1678

NetScaler deployment 1679

NetScaler feature usage 1681

Data governance 1688

Configure customer identity 1689

Workflow 1 - If you are a new user 1689

Workflow 2 - if you are an existing user upgrading to the latest ADM version 1690

Diagnostics and data collection 1690

Why data is collected? 1691

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Who can use this data? 1691
How long we keep your data? 1692
Database optimization using maintenance scripts 1692
Customer User Experience Improvement Program 1692
What usage-data is collected over CUXIP? 1692
How CUXIP helps you? 1693
How CUXIP works? 1693
How can I disable CUXIP on my ADM? 1693
Changes to our Privacy Policy 1693
References 1693
Back up and restore a NetScaler® ADM configuration in an HA pair 1694
Configure system notification settings 1695
Use jobs to upgrade NetScaler instances 1699
Create an upgrade maintenance job to upgrade ADC instances 1700
Clean up the ADC disk space 1708
Scheduling upgrade jobs for a NetScaler high-availability pair 1710
Download a consolidated diff report of an ADC upgrade job 1711
Configure sites for geomaps 1712
Modes of telemetry collection 1713
Automated telemetry collection mode 1713
Manual telemetry collection mode 1718
Notifications for telemetry uploads 1720

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release notes

The NetScaler Console 13.1 release notes describe the new features, enhancements to existing features, and the known issues in a build. The release notes document for the 13.1 release includes the following sections:

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

NOTE:

These release notes do not document security related fixes. For a list of security related fixes and advisories, see the security bulletin. NetScaler Console Security Advisory supports identification and remediation of CVEs. For more information about the latest and existing supported CVEs, see Supported CVEs through Security Advisory.

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

RELEASE NOTES FOR NETSCALER CONSOLE ON-PREM SOFTWARE VERSION 13.1	PUBLISHED DATE
Build 13.1-62.27	Mar 25, 2026
Build 13.1-61.28	Mar 26, 2026
Build 13.1-60.33	Mar 26, 2026
Build 13.1-59.19	Jun 25, 2025
Build 13.1-58.32	Jun 17, 2025
Build 13.1-57.26	Feb 04, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE NOTES FOR NETSCALER CONSOLE ON-PREM SOFTWARE VERSION 13.1	PUBLISHED DATE
Build 13.1-56.18	Nov 18, 2024
Build 13.1-55.29	Sep 23, 2024
Build 13.1-54.29	Jul 22, 2024
Build 13.1-53.24	Jul 09, 2024
Build 13.1-52.19	Mar 12, 2024
Build 13.1-51.14	Dec 14, 2023
Build 13.1-50.23	Oct 20, 2023
Build 13.1-49.13	Jul 18, 2023
Build 13.1-48.47	Jun 14, 2023
Build 13.1-45.61	Apr 26, 2023
Build 13.1-42.47	Mar 23, 2023
Build 13.1-37.38	Dec 01, 2022
Build 13.1-33.50	Oct 31, 2022
Build 13.1-30.52	Oct 31, 2022
Build 13.1-27.62	Oct 31, 2022
Build 13.1-24.38	Oct 31, 2022
Build 13.1-21.53	Oct 31, 2022
Build 13.1-17.42	Oct 31, 2022
Build 13.1-12.50	Oct 31, 2022
Build 13.1-9.60	Oct 31, 2022

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE NOTES FOR NETSCALER CONSOLE ON-PREM SOFTWARE VERSION 13.1	PUBLISHED DATE
Build 113.1-4.43	Sep 14, 2021

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate on-premises NetScaler ADM to Citrix Cloud™

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

ADM service through Citrix Cloud enables you to get:

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

For a successful migration, you must:

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

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

Configure the ADM service agent

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Get the client and secret CSV file from Citrix Cloud

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

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

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

Validate the ADM service licenses

You must obtain licenses for ADM service.

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

  NOTE

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

- If you use ADM on-premises deployment as a license server, reallocate your licenses to ADM Service before migration. For more information, see Configure an ADM server only as the pooled license server and How to reallocate a license file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you are using the pooled licenses in on-premises ADM, you must obtain the pooled licenses for ADM service and then allocate licenses to the ADC instances. For more information, see Configure Pooled Licensing. The following supported ADC versions enable you to modify the license allocation from ADM:
  - NetScaler SDX: 13.0 74.11 or later versions.
  - NetScaler VPX and MPX: 13.0 47.24 or later versions, 12.1 58.14 or later versions, and 11.1 65.10 or later versions.

Migrate using a script

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

  Note

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

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

   Note

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Note

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

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

   a. `cd /mps/scripts`

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

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

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

```
-------------------------------------------------------
Checking For Pre-requisites before we start the Migration
-------------------------------------------------------

The no.of Agents in ADM Service are :1


VIP licenses available in ADM Service are: 2

No.of Vservers Licensed in ADM on-prem are: 72


All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
vServers will be licensed randomly. Do you want to continue ? [Y|N] y


User has started rerunning the migration.Providing the all options


-------------------------------------------------------------------------------
Citrix ADM on-prem to ADM Service Configuration Migration.
The following menu enables you to select the components to migrate.
Type the number of the component that you want to migrate, and then press Enter.
For example, type 1 if you want to migrate Management and Monitoring(M&M).
-------------------------------------------------------------------------------

    1. Management and Monitoring(M&M).
    2. Analytics.
    3. Stylebooks.
    4. PooledLicensing.
    5. All.

Select an option from 1 to 5 [1]: 1
```

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
1. Management and Monitoring Module Migration to ADM Service is Complete.
=========================================================================


ADCs,SDXs and SDWANOPs Addition and their SNMP,Syslog Configurations to ADM Service are Successful. Tool will now disable System Features in ADM on-prem

Device_Events : ['SUCCESS']
Device_SSL_Cert : ['SUCCESS']
Device_Syslog : ['SUCCESS']
Device_Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device_Perf_Reporting : ['SUCCESS']
Device_Config_Audit : ['SUCCESS']
Emon_Scheduler : ['SUCCESS']

Disable Status of ADM System Features: {'Device_Events': "['SUCCESS']", 'Device_SSL_Cert': "['SUCCESS']", 'Device_Syslog': "['SUCCESS']", 'Device_Backup': "['SUCCESS']", 'AgentCluster':
 "['SUCCESS']", 'Device_Perf_Reporting': "['SUCCESS']", 'Device_Config_Audit': "['SUCCESS']", 'Emon_Scheduler': "['SUCCESS']"}
1620286058


==============================================================
ADM on-prem to ADM service Migration is Successfully Completed.
==============================================================



--------------------------------------------------------------------------------
ADM On-rem to ADM Service Configuration Migration is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

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

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

The **Analytics** feature includes:

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

Note:

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

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

   a. `cd /mps/scripts`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

   a. Download the migration script from the following location: `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

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

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

   c. Run the following commands to migrate:

      i. `cd /var`

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

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

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

```
bash-3.2# python servicemigrationtool.py /var/baga.csv

 Trying to Get the Customer Id...


 The Customer Id: iaahfc73d8f4

 ADM Service FQDN: baga.adm.cloud.com

 The ADM on-prem IP: 10.106.150.37


 Citrix ADM Deployed with No Agents



-------------------------------------------------------
Checking For Pre-requisites before we start the Migration
-------------------------------------------------------

 The no.of Agents in ADM Service are :1


 VIP licenses available in ADM Service are: 2

 No.of Vservers Licensed in ADM on-prem are: 26


 All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
 vServers will be licensed randomly. Do you want to continue ? [Y|N]
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

- SSL certificates
- Syslog messages
- Backup
- Agent cluster
- Performance reporting

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configuration audit
- `Emon` scheduler

Roll back to onpremises ADM

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

Prerequisites

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

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

Use the rollback script

Note

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. cd /mps/scripts

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

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

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

```
bash-3.2# python rollback_to_onprem.py /var/tmp/baga_prod.csv

The Customer Id: iaahfc73d8f4

ADM Service FQDN: baga.adm.cloud.com

The ADM on-prem IP: 10.106.150.10

-----------------------------------------------------------------------------------------------------------------------------------------------------------------
On successful rollback operation,Instances will be removed from ADM Service. SNMP,Syslog,Analytics configurations and Pooled Licensing Server in Instances will point to on-prem ADM Serv
er and reports will be shown in ADM on-prem.
-----------------------------------------------------------------------------------------------------------------------------------------------------------------


Do you want to proceed for roll back operation from ADM Service to ADM on-prem ? [Y|N] y
-----------------------------------------------------------------------------
```

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

```
==========================Rollback Status Check================================


Removal of ADCs,SDXs,SDWANOPs and their respective Configurations from ADM Service are Successful.


Rollback operation from ADM Service to ADM on-prem is Successful


Enabling System features in ADM on-prem Server
Device_Events : ['SUCCESS']
Device_SSL_Cert : ['SUCCESS']
Device_Syslog : ['SUCCESS']
Device_Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device_Perf_Reporting : ['SUCCESS']
Device_Config_Audit : ['SUCCESS']
Emon_Scheduler : ['SUCCESS']

Enable Status of ADM System Features: {'Device_Events': "['SUCCESS']", 'Device_SSL_Cert': "['SUCCESS']", 'Device_Syslog': "['SUCCESS']", 'Device_Backup': "['SUCCESS']", 'AgentCluster':
"['SUCCESS']", 'Device_Perf_Reporting': "['SUCCESS']", 'Device_Config_Audit': "['SUCCESS']", 'Emon_Scheduler': "['SUCCESS']"}

-------------------------------------------------------------------------------------
ADM Service to ADM on-prem Rollback operation is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
-------------------------------------------------------------------------------------

bash-3.2#
```

4. For ADM earlier than 82.xx build:

   a. Download the rollback script from the following location:

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

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

      i. `cd /mps/scripts`

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. `cd /var`

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

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

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

FAQs

ADM service

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

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

Why ADM service?

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What happens if the agent goes down for any reason?

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

Is instance backup also migrated?

Backup is not included in migration.

Is historical data also migrated?

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

Are on-premises licenses also migrated?

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

What is not migrated from on-premises NetScaler ADM?

The following features cannot be migrated to ADM service:

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Migration tool

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

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

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

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

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

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

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

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

Yes. After you rerun the script, only the failed instances are migrated. Let’s assume that two out of five instances have failed to move. After you have taken corrective actions and rerun the migration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

script, three instances that were moved successfully earlier show the “Device already exists” message. And the other two instances that failed earlier are migrated successfully.

Is there a log file to check the migration status?

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

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

Rollback script

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

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

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

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

Troubleshooting

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

Note

> If you see an error message that displays “already exists”, it means that:

- You might have run the migration script for more than one time and some configurations are already migrated to ADM service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might have manually created the same configuration in ADM service, before running the migration script.

Refer to some of the following error messages:

Manual profile added to ADM service

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


60.26 : FAILURE : Profile 60.26 already exists


 The list of ADC profiles added to ADM Service are :

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

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

NetScaler device added to ADM service

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

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


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

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

StyleBook custom templates import to ADM service

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


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

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

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}
==============Stylebook repository Addition to ADM Service====================
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Jobs added to ADM service

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


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

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

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

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

IP blocks added to ADM service

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


ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

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

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

Network dashboard report addition status

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


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All how to articles

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

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

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

Instance management

How to monitor globally distributed sites

How to manage admin partitions of NetScaler instances

How to add instances to NetScaler ADM

How to create instance groups on NetScaler ADM

How to configure sites for Geomaps in NetScaler ADM

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

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

How to back up and restore an instance using NetScaler ADM

How to rediscover multiple NetScaler VPX instances

How to poll NetScaler instances and entities in NetScaler ADM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to unmanage an instance on NetScaler ADM

How to trace the route to an instance from NetScaler ADM

Configuration management

How to create a configuration job on NetScaler ADM

How to use SCP (put) command in configuration jobs

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

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

How to reuse executed configuration jobs

How to upgrade NetScaler instances using NetScaler ADM

How to use variables in configuration jobs on NetScaler ADM

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

How to create configuration jobs from corrective commands on NetScaler ADM

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

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

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

How to use the master configuration template on NetScaler ADM

How to poll configuration audit of NetScaler instances

How to reuse configuration audit templates in configuration jobs

How to import and export configuration templates

How to generate configuration audit diff for ConfigChange SNMP traps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate management

How to configure an enterprise policy on NetScaler ADM

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

How to update an installed certificate from NetScaler ADM

How to link and unlink SSL certificates by using NetScaler ADM

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

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

How to use the SSL dashboard on NetScaler ADM

How to poll SSL certificates from NetScaler Instances

StyleBooks

How to view different groups of StyleBooks

How to create your own StyleBooks

How to use user-defined StyleBooks in NetScaler ADM

How to use API to create configurations from StyleBooks

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

How to create a StyleBook to upload files to NetScaler ADM

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

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

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

How to use Microsoft Skype for Business StyleBook in business enterprises

How to use Microsoft Exchange StyleBook in business enterprises

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use Microsoft SharePoint StyleBook in business enterprises

Analytics

How to enable analytics on instances

How to configure adaptive thresholds

How to configure SLA management

How to configure database summarization for analytics

How to create thresholds and alerts using NetScaler ADM

How to disable URL data collection for analytics from NetScaler ADM

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

How to view the peak data rate for a particular time framehttps://author-p185304-e1959210.adobeaemcloud.com/en-us/netscaler-application-delivery-management-software/13-1/analytics/video-insight/view-peak-data-rate-specific-time-frame.html

How to view the network efficiency

Event management

How to set event age for events on NetScaler ADM

How to schedule an event filter by using NetScaler ADM

How to set repeated email notifications for events from NetScaler ADM

How to suppress events by using NetScaler ADM

How to use the events dashboard to monitor events

How to create event rules on NetScaler ADM

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

How to view the events summary in NetScaler ADM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

How to export syslog messages using NetScaler ADM

How to suppress syslog messages in NetScaler ADM

How to configure prune settings for instance events

Authentication

How to enable fallback and cascade external authentication servers

How to add RADIUS authentication servers

How to add LDAP authentication servers

How to add TACACS authentication servers

How to extract authentication server group in NetScaler ADM

How to enable fallback local authentication

NetScaler ADM system

How to upgrade NetScaler ADM

How to reset the password for NetScaler ADM

How to generate a tech support file for NetScaler ADM

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

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

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

How to configure NTP server on NetScaler ADM

How to configure SSL settings for NetScaler ADM

How to configure syslog purging interval for NetScaler ADM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to view auditing information of NetScaler ADM

How to configure system notification settings of NetScaler ADM

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

How to configure a cipher group for NetScaler ADM

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

How to assign a host name to a NetScaler ADM server

How to configure system prune settings for NetScaler ADM

How to configure system backup settings by using NetScaler ADM

How to configure and view system alarms on NetScaler ADM

Network functions

How to generate reports for load balancing entities

How to export or schedule export of network functions reports

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview

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

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

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

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

Features and solutions

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

Application Analytics and Management

Application performance analytics

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

Application security analytics

The App Security Dashboard provides a holistic view of the security status of your applications. For example, it shows key security metrics such as security violations, signature violations, threat

© 1997–2026 Citrix Systems, Inc. All rights reserved.

indexes. App Security dashboard also displays attack related information such as SYN attacks, small window attacks, and DNS flood attacks for the discovered ADC instances.

Networks

Instances

Enables you to manage the NetScaler and NetScaler Gateway instances.

Instance groups

Enables you to group your instances as follows:

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

Event management

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

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

Certificate management

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

Configuration management

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

Configuration audit

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Network reporting

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

Analytics

Web Insight

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

HDX Insight

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

Gateway Insight

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

Security Insight

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

SSL Insight

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

TCP Insight

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Video Insight

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

Orchestration

Cloud Orchestration

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

Orchestration

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

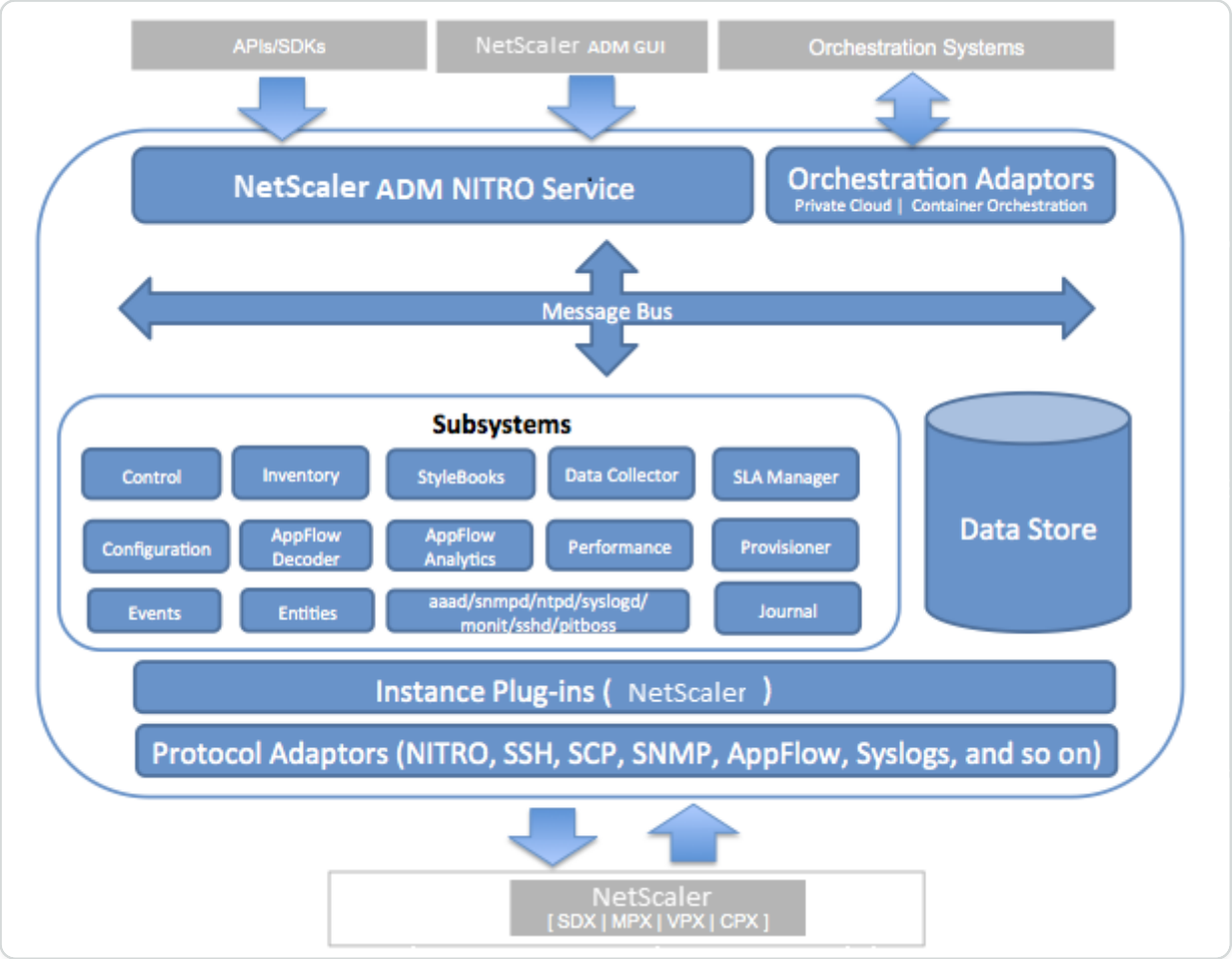
Architecture

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

How NetScaler® ADM discovers instances

Instances are NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Application Delivery Management (ADM). To manage and monitor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

these instances, you must add them to the NetScaler ADM server. You can add the following NetScaler ADC appliances and virtual appliances to ADM:

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

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

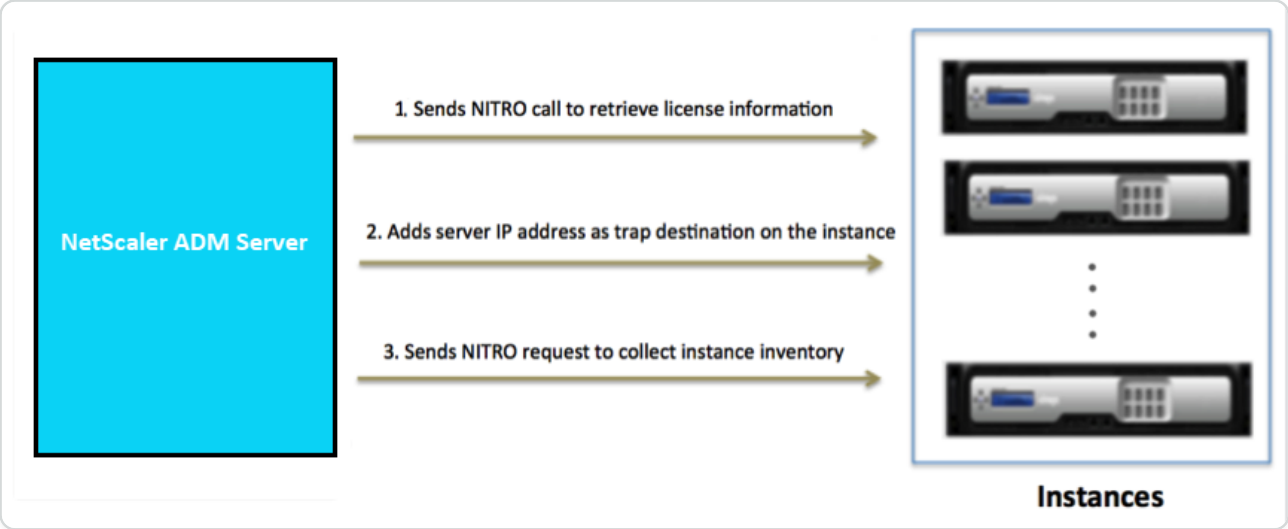
NOTE

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

If you want to add an ADC HA pair using SNIP, ensure to enable the Independent Network Configuration (INC) mode on the ADC HA pair. For more information to add instances, see Add instances.
When you add an instance to the ADM server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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

   NOTE

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

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

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

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

   This step might fail because of network or firewall issues.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Polling overview

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

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

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

How NetScaler® ADM polls managed instances and entities

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

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

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
Instance polling	Every 1 minute (by default)	Statistical information such as state, HTTP requests per second,	NITRO call.	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
		CPU usage, memory usage, and throughput.		
Inventory polling	Every 60 minutes (by default)	Inventory details such as build version, system information, licensed features, and modes.	NITRO calls and SSH	No
Performance data collection	Every 5 minutes (by default)	Network reporting information	NITRO call	No
Instance backup polling	Every 12 hours (by default)	Backup file of the current state of the managed ADC instances	NITRO calls, SSH, and SCP.	Yes. Navigate to **Infrastructure > Instances > NetScaler**. Select the instance and from the **Select Action** list, click **Backup/ Restore**.
Configuration audit polling	Every 10 hours (by default)	Configuration changes that occur on ADC instances (for example, running vs. saved configuration)	SSH, SCP, and NITRO call	Yes. Navigate to **Infrastructure > Configuration Audit**. On the Configuration Audit page, click **Settings** and configure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
				the polling interval for Configuration Audit Polling.
				You can poll configuration audits manually and add all configuration audits of the instances immediately to NetScaler ADM. To do so, navigate to **Infrastructure > Configuration Audit** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network.
SSL certificates polling	Every 24 hours (by default)	SSL certificates that are installed on NetScaler instances.	NITRO calls and SCP	Yes. Navigate to **Infrastructure > SSL Dashboard**. On the SSL Dashboard page, click **Settings** to configure the polling interval

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
				You can poll entities manually and add all entities of the instances immediately to NetScaler ADM. To do so, navigate to **Infrastructure > Network Functions** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network

NOTE

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

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

Different ways of polling instances

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Global polling of instances

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

Manual polling of instances

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

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

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

To poll specific instances in NetScaler ADM:

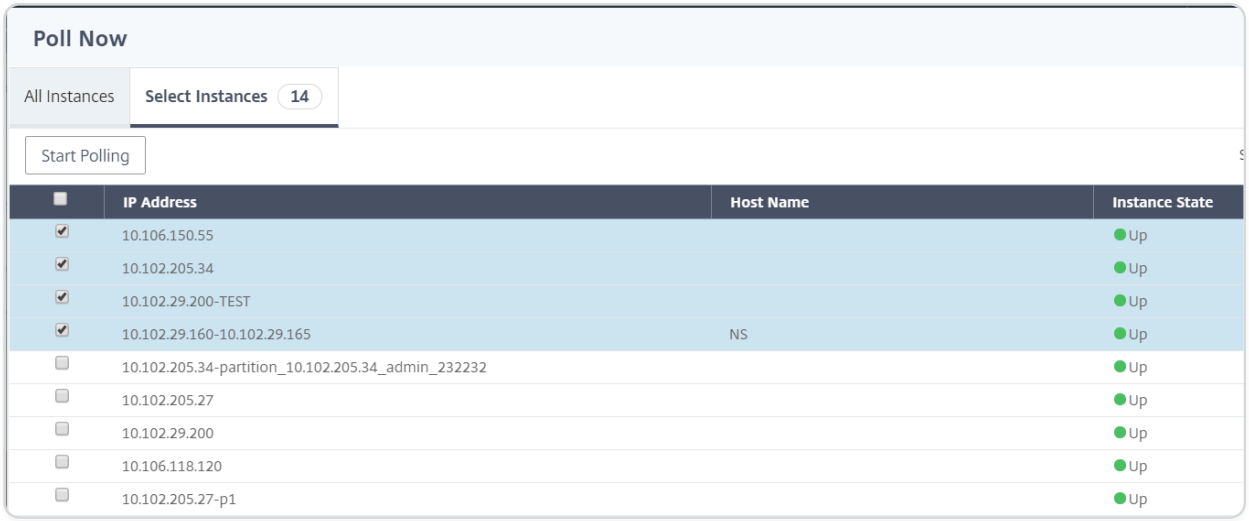
1. In NetScaler ADM, navigate to **Infrastructure > Network Functions**.
2. On **Network Functions** page, at the top right-hand corner, click **Poll Now**.
3. The pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network or poll the selected instances.

    a. **All Instances** tab - click **Start Polling** to poll all the instances.

    b. **Select Instances** tab - select the instances from the list

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Start Polling**.



NetScaler ADM initiates manual polling and adds all the entities.

Manual polling of entities

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

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

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

NOTE

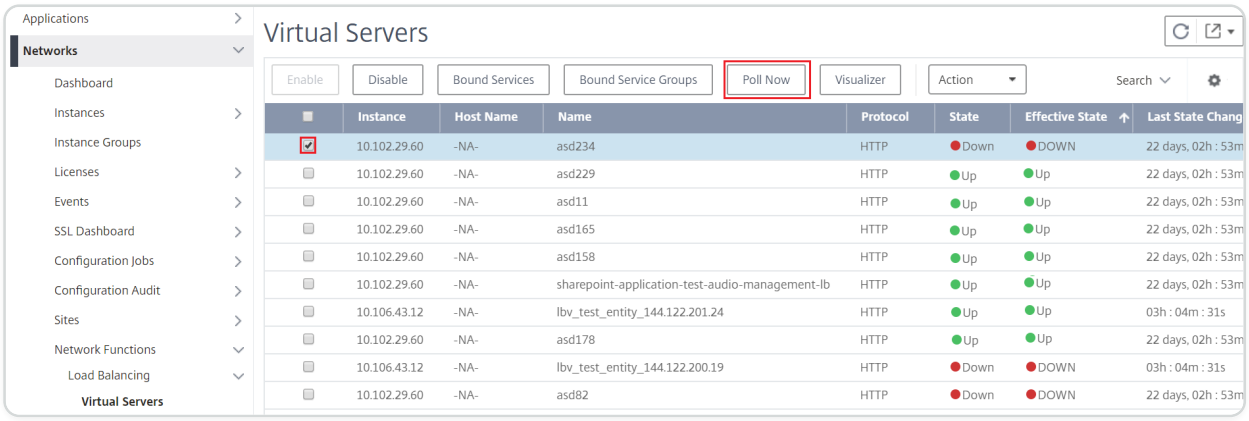
If you poll a virtual server, only that virtual server is polled. The associated entities such as services, service groups, and servers are not polled. If you need to poll all associated entities, you must manually poll the entities or you must poll the instance.

To poll specific entities in NetScaler ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® telemetry program

Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. You may automatically or manually upload the required license and feature usage data to remain compliant with the NetScaler telemetry program described here. NetScaler Console configuration and feature usage data is also collected to manage, measure, and improve Citrix products and services. If you are an existing NetScaler Console customer, you must ensure to be compliant with the NetScaler telemetry program. We highly recommend adding NetScaler instances to NetScaler Console to improve and simplify your NetScaler operations overall and support the enhancement of our products and services by sending NetScaler feature usage data. Learn more.

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

- **Automated collection mode** - This mode is enabled by default after you upgrade to **14.1-25.53 or later** / **13.1-53.22 or later** build. The automated mode creates an outbound connection to use the auto-enabled channel (endpoint URLs) and uploads the telemetry data automatically. You must only ensure that the endpoint URLs are reachable. Since the upload happens automatically, no action is required from your end unless the prerequisites fail. For more information, see Automated collection mode.
- **Manual collection mode** - This mode is enabled only if the automated mode is disabled. You must download the required telemetry data from the NetScaler telemetry home page in NetScaler Console on-prem and complete the first upload to NetScaler Console service within 30 days. The subsequent uploads must be done every 90 days to remain compliant. For more information, see Manual collection mode.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As part of the NetScaler telemetry program, the following configurations were pushed to the managed NetScaler instances:

- AppFlow configuration: `enable ns feature AppFlow`
- Telemetry metrics profile configuration: `add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metricsENABLED -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300`

NOTE:

For optimal telemetry collection, we recommend that you upgrade to the latest NetScaler Console build.

- Starting from **13.1-57.x** build, NetScaler Console removes the telemetry metrics profile configuration if it is present in your NetScaler instances. The removal of telemetry metrics profile configuration does not impact any existing features in your NetScaler instances.
- If you are not using the NetScaler or NetScaler Console analytics features, you can use the following command to remove the AppFlow configuration:

  `disable ns feature AppFlow`

The following table provides details about the AppFlow® and Telemetry metrics profile configurations in the latest build and earlier builds:

BUILD	CONFIGURATIONS PUSHED AS PART OF TELEMETRY PROGRAM	TELEMETRY MODE	ACTION REQUIRED
13.1-57.x	No	Automated and manual	Configurations are not pushed to NetScaler instances and the telemetry metrics profile configuration is removed from NetScaler instances if it is present. If you are not using the NetScaler or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BUILD	CONFIGURATIONS PUSHED AS PART OF TELEMETRY PROGRAM	TELEMETRY MODE	ACTION REQUIRED
			NetScaler Console analytics features, you can use `disable ns feature AppFlow` to remove the AppFlow configuration.
13.1-55.x	No	Automated and manual	Configurations are not pushed as part of the NetScaler telemetry program. If these configurations are present in your NetScaler instances and you want to remove these configurations, run the `rm analytics profile telemetry_metrics_profile` command on NetScaler to remove the telemetry metrics profile configuration and use `disable ns feature AppFlow` to remove the AppFlow configuration.
13.1-53.22	Yes. Both AppFlow and telemetry metrics profile configurations	Automated (with all prerequisites met)	Configurations are pushed as part of the NetScaler telemetry program, but not checked for every 24

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BUILD	CONFIGURATIONS PUSHED AS PART OF TELEMETRY PROGRAM	TELEMETRY MODE	ACTION REQUIRED
			hours. To remove these configurations, run the `rm analytics profile telemetry_metrics_profile` command on NetScaler to remove the telemetry metrics profile configuration and use `disable ns feature AppFlow` to remove the AppFlow configuration.
		Automated (with any prerequisites not met) or manual	NetScaler Console continues to check for these configurations every 24 hours and push it to NetScaler instances, if these configurations are missing. If you do not want the configurations to be pushed, you must be in the automated mode (with all prerequisites met) or upgrade to the latest build.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- The `/nsconfig/.telemetry.conf` file is updated with the following command for the Gateway telemetry. NetScaler Console checks for this command every hour and adds it, if this command is missing:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Some telemetry parameters are collected through scripts that are pushed from NetScaler Console to NetScaler instances. These scripts are read-only and do not change anything in NetScaler.
- The information collected through telemetry, such as email addresses, user names, and IP addresses, is securely pseudonymised by hashing the information at the source using one-way hashing algorithms. As a result, Citrix cannot access or read these values. This telemetry data is used solely for logical asset-matching purposes.

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

CATEGORIES	DESCRIPTION	WHAT DO WE USE IT FOR?	REQUIRED/ OPTIONAL
License, and NetScaler deployment and usage telemetry	Information about license entitlement, allocation, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Points to note:

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data governance

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

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

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

NOTES:

- After you upgrade to NetScaler Console **14.1-25.53 or later** / **13.1-53.22 or later** build, the following configuration is automatically pushed to your NetScaler instances through NetScaler Console. This configuration collects and stores the telemetry metrics in your NetScaler instances:

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- If you are in manual mode or automated mode (with any prerequisite not met), NetScaler Console continues to check for the above configuration every 24 hours and push it to NetScaler instances, if this configuration is missing. If you do not want the configuration to be pushed, you must be in the automated mode (with all prerequisites met) or upgrade to the upcoming build (**14.1-29.x** or **13.1-55.x**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `/nsconfig/.telemetry.conf` file is updated with the following command for the Gateway telemetry. NetScaler Console checks for this command every hour and adds it, if this command is missing:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Some telemetry parameters are collected through scripts that are pushed from NetScaler Console to NetScaler instances. These scripts are read-only and do not change anything in NetScaler.
- The information collected through telemetry, such as email addresses, usernames, and IP addresses, is securely pseudonymised by hashing the information at the source using one-way hashing algorithms. As a result, Citrix cannot access or read these values. This telemetry data is used solely for logical asset-matching purposes.

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

CATEGORIES	DESCRIPTION	WHAT DO WE USE IT FOR?	REQUIRED / OPTIONAL
License, and NetScaler deployment and usage telemetry	Information about license entitlement, allocation, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

To disable the optional parameters:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing

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

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

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

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

Points to note:

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

Post upgrade to build 13.1-12.x:

- All the Express default free virtual servers remain functional for 30 days. You can select the 2 virtual servers and apply the 2 default licenses within the 30 days grace period. If no user action is taken 30 days post upgrade, ADM randomly applies license to 2 virtual servers and unlicenses the remaining virtual servers. You must buy and apply new Advanced licenses to enable these virtual servers.
- Post upgrade, the following are the changes in the ADM behavior:
    - ADM enforces a 30-day grace period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Within the 30-day grace period, the allocation of new virtual servers for the 30 express free virtual servers is blocked.
  - For example, if the number of available virtual server licenses before you upgraded to 12.x was 30 and only 20 licensed virtual servers were used, you are only allowed to use the 20 virtual servers and not allowed to license the remaining 10 virtual servers in the 30-day grace period.
- However, within the 30-day grace period, as an administrator, you can still apply Advanced ADM licenses and allocate new virtual servers.

FEATURES	OPTIONS	EXPRESS EDITION	ADVANCE EDITION	NETSCALER LICENSE
Applications	Application Dashboard	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NetScaler Web App Firewall related information on App Dashboard needs Premium (or) Advanced with App Firewall license.
	Web Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
	Service Graph	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
	Configuration > StyleBooks	Unlimited	Unlimited	NA
Security	Security Dashboard	Up to two virtual servers.	Entitled for all purchased	NetScaler Web App Firewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURES	OPTIONS	EXPRESS EDITION	ADVANCE EDITION	NETSCALER LICENSE
			virtual server licenses and extra two virtual servers.	related information on Security Dashboard needs Premium (or) Advanced with App Firewall license.
	Security Violations	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Premium (or) Advanced with App Firewall license
	Users and endpoints	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
Gateway	HDX Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
	Gateway Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
Infrastructre	Infrasturcture Analytics	Unlimited	Unlimited	NA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURES	OPTIONS	EXPRESS EDITION	ADVANCE EDITION	NETSCALER LICENSE
	Instances	Unlimited	Unlimited	NA
	SSL Dashboard	Unlimited	Unlimited	NA
	Events	Unlimited	Unlimited	NA
	Network Functions	Unlimited	Unlimited	NA
	Network Reporting	Unlimited	Unlimited	NA
	Pooled licenses	Unlimited	Unlimited	NA
	Configuration > Configuration Jobs, Configuration Templates, and Configuration Advice	Unlimited	Unlimited	NA
	Upgrade Jobs	Unlimited	Unlimited	NA
	Orchestration	Unlimited	Unlimited	NA
Settings	RBAC & External Authentication (instance level)	Unlimited	Unlimited	NA
	RBAC & External Authentication	Unlimited	Unlimited	NA

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

High Availability

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

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

NOTE

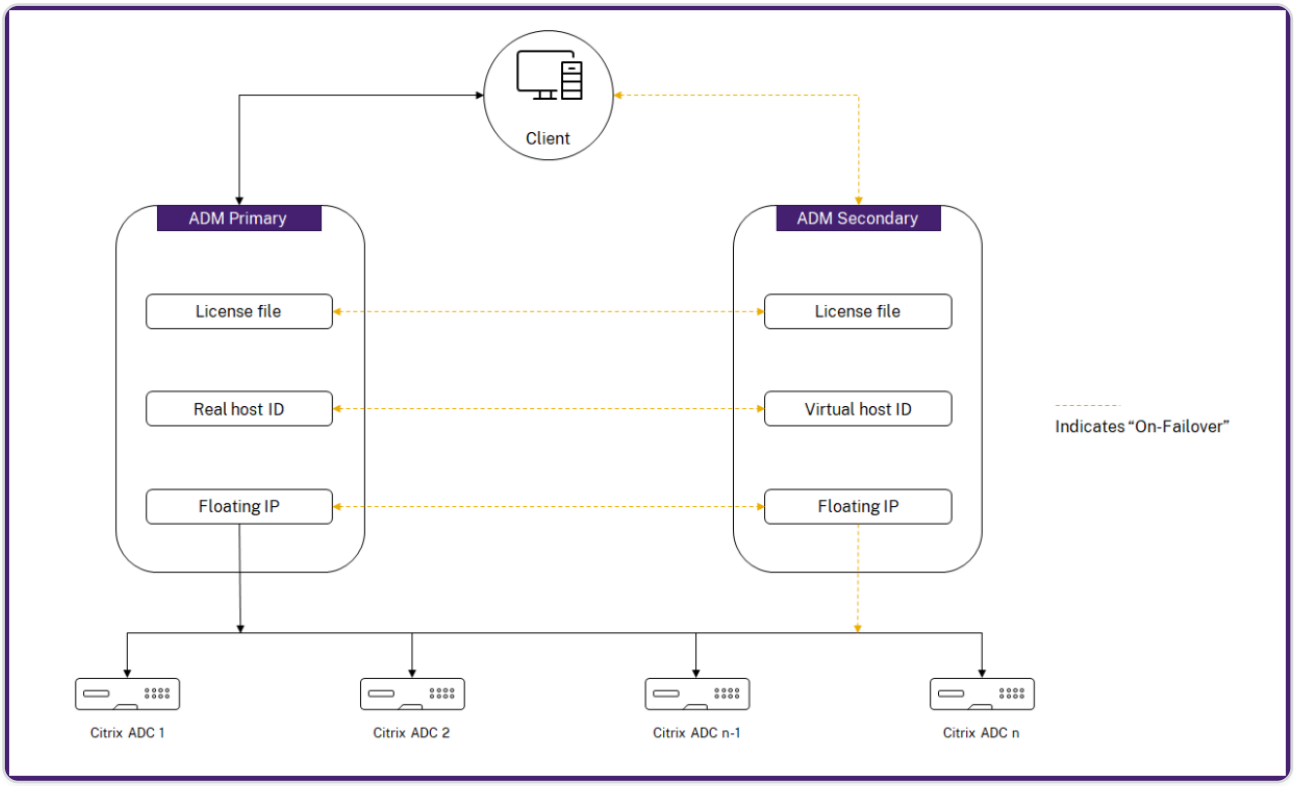
- If you have installed NetScaler ADM 12.1.49.x or earlier releases, you get a grace period of 30 days to maintain the licensing on the secondary node. After the grace period, you must contact Citrix to rehost the original license.
- For 12.1.50.x or later releases, the NetScaler ADM license is automatically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

How licenses are synchronized between ADM high-availability nodes?

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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

Orchestration

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade the virtual server licenses

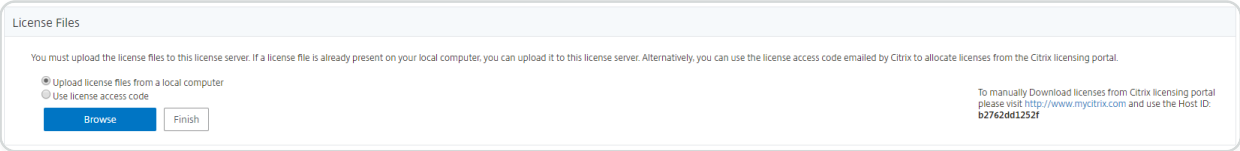
You can upgrade the licensing on NetScaler ADM to monitor and manage more virtual servers hosted on the NetScaler appliances.

To upgrade your appliance licenses:

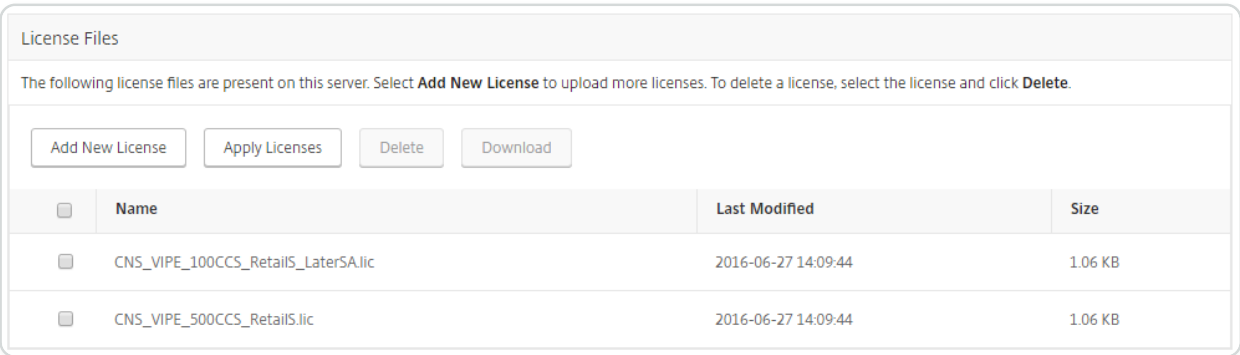
1. Log on to NetScaler ADM using the administrator credentials.
2. Navigate to **Infrastructure > Pooled Licensing**.
3. Go to **License Files**, and select one of the following options:
   - **Upload license files from a local computer**. If a license is already present on your local computer, click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

NOTE

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



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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verification

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

Manage virtual servers

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

POINTS TO NOTE

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

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

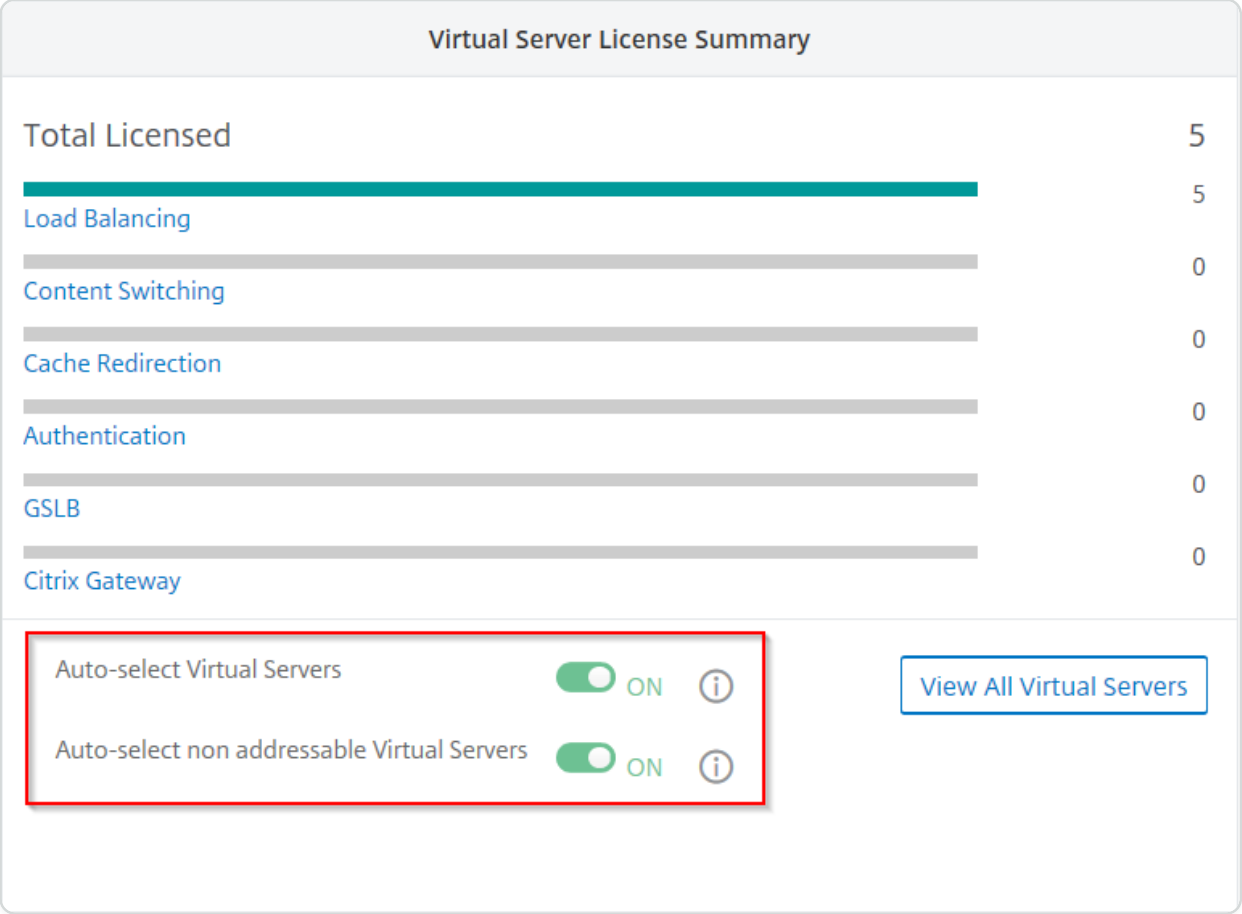
Disable auto-licensing virtual servers

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



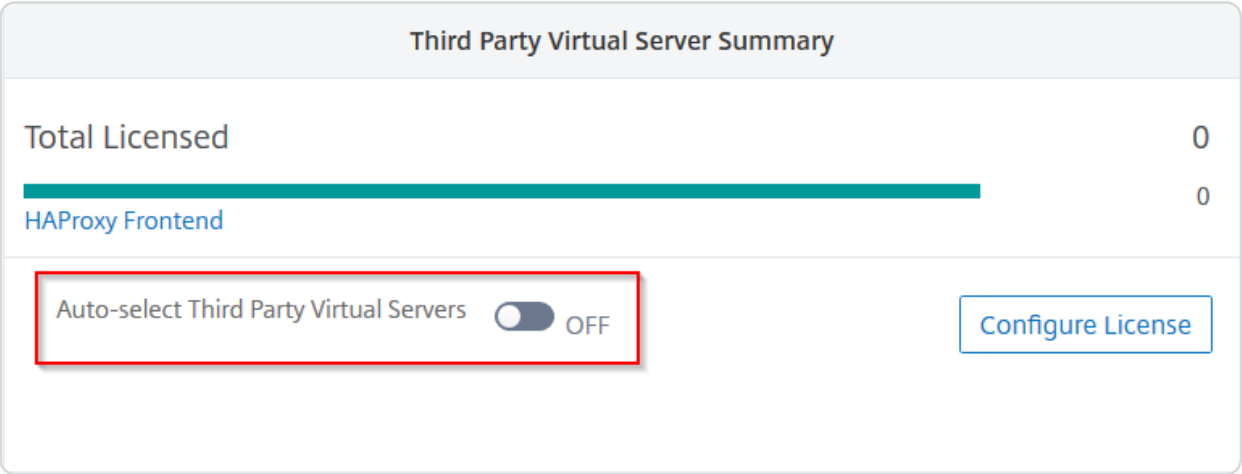
Select third-party virtual servers for licensing

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Apply virtual server licenses manually

You can manually apply licenses to an individual virtual server.

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

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

Configure policy based virtual server licensing

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

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

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

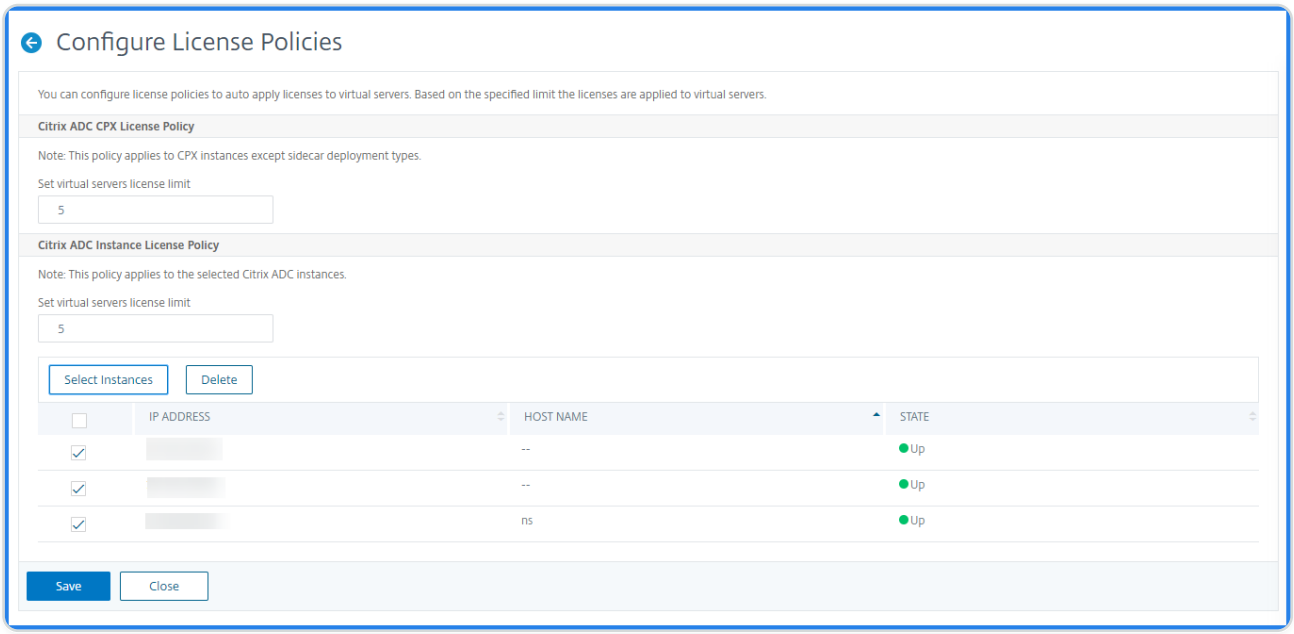
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

This limit applies to CPX instances except sidecar deployment types.

To view CPX instances of sidecar deployment types, filter the virtual servers using the property: `License Type: Freely Managed`.

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



View the licensed virtual servers

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure auto license support for non-addressable virtual servers

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

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

NOTE

- NetScaler ADM, by default, still does not automatically select non-addressable virtual servers for licensing.
- Application analytics (App Dashboard) is the only analytics supported currently on licensed non-addressable virtual servers.

Expiry Checks for virtual server licenses

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

To view the status of the licenses:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure the notification settings of licenses:

1. Navigate to **Infrastructure > Pooled Licensing > Settings**.
2. In the **Notification Settings** section, click the pencil icon and edit the parameters.

    - **Email profile:** Email profile or distribution list for sending notifications when licenses reach the threshold, or going to expire.
    - **SMS (Text Message):** SMS profile or distribution list for sending notifications when licenses reach the threshold, or going to expire.
    - **Slack** - Specify Slack profile details.
    - **PagerDuty alerts** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
    - **Notify me:** Set the percentage of pooled licenses to notify administrators by Email or SMS.
    - **License Expiry Threshold:** Number of days before the number of licenses determined by Alert Threshold expire.
    - **Expiry of licenses:** Number of days remaining before expiry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System requirements

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

Requirements for NetScaler ADM

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
	Note: Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.
Storage space	The default storage space required is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation.
	If your NetScaler ADM storage requirement exceeds 120 GB, you to have to attach an additional disk. You can add only one additional disk.
	Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment.
	For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements for NetScaler ADM on-prem agent

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual network interfaces	1
Throughput	1 Gbps

NOTE

AMD processor is supported in:

- **NetScaler ADM 13.1 build 4.43 or later**.
- **NetScaler agent 13.1 build 17.42 or later**.

Minimum NetScaler version required for NetScaler ADM features

IMPORTANT

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

NETSCALER ADM FEATURE	NETSCALER SOFTWARE VERSION
StyleBooks	10.5 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER ADM FEATURE	NETSCALER SOFTWARE VERSION
OpenStack/CloudStack Support	11.0 and later, if a partition is required
	11.1 and later, if partition on shared virtual LAN is required
NSX Support	11.1 Build 47.14 and later (VPX)
Mesos/Marathon Support	10.5 and later
Backup/Restore	For NetScaler, 10.1 and later
	For NetScaler SDX, 11.0 and later
Monitoring/Reporting and Configuration using Jobs	10.1 and later
Analytics Features	
Web Insight	10.5 and later
HDX Insight	10.1 and later
WAF Security Violations	11.0.65.31 and later
Gateway Insight	11.0.65.31 and later
Cache Insight	10.5 and later*
SSL Insight	12.0 and later

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements for NetScaler ADM analytics

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

NETSCALER ADM FEATURE	CITRIX VIRTUAL APPS AND DESKTOPS VERSION
HDX Insight	Citrix Virtual Apps and Desktops 7.0 and later

NOTE

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

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

Thin clients supported for HDX™ insight

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux based Thin Clients
- Dell Wyse ThinOS based Thin Clients
- 10ZiG Ubuntu based Thin Clients

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

NetScaler instance license required for HDX insight

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

NETSCALER LICENSE/ DURATION	5 MINUTES	1 HOUR	1 DAY	1 WEEK	> 1 MONTH
Standard	No	No	No	No	No
Advanced	Yes	Yes	No	No	No
Premium	Yes	Yes	Yes	Yes	Yes

Supported hypervisors

The following table lists the hypervisors supported by NetScaler ADM.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported operating systems and Workspace versions

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

OPERATING SYSTEM	WORKSPACE VERSION
Windows	4.0 Standard Edition
Linux	13.0.265571 and later
Mac	11.8, build 238301 and later
HTML5	1.5
Chrome App	1.5

Supported browsers

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

WEB BROWSER	VERSION
Microsoft Edge	79 and later
Google Chrome	51 and later
Safari	10 and later
Mozilla Firefox	52 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

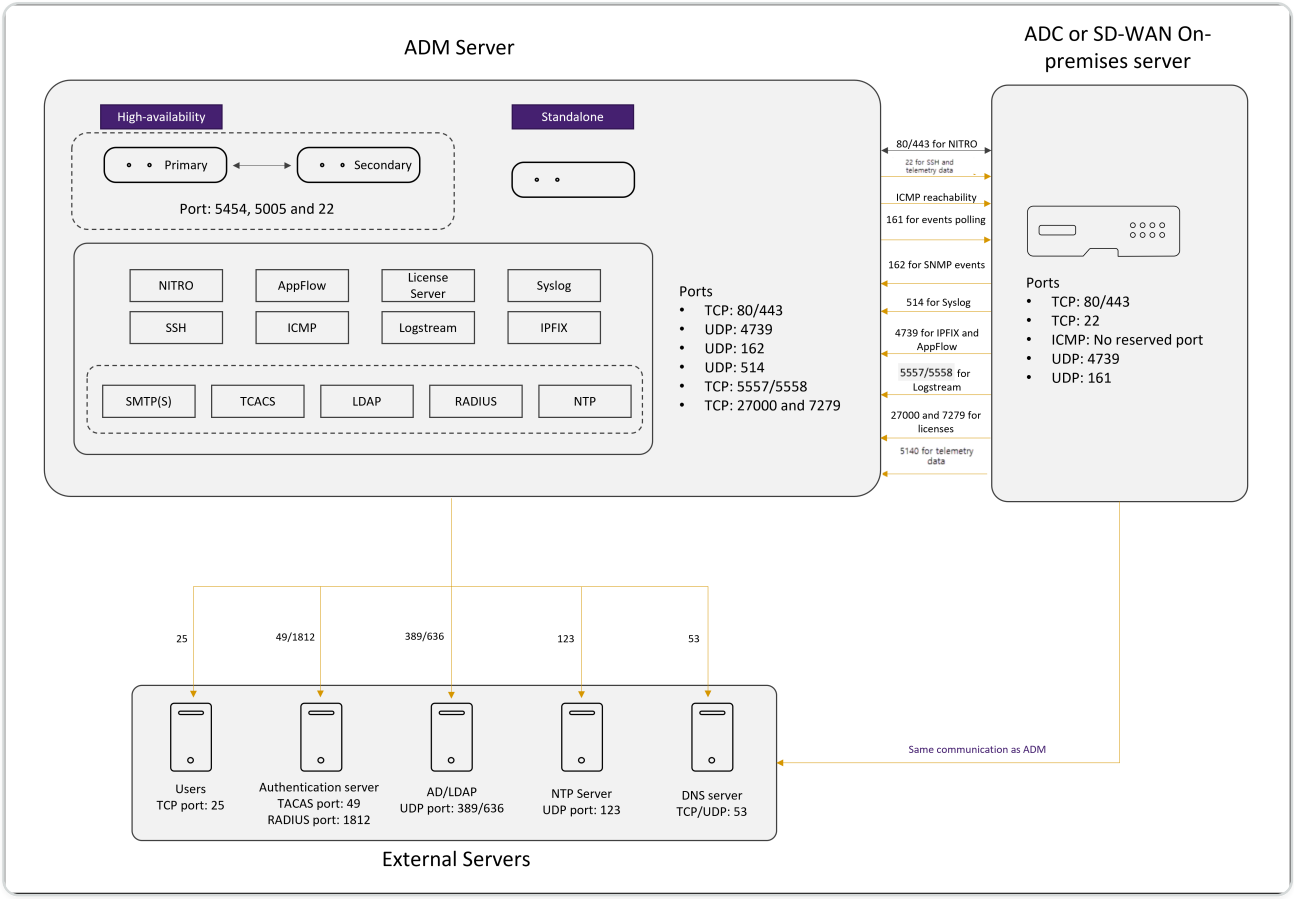
Supported ports

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

NOTE

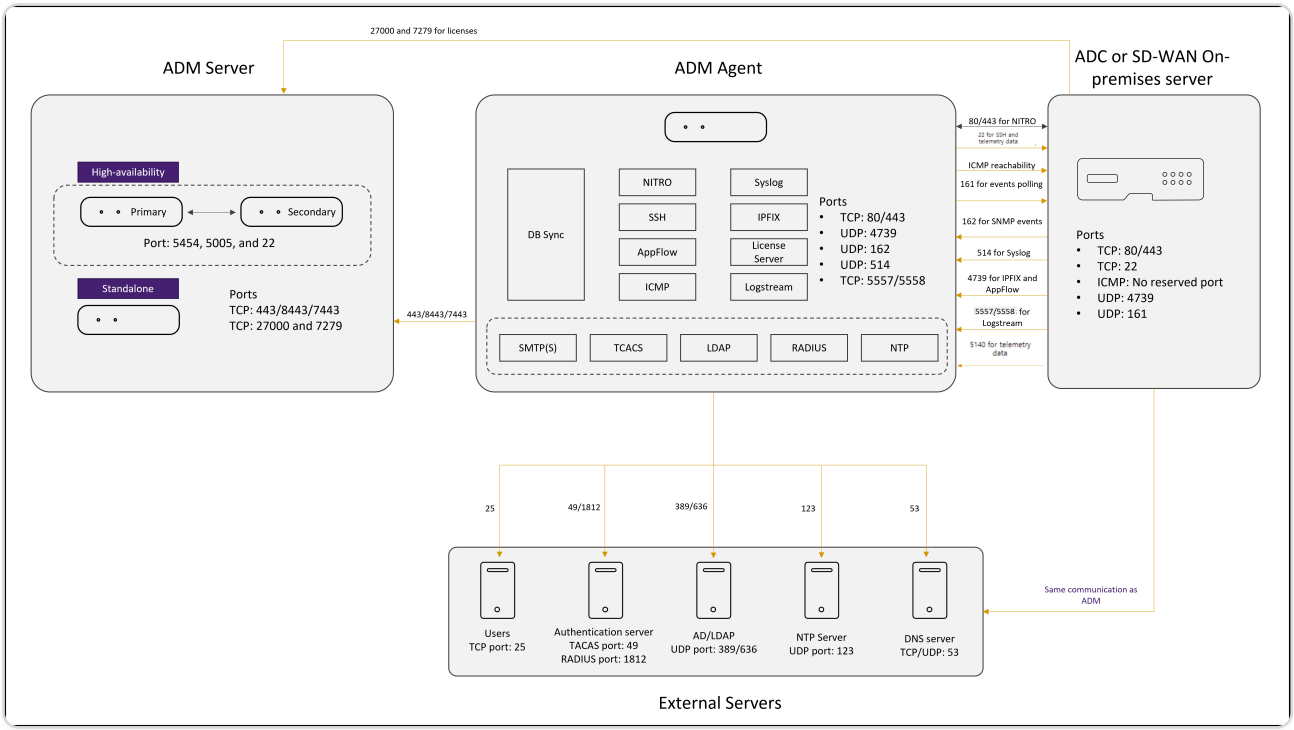
If you have configured NetScalers in High Availability mode, NetScaler ADM uses NSIP to communicate with NetScaler and the required ports remain the same.

Network port diagram for agentless deployment:



Network port diagram for the deployment that includes ADM agent:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following sections explain the required ports and their purpose:

- ADM server
- ADM agent
- ADC instance
- External servers

Ports for the ADM server

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

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443/5454/22	TCP	Default port for communication, and database synchronization in between NetScaler ADM nodes in high availability mode. **Note:** This port is	NetScaler ADM primary node to NetScaler ADM secondary node

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
		also used for NetScaler telemetry.	
443/8443/7443	TCP	Port for communication between NetScaler agent and NetScaler ADM.	NetScaler agent initiates the communication with NetScaler ADM. Then, NetScaler ADM and agent interact with each other.
27000 and 7279	TCP	License ports for communication between NetScaler ADM license server and ADC instance. These ports are also used for ADC pooled licenses.	NetScaler to NetScaler ADM
5005	UDP	Port to exchange heartbeats between HA nodes.	NetScaler ADM primary node to secondary node. NetScaler ADM secondary node to primary node.
5140	UDP	Port to receive NetScaler Gateway telemetry data.	NetScaler to NetScaler Console

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

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443	TCP	For NITRO communication from	NetScaler agent to NetScaler and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
		NetScaler ADM to NetScaler instance.	NetScaler to NetScaler agent
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
5557/5558	TCP	For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from NetScaler to NetScaler ADM.	NetScaler to NetScaler ADM
5563	TCP	To receive ADC metrics (counters), system events, and Audit Log messages from NetScaler instance to NetScaler ADM	NetScaler to NetScaler ADM

Ports for the ADM agent

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443	TCP	For NITRO communication from NetScaler ADM to NetScaler instance.	NetScaler agent to NetScaler and NetScaler to NetScaler agent
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages from NetScaler instance to NetScaler ADM.	NetScaler to NetScaler agent
5557/5558	TCP	For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from NetScaler to NetScaler ADM.	NetScaler to NetScaler ADM

Ports for ADC instances

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443	TCP	For NITRO communication from NetScaler ADM to NetScaler instance. For NITRO communication between NetScaler ADM servers in high availability mode.	NetScaler ADM to NetScaler and NetScaler to NetScaler ADM
22	TCP	For SSH communication from NetScaler ADM to NetScaler instance. For synchronization between NetScaler ADM servers deployed in high availability mode. And, this port is required for the SSH communication between the ADM agent and NetScaler.	NetScaler ADM to NetScaler. Or, NetScaler agent to NetScaler.
No reserved port	ICMP	To detect network reachability between NetScaler ADM and NetScaler instances, or the secondary NetScaler ADM server deployed in high availability mode.	NetScaler ADM to NetScaler
161	UDP	To poll events from ADC instances.	NetScaler ADM to NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ports for ADC built-in agent

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

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
443	TCP	For all communication from NetScaler ADM to NetScaler built-in agent	NetScaler ADM to NetScaler built-in agent and NetScaler built-in agent to NetScaler ADM

NOTE:

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

Ports for external servers

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

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
25	TCP	To send SMTP notifications from NetScaler ADM to users.	NetScaler ADM to users.
389/636	TCP	Default port for authentication protocol. For communication between NetScaler ADM and LDAP external	NetScaler ADM to LDAP external authentication server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
		authentication server.	
123	UDP	Default NTP server port for synchronizing with multiple time sources.	NetScaler ADM to NTP server
1812	RADIUS	Default port for authentication protocol. For communication between NetScaler ADM and RADIUS external authentication server.	NetScaler ADM to RADIUS external authentication server
49	TACACS	Default port for authentication protocol. For communication between NetScaler ADM and TACACS external authentication server.	NetScaler ADM to TACACS external authentication server

Limitations

From NetScaler ADM 12.1 or later, the IPv6 format of IP addresses is supported. To configure IPv6, navigate to **Settings > Administration**, select **IP Address, Second NIC, Host Name and Proxy Server** under **Network Configurations**, enable **IPv6**, provide the IPv6 configuration details, and click **Save**.

The following table describes the supported and not supported list of features for IPv6:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IPV6 SUPPORTED FEATURES	IPV6 NOT SUPPORTED FEATURES
Management access for NetScaler ADM GUI	High availability floating IP
Management access for NetScaler	Syslogs received from ADCs that support IPv6
Registration and inventory	StyleBooks on ADCs that support IPv6
Network dashboard	Analytics
SSL dashboard	Pooled licensing
Config jobs	
Config audit	
Network functions	
Network reporting	
Backup and restore of ADC instances	
SNMP events from NetScaler instances	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting started

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

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

Step 1 - Review the system requirements

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2 - Deploy NetScaler ADM

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

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

Step 3 - Add instances to NetScaler ADM

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

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

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

Learn More

Step 4 - Enable analytics on virtual servers

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

Learn More

Step 5 - Configure NTP server on NetScaler ADM

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

Learn More

Step 6 - Configure system settings for optimal NetScaler ADM performance

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

  Learn More

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's next

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy

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

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

Note

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

- **Migrate from NetScaler Insight Center to NetScaler Console**: You can migrate your NetScaler Insight Center deployment to NetScaler Console without losing the existing configuration, settings, or data. With NetScaler Console you can not only view the various

© 1997–2026 Citrix Systems, Inc. All rights reserved.

analytics generated by the NetScaler, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console. See: Migrating from NetScaler Insight Center to NetScaler Console

- **Integrate NetScaler Console with Director**: Director integrates with NetScaler Console for network analysis and performance management. See: Integrate NetScaler Console with Director

Prerequisites for installing NetScaler® ADM

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

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

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

General requirements for NetScaler ADM

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	Citrix recommends using Solid State Drive (SSD) technology for NetScaler ADM deployments.
	The default storage space required is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPONENT	REQUIREMENT
	If your NetScaler ADM storage requirement exceeds 120 GB, you to have to attach an extra disk.
	Citrix recommends you to estimate storage and attach an extra disk at the time of initial deployment. You can add only one extra disk.
	For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps

Note:

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

NetScaler ADM on Citrix Hypervisor™

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

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

Prerequisites

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

- Citrix Hypervisor version 7.1 or later is installed on hardware that meets the minimum requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

XenCenter system requirements

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

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

Install NetScaler Application Delivery Management

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

NOTE

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

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

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

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

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

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

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

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verification

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

The browser displays the NetScaler ADM configuration utility.

NetScaler® ADM on Microsoft Hyper-V

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

Prerequisites

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

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

Microsoft Hyper-V system requirements

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

COMPONENT	REQUIREMENT
Operating System	Windows Server 2012 R2
.NET framework	Version 2.0 or later
CPU	750 MHz (MHz), Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB, Recommended: 2 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

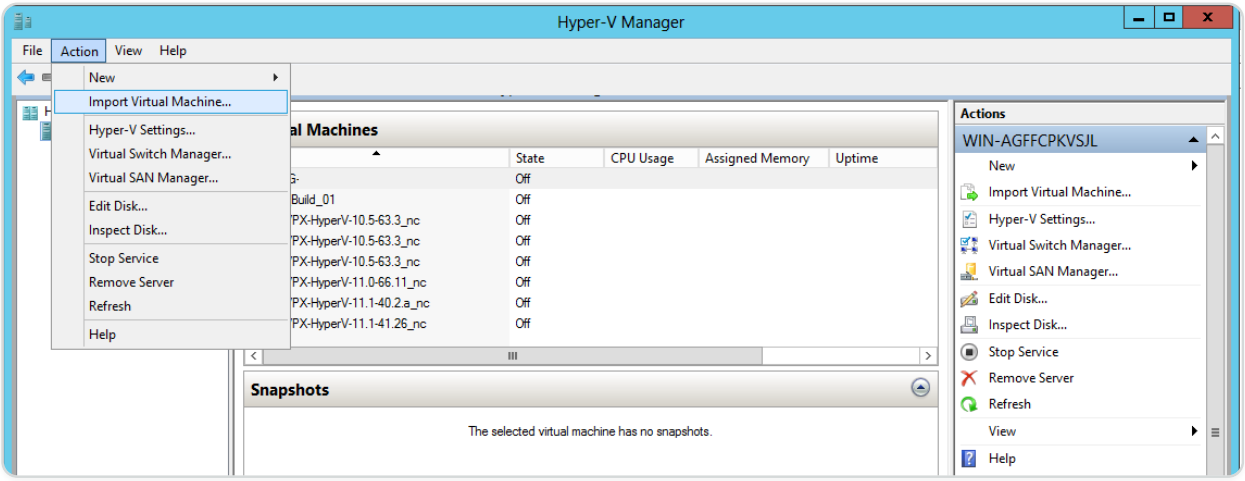
COMPONENT	REQUIREMENT
NIC	100 megabits per second (Mbps) or faster NIC

Installing NetScaler Application Delivery Management

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

To install NetScaler ADM:

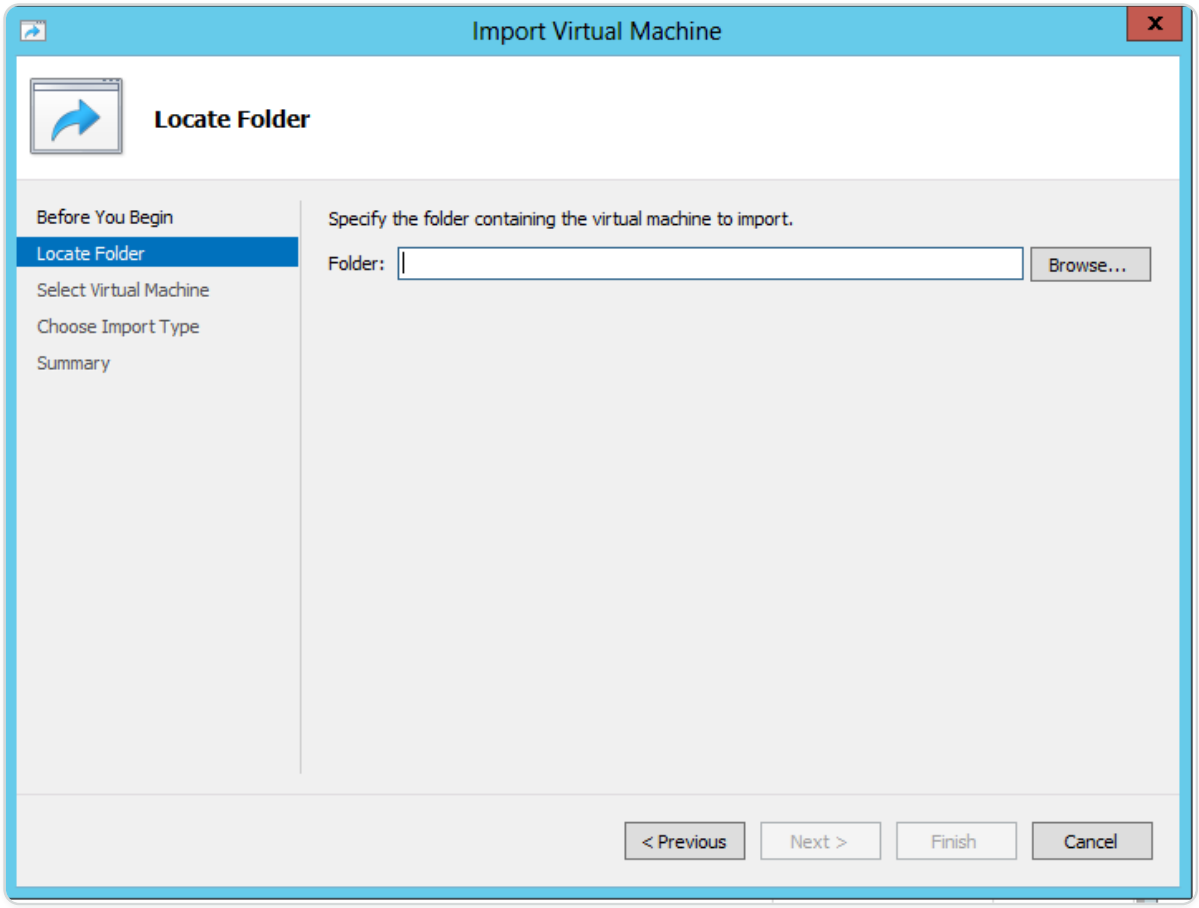
1. Start the Hyper-V Manager client on your workstation.
2. On the **Action** menu, click **Import Virtual Machine**.



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

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

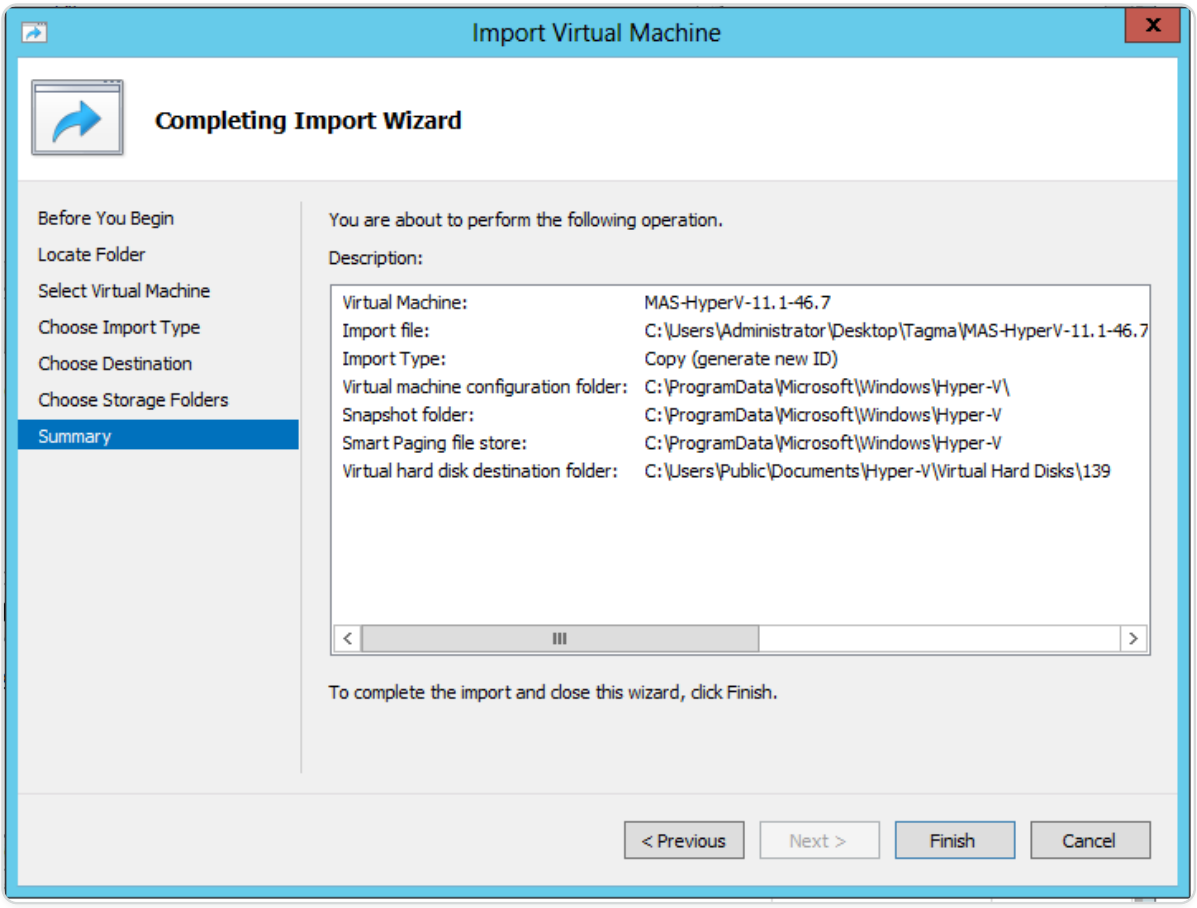
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

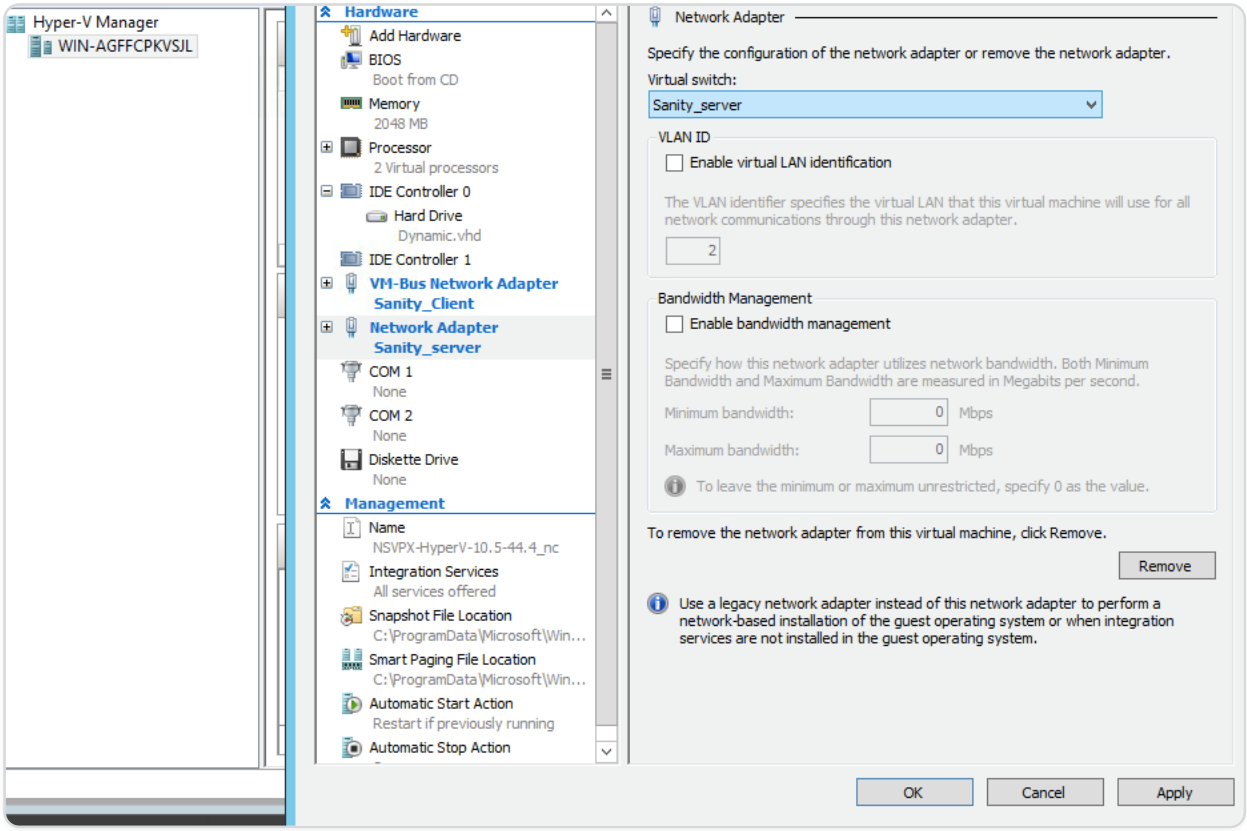
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

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

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

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

```
deployment_type.py
```

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

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

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

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

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

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

NOTE

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

Verification

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The browser displays the NetScaler ADM configuration utility.

NetScaler® ADM on VMware ESXi

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

Prerequisites

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

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

Note

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

To install NetScaler ADM

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

NOTE

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

1. Start the VMware vSphere client on your workstation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

   NOTE

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

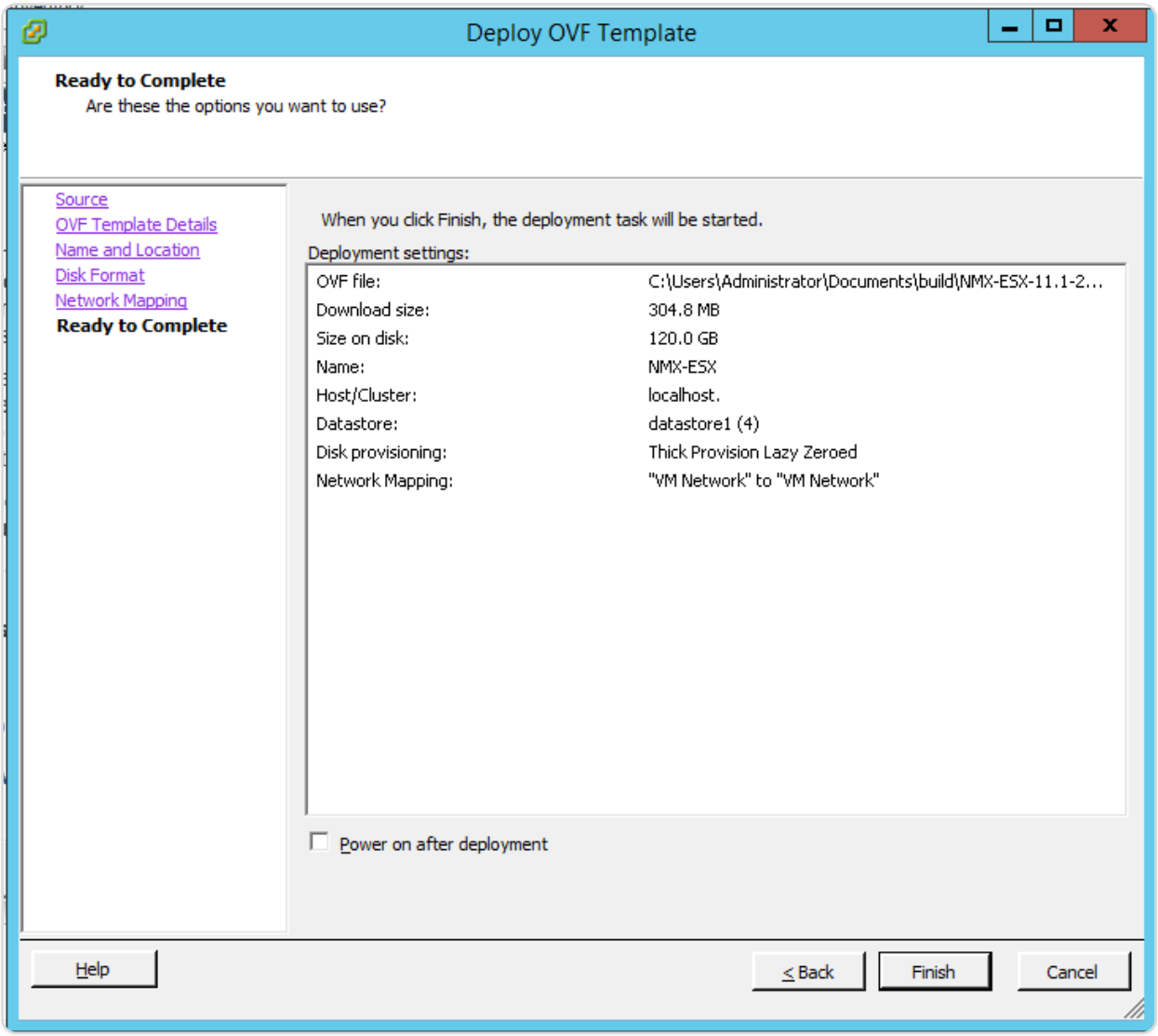
6. On the **OVF Template Details** page, click **Next**.
7. Type a name for the NetScaler ADM virtual appliance, and then click **Next**.
8. Specify the Disk Format by selecting either Thin provisioned format or Thick provisioned format.

   NOTE

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

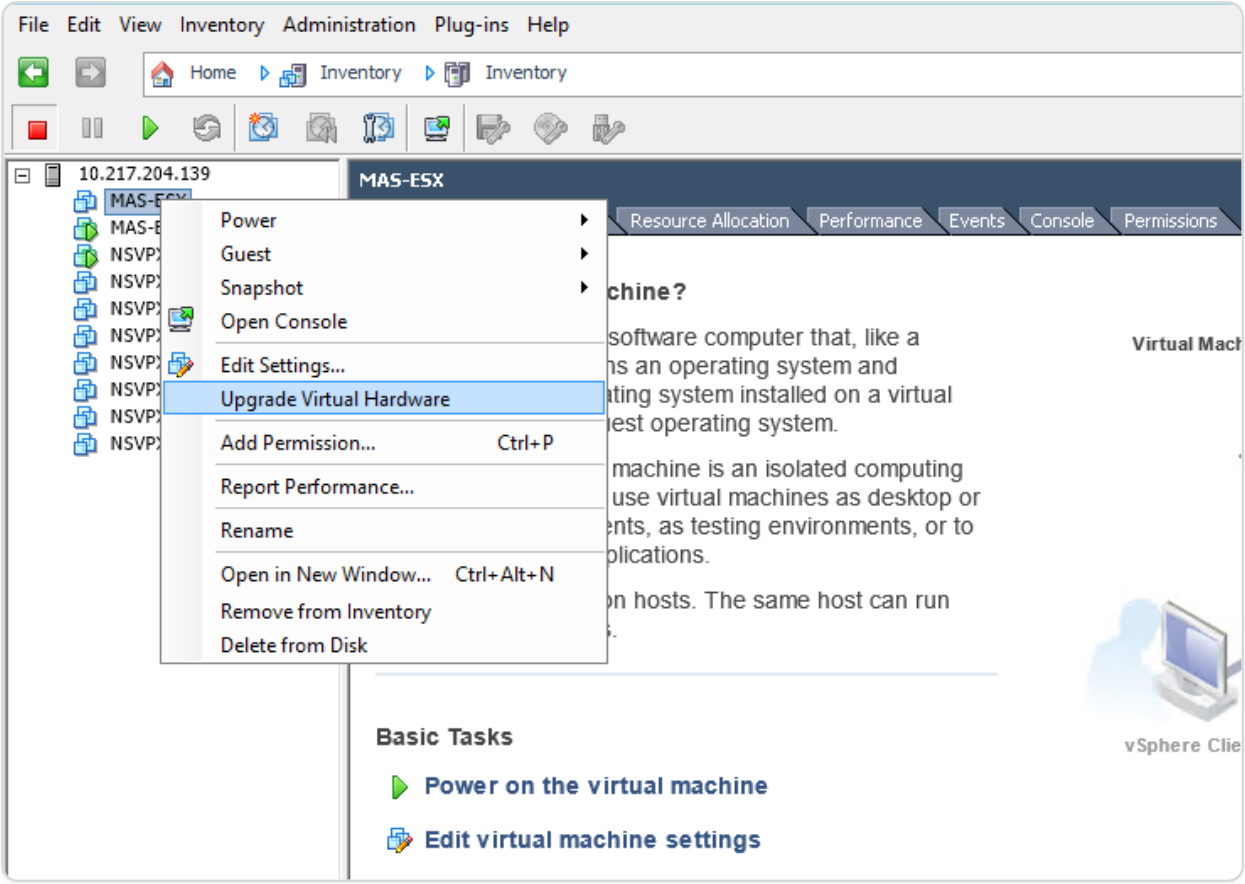
9. Click **Finish** to start the installation process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



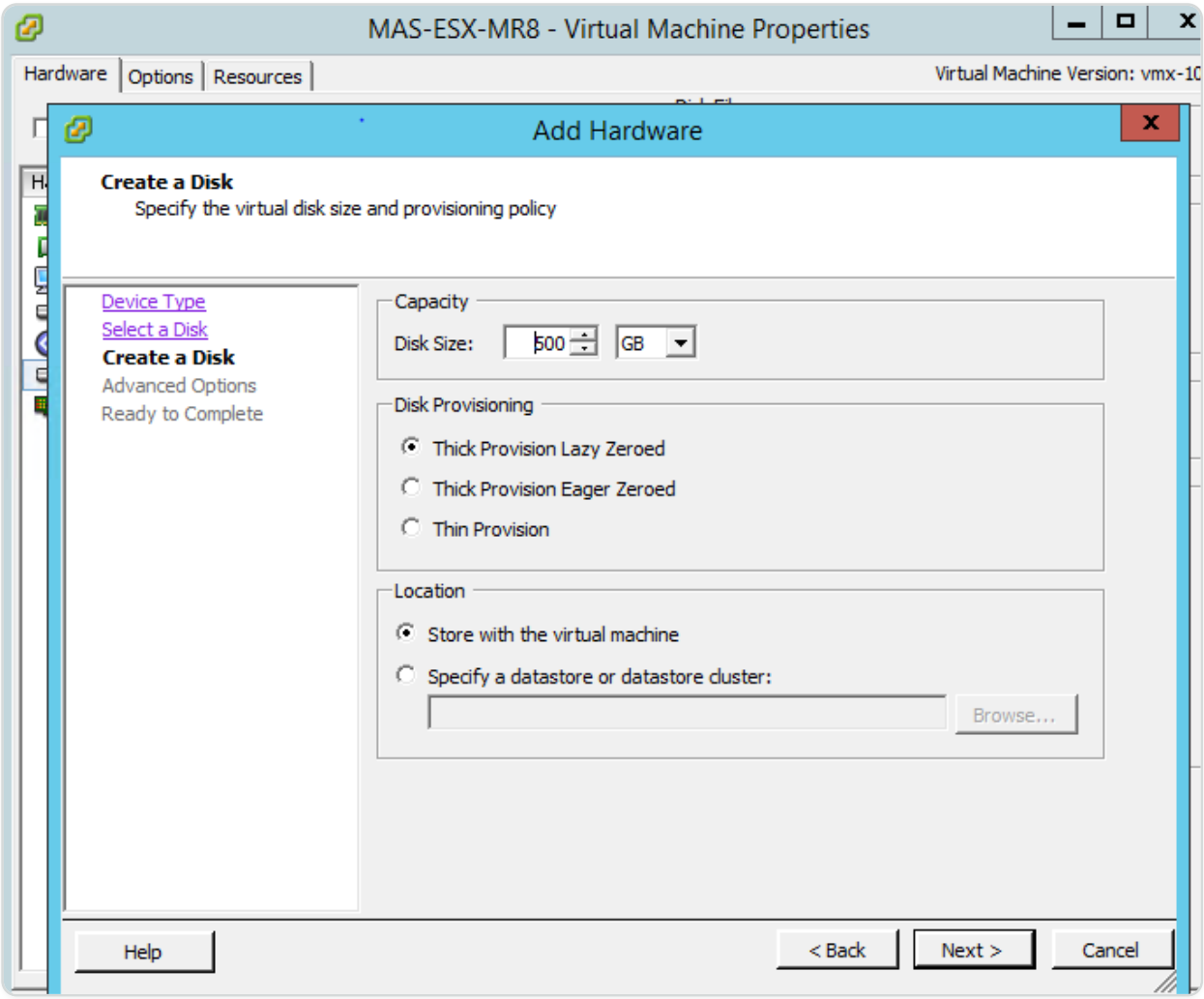
10. You are now ready to start the NetScaler ADM virtual appliance.
11. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, right-click on the **Virtual Machine**, and then click **Upgrade Virtual Hardware**. In the **Confirm Virtual Machine** dialog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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



16. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, click **Virtual Machine**, click **Power**, and then click **Power On**.

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

NOTE

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

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

```
deployment_type.py
```

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

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

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

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

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

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verification

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

The browser displays the NetScaler ADM configuration utility.

NOTE

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

Automate deployment of NetScaler agent on VMware ESXi

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

As an admin, you can automate the following actions:

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

Configure the NetScaler agent

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

Register the NetScaler agent and change the default password

NOTE

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

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

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

Prerequisites

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

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

How to configure and register a NetScaler agent

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Download and edit the .OVF file

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

```
<ProductSection>

    <Info>Information about the installed software</Info>

    <Product>Application Delivery management</Product>

    <Vendor>Citrix</Vendor>



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

    ovf:key="eth0.ip">

    <Label>IPAddress</Label>

    </Property>



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

    ovf:key="eth0.netmask">

    <Label>Netmask</Label>

    </Property>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

    ovf:key="eth0.gateway">

    <Label>Gateway</Label>

    </Property>



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

    ovf:key="eth0.nameserver">

    <Label>Nameserver</Label>

    </Property>



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

    ovf:key="eth0.hostname">

    <Label>Hostname</Label>

    </Property>



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

    ovf:key="eth0.ServerIP">

    <Label>ADM Server IP</Label>

    </Property>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

    ovf:key="eth0.ServerUname">

    <Label>ADM Username</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

    ovf:type="string" ovf:key="eth0.ServerPassword">

    <Label>ADM Password</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

    ovf:type="string" ovf:key="eth0.NewPassword">

    <Label>Agent New Password</Label>

    </Property>



</ProductSection>
```

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

   - To configure the NetScaler agent, add the values to the following parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - IPAddress
    - Netmask
    - Gateway
    - Nameserver
    - Hostname

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

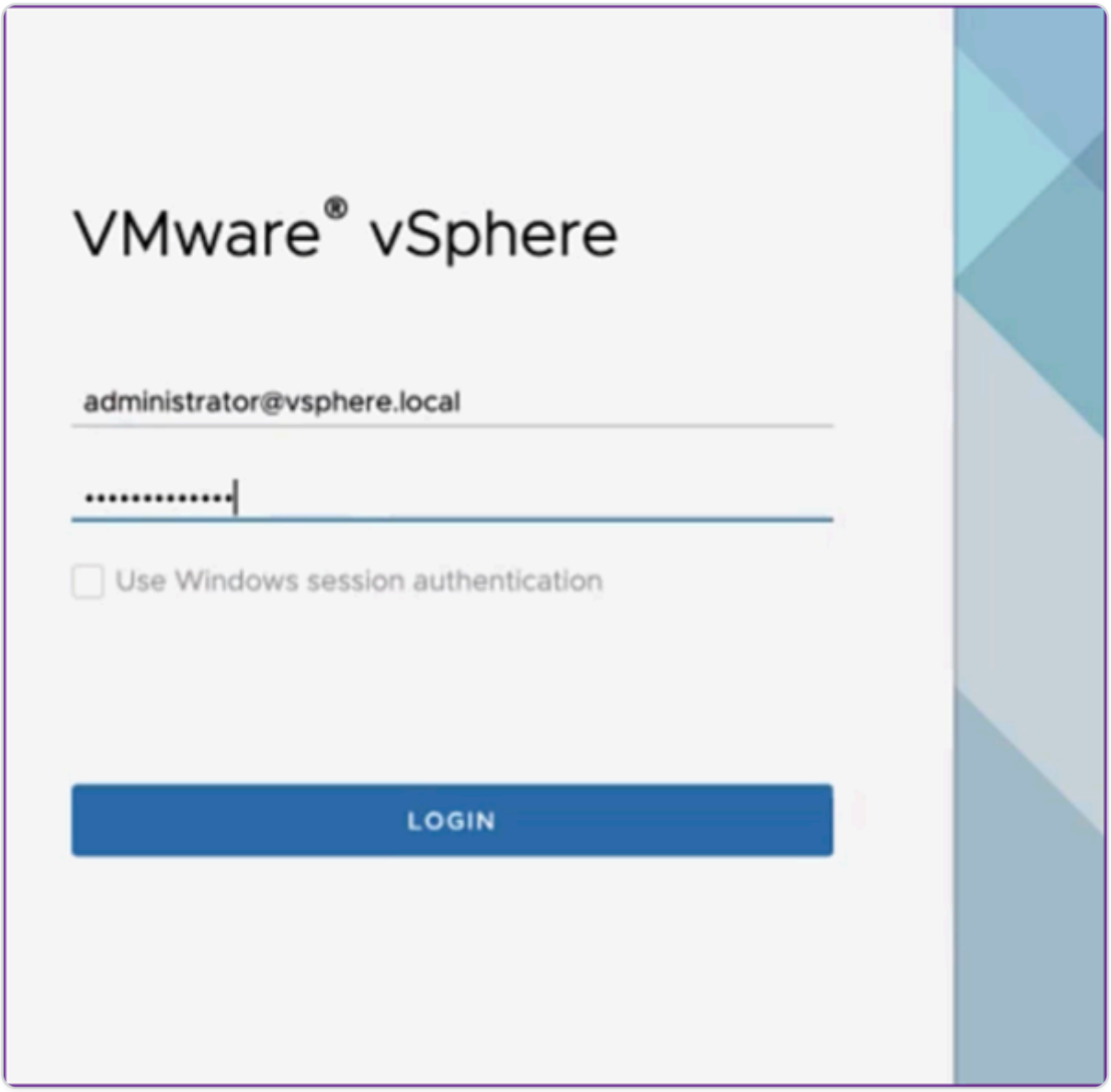
```
  <Property ovf:key="guestinfo.ovfEnvTransport" ovf:value="com.vmware.guestInfo"/>
</VirtualHardwareSection>
<ProductSection>
  <Info>Information about the installed software</Info>
  <Product>Application Delivery management</Product>
  <Vendor>Citrix</Vendor>
  <vssd:Transport ovf:required="true">
    <vssd:TransportName>com.vmware.guestInfo</vssd:TransportName>
  </vssd:Transport>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.98" ovf:type="string" ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="255.255.255.0" ovf:type="string" ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.1" ovf:type="string" ovf:key="eth0.gateway">
    <Label>Gateway</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.105.99.99" ovf:type="string" ovf:key="eth0.nameserver">
    <Label>Nameserver</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="admagent" ovf:type="string" ovf:key="eth0.hostname">
    <Label>Hostname</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.50" ovf:type="string" ovf:key="eth0.ServerIP">
```

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

Install NetScaler ADM virtual appliance on VMware ESXi

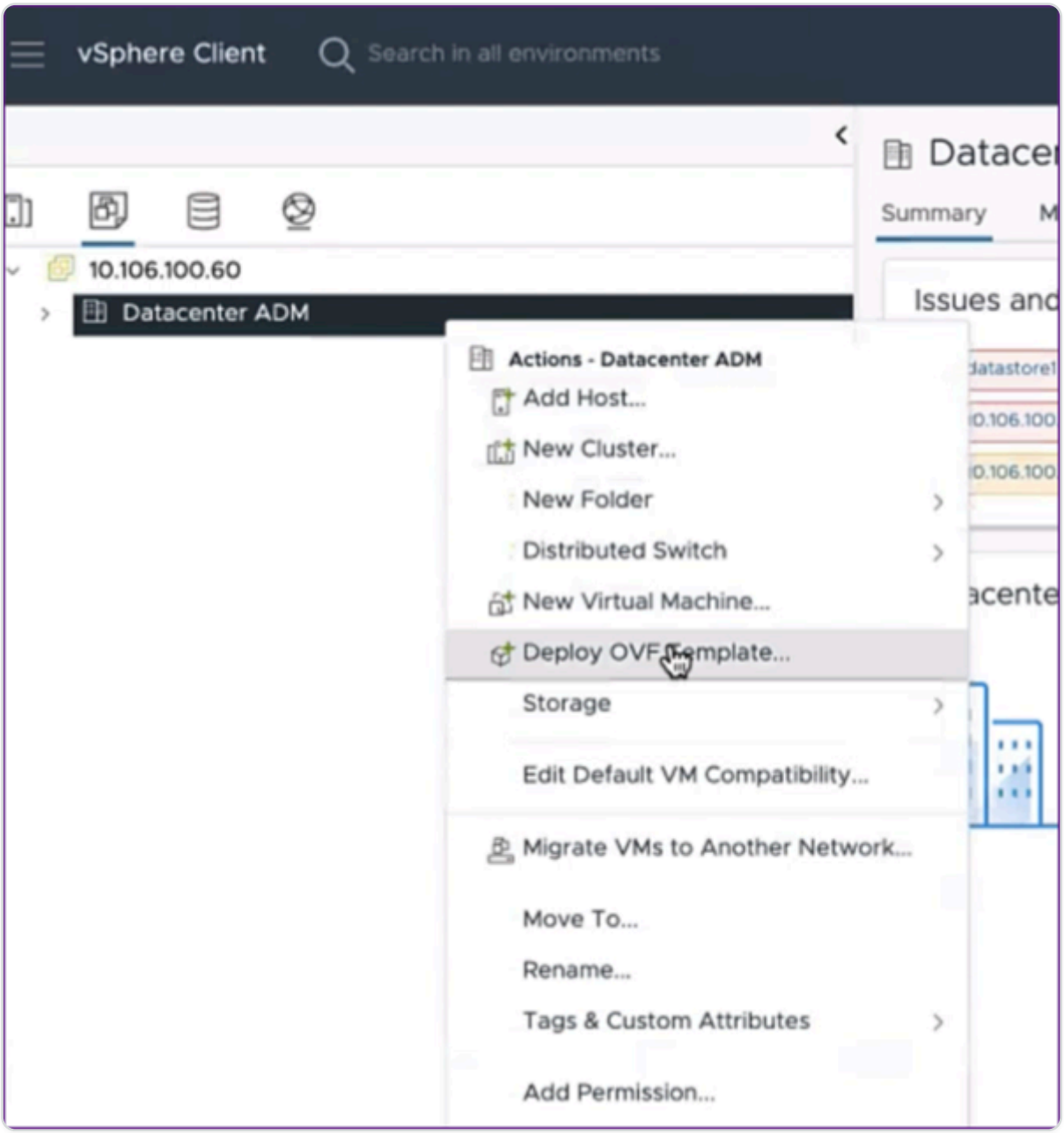
1. Log in to the **VMWare vSphere Client** and type the administrator credentials. Click **Login**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

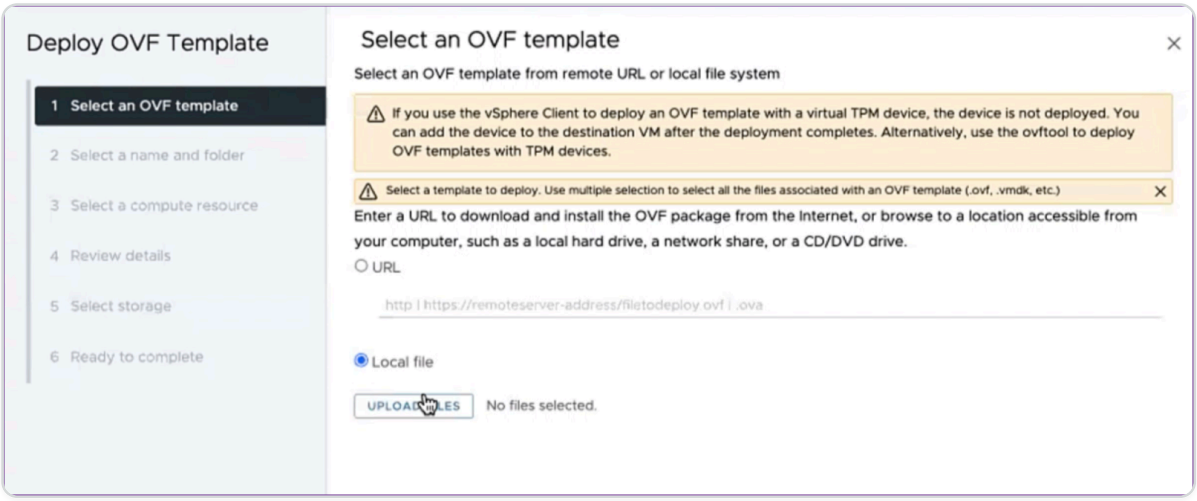
© 1997–2026 Citrix Systems, Inc. All rights reserved.



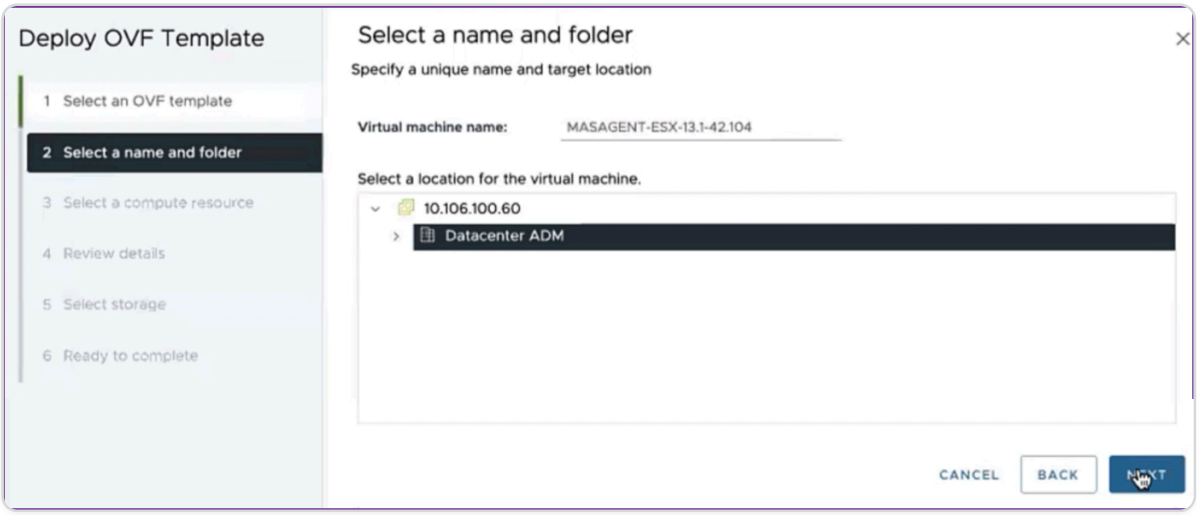
3. In the **Deploy OVF Template** page:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

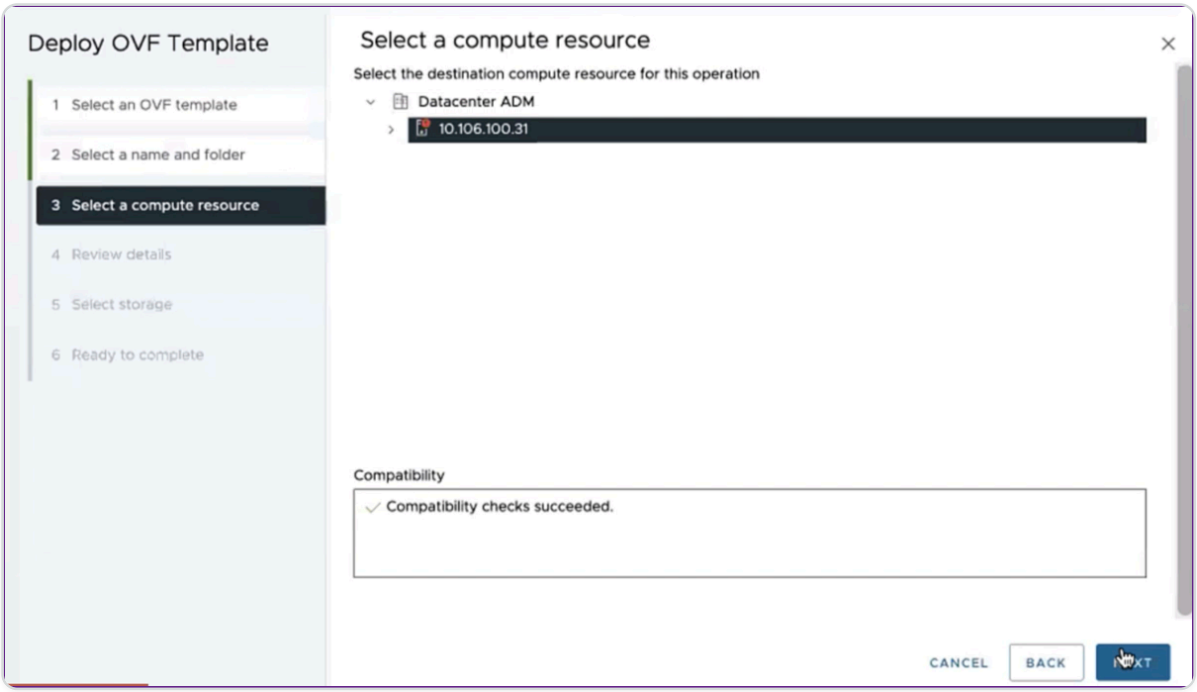


b. **Select a name and folder**: Add a name for the virtual appliance and select the location on the ESXi where you want to deploy the virtual machine. Click **Next**.

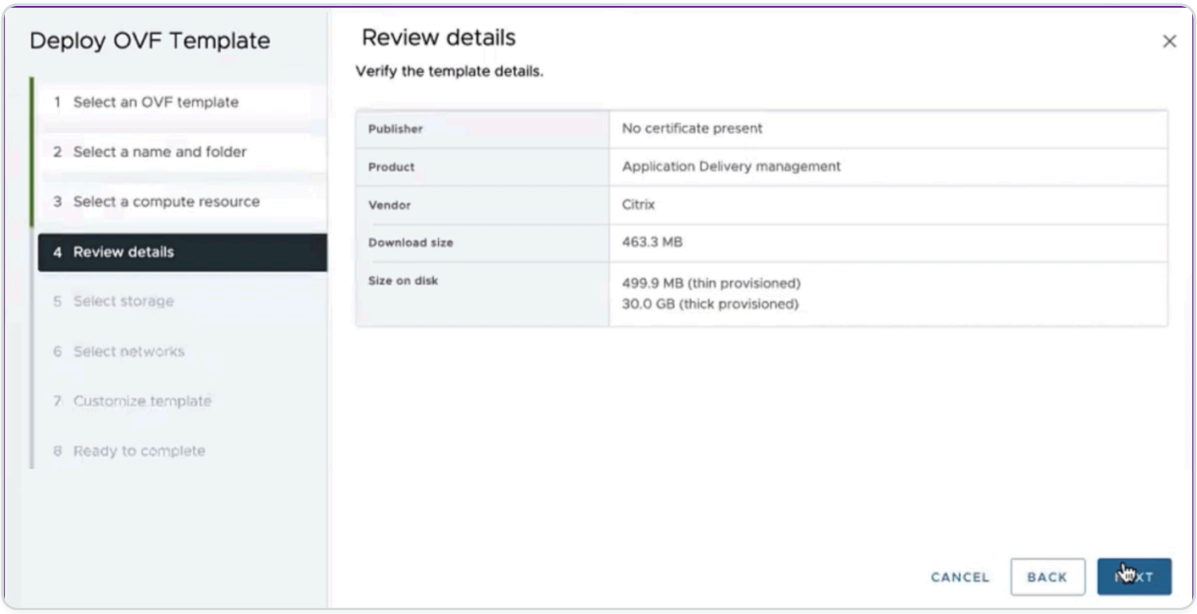


c. **Select a compute resource**: Select a resource on which to run the template after it is deployed. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

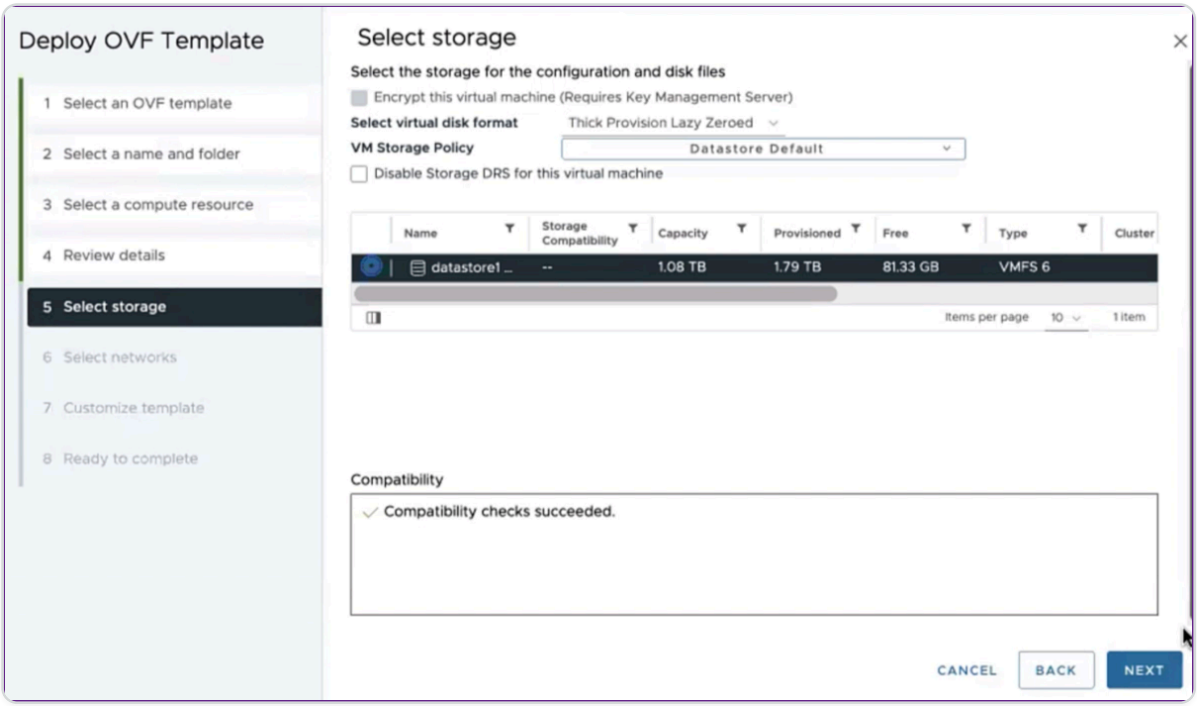


d. **Review details**: Verify the OVF template details. Click **Next**.

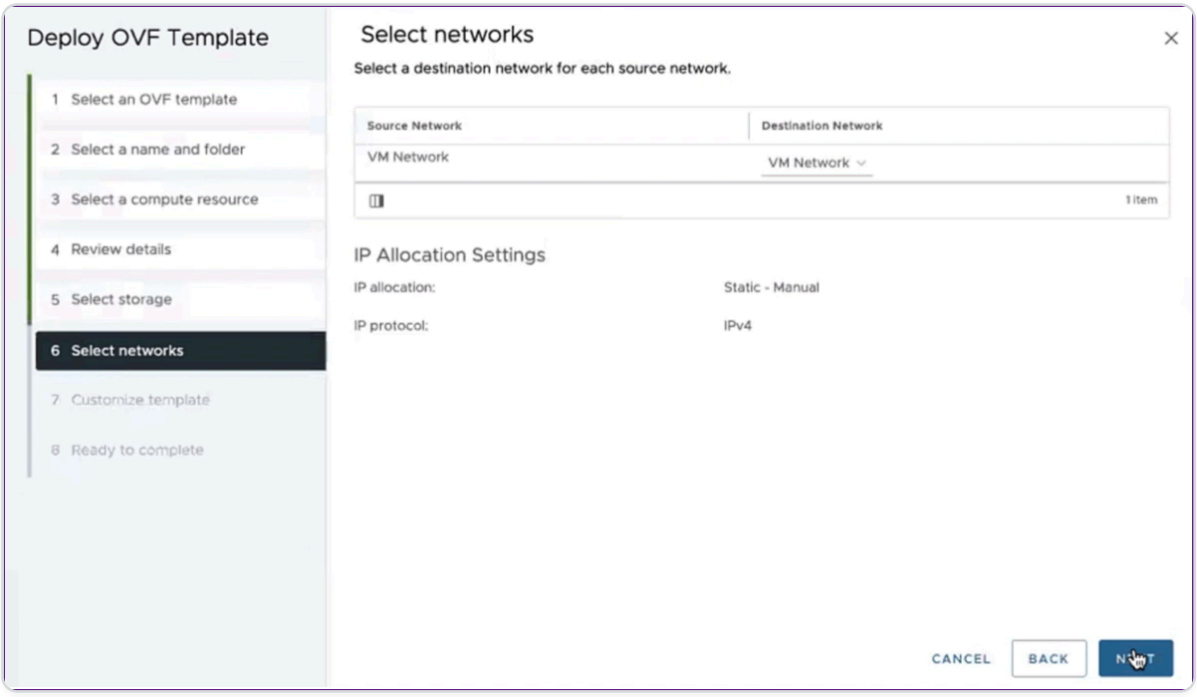


e. **Select storage**: Select a datastore to store the OVF template. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

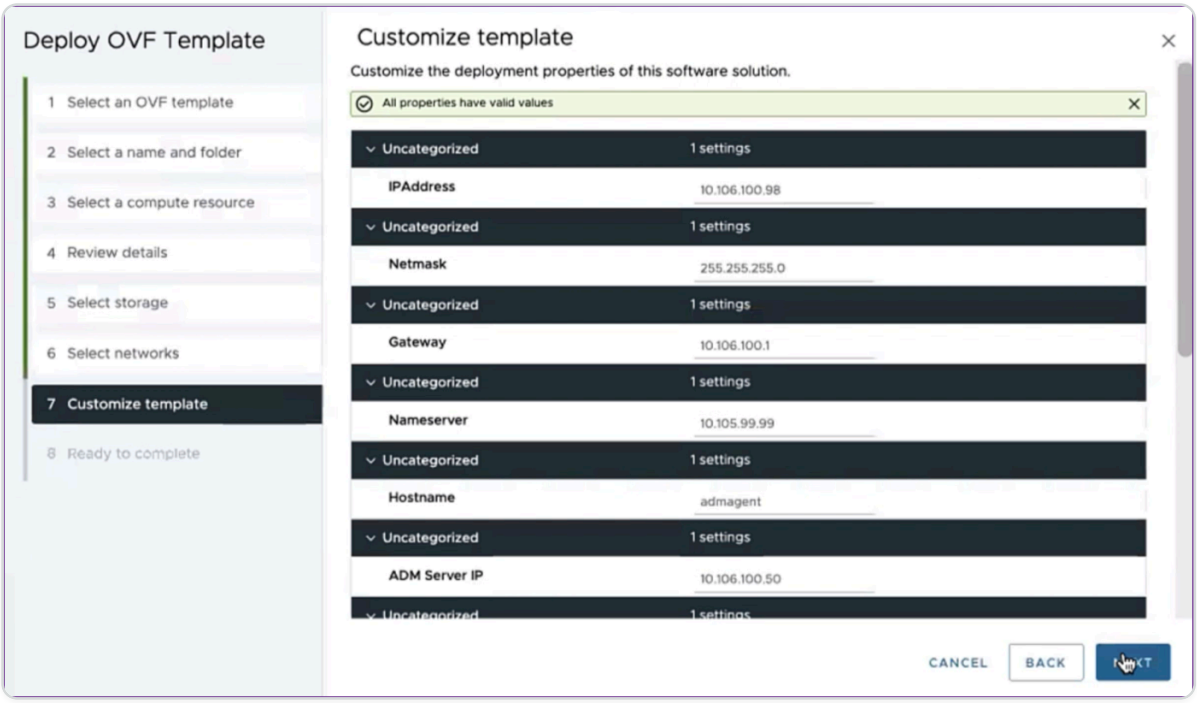


f. **Select networks**: Proceed with the default settings. Click **Next**.

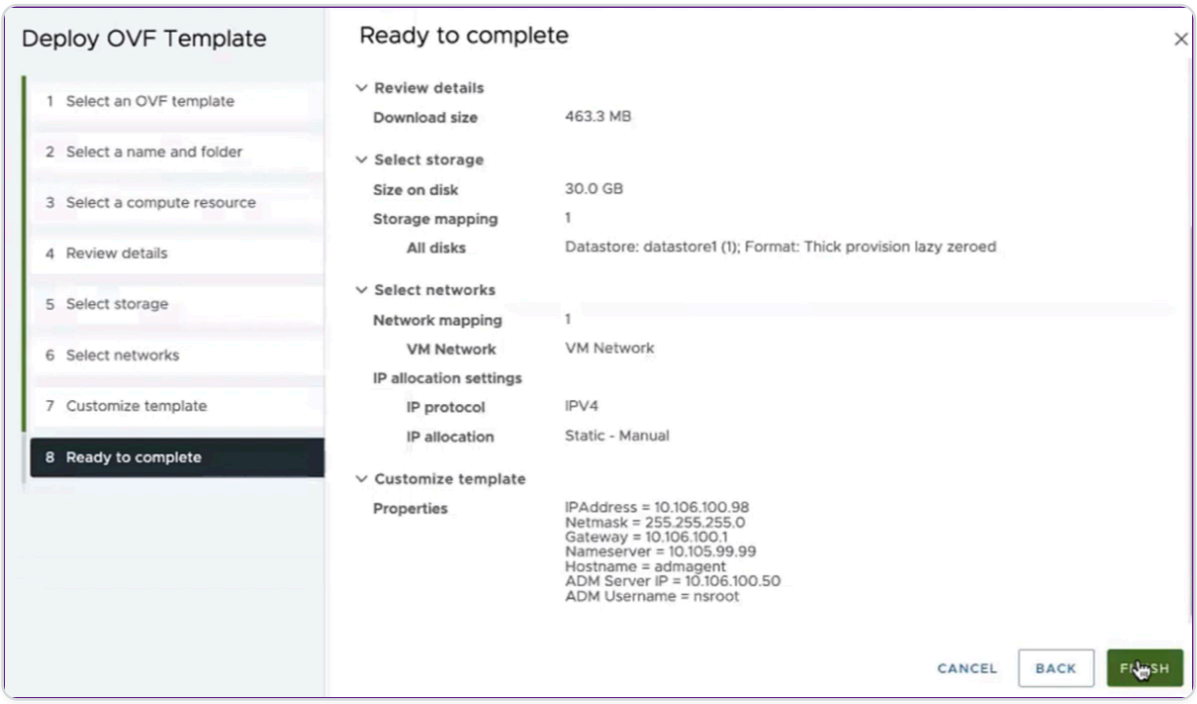


g. **Customize template**: Review all the properties of the OVF template. All the parameters and values you added in the .ovf file in the Download and edit the .OVF file section are displayed.

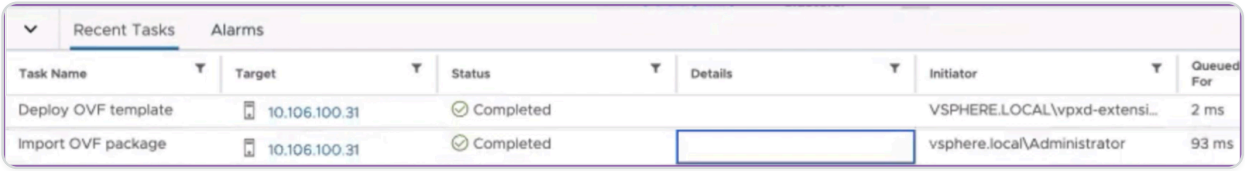
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



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

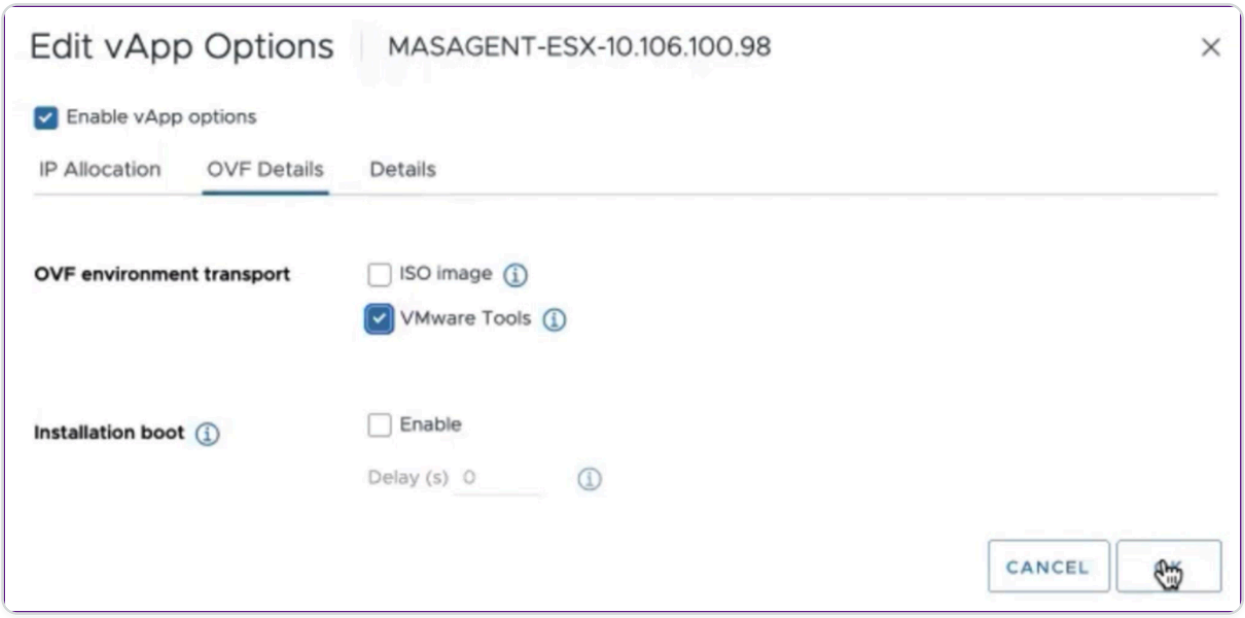


© 1997–2026 Citrix Systems, Inc. All rights reserved.

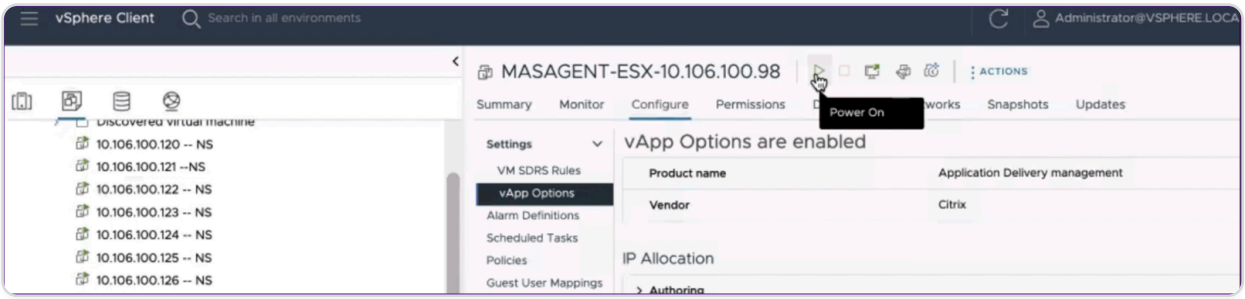
IMPORTANT

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

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

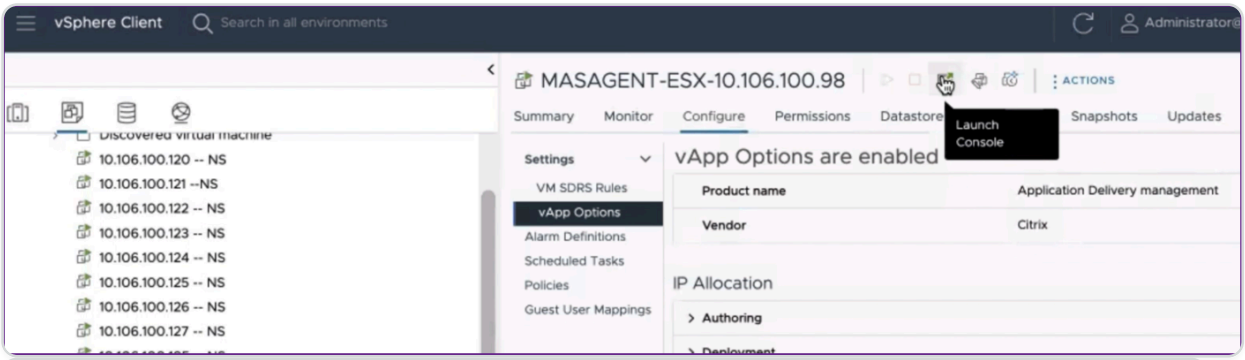


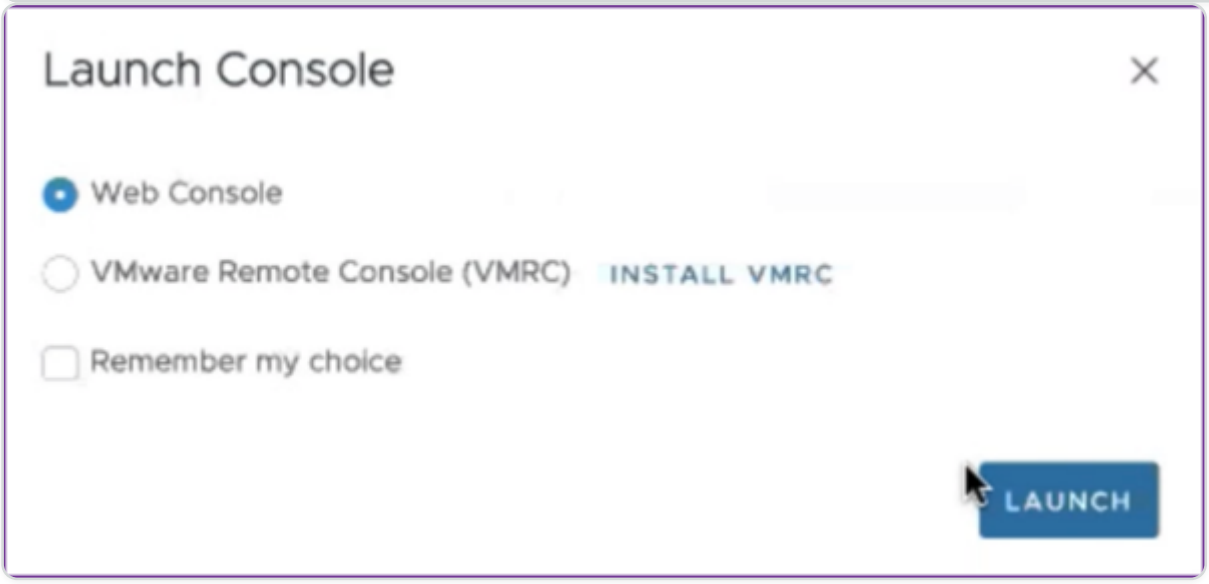
6. Right-click on the virtual machine and click **Power On**. As an alternative, you can select the virtual machine's **Summary** tab and click **Power On**.



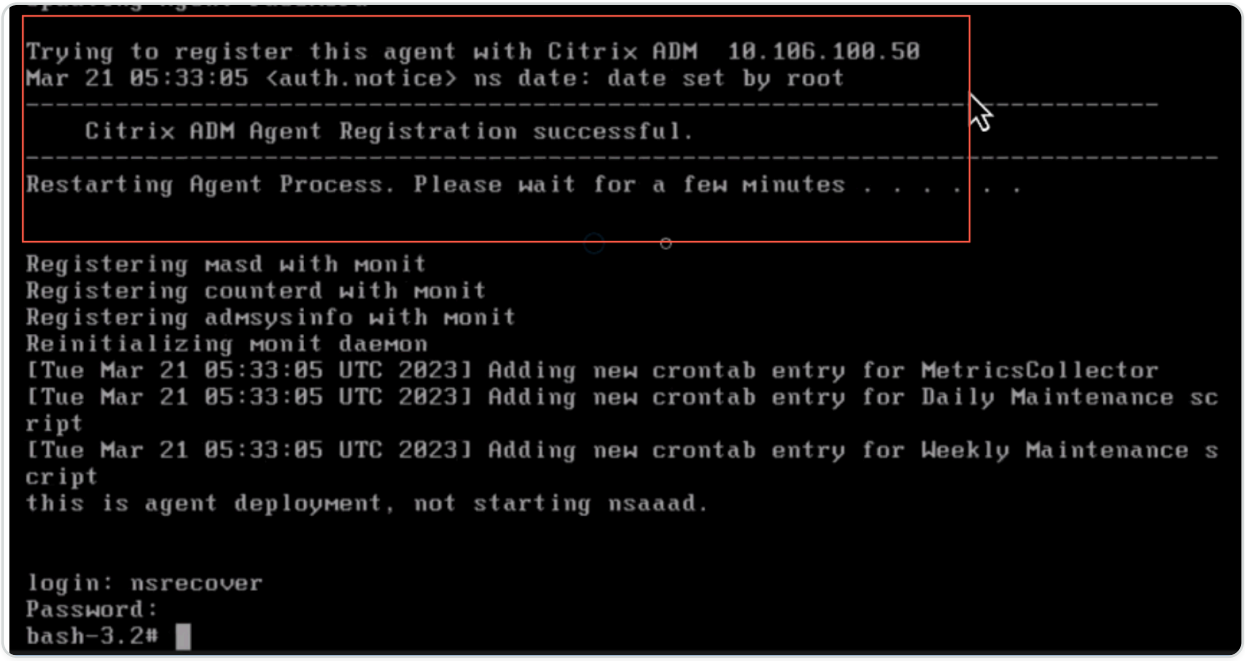
7. In the **Summary** tab, select **Launch Web Console**. In the **Launch Console** window, select **Web Console**. Click **Launch**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify

To verify that the NetScaler agent is deployed:

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

NetScaler® ADM on Kubernetes cluster

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

Prerequisites

Ensure the following prerequisites are met before you install ADM.

Kubernetes cluster

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NFS share

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

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

Note

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

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

NetScaler appliance

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

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

Install ADM on Kubernetes cluster

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

1. Go to the NetScaler site and download the file for the NetScaler ADM Helm Chart for Kubernetes.
2. Extract the downloaded Helm Chart tarball into the /var directory of the main node of the Kubernetes cluster.
3. Open the `values.yaml` file under the `/var/citrixadm` directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Enter a password for the database in the `dbpasswd` field in the file.
5. Change the following values. The ADM application uses these values to configure the NetScaler appliance so that the services are exposed to the external world:
   - `ingressIP`: a Virtual IP configured in the NetScaler for accessing the application.
   - `applicationID`: a unique ID to distinguish the ingress configuration from the rest of the configuration on the NetScaler appliance.
   - `ingressADCIP`: NetScaler IP address (NSIP), which is used as an ingress for the ADM application.
   - `ingressADCUsername`: a user name to access the NetScaler appliance. This user must have write privileges.
   - `ingressADCPassword`: Password for the user name.

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

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

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

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

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

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

6. Change the following values in the **storage** section. These values specify the persistence required to store files required by the ADM application.
   - `nfsServer`: Host name or IP address of the NFS server
   - `path`: mount the path for the folder to store application files.
   - `size`: at least 10 GB.

   Note

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

7. Go to **storage** section under `pg-datastore` and change the following values. These values specify the persistence used for creating a database.
   - `nsfServer`: Host name or IP address of the NFS server.
   - `size`: mount a path for the folder used for the datastore.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `path`: at least 100 GB.

Note

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

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

   Note

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

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

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

Note

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

NetScaler® ADM on Linux KVM server

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

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

Hardware requirements

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Software requirements

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

Network requirements

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

Download NetScaler ADM setup files

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

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

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

Install the NetScaler Application Delivery Management on Linux-KVM

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

   iii. A domain disk image

```
tar -xvfz MAS-KVM.tgz

MAS-KVM.xml

MAS-KVM.qcow2

checksum.txt
```

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

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

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

      i. `name` - Specify the name.

      ii. `mac` - Specify the MAC address.

      iii. `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.

      iv. `mode` - Specify the mode.

      v. `model type` - Set to virtIO.

      vi. `source dev` - Specify the interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<name> MAS1-KVM</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/var/ MAS-KVM.qcow2'/>

<source dev='eth0' mode='bridge'/>

<model type='virtio'/>
```

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

```
virsh define MAS-KVM.xml

Domain MAS defined from MAS-KVM.xml
```

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

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

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

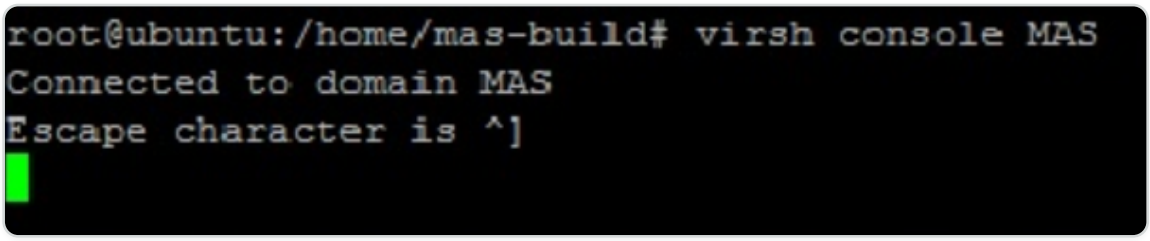
```
virsh start MAS

Domain MAS started
```

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
virsh console MAS

Connected to domain MAS

Escape character is ^]
```



Configure the NetScaler Application Delivery Management

NOTE

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

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

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

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

1. At the command line, use the default system administrator credentials to log on to the system:
   - User name: `nsroot`
   - Password: `nsroot`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

2. At the prompt, type: *shell*
3. Type **networkconfig** to enter the NetScaler ADM initial network configuration menu. Configure the management IP address.
4. To complete the initial network configuration of NetScaler ADM, follow the prompts. The console displays the NetScaler ADM initial network configuration options for setting the following parameters for the NetScaler ADM. The host name is populated by default.

   a. Enter **2** to update NetScaler ADM IPv4 address - management IP address at which you access a NetScaler ADM

   b. Enter **3** to update Netmask - subnet mask associated with the Management IP address

   c. Enter **4** to update Gateway IPv4 address - default gateway IP address for the subnet of the Management IP address of the NetScaler ADM

   d. Enter **7** to save and quit - saves your configuration changes and exits the system.

```
-----------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------------
      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

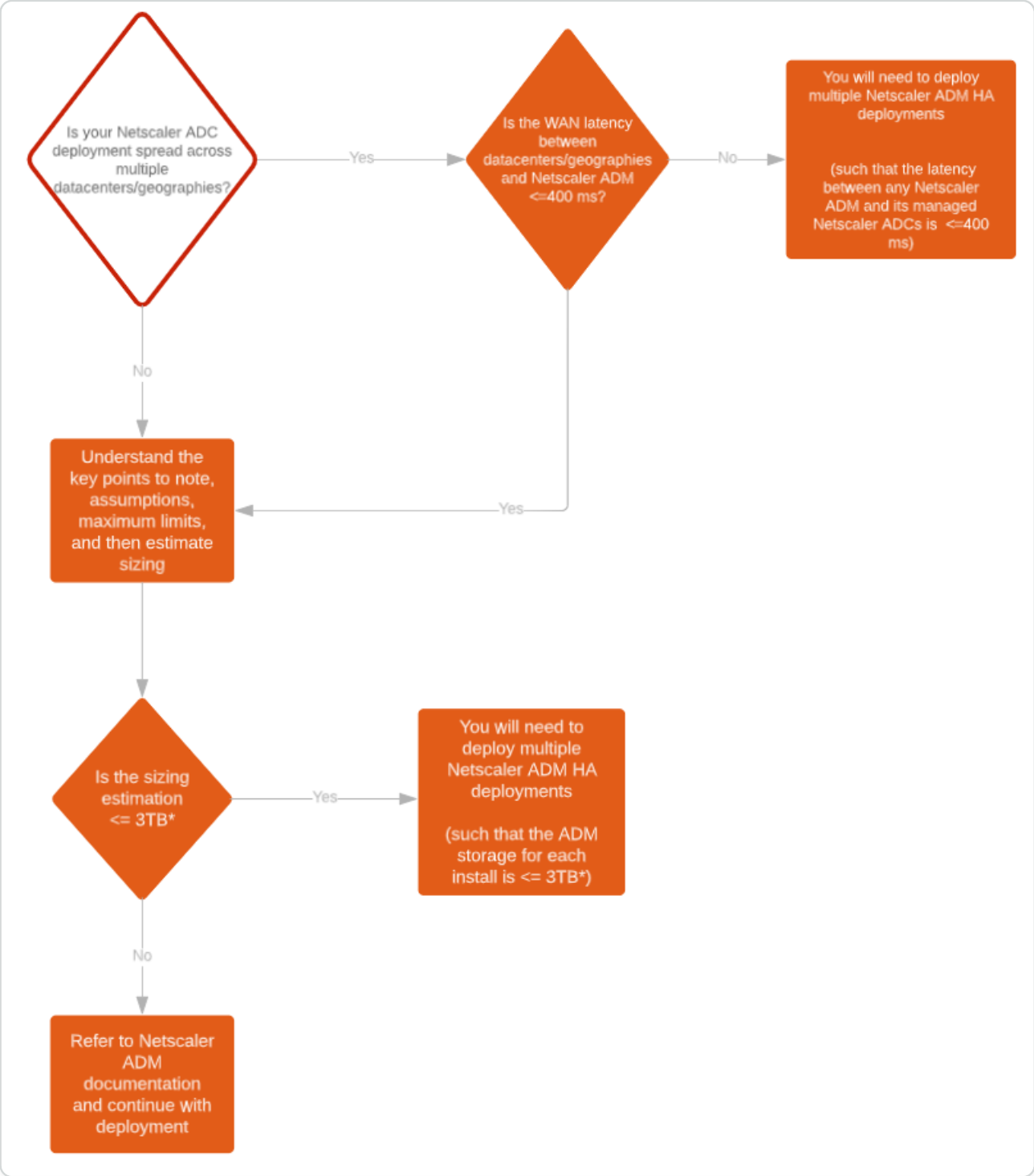
   You can later access the NetScaler ADM by typing the IP address of the NetScaler ADM server in the address bar of your browser. The default administrator credentials to log on to the server are *nsroot/nsroot*.

Configure high availability deployment

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deployment scenario



NOTE

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

Important

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To access NetScaler ADM 12.1 build 48.18 or later versions using HTTPS:

If you have configured a NetScaler instance to load balance NetScaler ADM in a high availability mode, first remove the NetScaler instance. Then, configure a floating IP address to access NetScaler ADM in high availability mode.

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

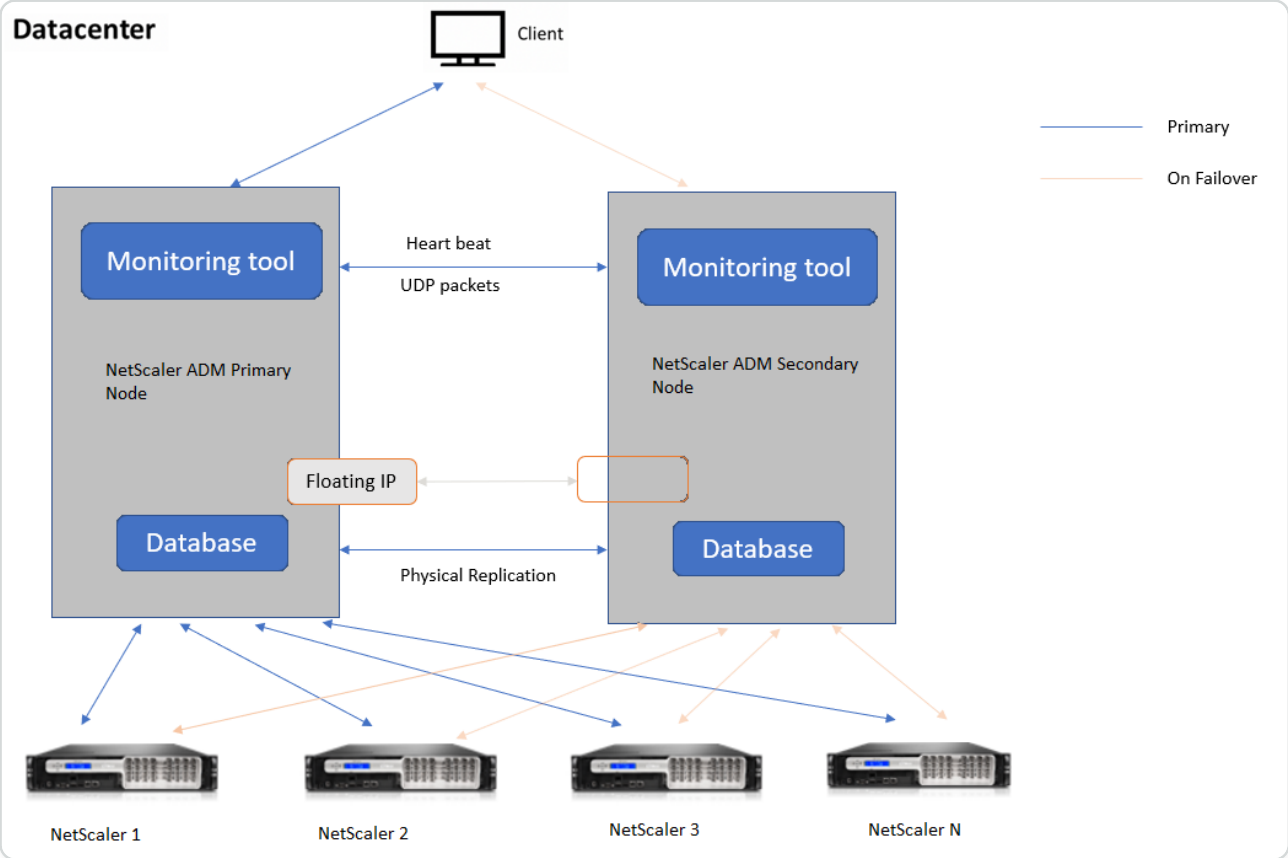
TERMS	DESCRIPTION
	primary to the new one. It is useful in high availability setup because it allows clients to communicate with the high availability nodes using a single IP address.

NOTE

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

Components of high availability architecture

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



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring tool

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

Primary node

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

Secondary node

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

Physical streaming replication

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

Heartbeat messages

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Floating IP address

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

Key points to note

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

    NOTE

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

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

    NOTE

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

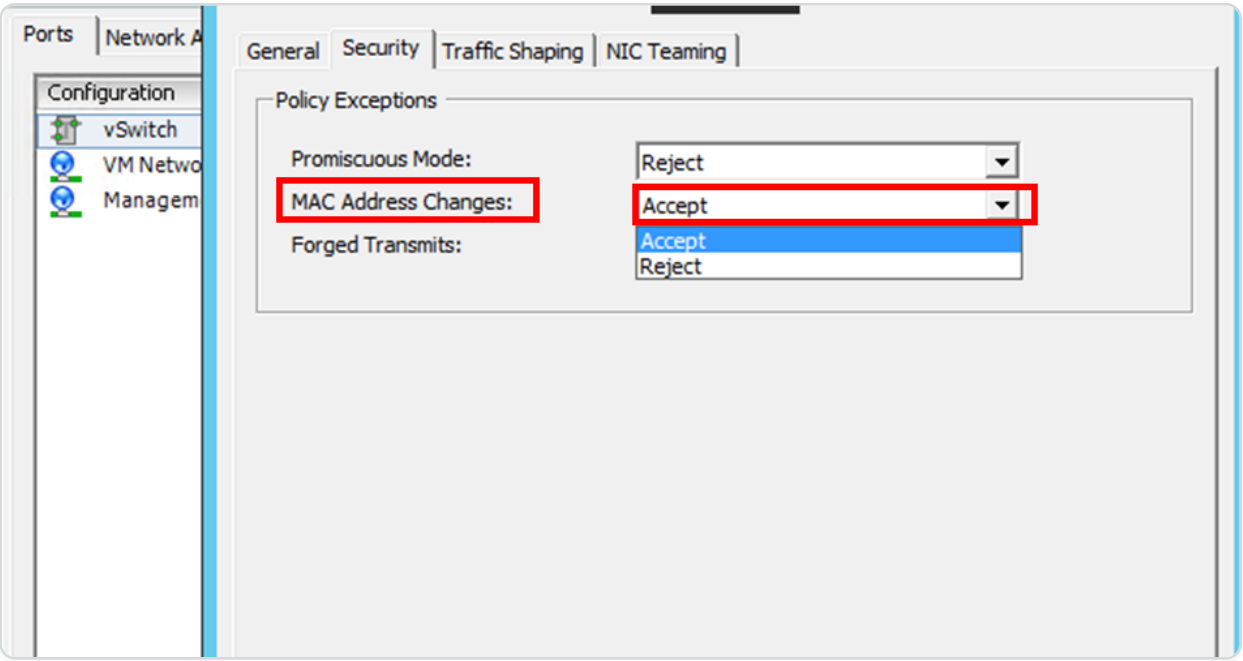
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

NOTE

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

If the NetScaler ADM is deployed on the ESXI version lower than 6.7, ensure the **MAC Address Changes** option is set to **Accept** only.



Prerequisites

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

- The NetScaler ADM high availability deployment is supported from NetScaler ADM version 12.0 build 51.24.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Download the NetScaler Application Delivery Management image file (.xva) from the NetScaler site: `<https://www.citrix.com/downloads/>`

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set up NetScaler ADM in high availability mode

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

Register and deploy the first server (primary node)

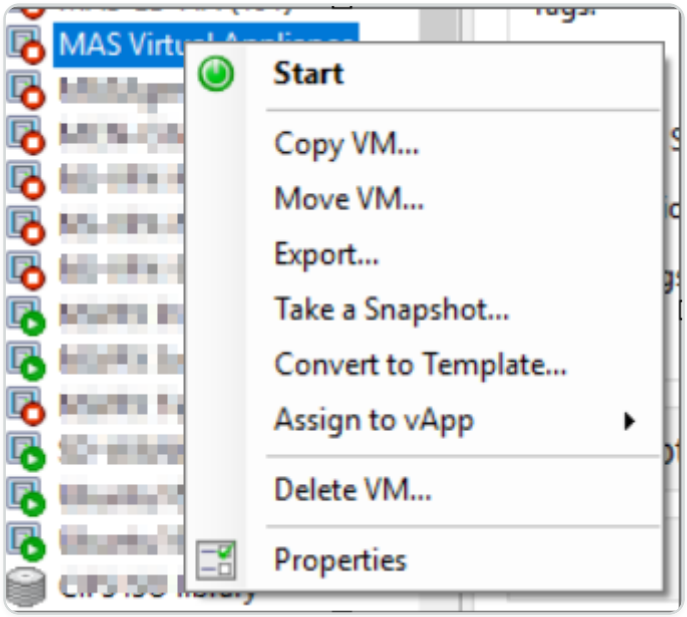
To register the first node:

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

   NOTE

   It might take a few minutes for the .xva image file to import and get started. You can see the status on the bottom of the screen.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-----------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------------
      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

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

NOTE

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes
```

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

Register and deploy the second server (secondary node)

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

```
-------------------------------------------------------------------------------
-------------

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

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

-------------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-----------------------------------------------------------------------------
-------------

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

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

-----------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
    Enter Floating IP address:10.102.29.97
```

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

NOTE

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

Deploy the primary and secondary node as a high availability pair

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

NOTE

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

To deploy nodes as a high availability pair:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

   NOTE

   You can now start using the Floating IP address.

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

   a. Add NetScaler instances

   b. Configure Customer Identity

   NOTE

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

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

   For more information, see the Frequently Asked Questions.

Disable high availability

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

NOTE

Disable high availability from the primary node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To disable the high availability:

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

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

Redeploy high availability

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

NOTE:

After disabling NetScaler Console high availability, use only one console node as the standalone license server. The second node must be reprovisioned.

High availability failover scenarios

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

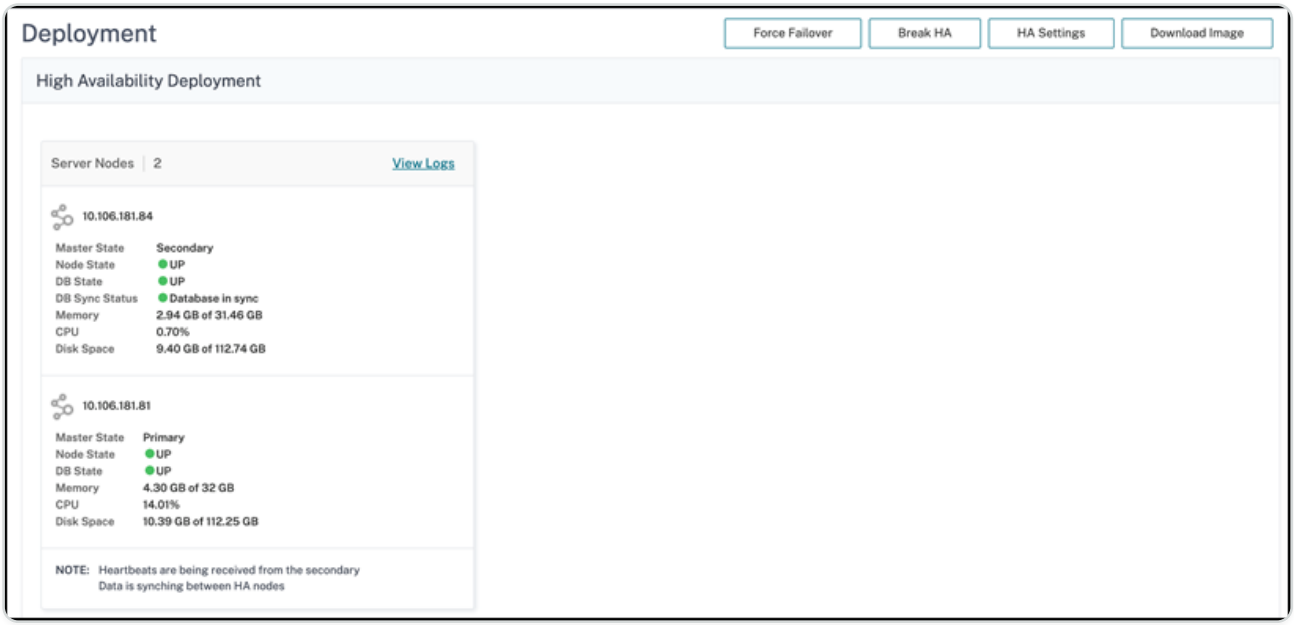
- **Node failure**: Primary node goes down, no heartbeat is detected from primary node for 180 seconds.
- **Application health failure**: Primary node is up and running but one of the NetScaler ADM processes is down.

View Database Synchronization Log messages

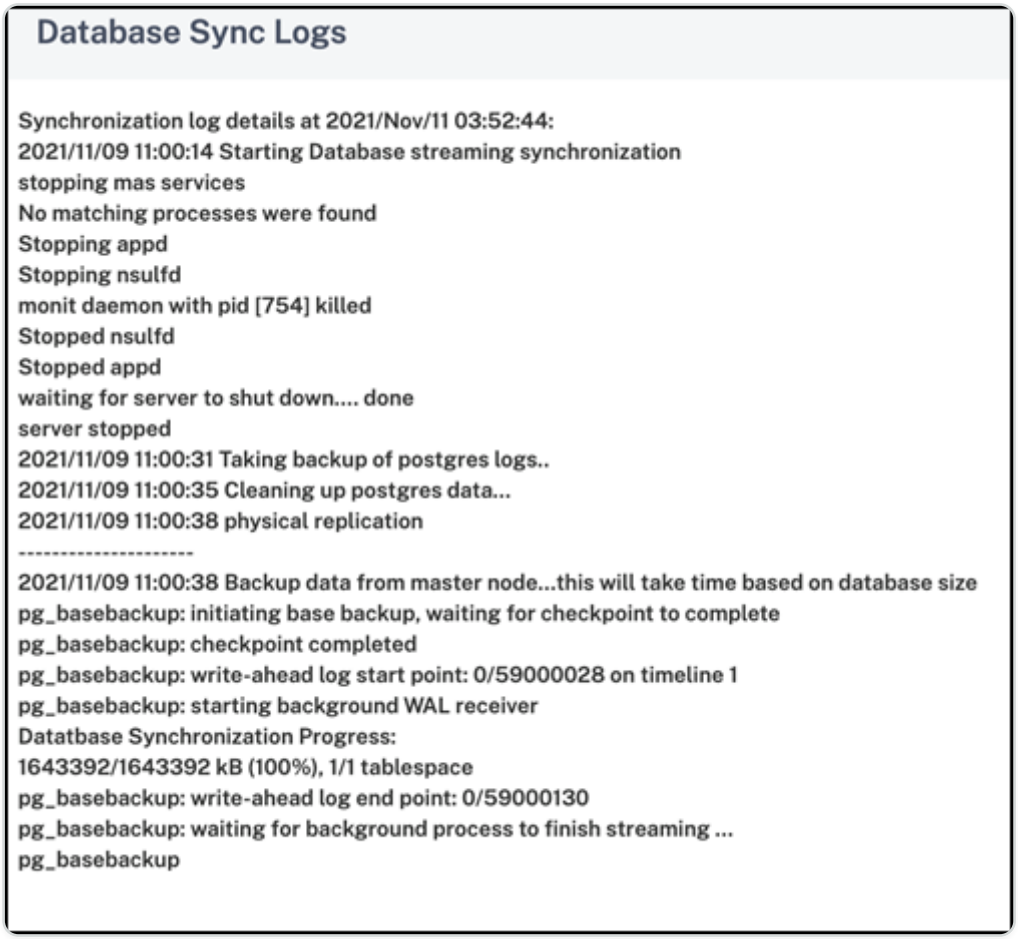
In the NetScaler ADM HA pair, the configuration files are synchronized automatically from the primary node to the secondary node and the physical streaming replication of database happens.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



Split-brain scenario

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

NOTE

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

Configure disaster recovery for high availability

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

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

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

TERMS	DESCRIPTION
Primary site (Data center A)	The primary site has NetScaler ADM nodes deployed in high availability mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TERMS	DESCRIPTION
Recovery site (Data center B)	The recovery site has a disaster recovery node deployed in standalone mode. This node is in read-only mode and is not operational until the primary site is down.
Disaster recovery node	The recovery node is a standalone node deployed in the recovery site. This node is made operational (to the new primary) in case a disaster occurs at the primary site and it is nonfunctional.

NOTE

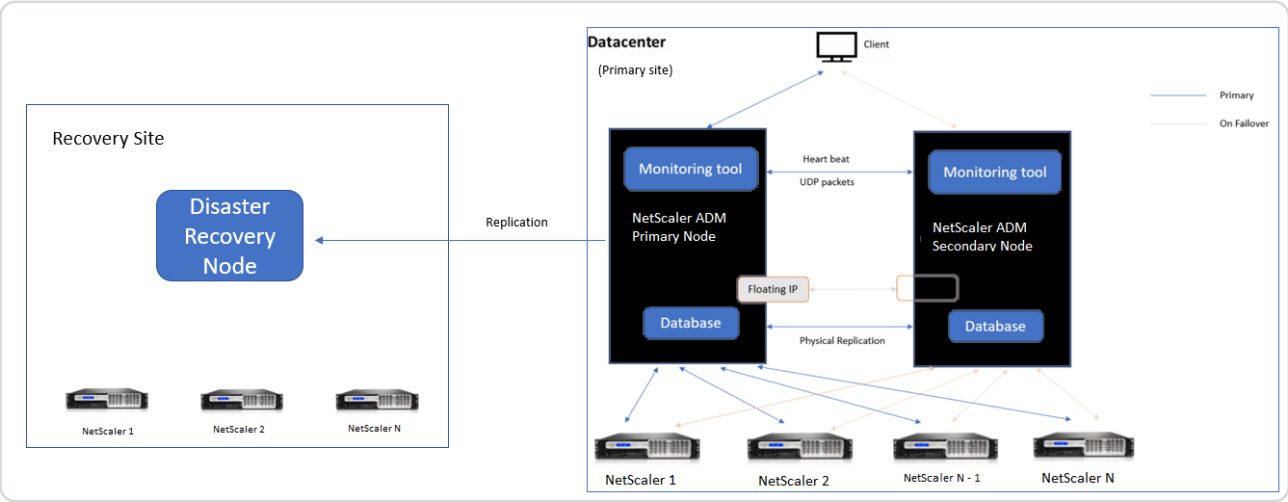
The primary site and DR site communicate with each other through ports 5454 and 22, and these ports are enabled by default.

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

Disaster recovery workflow

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

Initial setup before disaster



The image shows the disaster recovery setup before disaster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Prerequisites

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

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

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

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

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
Storage Space	Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler ADM sizing estimation. If your NetScaler ADM storage requirement exceeds 120 GB, you have to attach an extra disk. **Note** You can add only one more disk. Citrix recommends you to estimate storage and attach more disk at the time of initial

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPONENT	REQUIREMENT
	deployment. For more information, see How to Attach an Additional Disk to NetScaler ADM.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu and Fedora

First time disaster recovery setup

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

Deploy NetScaler ADM in high availability mode

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

To register the NetScaler ADM disaster recovery node:

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

   NOTE

   The disaster recovery node can be on a different subnet.

   ```
   ------------------------------------------------------------------------------
   Citrix ADM initial network configuration.
   This menu allows you to set and modify the initial IPv4 network addresses.
   The current value is displayed in brackets ([]).
   Selecting the listed number allows the address to be changed.
   ------------------------------------------------------------------------------
         1. Citrix ADM Host Name [DR]:
         2. Citrix ADM IPv4 address [10.102.29.53]:
         3. Netmask [255.255.255.0]:
         4. Gateway IPv4 address [10.102.29.1]:
         5. DNS IPv4 Address [127.0.0.2]:
         6. Cancel and quit.
         7. Save and quit.

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

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

   IMPORTANT

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

The disaster recovery node is now registered successfully.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

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

```
/mps/change_freebsd_password.sh <username> <password>
```

Example:

```
/mps/change_freebsd_password.sh nsroot new_password
```

Deploy the disaster recovery node using NetScaler ADM GUI

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

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

NOTE

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

For more information, see the FAQs.

IMPORTANT

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

Workflow after the disaster

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

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

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

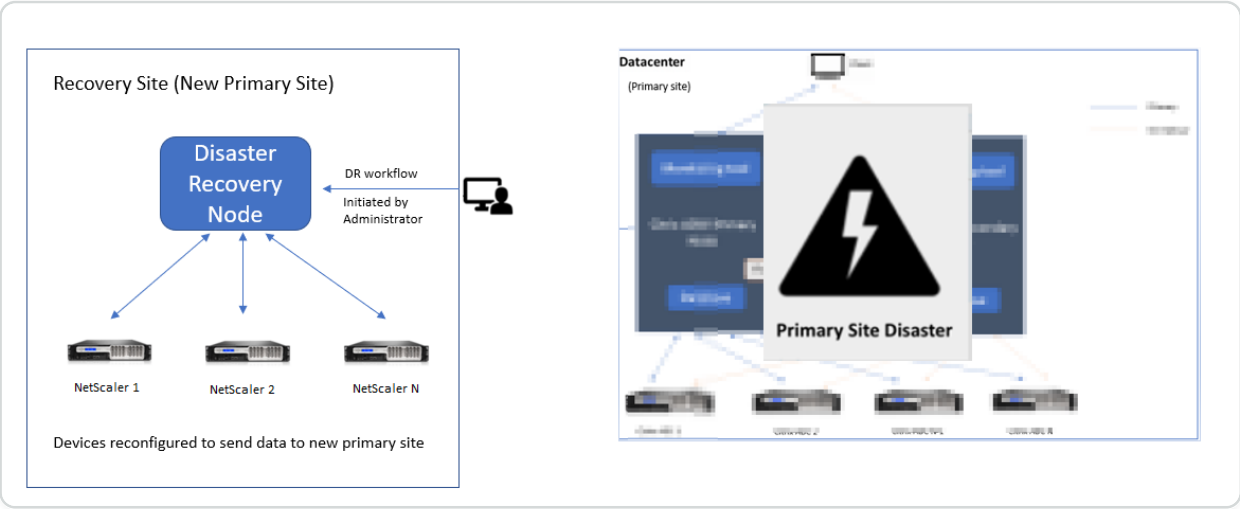
   - Configure the DR node as a license server also:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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



NOTE:

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

Post disaster recovery

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

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

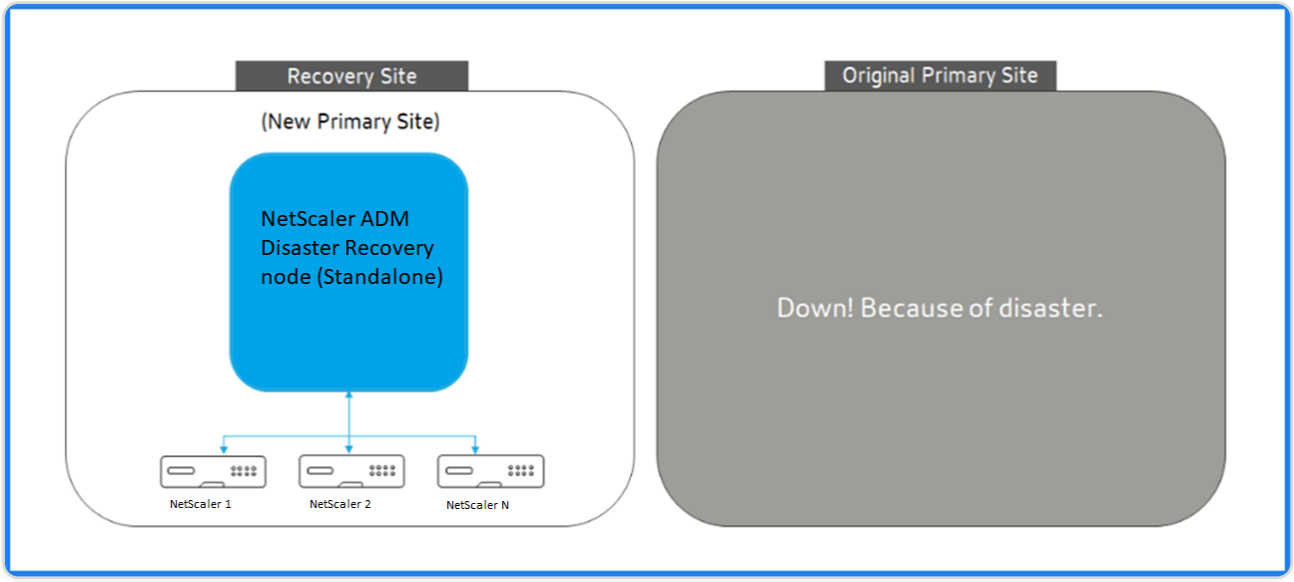
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

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

Revert configurations to the original primary site

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



For more information, see Workflow after the disaster.

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

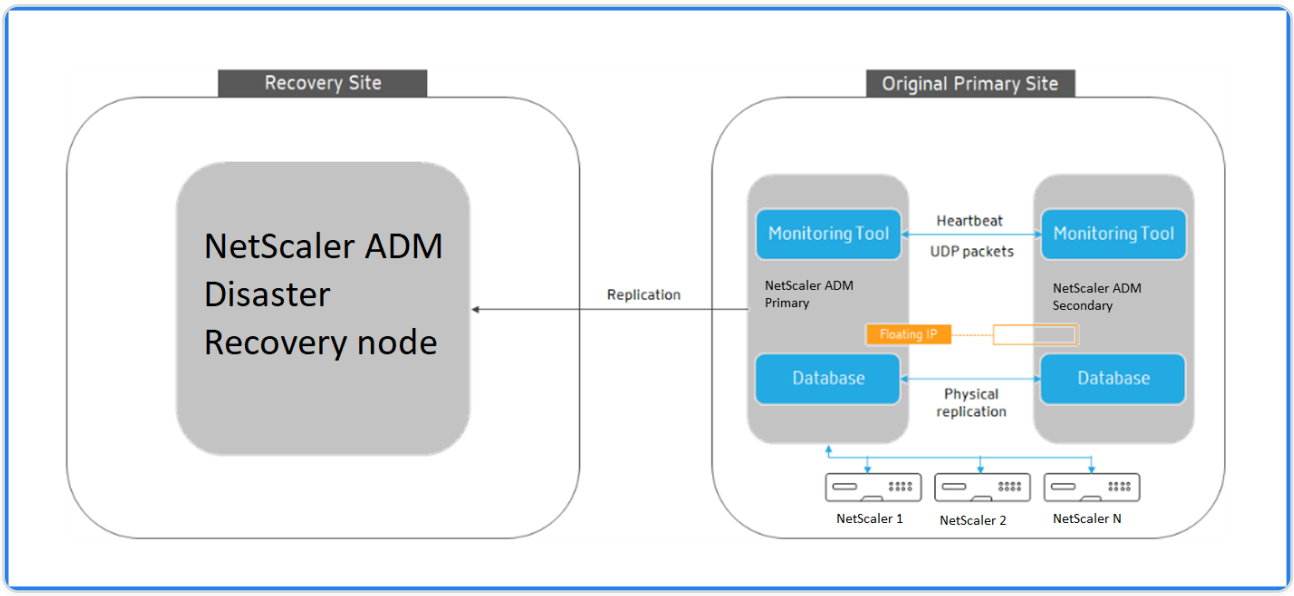
This command configures only Syslog, SNMP, and Analytics to the primary site.

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

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

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

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



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

Configure on-prem agents for multisite deployment

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

NOTE

- Installing agents for instances in remote data center is recommended but not mandatory. If necessary, users can directly add NetScaler instances to primary NetScaler ADM.
- If you have installed agents for one or more remote data centers, then the communication between the agents and the primary site is through floating IP address. For more information, see port.
- You can install agents and apply pooled licenses to the instances at one or more remote data centers. In this scenario, the communication between the primary site and one or more remote data centers is through the floating IP address.
- NetScaler ADM on-premises agent doesn't support pooled licensing.

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

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

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

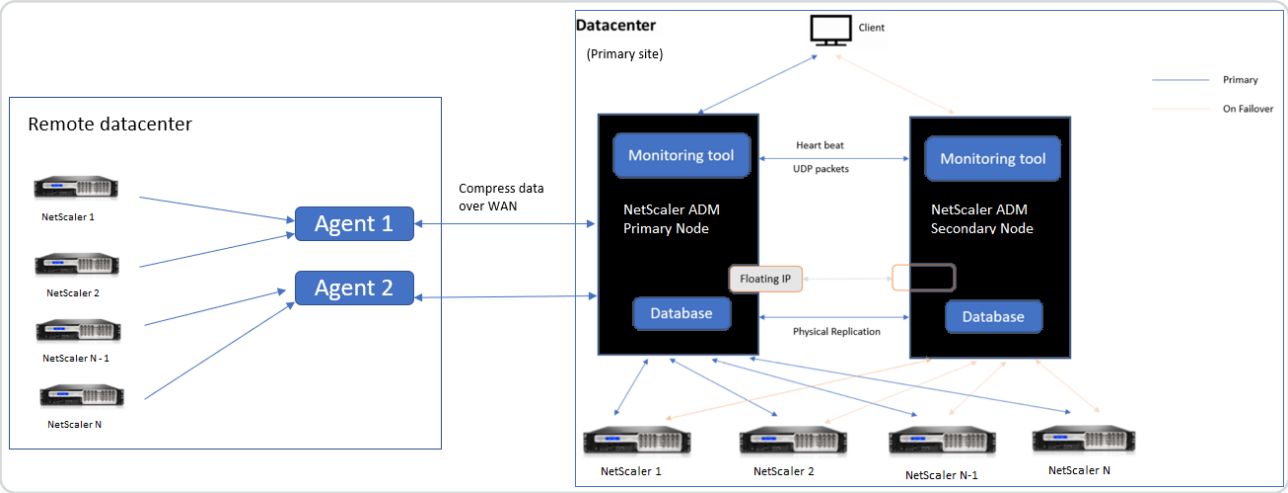
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

Architecture

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



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

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

Get started

- Install the agent in a data center
  - Register the agent
  - Attach the agent to a site
- Add NetScaler instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Add new instance
- Update an existing instance

Install the agent in a data center

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

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

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

NOTE

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

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

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

Ports

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	PORT	DETAILS	DIRECTION OF COMMUNICATION
TCP	8443, 7443, 443	For outbound and inbound communication between agent and the NetScaler ADM on-prem server.	NetScaler agent to NetScaler ADM

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

TYPE	PORT	DETAILS	DIRECTION OF COMMUNICATION
TCP	80	For NITRO communication between agent and NetScaler instance.	NetScaler ADM to NetScaler and NetScaler to NetScaler ADM
TCP	22	For SSH communication between agent and NetScaler instance. For synchronization between NetScaler ADM servers deployed in high availability mode.	NetScaler ADM to NetScaler and NetScaler agent to NetScaler
UDP	4739	For AppFlow communication between agent and NetScaler instance.	NetScaler to NetScaler ADM
ICMP	No reserved port	To detect network reachability between NetScaler ADM and NetScaler instances, or the secondary NetScaler ADM server deployed in	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	PORT	DETAILS	DIRECTION OF COMMUNICATION
		high availability mode.	
UDP	161, 162	To receive SNMP events from NetScaler instance to agent.	Port 161 - NetScaler ADM to NetScaler
			Port 162 - NetScaler to NetScaler ADM
UDP	514	To receive syslog messages from NetScaler instance to agent.	NetScaler to NetScaler ADM
TCP	5557	For Logstream communication between agent and NetScaler instances.	NetScaler to NetScaler ADM

Register the agent

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

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

      1. Citrix ADM Host Name [ADMAGENT]:
      2. Citrix ADM IPv4 address [10.102.29.214]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

```
bash-3.2# /mps/register_agent_onprem.py

--------------------------------------------------------------------------------
----------------------------------------
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows y
ou to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix AD
M floating IP Address.
--------------------------------------------------------------------------------
----------------------------------------
    Enter IP Address or URL:10.102.29.211
    Enter User Name:nsroot
    Enter Password:

Trying to register this agent with Citrix ADM  10.102.29.211
Dec  3 18:07:52 <auth.notice> ns date: date set by nsrecover
--------------------------------------------------------------------------
    Citrix ADM Agent Registration successful.
--------------------------------------------------------------------------------
```

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

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

NOTE

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

Attach an agent to a site

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

Agent actions

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

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

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

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

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

Add NetScaler instances

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

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

For more information, see Add instances to NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Attach an existing instance to the agent

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

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

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

Access the GUI of an instance to validate events

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler agent failover

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

IMPORTANT

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

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

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

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

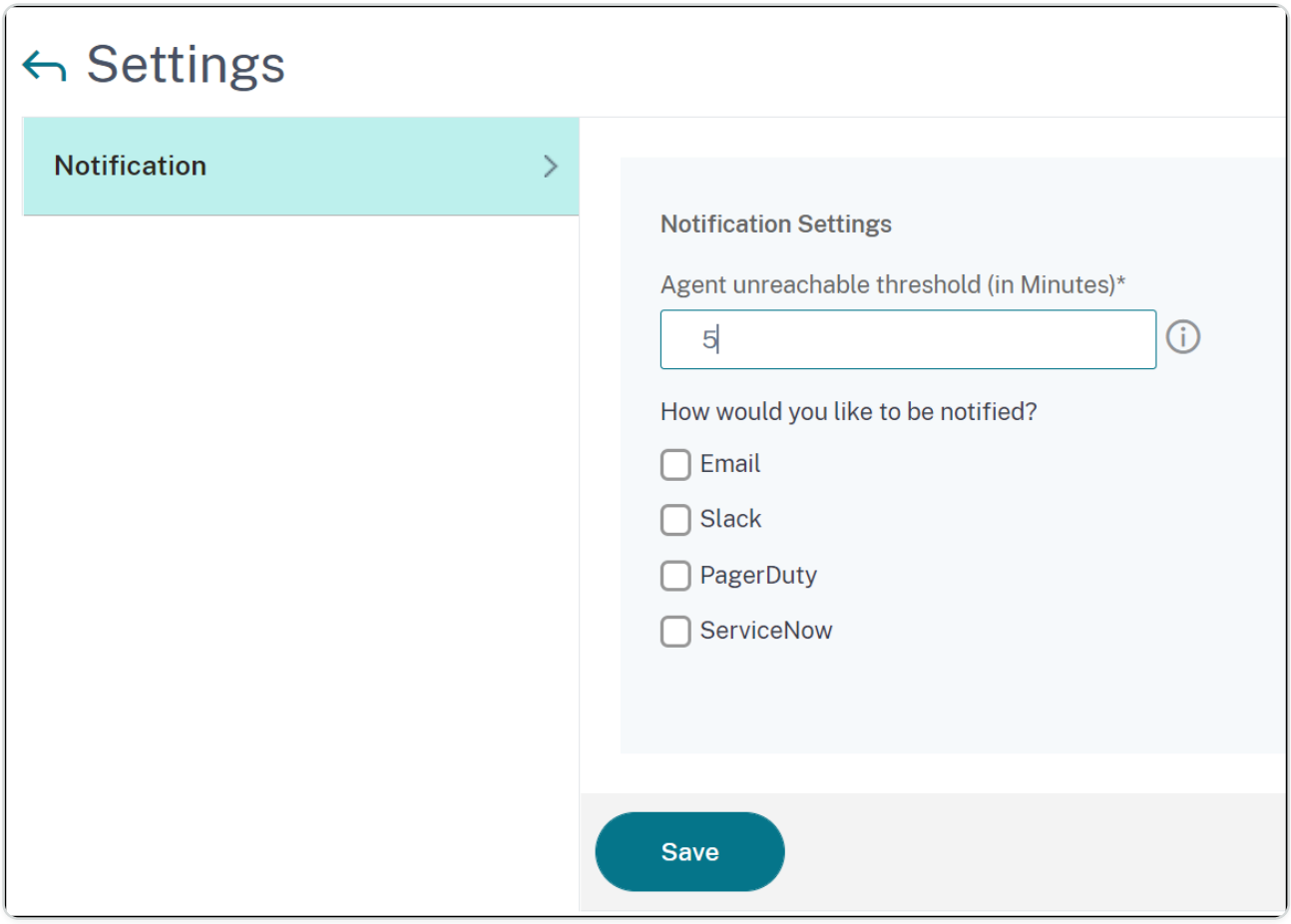
When a NetScaler agent becomes inactive (Down state) in a site, NetScaler ADM waits for five minutes for the agent to become active (Up state). If the agent remains inactive, NetScaler ADM automatically redistributes the instances among available agents in the same site.

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

Configure agent unreachable threshold and notification

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Install an ADM agent as a microservice on a Kubernetes cluster

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

Note

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

Get started

1. In NetScaler® ADM, navigate to **Infrastructure > Instances > Agents**.
2. From the **Select Action** list, select the **Download Agent Microservice** option.
3. In the **Download Agent Microservice** page, specify the following parameters:
   a. **Application ID** – A string id to define the service for the agent in the Kubernetes cluster and distinguish this agent from other agents in the same cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Note

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

d. Click **Download Yaml File**.

Install NetScaler agent in Kubernetes cluster

In the Kubernetes main node:

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

   `kubectl create -f <yaml file>`

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

   The agent is successfully created.

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

Modify the existing NetScaler ADM server node

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

5. 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.

```
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
 [yes/no]:yes
```

Provision the second server node

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-----------------------------------------------------------------------------
-------------

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

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

-------------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -----------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

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

```
-----------------------------------------------------------------------------
-------------

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

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

-------------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -----------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
    Enter Floating IP address:10.102.29.97
```

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

Deploy the two servers in a high availability mode

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

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

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

   NOTE

   After you deploy NetScaler ADM in high availability, you can either access the primary node or the floating IP address. You cannot access the secondary node from 12.1 release onwards.

5. Though you have entered the floating IP while configuring the second server node, you have an option to update the FIP on the **Systems** page. Click **HA Settings** > **Configure Floating IP Address for High Availability Mode**. You can view the floating IP address you configured earlier. You can enter a new IP address and click **OK**.

Migrate from NetScaler® Insight Center to NetScaler ADM

You can now migrate your NetScaler Insight Center deployment to NetScaler ADM without losing the existing configuration, settings, or data. With NetScaler ADM you can not only view the various analytics generated by the NetScaler instances associated with an application, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

NOTE

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

Prerequisites

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

> **NOTE**
>
> You must install NetScaler ADM 12.0 build 57.24 and then upgrade to the latest NetScaler ADM 13.1 build. For more information, see Upgrade.

- You have downloaded the NetScaler ADM 13.1 latest build .tgz image file.

Hardware requirement

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	120 GB
	Note Citrix recommends that you use **500 GB** for better performance. Also, Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor Requirements	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installation procedure

To migrate NetScaler Insight Center to NetScaler ADM:

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

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. Install NetScaler ADM by using the **./installmas** command.

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

5. After installing NetScaler ADM 12.0 build 57.24, you need to upgrade to the latest NetScaler ADM 13.1 build by performing the above steps.

After the migration, all the NetScaler instances that were discovered in the NetScaler Insight Center inventory appear in the **Infrasturcture > Instances** section of NetScaler ADM. However, for the first time you need to manually poll the virtual servers hosted in the discovered appliances.

NOTE

In NetScaler ADM, by default, there is no licensing cost to manage and monitor two virtual servers created within the discovered NetScaler instances. To monitor and manage more than two virtual servers, install the required NetScaler ADM licenses. For more details, see NetScaler ADM Licensing.

Integrate NetScaler® ADM with Citrix Director

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

- Network analysis obtains HDX™ Insight reports from NetScaler ADM and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

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

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

Prerequisites

Hardware requirements for HDX Insight to NetScaler ADM Migration

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8
Storage Space	500 GB. Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps

Minimal requirements

Before you configure the network integration, ensure that you create an RBAC user with HDX Insights access.

Software requirements

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Limitations

- The availability of this feature depends on your organization's license and your administrator permissions.
- ICA session Round Trip Time (RTT) shows data correctly for Citrix Workspace for Windows 3.4 or later and for Citrix Workspace for Mac 11.8 or later. For earlier versions of these Workspaces, the data does not display correctly.
- In the Trends view, HDX connection logon data is not collected for VDAs earlier than version 7. For earlier VDAs, the chart data is displayed as 0.
- For deployments that already have an external hard disk with storage space less than 500 GB, you cannot add another hard disk.

NOTE

- For more information on Director and for steps to integrate NetScaler ADM with Director, see `<https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html>`.
- For more information on HDX Insight, see `<http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html>`.

Attach an extra disk to NetScaler® ADM

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- Estimate storage requirements and attach an extra disk to the server at the time of initial deployment of NetScaler ADM.
- For a NetScaler ADM single-server deployment, you can attach only one disk to the server in addition to the default disk.
- For a NetScaler ADM high availability deployment, you must attach an extra disk to each node. The size of both disks must be identical.
- If you had earlier attached an external disk of lower capacity, you must remove the disk before attaching a new disk.
- You can attach an extra disk of capacity greater than 2 terabytes. If necessary, the size of the disk can be lower than 2 terabytes also.
- Citrix recommends using solid-state drive (SSD) technology for NetScaler ADM deployments.

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

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

Attach an extra disk in a standalone NetScaler ADM

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Start the NetScaler ADM virtual machine.

NetScaler ADM disk partition tool

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

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

   NOTE

   - It is not possible to resize existing disks beyond 2 terabytes without losing data. This is due to a known limitation on the platform.
   - To create a storage capacity greater than 2 terabytes, you must remove the existing partitions and create partitions using this new tool.

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

   NOTE

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

Launch the disk partition tool

1. Open an SSH connection to the NetScaler ADM by using an SSH client, such as PuTTY.
2. Log on to the NetScaler ADM by using the `nsrecover/nsroot` credentials.
3. Switch to the shell prompt and type:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bash-3.2# /mps/DiskPartitionTool.py

-------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
-------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

NOTE

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

Create partitions in the new additional disk

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

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

NOTE

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

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

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

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

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

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

System going down IMMEDIATELY
```

After the restart, the new partition is mounted at /var/mps.

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

The swap partition added shows up as swap space in the output of the "create" command.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resize the partitions in the existing additional disk

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

NOTE

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

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

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

The "resize" command checks for all preconditions and proceeds if all preconditions are met and after you have given consent to resizing. It stops the processes accessing the disk, which includes the NetScaler ADM subsystems, PostgreSQL DB processes, and NetScaler ADM monitor process. Once the processes are stopped, the disk is unmounted to prepare it for resizing. The resizing is done by extending the partition to occupy the complete available space and then growing the file system. If a swap partition exists on the disk, it is deleted and recreated at the end of the disk after resizing. The swap partition is discussed in the **Create** command section of the document.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

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

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

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

System going down IMMEDIATELY
```

After rebooting, the increase in size can be observed using the "df" command. Here is the before and after details after you increase the size:

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove the partitions in the additional disk

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

NOTE

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

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

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

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

```
(dpt): remove

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

Are you sure you want to continue (Y/N): y
```

When you type "y," the command unmounts the disk and removes all partitions on the disk.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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

Restart the virtual machine

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

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

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

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...

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

System going down IMMEDIATELY
```

Create a backup file of the disk data

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

NOTE

Creating a backup file requires disk space. Citrix recommends that you ensure there is sufficient disk space available (50% or more) before backup commands are run.

1. Stop ADM.

   ```
   /mps/masd stop
   ```

2. Stop PostgreSQL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

3. Stop ADM Monitor.

```
/mps/scripts/stop_mas_monit.sh
```

4. Create a tarball.

```
cd /var

tar cvfz /var/mps/mps_backup.tgz mps
```

NOTE

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

5. Generate checksum.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. Copy the tarball and checksum files to a remote server.
7. Validate the correctness of the copied tarball. Generate a checksum of the transferred file and compare with the source checksum.
8. Remove the tarball from the ADM virtual machine.

```
cd /var/mps/

rm mps_backup.tgz  mps_backup_checksum
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

Info command:

The **info** command provides information about the attached secondary disk if the disk exists. The command provides the device name, the partition scheme, size in human-readable form, and the number of disk blocks. The scheme can be MBR or GPT. An MBR scheme means the disk was partitioned using an earlier version of NetScaler ADM version. The MBR/GPT based partition can be resized but not beyond 2 terabytes. GPT partition scheme means that the disk was partitioned using NetScaler ADM 12.1 or later.

NOTE

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

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

Create_swapfile command:

The default swap partition on the primary disk of NetScaler ADM is 4 GB and therefore, the default swap space is 4 GB. For the default memory configuration of NetScaler ADM which is 2 GB, this swap space is sufficient. However, when you run NetScaler ADM with a higher memory configuration, you need to have more swap space allocated on the disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Swap partition is usually a dedicated partition that is created on a hard disk drive (HDD) during the installation of the operating system. Such a partition is also referred to as a swap space. Swap partition is used for virtual memory that simulates the additional main memory.

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

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

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

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
CPU:  1.7% user,  0.0% nice,  0.8% system,  0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user,  0.0% nice,  7.6% system,  5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

Exit command:

To exit from the tool, type exit and press the **Enter** key.

```
(dpt): exit
bash-3.2#
```

Attach additional disks to NetScaler ADM deployed in high availability

Consider that you have configured a pair of NetScaler ADM servers in a high availability set up without any secondary disks. Also, consider that you have added 2 or more NetScaler instances, checked and ensured all processes are running. You might want to add secondary disks to the virtual machines in this setup. In a high availability set up, you must add additional disks to both nodes as detailed in this task:

1. Shut down the secondary node.
2. Add an additional disk through the hypervisor.

   NOTE

   Ensure not to extend the secondary node main disk.

3. Start the secondary node.
4. Run the partition tool on the secondary node.
5. After the disk is added, the secondary node restarts.
6. Shut down the secondary node after it restarts.
7. Shut down the primary node.
8. Add an additional disk through the hypervisor.

   NOTE

   Ensure not to extend the primary node main disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Start the primary node.
10. Run the partition tool on the primary node.
11. After the disk is added, the primary node restarts.
12. After the primary node is up and running, start the secondary node.
13. Ensure that the secondary node is up and running and the databases have synchronized.
14. Confirm that all data still exists.

To increase the capacity of RAM on both the nodes:

1. Shutdown ADM_Secondary and increase the RAM size as required. Don't restart the node.
2. Shutdown ADM_Primary and increase the RAM size as required.

   Ensure that you increase the RAM size equally on both nodes. For example, if you increase the RAM size on the primary node to 16 GB, do the same on the secondary node as well.
3. Restart the ADM_Primary.
4. After the ADM_Primary reboots, check that it is the primary node.
5. Now start the ADM_Secondary node. After it restarts, ensure that it has come up as secondary and the DB sync is working.
6. Now confirm that all data still exists.

NOTE

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure

You can access a NetScaler® ADM server only by using the GUI. You have to access the GUI to add instances, manage, and monitor your instances and apps, view analytics, and configure the NetScaler ADM server.

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

The following browsers are supported.

WEB BROWSER	VERSION
Internet Explorer	11.0 and later
Google Chrome	Chrome 19 and later
Safari	Safari 5.1.1 and later
Mozilla Firefox	Firefox 3.6.25 and later

To access the NetScaler ADM GUI:

Log on to NetScaler ADM using the administrator credentials.

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

- Add instances to NetScaler ADM. You must add instances to the NetScaler ADM server if you want to manage and monitor these instances.
- Enable analytics on virtual servers. To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.
- Configure NTP server on NetScaler ADM. You have to configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize its clock with the NTP server.
- Configure system settings for optimal NetScaler ADM performance. Before you start using NetScaler ADM to manage and monitor your instances and applications, it is recommended that you configure a few system settings that ensure optimal performance of your NetScaler ADM server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add instances to NetScaler® ADM

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

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

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

NOTE

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

How to create a NetScaler profile

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

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

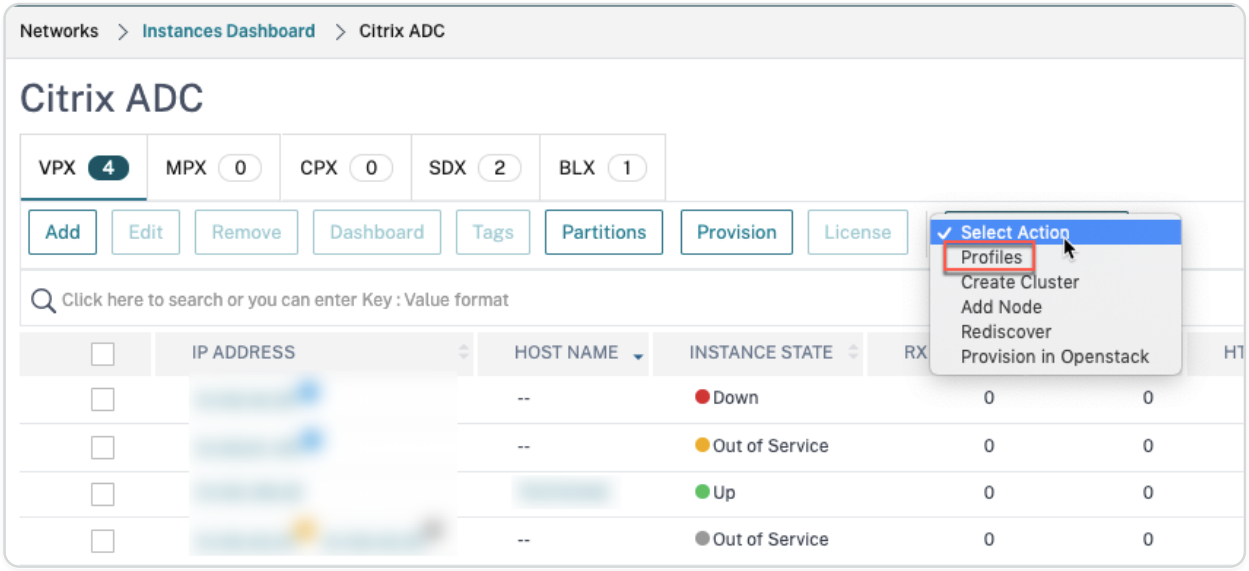
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Ensure to use the super administrator account to create an instance profile.

To create a NetScaler profile from the Instance page:

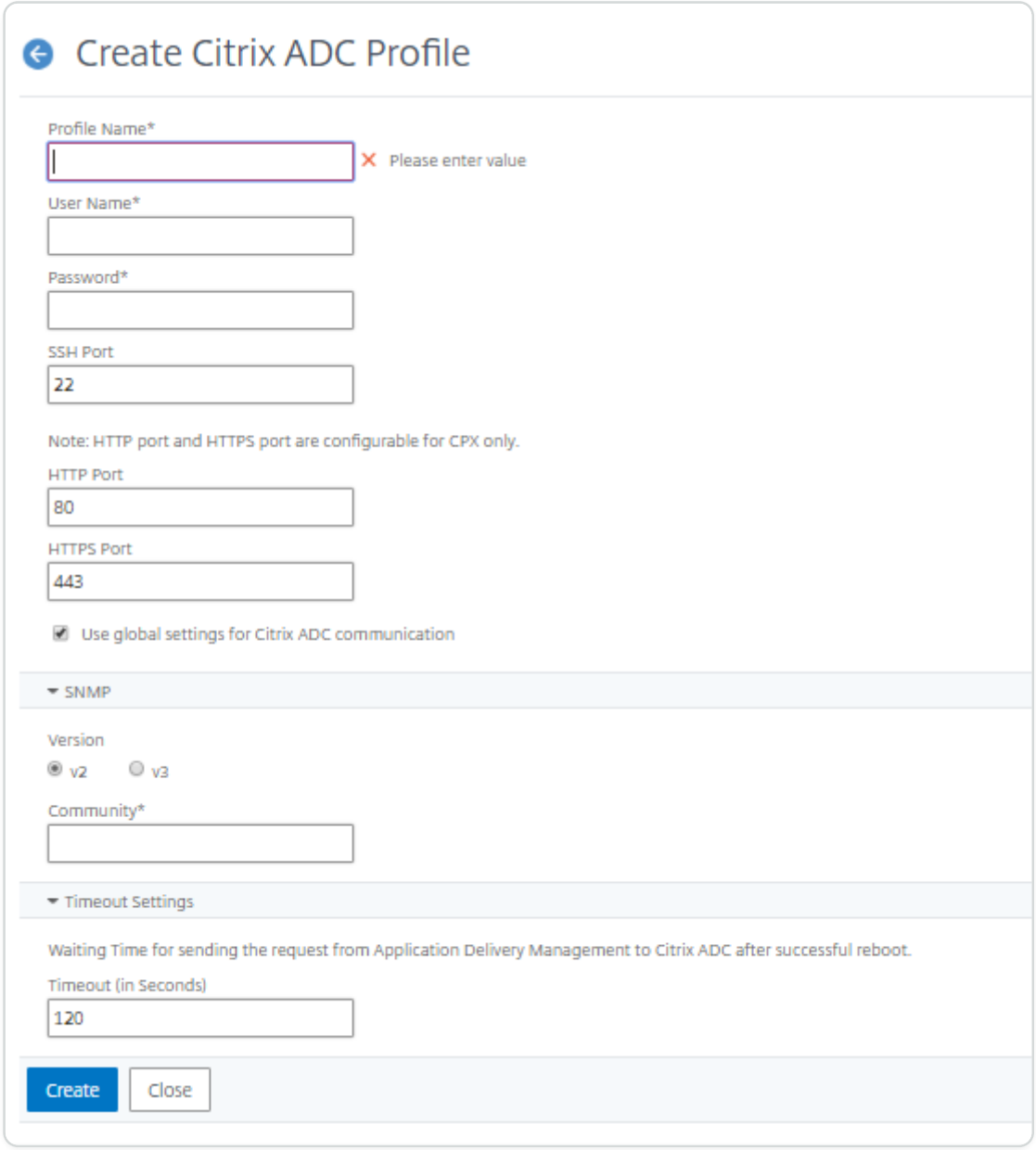
1. Navigate to **Infrastructure > Instances**.
2. Select an Instance. For example, NetScaler.
3. On the NetScaler page, under **Select Action** select **Profiles**.



4. On the **Admin Profiles** page, select **Add**.

5. On the **Create NetScaler Profile** page, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. **Profile Name**: Specify a profile name for the NetScaler instance.

b. **User Name**: Specify a user name to log on to the NetScaler instance.

c. **Password**: Specify a password to log on to the NetScaler instance.

d. **SSH Port**: Specify the port for SSH communication between NetScaler ADM and the NetScaler instance.

e. **HTTP Port**: Specify the port for HTTP communication between NetScaler ADM and the NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE**
>
> The default HTTP port is 80. You can also specify the non-default or customized HTTP port that you might have configured in your NetScaler CPX instance. The customized HTTP port can be used for communication only between NetScaler ADM and NetScaler CPX.

f. **HTTPS Port**: Specify the port for HTTPS communication between NetScaler ADM and the NetScaler instance.

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

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

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

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

   ii. If you select SNMPv3, specify the **Security Name** and **Security Level**. Based on the security level, select the **Authentication Type** and **Privacy Type**.

   > **NOTE**
   >
   > For NetScaler SDX, only **SNMPv2** is supported.

i. **Timeout Settings**: Specify the time that NetScaler ADM must wait before sending a connection request to the NetScaler instance after a restart.

j. Select **Create**.

Add ADC instances to NetScaler ADM

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

NOTE

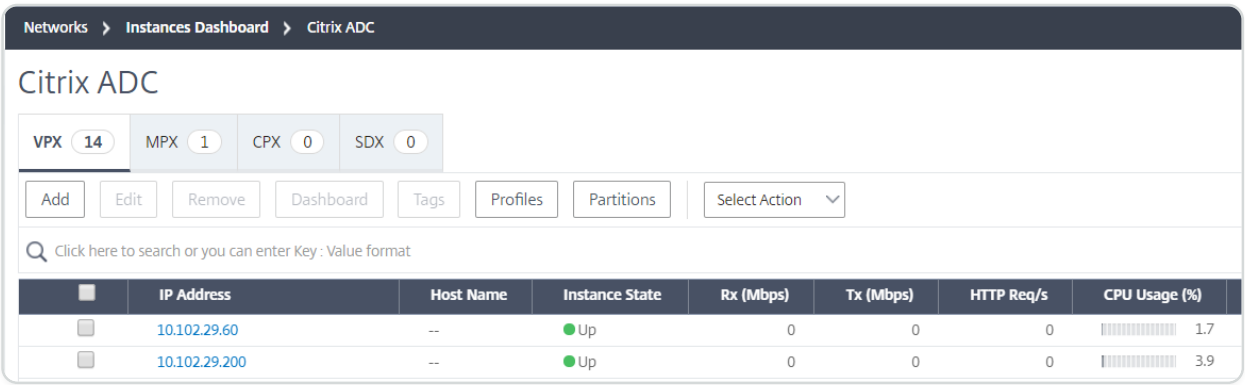
- To add NetScaler instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on NetScaler ADM, the cluster is represented by the cluster IP address only.
- For NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

If two NetScaler ADM servers are set up in high availability mode, when an instance is added, the traffic source is through the ADM floating IP address.

When you add an instance from a remote data that is configured with an on-prem agent, the traffic source is through the ADM agent.

To add an instance to NetScaler ADM:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Infrastructure > Instances > NetScaler**. Select the type of instance you want to add (for example, NetScaler VPX) and click **Add**.



3. Select one of the following options:

   - **Enter Device IP address** - For NetScaler instances, specify either the host name or IP address of each instance, or a range of IP addresses.

     If you want to discover an ADC HA pair using SNIP, ensure the Independent Network Configuration (INC) mode is enabled. And, specify the SNIP addresses in the following format:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<SNIP of primary instance>#<SNIP of secondary instance>
```

For example, `10.10.10.11#10.10.10.12`

- **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.

4. From **Profile Name**, select the appropriate instance profile, or create a new profile by clicking the + icon.
5. From **Site**, select the location where you want to add the instance, or create a new location by clicking the **+** icon.
6. Click **OK** to initiate the process of adding instances to NetScaler ADM.

NOTE

If you want to rediscover an instance, navigate to **Infrastructure > Instances > NetScaler**. Select the instance type (for example, VPX) and select the instance you want to rediscover, and then from the **Select Action** list, click **Rediscover**.

Add NetScaler CPX instances to NetScaler ADM

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

1. Navigate to **Infrastructure > Instances > NetScaler** and click **CPX** tab.
2. Click **Add** to add new CPX instances in NetScaler ADM.
3. The **Add NetScaler CPX** page opens. Enter the values for the following parameters:

   a. You can add CPX instances by providing either the reachable IP address of the CPX instance or the IP address of the Docker container where the CPX instance is hosted.

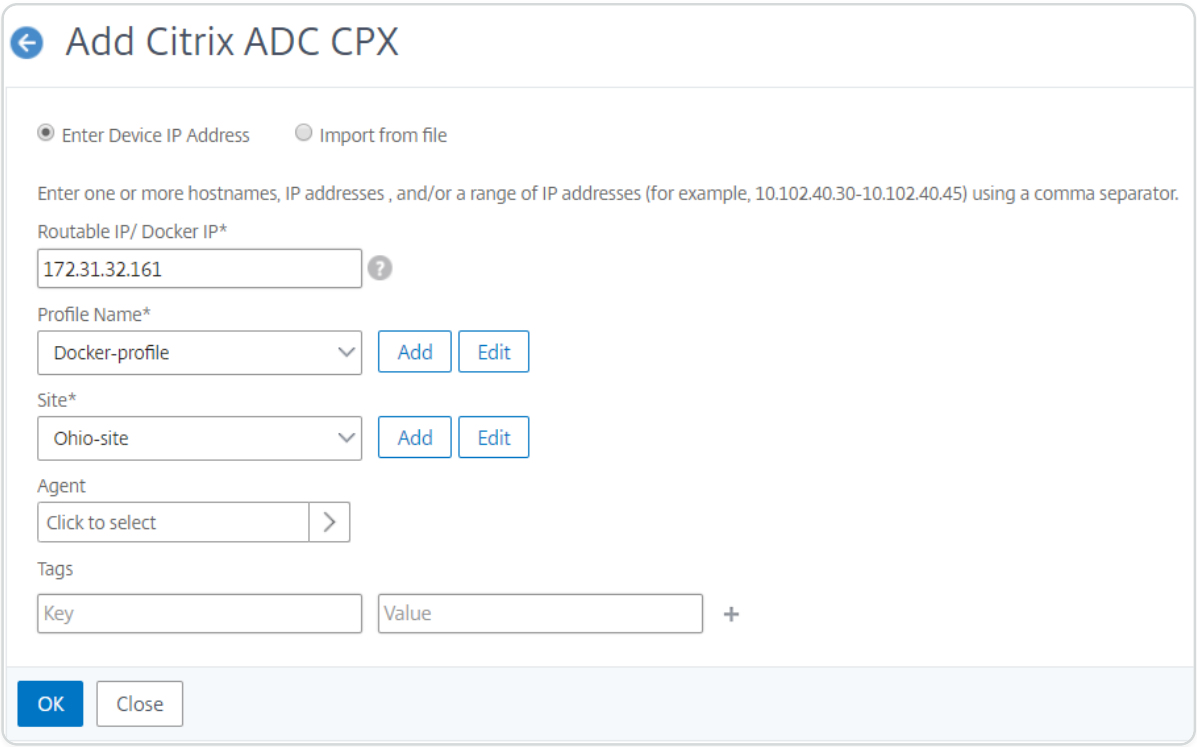
   b. Select the profile of the CPX instance.

   c. Select the site where the instances are to be deployed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Select the agent.

e. As an option, you can enter the key-value pair to the instance. Adding key-value pair makes it easy for you to search for the instance later.



NOTE

For NetScaler CPX instances, you must specify the **HTTP, HTTPS, SSH**, and **SNMP** port details of the host while creating the CPX instance profile. You can also specify the range of ports that were published by the host in the **Start Port** and **Number of ports** field.

4. Click **OK**.

Add a standalone NetScaler BLX instance in NetScaler ADM

A standalone NetScaler BLX instance is a single instance that is running on the dedicated host Linux server.

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **BLX** tab, click **Add**.
3. Select the **Standalone** option from the **Instance Type** list.
4. In the **IP address** field, specify the IP address of the BLX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
6. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

   IMPORTANT

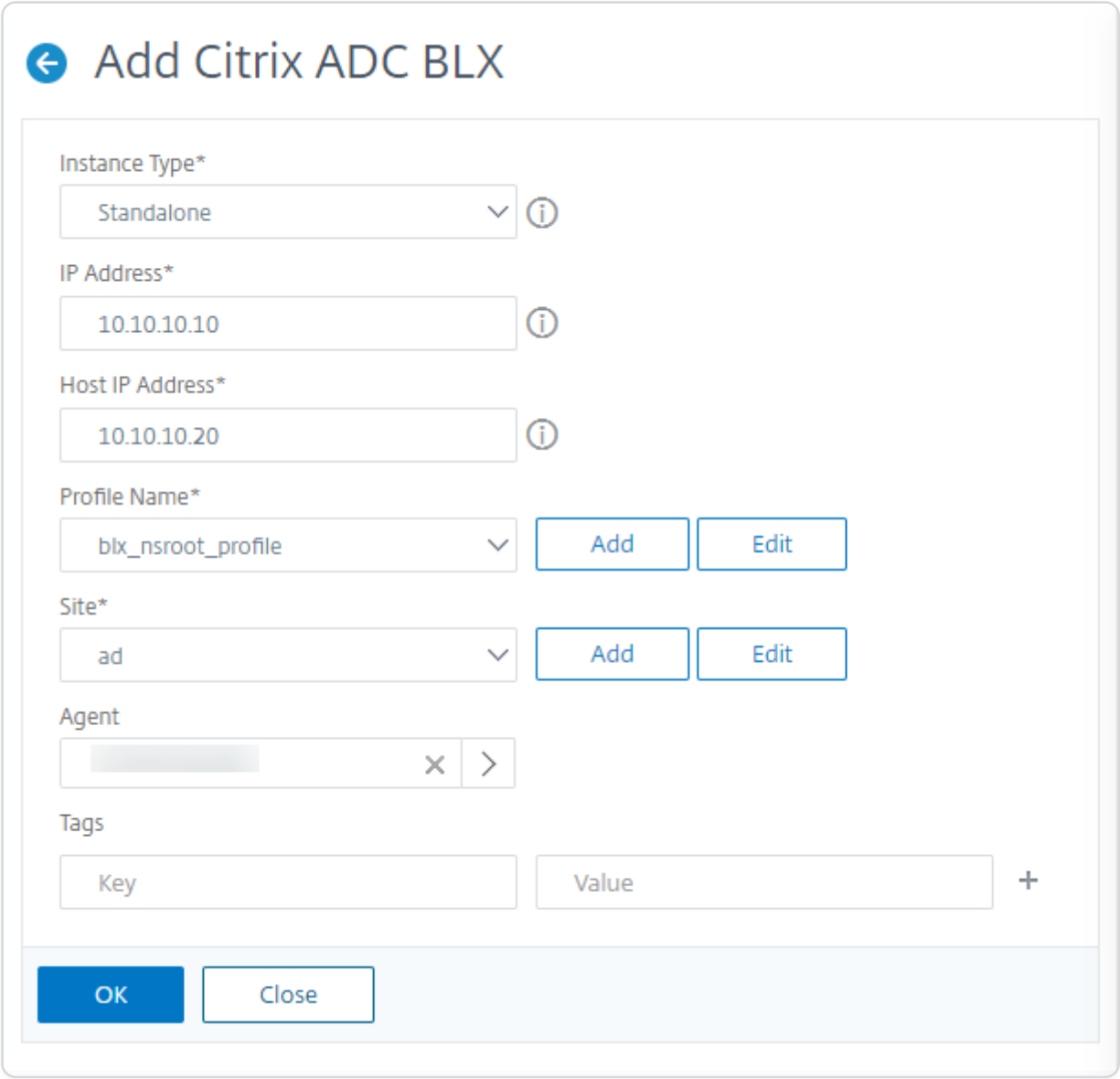
   Ensure you have specified the correct host user name and password of the Linux server in the profile.

7. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.
8. In the **Agent** list, select the NetScaler agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler ADM, that agent is selected by default.
9. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Add high-availability NetScaler BLX instances in NetScaler ADM

The high-availability NetScaler BLX instances that run on different host Linux servers. A Linux server cannot host more than one BLX instances.

1. In the **BLX** tab, click **Add**.
2. Select the **High Availability** option from the **Instance Type** list.
3. In the **IP address** field, specify the IP address of the BLX instance.
4. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
5. In the **Peer IP address** field, specify the IP address of the peer BLX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In the **Peer Host IP address** field, specify the IP address of the Linux server where the peer BLX instance is hosted.
7. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

   IMPORTANT

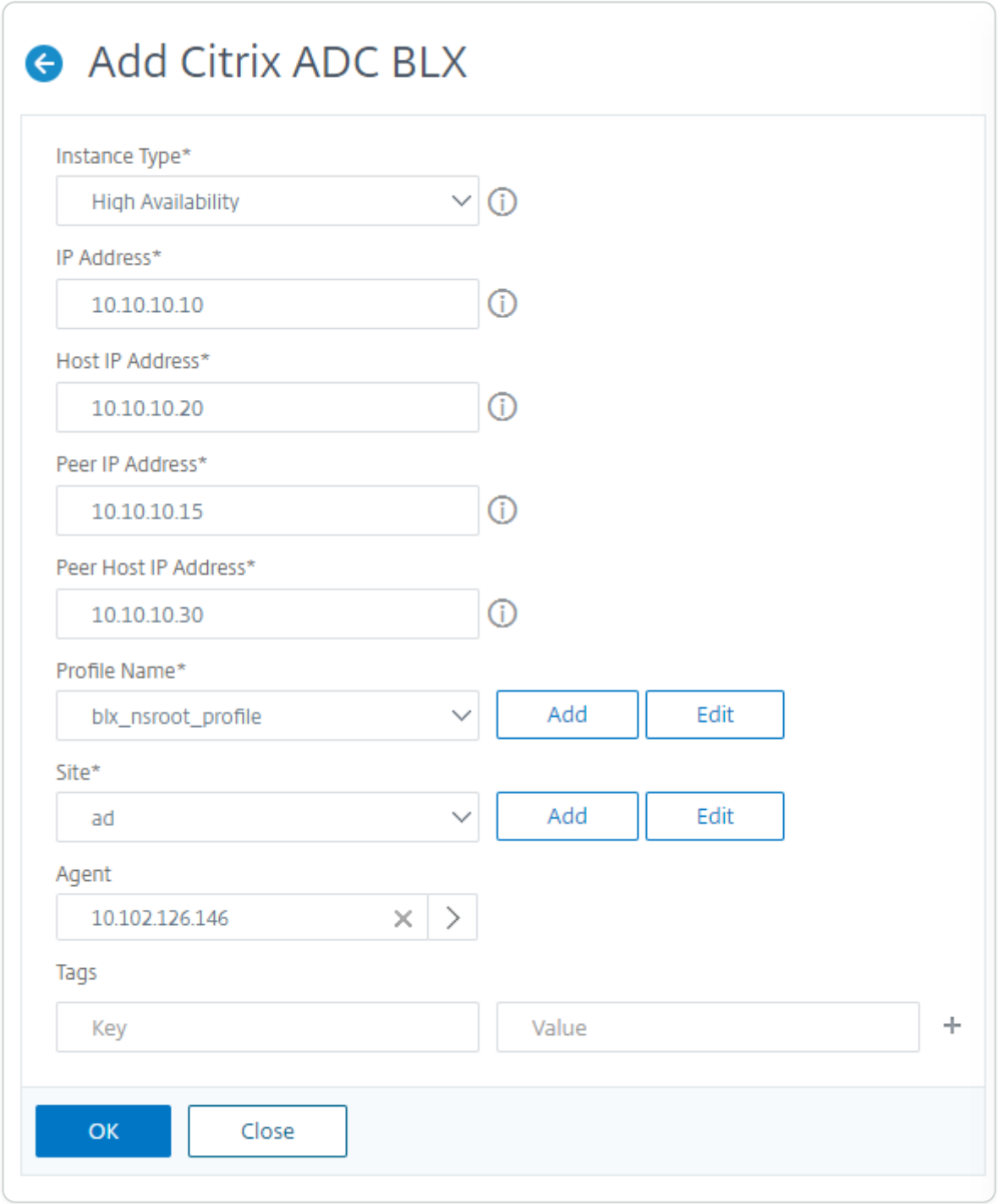
   Ensure you have specified the correct host user name and password of the Linux server in the profile.

8. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.
9. In the **Agent** list, select the NetScaler agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler ADM, that agent is selected by default.
10. Click **OK**.

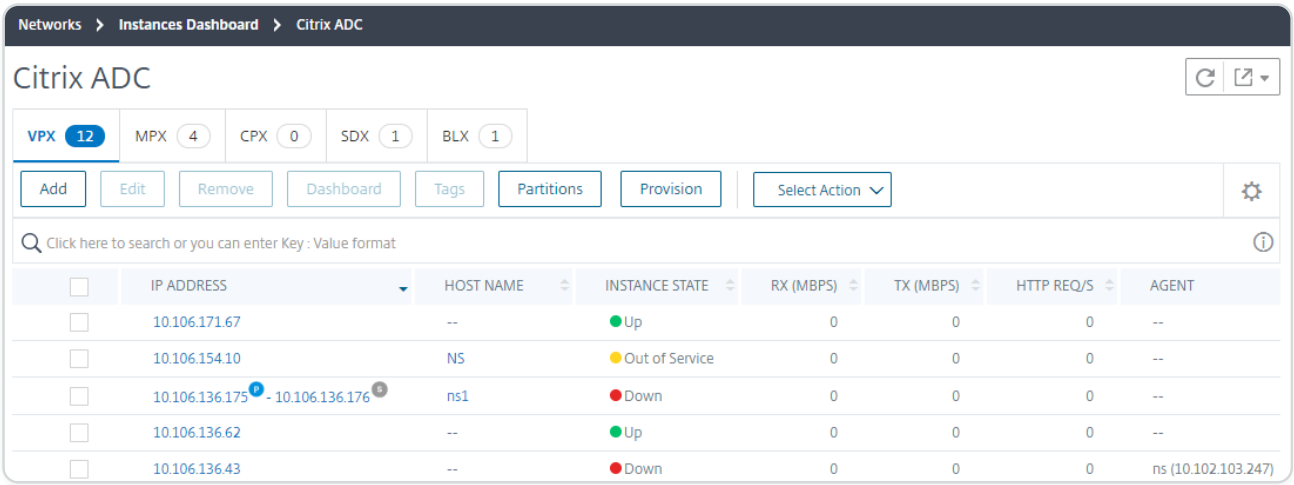
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Access an instance GUI from the NetScaler ADM

1. Navigate to **Infrastructure > Instances** > **NetScaler**.
2. Select the type of instance you want to access (for example, VPX, MPX, CPX, SDX, or BLX).
3. Click the required NetScaler IP address or host name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

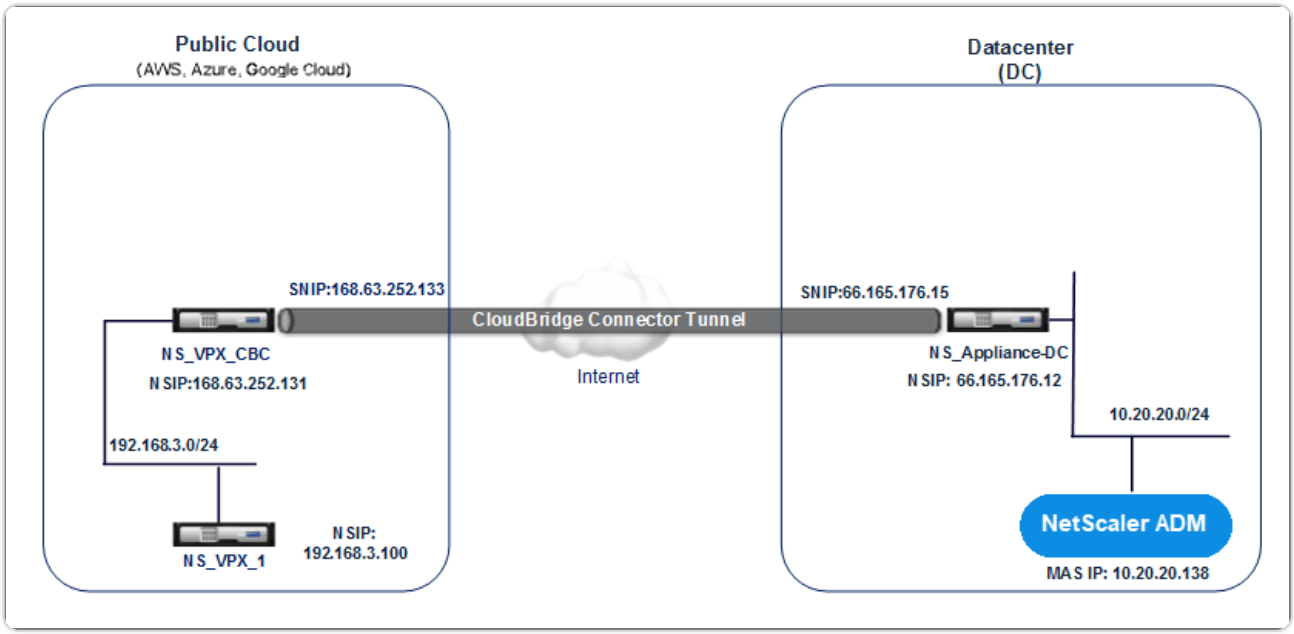


The GUI of the selected instance appears in a pop-up window.

Add NetScaler VPX instances deployed in cloud to NetScaler ADM

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

The following sample topology uses Citrix CloudBridge Connector for Layer 3 connectivity between NetScaler ADM and the NetScaler VPX instances deployed in the cloud.



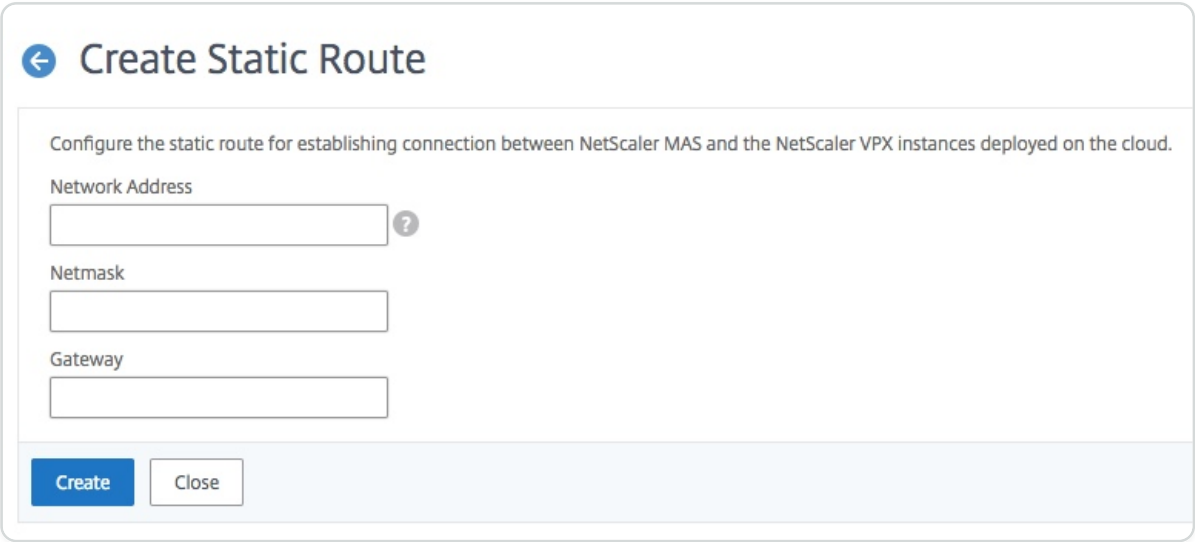
A Citrix CloudBridge Connector tunnel is set up between NetScaler appliance NS_Appliance-DC, in a data center DC, and NetScaler virtual appliance (VPX) NS_VPX_CBC in the public cloud. NS_Appliance-DC and NS_VPX_CBC enable the communication between NetScaler ADM and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the NetScaler VPX instance, NS_VPX_1, deployed in the public cloud. After the communication is established, you can discover NS_VPX_1 in NetScaler ADM.

To configure this topology:

1. Install, configure, and start a NetScaler VPX instance in the public cloud.
   - For instructions, see Install NetScaler VPX on AWS.
   - For instructions, see Install NetScaler VPX on Microsoft Azure.
   - For instructions, see Install NetScaler VPX on Google Cloud.
2. Deploy and configure a NetScaler physical appliance, or provision and configure a NetScaler virtual appliance (VPX) on a virtualization platform in the data center.
   - For instructions, see Install a NetScaler VPX instance on Citrix Hypervisor.
   - For instructions, see Install Citrix virtual appliances on VMware ESXi.
   - For instructions, see Install NetScaler virtual appliances on Microsoft Hyper-V.
3. Configure the Citrix CloudBridge Connector between the data center and the public cloud. For instructions, see Configuring Citrix CloudBridge Connector.
4. Configure the static route for establishing connection between NetScaler ADM and the NetScaler VPX instances deployed on the cloud, as follows:
   a. Log on to NetScaler® ADM.
   b. Navigate to **System \> Static Routes** and click **Add**.



   c. In the **Network Address** field, enter the address of the network that you want to establish a static route from NetScaler ADM through the connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. In the **Netmask** field, enter the netmask for the network.

e. In the **Gateway** field, enter the address of the gateway.

5. Add the NetScaler VPX cloud instances to the NetScaler ADM by specifying the range of IP addresses of NetScaler VPX instances in the public cloud. For detailed instructions, Add Instances to NetScaler ADM.

Manage licensing and enable analytics on virtual servers

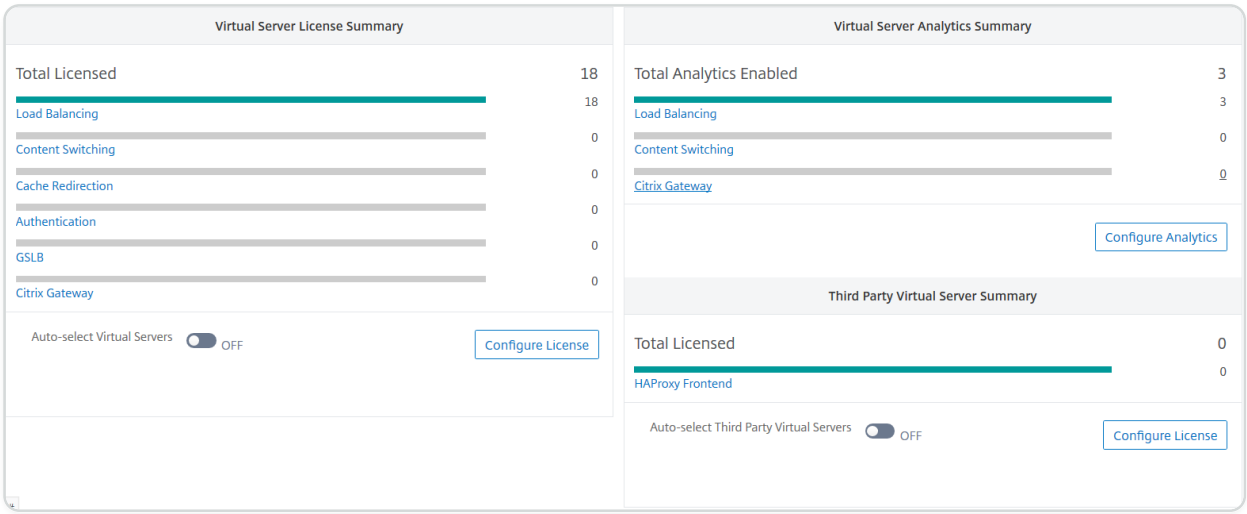
NOTE

- By default, the **Auto Licensed Virtual Servers** option is enabled. You must ensure to have sufficient licenses to license the virtual servers. If you have limited licenses and want to license only the selective virtual servers based on your requirement, disable the **Auto Licensed Virtual Servers** option. Navigate to **Settings > Licensing & Analytics Configuration** and disable the **Auto Licensed Virtual Servers** option under **Virtual Server License Allocation**.

The process of enabling analytics is simplified. You can license the virtual server and enable analytics in a single workflow.

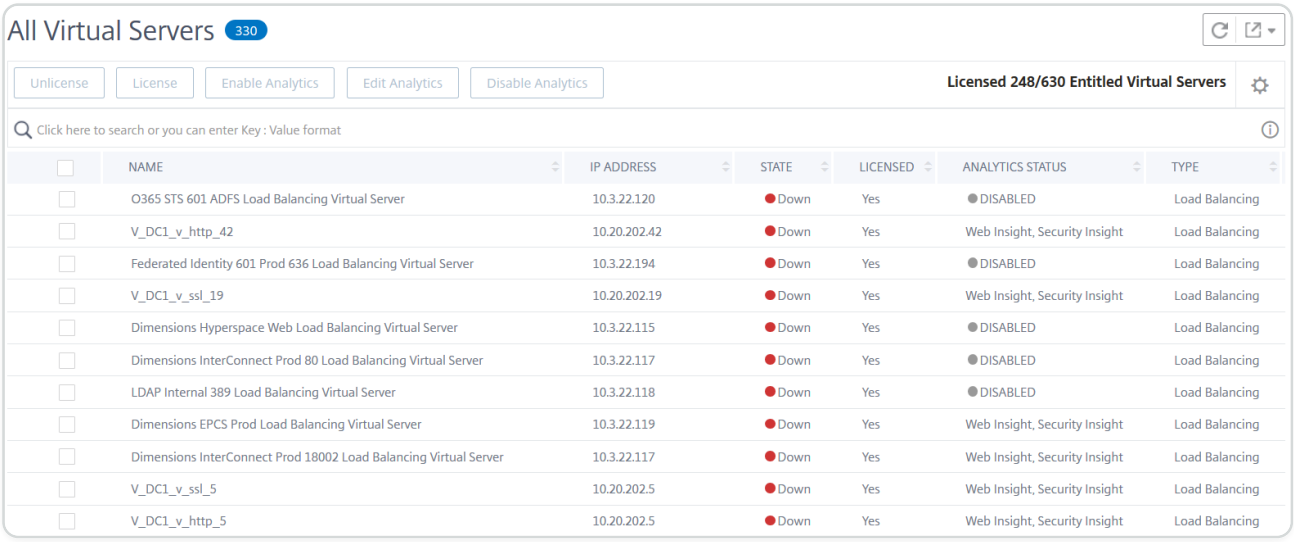
Navigate to **Settings > Licensing & Analytics Configuration** to:

- View the **Virtual Server Licence Summary**
- View the **Virtual Server Analytics Summary**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you click **Configure License** or **Configure Analytics**, the **All Virtual Servers** page is displayed.



On the **All Virtual Servers** page, you can:

- Apply license for unlicensed virtual servers
- Remove license for licensed virtual servers
- Enable analytics on licensed virtual servers
- Edit analytics
- Disable analytics

NOTE

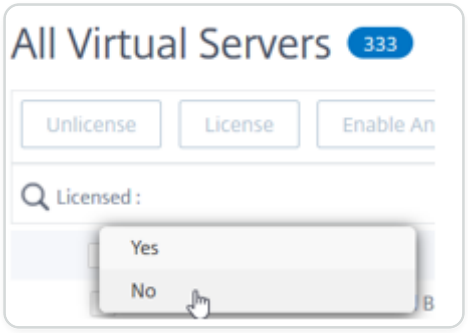
The supported virtual servers to enable analytics are Load Balancing, Content Switching, and NetScaler Gateway.

Manage licensing on virtual servers

To license the virtual servers, from the **All Virtual Servers** page:

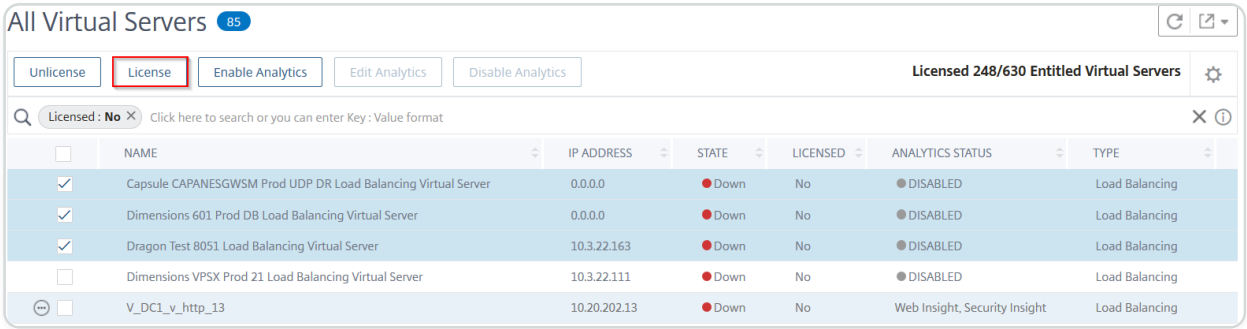
1. Click the search bar, select **Licensed**, and select **No**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The filter is now applied and only the unlicensed virtual servers are displayed.

2. Select the virtual servers and then click **License**.



To unlicense the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **Yes**.
2. Select the virtual servers and click **Unlicense**.

Enable analytics

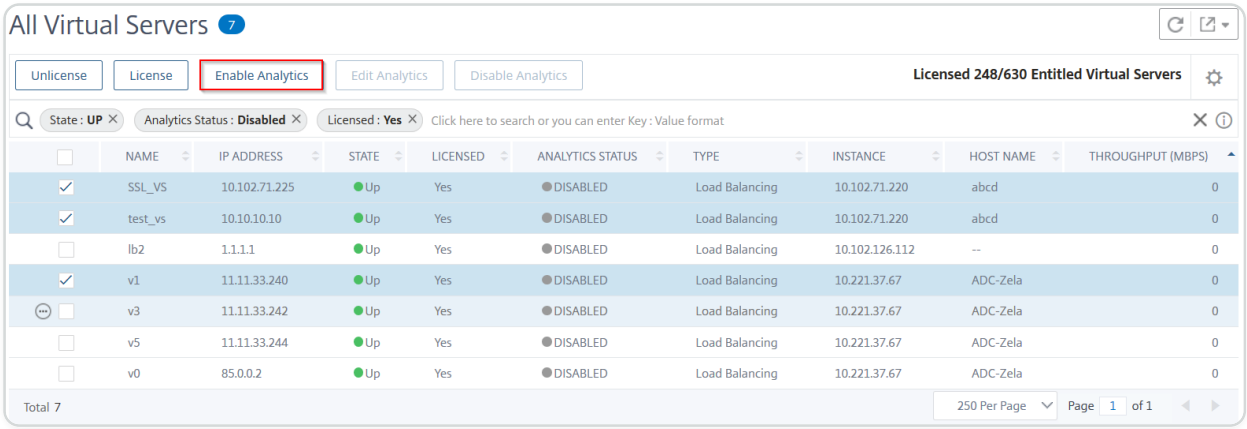
The following are the prerequisites to enable analytics for virtual servers:

- Ensure that virtual servers are **licensed**
- Ensure that analytics status is **Disabled**
- Ensure that virtual servers are in **UP** status

You can filter the results to identify the virtual servers that are mentioned in the prerequisites.

1. Click the search bar and select **State** and then select **UP**.
2. Click the search bar and select **Licensed**, and then select **Yes**.
3. Click the search bar and select **Analytics Status**, and then select **Disabled**.
4. After applying the filters, select the virtual servers, and then click **Enable Analytics**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

Alternatively, you can enable analytics for a particular instance:

a. Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.

b. Select the instance and from **Select Action** list, select **Configure Analytics**

c. On the Configure Analytics on Virtual Servers page, select the Virtual Server and click **Enable Analytics**.

5. On the **Enable Analytics** window:

a. Select the insight types (Web Insight or WAF Security Violations)

b. Select **Logstream** as Transport Mode

NOTE

For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.

For more information about IPFIX and Logstream, see Logstream overview.

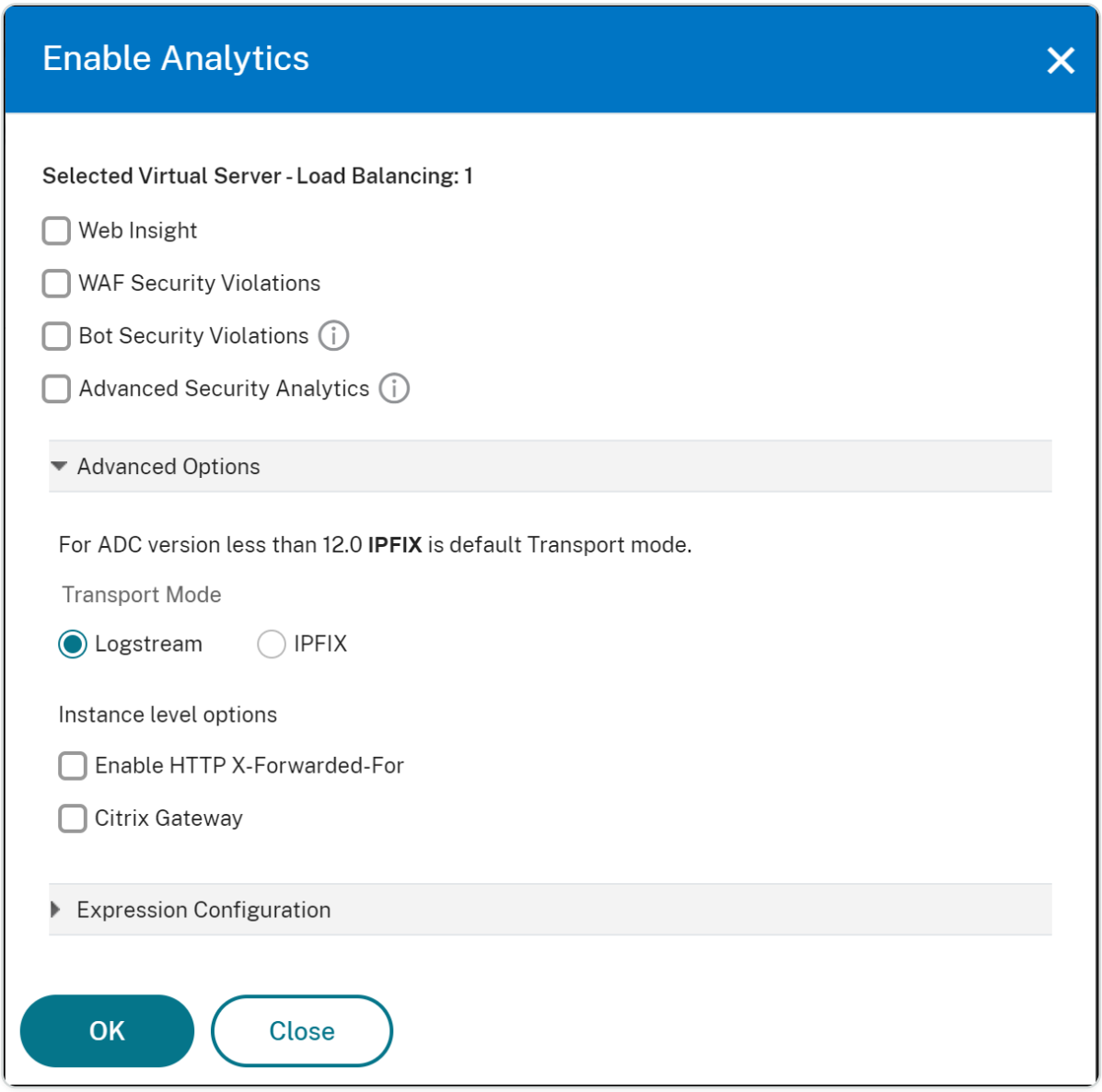
c. Under **Instance level options**:

- **Enable HTTP X-Forwarded-For** - Select this option to identify the IP address for the connection between client and application, through HTTP proxy or load balancer.
- **NetScaler Gateway** - Select this option to view analytics for NetScaler Gateway.

d. The Expression is true by default

e. Click **OK**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

- If you select virtual servers that are not licensed, then NetScaler® ADM first licenses those virtual servers and then enables analytics
- For admin partitions, only **Web Insight** is supported
- For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

After you click **OK**, NetScaler ADM processes to enable analytics on the selected virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

NetScaler ADM uses NetScaler SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between NetScaler agent and NetScaler instance, ensure you open the following port to enable NetScaler ADM to collect AppFlow traffic:

TRANSPORT MODE	SOURCE IP	TYPE	PORT
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Edit analytics

To edit analytics on the virtual servers:

1. Select the virtual servers

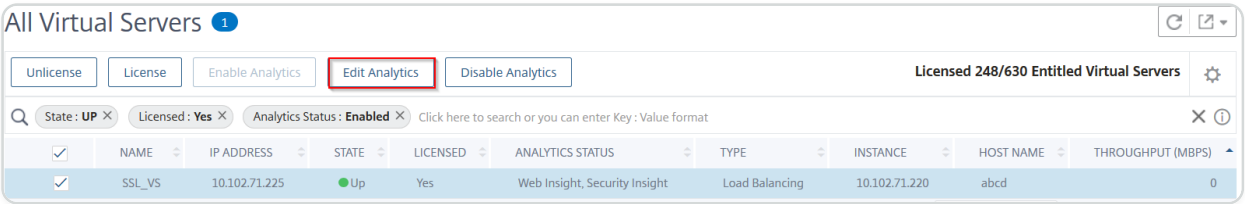
   Note

   Alternatively, you can also edit analytics for a particular instance:

   a. Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.

   b. Select the instance and click **Edit Analytics**.

2. Click **Edit Analytics**



3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window

4. Click **OK**.

Disable analytics

To disable analytics on the selected virtual servers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Select the virtual servers
2. Click **Disable Analytics**

NetScaler ADM disables the analytics on the selected virtual servers

The following table describes the features of NetScaler ADM that supports IPFIX and Logstream as the transport mode:

FEATURE	IPFIX	LOGSTREAM
Web Insight	•	•
WAF Security Violations	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

A unified process to enable analytics on virtual servers

Apart from the existing process to enable analytics, you can also use a single-pane workflow to configure analytics on:

- All the existing licensed virtual servers
- The subsequent licensed virtual servers

After configuration, this feature eliminates the necessity to manually enable analytics on the existing and subsequent virtual servers.

Points to note:

Before you configure analytics, you must understand the following behaviors of NetScaler® ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you configure this feature for the first time, you must ensure that the prerequisites mentioned in this document are met.
- Modify the analytics settings later.

  Consider that you have configured the analytics settings for the first time by selecting Web Insight, HDX™ Insight, and Gateway Insight. If you want to modify the analytics settings later and deselect Gateway Insight, the changes do not impact the virtual servers that are already enabled with analytics.
- The virtual servers that are already enabled with analytics.

  Consider that you have 10 licensed virtual servers and two of them are already enabled with analytics. In this scenario, this feature enables analytics only for the remaining eight virtual servers.
- The virtual servers that are manually disabled with analytics.

  Consider that you have 10 licensed virtual servers and you have manually disabled analytics for two virtual servers. In this scenario, this feature enables analytics only for the remaining eight virtual servers and skips the virtual servers that are manually disabled with analytics.
- **Bot Security Violations** and **WAF Security Violations** options are supported only in premium licensed virtual servers. If the virtual servers are not premium licensed, then **Bot Security Violations** and **WAF Security Violations** are not enabled.

Prerequisites

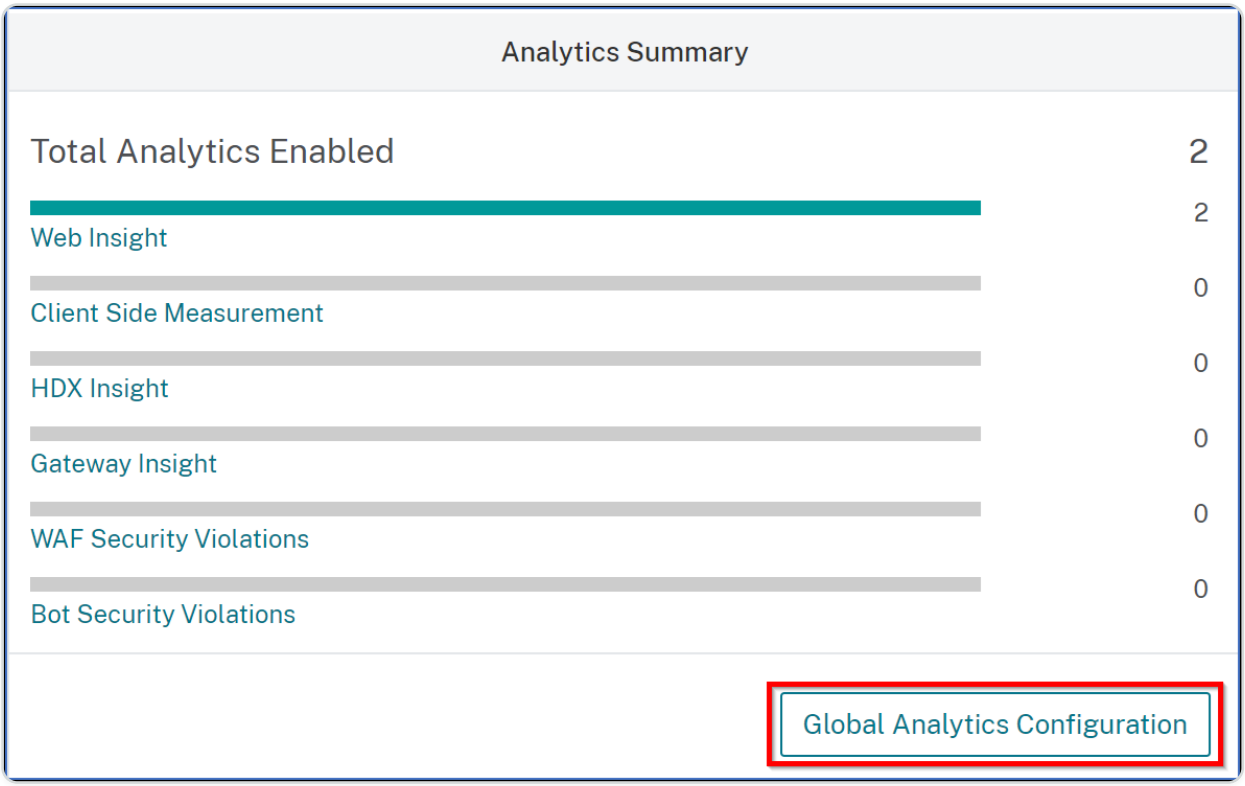
Ensure that:

- All existing virtual servers are licensed.
- Auto-licensed option is enabled to license all the subsequent virtual servers. Navigate to **Settings > Licensing & Analytics Config** and under **Virtual Server License Allocation**, turn on the **Auto Licensed Virtual Servers** option.

Enable analytics

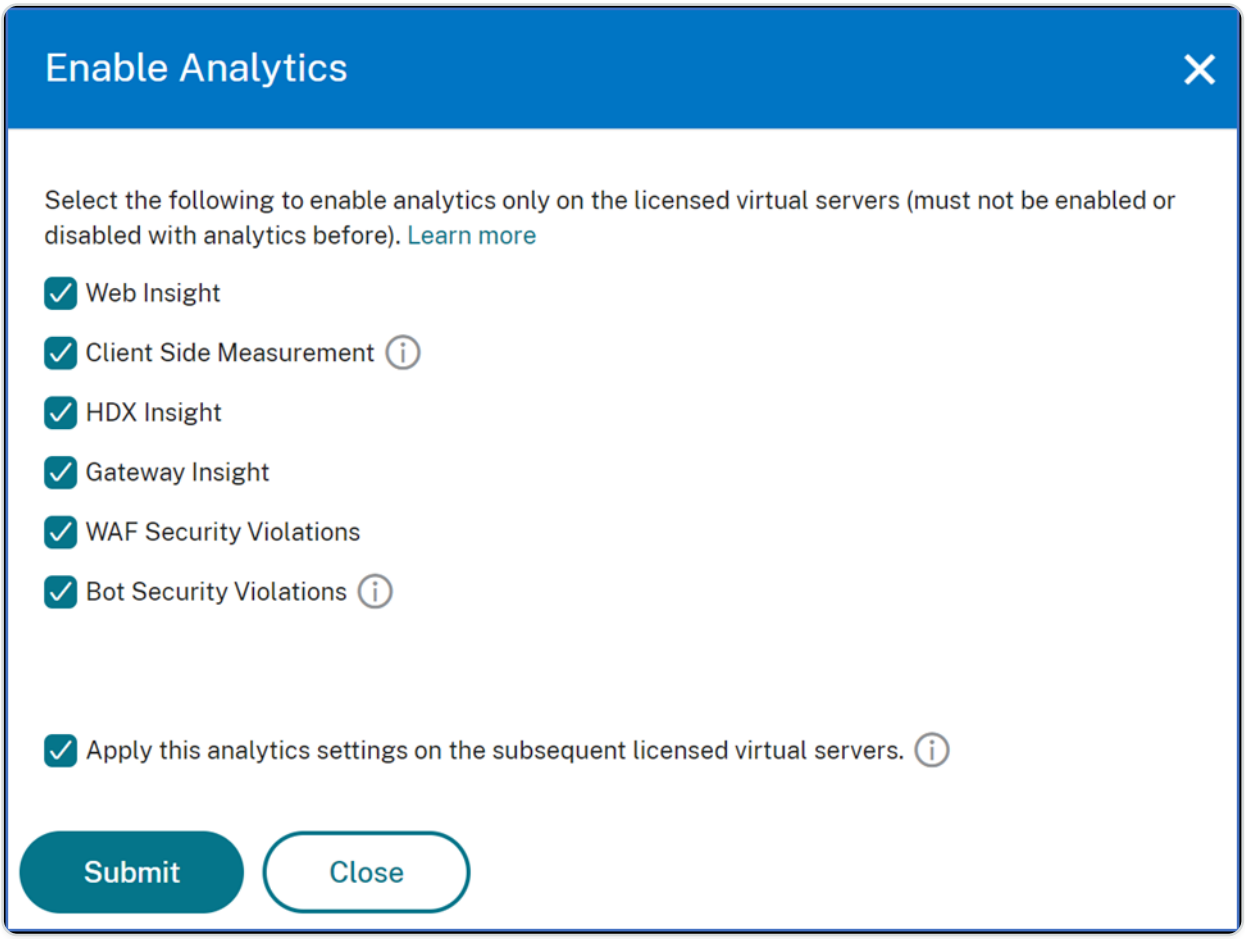
1. Navigate to **Settings > Licensing & Analytics Config**.
2. Under **Analytics Summary**, click **Global Analytics Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select the analytics features that you want to enable analytics on the virtual servers.
4. To enable analytics on the subsequent virtual servers, select the **Apply this analytics settings on the subsequent licensed virtual servers** check box.
5. Click **Submit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure NTP server

You can configure a Network Time Protocol (NTP) server in NetScaler® ADM to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server on NetScaler ADM:

1. From the ADM GUI, navigate to **Settings > Administration**. In the **System Administration** page, under **Network Configurations**, click **NTP Servers**. Then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
   - **Server Name/IP Address** – Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - **Minimum Poll Interval** – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2\^6, enter 6

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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. To find the key identifier, see your NTP server's documentation.
- **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
- **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

To enable NTP synchronization on NetScaler ADM:

1. Navigate to the **NTP Servers** home page.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** checkbox.
3. Click **OK**.

   A confirmation window appears to restart NetScaler ADM. Click **Yes** to continue.

Configure system settings

Before you start using NetScaler® ADM to manage and monitor your instances and applications, it is recommended that you configure a few system settings ensure optimal performance of your NetScaler ADM server.

Configure system alarms

Configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, loginFailure), a message is recorded in the system and you can view the message as a syslog message.

To configure system alarms:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > SNMP**, and then click the **Alarms** tab on the upper-right corner.
2. Select the alarm you want to configure, and click **Edit**.
3. On the **Configure Alarm** page, select the alarm severity, and set the Threshold.
4. To view the alarms that have breached the threshold or for which an event has occurred, navigate to **Settings > Auditing** and click **Syslog Messages**.

Configure system notifications

You can send notifications to select groups of users for various system-related functions. You can set up a notification server in NetScaler ADM, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. Setting notification ensures that you are notified of any system-level activities such as user login or system restart.

To configure system notifications:

1. Navigate to **Settings > Administration**. In the **System Administration** page, under **Event Notifications**, click **Configure Event Notification and Digest > Event Notification**.
2. On the **Configure System Notification Settings** page, select the category or category of events generated by NetScaler ADM.
3. Then, configure either the email server or the SMS server to receive notification through email or SMS or both.

Configure system prune settings

To limit the amount of reporting data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

To configure system prune setting:

1. Navigate to **Settings > System Administration**. Under **Data Pruning**, click **System and Instance Data Pruning**.
2. In the **System** page, specify the number of days for which to retain data, and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure instance syslog prune settings

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the generic syslog data is deleted from NetScaler ADM.

To configure instance syslog purge settings:

1. Navigate to **Settings > Administration > Data Pruning**.
2. Click **System and Instance Data Pruning > Instance Syslog**.
3. In **Configure Instance Syslog Prune Settings page**, specify the number of days between 1 and 180 in **Retain Syslog Generic Data** field.
4. Click **Save**.

Configure instance event prune settings

To limit the amount of event messages data being stored in your NetScaler ADM server's database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).

To configure instance event prune settings:

1. Navigate to **Settings > Administration**.
2. From the **System Administration** page, under **Data Pruning**, click **System and Instance Data Pruning**.
3. In the **Data Pruning** page, click **Instance Events**.
4. In the **Data to keep (days)** field, enter the time interval, in days, for which you want to retain data on the NetScaler ADM server and click **Save**.

Configure system backup settings

NetScaler ADM automatically backs up the system every day at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system. You can also encrypt the backup file. You can also choose to save the backup on an external server.

To configure system backup settings:

1. Navigate to **Settings > Administration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **System** and on the **Configure System Backup Settings** page, specify the required values.

Configure instance backup settings

If you back up the current state of a NetScaler instance, you can use the backup files to restore stability if the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.

To configure instance backup settings:

1. Navigate to **Settings > Administration**.
2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **Instance**, under **Configure Instance Backup Settings**, and specify the required values.

Enable or disable ADM features

As an administrator, you can enable or disable the following features in the **Settings > Administration > Configurable Features** page:

- **Agent failover** - The agent failover can occur on a site that has two or more active agents. When an agent becomes inactive (DOWN state) in the site, the NetScaler ADM service redistributes the ADC instances of the inactive agent with other active agents. For more information, see Configure on-prem agents for multisite deployment.
- **Entity polling network function** - An entity is either a policy, virtual server, service, or action attached to an ADC instance. By default, NetScaler ADM automatically polls configured network function entities every 60 minutes. For more information, see Polling overview.
- **Instance backup** - Back up the current state of a NetScaler instance and later use the backed-up files to restore the ADC instance to the same state. For more information, see Back up and restore NetScaler instances.
- **Instance configuration audit** - Monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations. For more information, see Create audit templates.
- **Instance events** - Events represent occurrences of events or errors on a managed NetScaler instance. Events received in NetScaler ADM are displayed on the **Events Summary** page

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**). For more information, see Events.

- **Instance network reporting** - You can generate reports for instances at a global level. Also, for entities such as the virtual servers and network interfaces. For more information, see Network Reporting.
- **Instance SSL certificates** - NetScaler ADM provides a centralized view of SSL certificates installed across all managed NetScaler instances. For more information, see SSL Dashboard.
- **Instance Syslog** - You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler ADM.

To enable a feature, perform the following steps:

1. Select the feature from the list that you want to enable.
2. Click **Enable**.

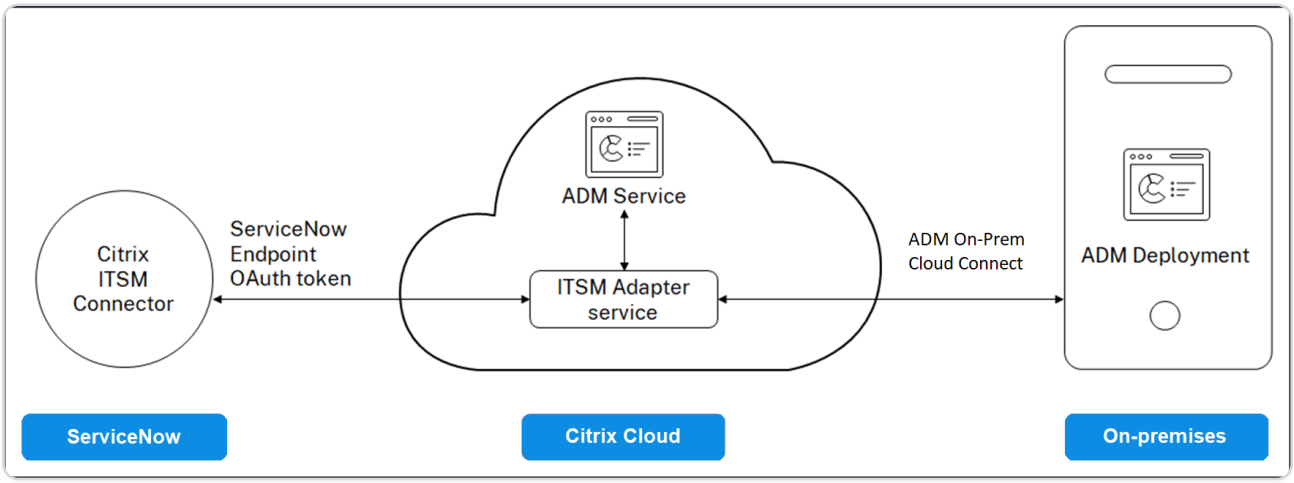
IMPORTANT

If a feature is disabled, the user cannot perform the operations associated with that feature.

Integrate NetScaler® ADM with the ServiceNow instance

When you want to enable ServiceNow notifications for NetScaler and ADM events, integrate NetScaler ADM with the ServiceNow instance. This integration uses Citrix ITSM connector to communicate between NetScaler ADM and the ServiceNow instance.

The ServiceNow integration with ADM uses the ITSM Adapter service for token based authentication. To do so, it creates an endpoint instance in ServiceNow. For more information, see How ITSM Adapter works.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To connect your ADM on-premises deployment with an ITSM adapter, ensure to configure customer identity. For more information, see, Configure customer identity.

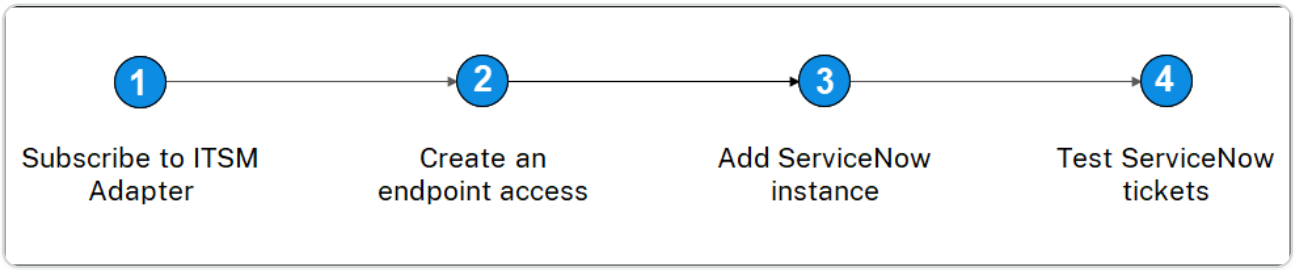
Prerequisites

Before you integrate ADM with ServiceNow, ensure the following:

1. Sign Up for Citrix Cloud. Make sure you have access to manage Citrix Cloud administrators. For more information, see Manage Citrix Cloud administrators.

How to integrate ADM with ServiceNow?

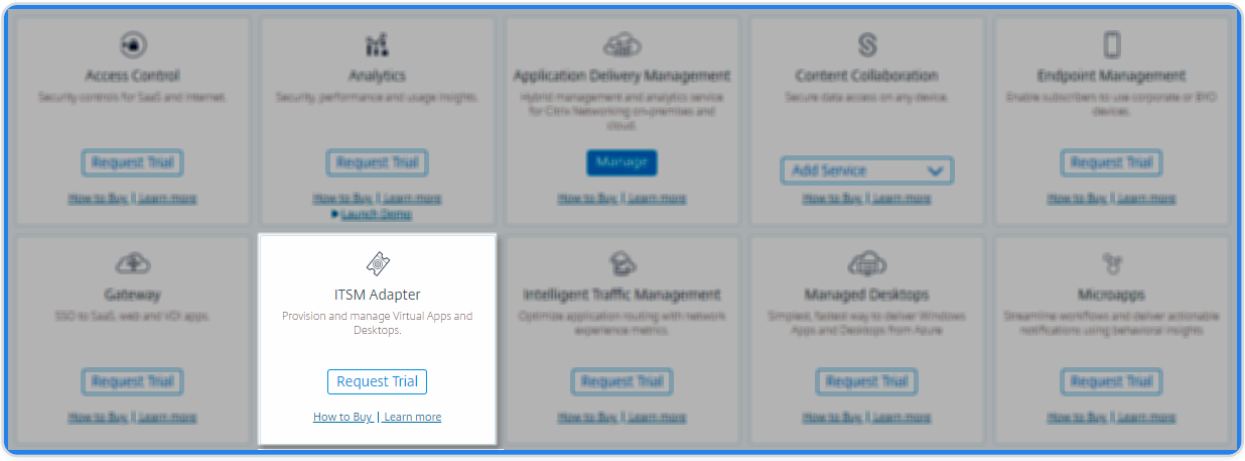
Perform the following steps to integrate NetScaler ADM with ServiceNow using the ITSM connector:



1. Subscribe to ITSM Adapter service in Citrix Cloud™.
2. Create an endpoint access in the ServiceNow instance.
3. Add a ServiceNow instance.
4. Test auto-generation of ServiceNow tickets in ADM.

Step 1 - Subscribe to ITSM Adapter service in Citrix Cloud

1. On the **ITSM Adapter** tile, click **Request Trial**.

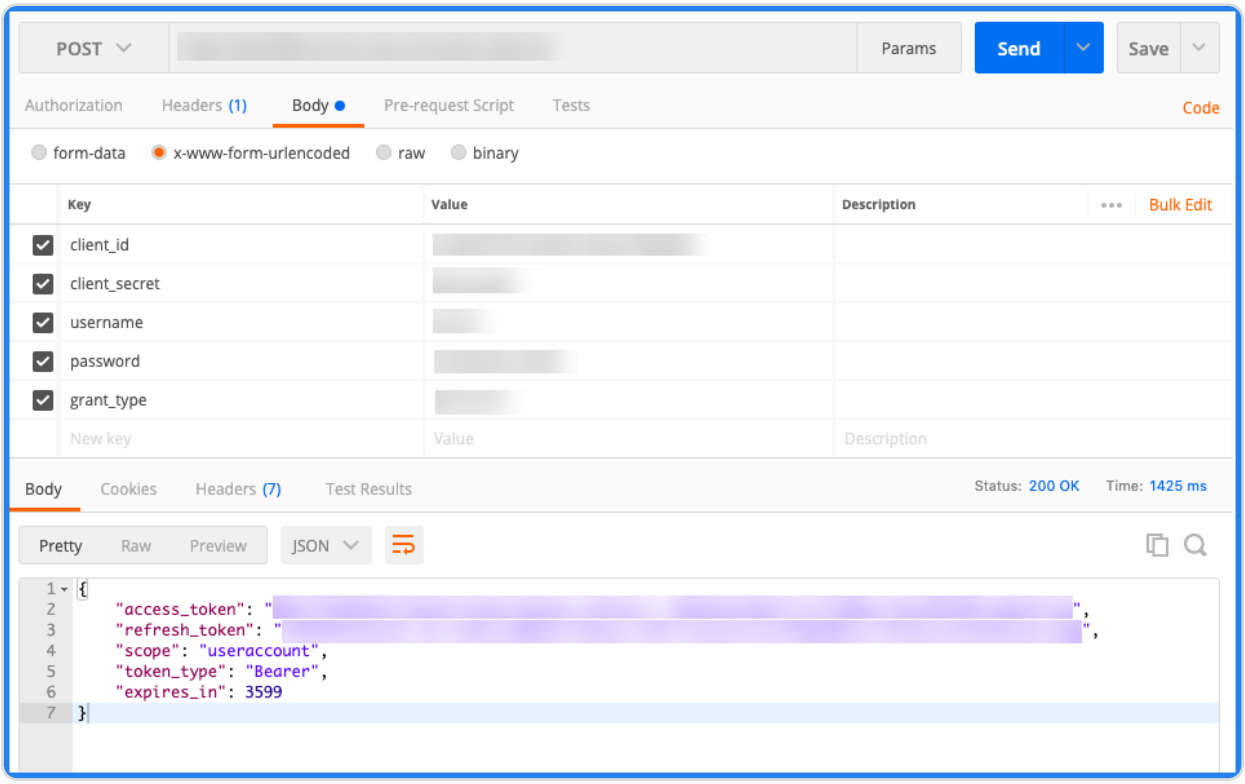


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigate to **Identity Access and Management** > **API Access** and note the **Client ID** and **Client Secret** information.

Step 2 - Create an endpoint access in the ServiceNow instance

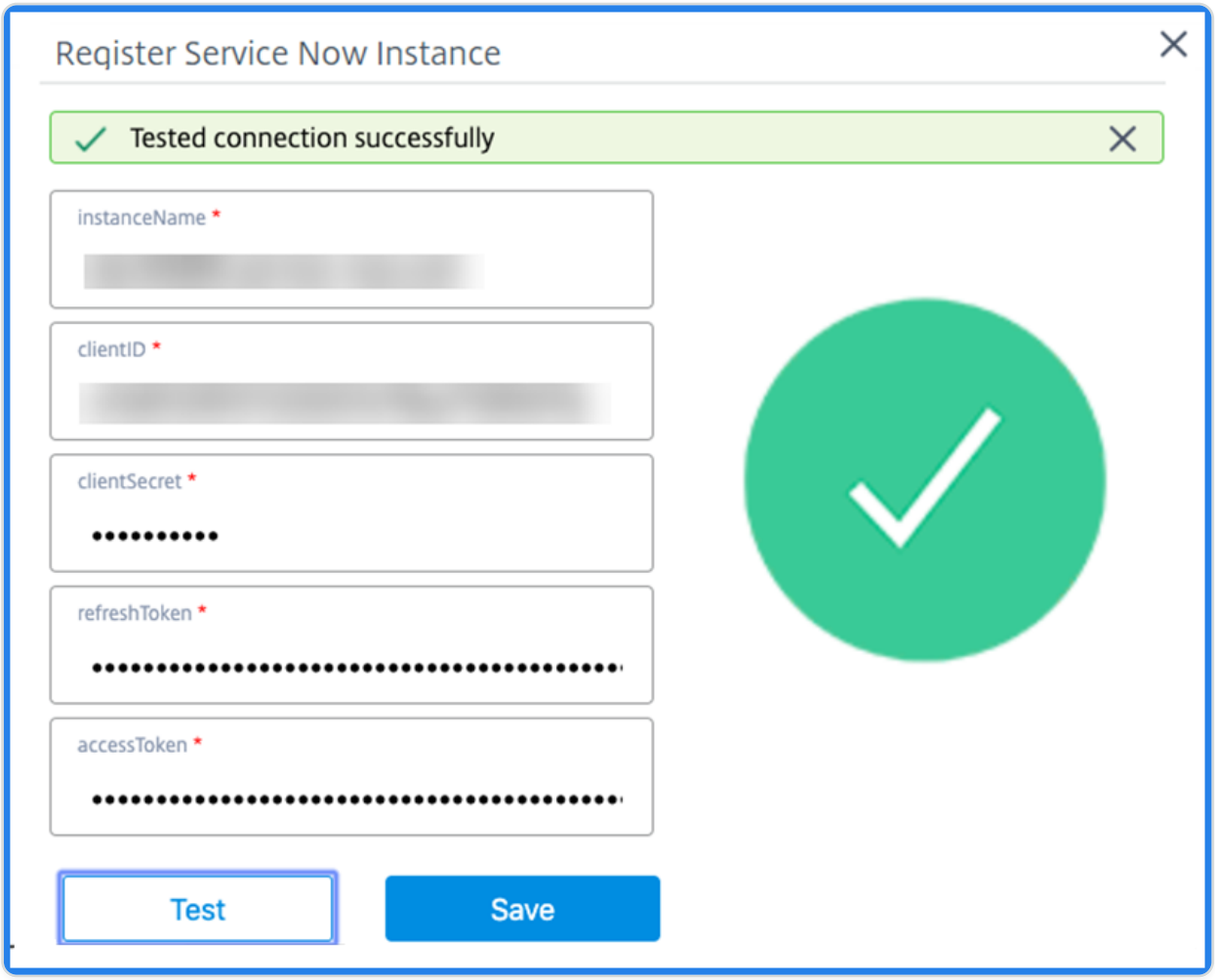
1. Log in to your ServiceNow instance with an administrator credentials.
2. Go to ServiceNow store. Download and install the **Citrix ITSM connector**.
3. On the **Citrix ITSM Connector** pane, select **Home** and then click **Authenticate**. Type the Client ID and Secret that you have noted from Citrix Cloud.
4. Test the connection.
5. Save the configuration. An acknowledgment from ServiceNow appears indicating that the connection is active.
6. Create an endpoint to access a ServiceNow instance. See Create an endpoint for clients to access the instance.
7. Obtain the Access and Refresh tokens using the Client ID and Client Secret. See OAuth tokens.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3 - Add a ServiceNow instance

1. In the **Manage** tab, select Add ServiceNow Instance.
2. Specify the **Instance Name**, **Client ID**, **Client Secret**, **Refresh Token**, and **Access Token**.
3. Click **Test**.



The ServiceNow instance is now connected to the ITSM Adapter service.

4. After testing the connection successfully, click **Save** to add a ServiceNow instance.

Step 4 - Test auto-generation of ServiceNow tickets in ADM

1. Log in to NetScaler ADM.
2. Navigate to **Account > Notifications** and select **ServiceNow**.
3. Select the ServiceNow profile from the list.
4. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   If you want to view ServiceNow tickets in the NetScaler ADM GUI, select **ServiceNow Tickets**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set ServiceNow notifications in ADM

After the ServiceNow instance is registered on the ITSM adapter, you can set up ServiceNow notifications for the following events in the NetScaler ADM GUI:

IMPORTANT

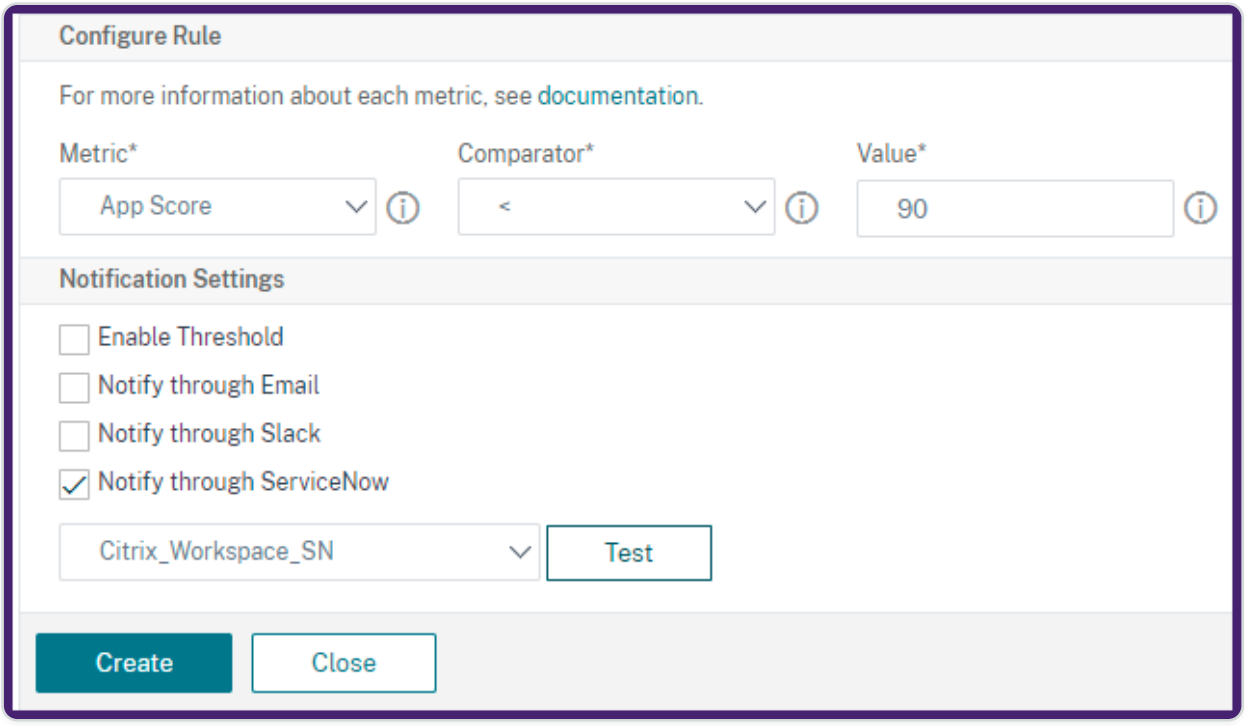
This feature is supported on ServiceNow Cloud.

- **NetScaler events**: NetScaler ADM can generate the ServiceNow incidents for the selected set of NetScaler events from selected managed NetScaler instances.

  To send ServiceNow notifications for NetScaler events from the managed instances, you must configure an event rule and assign the rule action as **Send ServiceNow Notifications**.

  Create an event rule on the ADM by navigating to **Infrastructure > Events > Rules**. For more information, see Send ServiceNow notifications.

- **Application Analytics**: NetScaler ADM can generate ServiceNow incidents for the applications that breach the specified threshold.



  In this example, a ServiceNow incident is generated when the App score of applications falls under 90.

- **The SSL certificate and ADM license events**: NetScaler ADM can generate the ServiceNow incidents for the SSL certificate expiry and ADM license expiry events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To send ServiceNow notifications for an SSL certificate expiry, see The SSL certificate expiry.

To send ServiceNow notifications for an ADM license expiry, see The NetScaler ADM license expiry.

Export or schedule export reports

In NetScaler® ADM, you can export a comprehensive report for the selected NetScaler ADM feature. This report provides you an overview of the mapping between the instances, partitions, and corresponding details.

NetScaler ADM displays feature-specific scheduled export reports under individual ADM features, which you can view, edit, or delete. For example, to view the export reports of NetScaler instances, navigate to **Network > Instances > NetScaler** and click the export icon. You can export these reports in PDF, JPEG, PNG, and CSV file format.

In **Export Reports**, you can perform the following actions:

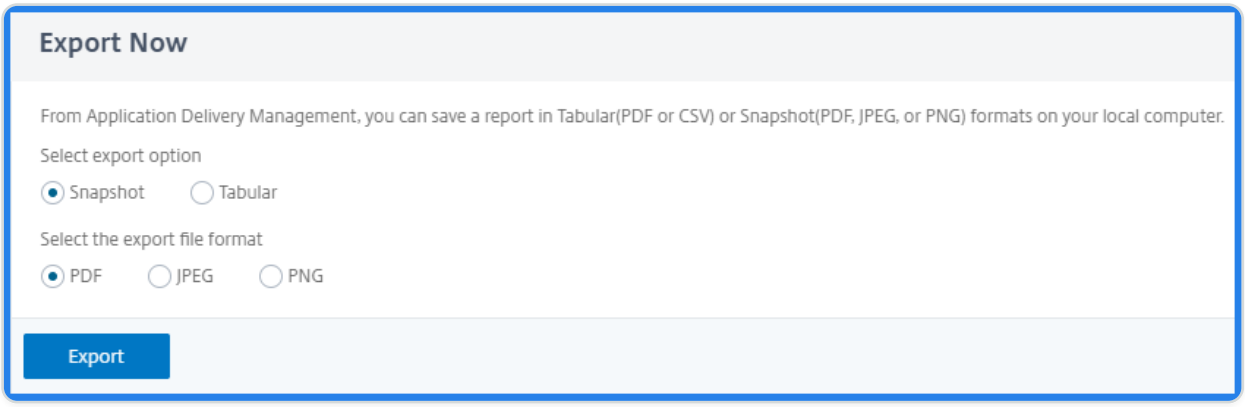
- Export a report to a local computer
- Schedule export reports
- View, edit, or delete the scheduled export reports

Export a report

To export a report from the ADM to the local computer, perform the following steps:

1. Click the export icon at the top-right corner of the page.
2. Select **Export Now**.
3. Select one of the following the export options:
    - **Snapshot** - This option export ADM reports as a snapshot.
    - **Tabular** - This option export ADM reports in a tabular format. You can also choose how many data records to export in a tabular format

© 1997–2026 Citrix Systems, Inc. All rights reserved.



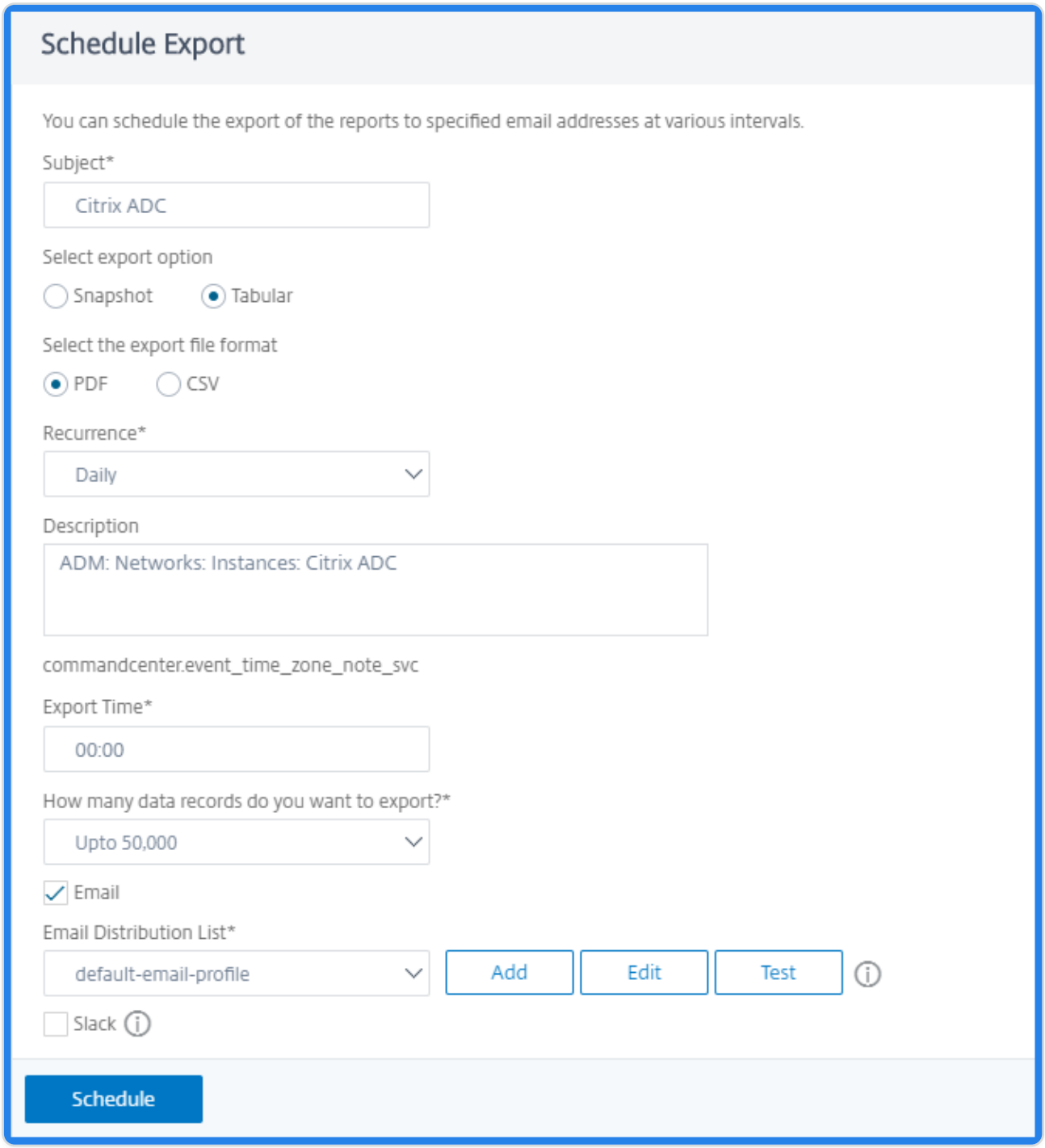
4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

Schedule export report

To schedule the export report at regular intervals, specify the recurrence interval. NetScaler ADM sends the exported report to the configured email or slack profile.

1. Click the export icon at the top-right corner of the page.
2. Select **Schedule Export** and specify the following:
   - **Subject** - By default, this field auto-populates the selected feature name. However, you can rewrite it with a meaningful title.
   - **Export option** - Export ADM reports in a snapshot or a tabular format. You can also choose how many data records to export in a tabular format
   - **Format** - Select the file format that you want to receive the report on the configured email or slack profile.
   - **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the list.
   - **Description** - Specify the meaningful description to a report.
   - **Export Time** - Specify at what time you want to export the report.
   - **Email** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
   - **Slack** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
3. Click **Schedule**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View and edit the scheduled export reports

To view the export reports, perform the following:

1. Click the export icon at the top-right corner of the page.

   The **Export Report** page displays all the feature-specific export reports .

2. Select the report that you want to edit and click **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade

Each NetScaler ADM release offers new and updated features with increased functionality. Citrix recommends you upgrade NetScaler ADM to the latest release to avail of the new features and bug fixes. A comprehensive list of enhancements, known issues, and bug fixes is included in the release notes accompanying every release announcement. It is also important to understand the licensing framework and the types of licenses that can be used before you start to upgrade. For NetScaler ADM licensing information, see Licensing.

The Upgrade path information is also available in the Citrix Upgrade Guide.

Before you upgrade

Download the upgrade package from the NetScaler ADM Downloads page and follow the instructions in this article to upgrade your system to the latest 13.1 build. After the upgrade process begins, ADM restarts and the existing connections are terminated and reconnected when the upgrade completes. The existing configuration is preserved, but NetScaler ADM does not process any data until the upgrade completes.

IMPORTANT

The NetScaler ADM version and build should be **equal to or higher** than your NetScaler version and build. For example, if you have installed NetScaler ADM 12.1 Build 50.39, then ensure you have installed NetScaler 12.1 Build 50.28/50.31 or earlier.

Points to note before upgrading to 13.1:

- If you upgrade from version 11.1 or version 12.0 56.x and previous builds, perform the following steps:

  a. Upgrade from the existing version to 12.0 build 57.24.

  b. Upgrade to the latest build of version 12.1.

  c. Upgrade to version 13.1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you upgrade from 12.0 build 57.24 and higher, first upgrade to 12.1 and then to 13.1.
- If you upgrade from 12.1, you can directly upgrade to 13.1.
- If you upgrade from versions lower than 13.0 64.xx, for better user experience, first upgrade to 13.0 64.xx and then to 13.1.

Important points to note before upgrading to 13.1-xx.xx and later

When you upgrade the ADM software to version 13.1-xx.xx, your ADM database is also migrated. This data migration happens because ADM now uses PostgreSQL version 10.11.

NOTE

Downgrading the ADM software is unsupported. Do not attempt to downgrade.

Recommended precautions:

- Take a snapshot of the NetScaler ADM server if you are upgrading to 13.1-xx.xx and later.
- Back up the NetScaler® ADM server before you upgrade.
- After the upgrade, you might have to reestablish connections between the NetScaler ADM server and the managed instances. A confirmation prompt warns you that connections can fail if you proceed.
- If you upgrade to any version between 13.1.9.x and 13.1.30.x, NetScaler ADM rolls back the existing StyleBooks ConfigPacks to its earlier version.

  To avoid this issue, upgrade to 13.1.33.50 build.
- For NetScaler ADM servers in high availability setup, when upgrading, do not make any configuration changes on either of the nodes.

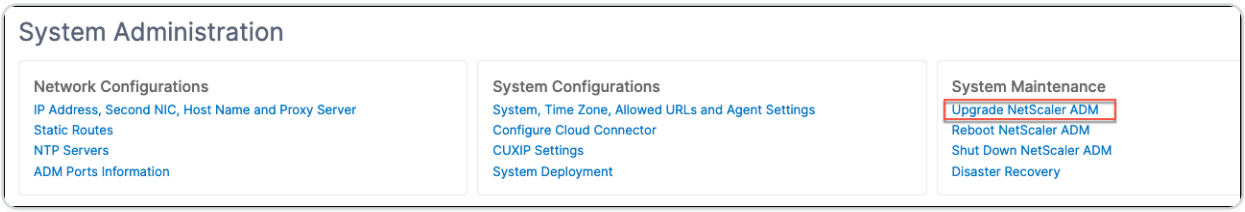
  WARNING

  Do not refresh the browser until the upgrade process is successfully completed. Check the GUI for the approximate time for the upgrade to complete.
- After upgrade, the active node can change in a high availability pair.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade a single NetScaler ADM server to 13.1-12.x

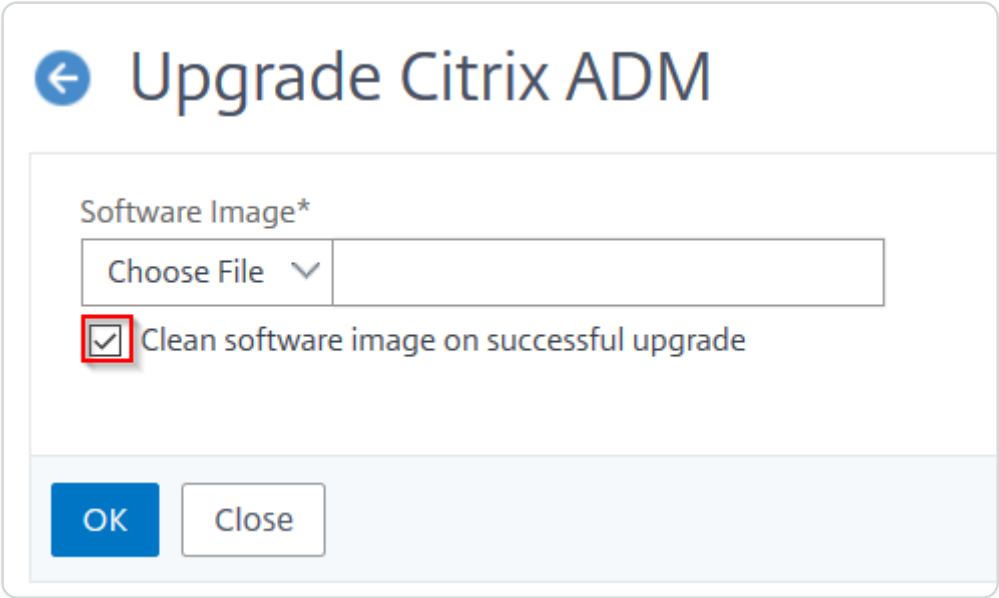
1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Settings > Administration**. Under **System Maintenance**, click **Upgrade NetScaler ADM**.



3. On the **Upgrade NetScaler ADM** page, select the **Clean software image on successful upgrade** check box to delete image files after upgrade. Selecting this option removes the NetScaler ADM image files automatically upon upgrade.

NOTE

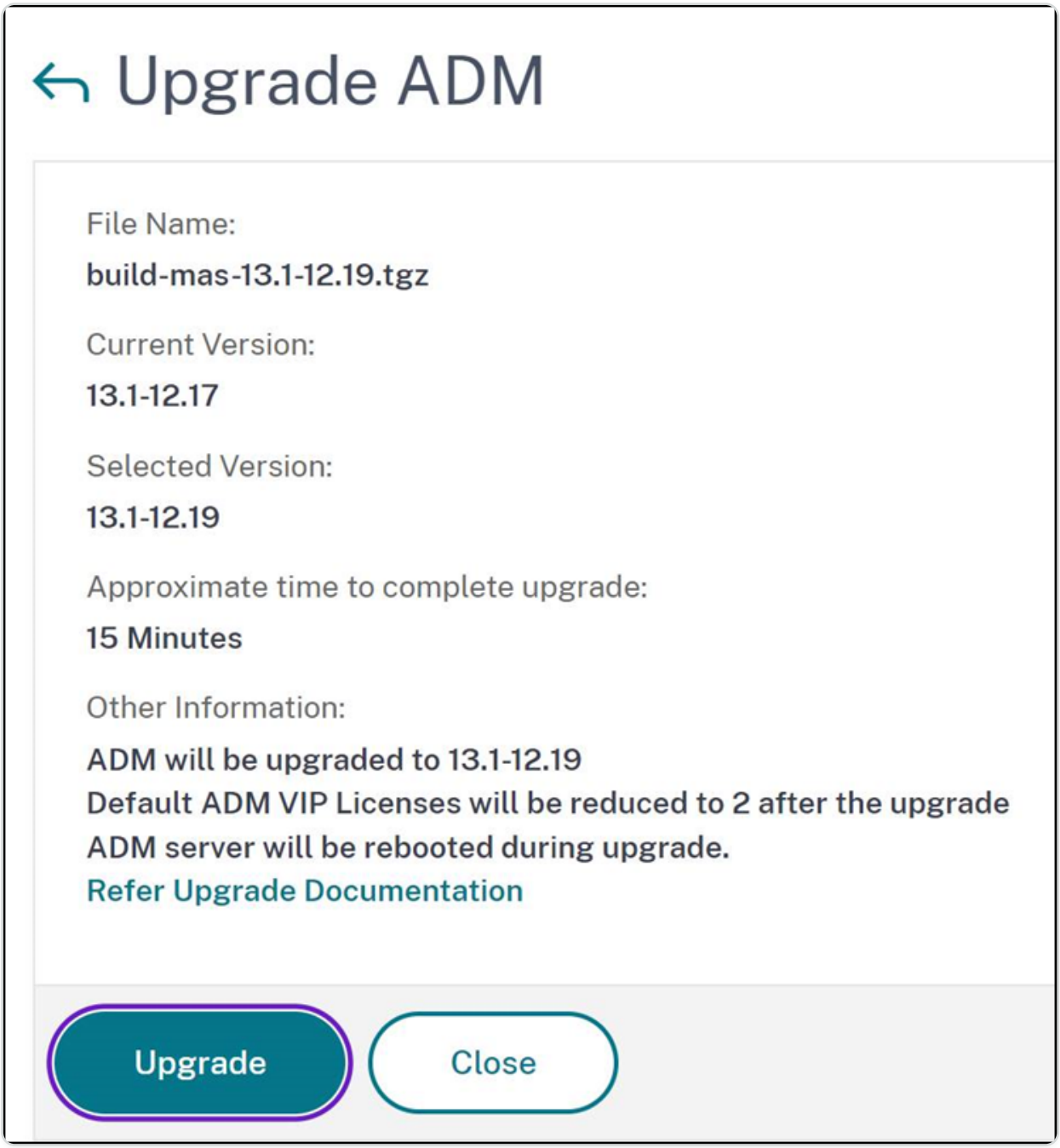
This option is selected by default. If you do not select this check box before starting the upgrade process, you must manually delete the images.



4. You can then upload a new image file by selecting either **Local** (your local machine) or **Appliance**. The build file must be present on the NetScaler ADM virtual appliance.
5. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

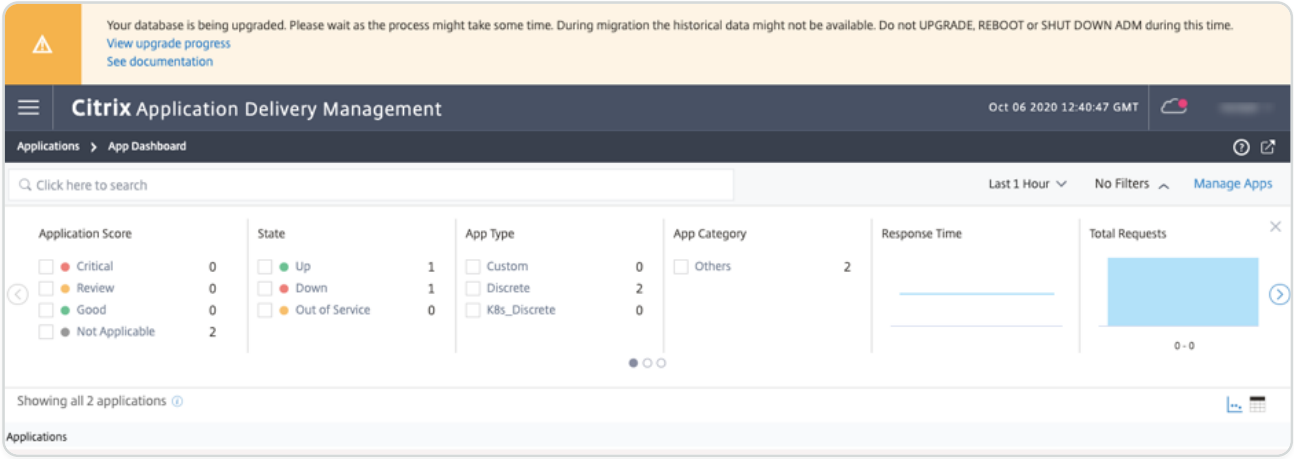
6. The **Upgrade ADM** page displays few details such as file name, selected version, estimated time to complete. Click **Upgrade**.



The upgrade process starts.

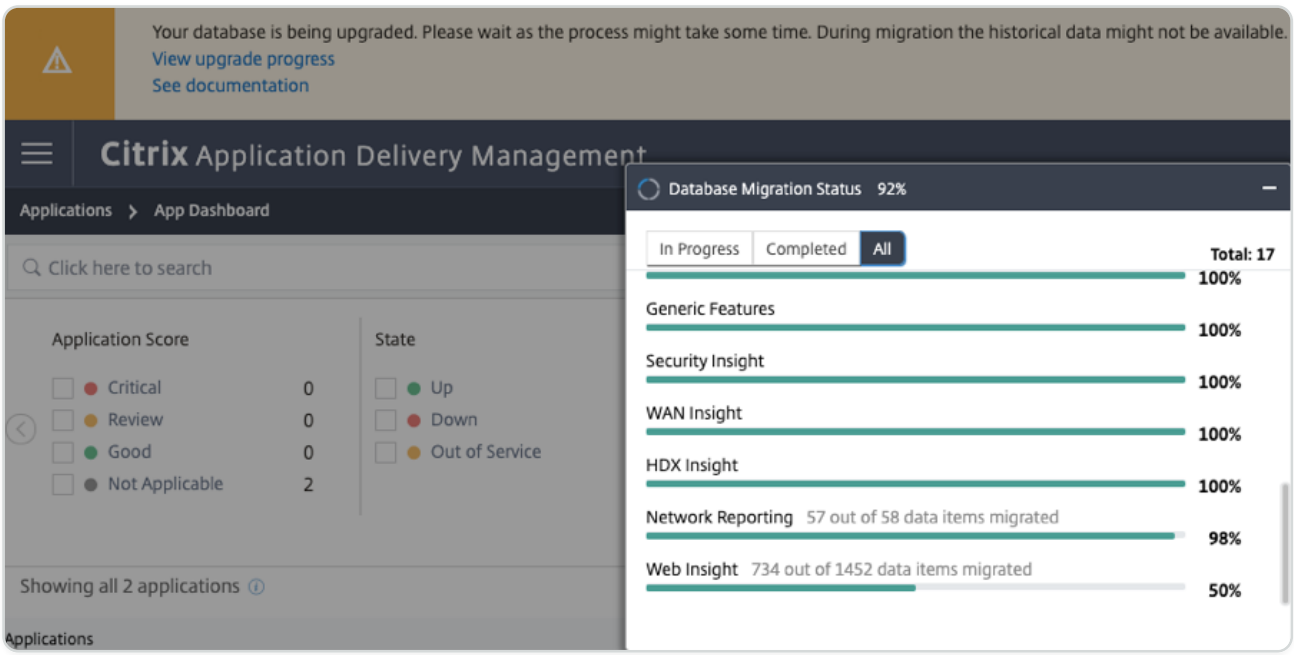
After your configuration is migrated, you can log on to the ADM GUI. Upon logon, the historical data starts to migrate at the background while you can continue to work on ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

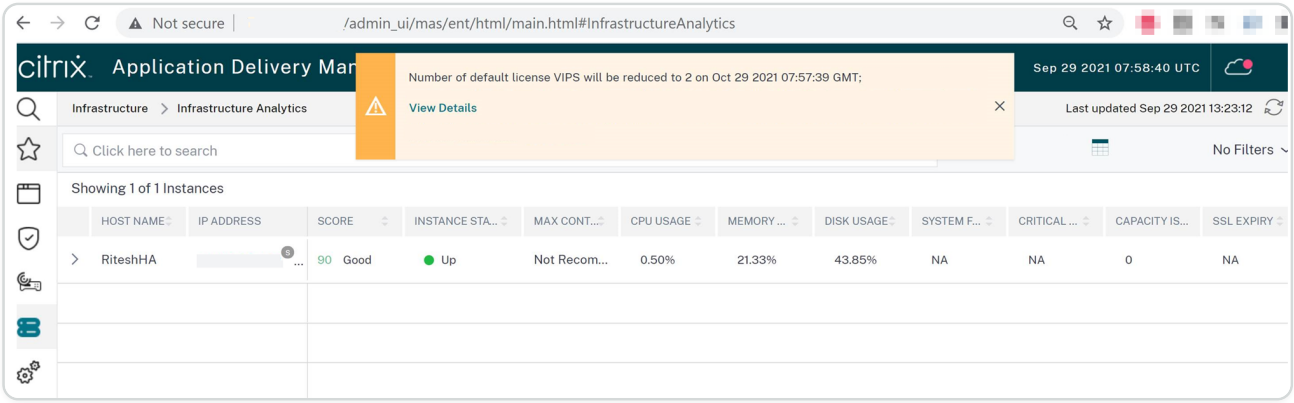


During historical data migration, some of the old data might not be available. The time taken to migrate your database depends on the size of data and the number of tables.

You can monitor the database migration using the ADM GUI. Click **View upgrade progress** and the **Database Migration Status** appears.



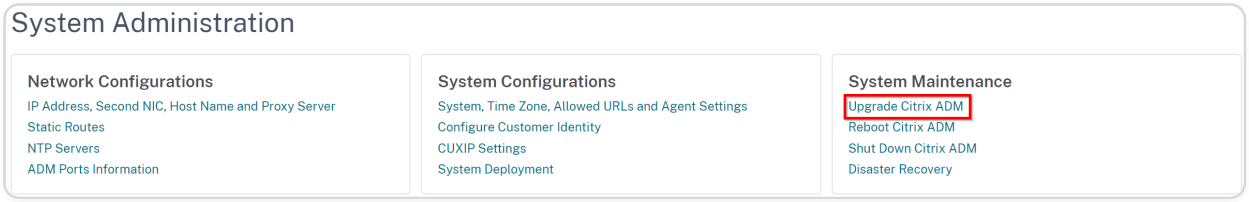
After the upgrade is complete, you can view the message that the default free licenses get reduced to two. Click **View Details** for more information.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

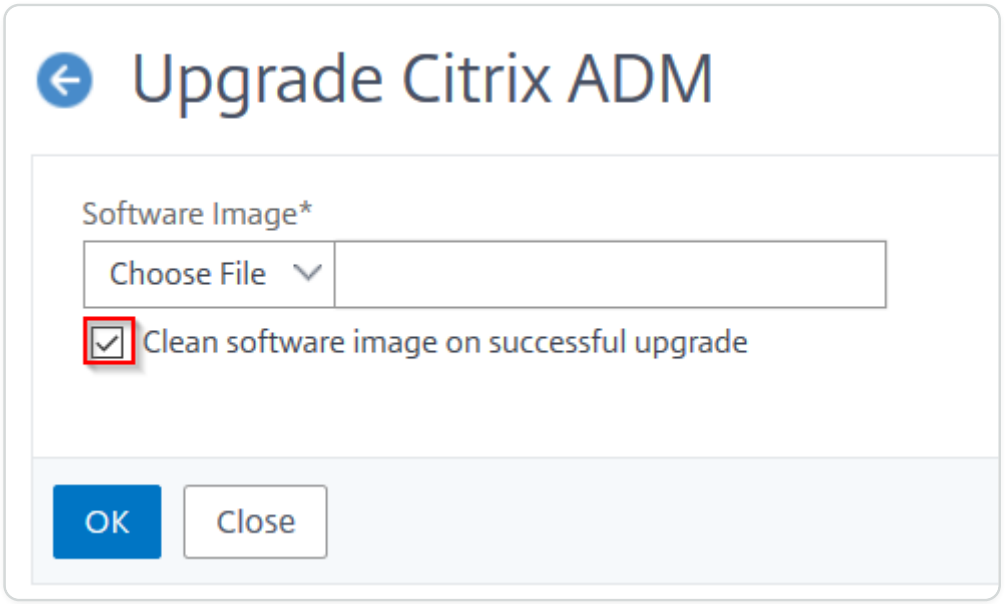
Upgrade a single NetScaler ADM server to 13.1-4.x or 13.1-9.x

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **System** \> **System Administration**. Under the **System Administration** subheading, click **Upgrade NetScaler ADM**.



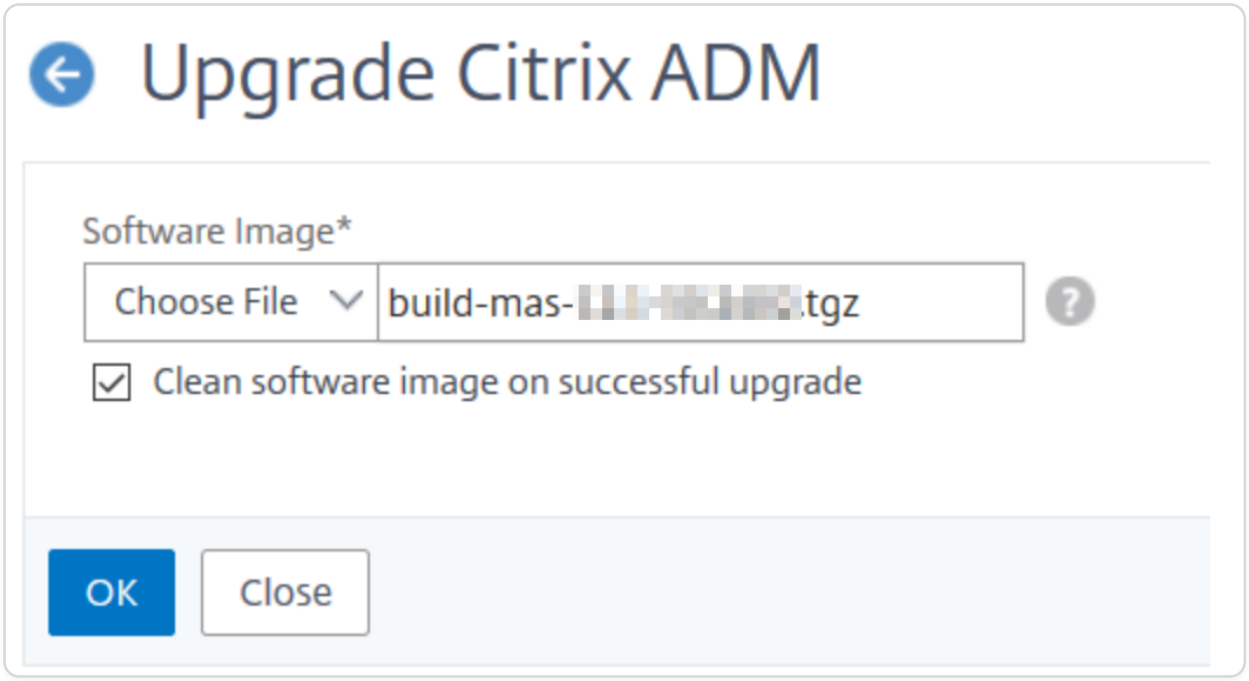
3. On the **Upgrade NetScaler ADM** page, select the **Clean software image on successful upgrade** check box to delete image files after upgrade. Selecting this option removes the NetScaler ADM image files automatically upon upgrade.

> **NOTE**
>
> This option is selected by default. If you do not select this check box before starting the upgrade process, you must manually delete the images.



4. You can then upload a new image file by selecting either **Local** (your local machine) or **Appliance**. The build file must be present on the NetScaler ADM virtual appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

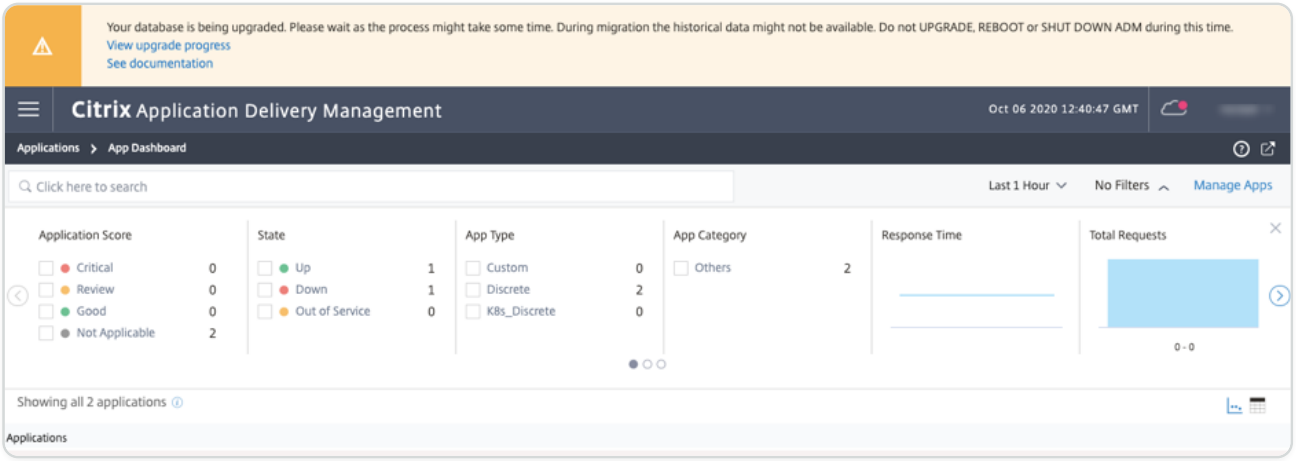


5. Click **OK**.

   The Confirm dialog box is displayed. Click **Yes**.

   The upgrade process starts.

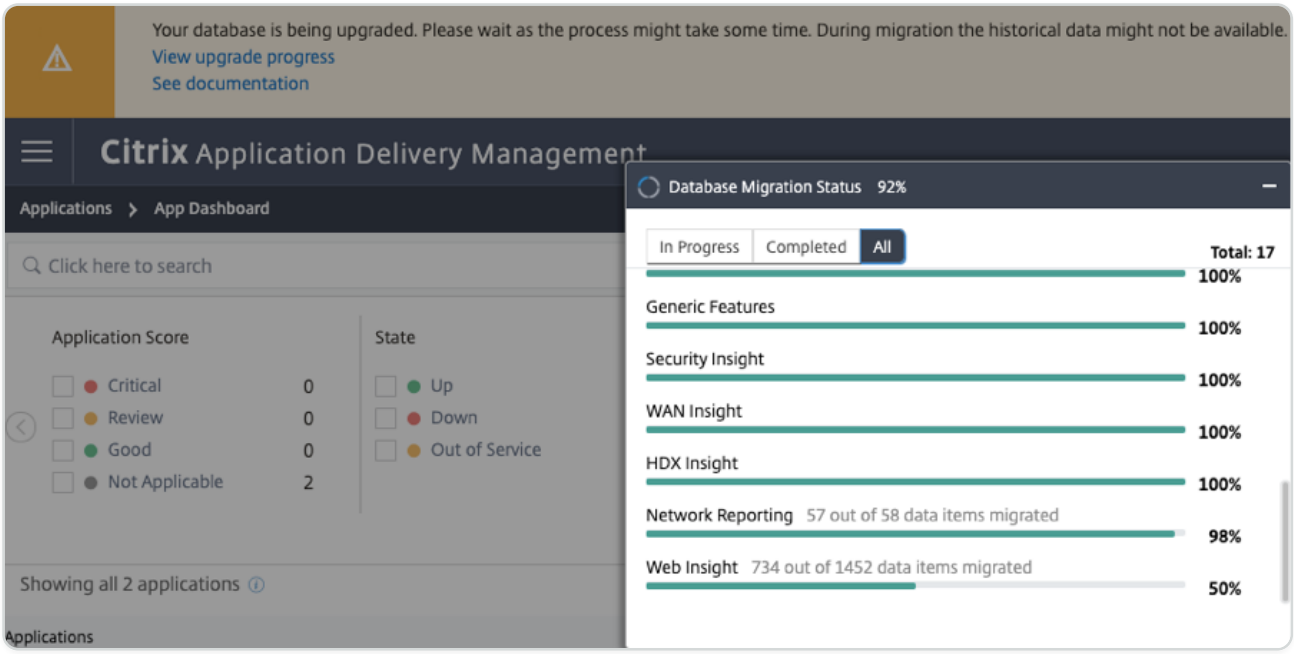
After your configuration is migrated, you can log on to the ADM GUI. Upon logon, the historical data starts to migrate at the background while you can continue to work on ADM.



During historical data migration, some of the old data might not be available. The time taken to migrate your database depends on the size of data and the number of tables.

You can monitor the database migration using the ADM GUI. Click **View upgrade progress** and the **Database Migration Status** appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting database migration issues

During the upgrade process to 13.1-xx.xx and later, sometimes the migration of Web Insight historical data might appear to be stuck. In such cases, to check details of data migration, do the following.

Log on to the ADM shell prompt and run the following command to see the granular details of the progress.

```
cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
```

Here's an example output

```
bash-3.2# cat /var/mps/log/db_upgrade/
web_insight_mapping_migration_status

Tue Oct  6 07:41:55 GMT 2020

157 out of 127346 done in 54 seconds
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    File

     /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
af_app_client_server_resp_second_l3p_d7_dump

    bash-3.2#
```

In this example, `af_app_client_server_resp_second_l3p_d7` is the entry that is being upgraded. And 157 entries out of 127,346 is migrated in 54 seconds.

Upgrade a high availability pair from 12.1 release to 13.1 release

For NetScaler ADM servers in a high availability mode, you can upgrade by either accessing the active node or the floating IP address. Both the NetScaler ADM servers are automatically upgraded to the latest build once you initiate the upgrade process in either of the servers.

Upgrade NetScaler ADM disaster recovery deployment

Upgrading NetScaler ADM disaster recovery deployment is a two-step process:

- Upgrade the NetScaler ADM nodes configured in high availability mode in the primary site. Later you must upgrade the disaster recovery node.
- Ensure that you have upgraded the NetScaler ADM servers that are deployed in high availability, before upgrading the disaster recovery node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade the NetScaler ADM disaster recovery node

1. Download NetScaler ADM upgrade image file from NetScaler site.
2. Upload this file to the disaster recovery node using `nsrecover` credentials.
3. Log on to the disaster recovery node using the `nsrecover` credentials.
4. Navigate to the folder where you placed the image file and unzip the file.
5. Run the following script:

   ./installmas

   ```
   bash-3.2# ./installmas
   ```

Upgrade on-prem agents for multisite deployment

Upgrading NetScaler agent deployment is a three-step process. Ensure that you have completed the following tasks before upgrading the on-prem agents:

1. Upgrade the NetScaler ADM servers that are deployed in high availability.
2. Upgrade the NetScaler ADM disaster recovery node.

   For more information, see Upgrade NetScaler ADM disaster recovery deployment.

Upgrade the on-prem agent

1. Download NetScaler agent upgrade image file from NetScaler site.
2. Upload this file to the agent node using `nsrecover` credentials.
3. Ensure that you download the correct agent upgrade image.
4. Log on to the on-prem agent using the `nsrecover` credentials.
5. Navigate to the folder where you placed the image file and unzip the file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Run the following script:

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

Add an extra disk to the NetScaler ADM server

If your NetScaler ADM storage requirement exceeds the default disk space (120 GB), you can attach an extra disk. You can attach more disk in both single-server and high availability deployments.

When you upgrade NetScaler ADM from release version 12.1–13.1Œ, the partitions that you had created on the additional disk in the earlier version remain the same. The partitions are not removed or resized.

The procedure to attach more disk remains the same in the upgraded build. You can now use the new disk partitioning tool in NetScaler ADM to create partitions in the newly added disk. You can also use the tool to resize the partitions in the existing more disk. For more information on how to attach more disks and to use the new disk partitioning tool, see How to attach an extra disk to NetScaler ADM.

Provision NetScaler instances in OpenStack using StyleBooks

From NetScaler ADM 12.1 build 49.23 onwards, the architecture of an OpenStack orchestration workflow has been updated. The workflow now uses NetScaler ADM StyleBooks to configure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler instances. If you upgrade to NetScaler ADM 13.1 from version 12.0 or 12.1 build 48.18, you must run the following migration script:

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

For more information about the `os-cs-lb-mon` StyleBook and the migration script, see Provisioning of NetScaler VPX instance on OpenStack using StyleBook

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication

Users can be authenticated either internally by NetScaler® ADM, externally by an authenticating server, or both. If local authentication is used, the user must be in the NetScaler ADM security database. If the user is authenticated externally, the user “external name” must match the external user identity registered with the authenticating server, depending on the selected authentication protocol.

NetScaler ADM supports external authentication by RADIUS, LDAP, and TACACS servers. This unified support provides a common interface to authenticate and authorize all the local and external Authentication, Authorization, and Accounting server users who are accessing the system. NetScaler ADM can authenticate users regardless of the actual protocols they use to communicate with the system. When a user attempts to access a NetScaler ADM implementation that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. If the authentication is successful, the user is granted access to NetScaler ADM.

External authentication servers

NetScaler ADM sends all authentication, authorization, and auditing service requests to the remote RADIUS, LDAP, or TACACS server. The remote authentication, authorization, and auditing server receive the request, validates the request, and sends a response to NetScaler ADM. When configured to use a remote RADIUS, TACACS, or LDAP server for authentication, NetScaler ADM becomes a RADIUS, TACACS, or LDAP client. In any of these configurations, authentication records are stored in the remote host server database. The account name, assigned permissions, and time-accounting records are also stored on the authentication, authorization, and auditing server for each user.

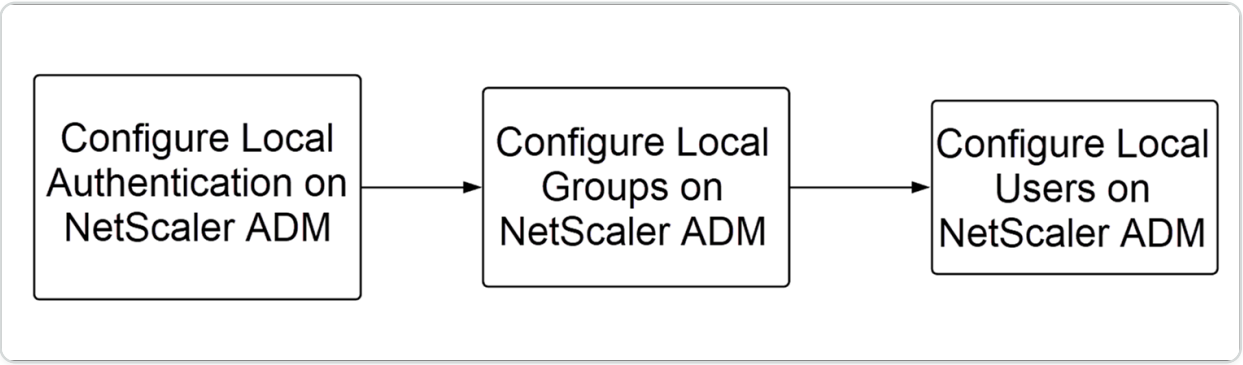
Also, you can use the internal database of NetScaler ADM to authenticate users locally. You create entries in the database for users and their passwords and default roles. You can also select the authentication order for specific types of authentication. The list of servers in a server group is an ordered list. The first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers to include the internal database as a fallback authentication backup to the configured list of authentication, authorization, and auditing servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

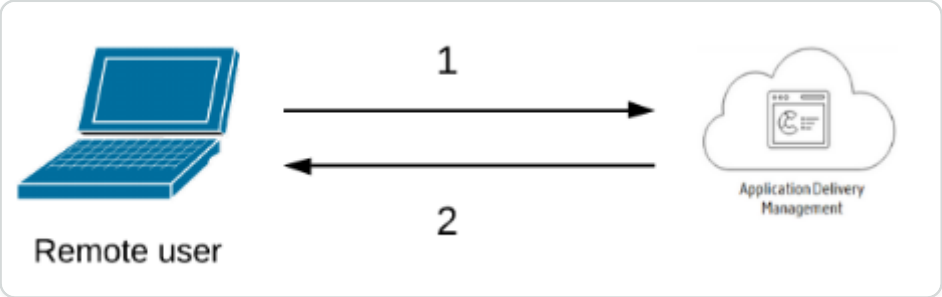
Authenticate users in NetScaler ADM

You can authenticate your users in NetScaler ADM in two ways:

- Local users configured in NetScaler ADM



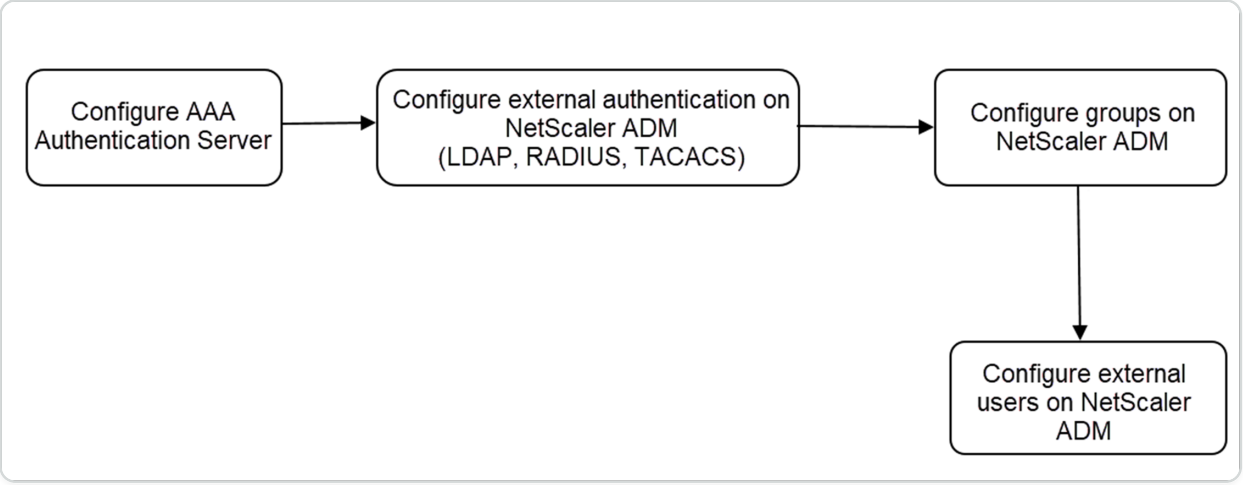
After configuration, the following is the workflow for user authentication in the local server.



1 – The user logs on to NetScaler ADM

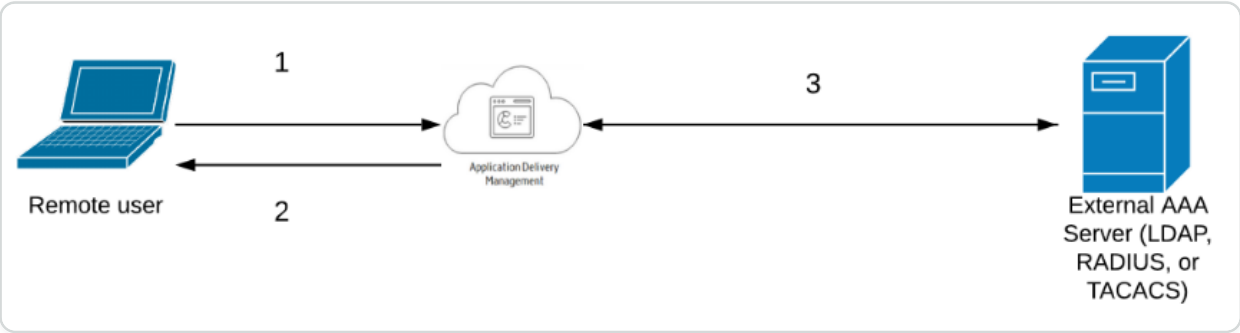
2 – NetScaler ADM prompts the users for credentials for authentication and checks if the credentials match in the ADM database.

- Using external authentication servers



After configuration, the following is the workflow for user authentication in the external authentication, authorization, and auditing server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – The user connects with NetScaler ADM

2 – NetScaler ADM prompts the user for credentials

3 – NetScaler ADM validates the user credentials with the external authentication, authorization, and auditing server. If the validation is successful, the user can continue to log on

Configure external authentication servers in NetScaler® ADM

After you configure the LDAP, RADIUS, or TACACS server, you can add these servers in NetScaler ADM.

Add LDAP authentication server

When you integrate LDAP protocol with RADIUS and TACAS authentication servers, you can use ADM to search and authenticate user credentials from distributed directories.

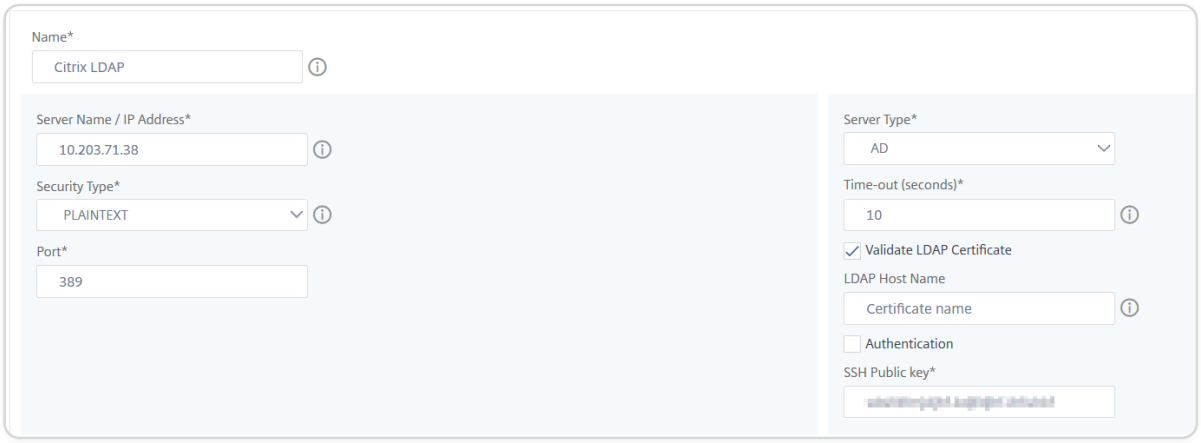
1. Navigate to **Settings > Authentication**.
2. Select the **LDAP** tab and then click **Add**.
3. On the **Create LDAP Server** page, specify the following parameters:
   a. **Name** – Specify the LDAP server name
   b. **Server Name/IP address** – Specify the LDAP IP address or server name
   c. **Security Type** – Type of communication required between the system and the LDAP server. Select from the list. If plain text communication is inadequate, you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL
   d. **Port** – By default, port 389 is used for PLAINTEXT. You can also specify port 636 for SSL/TLS
   e. **Server Type** – Select Active Directory (AD) or Novell Directory Service (NDS) as the type of LDAP server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

f. **Time-out (seconds)** – Time in seconds for which the NetScaler® ADM system waits for a response from the LDAP server

g. **LDAP Host Name** – Select Validate LDAP Certificate check box and specifying the host name to be entered on the certificate

Clear the **Authentication** option and specify the SSH Public Key. With key-based authentication, you can now fetch the list of public keys that are stored on the user object in LDAP server through SSH.



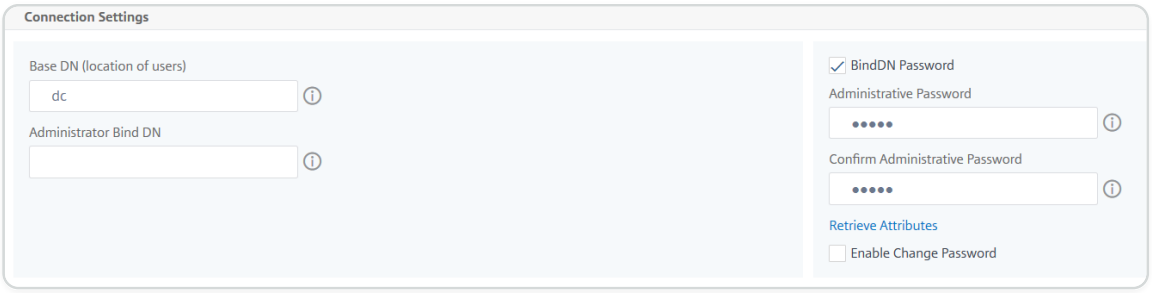
Under Connection Settings, specify the following parameters:

i. **Base DN** – The base node for LDAP server to start the search

ii. **Administrator Bind DN** – User name to it bind to LDAP server. For example, admin@aaa.local.

iii. **Bind DN password** – Select this option to provide a password for authentication

iv. **Enable Change Password** – Select this option to enable password change



Under **Other Settings**, specify the following parameters

i. **Server Log on Name Attribute** – Name attribute used by the system to query the external LDAP server or an Active Directory. Select **samAccountname** from the list.

ii. **Search Filter** – Configure external users for two-factor authentication according to the search filter configured in LDAP server. For example, vpnallowed=true with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ldaploginame `samaccount` and the user-supplied user name bob would yield an LDAP search string of: `&(vpnallowed=true)(samaccount=bob)`.

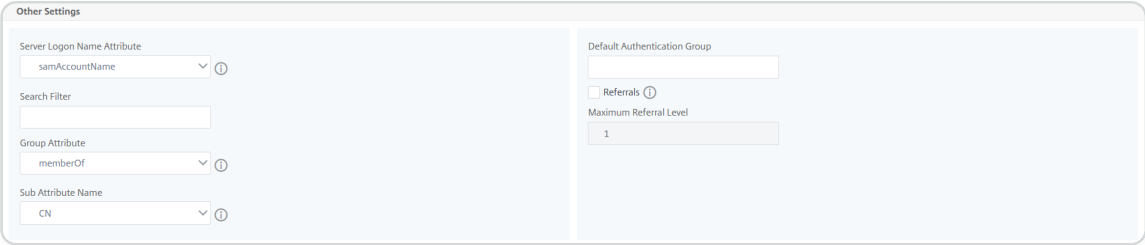
Note

> By default, the values in the search filter are enclosed in brackets.

iii. **Group Attribute** – Select memberOf from the list.

iv. **Sub Attribute Name** – The Sub attribute name for group extraction from the LDAP server.

v. **Default Authentication Group** – Default group to choose when the authentication succeeds in addition to extracted groups.



4. Click **Create**.

   The LDAP server is now configured.

   NOTE

   .

   > If the users are Active Directory group members, the group and the users' names on NetScaler ADM must have the same names of Active Directory group members.

5. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add RADIUS authentication server

1. Navigate to **Settings > Authentication**.
2. Select the **RADIUS** tab and then click **Add**.

   On the **Create RADIUS Server** page, specify the following parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Name** – Specify a RADIUS server name

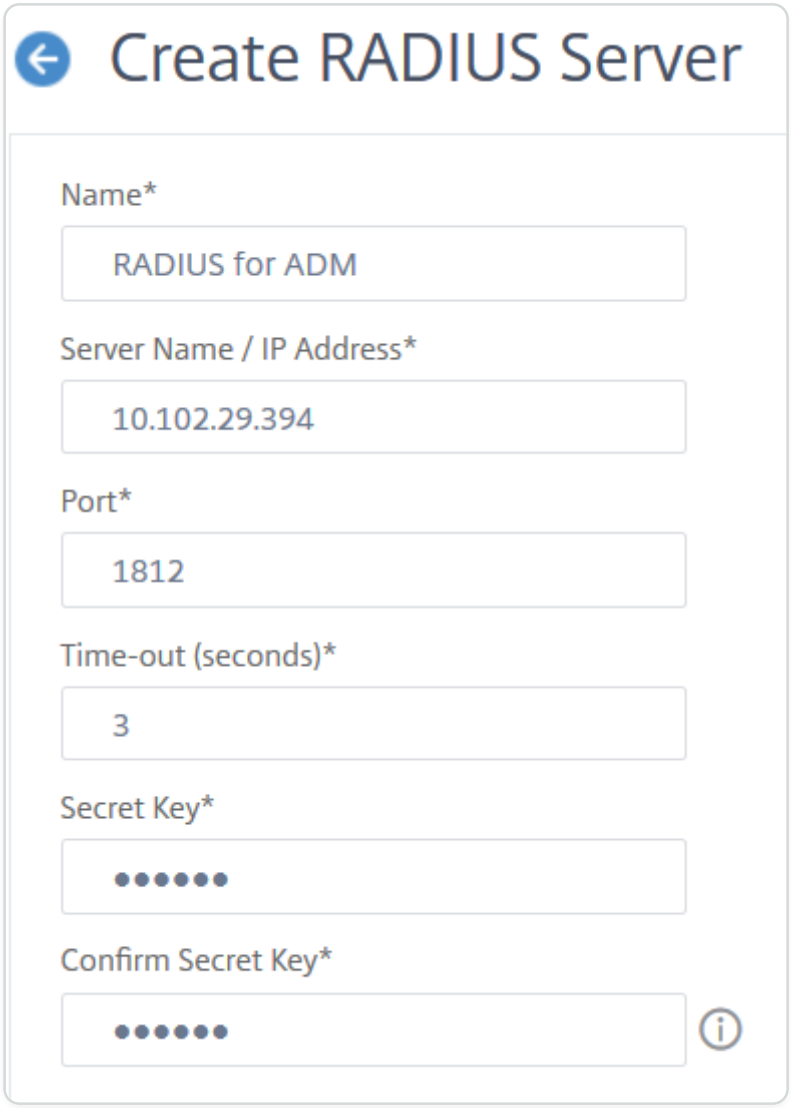
b. **Server Name / IP address** – Specify the RADIUS server IP address

c. **Port** – Specify the port number on which the RADIUS server is hosted. The default port is 1812

d. **Time-out (seconds)** – Time in seconds for which the NetScaler® ADM system waits for a response from the RADIUS server

e. **Secret Key** – Specify the RADIUS secret key for authentication

f. **Confirm Secret Key** – Specify the key again for confirmation



Under **Details**, specify the following parameters:

i. **NAS ID** – Specify the ID to send the identifier to RADIUS server

ii. **Group Vendor Identifier** – Specify the vendor ID for using RADIUS group extraction

iii. **Group Prefix** - A string that precedes group names within a RADIUS attribute for RADIUS group extraction

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iv. **Group Attribute Type** – Specify the attribute type for RADIUS group extraction

v. **Group Separator** – A string that delimits group names within a RADIUS attribute for RADIUS group extraction

vi. **IP Address Vendor Identifier** – Vendor ID in RADIUS denotes the intranet IP. A value of 0 denotes that the attribute is not vendor encoded

vii. **Password Vendor Identifier** – Vendor ID password in RADIUS response to extract the user password

viii. **IP Address Attribute Type** – Remote IP address attribute for the RADIUS to respond

ix. **Password Attribute Type** – The password attribute for the RADIUS to respond

x. **Password encoding** – Select pap, chap, mschapv1, or mschapv2 from the list. This denotes how passwords should be encoded in the RADIUS packets traveling from the system to the RADIUS server.

xi. **Default Authentication Group** – Default group to choose when the authentication succeeds in addition to extracted groups

Select Accounting if you want the appliance to log audit information with RADIUS server.

3. Click **Create**.

   The RADIUS server is now configured.

4. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add TACACS authentication server

1. Navigate to **Settings > Authentication**.
2. Select the **TACACS** tab and then click **Add**.
3. On the **Create TACACS** page, specify the following parameters:

   a. **Name** – Specify a TACACS server name

   b. **IP address** – Specify the TACACS IP address

   c. **Port** – Specify the port number on which the TACACS server is hosted. The default port is 49

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. **Time-out (seconds)** – Time in seconds for which the NetScaler® ADM system waits for a response from the LDAP server

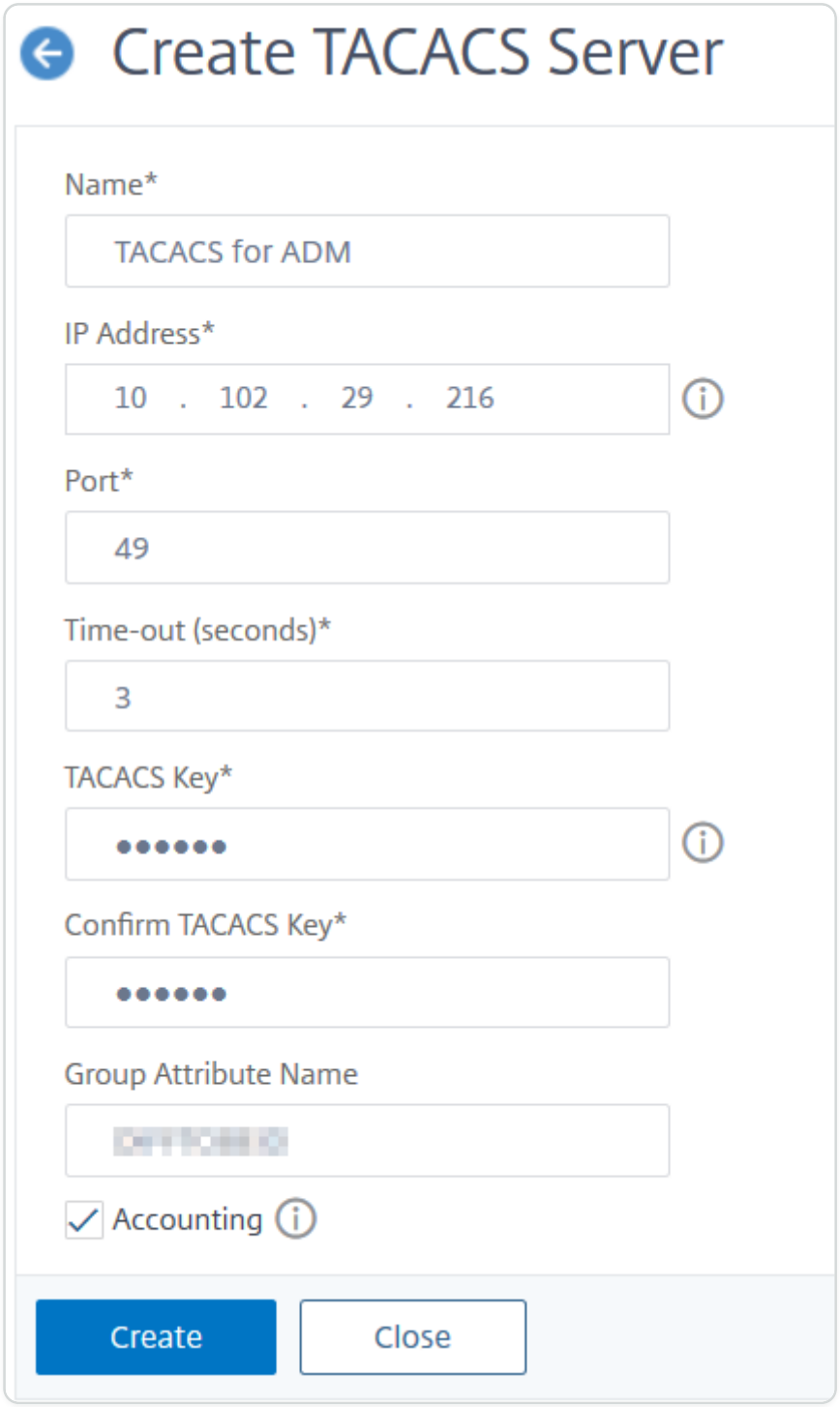
e. **TACACS Key** – Specify the TACACS key for authentication

f. **Confirm TACACS Key** – Specify the TACACS key again for confirmation

g. **Group Attribute Name** – Specify the group name

Select **Accounting** if you want the appliance to log audit information with TACACS server.

4. Click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Users in NetScaler® ADM

You can create user accounts locally on NetScaler ADM to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server.

For more information on configuring users, see Configure Users.

Note

> If the users are on Active Directory, ensure that the group name in NetScaler ADM is same as the one for the Active Directory group on the external server.

User Groups in NetScaler ADM

NetScaler ADM allows you to authenticate and authorize your users by creating groups and adding the users to the groups. A group can have either “admin” or “read-only” permissions and all users in that group will receive equal permissions.

In NetScaler ADM:

- A group is defined as a collection of users having similar permissions
- A group can have one or multiple roles
- A user is defined as an entity that can have access based on the permissions assigned
- A user can belong to one or more groups

You can create local groups in NetScaler ADM and use local authentication for the users in the groups. If you are using external servers for authentication, configure the groups on NetScaler ADM to match the groups configured on authentication servers in the internal network. When a user logs on and is authenticated, if a group name matches a group on an authentication server, the user inherits the settings for the group on NetScaler ADM. If you are using local authentication, create users and add them to groups configured on NetScaler ADM. The users then inherit the settings for those groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on configuring groups and assigning group permissions, see Configure Groups.

Extract an authentication server group

NOTE

TACACS server extraction is supported from **NetScaler ADM 13.0**.

NetScaler® ADM enables you to:

- Extract the list of groups that a user belongs to on the external authentication server.
- Assign them to the group settings that match with the groups configured on the external server.

Advantages:

- You do not have to create users in NetScaler ADM, as they are managed on the external server.
- NetScaler ADM performs the authorization of users by assigning group permissions to access specific load balancer virtual servers, and for specific applications on the system.

Enable external authentication servers and fallback options

Fallback option enables local authentication to take over if the external server authentication fails. A user configured on both NetScaler® ADM and external authentication server can log on to NetScaler ADM, even if the configured external authentication servers are down or not reachable. To ensure fallback authentication work:

- Non-nsroot users must be able to access NetScaler ADM if external server is down or not reachable
- You must add at least one external server

NetScaler ADM also supports a unified system of authentication, authorization, and accounting (AAA) protocols (LDAP, RADIUS, and TACACS), along with local authentication. This unified support provides a common interface to authenticate and authorize all users and external AAA clients accessing the system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM can authenticate users regardless of the actual protocols they to communicate with the system. Cascading external authentication servers provides a continuous non-failing process for authenticating and authorizing external users. If authentication fails on the first authentication server, NetScaler ADM attempts to authenticate the user by using the second external authentication server, and so on. To enable cascade authentication, you must add the external authentication servers in NetScaler ADM. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS).

For example, consider that you want to add four external authentication servers and configured two RADIUS servers, one LDAP server, and one TACACS server. NetScaler ADM attempts to authenticate with the external servers, based on the configurations. In this example scenario, NetScaler ADM attempts to:

- Connect with the first RADIUS server
- Connect with the second RADIUS server, if the authentication has failed with first RADIUS server
- Connect with the LDAP server, if the authentication has failed with both RADIUS servers
- Connect with the TACACS server, if the authentication has failed with both RADIUS servers and LDAP server.

Note

> You can configure up to 32 external authentication servers in NetScaler ADM.

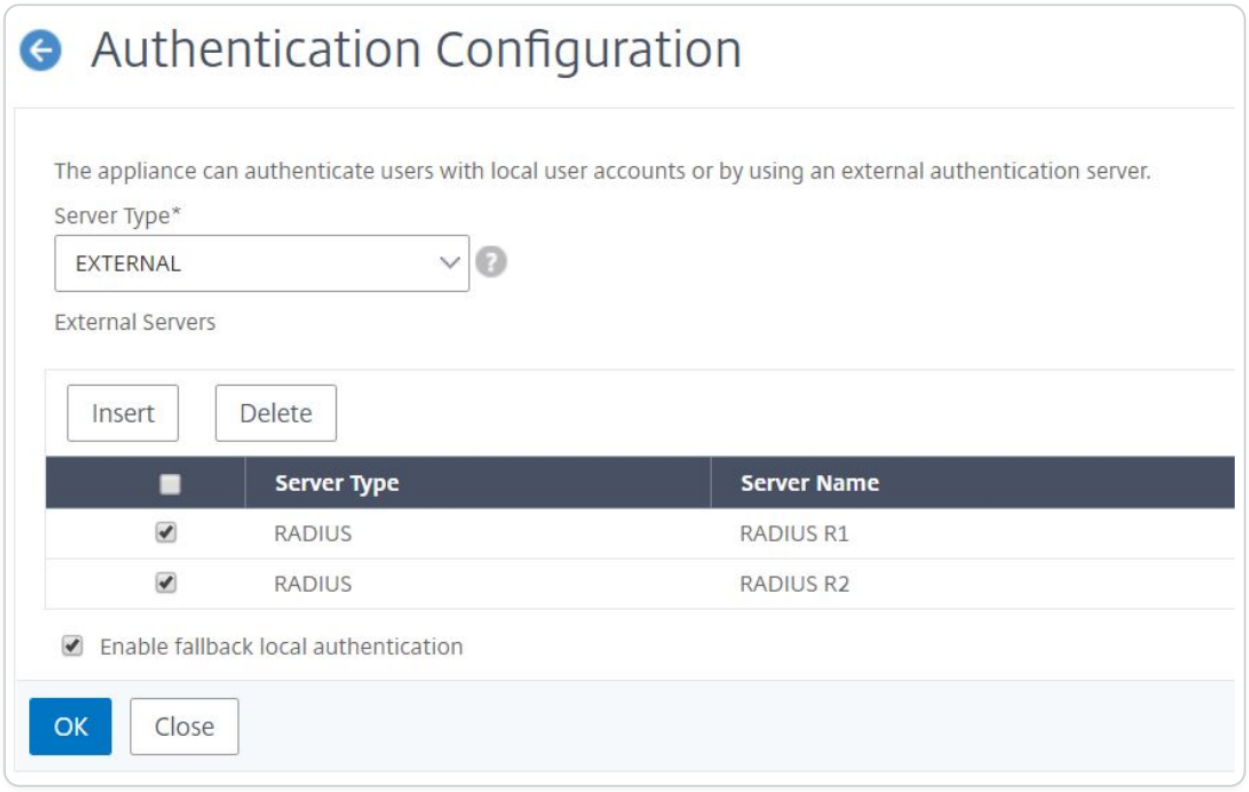
Configure fallback and cascade external servers

1. Navigate to **Settings > Authentication**.
2. On the **Authentication** page, click **Settings**
3. On the **Authentication Configuration** page, select **EXTERNAL** from the **Server Type** list (only external servers can be cascaded).
4. Click **Insert**, and on the **External Servers** page, select one or multiple authentication servers to cascade.
5. Select the **Enable fallback local authentication** check box if you want the local authentication to take over if the external authentication fails.
6. Select the **Log external group information** check box if you want to capture the external user group information in the system audit log.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Click **OK** to close the page.

   The selected servers are displayed under External Servers:



You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Control

Authentication is a process by which you verify that someone is who they claim they are. To perform authentication, a user must already have an account created in a system which can be interrogated by the authentication mechanism, or an account must be created as part of the process of the first authentication. NetScaler® Application Delivery Management (ADM) provides a method for authenticating both local users and external users. While local users are authenticated internally, NetScaler ADM supports external authentication with RADIUS, LDAP, and TACACS protocols. When a user attempts to access NetScaler ADM that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. Once authenticated, the required protocol is used to identify the user on NetScaler ADM.

Access Control is the process of enforcing the required security for a particular resource. It is a security technique that can be used to regulate who can view or use resources in a computing environment. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, and what programs running on behalf of the users are allowed to do. In this way access control seeks to prevent activity that can lead to a breach of security. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control through a reference monitor. NetScaler ADM allows fine-grained, role-based access control (RBAC) by which the administrators can provide access permissions to users based on the roles of individual users within an enterprise. RBAC in NetScaler ADM is achieved by creating access policies, roles, groups, and users.

Role-based access control

NetScaler® ADM provides fine-grained, role based access control (RBAC), with which you can grant access permissions based on the roles of individual users within your enterprise. In this context, access is the ability to perform a specific task, such as view, create, modify, or delete a file. Roles are defined according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and help creating configuration templates.

Roles are determined by in policies. After creating policies, you create roles, bind each role to one or more policies, and assign roles to users. You can also assign roles to groups of users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A group is a collection of users who have permissions in common. For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users or groups based on specific conditions. In NetScaler ADM, creating roles and policies are specific to the RBAC feature in NetScaler. Roles and policies can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

Roles can be feature based or resource based. For example, consider an SSL/security administrator and an application administrator. An SSL/security administrator must have complete access to SSL Certificate management and monitoring features, but must have read-only access for system administration operations. An application administrator must be able to access only the resources within the scope.

Example:

Chris, the ADC group head, is the super administrator of NetScaler ADM in his organization. Chris creates three administrator roles: security administrator, application administrator, and network administrator.

David, the security admin, must have complete access for SSL Certificate management and monitoring but also have read-only access for system administration operations.

Steve, an application admin, needs access to only specific applications and only specific configuration templates.

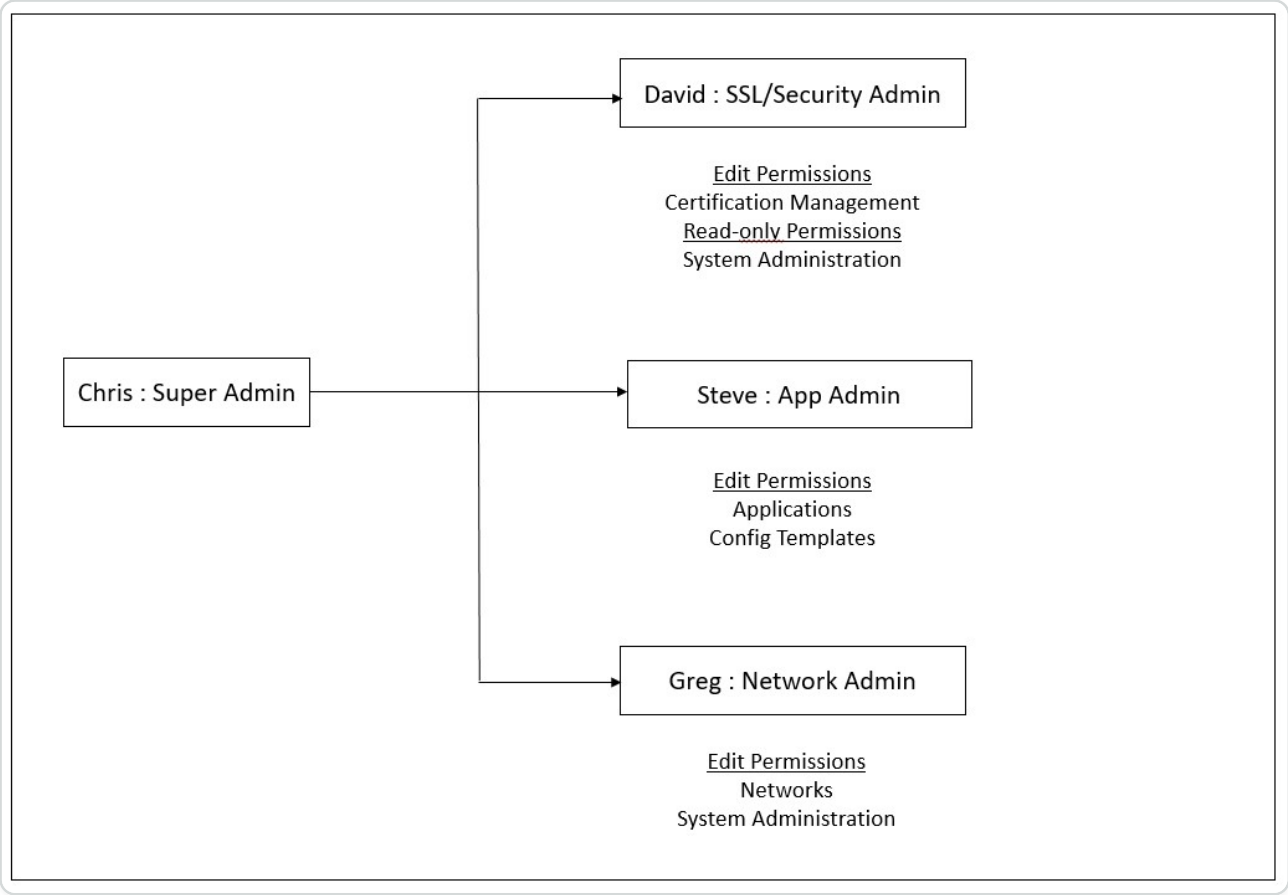
Greg, a network admin, needs access to system and network administration.

Chris also must provide RBAC for all users, irrespective of the fact that they are local or external.

NetScaler ADM users can be locally authenticated or can be authenticated through an external server (RADIUS/LDAP/TACACS). RBAC settings must be applicable to all users irrespective of the authentication method adopted.

The following image shows the permissions that the administrators and other users have and their roles in the organization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Limitations

RBAC is not fully supported for the following NetScaler ADM features:

- **Analytics** - RBAC is not supported fully in the analytics modules. RBAC support is limited to instance level, and it is not applicable at application level in the Web Insight, SSL Insight, Gateway Insight, HDX™ Insight, and WAF Security Violations analytics modules. For example:

Example 1: Instance based RBAC (Supported)

An administrator who has been assigned a few instances can see only those instances under **Web Insight** \> **Instances**, and only the corresponding virtual servers under **Web Insight** \> **Applications**, because RBAC is supported at instance level.

Example 2: Application based RBAC (Not Supported)

An administrator who has been assigned a few applications can see all virtual servers under **Web Insight** \> **Applications** but cannot access them, because RBAC is not supported at applications level.

- **StyleBooks** – RBAC is not fully supported for StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In NetScaler ADM, StyleBooks and configuration packs are considered as separate resources. Access permissions, either view, edit, or both, can be provided for StyleBook and configuration packs separately or concurrently. A view or edit permission on configuration packs implicitly allows the user to view the StyleBooks, which is essential for getting the configuration pack details and creating configuration packs.
- Access permission for specific StyleBook or configuration packs is not supportedExample: If there is already a configuration pack on the instance, users can modify the configuration on a target NetScaler instance even if they don't have access to that instance.

- **Orchestration** - RBAC is not supported for Orchestration.

Configure access policies

Access policies define permissions. A policy can be applied to a single user or group, or to multiple users and multiple groups. NetScaler® Application Delivery Management (ADM) provides four predefined access policies:

1. **adminpolicy**. Grants access all NetScaler ADM features. The user has both view and edit permissions, can view all NetScaler ADM content, and can perform all edit operations. That is, the user can perform add, modify, and delete operations on the resources.
2. **readonlypolicy**. Grants read-only permissions. The user can view all content on NetScaler ADM, but is not authorized to perform any operations.
3. **appAdminPolicy**. Grants administrative permissions for accessing the application features in NetScaler ADM. A user bound to this policy can add, modify, and delete custom applications, and can enable or disable the services, service groups, and the various virtual servers, such as content switching, cache redirection, and HAProxy virtual servers.
4. **appReadOnlyPolicy**. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.

NOTE:

The predefined policies cannot be edited.

You can also create your own (user-defined) policies.

To create user-define access policies:

1. In NetScaler ADM, navigate to **Settings > Users & Roles > Access Policies**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Add**.
3. In the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.

   The **Permissions** section lists of all NetScaler ADM features, with options for specifying read-only, enable-disable, or edit access.
4. Click the (+) icon to expand each feature group into multiple features.

   a. Select the permission check box next to the feature name to grant permissions to the users.

      - **View:** This option allows the user to view the feature in NetScaler ADM.
      - **Enable-Disable:** This option is available only for the **Network Functions** features that allow enable or disable action on NetScaler ADM. User can enable or disable the feature. And, user can also perform the **Poll Now** action.

        When you grant the **Enable-Disable** permission to a user, the **View** permission is also granted. You cannot deselect this option.
      - **Edit:** This option grants the full access to the user. User can modify the feature and its functions.

        If you grant the **Edit** permission, both **View** and **Enable-Disable** permissions are granted. You cannot deselect the auto-selected options.

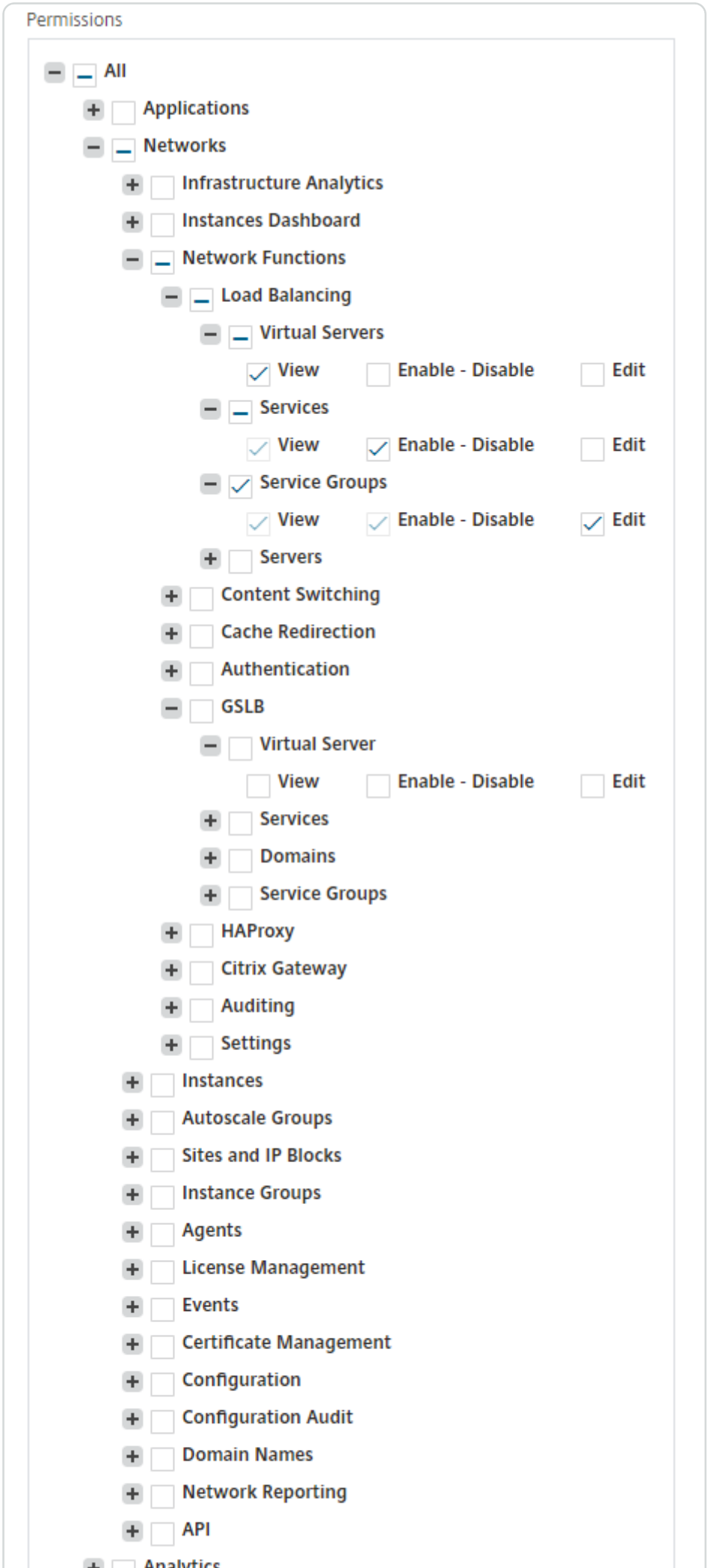
   If you select the feature check box, it selects all the permissions for the feature.

   NOTE:

   Expand Load Balancing and GSLB to view more configuration options.

   In the following image, the configuration options of the Load Balancing feature have different permissions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Permissions
All
Applications
Networks
Infrastructure Analytics
Instances Dashboard
Network Functions
Load Balancing
Virtual Servers
View
Enable - Disable
Edit
Services
View
Enable - Disable
Edit
Service Groups
View
Enable - Disable
Edit
Servers
Content Switching
Cache Redirection
Authentication
GSLB
Virtual Server
View
Enable - Disable
Edit
Services
Domains
Service Groups
HAProxy
Citrix Gateway
Auditing
Settings
Instances
Autoscale Groups
Sites and IP Blocks
Instance Groups
Agents
License Management
Events
Certificate Management
Configuration
Configuration Audit
Domain Names
Network Reporting
API
Analytics

The **View** permission is granted to a user for the **Virtual Servers** feature. User can view the load balancing virtual servers in NetScaler ADM. To view virtual servers, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Virtual Servers** tab.

The **Enable-Disable** permission is granted to a user for the **Services** feature. This permission also grants the **View** permission. User can enable or disable the services bound to a load balancing virtual server. Also, user can perform **Poll Now** action on services. To enable or disable services, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Services** tab.

NOTE:

If a user has the **Enable-Disable** permission, the enable or disable action on a service is restricted in the following page:

a. Navigate to **Infrastructure > Network Functions**.
b. Select a virtual server and click **Configure**.
c. Select the **Load Balancing Virtual Server Service Binding** page. This page displays an error message if you select **Enable** or **Disable**.

The **Edit** permission is granted to a user for the **Service Groups** feature. This permission grants the full access where **View** and **Enable-Disable** permissions are granted. User can modify the service groups that are bound to a load balancing virtual server. To edit service groups, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Service Groups** tab.

5. Click **Create**.

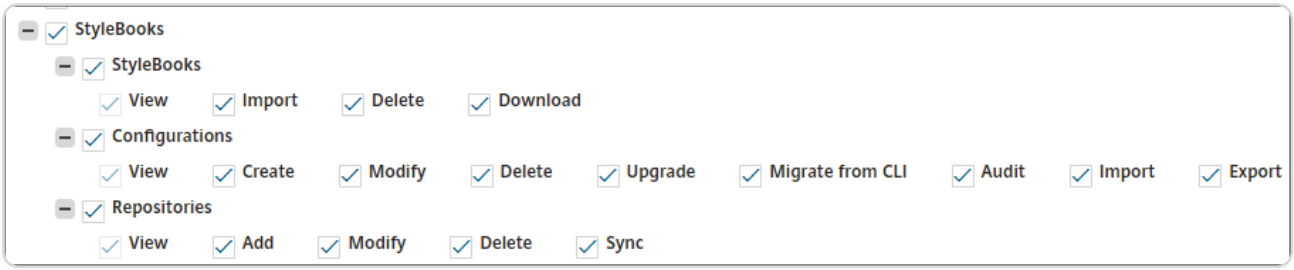
Grant StyleBook permissions to users

You can create an access policy to grant StyleBook permissions such as import, delete, download, and more.

NOTE:

The View permission is automatically enabled when you grant other StyleBook permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure groups

In NetScaler ADM, a group can have both feature-level and resource-level access. For example, one group of users might have access to only selected NetScaler instances; another group with only a selected few applications, and so on.

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. All users in that group are assigned the same access rights in NetScaler® ADM.

You can manage a user access in NetScaler ADM at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.

NetScaler ADM treats virtual server, services, service groups, and servers as network function entities.

- **Virtual server (Applications)** - Load Balancing(lb), GSLB, Context Switching (CS), Cache Redirection (CR), Authentication (`Auth`), and NetScaler Gateway (VPN)
- **Services** - Load balancing and GSLB services
- **Service Group** - Load balancing and GSLB Service groups
- **Servers** - Load balancing Servers

Create a user group

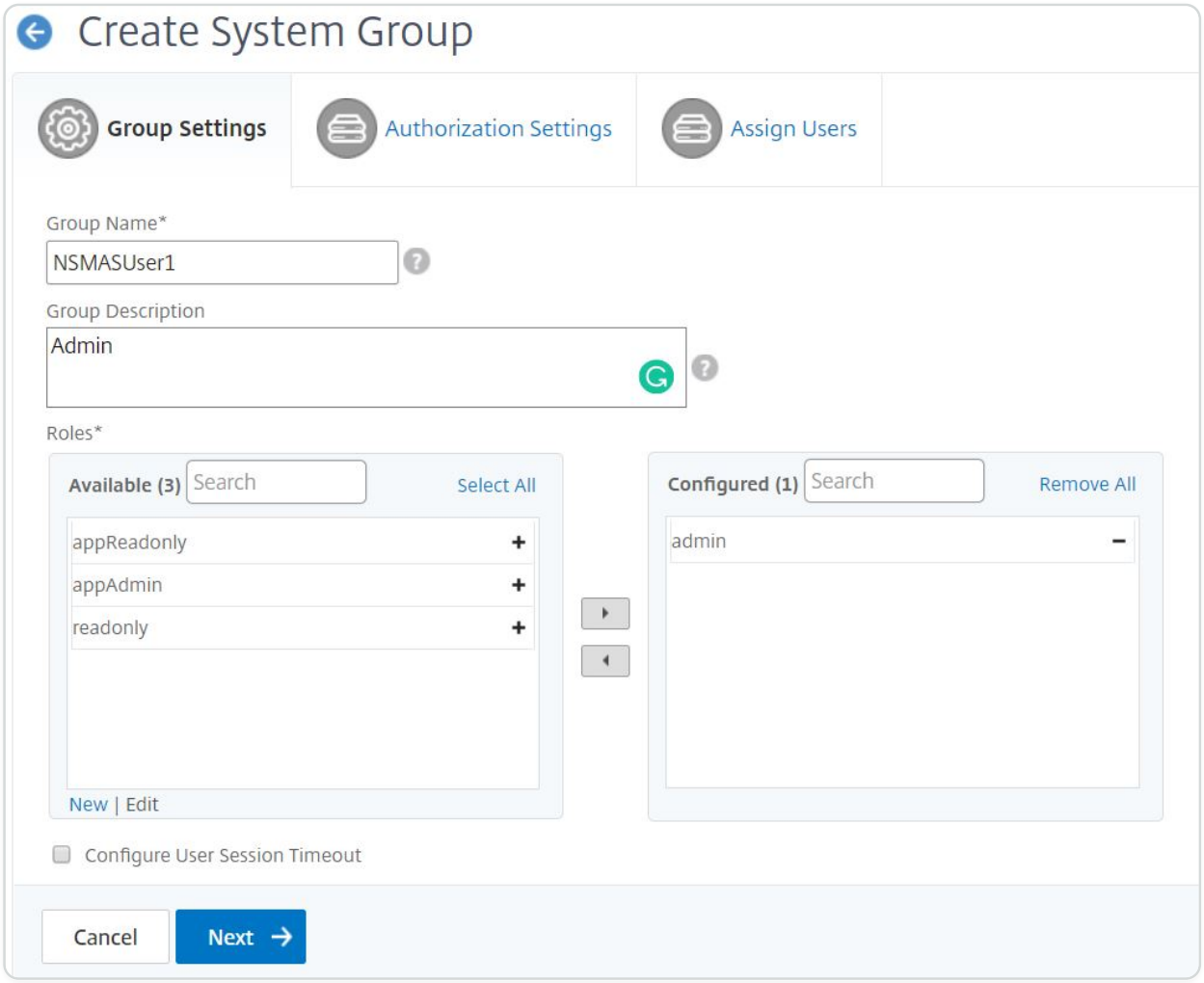
1. In NetScaler ADM, navigate to **Settings > Users & Roles > Groups**.
2. Click **Add**.

   The **Create System Group** page is displayed.
3. In the **Group Name** field, enter the name of the group.
4. In the **Group Description** field, type in a description of your group. Providing a good description of the group helps you to understand the role and function of the group in a better way at a later point.
5. In the **Roles** section, add or move one or more roles to the **Configured** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

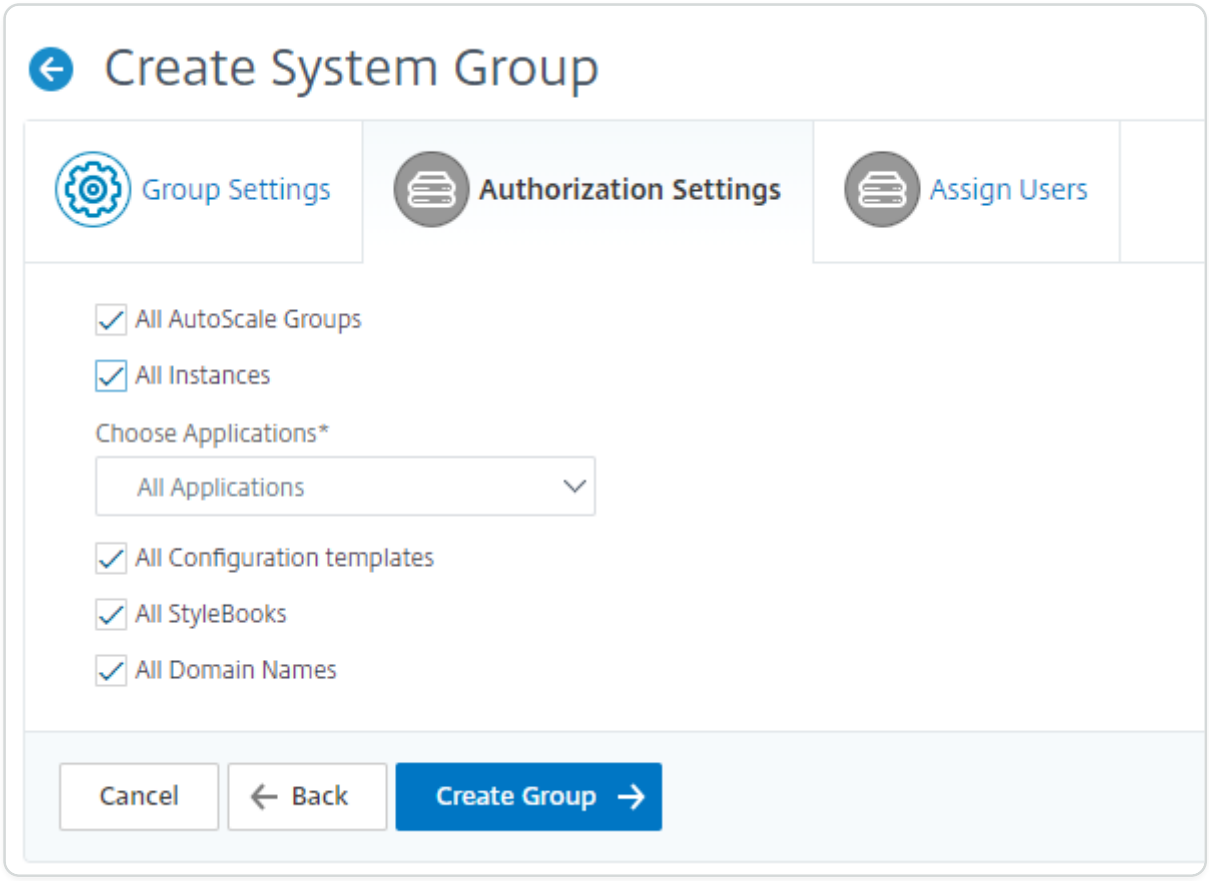
Under the **Available** list, you can click **New** or **Edit** and create or modify roles. Alternatively, you can navigate to **Settings > Users & Roles > Users** and create or modify users.



6. Click **Next**. On the **Authorization Settings** tab, you can provide authorization settings for the following resources:

   - Autoscale™ Groups
   - Instances
   - Applications
   - Configuration Templates
   - StyleBooks
   - Configpacks
   - Domain Names

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You might want to select specific resources from the categories to which users can have access.

Autoscale Groups:

If you want to select the specific Autoscale groups that a user can view or manage, perform the following steps:

a. Clear the **All AutoScale Groups** check box and click **Add AutoScale Groups**.

b. Select the required Autoscale groups from the list and click **OK**.

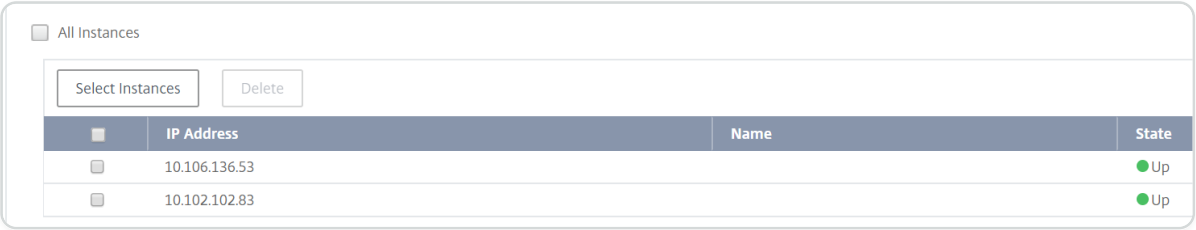
Instances:

If you want to select the specific instances that a user can view or manage, perform the following steps:

a. Clear the **All Instances** check box and click **Select Instances**.

b. Select the required instances from the list and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Applications:

The **Choose Applications** list allows you to grant access to a user for the required applications.

You can grant access to applications without selecting their instances. Because applications are independent of their instances to grant user access.

When you grant a user access to an application, the user is authorized to access only that application regardless of instance selection.

This list provides you the following options:

- **All Applications:** This option is selected by default. It adds all the applications that are present in the NetScaler ADM.
- **All Applications of selected instances:** This option appears only if you select instances from the **All Instances** category. It adds all the applications present on the selected instance.
- **Specific Applications:** This option allows you to add the required applications that you want users to access. Click **Add Applications** and select the required applications from the list.
- **Select Individual Entity Type:** This option allows you to select a specific type of network function entity and corresponding entities.

  You can either add individual entities or select all entities under the required entity type to grant access to a user.

  The **Apply on bound entities also** option authorizes the entities that are bound to the selected entity type. For example, if you select an application and select **Apply on bound entities also**, NetScaler ADM authorizes all the entities that are bound to the selected application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

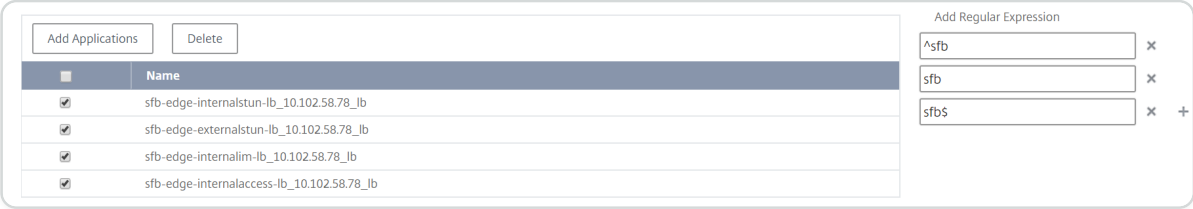
Ensure you have selected only one entity type if you want to authorize bound entities.

You can use regular expressions to search and add the network function entities that meet the regex criteria for the groups. The specified regex expression is persisted in NetScaler ADM. To add regular expression, perform the following steps:

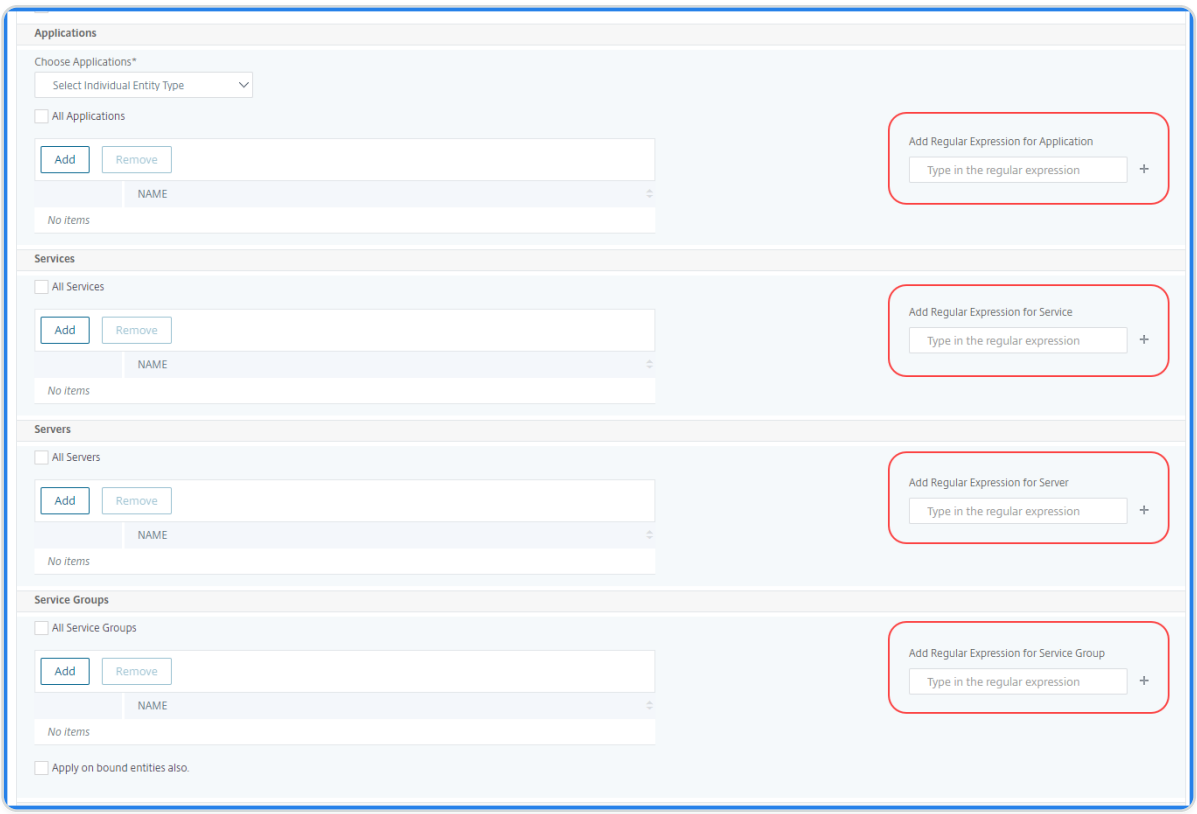
a. Click **Add Regular Expression**.

b. Specify the regular expression in the text box.

The following image explains how to use regular expression to add an application when you select the **Specific Applications** option:



The following image explains how to use regular expression to add network function entities when you choose the **Select the Individual Entity Type** option:



If you want to add more regular expressions, click the **+** icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The regular expression only matches the server name for the **Servers** entity type and not the server IP address.

If you select the **Apply on bound entities also** option for a discovered entity, a user can automatically access the entities that are bound to the discovered entity.

The regular expression is stored in the system to update the authorization scope. When the new entities match the regular expression of their entity type, NetScaler ADM updates the authorization scope to the new entities.

Configuration Templates:

If you want to select the specific configuration template that a user can view or manage, perform the following steps:

a. Clear the **All Configuration templates** check box and click **Add Configuration Template**.
b. Select the required template from the list and click **OK**.

StyleBooks:

If you want to select the specific StyleBook that a user can view or manage, perform the following steps:

a. Clear the **All StyleBooks** check box and click **Add StyleBook to Group**. You can either select individual StyleBooks or specify a filter query to authorize StyleBooks.

   If you want to select the individual StyleBooks, select the StyleBooks from the **Individual StyleBooks** pane and click **Save Selection**.

   If you want to use a query to search StyleBooks, select the **Custom Filters** pane. A query is a string of key-value pairs where keys are `name`, `namespace`, and `version`.

   You can also use regular expressions as values to search and add StyleBooks that meet regex criteria for the groups. A custom filter query to search StyleBooks supports both `And` and `Or` operation.

   Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
version=1.0
```

This query lists the StyleBooks that meet the following conditions:

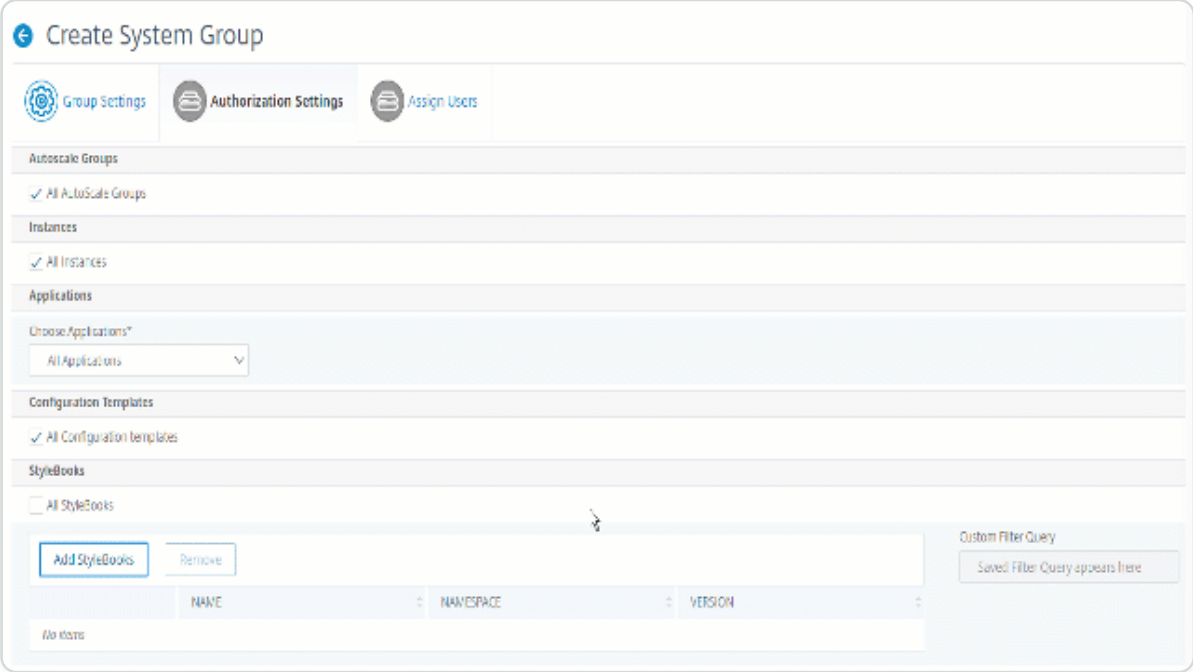
- StyleBook name is either `lb-mon` or `lb`.
- StyleBook namespace is `com.citrix.adc.stylebooks`.
- StyleBook version is `1.0`.

Use an `Or` operation between value expressions that is defined to the key expression.

Example:

- The `name=lb-mon|lb` query is valid. It returns the StyleBooks having a name either `lb-mon` or `lb`.
- The `name=lb-mon | version=1.0` query is invalid.

Press `Enter` to view the search results and click **Save Query**.



The saved query appears in the **Custom Filters Query**. Based on the saved query, the ADM provides user access to those StyleBooks.

b. Select the required StyleBooks from the list and click **OK**.

You can select the required StyleBooks when you create groups and add users to that group. When your user selects the permitted StyleBook, all dependent StyleBooks are also selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configpacks:

In **Configpacks**, select one of the following options:

- **All Configrations**: This option is selected by default. It adds all the configuration packs that are in ADM.
- **All Configrations of the selected StyleBooks**: This option adds all the configuration packs of the selected StyleBook.
- **Specific Configurations**: This option allows you to add the required cofiguration packs.

  You can select the required configuration packs when you create groups and add users to that group.

Domain Names:

If you want to select the specific domain name that a user can view or manage, perform the following steps:

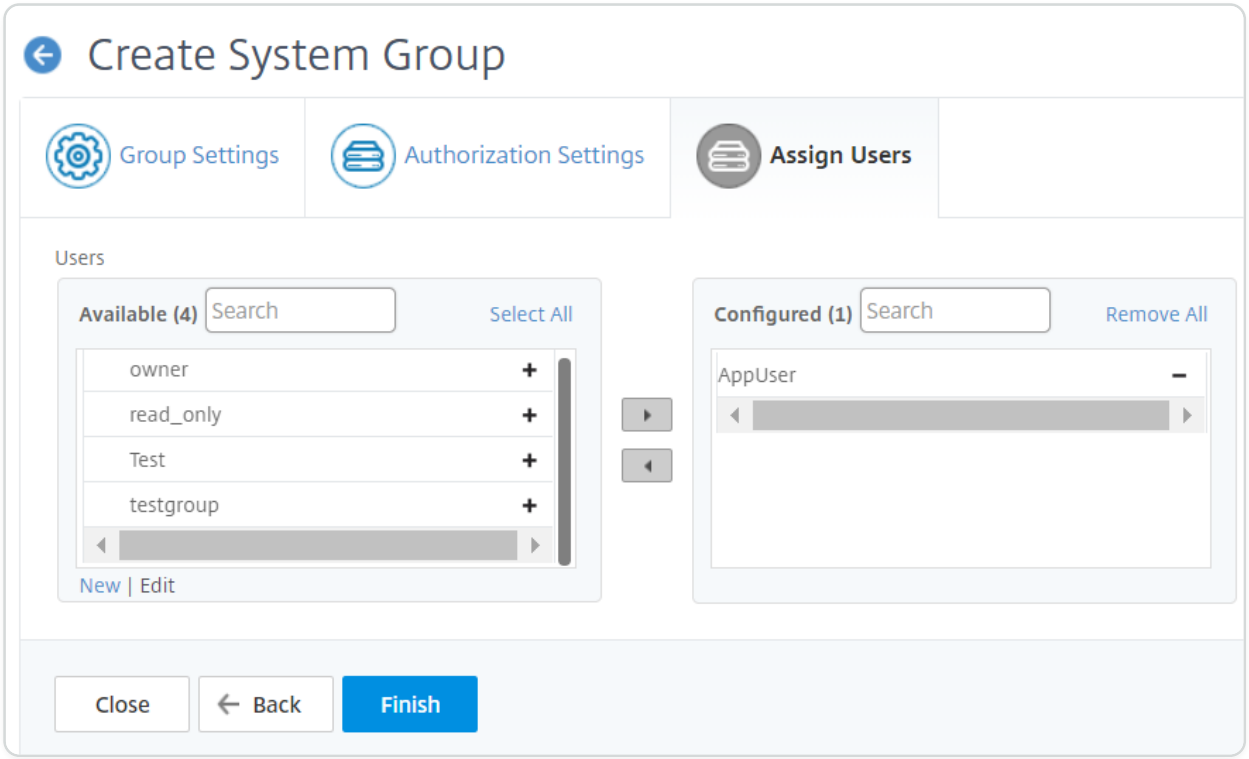
a. Clear the **All Domain Names** check box and click **Add Domain Name**.
b. Select the required domain names from the list and click **OK**.

7. Click **Create Group**.
8. In the **Assign Users** section, select the user in the **Available** list, and add the user to the **Configured** list.

NOTE:

You can also add users by clicking **New**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Click **Finish**.

Manage user access across multiple network function entities

As an administrator, you can manage user access at the individual level of network function entities in NetScaler ADM. And, you can dynamically assign specific permissions to the user or a group at the entity level by using the regular expression filter.

This document describes how to define user authorization at the entity level.

Before you begin, create a group. See Configure groups on NetScaler ADM for more information.

Usage scenario:

Consider a scenario where one or more applications (virtual servers) are hosted on the same server. A super administrator (George) wants to grant Steve (an application administrator) access only to App1 and not to the hosting server.

The following table illustrates this environment, where Server-A hosts applications App-1 and App-2.

HOST SERVER	APPLICATION (VIRTUAL SERVER)	SERVICE	SERVICE GROUP
Server A	App1	App-service-1	App-service-group-1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HOST SERVER	APPLICATION (VIRTUAL SERVER)	SERVICE	SERVICE GROUP
Server A	App2	App-service-2	App-service-group-2

NOTE

NetScaler ADM treats virtual server, services, service groups, and servers as network function entities. The entity type virtual server is referred as an application.

To assign user permissions to network function entities, George defines the user authorization as follows:

1. Navigate to **Account > User Administration > Groups** and add a group.
2. In the **Authorization Settings** tab, select Choose Applications.
3. Choose **Select Individual Entity Type**.
4. Select the **All Applications** entity type and add the App-1 entity from the available list.
5. Click **Create Group**.
6. In **Assign users**, select the users who require the permission. For this scenario, George selects Steve's user profile.
7. Click **Finish**.

With this authorization setting, Steve can manage only App-1 and not other network function entities.

NOTE:

Ensure the **Apply on bound entities also** option is cleared. Otherwise, NetScaler ADM grants access to all network function entities that are bound to App-1. As a result, grants access to the hosting server as well.

A super administrator can specify the regular expressions (regex) for each entity type. The regular expression is stored in the system to update the user authorization scope. When new entities match the regular expression of their entity type, NetScaler ADM can dynamically grant users access to the specific network function entities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To grant user permissions dynamically, the super administrator can add regular expressions in the **Authorization Settings** tab.

In this scenario, George adds `App*` as a regular expression for the Applications entity type and the applications that match the regex criteria appear in the list. With this authorization setting, Steve can access all the applications that match the `App*` regex. However, his access is limited only to the applications not to the hosted server.

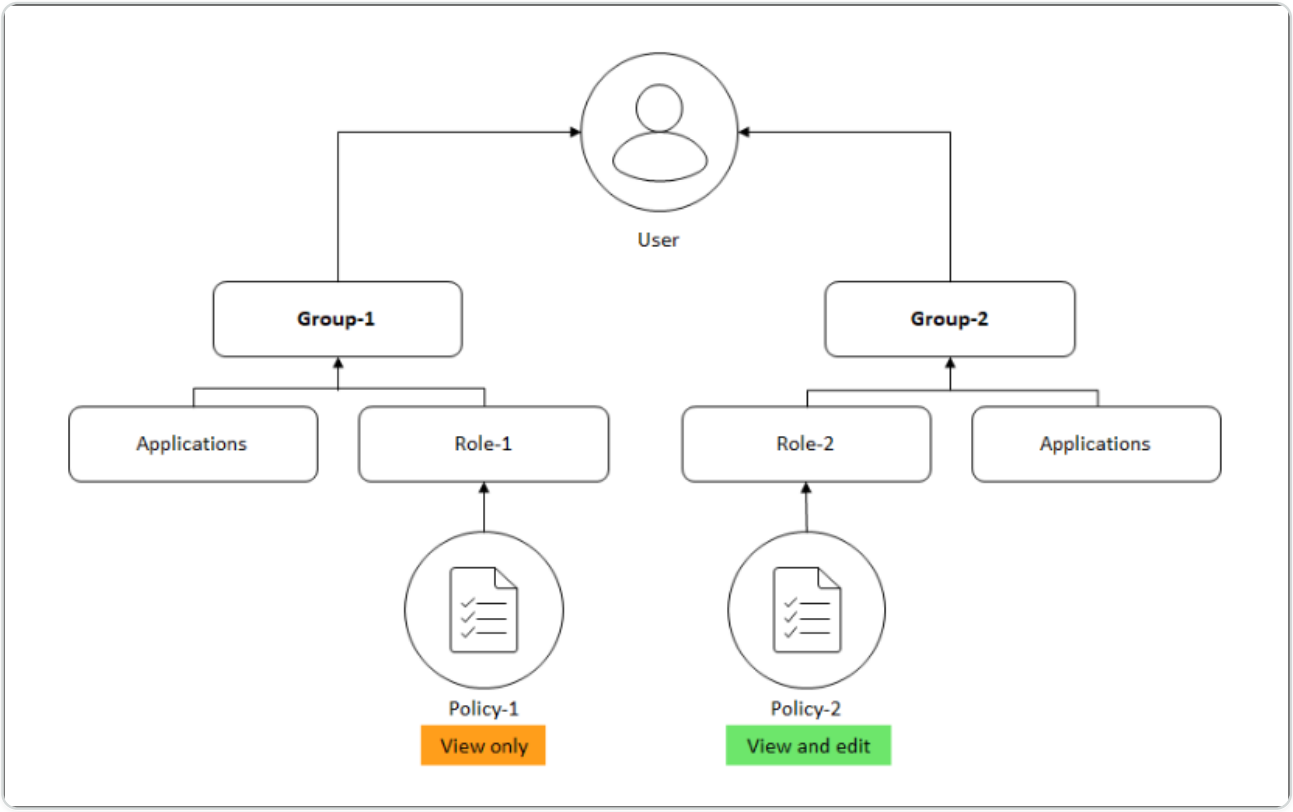
How user access changes based on the authorization scope

When an administrator adds a user to a group that has different access policy settings, the user is mapped to more than one authorization scopes and access policies.

In this case, the ADM grants the user access to applications depending on the specific authorization scope.

Consider a user who is assigned to a group that has two policies Policy-1 and Policy-2.

- **Policy-1** – View only permission to applications.
- **Policy-2** – View and Edit permission to applications.



The user can view the applications specified in Policy-1. Also, this user can view and edit the applications specified in Policy-2. The edit access to Group-1 applications are restricted as it is not under Group-1 authorization scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mapping of RBAC when upgrading NetScaler ADM from 12.0 to later releases

When you upgrade NetScaler ADM from 12.0 to 13.1, you do not see the options to provide "read-write" or "read" permissions while creating groups. These permissions have been replaced by "roles and access policies," which give you more flexibility to provide role-based permissions to the users. The following table shows how the permissions in release 12.0 are mapped to release 13.1:

12.0	ALLOW APPLICATIONS ONLY	13.1
admin read-write	False	`admin`
admin read-write	True	`appAdmin`
admin read-only	False	`readonly`
admin read-only	True	`appReadonly`

Configure roles

In NetScaler® Application Delivery Management (ADM), each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add NetScaler instances in NetScaler ADM, and the other policy might grant permission to create and deploy StyleBooks and to configure NetScaler instances.

When multiple policies define edit and read-only permissions for a single feature, the edit permissions have priority.

NetScaler ADM provides four predefined roles:

- **admin**. Has access to all NetScaler ADM features. (This role is bound to adminpolicy.)
- **readonly**. Has read-only access. (This role is bound to readonlypolicy.)
- **appAdmin**. Has administrative access to only the application features in NetScaler ADM. (This role is bound to appAdminPolicy).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **appReadonly**. Has read-only access to the application features. (This role is bound to appReadOnlyPolicy.)

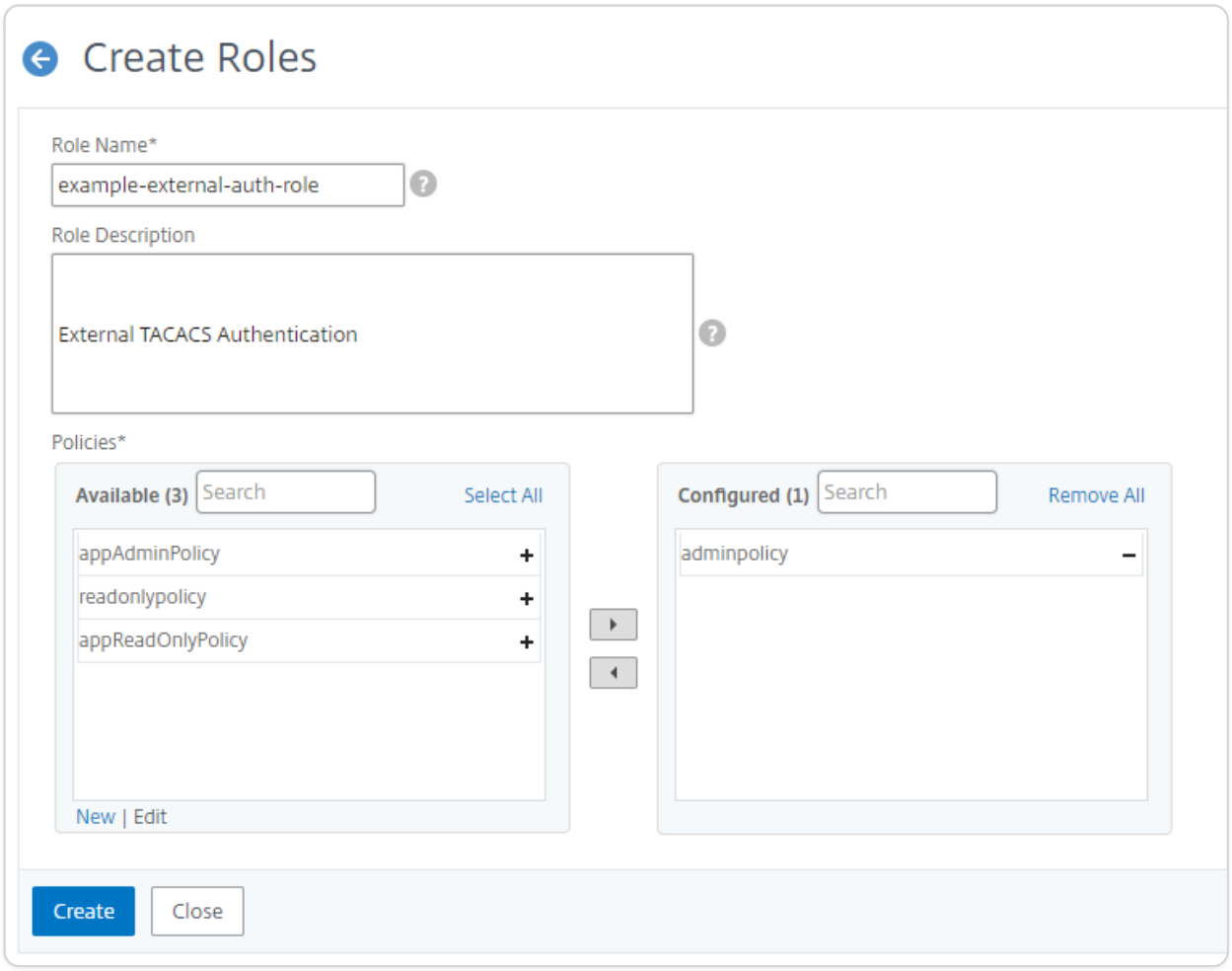
NOTE:

The predefined roles cannot be edited.

You can also create your own (user-defined) roles.

To create roles and assign policies to them:

1. In NetScaler ADM, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. In the **Role Name** field, enter the name of the role, and provide the description in the **Role Description** field (optional.)
4. In the **Policies** section, add or move one or more policies to the **Configured** list.



5. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure users

By default, NetScaler® Application Delivery Management (ADM) has one user:

nsroot - The root user (nsroot) has full administrative privileges on the appliance. The nsroot user is the super admin of NetScaler ADM.

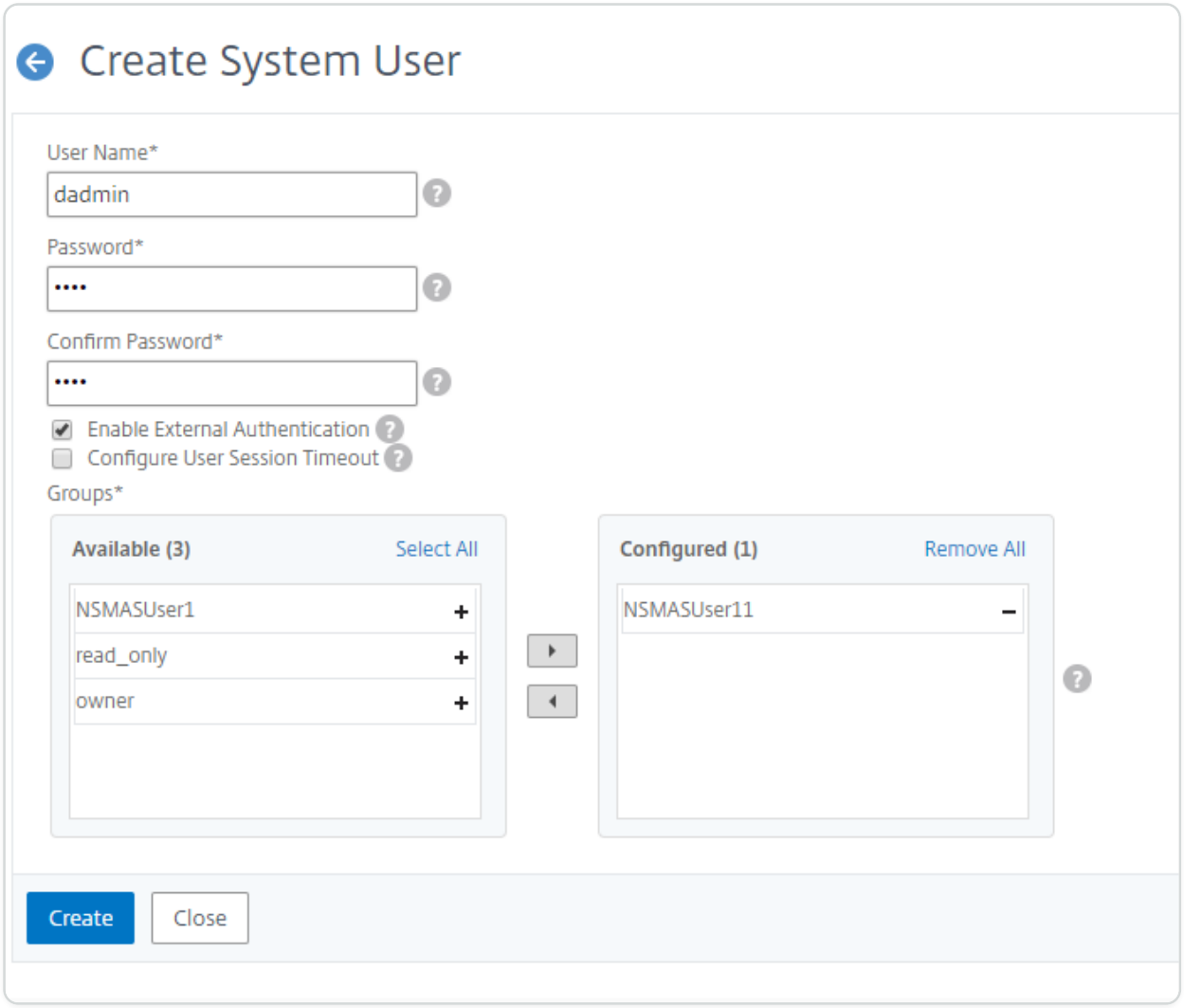
You can create additional users by configuring accounts for them. When you add new users to NetScaler ADM, you can define their permissions by assigning the appropriate groups, roles, and policies.

You can assign a user to a group and bind the group to roles. You can define one-to-one, one-to-many, or many-to-many relationship between users, groups, roles, and access policies. A user can be assigned to multiple groups. A group can have multiple roles, and multiple groups can have identical roles.

To configure users in NetScaler ADM:

1. In NetScaler ADM, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. Enter the following details:
   a. **User Name**. Name of the user
   b. **Password**. Password with which the user logs on to NetScaler ADM
4. Optionally, select **Enable External Authentication**, so that the user can be authenticated through an external authentication server.
5. If you have created groups and want to assign the user to a group, in the **Groups** section, move one or more groups from the **Available** list to the **Configured** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

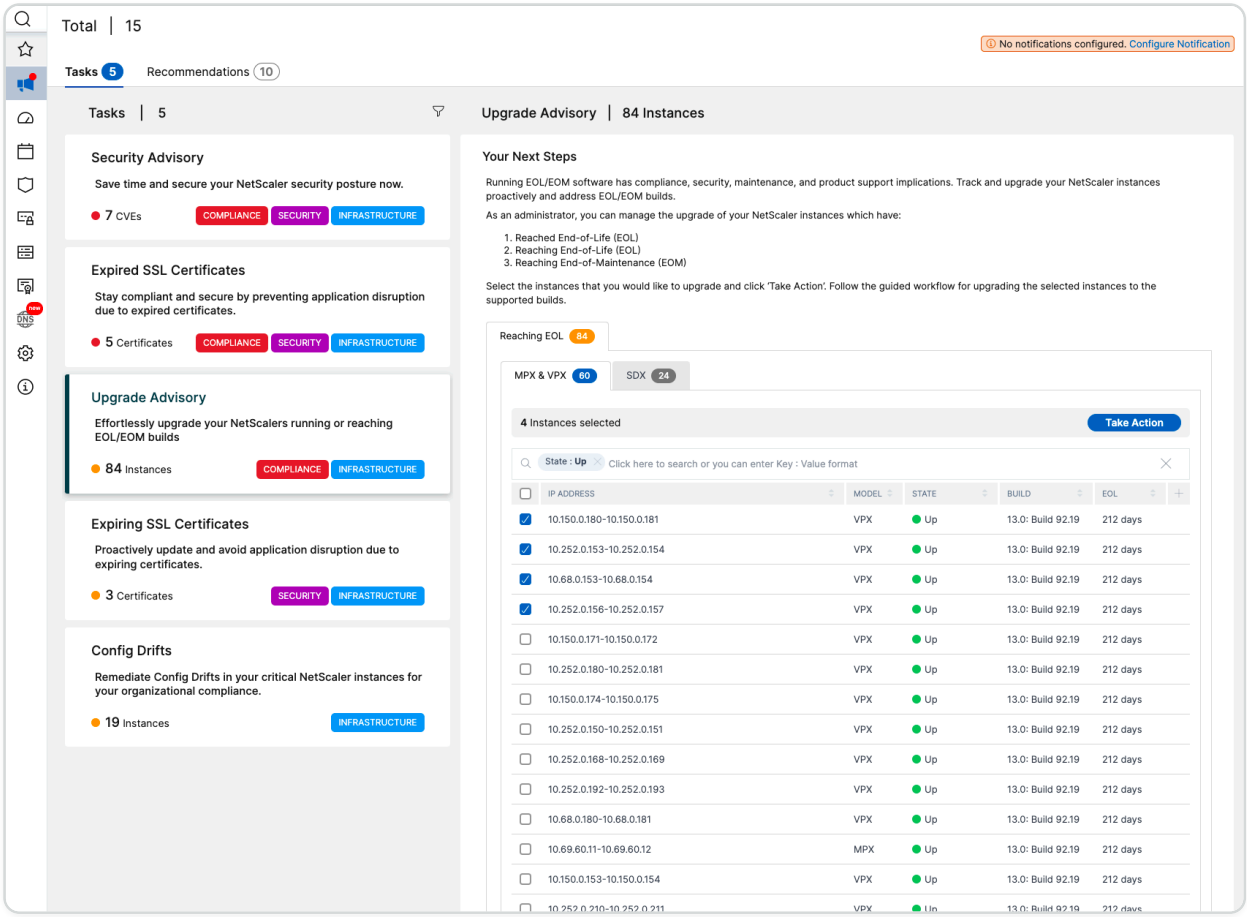
View recommendations and manage your ADCs and applications efficiently

You might have hundreds of discovered NetScaler instances and configured multiple virtual servers (applications) from each ADC instance. As an administrator, you must ensure that all the NetScaler instances and your applications are efficiently managed to get insights for better prioritizing and troubleshooting.

As you scale-up your infrastructure more, you might also need to focus on instances and apps that need immediate attention. The Tasks feature in NetScaler® ADM provides recommendations based on the subscription and current utilization that:

- Help the admins to know how NetScaler ADM can provide an efficient deployment, by using the actionable Guide me workflows.
- Reduce the crucial time and effort of admins by either completing the tasks or acknowledging them to complete later.
- Ensure the admins are making use of all the capabilities of NetScaler ADM, enable product discovery and functionalities recommended by the product for efficient administration of the deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In the **Set-up tasks** page, you can view the following tabs:

- **To Do** – Enables you to view a list of recommendations. You can review and click **Guide Me** to complete the task or click **Acknowledge** to skip this task.
- **Archive** – Enables you to view the list of all completed or acknowledged tasks. You can also use the Guide Me option to complete the recurring requirements.

The following table describes the tasks or recommendations that you can view in the NetScaler ADM GUI:

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
Add an ADC	After you onboard to NetScaler ADM and if no ADC instance is discovered.
Application Analytics is crucial! Enable it on your licensed Virtual Servers and triage application issues faster	If you have multiple licensed virtual servers but are not enabled with analytics.
Want to reallocate bandwidth on your ADC? It's simple!	If the pooled licenses are allocated in the ADC GUI and those ADC instances are discovered

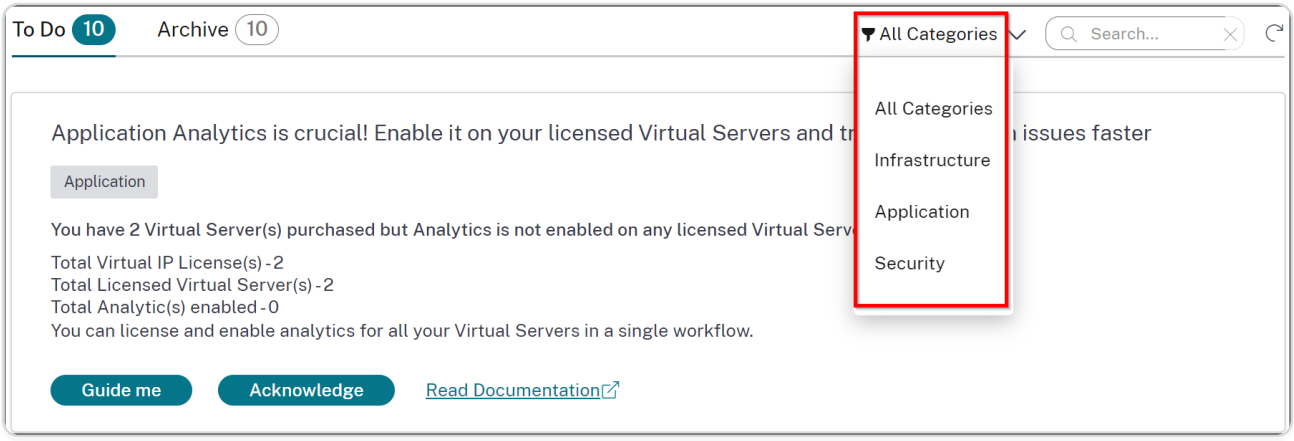
© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
	in NetScaler ADM, you can make the reallocation using NetScaler ADM.
Get more value from your Virtual IP entitlement! Enable more Virtual IP licenses on your remaining discovered Virtual Servers	If you have the required licenses, but not licensed to all the virtual servers.
Enable Granular Role based access for your key enterprise users	If role-based access control (RBAC) is not yet configured in NetScaler ADM.
Configure rules and never miss any critical events on your ADC instances	If a custom event rule is not configured yet.
Need to monitor multiple applications and their performance? Just create a Custom Application	If the custom app is not configured yet.
Avoid application outages and never miss expiring SSL certificates in an application	If no alerts or notifications configured for the expiring SSL certificates
Security Advisory - Keep your ADCs up-to-date with CVEs and mitigations	If the ADC instances have any CVE impact.
Configure an enterprise policy and monitor for any deviations	If the SSL enterprise settings are not changed or still in default.
Repeating tasks manually? Create Configuration Jobs and apply them to multiple ADCs	If **Config Job** task is not configured yet.
Manage and monitor your instance score by selecting custom indicators of your choice	If the default settings and thresholds in **Instance Score Settings** are not modified.
Track your application score by selecting custom indicators of your choice	If the App Score components in the App Dashboard are used in default and no customization is made.
Add private IP blocks to visualize client requests in the Geo Map	If IP blocks are not configured. You can create IP Blocks for mapping and visualizing client requests on a Geo Map based on their private IPs/range.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
Save time! Simplify Application deployment and management with StyleBooks	If default stylebook is not yet configured.
Subscribe and export your AppSec violations to Splunk in realtime	If Splunk integration in NetScaler ADM is not yet configured.
Customize the default threshold or create a new threshold for your Kubernetes services	If only default thresholds are used in service graph and no single or double threshold is applied to the services.
Proactively configure notification profiles and get notifications in your communication destinations	If a notification profile is not yet configured.
Schedule recurring exports and get notifications on the infrastructure details	If no export schedules configured yet in **Infrastructure > Instances**.
Having ServiceNow and looking to integrate with ADM?	If ServiceNow integration in NetScaler ADM is not yet configured.

By default, you can view the top 5 recommendations. Click **Show All** to view all recommendations. You can use the category list and select a category to filter specific recommendations based on the selection.

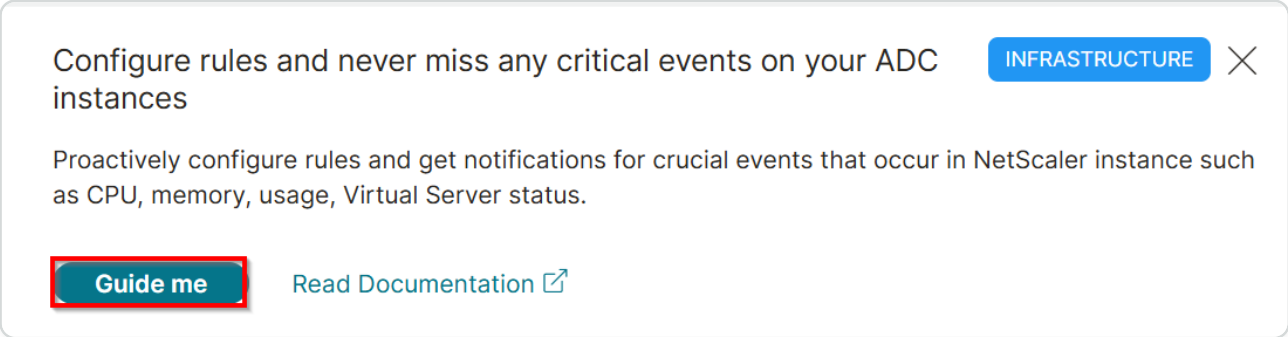


Alternatively, you can also use the Search bar, type in the first few characters to drill down to the task.

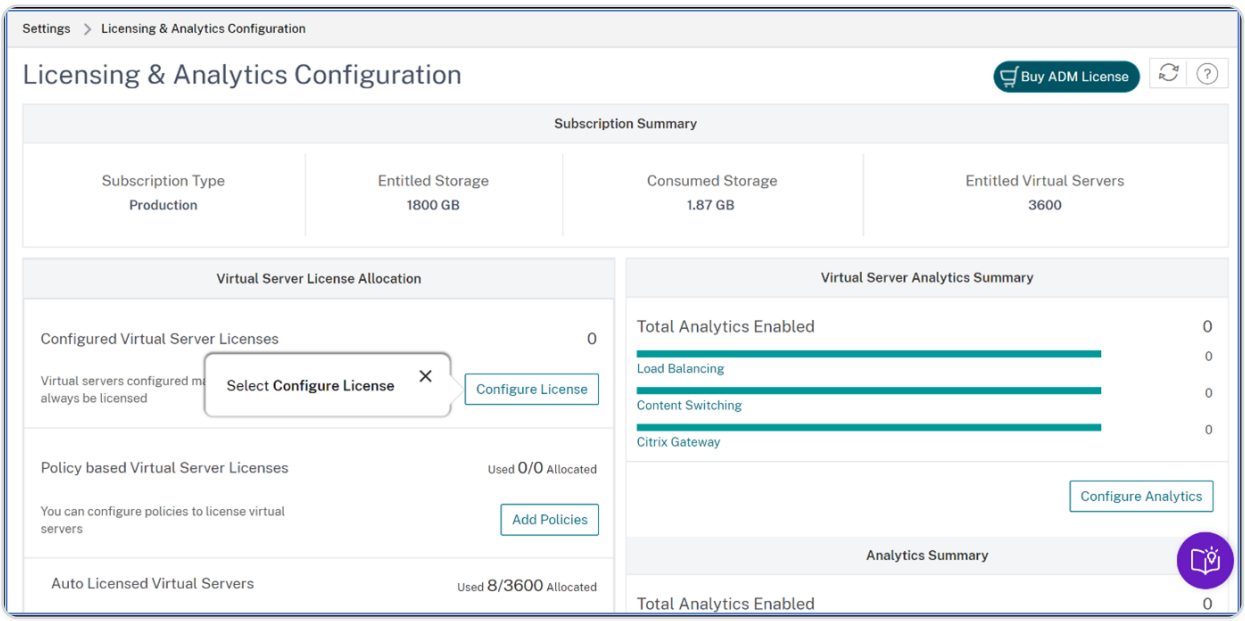
© 1997–2026 Citrix Systems, Inc. All rights reserved.

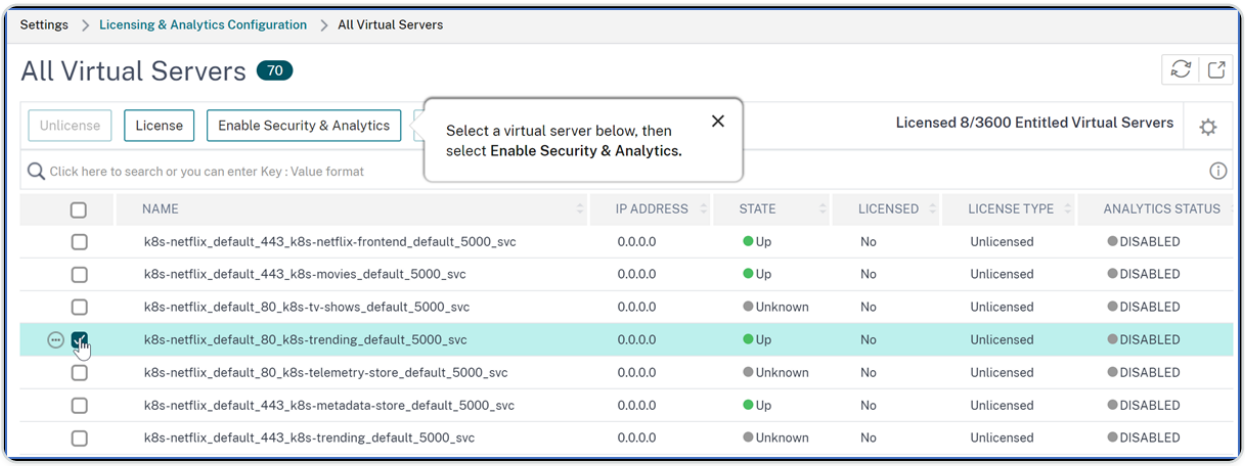
How to use the Guide me workflow and complete the task?

Consider that you want to enable analytics for all the licensed virtual servers. Click **Guide me** for the following task:

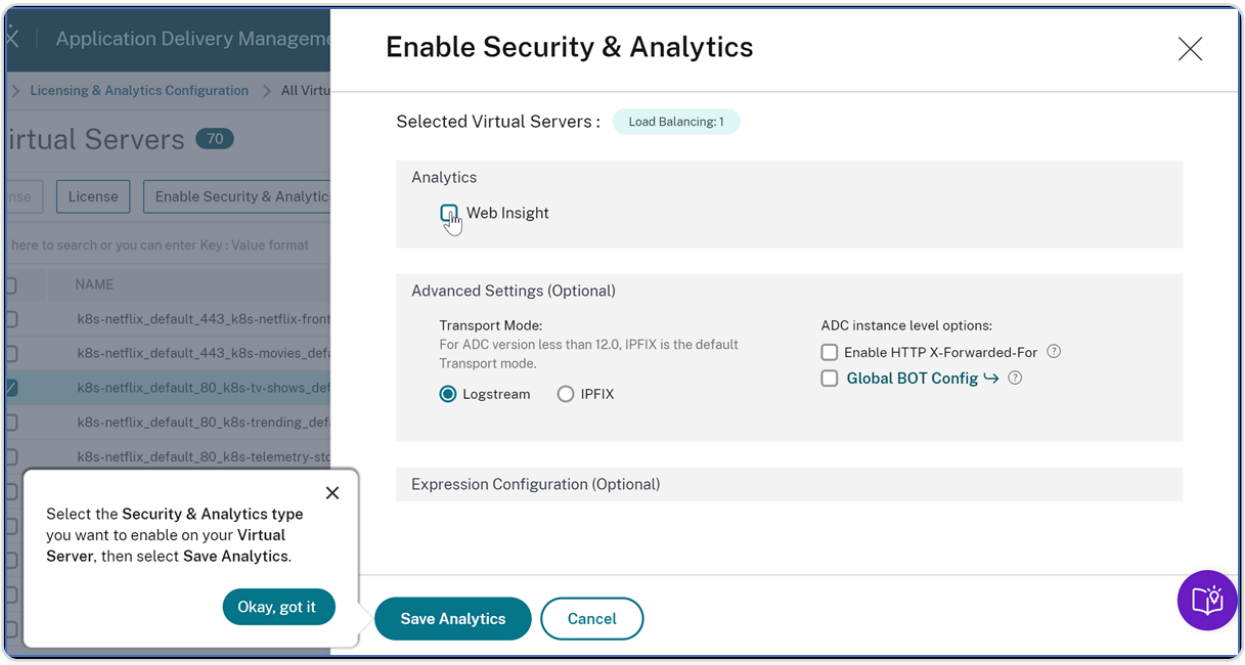


The workflow provides the required suggestions to complete the task. In this example, after you click **Guide me**, follow the tool-tip suggestions provided:

1. 

2. 

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 

After you select the analytics type and click **Save Analytics**, the task is complete. This task gets moved to the **Archived** tab.

Similarly, you can also use the same workflow for the recurring requirements in the **Archive** tab.

Under **Popular Features**, you can see the important features of NetScaler ADM and it enables you to explore these features by clicking a feature.

FAQs

1. **Guide me** does not show tool-tip and only does redirection of UI? What should I do to fix this?

   This issue can happen if your firewall is blocking Pendo FQDN. Refer to Enable Pendo for your enterprise and ensure that the FQDN is allowed in the firewall. Allowing Pendo FQDN enables the **Guide me** to show tool tips. You can experience the **Guide me** workflow at its best only when Pendo is available.

2. Why type of tasks is present for the administrators?

   Currently, the recommendations are specific to deployments that help the admins more on configurations and setup tasks for making the deployment efficient. It also enables better product discovery and admins can know what a task does and how it can help without any prior knowledge or knowing if the feature exists in ADM or not.

3. Can I bring back a task from **Archive** to **To Do** ?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Any task in archive goes back to **To Do** only based on specific conditions. For example, if the event rules are all removed or all ADCs are removed, an archived task moves to To-Do tasks for the admins again, to get their attention.

4. Does the progress bar complete if I acknowledge?

   Yes! But it is recommended to complete these tasks. However, if you want to do it later, you can acknowledge that you are aware of the product recommendation and go back to Archive to complete it later.

5. Does the task go to Archive if I start a guide me and leave it in the middle?

   No, the task continues to be available in To Do unless the action is saved or completed.

6. Can I perform search or filtering?

   Yes! You can use the search bar or narrow down to specific tasks by selecting the category from the list.

7. Will I get tasks to take actions on dynamic events like ADC memory spike, App down, LB virtual server down, and so on?

   All these are part of enhancements and are planned to be available in the upcoming releases.

8. Will this be available for on-premises ADM?

   This feature is currently available only in ADM service.

9. Will all my 20+ tasks show up even if I do not have an ADC added in NetScaler ADM?

   No. You must have both ADC instance and virtual servers available in NetScaler ADM to show all these tasks.

10. How often will the tasks refresh?

    ```
    When you click **Tasks** from the left navigation pane, they are
    refreshed and available at the latest status. The details for each task
    are fetched and updated. The tasks are automatically refreshed every 24
    hours. For better administrative control, you can also do a manual
    refresh of tasks to get the latest status.
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications

The application analytics and management feature of NetScaler® ADM enables you to monitor the applications through application-centric approach. This approach helps you to:

- Check the score and analyze the overall performance of the applications
- Check for any issues that persist with server or client
- Detect anomalies in the application traffic flows and take corrective actions

> **NOTE**
>
> Applications refer to one or more virtual servers that are configured on the instances (NetScaler).

You can monitor the applications for the time duration such as 1 hour, 1 day, 1 week, and 1 month.

Prerequisites

- Ensure you have added NetScaler instances in NetScaler ADM
- Ensure you have valid license for your NetScaler instances. For more information, see Licensing
- Ensure you have applied license for virtual servers. For more information, see Manage licensing on virtual servers

Application overview

Applications can be:

- Discrete applications
- Custom applications
- Microservices applications (k8s_discrete)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Discrete applications

All virtual servers that are licensed are referred to as discrete applications.

Custom applications

The virtual servers under one category are referred to as custom applications. As an administrator, you must add custom applications based on a category. You can then manage and monitor the applications through the dashboard. You get an ease of monitoring specific applications that are grouped under one category.

For example, you can create a category for your data center1 and add its ADC instances. After you define a category and add the instance for your data center1, the application dashboard is displayed with a separate category, comprising all the applications related to your data center1.

Points to note

- The discrete applications that are added to the custom applications are removed from the discrete applications.
- All applications that are not added to any category are available as **"others"**.
- By default, NetScaler ADM enables you to add licenses for up to 2 applications. Depending upon your license, you can select and apply licenses for the applications that you want to monitor.

Microservices applications

In a Kubernetes cluster, NetScaler provides an Ingress Controller for NetScaler MPX (hardware), NetScaler VPX (virtualized), and NetScaler CPX (containerized). For more information, see NetScaler Ingress Controller.

The discrete applications that are configured using the NetScaler CPX instances are referred to as microservices applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application management and application dashboard

NetScaler® ADM enables you to manage applications from **Applications** page and view application details from **Dashboard** page.

Manage applications

From the application dashboard, click **Manage Apps** to view all custom and discrete applications.

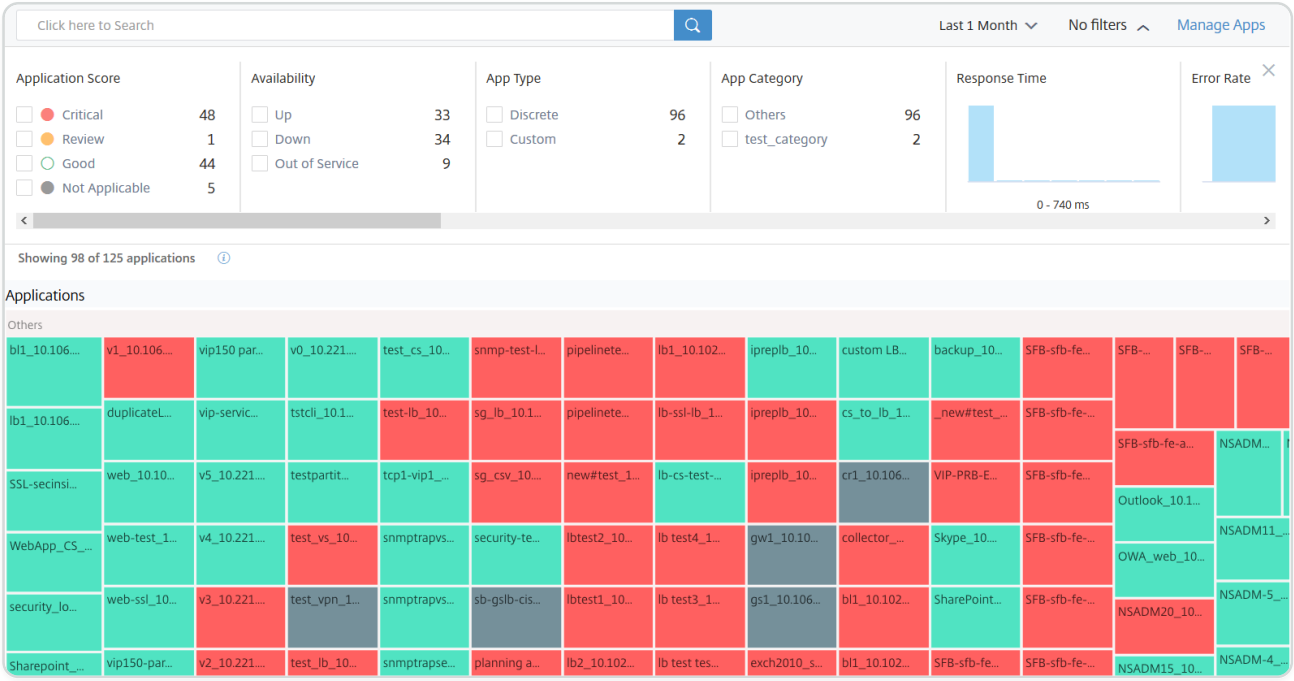
From the **Manage Applications** page, as an administrator, you can:

- Add applications
- View application details such as app name, app type, app category, associated virtual servers, associated services, and so on.
- Edit or delete custom applications

For more information, see Manage applications.

Application dashboard

Navigate to **Applications** > **Dashboard** to view the list of applications either in tabular view or in graph view.



All applications get displayed in the dashboard only after the applications start to populate data. From the dashboard, click an application to view detailed information of the application performance. For more information, see Application details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the application analytics is not displayed even after approximately 10–15 minutes duration, perform the troubleshooting steps at Troubleshoot App Dashboard.

Updates in the new dashboard behavior compared to the earlier dashboard

- After you add or edit a custom application, it may take a few minutes to reflect the application in the dashboard.
- If you delete a custom application, the dashboard still displays the deleted application, until ADM has its analytics data (maximum of 1-month duration).

  Consider a scenario that you have created an application on Jan 2, 2020 and you have deleted the application on Jan 4, 2020. In this scenario:

  - The dashboard can still display the deleted application on Jan 4, 2020, when you select the time duration for the last 1-day, 1-week and 1-month.
  - The dashboard can still display the deleted application on Jan 5, 2020, when you select the time duration for the last 1-week and 1-month.
  - When the duration exceeds the app deletion date, the application is not displayed in the dashboard. That is, the dashboard is not displayed with the deleted application on Jan 6, 2020 (for the last 1 day), Jan 12, 2020 (for the last 1-week), and after February 5, 2020 (for the last 1-month).

    NOTE

    After you add an application, if the associated NetScaler instance is Down, out of service, or not reachable because of a temporary network glitch:

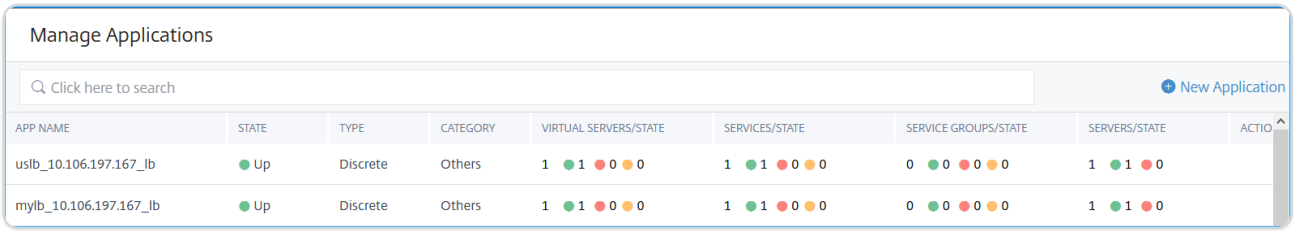
    -The applications associated with the ADC instance are only visible in **Applications** page, but not in the dashboard.
    -The applications are displayed in the dashboard after the ADC instance is up and running.

Manage applications

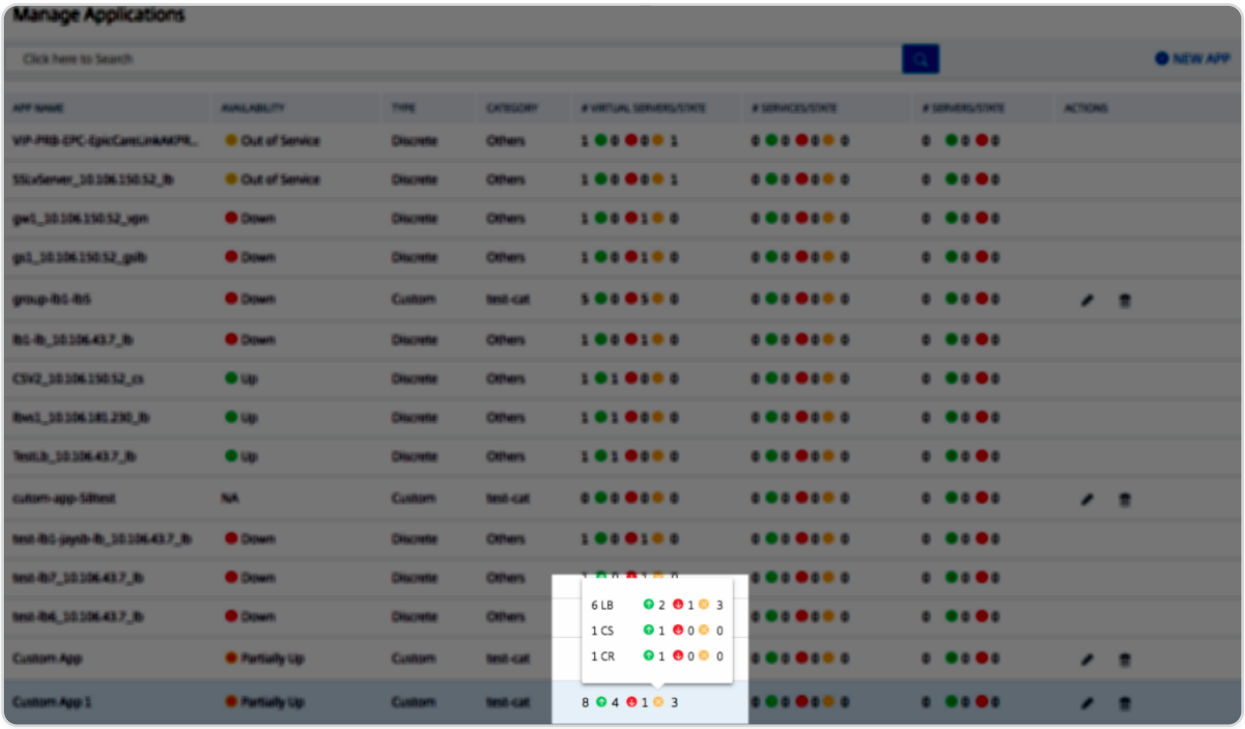
From the dashboard, click **Manage Apps** to view application details and add, edit, or delete custom applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View application details



- **App name** – Denotes the application name
- **Availability** – Denotes the current availability of the application, such as **Up**, **Down**, **Partially Up**, **Out of Service**, and **NA**
  - **Up** – All virtual servers associated with the application are Up.
  - **Down** – All virtual servers associated with the application are Down
  - **Partially Up** – Either one virtual associated with the application is Down or out of service
  - **Out of Service** – All virtual servers associated with the applications are out of service
  - **NA** – No virtual servers is configured for the application
- **Type** – Denotes if the application belongs to Custom or Discrete
- **Category** – Denotes the application category that is grouped
- **Virtual server/state** – Denotes the total virtual servers configured and current status of all virtual servers. Hover the mouse pointer to see the details such as total virtual servers, virtual server type, and virtual server status



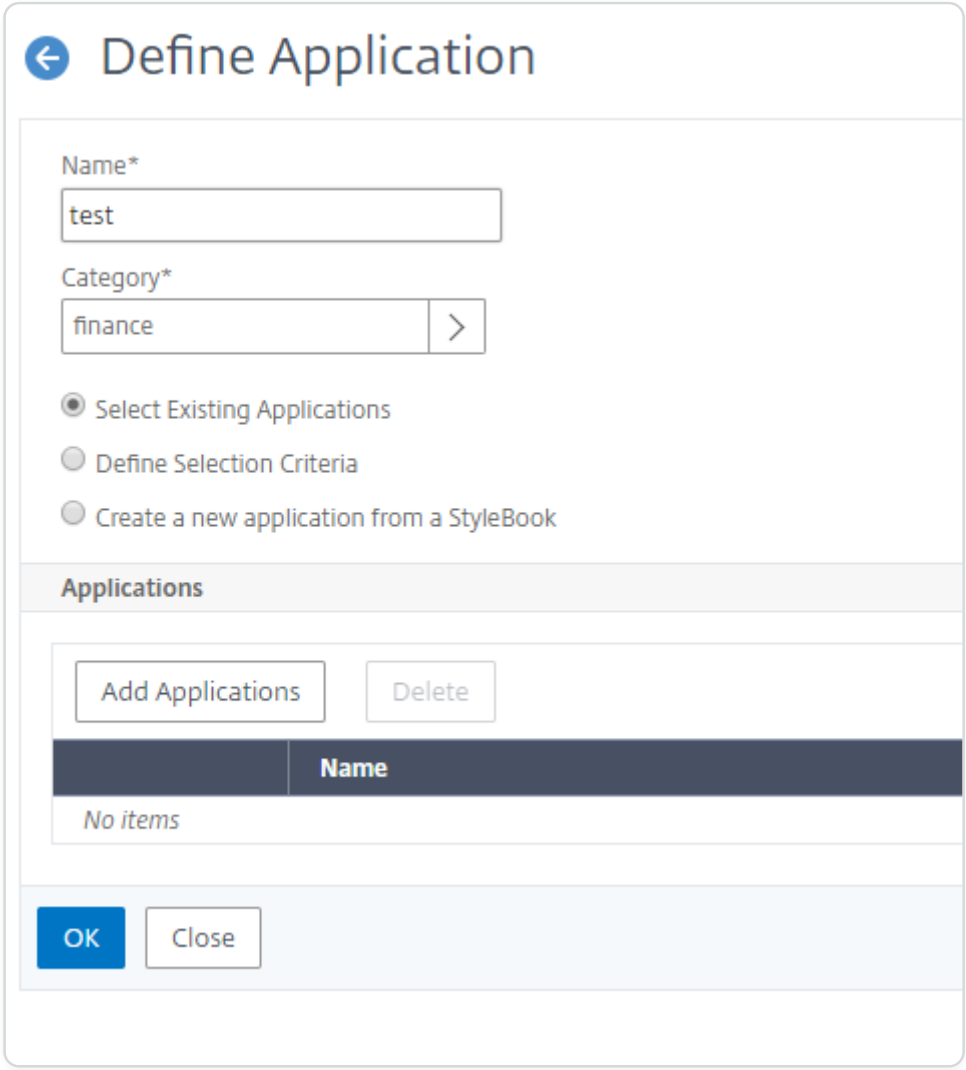
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Services/state** – Denotes the total services configured and current status of all services
- **Service Goups/state** – Denotes the total service groups configured and status of all service groups
- **Servers/state** – Denotes the total servers configured for the application and the current status of all servers
- **Actions** – Enables you to either edit or delete the custom applications

Add an application

1. Click **New Application** to create a new application

   The **Define Application** page is displayed



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can also click **Applications** and then select **New Application** to add a new application

2. Set the following parameters:

FIELD	DESCRIPTION
Name	Name of the custom application. For example, LB_TEST.
Category	The category that you can group the applications. Click to get the Application Category page. Select the category and click **Select**. To add a category:
	1. Click **Add**
	2. Enter a name of your choice.
	3. Click **Create**
Select Existing Applications	Enables you to select the existing applications added to the NetScaler instances.
Add Application	Displays all the virtual servers that are configured on the instances. Select the applications from the list and click **OK**.
Define Selection Criteria	Option to define application by virtual server range, or by origin server/service IP address range.
	- **Server.** Specify the server or service IP address, server name, or the port of the back-end 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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION
	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 back-end 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.
Create a new application from a StyleBook	Enables you to create an application using the StyleBook. For more information, see Create an application using the StyleBook.

3. Click **OK**.

NOTE:

Currently, Application Dashboard supports only load balancing and content switching virtual servers.

The application dashboard is now displayed with the category and all the applications are grouped underneath.

If you select **Create a new application from a StyleBook** option for the custom application, you must allow NetScaler® ADM to auto-select the virtual servers for licensing. To enable auto-selection for the virtual servers:

a. Navigate to **Settings** > **Licensing & Analytics Configuration**.
b. Under **Virtual Server License Allocation**, click **Auto-select Virtual Servers** and **Auto-select non addressable Virtual Servers** to enable.

Create an application using the StyleBook

To create an application using the StyleBook:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler ADM, navigate to **Applications** > **Dashboard** and click **Define Custom App** to create a custom application.
2. In the **Define Application** page, type the name of the application in the **Name** field.
3. Select the application category from the Category section. NetScaler ADM allows you to define categories to group the user-defined applications. You can also add more categories if necessary.
4. Click to select **Create a new application from a StyleBook** and click **OK**.

   The Choose StyleBook page is displayed. This page contains all the default StyleBooks available in NetScaler ADM.
5. Select the StyleBook. The **Configuration Details** page is displayed.
6. 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, see Use Default StyleBooks.
7. Click **Create**.

   You can also click **Dry Run** to check the configurations that NetScaler ADM attempts to create on the selected NetScaler instance. This option is just for your test purpose to see the final check on the configurations. Even if Dry Run option is successful, the actual configuration on the selected NetScaler might still fail due to various reasons (IP conflict, instance not reachable, and so on.)

Edit or delete an application

From the **Applications** page, you can either edit or delete the custom applications. Click the edit button to edit an application and click the delete button to remove the application.

Export reports of app dashboard and security dashboard

NetScaler ADM allows you to take a snapshot of the current App Dashboard 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, .jpeg, or .pdf reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Unlike other report export options in NetScaler ADM, you can export the App Dashboard and Security Dashboard reports only as .pdf or .png files. The .csv format is not supported currently.

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.

View applications

By default, the application dashboard displays all applications. Depending upon your requirement, you can use the filter option to view applications.

Showing 98 of 125 applications

APP NAME	APP SCORE	AVAILABILITY	APP TYPE	APP CATEG...	TOP ISSUE	TOP ISSUE CATEGORY	ISSUE COU...	RESPONSE ...	ERROR PER...	TOTAL REQ...	THROUGHP...	DATA VOLU
web_10.107.98.70_lb	85 Good	Up	Discrete	Others	Active Services Last Monday at 1:00 AM	Performance	1	0	0%	0	0	0 Bytes
web-test_10.107.98.70_lb	85 Good	Up	Discrete	Others	Active Services Last Monday at 1:00 AM	Performance	1	0	0%	0	0	0 Bytes
web-ssl_10.107.98.70_lb	85 Good	Up	Discrete	Others	Active Services Last Monday at 1:00 AM	Performance	1	0	0%	0	0	0 Bytes

The dashboard displays the following application details:

- **App name** – Denotes the application name
- **App Score** – Denotes the application score and the status such as **Critical**, **Good**, **Fair**, and **Not Applicable**
- **Availability** – Denotes the current availability of the application, such as **Up**, **Down**, **Partially Up**, **Out of Service**, and **NA**
    - **Up** – All virtual servers associated with the application are Up.
    - **Down** – All virtual servers associated with the application are Down.
    - **Partially Up** – Either one virtual associated with the application is Down or Out of Service.
    - **Out of Service** – All virtual servers associated with the applications are out of service.
    - **NA** – No virtual servers is configured for the application.
- **Top issue** – Denotes the issue that has the maximum error counts on the application
- **Top issue category** – Denotes the category of the issue
- **Issue count** – Denotes the total issue counts for the application
- **Response time** – Denotes the average response time to respond from the application

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Error percentage** – Denotes the total error percentage of 5xx errors for the application

> **NOTE**
>
> The 5xx error percentage metric is displayed only for **NetScaler 13.0 or later**. For earlier versions, the value is displayed as **0**.

- **Total requests** – Denotes the total requests received by the application
- **Throughput** – Denotes the total network throughput for the application. Throughput is calculated by the Req Bytes / Sec + Res Bytes / Sec for the virtual servers
- **Data volume** – Denotes the total data processed by the application
- **Client connections** – Denotes the average client connections established by the application
- **Server connections** – Denotes the average server connections established by the application

Configure and associate an application to multiple custom applications

In **Application Dashboard**, you can configure an application and associate it to multiple custom applications. Using this feature, you can reuse the same application for multiple custom applications, rather than creating a separate application for each custom app.

Consider that you manage two e-commerce portals with the names **ComABC** and **ComCDE** respectively, and you wanted to use a payment gateway server with the name **PaymentApp** for both portals. In this scenario, you must:

- Create two custom apps with the name **ComABC** and **ComCDE**.
- Create an application with the name **PaymentApp** and associate it to **ComABC** and **ComCDE**.

To implement this scenario, you must:

- Create the **Custom Apps (ComABC and ComCDE)**:

  a. Navigate to **Applications > Dashboard**, and click **Manage Apps**.

  b. Click **New Application**.

  c. Specify a name and category.

  d. Select the type for choosing the application. In this example, **Select Existing Applications** option is selected. For more information, see Add an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. Under **Applications**, click **Add Applications**.

f. Select the applications from the list and click **OK** to create the custom app.

- Create the **PaymentApp**. For this, you must convert a discrete app to custom app:

  a. Navigate to **Applications > Dashboard**, and click **Manage Apps**.

  b. Click **New Application**.

  c. Specify a name and category.

  d. Select the type for choosing the application. In this example, Select Existing Applications option is selected. For more information, see Add an application.

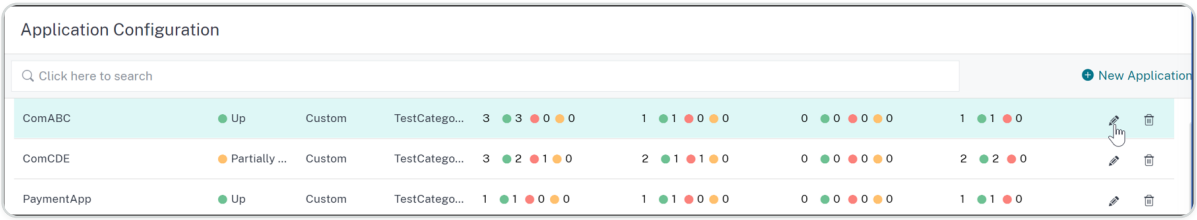
  e. Under **Applications**, click **Add Applications**.

  f. Select the applications from the list and click **OK** to create the custom app.

- Next, you can use the **PaymentApp** and associate to **ComABC** and **ComCDE**.

  a. Navigate to **Applications > Dasboard**, and **click Manage Apps**.

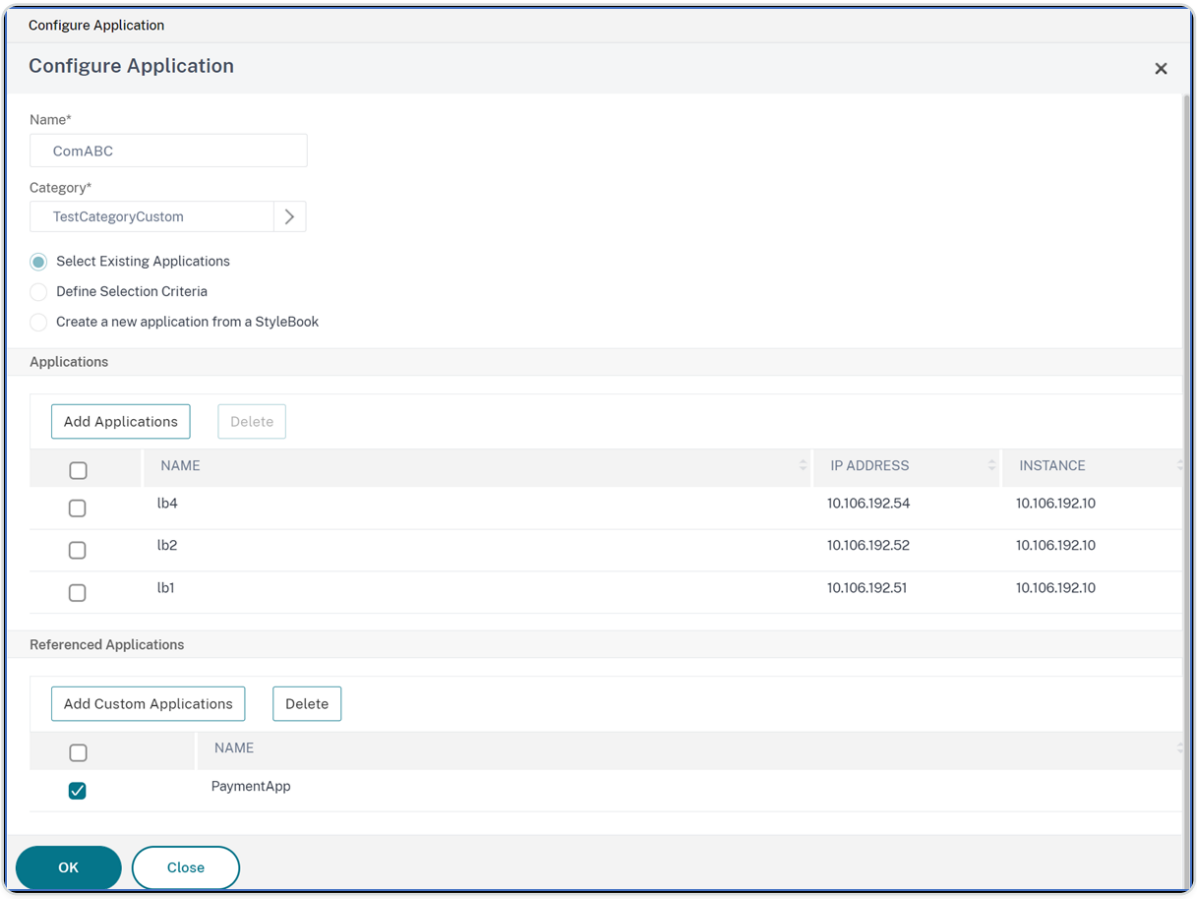
  b. Locate the **ComABC** app and click **Edit**.



  c. Under **Referenced Applications**, click **Add Custom Applications**, and select the **PaymentApp**.

  d. The **PaymentApp** is now available under **Referenced Applications**. Click **OK** to associate the **PaymentApp** to **ComABC** custom app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. Repeat the same procedure for **ComCDE** custom app.

NOTE:

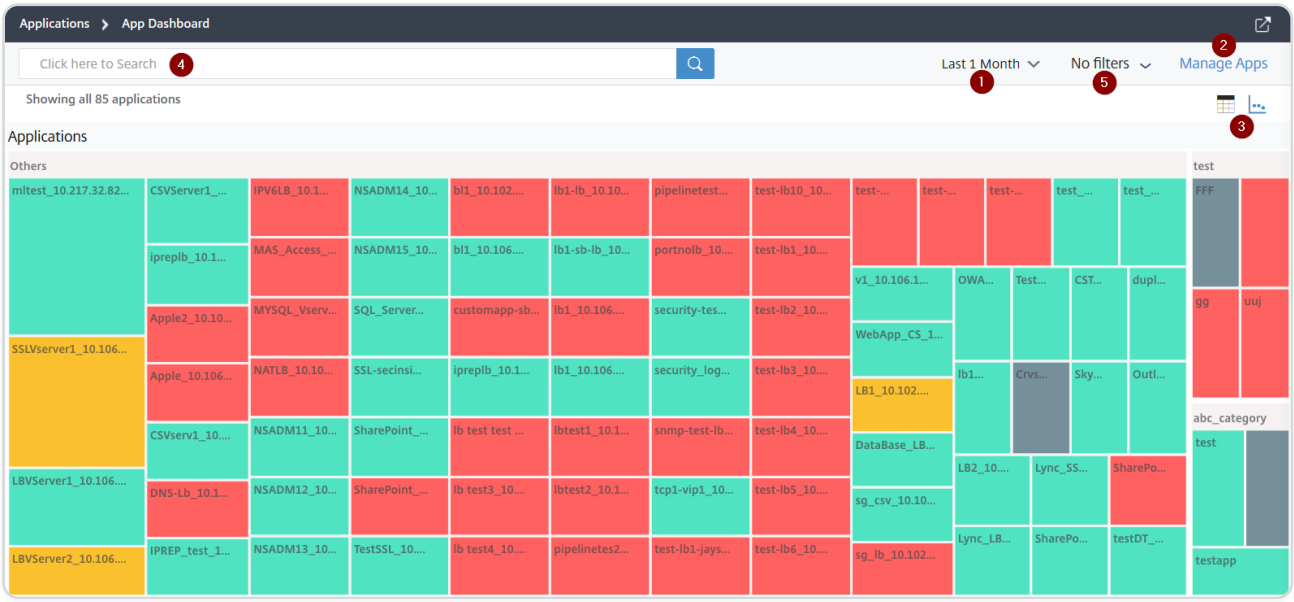
After the application is associated to the custom app, the final app score for the custom app is calculated based on the lowest score between the custom app and the referenced app. In this example, if **ComABC** app score is 85 and **PaymentApp** score is 69, the final score for **ComABC** app becomes 69.

Application dashboard overview

The application dashboard displays the discrete applications under **Others** and the custom applications that are grouped under their respective categories.

Navigate to **Application** > **Dashboard** to view the app dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



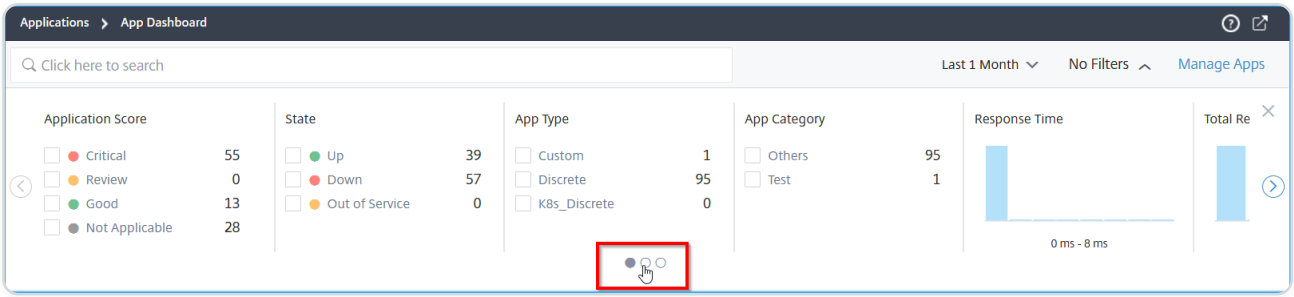
1 – Displays the application details for the selected time duration such as 1 hour, 1 day, 1 week, and 1 month.

2 – Enables you to manage applications and add new applications

3 – Enables you to view applications either in table view or in graph view

4 – Enables you to search an application using the search bar

5 – Enables you to apply filters to view applications. Click to view for details.



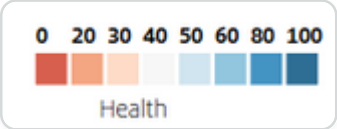
You can select the carousel slider that enables you an ease of access to all options.

You can:

- Select to view applications based on the scores.
  - **Critical** – Application score is between 0 and < 40
  - **Fair** – Application score is between 40 and < 75
  - **Good** – Application score is greater than 75
  - **Not Applicable** – No virtual servers are configured for the application

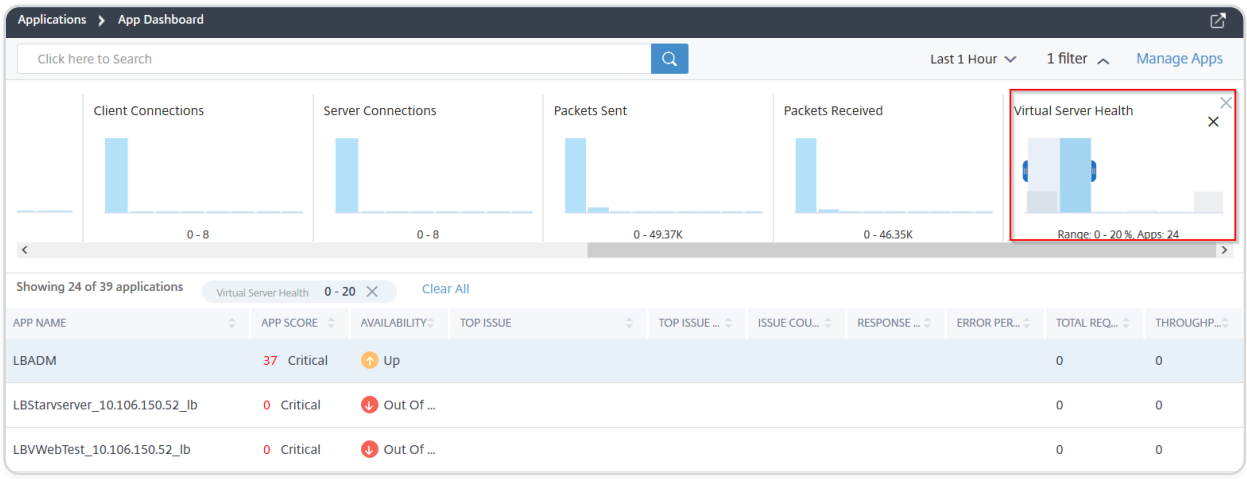
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following table describes the differences between the earlier app score and the present app score.

APPLICATION SCORE (CRITICAL, REVIEW, GOOD, NOT APPLICABLE)	APP SCORE (EARLIER VIEW WITH COLOR LEGENDS)
Score is calculated as **100 minus penalty score of all application current issues**	Score is calculated as **100 – (App server resource + NetScaler system resource)**
Applications are displayed in colors such **Red (critical)**, **Orange (review)**, **Green (good)**, and **Gray (Not Applicable)**	Applications are displayed in color legends. 

- Select to view applications based on the application status such as Up, Down, and Out of Service
- Select to view applications based on the application type such as Discrete or Custom
- Select to view applications based on the categories grouped underneath
- Drag the histogram to apply filters and view applications.

For example, if you want to view applications that have Virtual Server Health between 0 and 20, drag the Virtual Server Health histogram to filter the results.

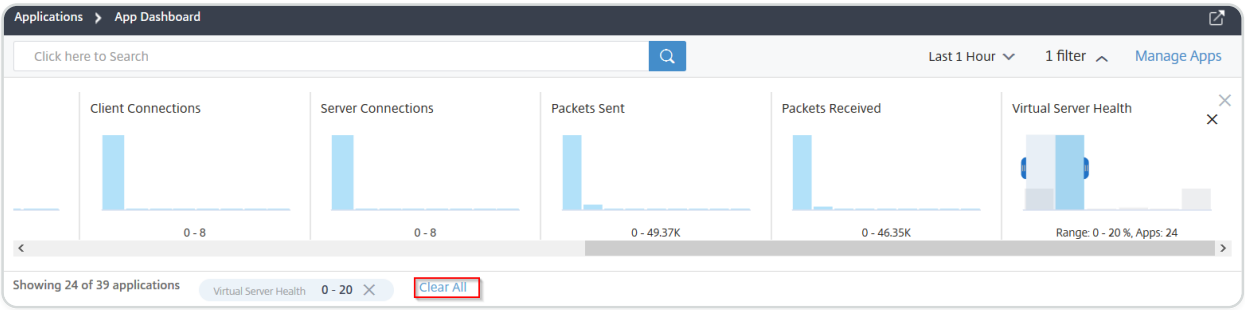


NOTE

You can also click the histogram to get the relevant applications displayed.

Click **Clear All** to clear the applied filter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following are the application summary for which you can apply filters:

- **Response Time** – A histogram that displays the average response time received by the applications
- **Error Rate** – A histogram that displays the average error percentage of 5xx errors for the applications
- **Total Requests** – A histogram that displays the total number of requests received by the applications
- **Throughput** – A histogram that displays the total network throughput processed by the applications
- **Data Volume** – A histogram that displays the total data processed by the applications. Data volume is calculated by the total request bytes and response bytes for the applications.
- **Client Connections** – A histogram that displays the average client connections established by the applications
- **Server Connections** – A histogram that displays the average server connections established by the applications
- **Packets Sent** – A histogram that displays the total packets sent by the applications
- **Packets Received** – A histogram that displays the total packets received by the applications
- **Virtual Server Health** – A histogram that displays the total applications between the score range 0% to 100%. A virtual server health is (%) of active services associated with the application. For example, if a virtual server is configured with 2 services and if one of them is down, the score is 50%.

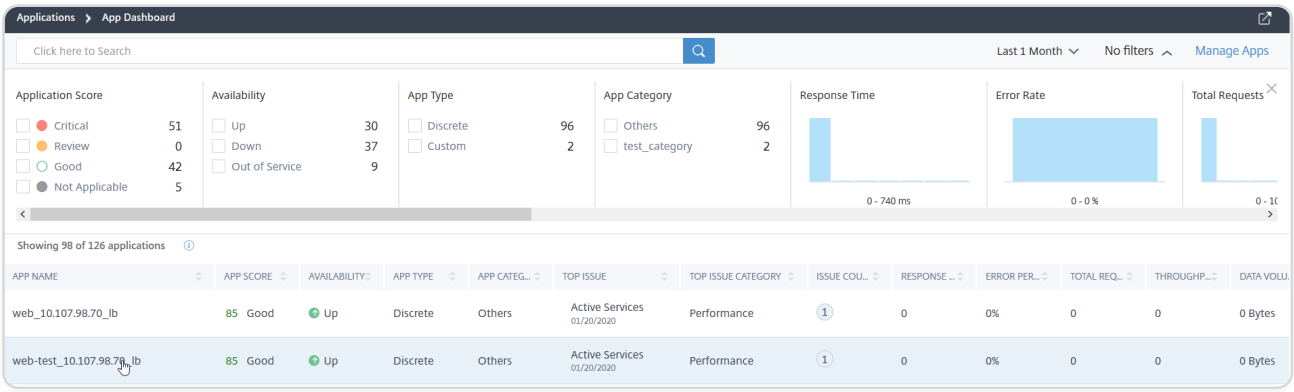
Search and filter results using the search bar

You can place the mouse pointer on the search bar and select the category to refine the search.

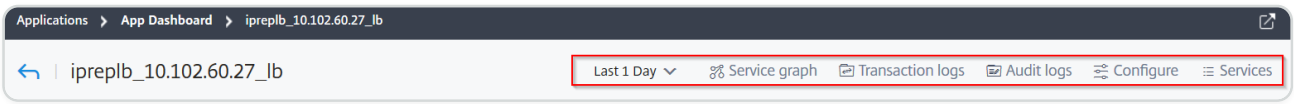
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application details

Click an application from the dashboard to drill down for further detailed information.



The selected application page is displayed.

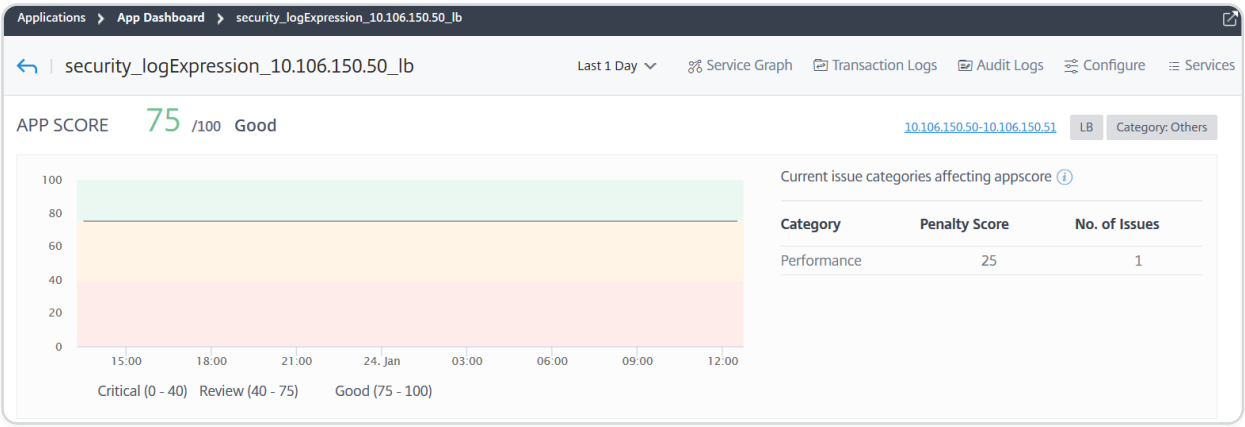


From the application details page:

- Select the time duration from the list to view details for the specific time duration
- Click **Service Graph** to view service graph for the selected application. For more information, see Service Graph for Applications
- Click **Transaction Logs** to view the detailed transactions for 5xx errors
- Click **Audit logs** to view the detailed audit log information
- Click **Configure** to view or edit the service and service group configuration for the application
- Click **Service** to view services that bound to the application

After you select the time duration, the following application details are displayed:

- **App Score** – The application score for the selected time duration. The final score is calculated as **100 minus total penalty**.



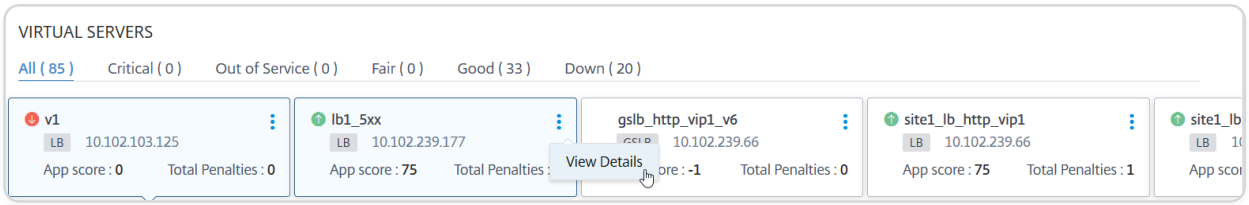
© 1997–2026 Citrix Systems, Inc. All rights reserved.

This dashboard also enables you to view the current issues that are affecting the app score. You can view the issues details under Issues.

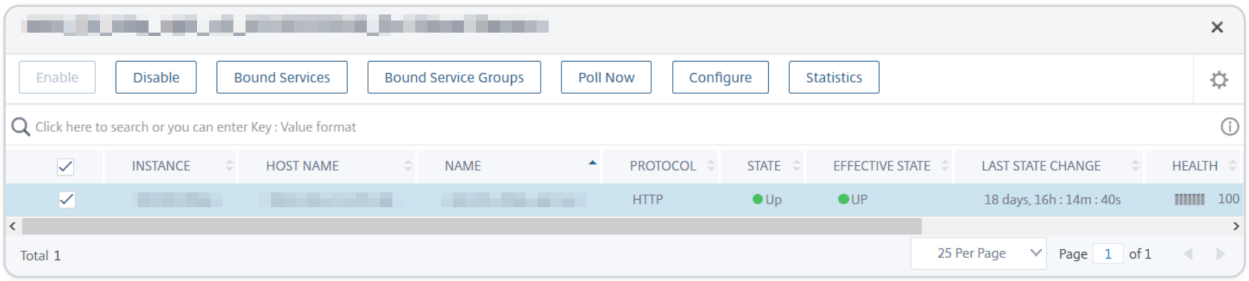
- **Virtual Servers** –

> **NOTE**
>
> The **Virtual Servers** section is displayed only for the custom applications. For discrete applications, click the **IP address** to view the virtual server details.

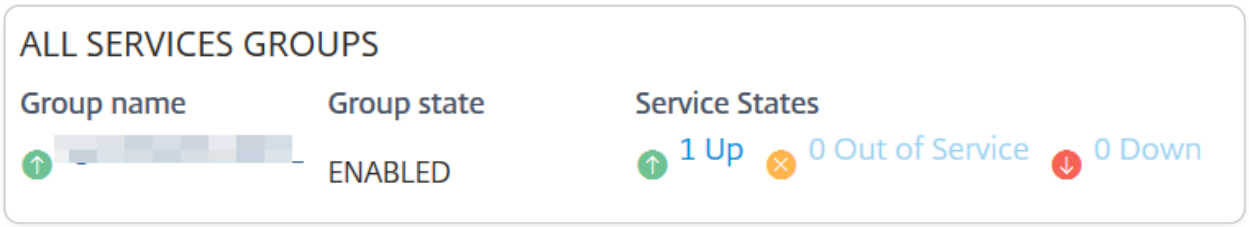
Displays all virtual servers associated with the custom application



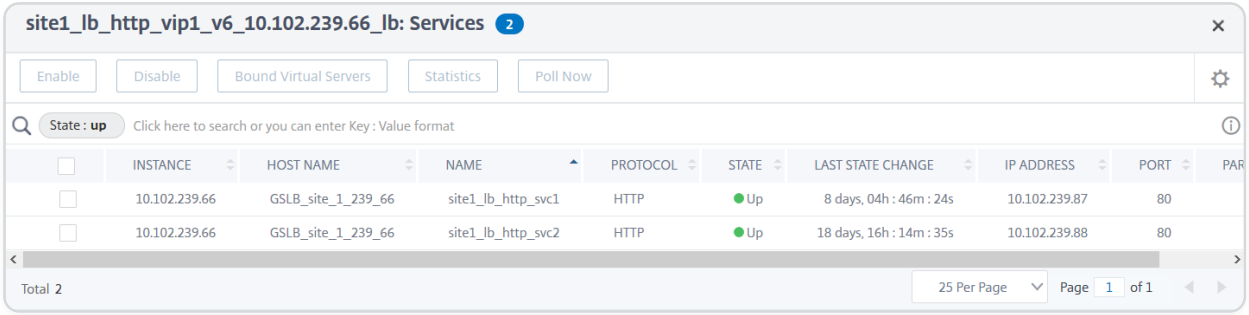
Click **View Details** to view and manage the virtual server settings.



- **All Services** – The services that are bound to the application



Click to view the service details and to manage the service settings



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Issues** – The issues that are applicable for selected application. You can view the following issues along with its category:

PERFORMANCE	INSTANCE HEALTH	CONFIG	SYSTEM RESOURCES
Response Time	Average CPU Usage	Unstable Server	Improper persistence type
Active Services	Memory Usage	Unusually large HTTP packets	NIC Card Saturation
Low Session Reuse		TCP reassemble queue limit hits	
SurgeQueue Buildup			
SSL Real Time Traffic			
Session buildup			
Service flaps			

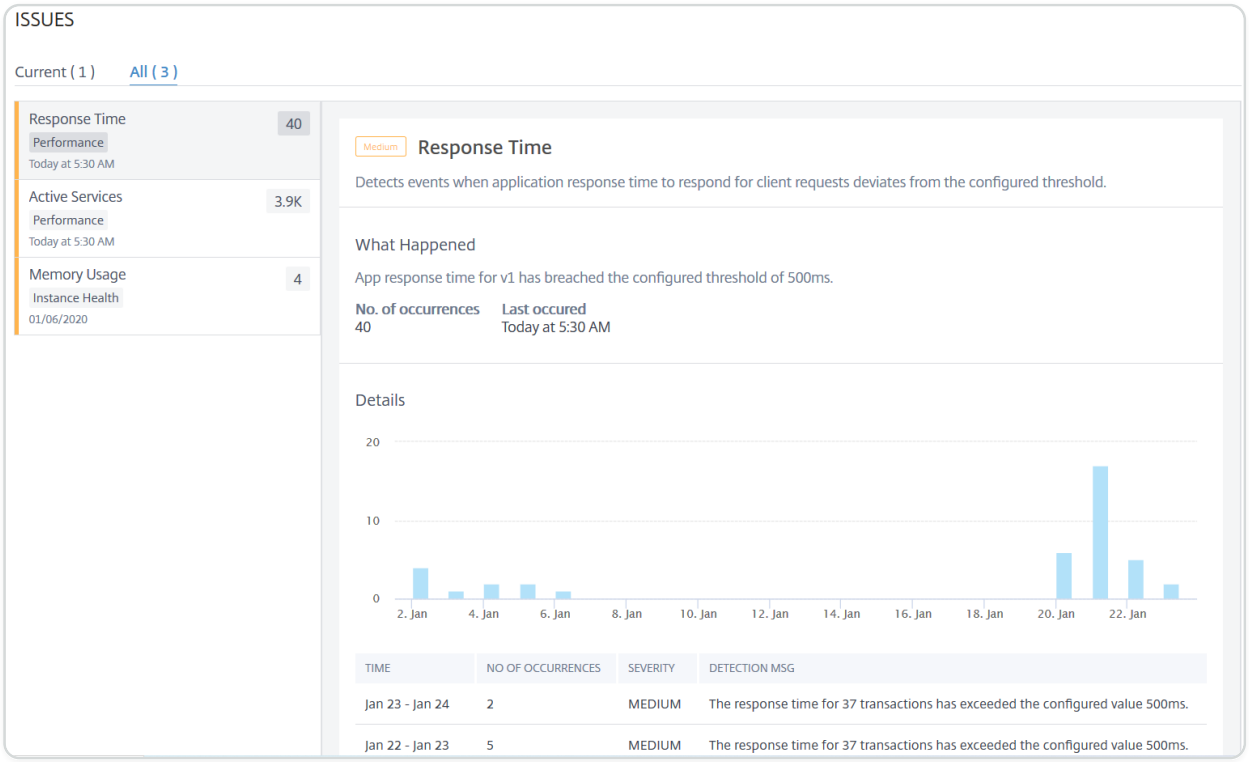
Click each issue to check details such as detection message, when the issue has occurred, Recommended actions, and details.

For more information, see Performance indicators for application analytics.

The following image is the earlier view of App Activity Investigator page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can now view all issues in the **Issues** section, along with the category that you could view in **App Activity Investigator** page.

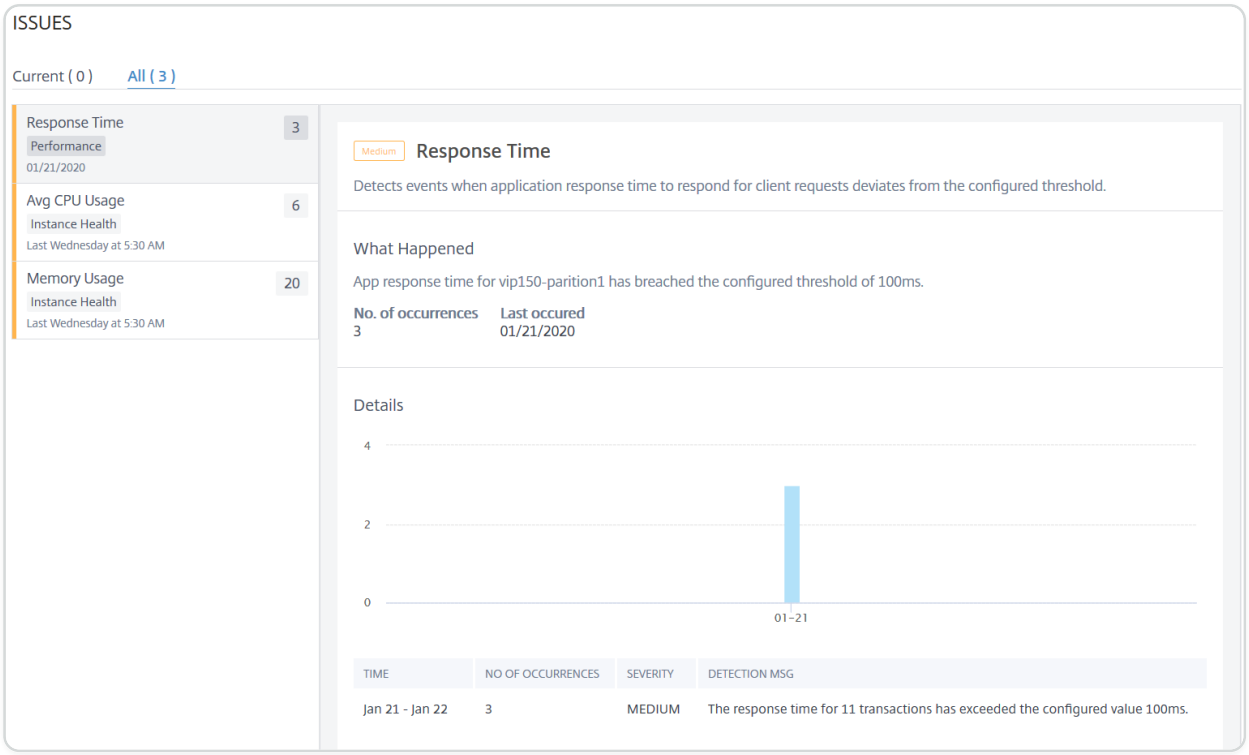


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The issues that display in **Current** tab refer to the application issues for the select time duration.
- The issues that display in **All** tab refer to total application issues.

The following example is the application issues for 1-day duration. The **Current** tab indicates no current issues impacting the app score.

The **All** tab displays the total issues detected for the 1-day duration.



Select App Score components and set thresholds

In **App Dashboard**, as an administrator, you can decide to select the components and configure thresholds for app score calculation. App Score is the scoring system that defines:

- How well an application is performing
- Whether the application is performing well in terms of responsiveness

Navigate to **Applications > Dashboard** and then select the settings icon.

In the **Configure App Score** page, you can select the components and configure thresholds to determine the final app score.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure App Score

Configure the contributing factors and their thresholds to calculate the App Score values

- [x] ADC Memory Usage
  - Low Memory Threshold (%): 70
  - High Memory Threshold (%): 85
- [x] Surge Queue Build-up
  - Lower Surge Queue Threshold: 0.05
  - Higher Surge Queue Threshold: 0.10
- [x] ADC CPU Usage
  - Low CPU Threshold (%): 80
  - High CPU Threshold (%): 90
- [x] Response Time
  - Response Time (ms): 500
- [x] App CPU Usage
  - Low App CPU Threshold (%): 70
  - High App CPU Threshold (%): 90
- [x] Active Services
  - Active Services Threshold (%): 100
- [x] Improper Persistence Type
- [x] Server Error 5xx
- [x] Unusually Large HTTP Packets
- [x] SSL Real Time Traffic
- [x] SSL Session Build-up
- [x] Low Session Reuse
- [x] NIC Card Saturation
- [x] TCP Reassemble Queue Limit Hits

OK | Close

App Score calculation is based on the following components:

APP SCORE COMPONENTS	USER CONFIGURED THRESHOLDS	DESCRIPTION
ADC Memory usage	Yes	The low and high threshold value for the total memory usage in the NetScaler instance
Surge queue buildup	Yes	The low and high threshold value for the total surge requests that are in queue and need a response.
ADC CPU usage	Yes	The low and high threshold value for the total CPU usage in the NetScaler instance.
Response time	Yes	The time interval between sending a request packet and receiving the first response packet from the service configured on the virtual server.
App CPU Usage	Yes	The low and high threshold value for the total CPU usage by the application.
Active services	Yes	The threshold value of the percentage of services that must be active which are bound to the virtual server.
Improper persistence type	No	Indicates if the persistence usage on a virtual server is low.
Server error (5xx)	No	Indicates if the web server responds with 5xx errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APP SCORE COMPONENTS	USER CONFIGURED THRESHOLDS	DESCRIPTION
Unusually large HTTP packets	No	Indicates the occurrences, if the HTTP messages with HTTP header size exceed the configured values in the NetScaler instance.
SSL real time traffic	No	Analyzes the SSL traffic to identify real time traffic and suggests optimal configuration settings for improving latency.
SSL session buildup	No	Indicates the session build-up over a period of time, which can lead to a large amount of memory being held up by these sessions in the NetScaler instance.
Low session reusage	No	Indicates if the actual number of sessions being reused by the NetScaler instance is less.
NIC card saturation	No	Indicates the total packets discarded by the interfaces.
TCP reassemble queue limit hits	No	Indicates if the Out-of-Order packets on a TCP connection exceed the configured out of order packet queue size.

By default, all components are enabled. If you disable any component, NetScaler® ADM performs the final app score calculation only based on the selected components.

Note

You can also continue to configure thresholds by navigating to **Settings > Analytics Settings** and clicking **Configure App Score**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application details for microservices applications

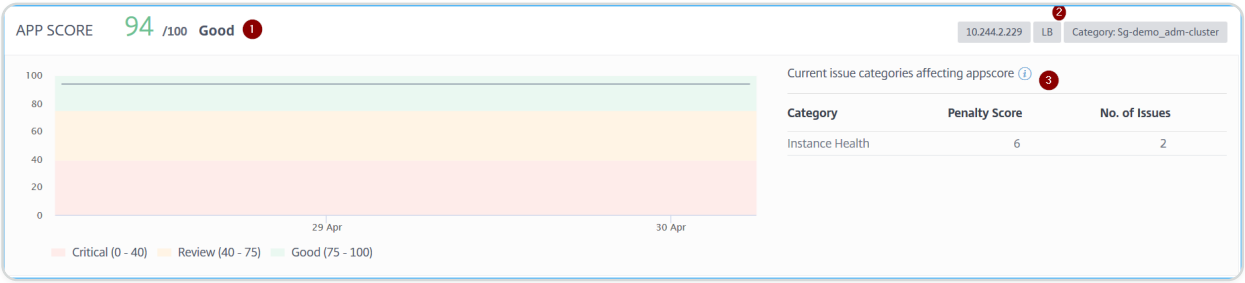
Click a microservices application from the dashboard to drill down for further detailed information.

The selected application page is displayed. From the application details page:

- Select the time duration from the list to view details for the specific time duration
- Click **Service Graph** to view service graph for the selected application. For more information, see Service Graph for Applications
- Click **Transaction Logs** to view the detailed transactions for the selected application
- Click **Audit logs** to view the detailed audit log information

After you select the time duration, the following application details are displayed:

- **App Score** – The application score for the selected time duration. You can also view the current application issues, which is known as the penalty score applicable based on the issue category. The final score is calculated as **100 minus total penalty**.



1 – Denotes the current app score

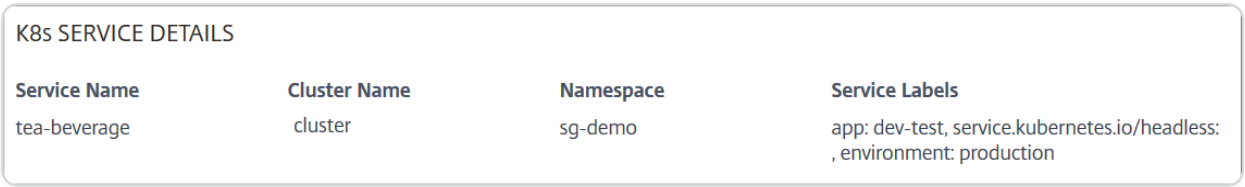
2 – Denotes the CPX IP address, application type such as load balancing or content switching, and service namespace and cluster name where the service is hosted

3 – Denotes the issues affecting the current application score

This dashboard also enables you to view the current issues that are affecting the app score. You can view the issues details under Issues.

- **K8s service details**

  You can view the following details:



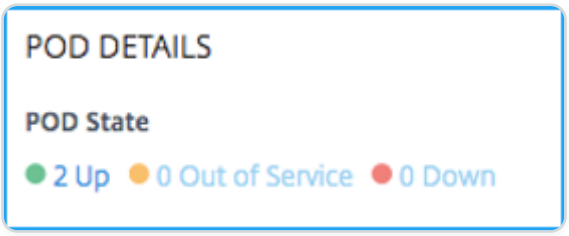
  - **Service Name** – The service name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

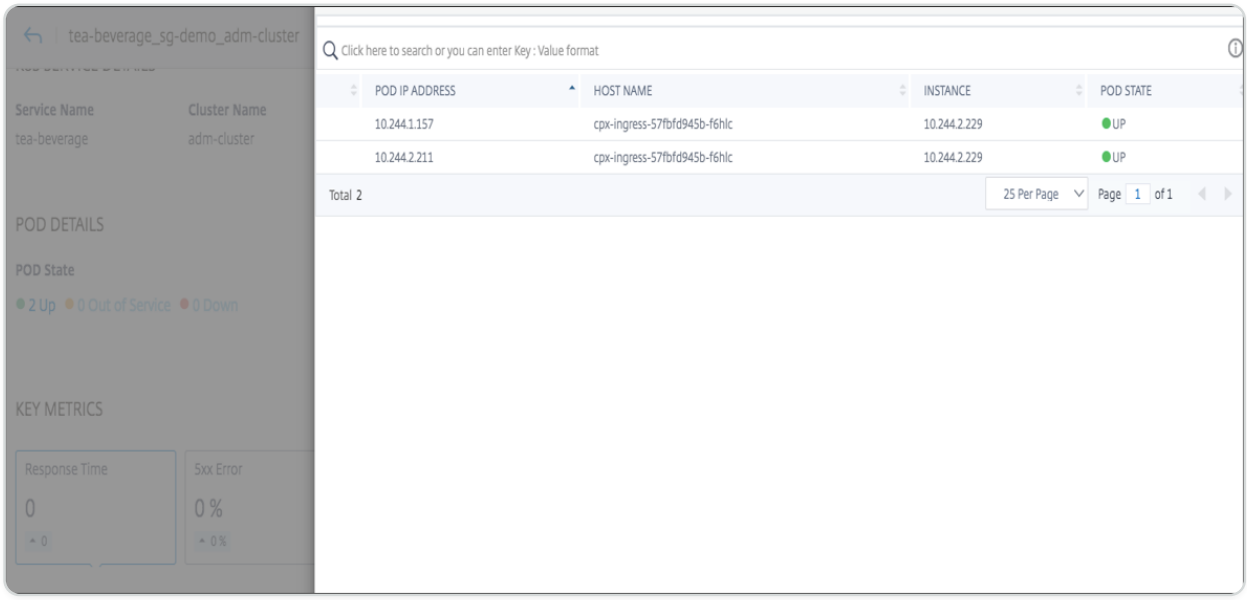
- **Cluster Name** – The cluster name where the service is hosted
- **Namespace** – The namespace assigned to the service
- **Service Labels** – The service labels assigned to the service

- **Pod Details**

  A pod is a group of containers hosted in the Kubernetes cluster. Inside a pod, you can deploy multiple containerized applications. Each pod is associated with an IP address.



Click the pod state to view the details



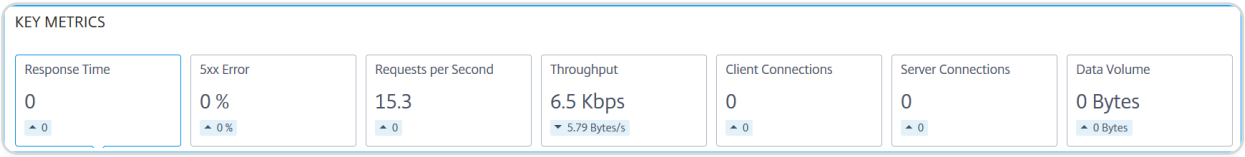
  - **Pod IP Address** – Denotes the Pod IP address
  - **Host name** – Denotes the host name assigned to the pod
  - **Instance** – Denotes the NetScaler CPX IP address
  - **POD state** – Denotes the pod current status

- **Key Metrics** – The key metrics details, such as **Response time**, **5xx errors**, **Requests per second**, **Throughput**, **Client Connections**, **Server Connections**, and **Data Volume** are displayed.

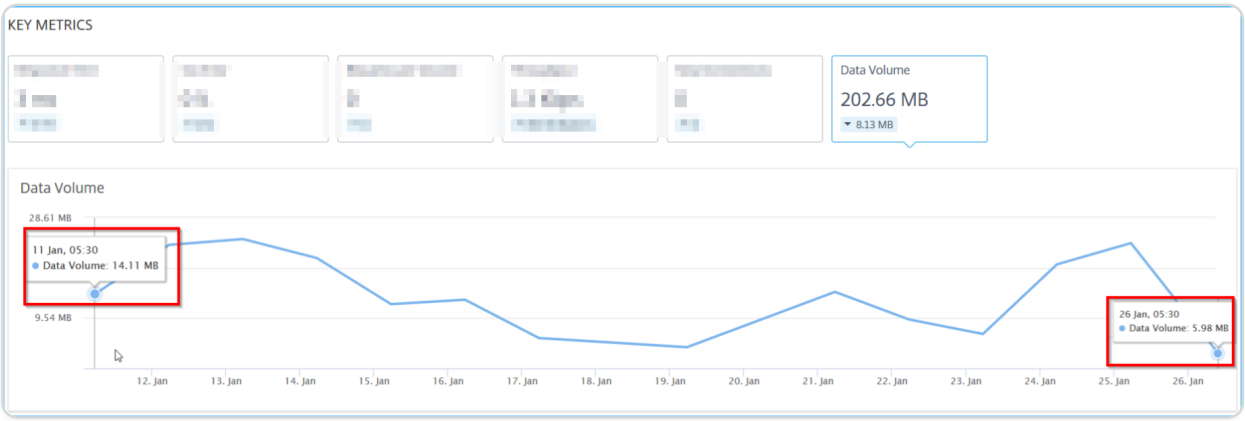
© 1997–2026 Citrix Systems, Inc. All rights reserved.

In each metric, you can view the average value and the difference value for the selected time duration. The difference value is calculated as the **first value minus the last value** of the selected time duration.

You can view the following instance metrics in a graph format for the selected time duration:



The following image is an example for **Data Volume** and the selected time duration is 1 month. The value 202.66 MB is the total Data Volume for the 1-month duration and the value 8.13 MB is the difference value. In the graph, the first value is 14.11 and the last value is 5.98. The difference value is 14.11 – 5.98 = 8.13 MB.



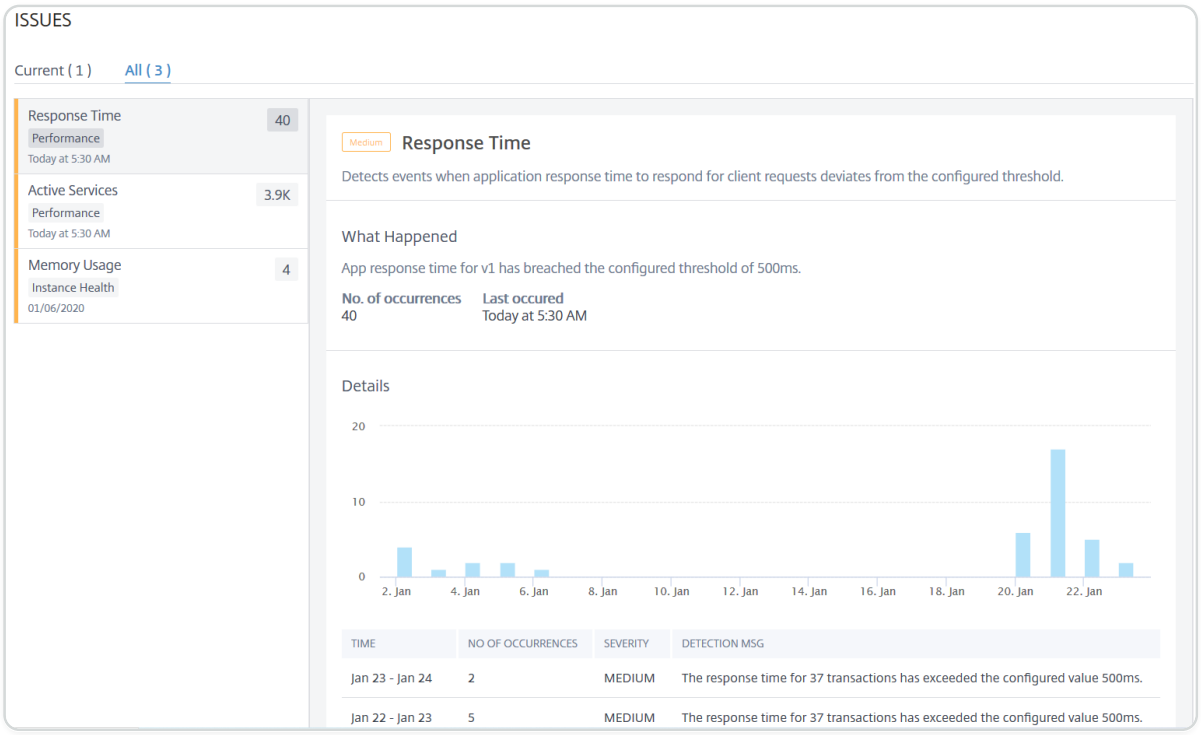
- **Issues** – The issues that are applicable for selected application. You can view the following issues along with its category:

PERFORMANCE	INSTANCE HEALTH	CONFIG	SYSTEM RESOURCES
Response Time	Average CPU Usage	High 5xx response	Improper persistence type
Low Session Reuse	Memory Usage	Unusually large HTTP packets	NIC Card Saturation
SurgeQueue Buildup		TCP reassemble queue limit hits	
SSL Real Time Traffic			

Click each issue to view the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Total occurrences
- Recommended Actions to troubleshoot the issue
- The issue details such as time, service name, total occurrences, severity, and detection message

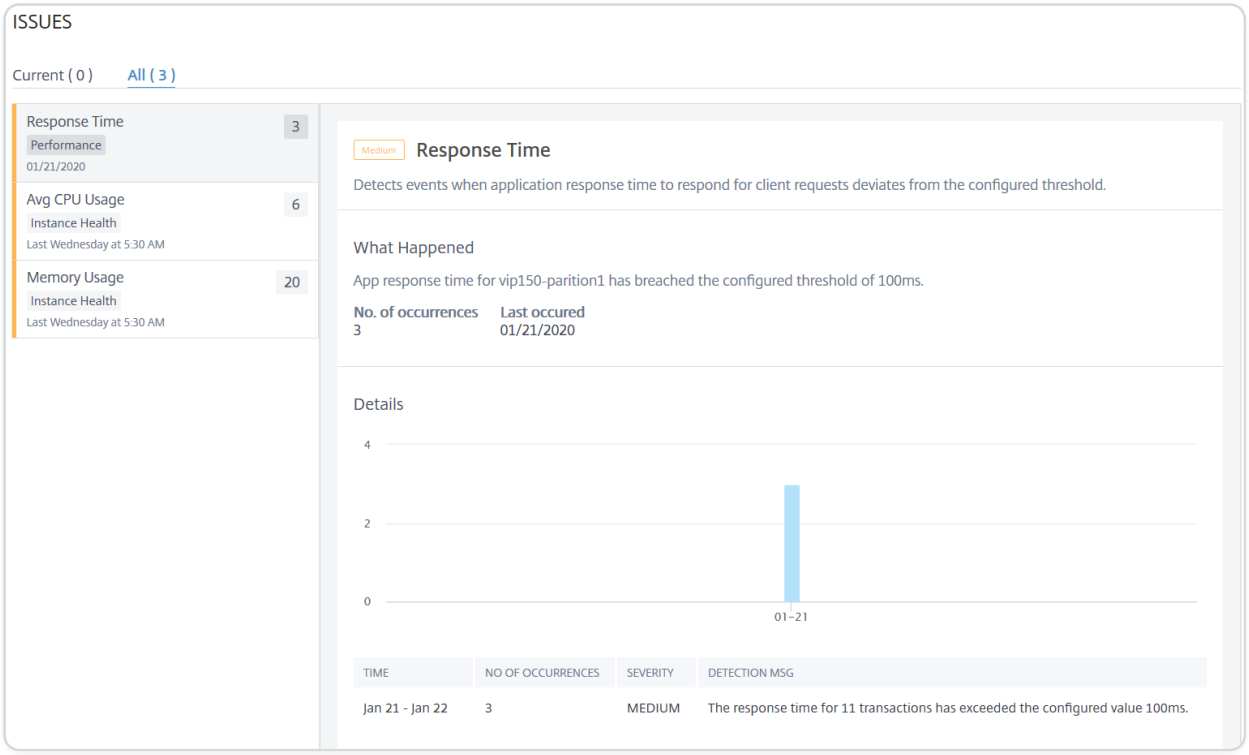


- The issues that display in **Current** tab refer to the application issues for the select time duration.
- The issues that display in **All** tab refer to total application issues.

The following example is the application issues for 1-day duration. The **Current** tab indicates no current issues impacting the app score.

The **All** tab displays the total issues detected for the 1-day duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Intelligent App Analytics

Intelligent App Analytics enables you to identify application performance issues using machine learning and rule-based algorithms. The Intelligent App Analytics feature of NetScaler® ADM:

- Provides an easy and scalable solution for monitoring and troubleshooting applications that are delivered through NetScaler instances.
- Monitors all levels of application to reduce the turnaround time for troubleshooting issues and improving the overall application uptime.

In a typical deployment, thousands of servers cater to the data needs of the users. The traffic sent to these servers is load balanced and monitored by virtual servers configured on NetScaler appliances. Each virtual server is bound to multiple services representing the backend servers. In such deployments, the Intelligent App Analytics feature helps you:

- Monitor, manage, and make decisions during outages and other events
- Monitor the virtual servers and services configured for an application
- Display critical information about virtual servers and services, so that you can change the configurations as required to achieve optimum performance by the applications.

When you scale-up your organization server farm, it becomes difficult to track the problems associated with the huge amount of traffic received on the servers and narrow down to the required troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

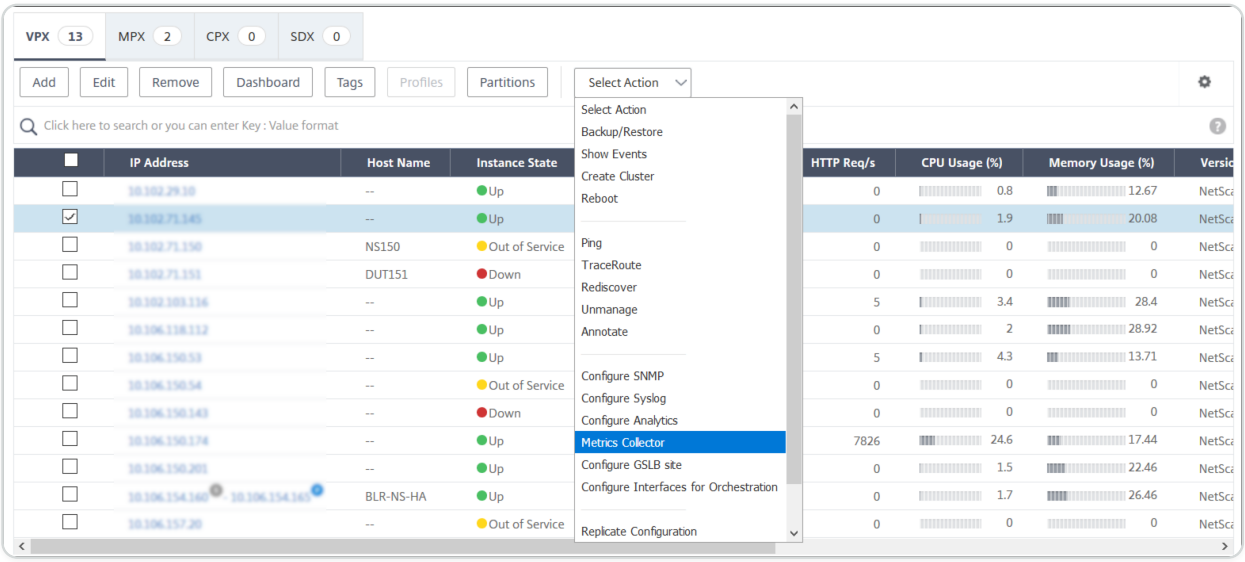
When an application is running and receiving large amount of traffic, you might various issues. You can view the performance indicators for application analytics by navigating to **Applications** > **Dashboard**, selecting an application, and scrolling down to view issues in **Issues** section.

Configure Intelligent App Analytics

The Intelligent App Analytics feature is supported only in **NetScaler 12.1.50.x or later**. **Metrics Collector** pushes the NetScaler counter data to NetScaler ADM, which is used to detect application issues. To use the Intelligent App Analytics feature, **Metrics Collector** must be configured on each NetScaler instance. By default, **Metrics Collector** is enabled on NetScaler, while you add the instance to NetScaler ADM.

To ensure if **Metrics Collector** is enabled:

1. Navigate to **Infrastructure > Instances > NetScaler** and select the type of instance you want to monitor (for example, NetScaler VPX).
2. Select the NetScaler instance.
3. From the **Select Action** list, select **Metrics Collector**.



4. On the **Configure Metrics Collector settings** page, the **Enable** option is selected by default. If this option is not selected, ensure to select the **Enable** option and then click **OK**.

NOTE

To view anomalies for **Server Errors** and its **detailed web transaction**, you must enable analytics on virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance indicators for application analytics

You can view the performance indicators, along with its categories that occur in NetScaler web applications. To view these indicators, you must ensure to enable analytics and metrics collector on the ADC instance:

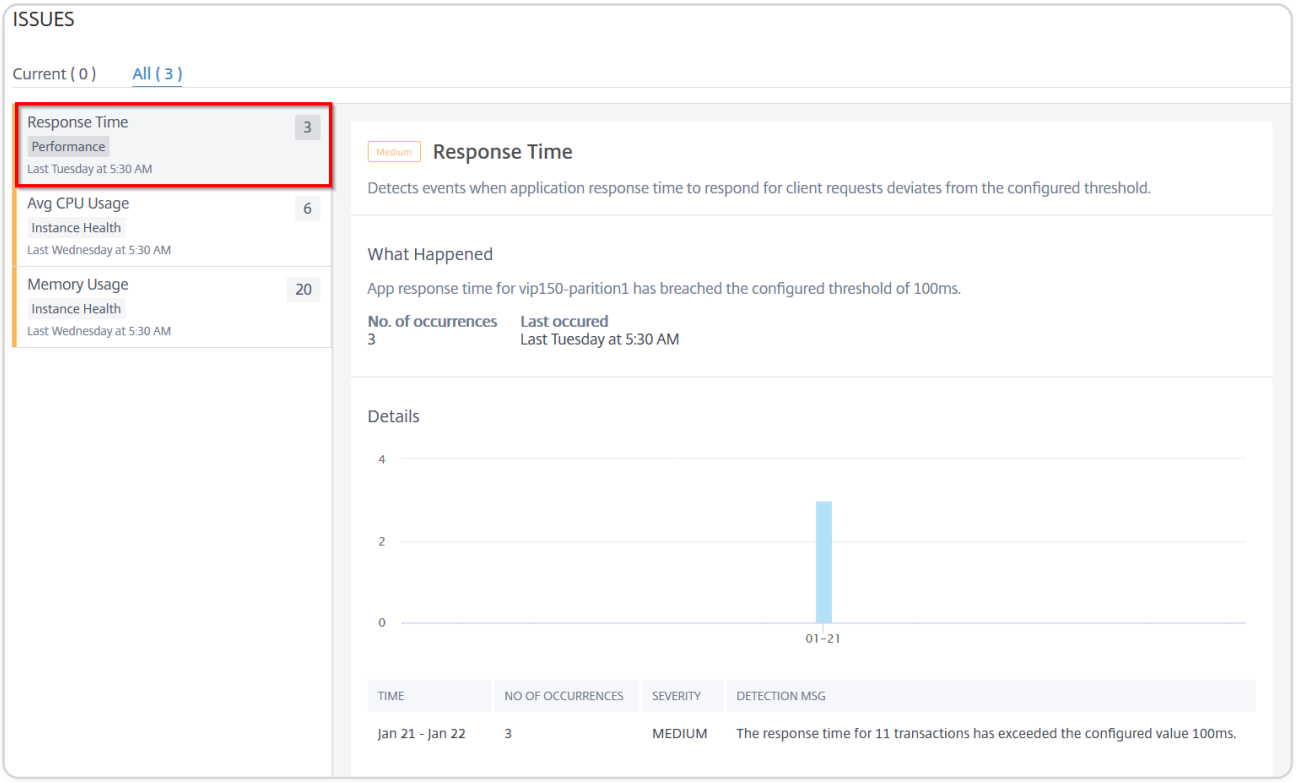
After you enable analytics and metrics collector, you can view the following indicators by navigating to **Applications** > **Dashboard**, selecting an application, and scrolling down to **Issues** section:

- Response Time
- Active Services
- Average CPU Usage
- Memory Usage
- NIC Card Saturation
- Service Flaps
- Low session reuse
- Improper Persistence Type
- Unstable Server (5xx)
- SSL Real Time Traffic
- Unusually Large HTTP packets
- TCP reassembly queue limit hits
- Surge Queue Buildup

Response Time

This issue detects when the application response time to respond to client requests deviates from the configured threshold value. Click the **Response Time** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



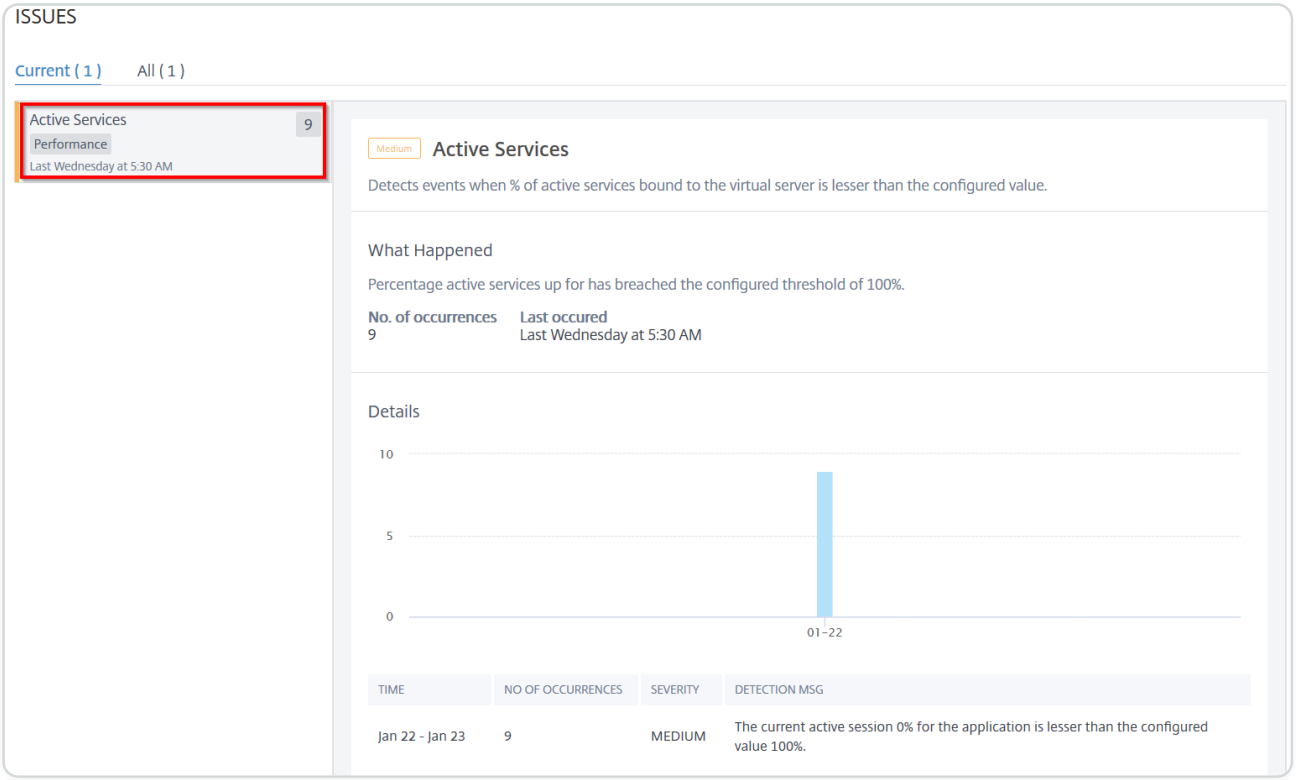
Under **Details**, you can view:

- The graph indicating the total events for the selected time. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time
- The issue severity such as low, medium, and high
- The detection message indicating the total transaction response time exceeding the configured threshold value

Active Services

This issue detects when the % of active services bound to the virtual server is lesser than the configured threshold value. Click the **Active Services** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



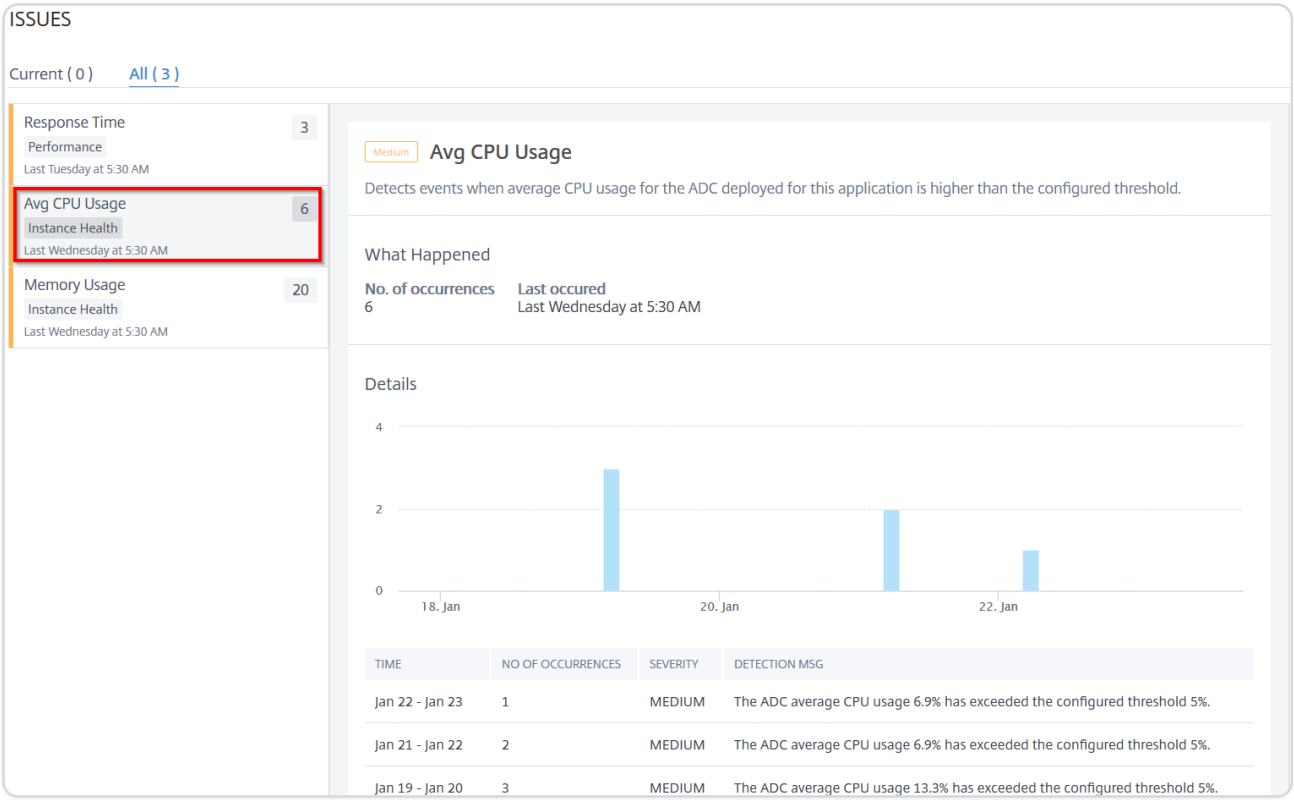
Under **Details**, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the % of active service sessions and the configured threshold value

Average CPU Usage

This issue detects when the ADC CPU usage for this application exceeds the configured threshold value. Click the **Average CPU Usage** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



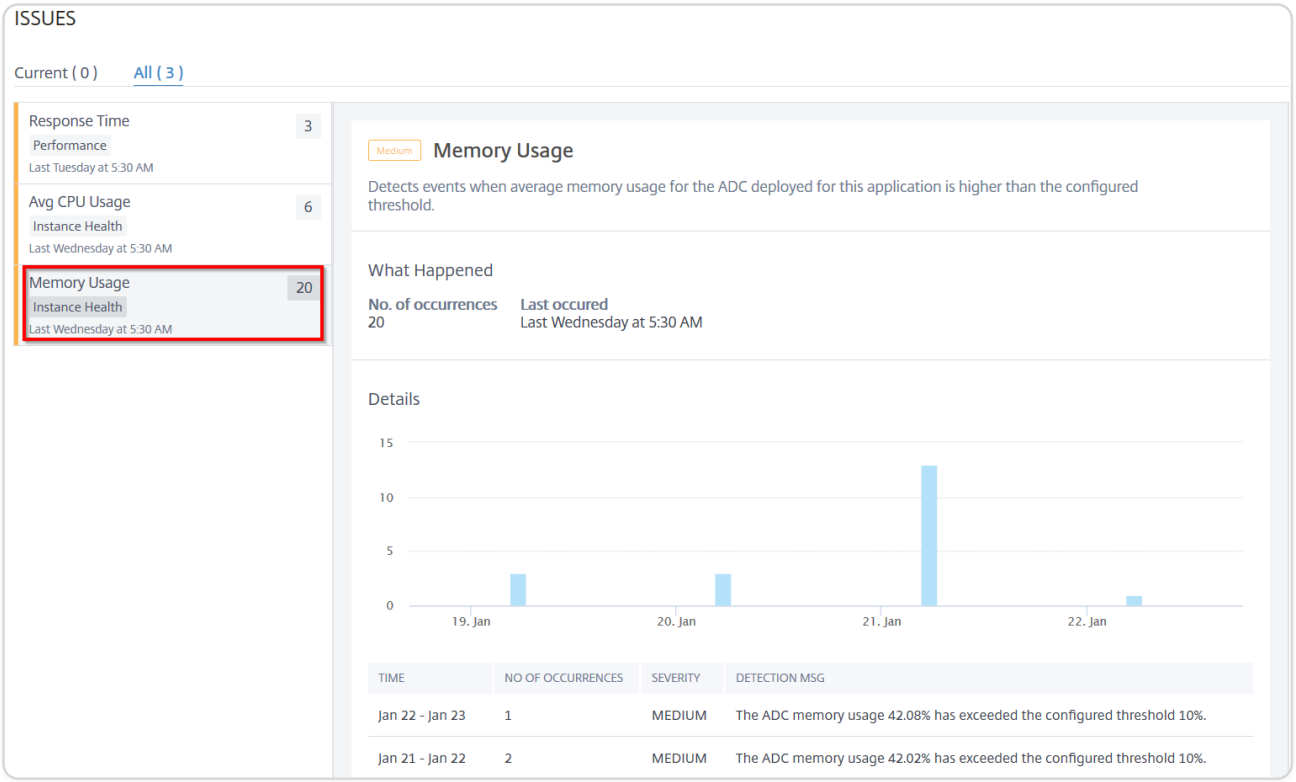
Under **Details**, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the ADC average CPU usage % and the configured threshold value

Memory Usage

This issue detects when the ADC memory usage for this application exceeds the configured threshold value. Click the **Memory Usage** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Under **Details**, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the ADC average memory usage % and the configured threshold value

Service Flaps

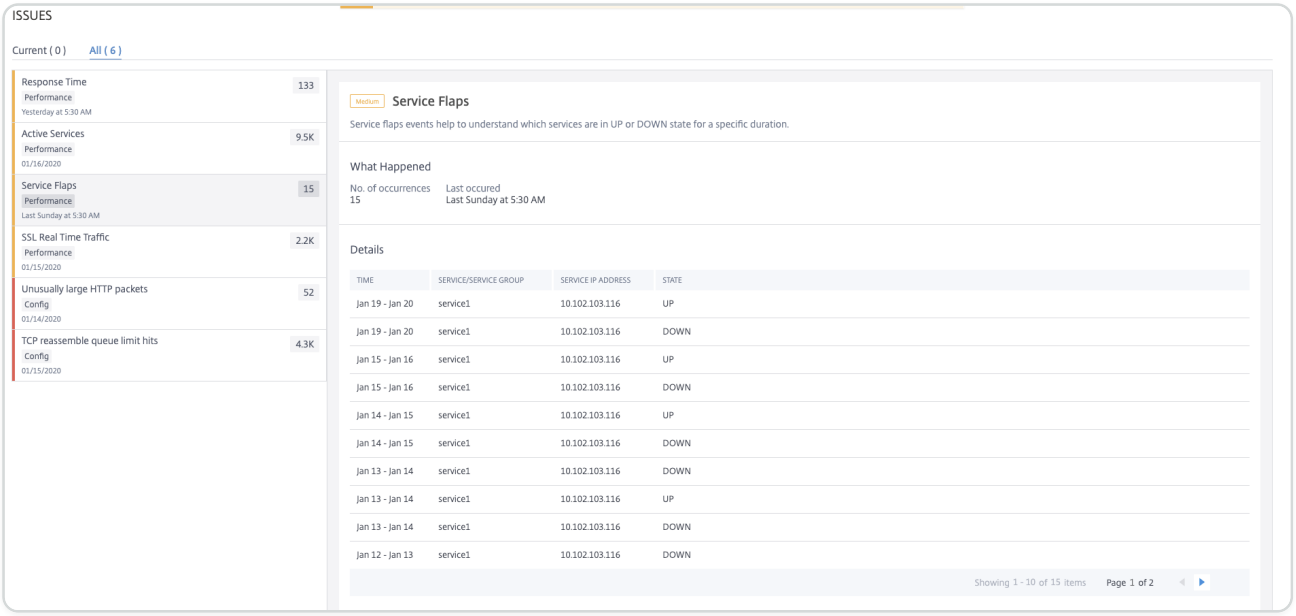
As a network administrator, you must ensure for optimal availability of the application. When there are any network issues or configuration issues, the status and availability of an application server might impact the overall performance.

Using the service flaps events, you can identify the application that has issues. Service flaps events also help you:

- Understand which service is in DOWN status for a specific duration
- Understand how many services are in UP or DOWN state for a specific duration

Click the **Service Flaps** tab to view the service flaps details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can view details such as number of occurrences and the time of last occurrence.

Under **Details**, you can view:

- The time that occurred the service flap anomaly
- The service/service group name
- The service IP address
- The current service status

Unstable Server

In some scenarios, the web server responds with status codes when it is unable to handle the requests for reasons such as invalid requests, temporary overloading, or server maintenance. These errors are displayed with error codes, which define various scenarios of the errors. For example,

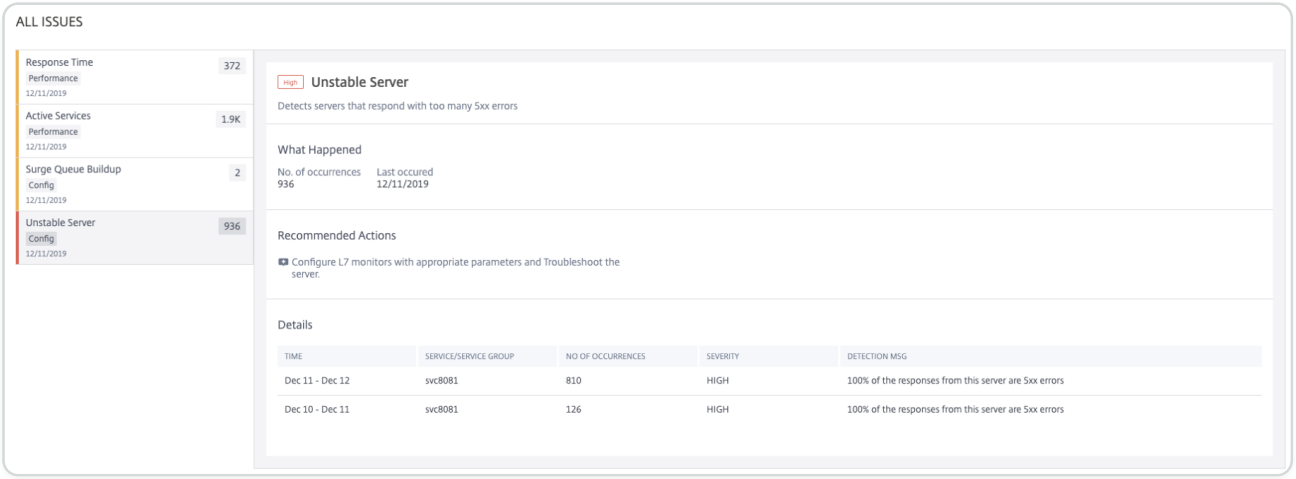
- **502 Bad Gateway** The server is acting as a gateway or proxy and received an invalid response from the upstream server.
- **503 Service Unavailable** The server is currently unavailable. The servers might be overloaded or down for maintenance.
- **504 Gateway Time-out** The server is acting as a gateway or proxy and did not receive a timely response from the upstream server.

These can be temporary conditions, but sometimes you have to implement a corrective measure on the webservers to make the webpages up and available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the **Unstable Server** indicator, you can view these failures and take decisions about corrective actions to overcome the issues and ensure the client requests are served and the webpages are always available.

Select the **Unstable server** tab to view the issue details.



The **Recommended Actions** to troubleshoot the issue are:

- Configure L7 monitors with appropriate parameters for the server that responds with 5xx errors. A monitor is an entity that tracks the service health. The appliance periodically probes the servers using the monitor bound to each service. If a server does not respond within a specified response timeout, and the specified probes fail, the service is marked DOWN. The appliance then performs load balancing among the remaining services. For more information to configure a monitor, see Custom Monitors
- Troubleshoot the server

Under **Details**, you can view:

- The time that occurred the unstable server anomaly
- The service/service group name
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating % of the responses from this service reporting 5xx errors

For detailed information on server error web transaction, see Web transaction analytics for server errors

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Buildup

For all secured transactions, NetScaler performs the SSL offloading process for the first transaction and then stores the SSL session based on the **Session Reuse** configuration.

Based on the traffic rate, session build-up may occur over a period of time, which can lead to a large amount of memory being held up by these sessions in NetScaler.

Session build-up events alert the administrators and provide recommended actions to resolve this event. Click the **Session Buildup** tab to view the issue details

Under **Details**, you can view:

- The time that occurred the session build-up anomaly
- The virtual server name
- The anomaly severity such as high, low, and medium
- The message indicating that **X** number of SSL sessions available in the virtual server and currently, there is **Y** number of SSL handshakes per second within the configured timeout session.

The **Recommended Action** to fix this anomaly is to either reduce the session timeout or disable the session reuse. For more information, see Session Timeout.

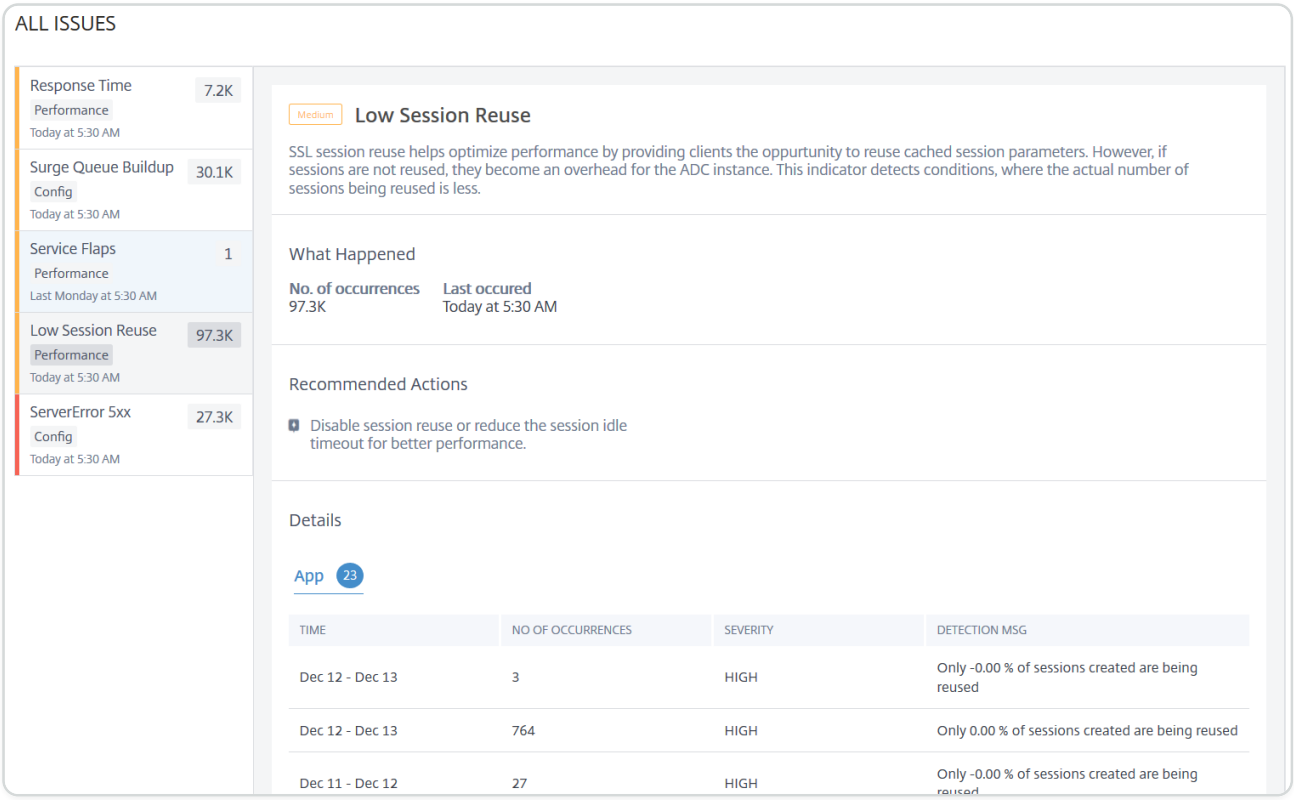
Low Session Reuse

NetScaler instances process SSL transactions by offloading the SSL handshake process from the server. Upon receiving the response from the server, the NetScaler instance completes the secure transaction with the client. Using the cached session parameters, the NetScaler instance completes the SSL handshake process for the consecutive requests.

If in case these sessions are not reused, they become an overhead for the NetScaler instances. Using the **Low Session Reuse** indicator, you can identify if the actual number of sessions being reused is less.

Click the **Low Session Reuse** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to either disable the session reuse or reduce the session timeout. For more information, see Session Reuse.

Under **Details**, you can view:

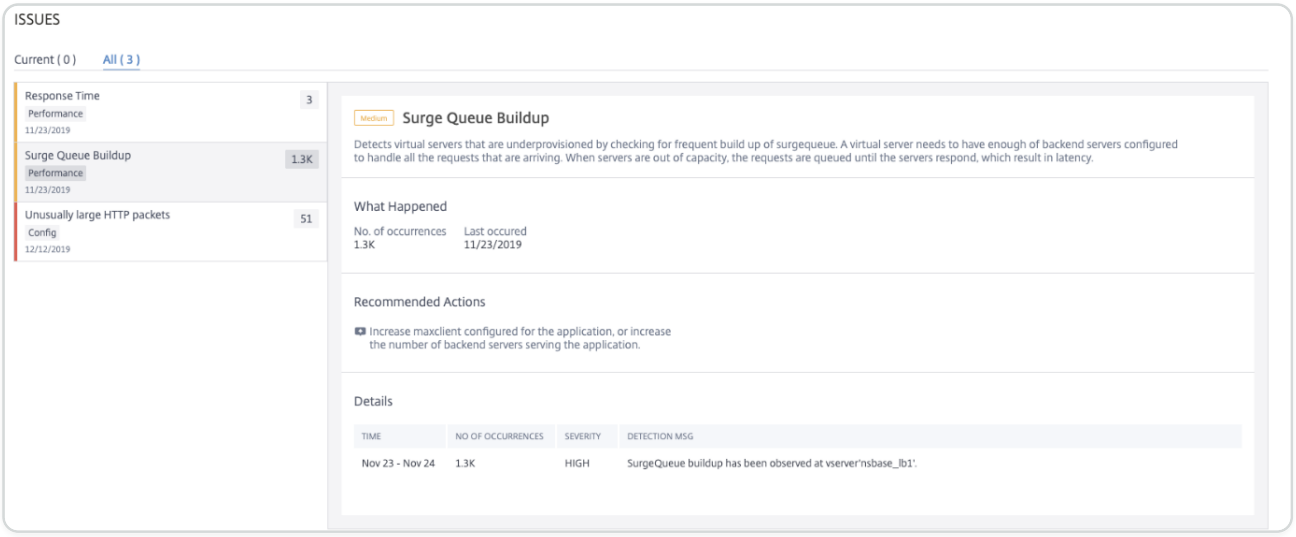
- Total applications that have Low session reusage
- The time that occurred the low session reuse anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating only % of the configured sessions are being reused

Surge Queue Buildup

When a server receives a surge of requests, the server becomes slow to respond to the clients. Often, the overload also causes clients to receive error pages. A virtual server needs to have enough back-end servers configured to handle the incoming requests.

Using the **Surge Queue Buildup** indicator, you can view the virtual servers that have surge queue buildup. Click the **Surge Queue Buildup** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue are:

- Increase the number of client connections limit. For more information, see Set a limit on the number of client connections
- Increase the back-end servers to serve the application requests

Under **Details**, you can view:

- The time that occurred the surge queue buildup anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the surge queue buildup on the virtual server

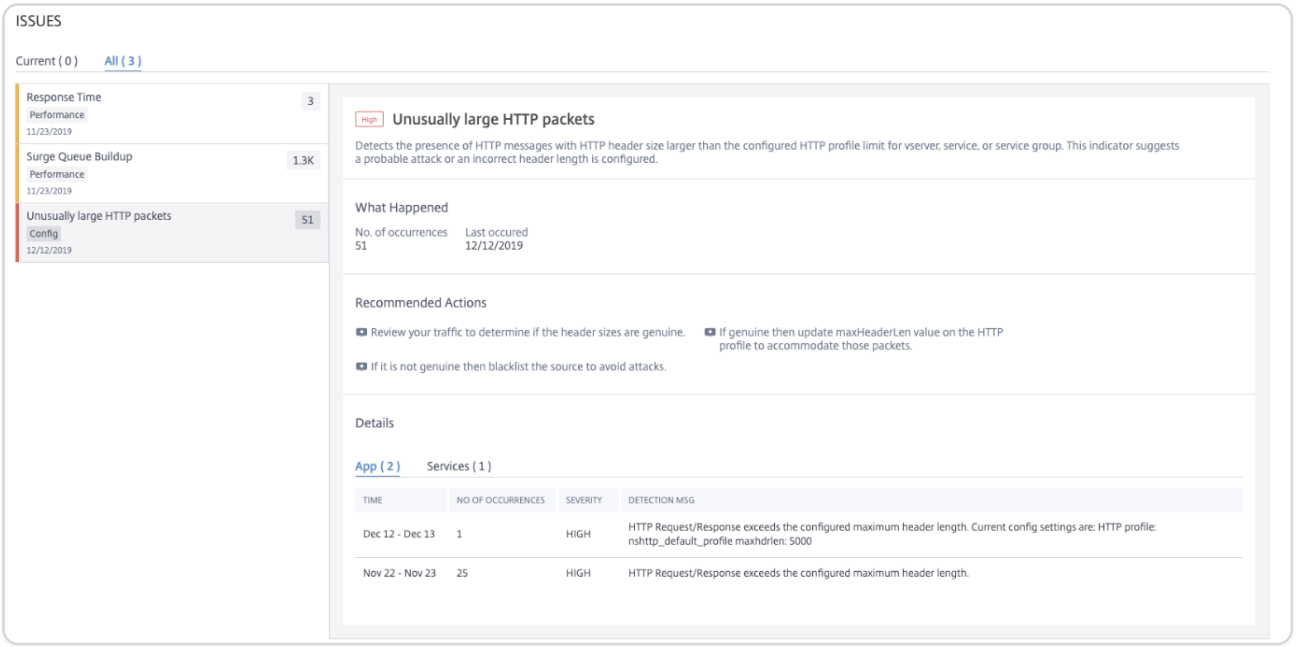
Unusually large HTTP packets

An HTTP transaction uses request-response messages between the client and the server. In the request and response messages, HTTP headers are the values that are displayed in the HTTP protocol. You can configure the HTTP header length in virtual server, service, or service group to avoid 4xx errors

When an HTTP request/response exceeds the maximum header length, it can be a possible attack. Using the **Unusually large HTTP packets** indicator, you can view the occurrences where the HTTP messages with HTTP header size exceed the configured values.

Click the **Unusually large HTTP packets** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue are:

- Review the traffic to determine the header size is genuine. If the header size is genuine, then update the header value on the HTTP profile. For more information, see Buffer Overflow Check.
- If the header size is not genuine, block list the source to avoid attacks.

Under **Details**, you can view:

- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the current HTTP header length configured on the virtual server, server, or service group

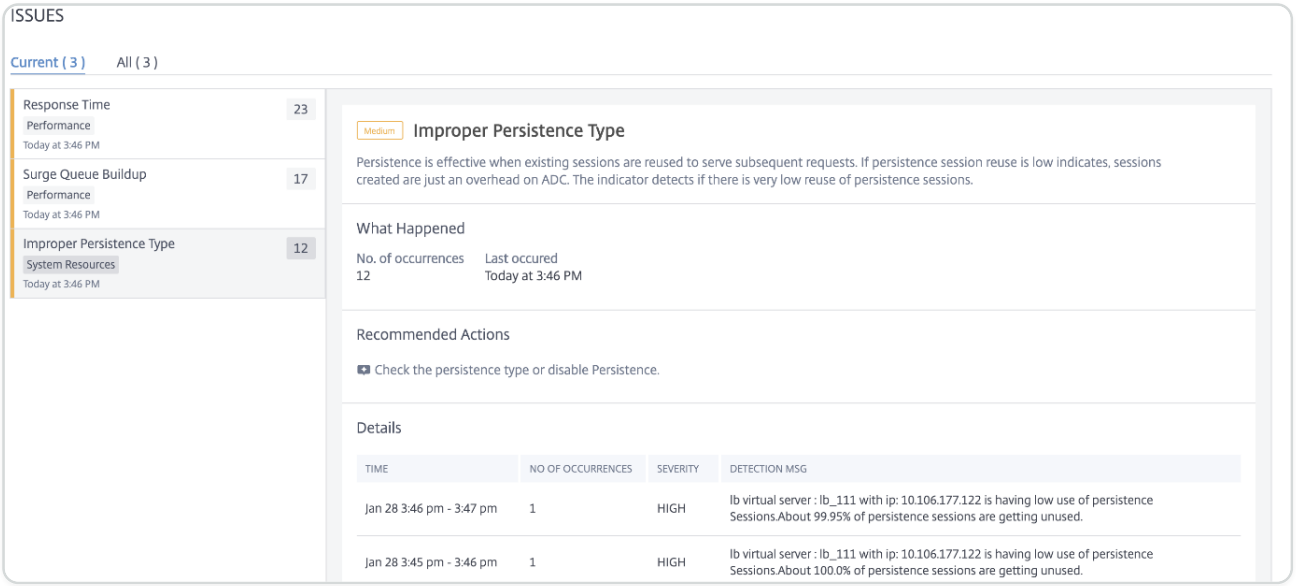
Improper Persistence Type

You must configure persistence on a virtual server if you want to maintain the states of connections on the servers represented by that virtual server (for example, connections used in e-commerce). The appliance then uses the configured load balancing method for the initial server selection, but forwards all subsequent requests to that same server from the same client.

Persistence is effective when existing sessions are reused to serve subsequent requests. If persistence session reuse is low, sessions created on ADC are just an overhead.

Using the **Improper Persistence Type** indicator, you can determine if the persistence usage on a virtual server is low. Click the **Improper Persistence Type** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to check the persistence type or disable persistence. For more information, see Persistence Settings.

Under **Details**, you can view:

- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the % of sessions that are unused

TCP reassemble queue limit hits

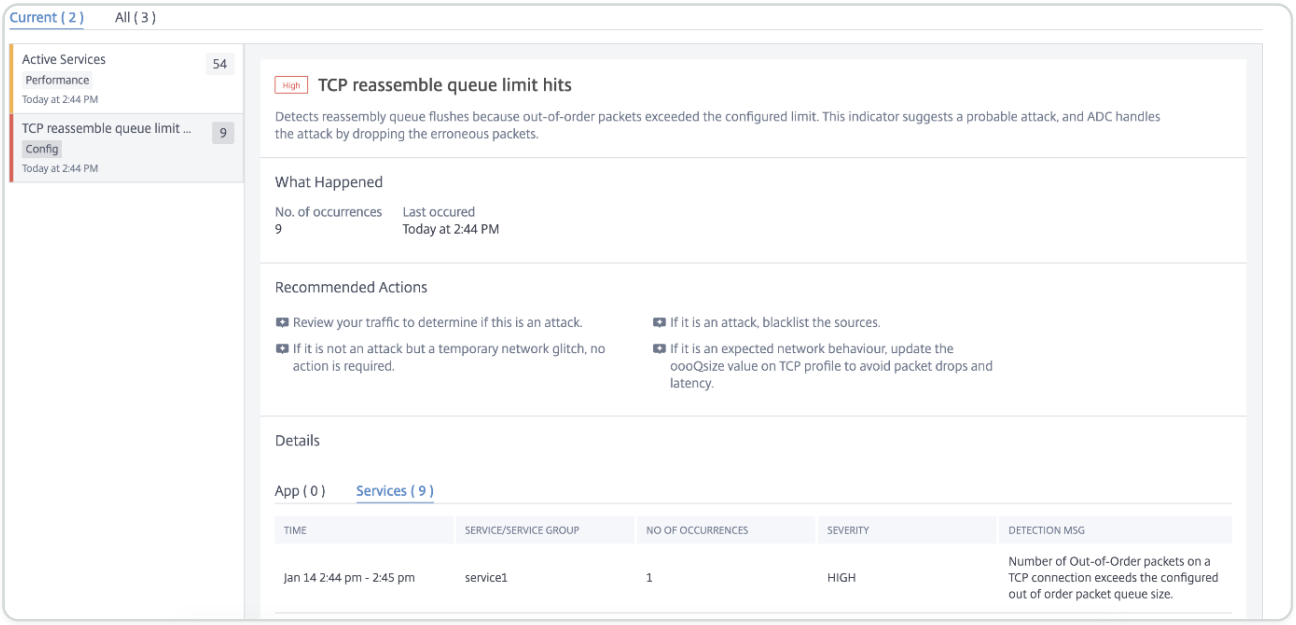
TCP maintains an Out-of-Order queue to keep the OOO packets in the TCP communication. This setting impacts NetScaler memory if the queue size is long as the packets need to be kept in runtime memory.

This queue size needs to be at an optimized level based on the network and application characteristics.

Using the **TCP reassemble queue limit hits** indicator, you can view if the Out-of-Order packets on a TCP connection exceed the configured out of order packet queue size.

Click the **TCP reassemble queue limit hits** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue are:

- Review the traffic and block list the source if it is an attack
- If this behavior is an expected network behavior, then update the out-of-order packets size value on TCP profile. For more information, see TCP Optimization
- If it is just a temporary network glitch, then no further action is required

Under **Details**, you can view:

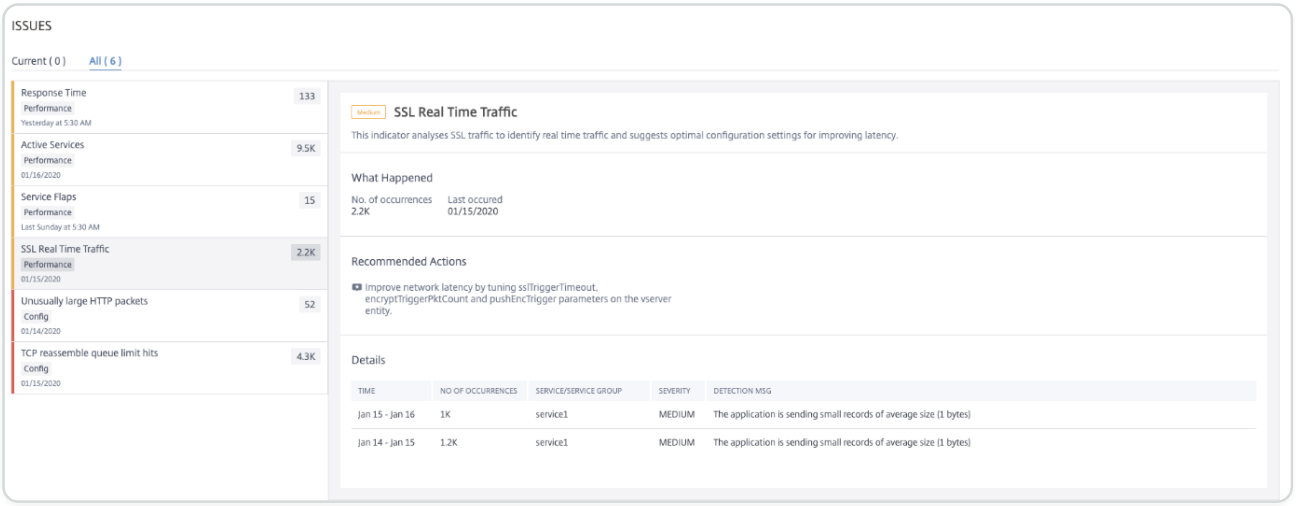
- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as low, medium, and high
- The detection message indicating the current TCP profile and oooQsize settings

SSL Real Time Traffic

In NetScaler instance, you can use an SSL profile for processing SSL traffic. The SSL profile comprises certain SSL parameters for virtual servers, services, and service groups. The **SSL Real Time Traffic** indicator analyzes the SSL traffic to identify real time traffic and suggests optimal configuration settings for improving latency.

Click the **SSL Real Time Traffic** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to improve the network latency by updating SSL parameters. For more information, see Global SSL Parameters.

Under **Details**, you can view:

- The time that occurred the anomaly
- The service/service group name
- The anomaly severity such as low, medium, and high
- The detection message with the current setting on the application

Troubleshoot App Dashboard

After you add an application in the App Dashboard, the dashboard immediately displays the app basic configuration details. The application analytics details such as app score, key metrics, and issues start to populate within a few minutes (approximately 10 to 15 minutes). For more information, see Applications.

You must ensure that there is no issue with metrics data flow (AppFlow collector or Analytics profile) from the NetScaler instance. You can get more information on AppFlow collector and analytics profile in this document.

This document describes the troubleshooting steps that you need to perform when:

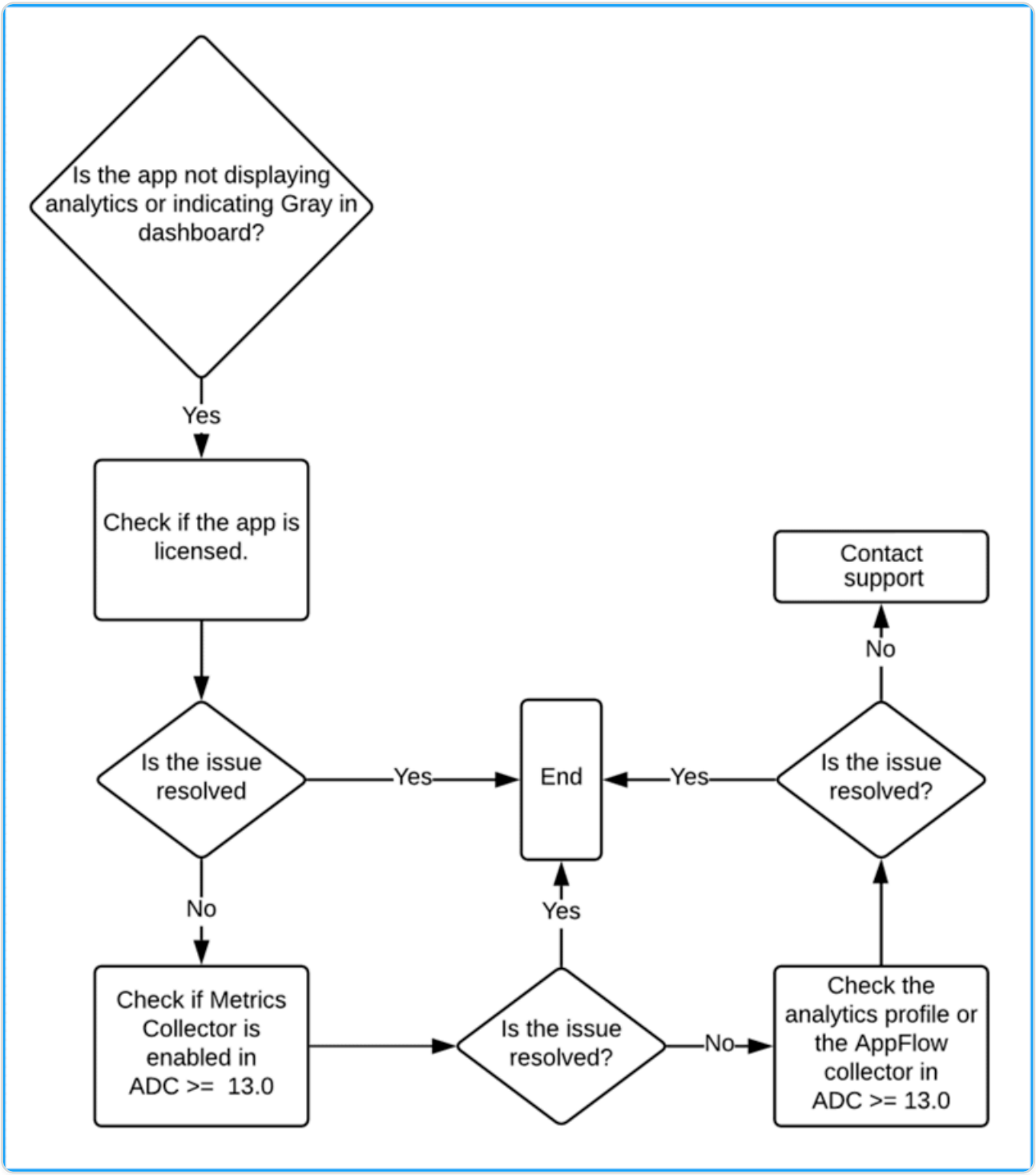
- You click an application, the analytics for the selected application do not display the required data even after the mentioned duration (10–15 minutes).
- The CS or LB application is always indicating Gray color (**Not Applicable** status) in App Dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The troubleshooting procedures mentioned in this document are only applicable to **Content Switching** and **Load Balancing** virtual servers.

Troubleshooting scenario



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application is licensed

You must ensure if the application is licensed. Navigate to **Settings > Licensing & Analytics Configuration** and verify if the application is licensed under **Virtual Server License Summary**. If the application is not licensed, see the following:

- **ADM service** - Manage licensing and enable analytics on virtual servers.
- **ADM on-prem** – Manage licensing and enable analytics on virtual servers.

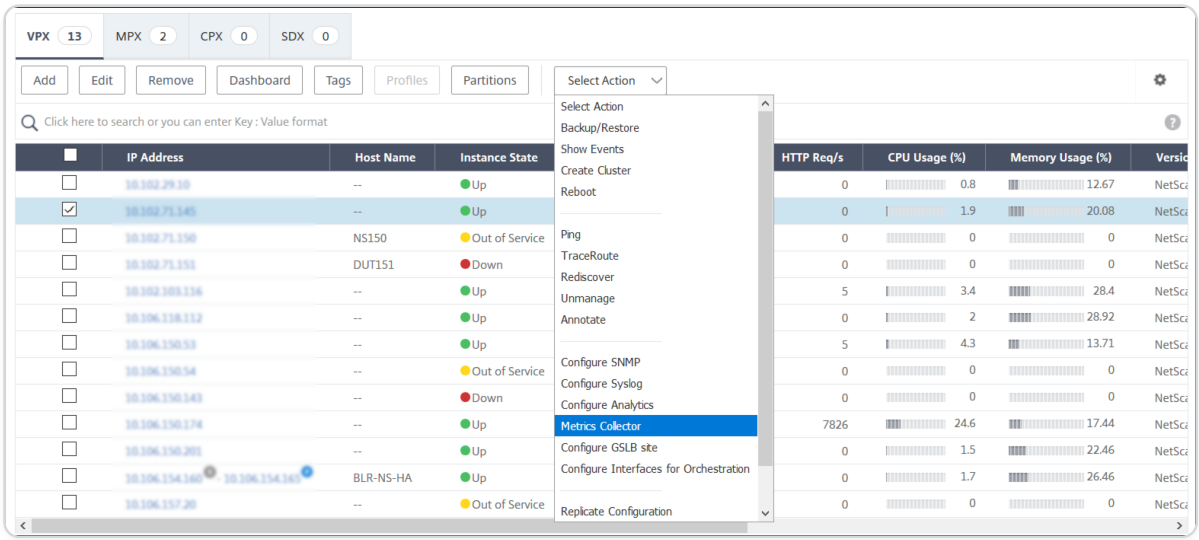
Metrics collector is enabled

You must ensure if **Metrics Collector** is enabled in the NetScaler instance.

For NetScaler version 13.0 or later, Metrics Collector is enabled by default, after the ADC instance is successfully added in ADM. To ensure if metrics collector is enabled:

1. Navigate to **Infrastructure > Instances**. Under Instances, select the type of instance (for example, NetScaler VPX).
2. Select the NetScaler instance.

   a. From the **Select Action** list, select **Metrics Collector**.



3. On the **Configure Metrics Collector settings** page, ensure if **Enable** option is selected. If not, select the **Enable** option and click **OK**.

After you enable metrics collector and if you are still not able to view the data, validate:

- The AppFlow collector in NetScaler instance version 13.0 **earlier than 47.x build**.
- The analytics profile in NetScaler instance build **47.x or later**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler instance earlier builds

In NetScaler:

1. Run the following command to ensure if the collector is **UP** and running at Port 5563:

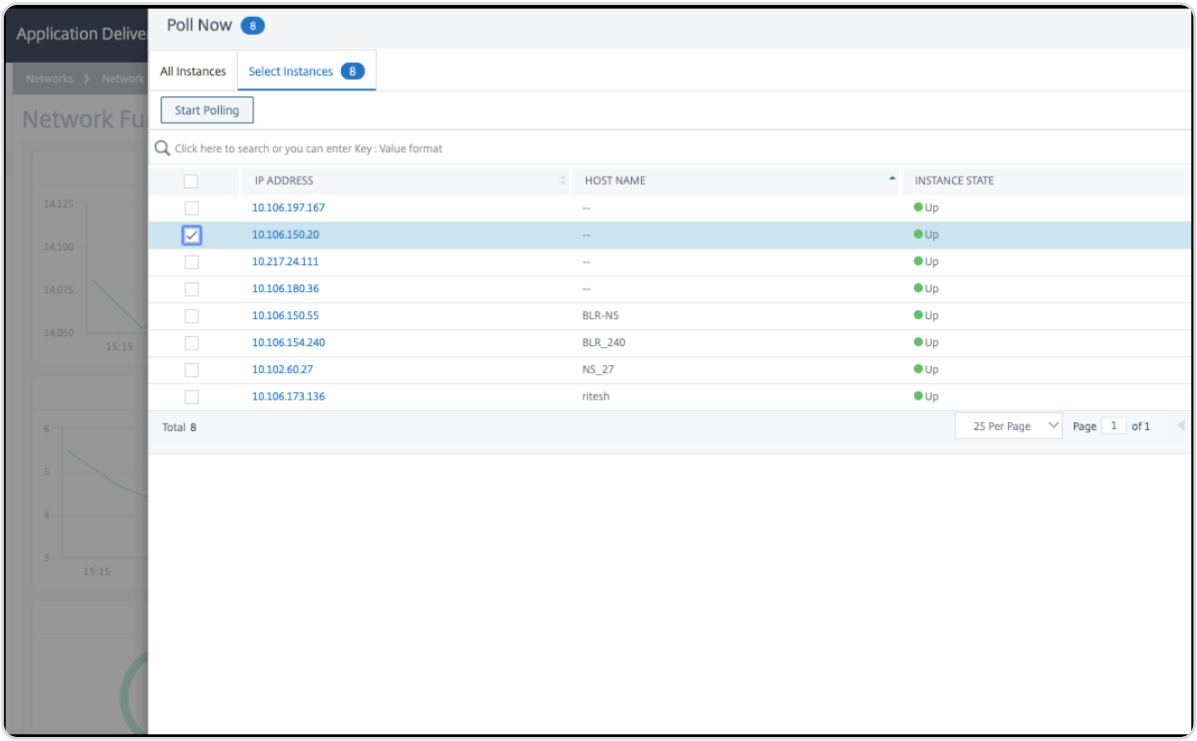
   `sh appflow collector af_collector_rest_<adm_receiver_ip>`

   ```
   > sh appflow collector af_collector_rest_10.102.103.114
   1) Name: af_collector_rest_10.102.103.114
   IPv4 address: 10.102.103.114
   Port: 5563
   Netprofile:
   Transport: rest
   State: UP
   Done
   ```

2. If no collector is available, do an instance manual polling in NetScaler® ADM.

   a. Navigate to **Infrastructure > Network Function > Poll Now**

   b. Select the instance and click **Start Polling**.



   If polling fails, remove the ADC instance from ADM and then add the ADC instance again. When you add the ADC instance, the collector gets added on ADC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the collector indicates **Down** status:

1. Ensure if SNIP is configured.

   ```
   > sh ip | grep SNIP
   2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
   ```

   If SNIP is not configured, you must configure SNIP. For more information, see Configuring SNIP.

2. Ensure that if ADC instance is reachable to ADM.

   You can validate by doing a ping test. Run `ping -S <SNIP> <adm_receiver_ip>`

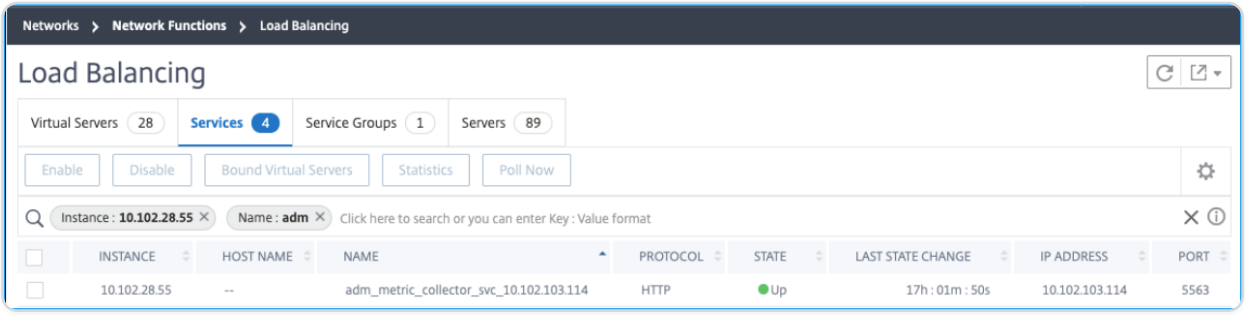
   ```
   > ping -S 10.106.150.34 10.102.103.114
   PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
   64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
   64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
   64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
   ```

NetScaler instance later builds

In NetScaler ADM, ensure that the metrics collector service is available:

1. Navigate to **Infrastructure > Network Function > Load Balancing > Services**.
2. On the search bar, filter by **Instance: (IP address)** and **Name: ADM**.
3. Ensure if `adm_metric_collector_svc_<adm_receiver ip>` is available. The IP address can be either the ADM management IP or the agent IP.

   Ensure that this service is in **UP** status and running at Port 5563.



If you still cannot view the data, ensure that the collector service is bound to time series analytics profile in NetScaler.

1. Log on to NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run the following command:

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

If the collector indicates **Down** status:

1. Ensure if SNIP is configured.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   If SNIP is not configured, you must configure SNIP. For more information, see Configuring SNIP.

2. Ensure that if ADC instance is reachable to ADM.

   You can validate by doing a ping test. Run `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Ensure that the traffic connectivity through telnet is able to connect the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

If telnet is able to connect the service, then a firewall exists and is blocking the metric data flow. You must resolve the firewall block issue.

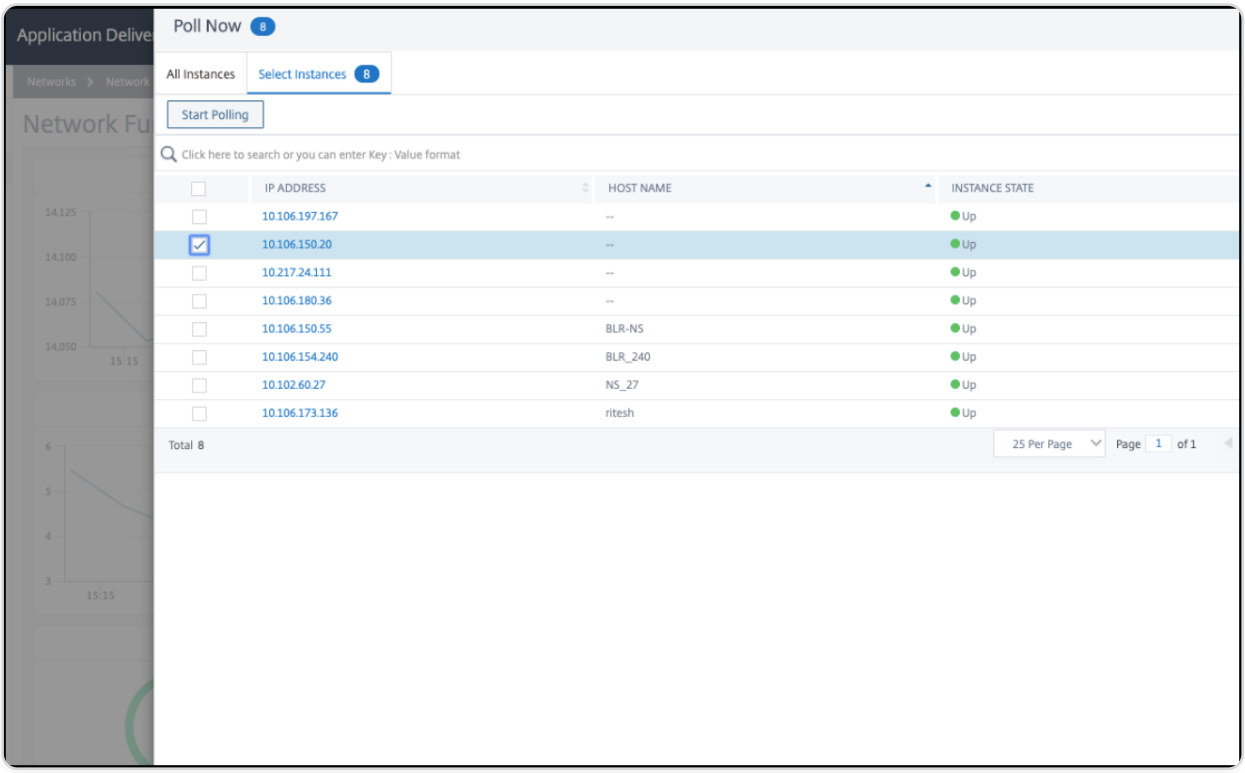
If no collector service is bound to time series analytics profile in NetScaler, the Collector is displayed as blank.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

You must do an instance manual polling in NetScaler ADM.

1. Navigate to **Infrastructure > Network Function > Poll Now**
2. Select the instance and click **Start Polling**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If polling fails, add the collector service directly at NetScaler instance using the following commands:

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
```

The analytics time series profile is updated.

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

If the issue still persists even after performing all the mentioned troubleshooting steps, contact **NetScaler support**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application usage and anomalies

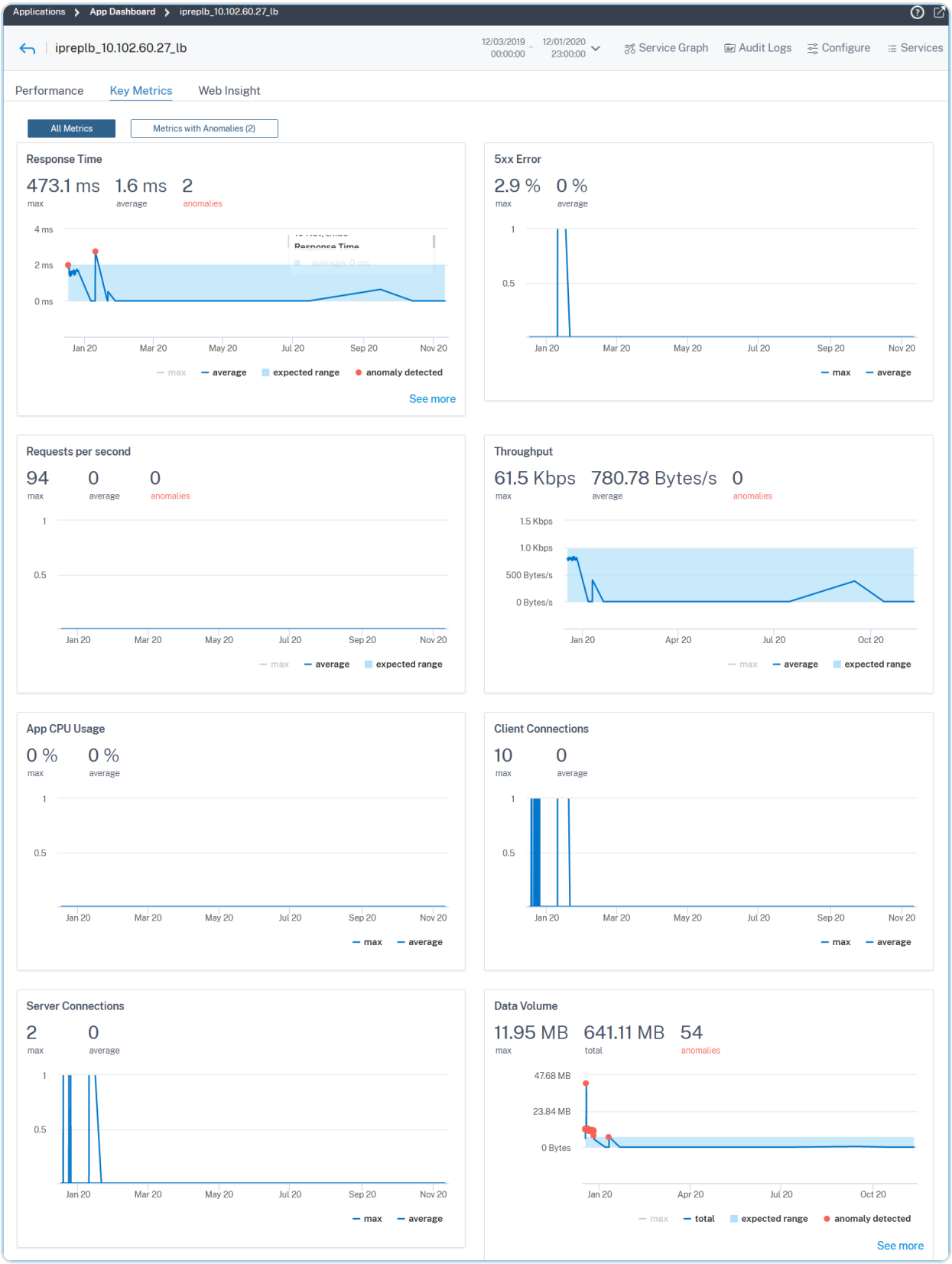
As an administrator, you must ensure how the application is getting utilized. The application key metrics can help you identify the application usage. Since the traffic range to the application is unpredictable, some unusual application performance deviations might occur for a specific duration. In such scenarios, as an administrator, you might want to view and analyze such sudden anomalies, and ensure if any immediate troubleshoot is required.

NetScaler® ADM detects such anomalies and provides necessary details. Navigate to **Applications > Dashboard**, click an application, and select the **Key Metrics** tab. NetScaler ADM monitors the traffic pattern and analyzes if the key metrics are in the expected range. If there is any deviation than the expected range, NetScaler ADM reports those deviations as anomalies.

You can view anomalies for the following key metrics:

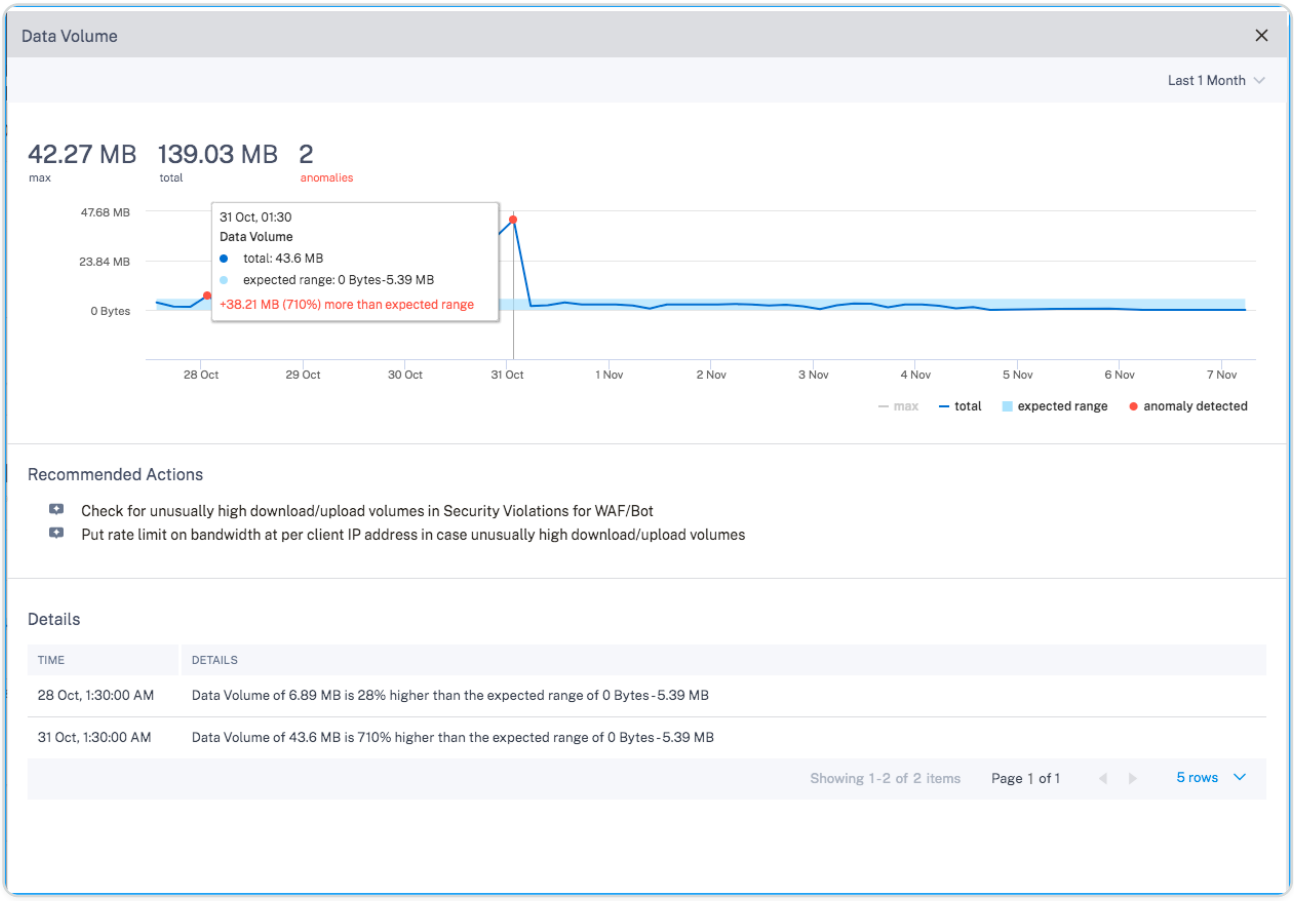
- Response Time
- Throughput
- Data Volume
- Requests per second

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In each metric, you can also click the **See more** option to view details. The following example is for the application data volume:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can view:

- The graph indicating the maximum value, total value, expected range, and anomalies
- The **Recommended Actions** to troubleshoot the issue
- The time and anomaly details under **Details**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application usage analytics

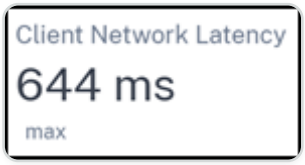
Application owners must have the ability to evaluate and visualize the complete application from the perspectives of performance and usage.

The improvised **App Dashboard** enables you to view all the application performances and usage metrics together. When you click an application, alongside the existing application performance metrics, the **Web Insight** tab displays the metrics details that help you:

- Understand your application usage.
- Correlate any performance deviations with the usage metrics.

NOTE

For each metric, you can view options that indicate maximum value and total value. For example:



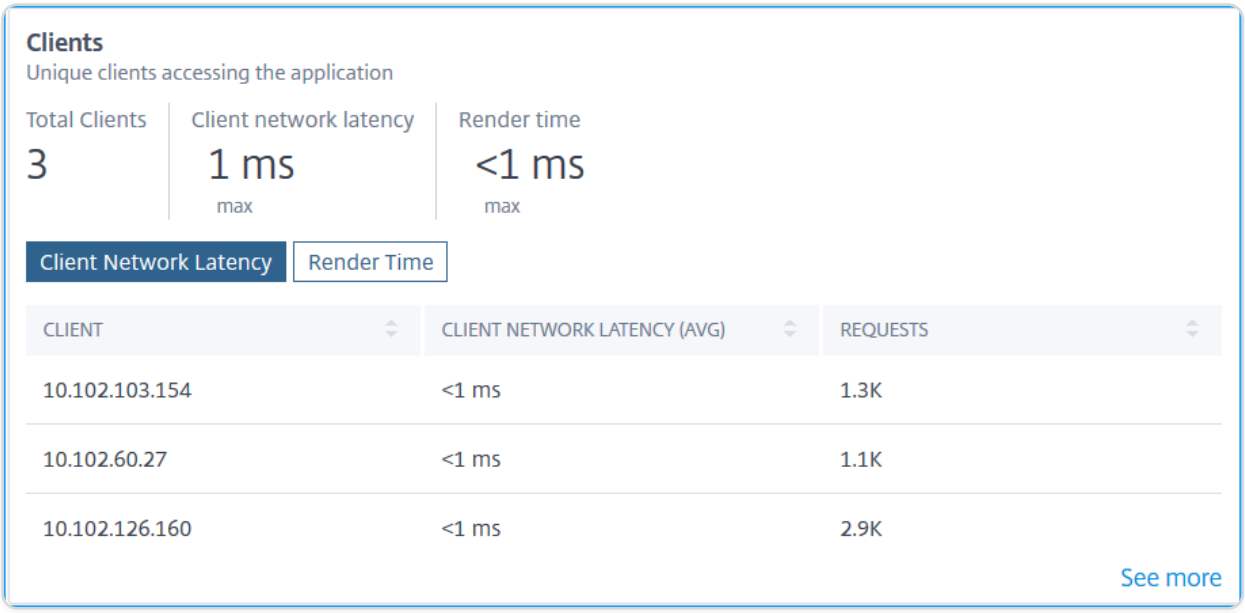
- The maximum client network latency for the selected duration. Consider that you have the network latency for client 1 = 644 ms, client 2 = 15 ms, and client 3 = 3 ms. In this scenario, the **Client Network Latency** displays 644 ms.

- The total bandwidth consumed across all available clients/servers for the selected duration. Consider that you have the bandwidth consumption for client 1 = 79.54 MB, Client 2 = 45 MB, Client 3 = 40 MB. In this scenario, the Bandwidth displays (79.54 MB + 45 MB + 40 MB) = 164.54 MB.

The following are the Web Insight metrics you can view from the **Usage** tab:

- **Clients** – Displays the insights for clients accessing the application:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



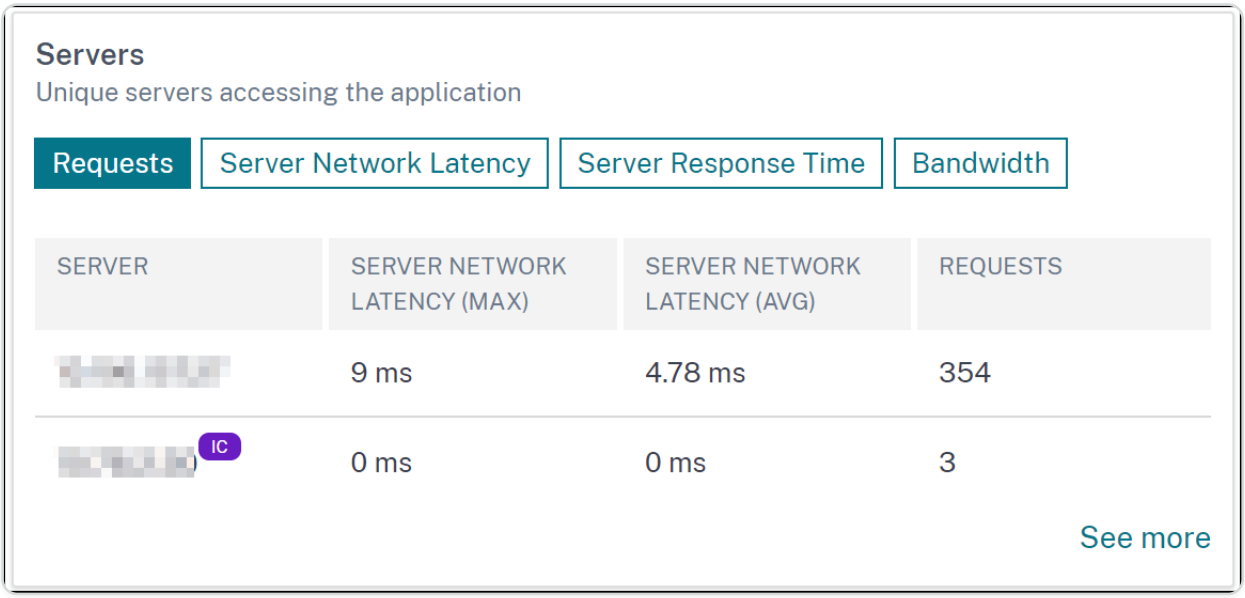
- **Total Clients** – Displays the total clients accessing the application.
- **Client Network Latency** – Displays the network latency from client to NetScaler. Click the **Client Network Latency** tab to view:
  - **Client** – The client IP address.
  - **Client Network Latency (avg)** – The average network latency from the client.
  - **Client Network Latency (max)** – The maximum network latency from the client.
  - **Requests** – The total requests from the client.
- **Render Time** – Displays the time taken to render the server response. Click the **Render Time** tab to view:
  - **Client** – The client IP address.
  - **Render Time (avg)** – The average render time from the client.
  - **Requests** – The total requests from the client.

- **Servers** – Displays the insights for servers accessing the application:

NOTE

For integrated cache requests, you can view the NetScaler virtual server IP address with an IC notification. For more information, see Integrated cache requests.

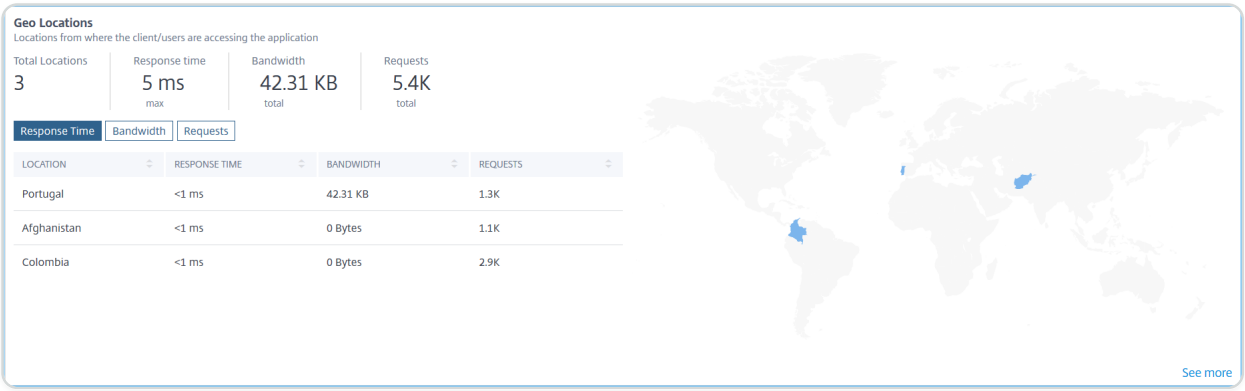
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Total Servers** – Displays the total servers accessing the application.
- **Server Network Latency** – Displays the network latency from the server to NetScaler. Click the **Server Network Latency** tab to view:
  - **Server** – The server IP address.
  - **Server Network Latency (avg)** – The average network latency from the server.
  - **Server Network Latency (max)** – The maximum network latency from the server.
  - **Requests** – The total requests from the server.
- **Server Response Time** – Displays the time taken for the server to respond to requests. Click the **Server Response Time** tab to view:
  - **Server** – The server IP address.
  - **Server Response Time (avg)** – The average response time from the server.
  - **Server Response Time (max)** – The maximum response time from the server.
  - **Requests** – The total requests from the server.
- **Bandwidth** – Displays the total bandwidth consumed by the servers. Click the **Bandwidth** tab to view:
  - **Server** – The server IP address.
  - **Bandwidth** – The total bandwidth consumed from the server.
  - **Requests** – The total requests from the server.

- **Geo Locations** – Displays the insights for clients accessing the application from a particular location:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

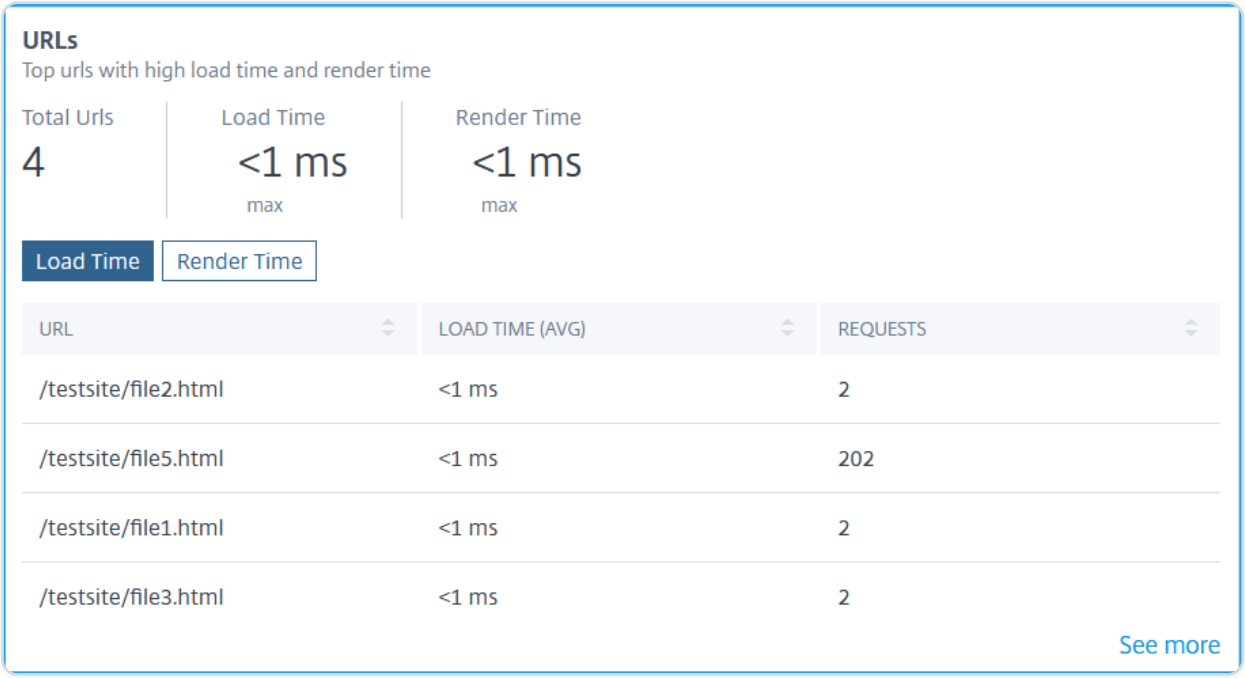


- **Total locations** – Displays the total client locations accessing the application.
- **Response Time** – Displays the response time from the client location.
- **Bandwidth** – Displays the total bandwidth consumed by clients across all locations.
- **Requests** – Displays the total requests from all client locations.

  Click each tab to view:

  - **Location** – The location name.
  - **Response Time** – The average response time from the client location.
  - **Bandwidth** – The bandwidth consumed from the client location.
  - **Requests** – The total requests from the client location.

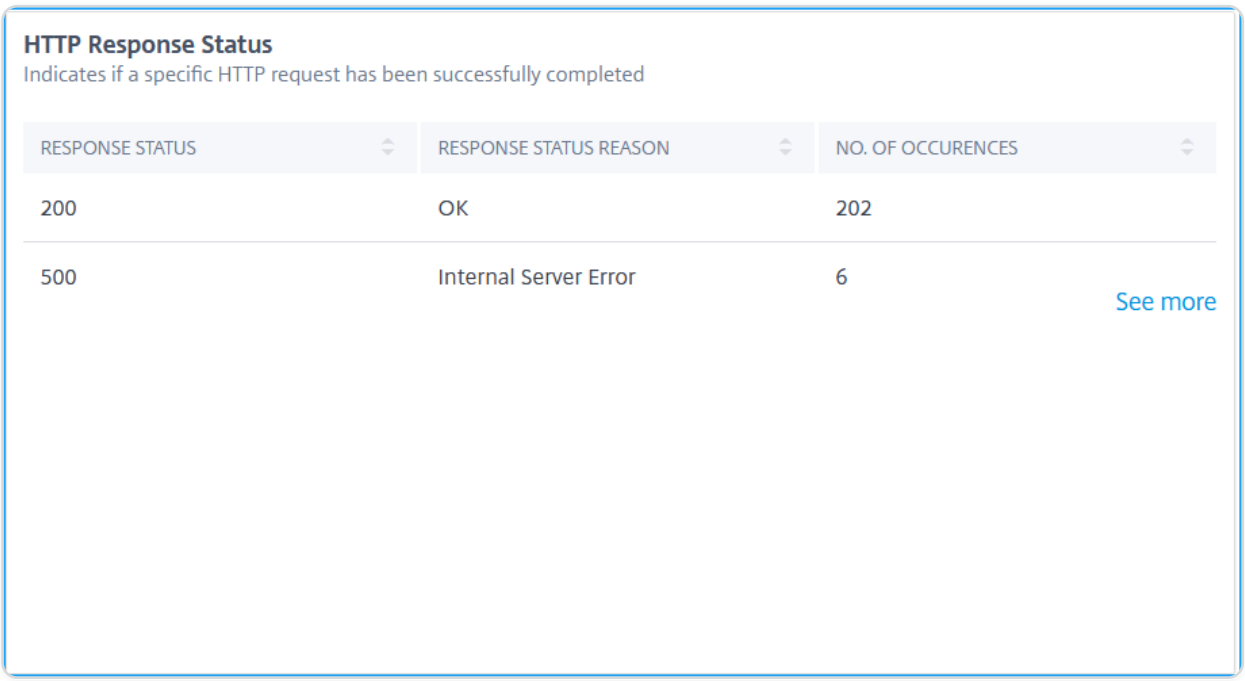
- **URLs** – Displays the insights for URLs with high load and render time:



  - **Total URLs** – Displays the total URLs.
  - Load Time – Displays the time taken for the URL to load. Click the **Load Time** tab to view:

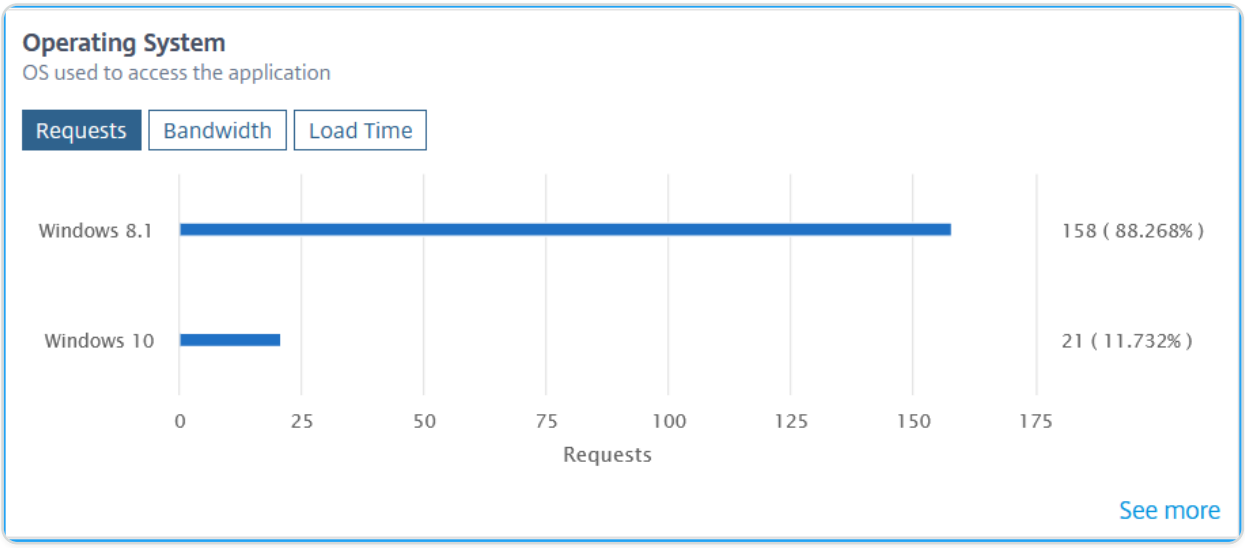
© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **URL** – The URL name.
    - **Load Time (avg)** – The average time taken for the URL to load.
    - **Requests** – The total requests from the URL.
  - **Render Time** – Displays the time taken for the URL to render and display. Click the **Render Time** tab to view:
    - **URL** – The URL name.
    - **Render Time (avg)** – The average time taken for the URL to render.
    - **Requests** – The total requests from the URL.
- **HTTP Response Status** – Displays the insights for a specific completed HTTP request.



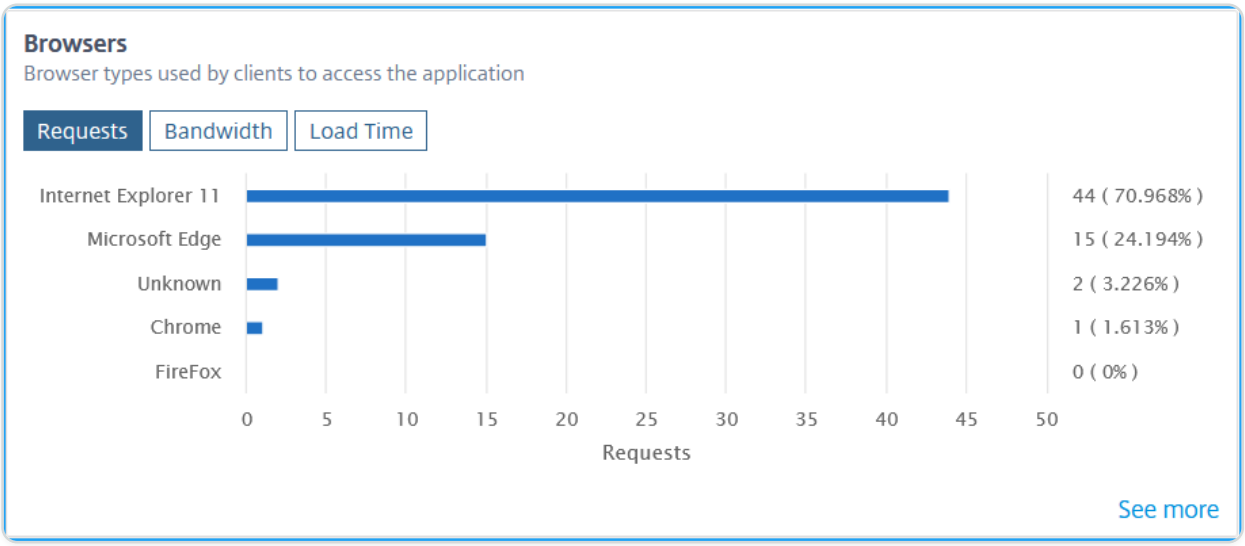
  - **Response Status** – Displays the response code such as 2xx, 4xx, 5xx, and so on.
  - **Response Status Reason** – Displays the response reason such as internal server error, Not found, and so on.
  - **No of Occurrences** – Displays the total number of occurrences.
- **Operating system** – Displays the insights for the OS accessing the application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Requests** – Displays the total requests from each operating system.
- **Bandwidth** – Displays the total bandwidth consumed by each operating system.
- **Load Time** – Displays the total time taken from each operating system to load from the server.

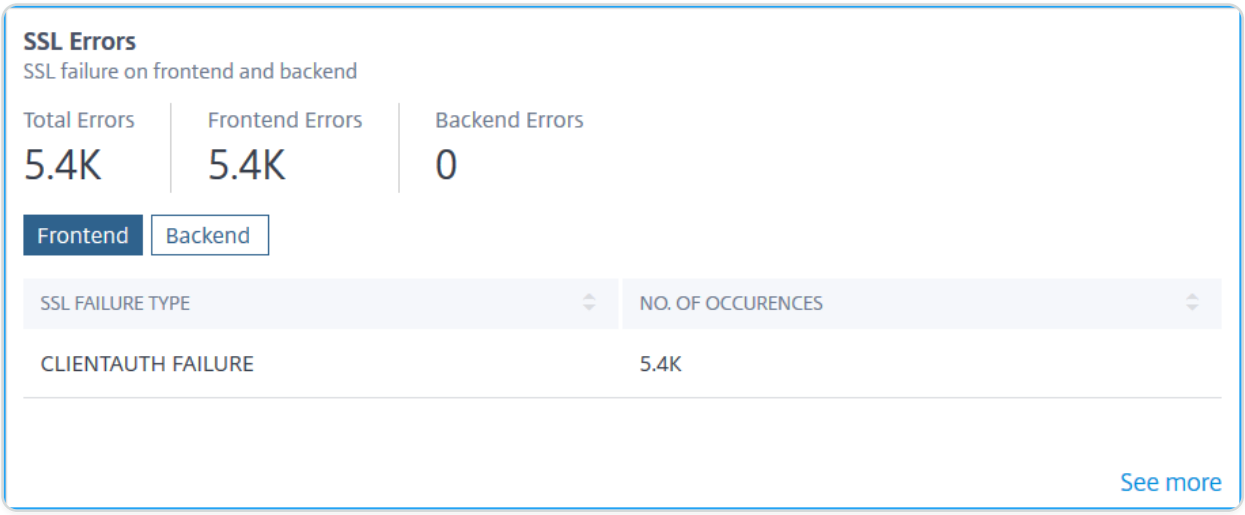
- **Browsers** – Displays the insights for the browser types used by the clients to access the application.



- **Requests** – Displays the total requests from each browser.
- **Bandwidth** – Displays the total bandwidth consumed by each browser.
- **Load Time** – Displays the total time taken for a browser to load from the server.

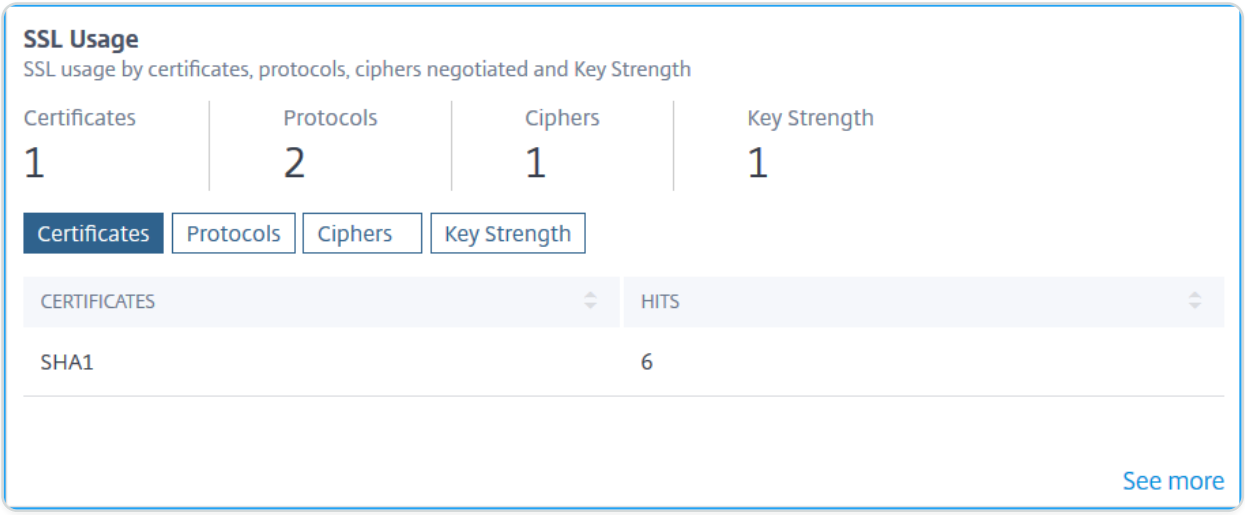
- **SSL Errors** – Displays the insights for the SSL errors from front-end server and back-end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Total Errors** – Displays the total SSL error occurrences.
- **Frontend** – Displays the total SSL errors from the front-end server. Click the **Frontend** tab to view the SSL error type and total occurrences.
- **Backend** – Displays the total SSL errors from the back-end server. Click the **Backend** tab to view the SSL error type and total occurrences.

- **SSL Usage** – Displays the insights for the SSL usage such as SSL certificates, protocols, Ciphers, and Key Strength.



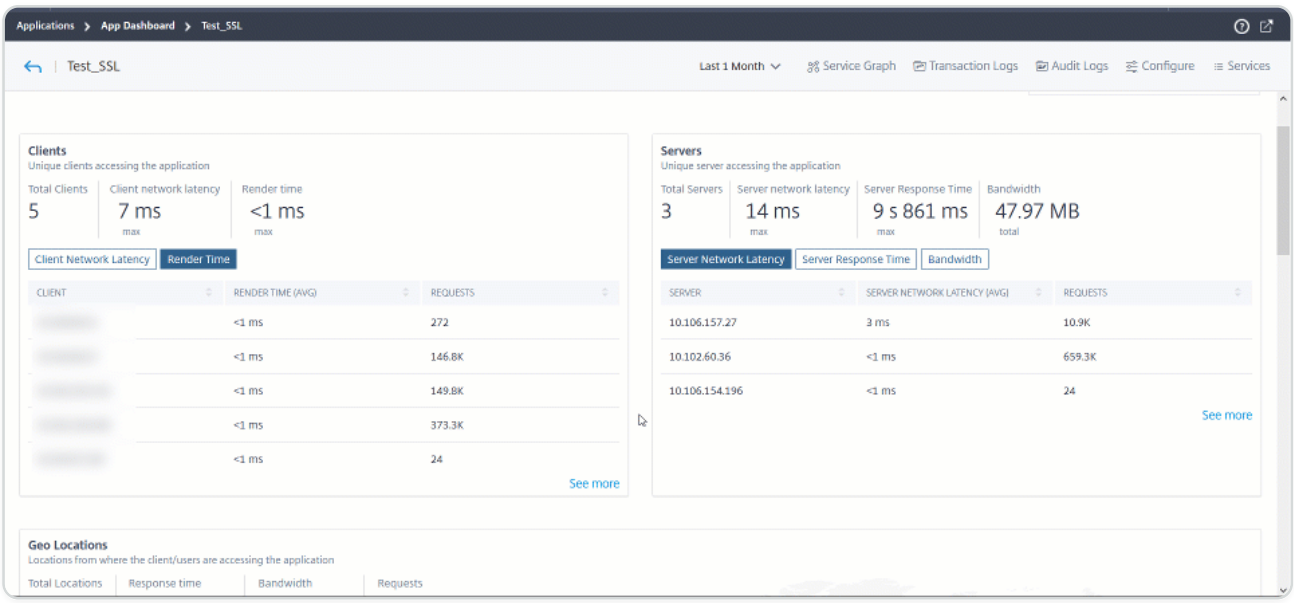
- **Certificates** – Displays the total SSL certificates. Click the **Certificates** tab to view the certificate name and total hits.
- **Protocols** – Displays the total SSL protocols. Click the **Protocols** tab to view details with SSL/TSL protocol and total hits.
- **Ciphers** – Displays the total Ciphers. Click the **Ciphers** tab to view details for each cipher suite name and total hits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Key Strength** – Displays the total key strength used in SSL certificates. Click the **Key Strength** tab to view details for each key strength and total hits.

View metrics details in graphical format

For each metric, you can view more details in a graphical format by clicking **See more** option. Click **>** to view details in a graphical format.



The following are the details you can view for each metric after you click the **See more** option:

INSIGHT NAME	METRICS	DESCRIPTION
Clients	Clients	Denotes the client list
	Render Time (AVG)	Denotes the average time taken for the client to render the server response
	Client Network Latency (AVG)	Denotes the average network latency from the client to NetScaler instance
	Requests	Denotes the total requests from the client
Servers	Server	Denotes the server list

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
	Server Processing Time (AVG)	Denotes the average time taken for the server to process the requests
	Server Network Latency (AVG)	Denotes the average network latency from the server to NetScaler instance
	Hits	Denotes the total hits received by the server
Geo Locations	Locations	Denotes the client locations
	Response Time	Denotes the total response time from the client location
	Bandwidth	Denotes the total bandwidth consumed from the location
	Requests	Denotes the total requests from the location
URL	Render Time (AVG)	Denotes the average time taken to load the page from the server
	Load Time (AVG)	Denotes the average time taken for the URL to render and display
	Hits	Denotes the total hits from the URL
HTTP Response Status	Name	Denotes the response status name such as OK, Not found, Internal Server Error, and so on
	Response Status	Denotes the response status code received from the server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
		such as 200, 400, 500, and so on
	Hits	Denotes the total hits from the response code
	Bandwidth	Denotes the total bandwidth consumed
Operating System	Operating System	Denotes the operating system name such as Windows, MAC
	Load Time	Denotes the total time taken for the operating system to load from the server
	Bandwidth	Denotes the total bandwidth consumed by the operating system
	Requests	Denotes the total requests from the operating system
Browsers	Browsers	Denotes the browser name such as Mozilla Firefox, Chrome, and so on
	Load Time	Denotes the total time taken for a browser to load from the server
	Bandwidth	Denotes the total bandwidth consumed by the browser
	Requests	Denotes the total requests from the browser
SSL Errors	SSL Failure Type	Denotes the error name such as CLIENTAUTH FAILURE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
	Occurrences	Denotes the total occurrences for the SSL error
SSL Usage	Denotes the protocol name and versions such as TLS, SSL	
	Hits	Denotes the total hits from the protocol

Troubleshoot Web Insight issues

For details, see the troubleshooting document Troubleshoot Web Insight issues

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Insight dashboard

The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and NetScaler instances. This improved Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, you can view Web Insight for:

- An application. Navigate to **Applications > Dashboard**, click an application, and select **Web Insight** tab to view the detailed metrics. For more information, see Application Usage Analytics.
- All applications. Navigate to **Applications > Web Insight** and click each tab (Applications, Clients, Instances) to view the following metrics:

APPLICATIONS	CLIENTS	INSTANCES
Applications	Clients	Instance Metrics
Servers	Geo Locations	Applications
Domains	HTTP Request Methods	Domains
Geo Locations	HTTP Response Status	URLs
URLs	URLs	HTTP Request Methods
HTTP Request Methods	Operating System	HTTP Response Status
HTTP Response Status	Browsers	Clients
SSL Errors	SSL Errors	Servers
SSL Usage	SSL Usage	Operating System
		Browsers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications Clients Instances Last 1 Month

Applications
Top apps with high bandwidth and response time

Requests | Bandwidth | Response Time

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
lb_114	9.15 MB	923 ms	14.9K
SSL_VS	0 Bytes	<1 ms	121
test_vs_ssl	0 Bytes	<1 ms	121
k8s-10.244.2.112_80_http	55.07 KB	20 ms	81
vpn_gw	0 Bytes	<1 ms	12

See more

Servers
Unique servers accessing the application

Requests | Server Network Latency | Server Response Time | Bandwidth

SERVER	SERVER NETWORK LATENCY (...	REQUESTS
10.102.103.113	921 ms	14.9K
10.102.71.225	<1 ms	121
10.102.71.226	<1 ms	121
10.244.1.95	<1 ms	23
10.102.71.228	<1 ms	12

See more

Domains
Top domains

Requests | Bandwidth | Response Time

DOMAIN	BANDWIDTH (AVG)	REQUESTS
10.102.103.99	8.51 MB	14.4K
--NA--	513.6 KB	453
10.102.103.99:80	62.67 KB	52
netflix-frontend-service	14.82 KB	23
recommendation-engine-s...	8.75 KB	12

See more

Geo Locations
Locations from where the clients/users are accessing the applications

Total Locations	Response Time	Bandwidth	Requests
1	20.51 s (max)	16.56 MB (total)	15.3K (total)

Requests | Response Time | Bandwidth

LOCATION	RESPONSE TIME	BANDWIDTH	REQUESTS
*	95 ms	16.56 MB	15.3K

See more

URLs
Top urls with high load time and render time

Total Urls	Load Time	Render Time
5.7K	<1 ms (max)	<1 ms (max)

Requests | Load Time | Render Time

URL	LOAD TIME (AVG)	RENDER TIME (AVG)	REQUESTS
/	<1 ms	<1 ms	446
/console/login/LoginForm.jsp	<1 ms	<1 ms	139
/index.php	<1 ms	<1 ms	116
/q79w_38jg__.shtml	<1 ms	<1 ms	96
/admin_ui/mas/ent/login.html	<1 ms	<1 ms	79

See more

HTTP Request Methods
Indicates HTTP request methods used to access the applications

REQUEST METHODS	BANDWIDTH	NO. OF OCCURENCES
GET	8.65 MB	14.5K
POST	459.6 KB	368
Unknown	35.85 KB	324
HEAD	17.1 KB	39
OPTIONS	35.1 KB	18

HTTP Response Status
Indicates if a specific HTTP request has been successfully completed

RESPONSE STATUS	RESPONSE STATUS REASON	NO. OF OCCURENCES
404	Not Found	12.2K
401	Unauthorized	2.2K
302	Found	337
0	Unknown	254
200	OK	152

In each metric, you can view the top 5 results. You can click to drill down further to analyze the issue and take troubleshooting actions faster.

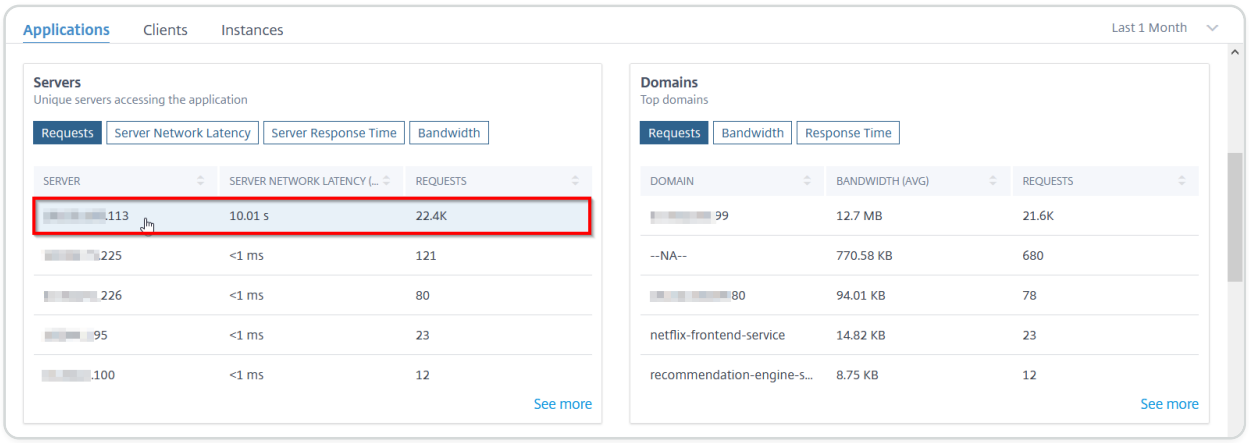
Note

> In some scenarios, NetScaler might not be able to calculate the RTT values for some transactions. For such transactions, NetScaler ADM displays the RTT values as

- **NA** – Displays when the ADC instance cannot calculate the RTT.
- **< 1ms** – Displays when the ADC instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

For example, consider that you want to analyze the server network latency for 1-month time duration and take decision whether to scale up or scale down the production environment. To analyze this:

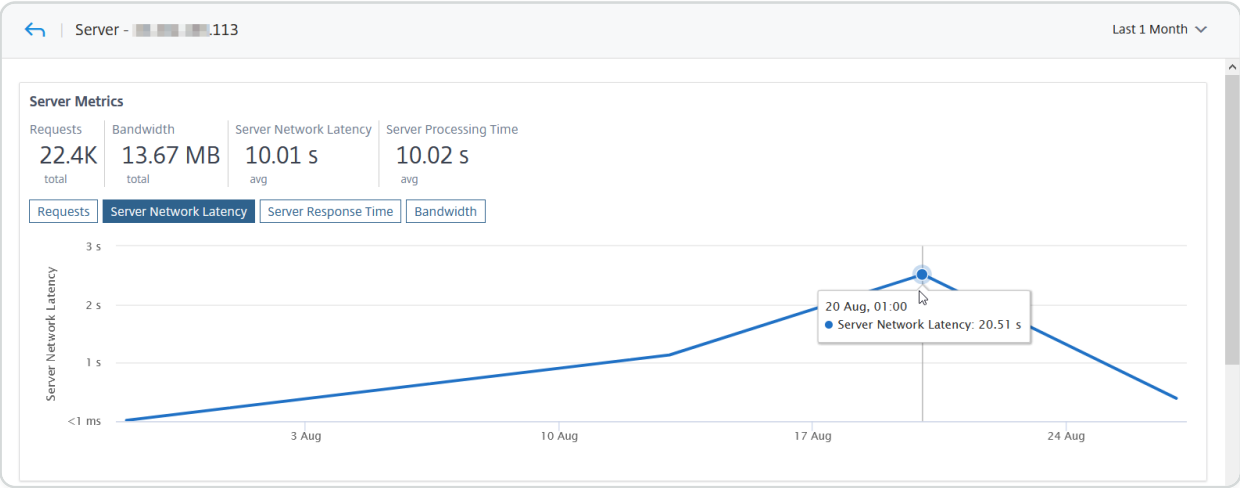
1. Select Last 1 Month from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.



   The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

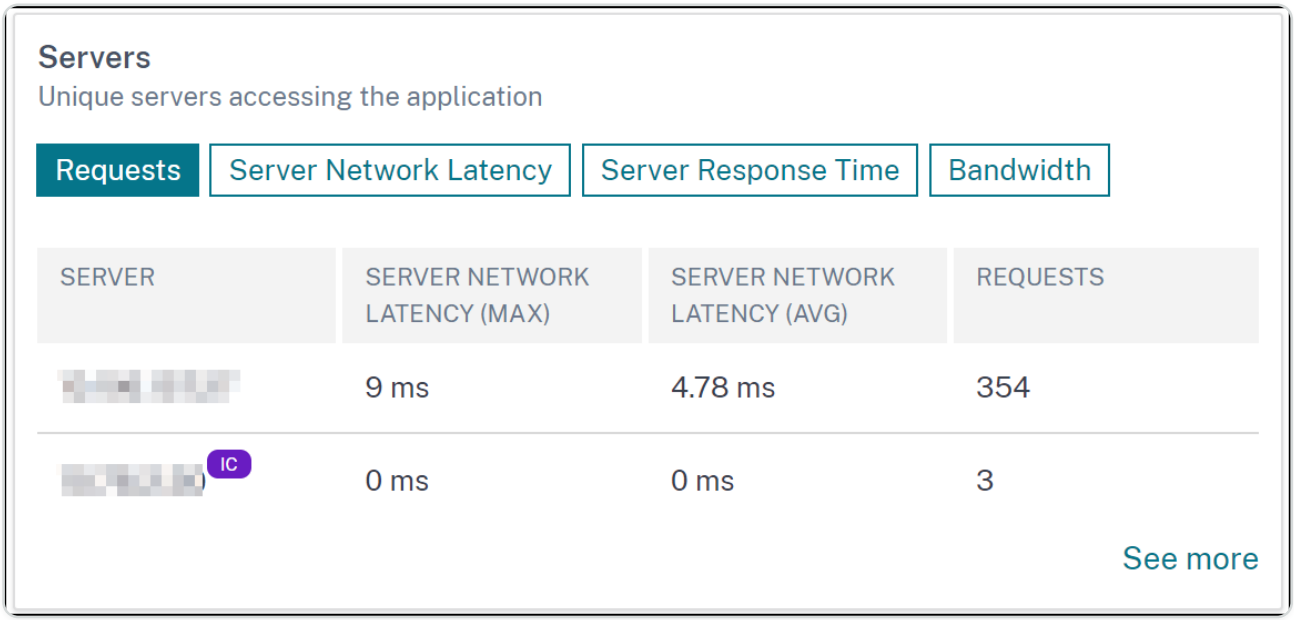


The average latency indicates 10.01 s and from the graph, you can analyze that the server network latency for the last 1 month seems to be high. As an administrator, you can take decision to scale up the production environment.

Integrated cache requests

The integrated cache provides in-memory storage on the NetScaler appliance and serves Web content to users without requiring a round trip to an origin server.

The integration cache requests are currently visible under **Servers** with an IC notification next to the ADC virtual server IP address. All other requests are visible with the origin server IP address.

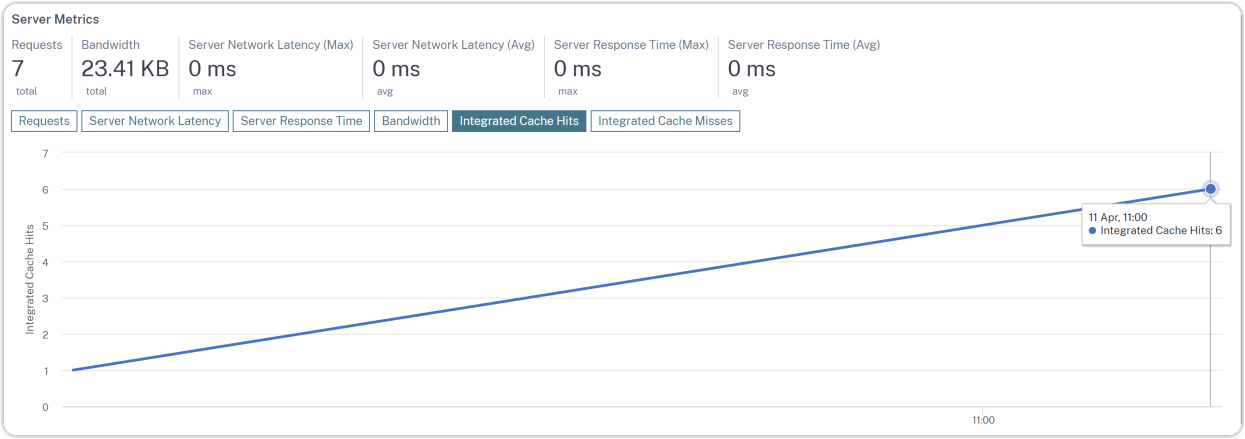


When you drill down a server to view more details, the **Server Metrics** display integrated cache hits and misses tabs.

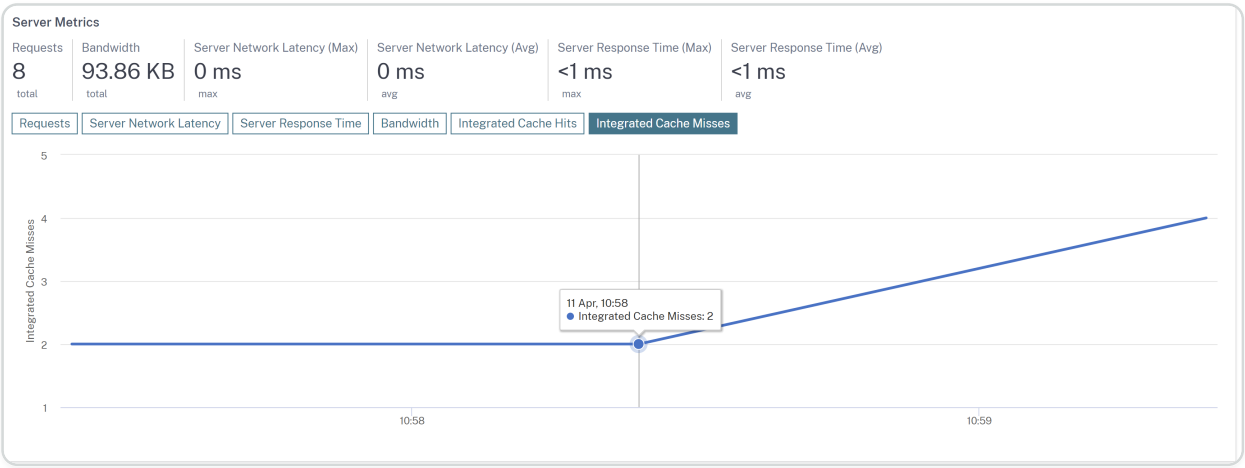
The graph view in:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.



- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.



Troubleshoot Web Insight issues

For details, see the troubleshooting document Troubleshoot Web Insight issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Graph

The service graph feature in NetScaler® ADM enables you to monitor all services in a graphical representation. This feature also enables you to view a detailed analysis and actionable metrics of the services. You can view service graph for:

- Applications configured across all NetScaler instances
- Kubernetes applications
- 3-tier Web applications

Service graph for applications across all NetScaler instances

The global service graph feature enables you to get a holistic visualization of the `clients to infrastructure to application` view. From this single-pane service graph view, as an administrator, you can:

- Understand from which region the users are accessing the specific applications (3-tier Web apps and microservices app)
- Visualize the infrastructure (NetScaler instance) view that the client request is processed
- Understand if the issues are occurring from the client, infrastructure, or application
- Further drill down to troubleshoot the issue

Navigate to **Applications > Service Graph** and click the **Global** tab to view:

- End-to-end details of all applications connected from client to back-end servers
- All NetScaler instances that are connected to its respective data centers

  NOTE

  You can view data centers only if you have GSLB apps.

- The client metrics information

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The NetScaler metrics information
- All NetScaler instances that have discrete applications, custom applications, and discrete microservice applications
- The top 4 low-scored applications that belong to custom apps, discrete apps, and microservices apps
- The metrics information for the top 4 low-scored virtual servers
- The applications (discrete apps, custom apps, and microservices apps) status such as **Critical**, **Review**, **Good**, and **Not Applicable**.

For more information, see Holistic view of applications in service graph.

Service graph for Kubernetes applications

Navigate to **Applications > Service Graph** and click the **Microservices** tab to view:

- Ensure end-to-end application overall performance
- Identify bottlenecks created by inter-dependency of different components of your applications
- Gather insights into the dependencies of different components of your applications
- Monitor services within the Kubernetes cluster
- Monitor which service has issues
- Check the factors contributing to performance issues
- View detailed visibility of service HTTP transactions
- Analyze the HTTP, TCP, and SSL metrics

By visualizing these metrics in NetScaler ADM, you can analyze the root cause of issues and take necessary troubleshooting actions faster. Service graph displays your applications into various component services. These services running inside the Kubernetes cluster can communicate with various components within and outside the application. To get started, see Setting up service graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph for 3-tier Web applications

Navigate to **Applications > Service Graph** and click the **Web Apps** tab to view:

- Details on how the application is configured (with content switching virtual server and load balancing virtual server)

  For GSLB applications, you can view data center, ADC instance, CS, and LB virtual servers.
- End-to-end transactions from client to service
- The location from where the client is accessing the application
- The data center name where the client requests are processed and the associated data center NetScaler metrics (only for GSLB applications)
- Metrics details for client, service, and virtual servers
- If the errors are from the client or from the service
- The service status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the service status based on service response time and error count.
  - **Critical (red)** - Indicates when average service response time > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average service response time > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average service response time < 200 ms
- The client status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the client status based on client network latency and error count.
  - **Critical (red)**- Indicates when average client network latency > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average client network latency > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average client network latency < 200 ms
- The virtual server status such as **Critical**, **Review**, and **Good**. NetScaler ADM displays the virtual server status based on the app score.
  - **Critical (red)** - Indicates when app score < 40

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Review (orange)** - Indicates when app score is between 40 and 75
- **Good (green)** - Indicates when app score is > 75

Points to note:

- Only Load Balancing, Content Switching, GSLB virtual servers are displayed in service graph.
- If no virtual server is bound to a custom application, the details are not visible in service graph for the application.
- You can view metrics for clients and services in service graph only if active transactions occur between virtual servers and web application.
- If no active transactions available between virtual servers and web application, you can only view details in service graph based on the configuration data such as load balancing, content switching, GSLB virtual servers, and services.
- If any changes made in the application configuration, it may take 10 minutes to reflect in service graph.

For more information, see Service graph for applications.

Service graph for Kubernetes apps

Use the service graph for Kubernetes apps to visualize, monitor, and troubleshoot the microservices in your Kubernetes cluster. The following topics help you set up, view, and analyze the service graph:

- Setting up service graph
- View details in service graph
- Configure thresholds in service graph
- View service details
- View ingress details for troubleshooting
- Distributed tracing
- View diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting up service graph

Software requirements

KUBERNETES DISTRIBUTION	KUBERNETES VERSION	CONTAINER NETWORK INTERFACES (CNI)	CPX VERSION	CIC VERSION	NETSCALER ADM VERSION	NETSCALER AGENT VERSION
Open source	v1.16.3	Flannel, Calico, or Canal	13.0–41.28 or later	1.5.25 or later	13.0–47.22 or later	13.0–47.22 or later

You can configure the Kubernetes cluster with various deployment topologies and the following table provides the topologies that are supported in service graph:

TOPOLOGY	SUPPORTED IN SERVICE GRAPH
Single-Tier or Unified ingress	Yes
Dual-Tier	Yes
Cloud	Yes, but cloud load balancer is not shown in the graph
Service mesh lite	Yes
Service mesh	Yes
Services of type LoadBalancer	No
Services of type NodePort	No

To complete setting up service graph in NetScaler® ADM, click the topology type that you have configured for your Kubernetes cluster and complete the mentioned procedures:

- Single-tier or Unified ingress topology
- Dual-tier or Service Mesh Lite topology
- Service mesh topology

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The procedure to set up service graph for dual-tier and service mesh lite topologies remains the same.

Before you begin

You can view service graph using the following scenarios:

- NetScaler ADM and Kubernetes cluster on the same network (for example, NetScaler ADM and Kubernetes cluster hosted on the same Citrix Hypervisor™).
- NetScaler ADM and Kubernetes cluster on a different network. In this scenario, you must configure an on-prem agent and register the agent on the network, where Kubernetes cluster is hosted.

Single tier or Unified ingress topology

Ensure that you have:

- Configured Kubernetes cluster with single tier or unified ingress topology.
- Added VPX, MPX, SDX, BLX instance in NetScaler ADM and enabled **Web Insight**.
- Added Kubernetes cluster in NetScaler ADM.

Dual tier or Service Mesh Lite topology

Ensure that you have:

- Configured Kubernetes cluster with any one of the supported topologies.
- Configured static routes on NetScaler ADM to enable communication between NetScaler ADM and NetScaler CPX.

  NOTE

  You can ignore this procedure if you have deployed NetScaler ADM as a microservice in the same cluster.

- Downloaded the sample deployment files from GitHub repository.
- Added required parameters in CPX YAML file to ensure successful CPX registration with NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Added a VPX, MPX, SDX, or BLX instance in NetScaler ADM.
- Added the Kubernetes cluster in NetScaler ADM.
- Deployed a sample microservice application.
- Deployed NetScaler CPX and registered CPX to ADM (applicable only for two-tier architecture)
- Enabled Auto-select Virtual Servers to license the virtual servers.
- Enabled Web transaction and TCP transaction settings to **All** for NetScaler agent to get HTTP and TCP transactions.
- Sent traffic to microservices.

Service mesh topology

Ensure that you have:

- Configured Kubernetes cluster version `1.14.0` with any one of the following service mesh topologies:
  - NetScaler CPX as a sidecar proxy for Istio
  - NetScaler as an Ingress Gateway for Istio
- Enabled `admissionregistration.k8s.io/v1beta1` API. You can verify the API by using:

  `kubectl api-versions | grep admissionregistration.k8s.io/v1beta1`

  The following output indicates that the API is enabled:

  `admissionregistration.k8s.io/v1beta1`
- Installed Istio `istio v.1.3.0`.
- Installed Helm version 3.x.
- Configured static routes on NetScaler ADM to enable communication between NetScaler ADM and NetScaler CPX.

  NOTE

  You can ignore this procedure if you have deployed NetScaler agent as a microservice in the same cluster.

- Configured the required parameters to populate the service mesh topology data.
- Deployed a sample application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Added the Kubernetes cluster in NetScaler ADM.
- Enabled Auto-select Virtual Servers to license the virtual servers.

> **NOTE**
>
> When CPX is deployed as a sidecar proxy in service mesh deployment, the virtual servers are licensed only if the IP address is matching with the CPX NS IP.

- Enabled Web transaction and TCP transaction settings to **All** for NetScaler agent to get HTTP and TCP transactions.
- Sent traffic to microservices.

View details in service graph

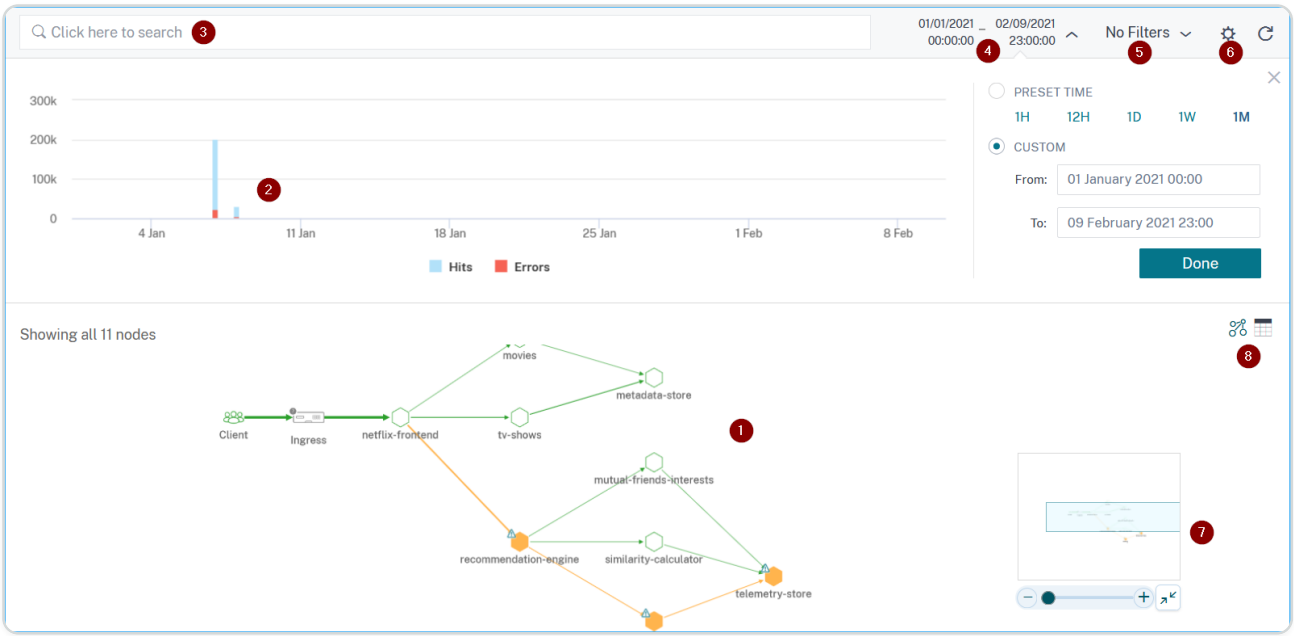
In NetScaler® ADM, navigate to **Applications > Service Graphs > Kubernetes service graph** and select the time duration from the list to view the service graph details.

TWO-TIER/SERVICE MESH LITE TOPOLOGY	SINGLE-TIER/UNIFIED INGRESS TOPOLOGY

- **Tier 1 ingress** – NetScaler Ingress Controller inside the Kubernetes cluster configures a NetScaler instance (VPX/MPX/SDX/BLX) outside the Kubernetes cluster.
- **Tier 2 ingress** – NetScaler Ingress Controller running as a sidecar along with NetScaler CPX instance inside the Kubernetes cluster.
- **Ingress** – Displays for all other deployment topologies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph dashboard



1 - End-to-end network map of your application that shows how your component services are communicating

2 – Graph that indicates hits and errors for a specific time duration

3 – Search bar to search for services

4 – Time list to select the time duration

5 - Apply filters to display services

6 – Setting icon

7 – Zoom in and zoom out view

8 – Graph view or tabular view

Based on the selected time duration, you can view the service graph.

SERVICE ICON	DESCRIPTION
	The edge width indicates the number of hits. The greater or more the edge width, indicates the number of hits is higher.
	Service with a warning icon indicates that the service has errors.

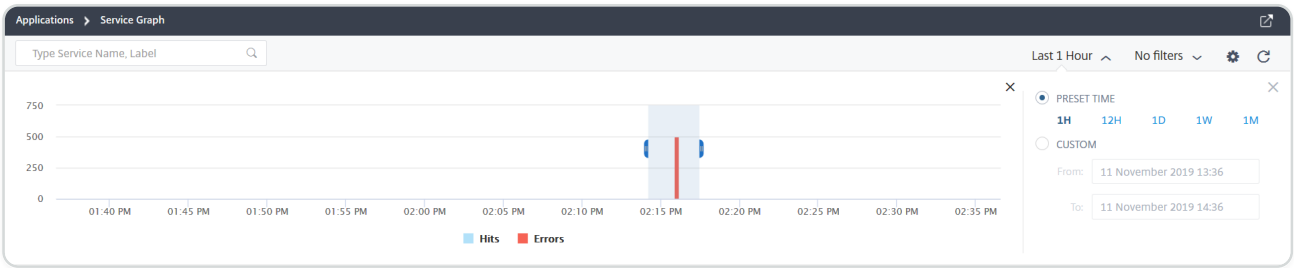
© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE ICON	DESCRIPTION
	Service with a stopwatch icon indicates that the service has latency or response time issues.
	Service with both stopwatch and warning icons indicate that the service has both errors and latency/response time issues.

NOTE

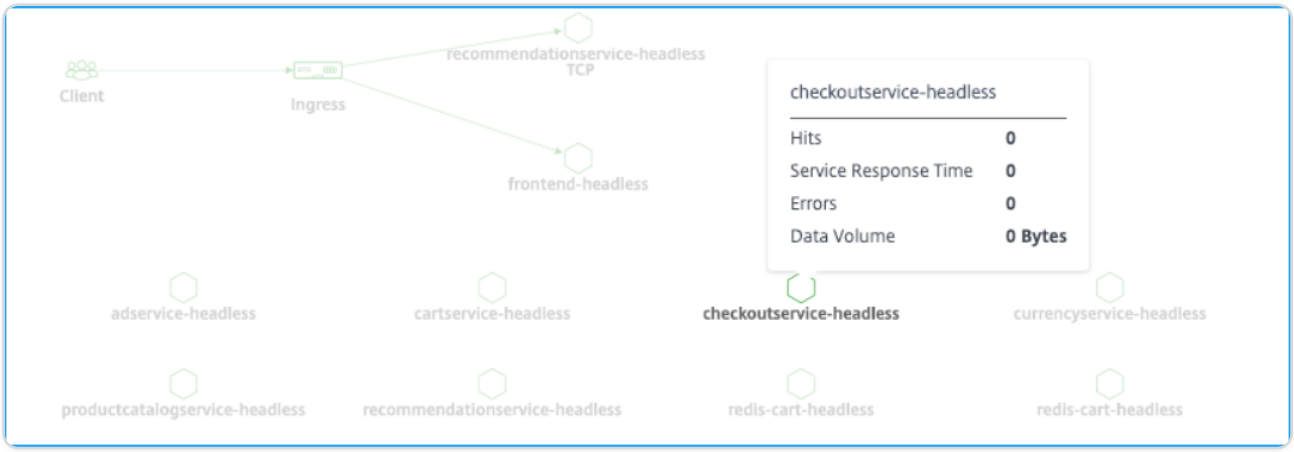
If a service has no warning or stopwatch icon, it indicates that the service has anomalies or threshold breach for Hits.

Based on the selected time duration, you can view the service graph. Select the time period from the graph that indicates hits to drill down further for additional information.



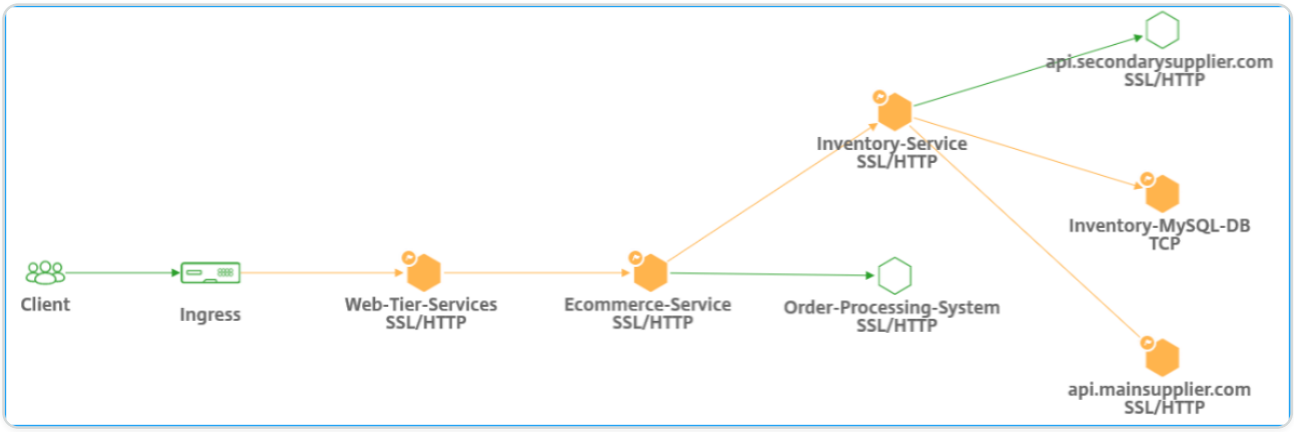
NOTE

If no active transactions received by NetScaler ADM, you can view only the services that are load balanced by the NetScaler instance. When you hover the mouse pointer on a service, all metrics are displayed as 0.



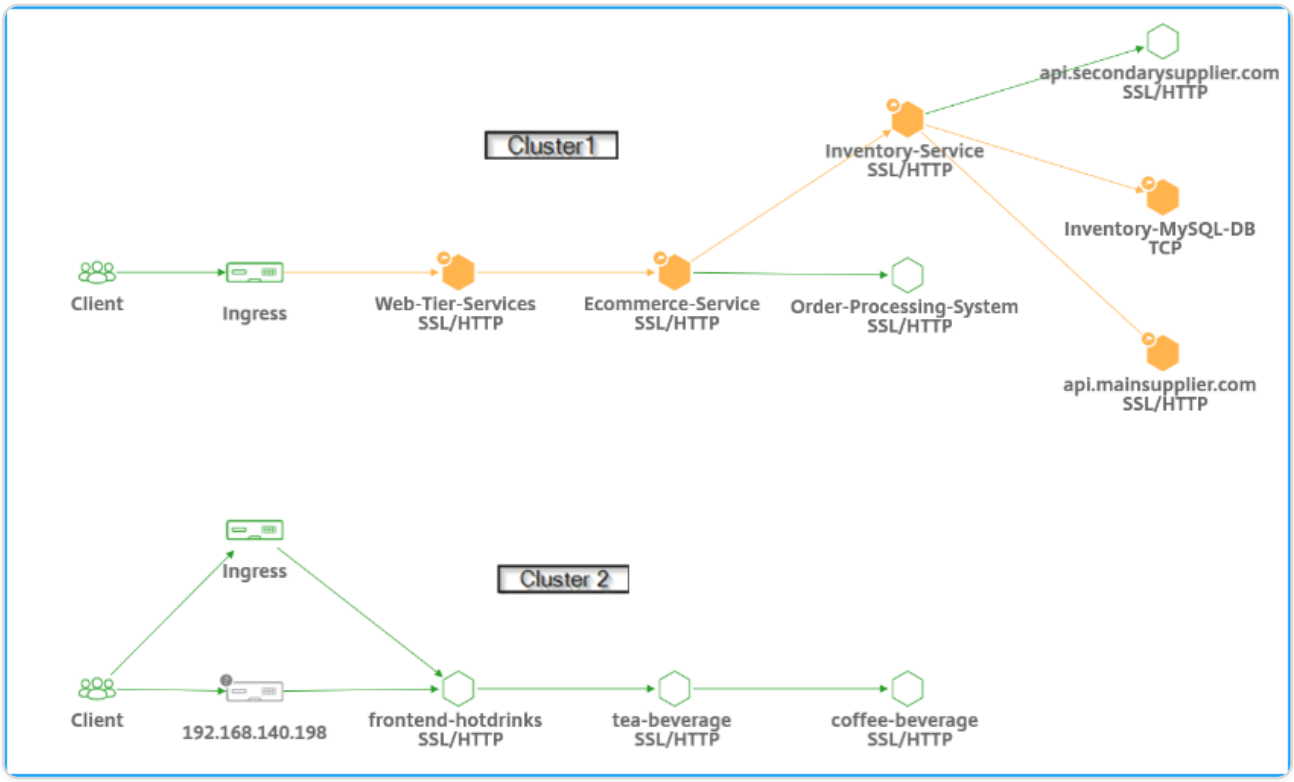
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The service graph is displayed with the protocol used by the services. Consider that you have the following services running in your Kubernetes cluster as shown in the image:



Note

> If you have added multiple clusters in **Orchestration** > **Kubernetes** > **Clusters**, you can view services associated with each cluster.



You can view the following status for your services:

- **Critical (red)** - Indicates when average service response time > 200 ms AND error count > 0
- **Review (orange)** - Indicates when average service response time > 200 ms OR error count > 0
- **Good (green)** - Indicates no error and average service response time < 200 ms

The following are protocols that enable you to identify the protocol used by a service:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TCP** – Indicates the service is using the TCP protocol.
- **SSL, HTTP** – Indicates the service is using the SSL over HTTP protocol.
- **SSL, TCP** – Indicates the service is using the SSL over TCP protocol.

> **NOTE**
>
> The service without a protocol indicates the service is using the HTTP protocol.

View key metrics trends using the tabular view

Using the tabular view, you can see:

- Key metrics for the service
- Key metrics between a source service to a destination service

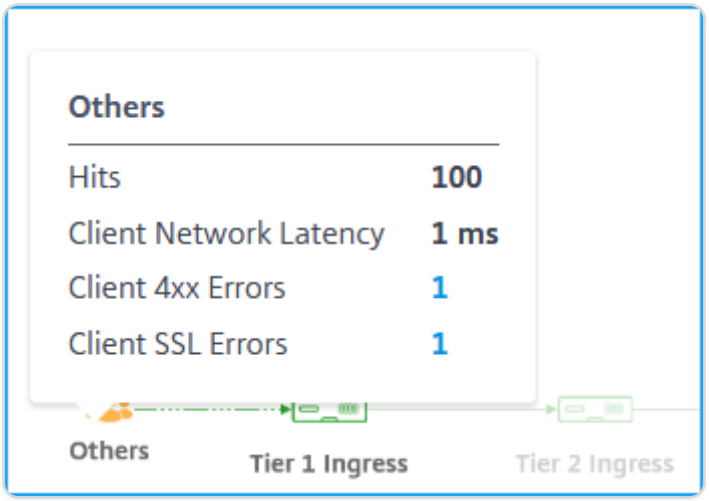
As an administrator, using these key metrics, you can analyze the trends of golden signals for the selected time duration.

View client metrics

You can view from which location the client is accessing the service. As an administrator, you can visualize the client metrics and analyze the issues that occur from the client.

Hover the mouse pointer on a client region to view the metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Hits** - Indicates the total hits received by the client.
- **Client Network Latency** - Indicates the average client network latency.
- **Client 4xx Errors** - Indicates the total client 4xx errors.
- **Client SSL Errors** - Indicates the total client SSL errors.

IP blocks in NetScaler ADM - NetScaler ADM can recognize the client location if the client uses a public IP address. NetScaler ADM has its built-in location CSV file that matches the location based on the client IP address range.

NetScaler ADM can recognize the client location with private IP address only when the IP address is added to the NetScaler ADM server. For example, if the client IP address falls within a private IP address range associated with City A, NetScaler ADM recognizes that the traffic is originating from City A for this client.

Create a private IP block

NetScaler ADM can recognize the location of a client when the client private IP address is added to the NetScaler 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, NetScaler ADM recognizes that the traffic is originating from City A for this client.

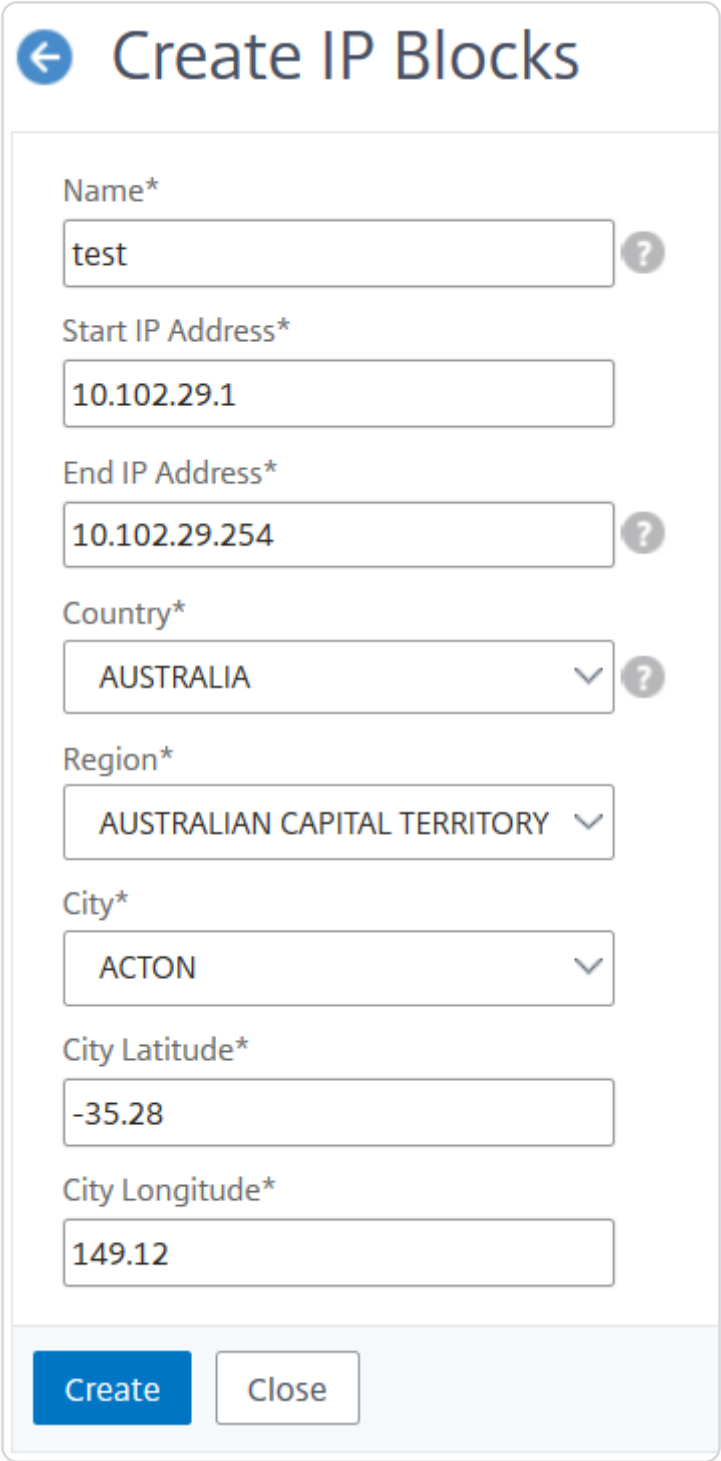
To create an IP block:

1. In NetScaler ADM, navigate to **Settings** > **Analytics Settings** > **IP Blocks**, and then click **Add**.
2. In **Create IP Blocks** page, specify the following parameters:
    - **Name**. Specify a name for the private IP block
    - **Start IP address**. Specify the lowest IP address range for the IP block.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.



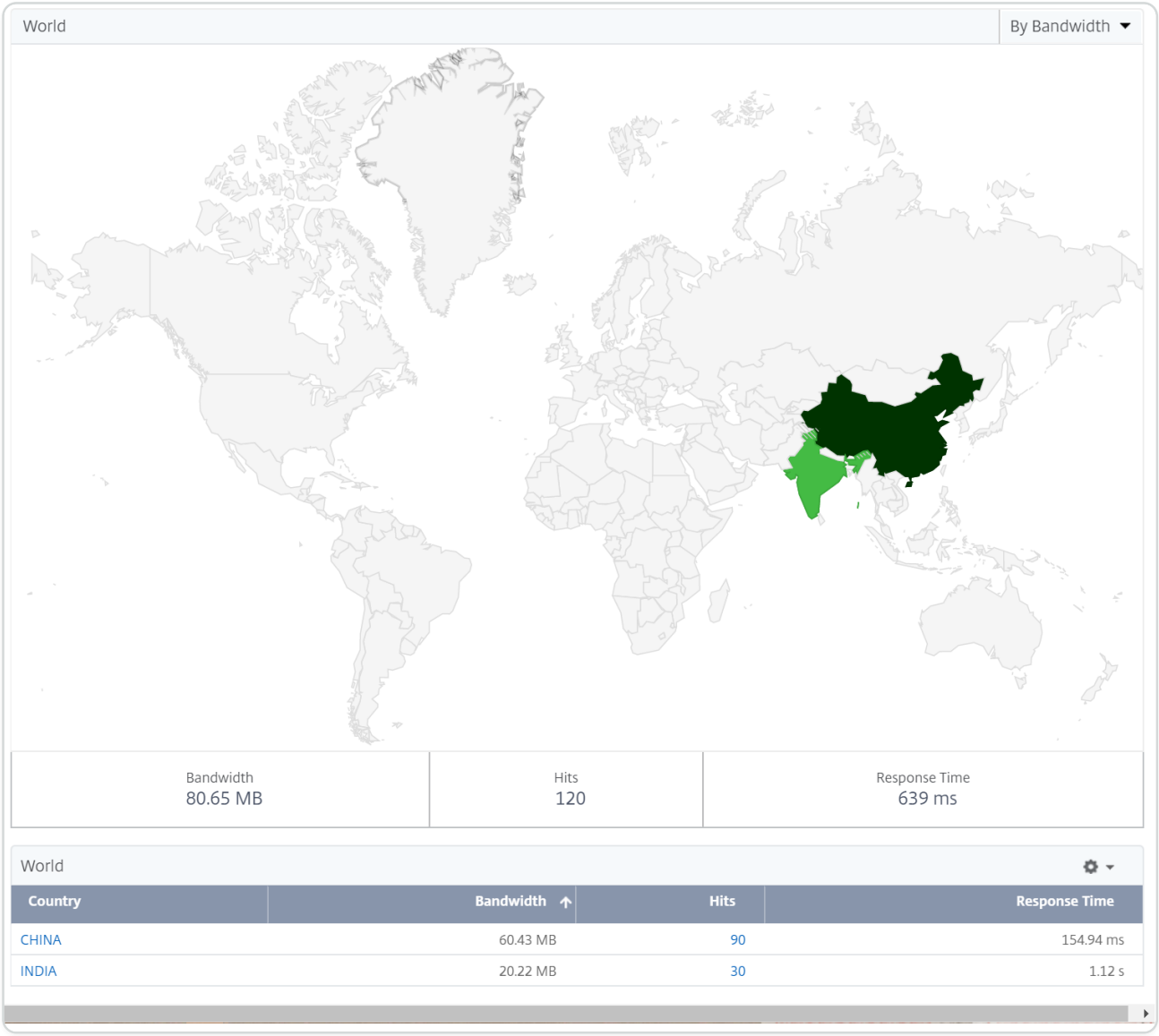
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Public IP blocks

NetScaler ADM can also recognize the location of a client if the client uses public IP address. NetScaler 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

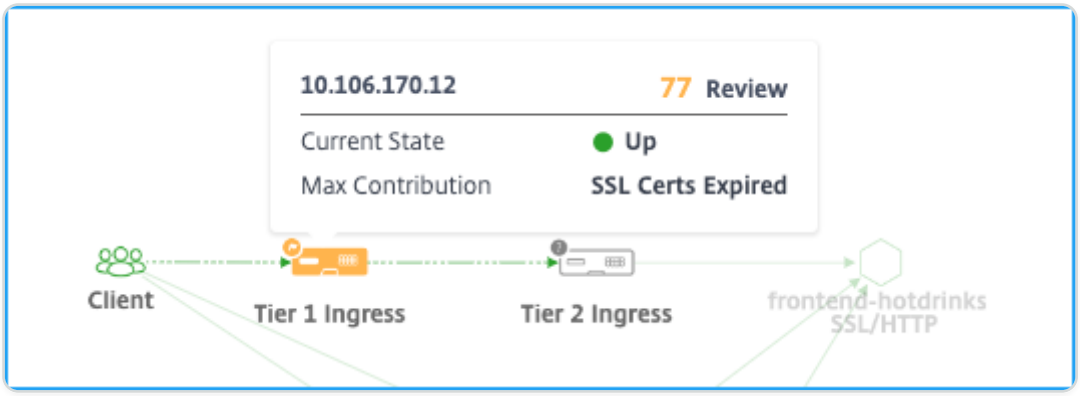
> NetScaler ADM requires an internet connection to display the geomaps for a particular geographical location. Internet connection is also required to export the GeoMap in .pdf, .png, or .jpg formats.



View ingress metrics

You can view the type of ingress used in the Kubernetes cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- NetScaler IP address and its score
- **Current State** – Indicates if the NetScaler instance is Up, Down, or Out of Status
- **Max Contribution** – Indicates the issue that is affecting the instance score

For the single-tier topology, you can view only a single **Ingress**.

Click the **Ingress** to drill down further for details. For more information, see View ingress details for troubleshooting issues.

View TCP and SSL metrics

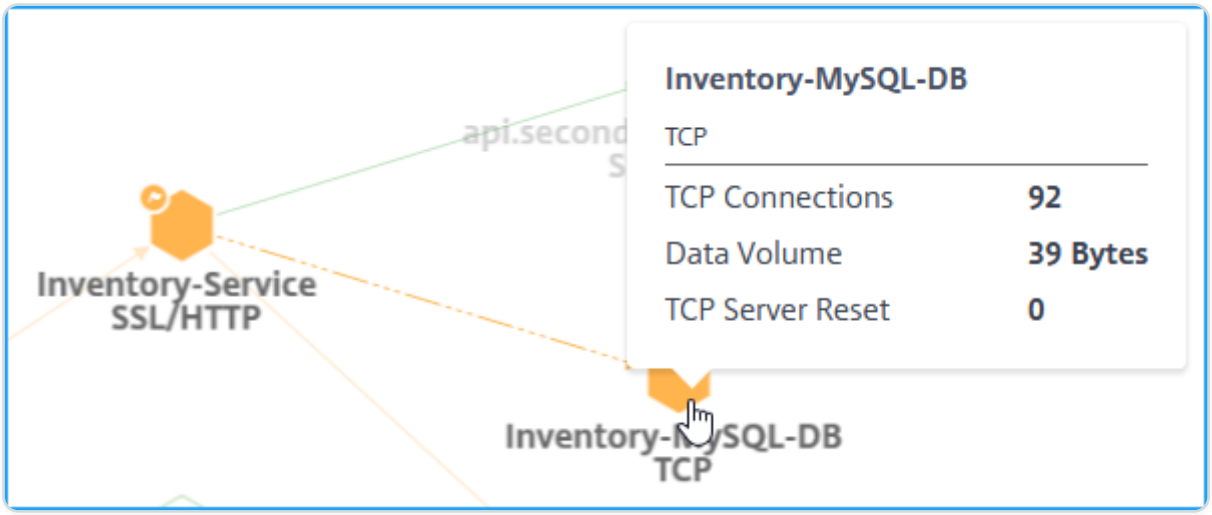
Using the TCP and SSL metrics, you can:

- View TCP connection details between services
- Determine if TCP-related issues are from the source or destination service
- View if the SSL error is from the source or destination service
- View the SSL protocol version used by SSL services

TCP metrics

Hover the mouse pointer over a TCP service or its associated incoming service to view the TCP metrics.

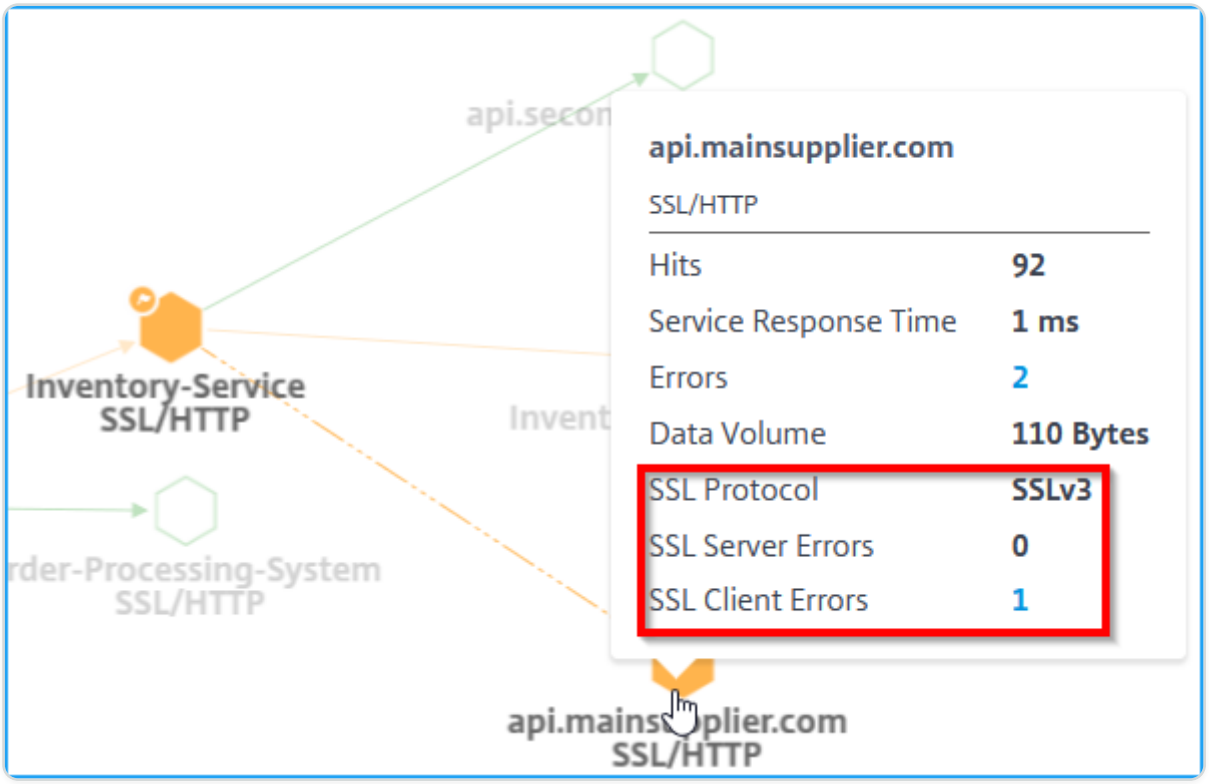
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **TCP connections** – Total connections established between the services
- **Data Volume** – Total data processed by the service
- **TCP Server Reset** – Total TCP resets initiated from the server

SSL metrics

Hover the mouse pointer on a service that uses SSL protocol to view the SSL metrics.



- **SSL Server Errors** – Indicates the total SSL errors from the server. (For example, SSL certificate unknown)
- **SSL Protocol** – Indicates the SSL protocol version used by the service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

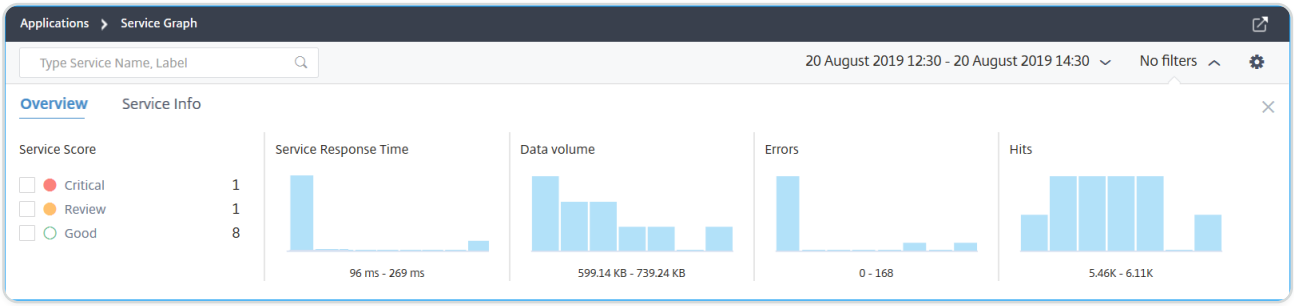
- **SSL Client Errors** - Indicate the total SSL errors from the client. (For example, SSL client authentication error)

View service details

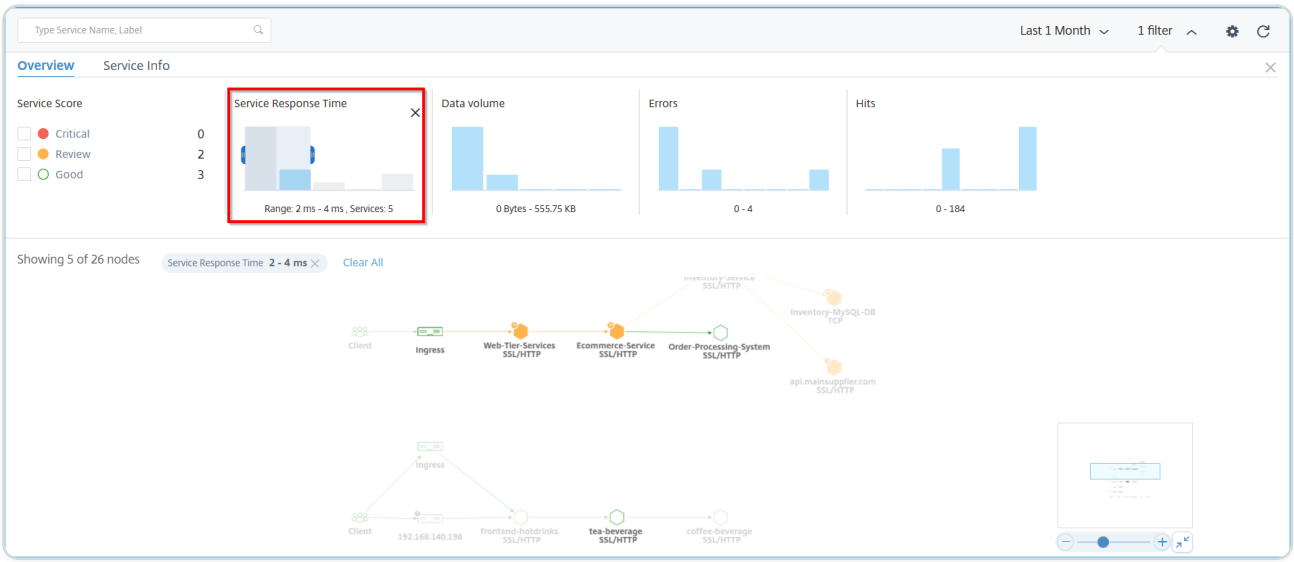
Click a service and select **View Details** to view the service details. For more information, see View service details.

Apply filters

You can apply filters to view specific service information. Click **No Filters** list to get the filter options.



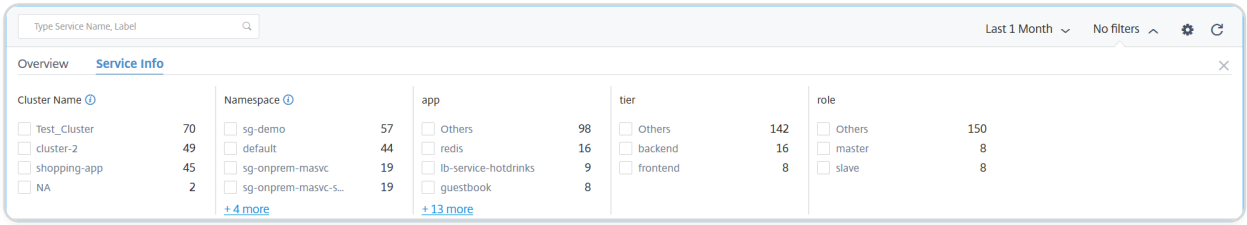
For example, if you want to view services that have latency less than 150 ms, then click the bar graph under **Service Response Time** to display the results.



Click **Service Info** to select and apply filters for:

- **Cluster** – Displays all services applicable for the selected cluster or clusters.
- **Namespace** – Displays all services applicable for the selected namespace.

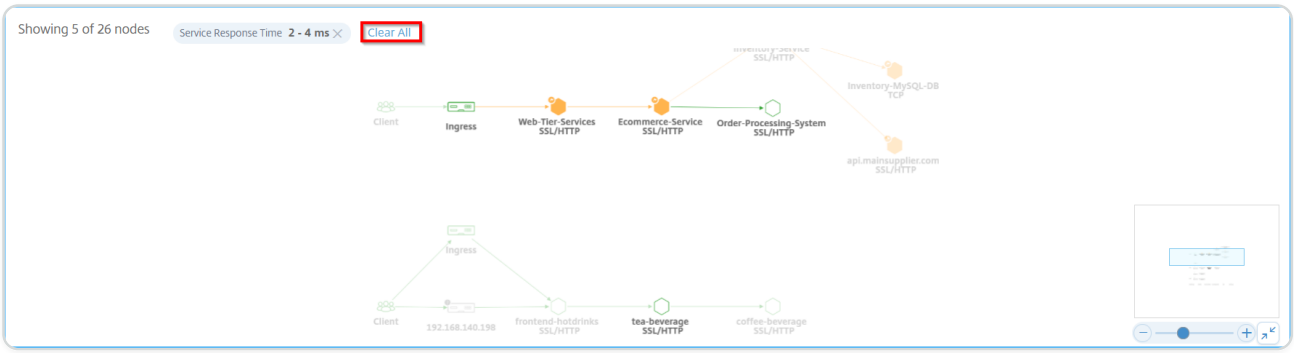
© 1997–2026 Citrix Systems, Inc. All rights reserved.



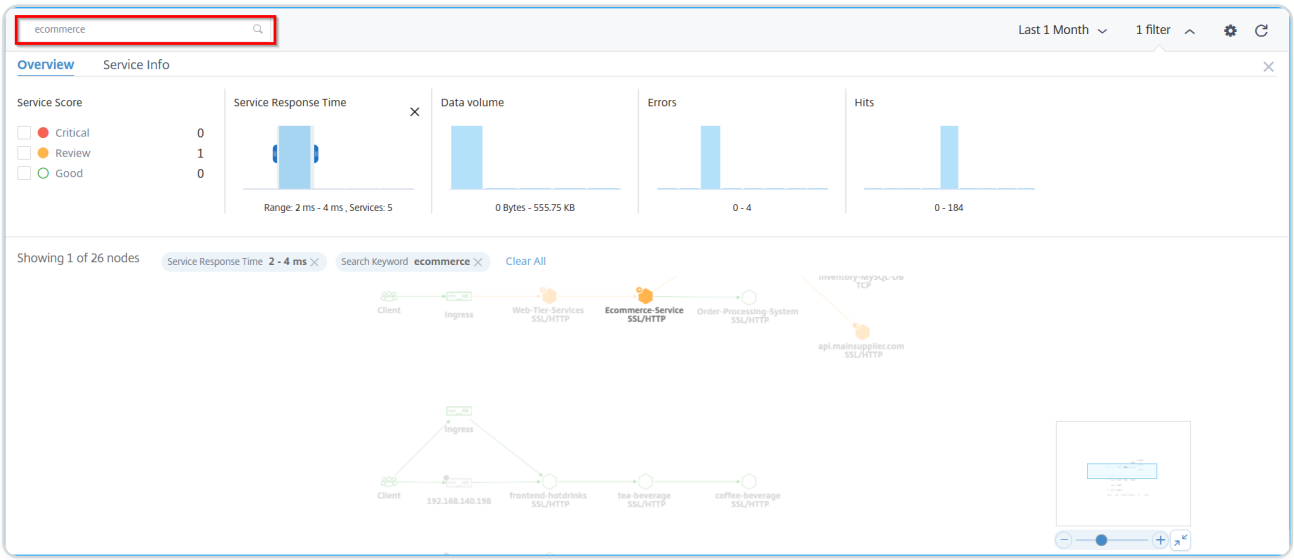
Note

> Depending upon the labels configured for the service in Kubernetes service definition YAML, you may also view more filter options.

Click **Clear All** to clear all filters.

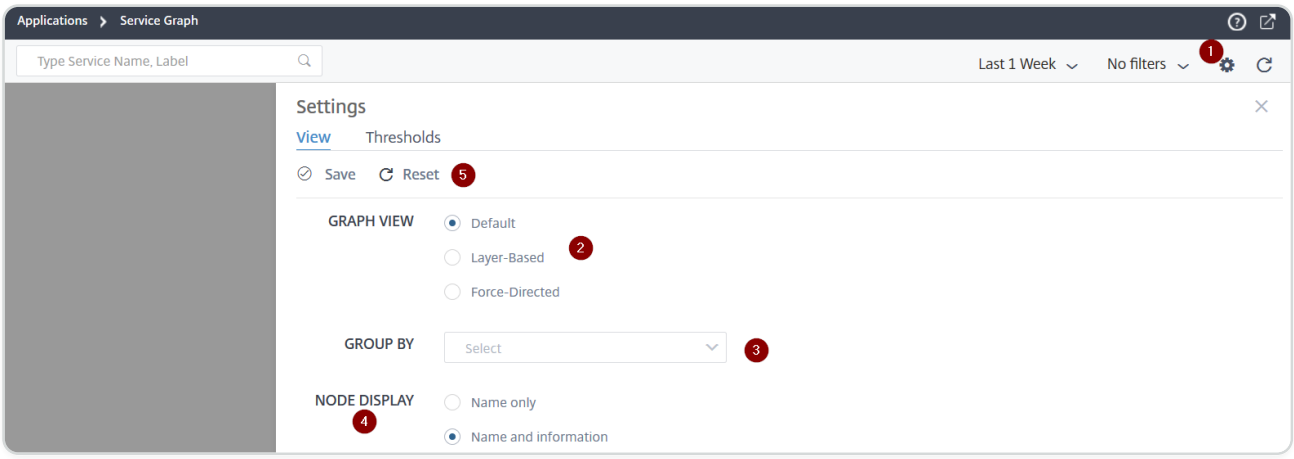


Alternatively, you can also use the search text box and type a service name to display the results on the service graph.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

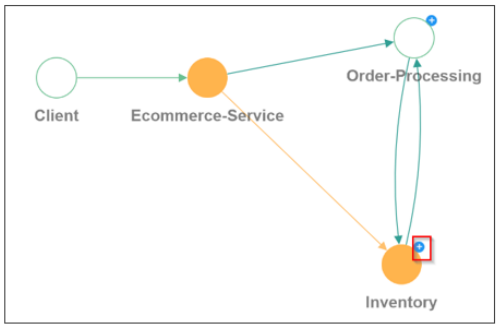
Using the settings option



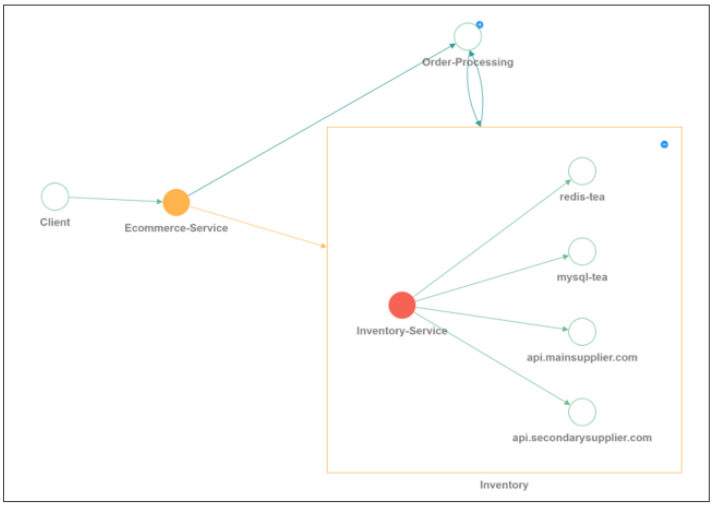
1 – Settings icon

2 – Options to display the service graph as Default, Layer-Based, or Force-Directed views

3 – Select the options from the list to view the services based on categories. After you select a category from the list, click **+** on the graph to view all services



Collapsed view



Expanded view

4 – Enables you select the option on how you want to display the services.

5 - Options to either save the settings or to reset to default.

Analyze the errors

Hover the mouse pointer on a service that indicates errors.

ERROR	DESCRIPTION
	The **TCP Server Reset** indicates the total TCP resets initiated from the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERROR	DESCRIPTION
	The **TCP Client Reset** indicates the total TCP resets initiated by the client.
	The SSL Client Errors indicate the total SSL errors from the client. (For example, SSL client authentication error).
	The SSL Server Errors Indicate the total SSL errors from the server. (For example, SSL certificate unknown)

NOTE

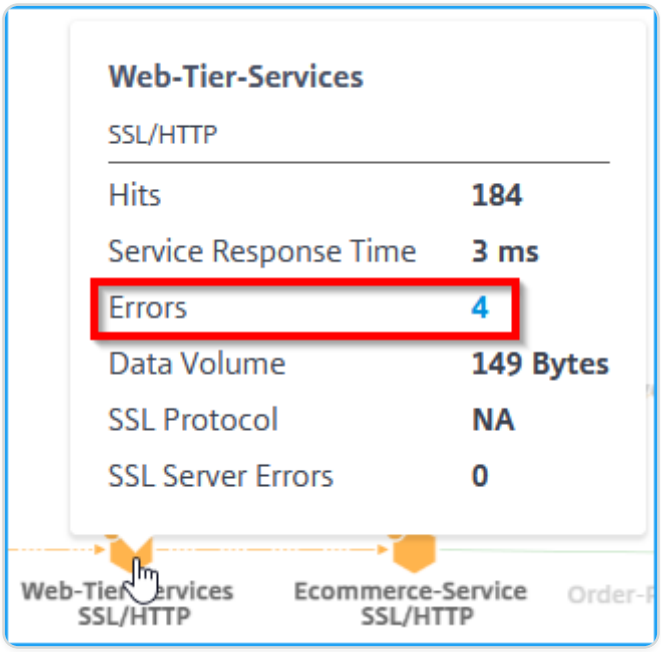
- Client error count (irrespective of the protocol type) is displayed in any service if the client error count is **1 or higher**.
- Clients error count displayed for any service indicates that the errors are from the client end.

View HTTP transaction details

NOTE

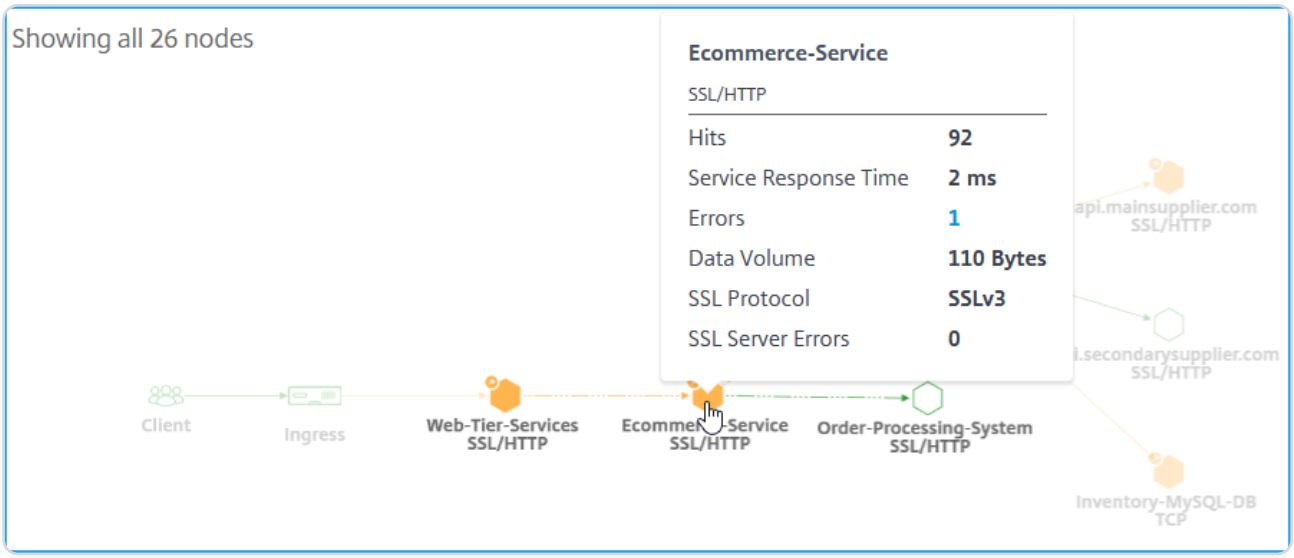
You can view the errors by hovering the mouse pointer on an erroneous service and click the issue count.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



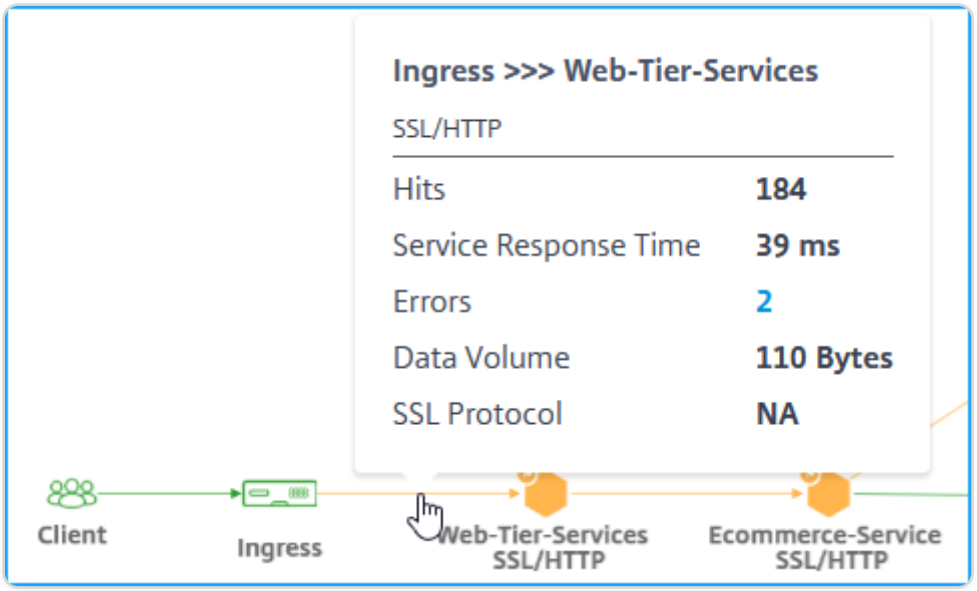
According to the example shown in the image, you can view an end-to-end network map of your application that shows how your component services are communicating.

When you hover the mouse pointer on the **Ecommerce-Service**, you can view metrics details for **Ecommerce-Service**.



NetScaler ADM also enables you to view transaction details between Ingress and services. Hover the mouse pointer to view details such as total errors, average service response time, and so on between the Ingress and service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Hits – Indicates the total number of hits received by the service.

Service Response Time – Indicates the average response time taken from the service to respond for Time To First Byte (TTFB).

Errors – Indicates the total errors such as 4xx, 5xx, and so on.

Data volume – Indicates the total volume of data processed by the service.

SSL Protocol – Indicates the SSL protocol version.

Click the arrow between **Ingress** and **service** to view the detailed transactions.

For more information, see View analytics for Web transactions.

Configure thresholds in service graph

As an administrator, you can configure thresholds for Kubernetes services. NetScaler® ADM displays the service status (Critical, Review, and Good) based on the service response time and error count. By default, you can view the **Default Threshold** (service response time = 200 ms and error count = 0) applied to all services.

NOTE

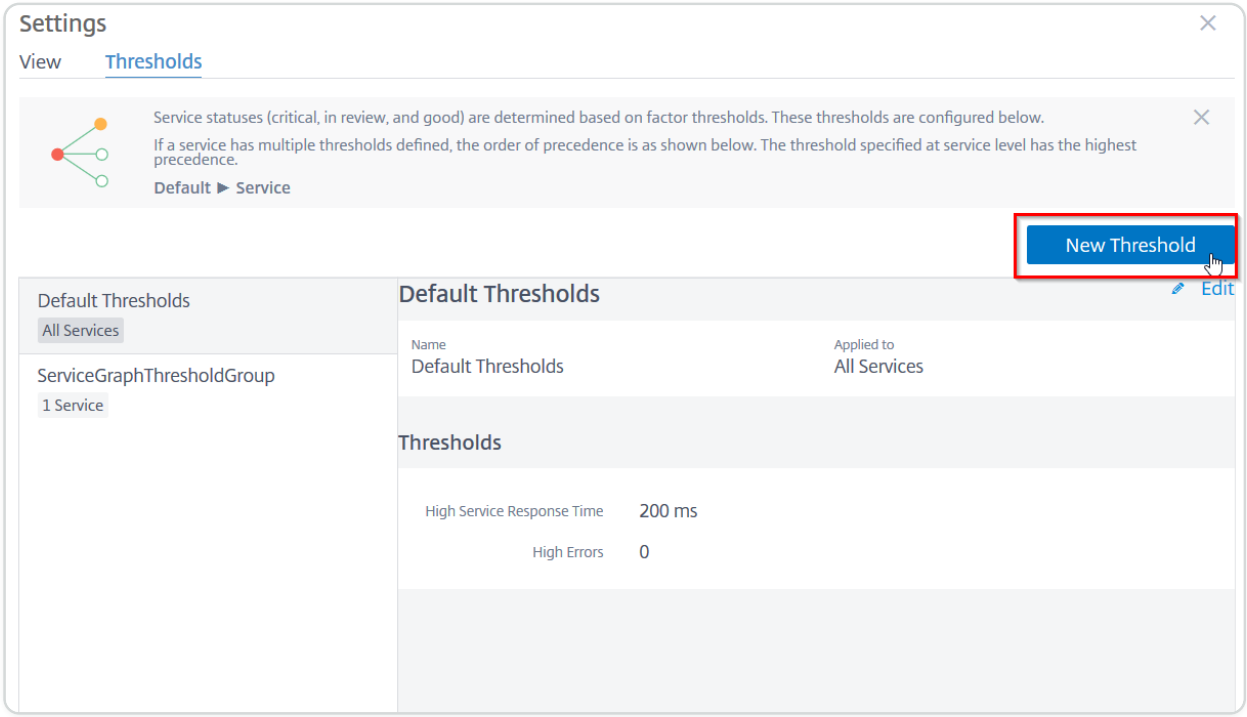
You cannot delete the Default Threshold.

To configure a new threshold:

In service graph:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click the settings icon and select the **Thresholds** tab.
2. Click **New Threshold** to configure a new threshold.



The **New Threshold** page is displayed.

3. Configure the following parameters:

   a. **Name** – Specify a name for the threshold.

   b. Under **Microservices**, select the services that you want to apply the threshold

   c. Under **Thresholds**, select **Single** or **Double** for High Response Time and High Errors

   d. Specify the threshold values.

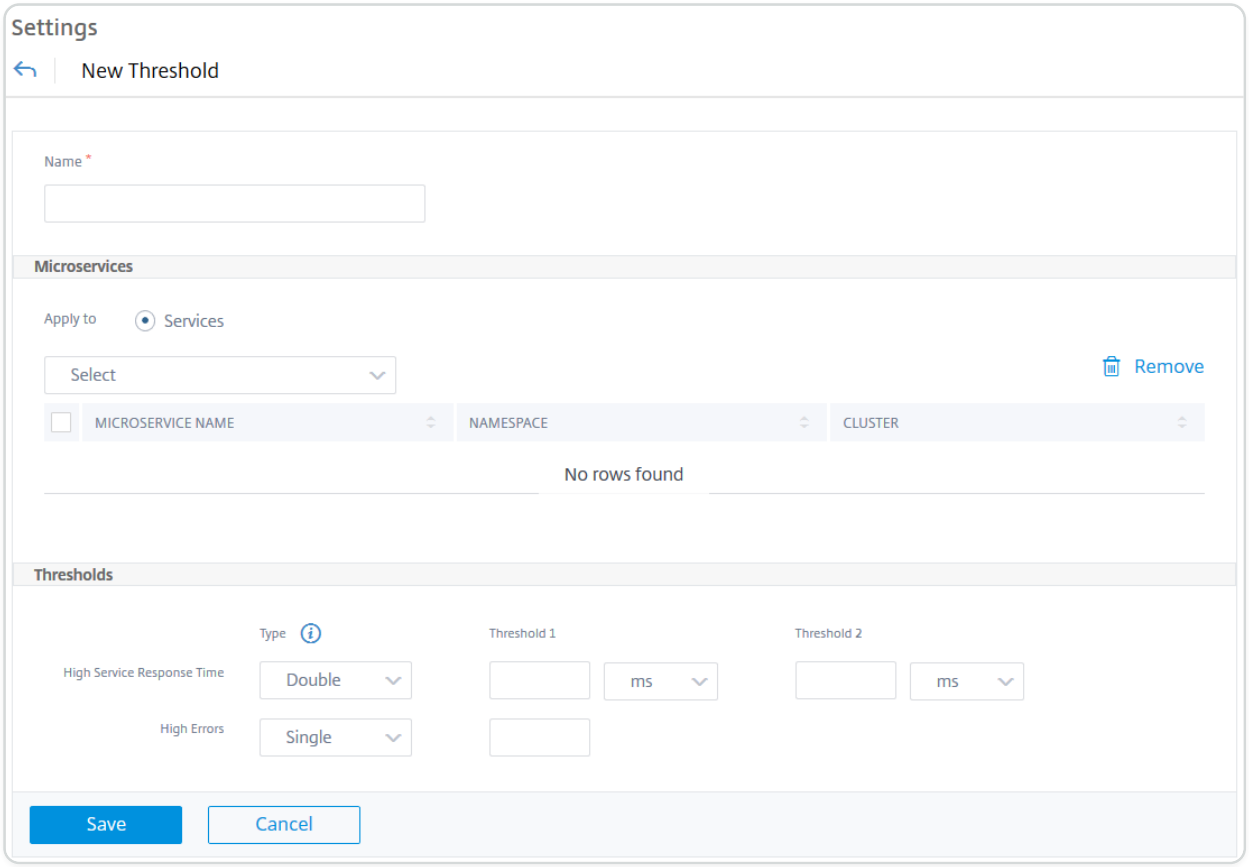
   NOTE

   If you select double threshold, ensure:

   - Threshold 1 value is lesser than Threshold 2 value. For example, if you configure Threshold 1 as 250 ms, Threshold 2 must be 251 ms or higher.
   - Threshold 1 value must not be the same as Threshold 2 value.

4. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The threshold is successfully created. You can view the threshold details in the **Thresholds** page.

Single threshold

When you configure single threshold, NetScaler ADM:

- Compares the current values with the configured threshold values
- Calculates the total penalty based on the exceeded thresholds
- Displays the service score and service status based on the penalty calculation

Double threshold

When you configure double threshold, NetScaler ADM:

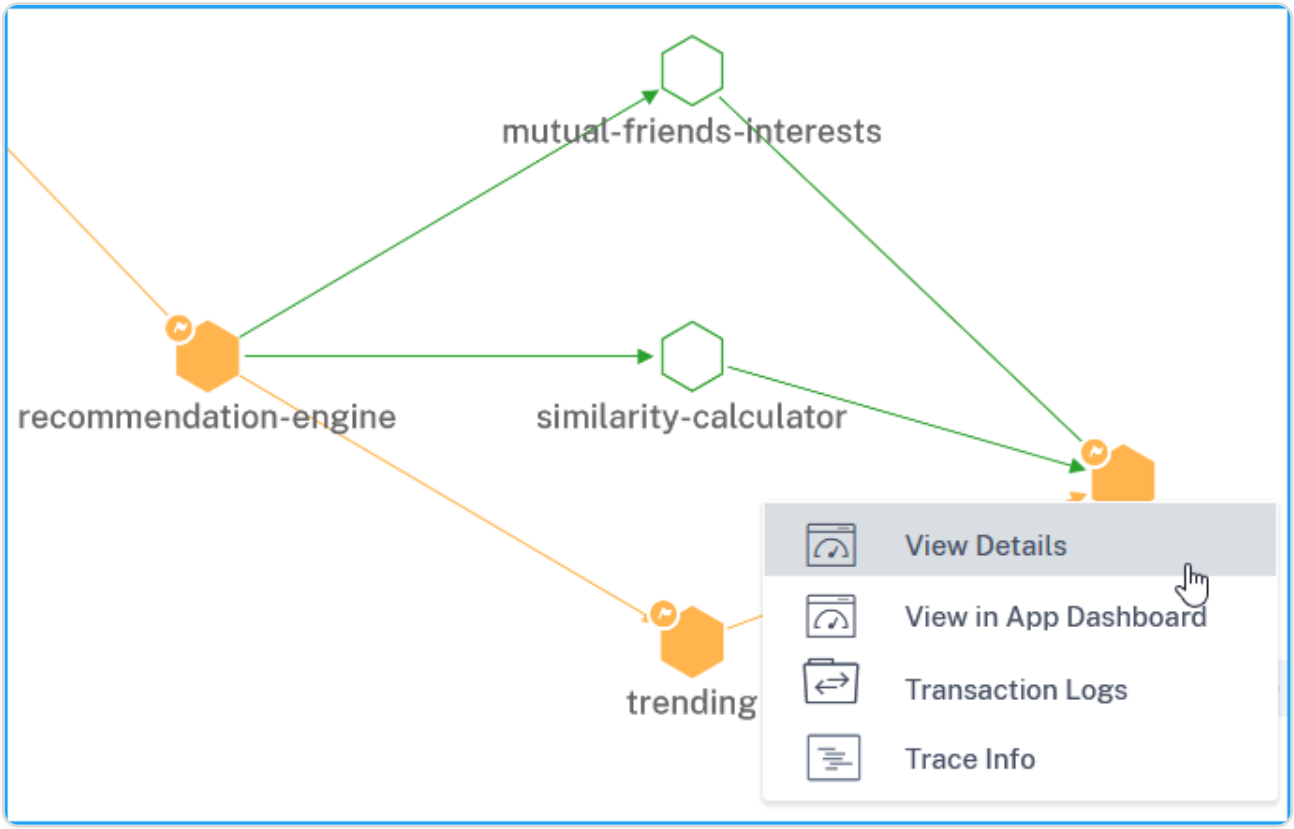
- Compares the current values with the configured threshold values
- Checks if the current values are:
  - Lesser than threshold 1
  - Between threshold 1 and threshold 2
  - Greater than threshold 2
- Calculates the total penalty based on the exceeded thresholds

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Displays the service score and service status based on the penalty calculation

View service details

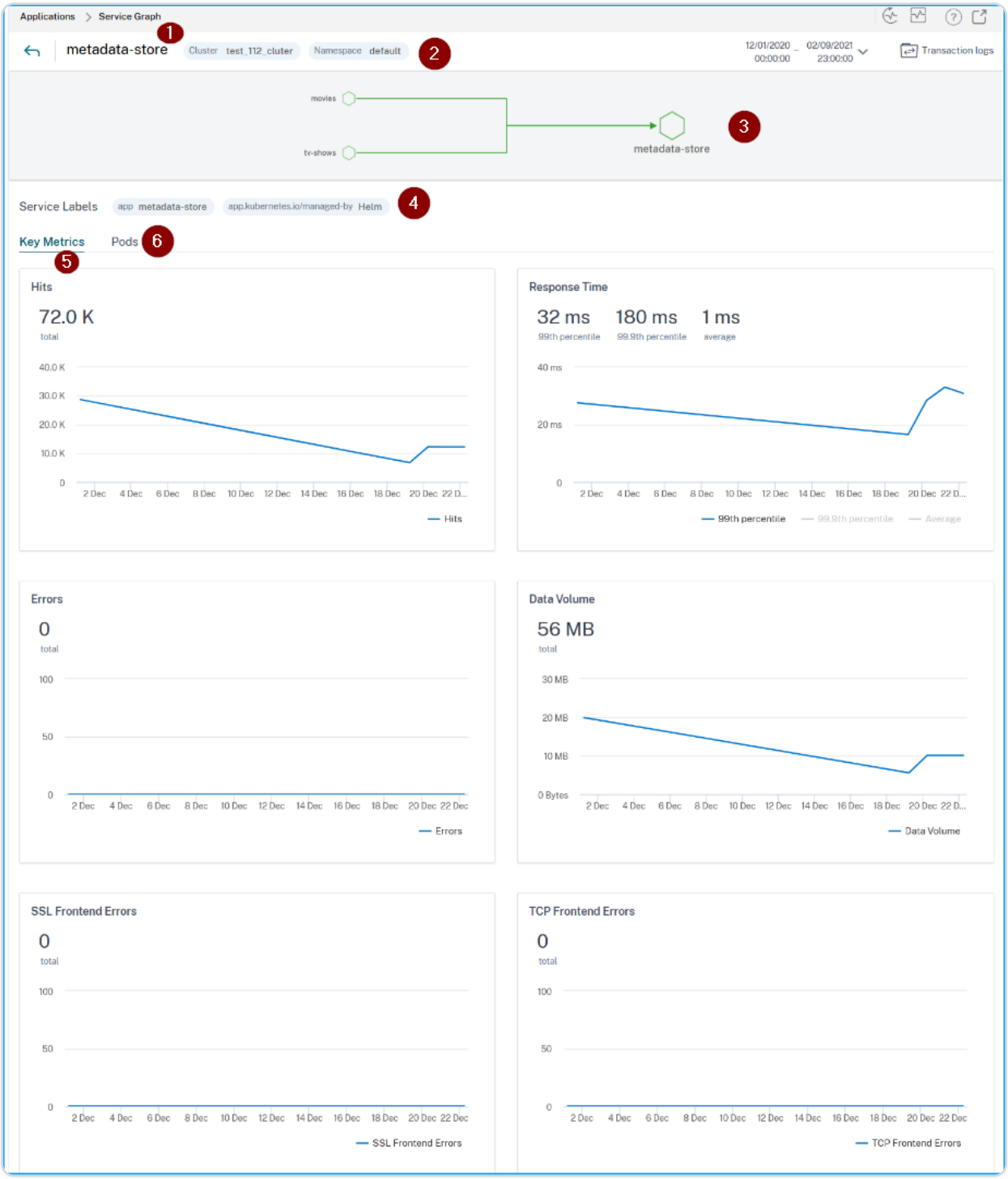
Click a service and select **View Details**.



The service details page enables you to view:

- The cluster name where the service is hosted (1)
- The namespace and service labels of the service (2) (4)
- All associated incoming and outgoing services connected with the selected service (3)
- Service key metrics in a graph format such as Hits, Response time, Errors, Data volume, SSL frontend errors, and TCP frontend errors (5).
- The backend pods associated with the service (6).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Using these key metrics trends, you can analyze how the service is performing for a specific time duration.

The **Response Time** metric enables you to view:

- **99th percentile** – Indicates that the 99% of the requests for the selected duration is less than 32 ms (according to the example image).
- **Average** – Indicates the average response time from the service
- **99.9th percentile** – Indicates the highest response time from the service

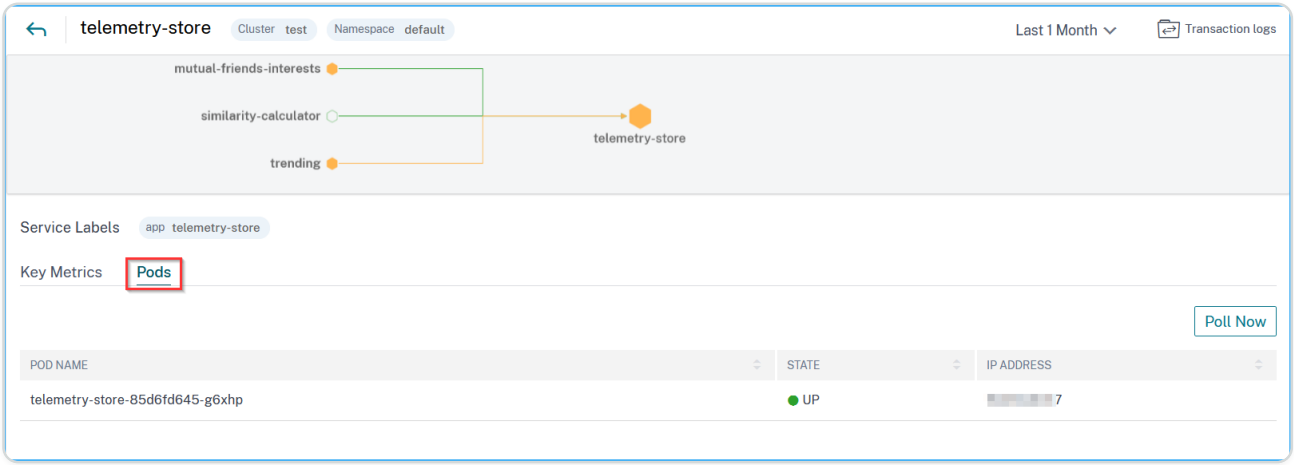
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Metrics details

METRICS	DESCRIPTION
Hits	The total number of requests received by the service
Errors	The total HTTP errors from the service
Service Response Time	The average response time taken from the service to respond for Time To First Byte (TTFB).
Data Volume	The total data volume processed by the service
SSL front-end errors	The total SSL front-end errors from the service. For example: SSL CLIENTAUTH FAILURE
SSL back-end errors	The total SSL back-end errors from the service. For example: SSL Client Errors
TCP back-end errors	The total TCP back-end errors from the service. For example: TCP Server Reset
TCP front-end errors	The total TCP front-end errors from the service. For example: TCP Client Reset

View backend pod details

Click the **Pods** tab to view the backend pods associated with the service.



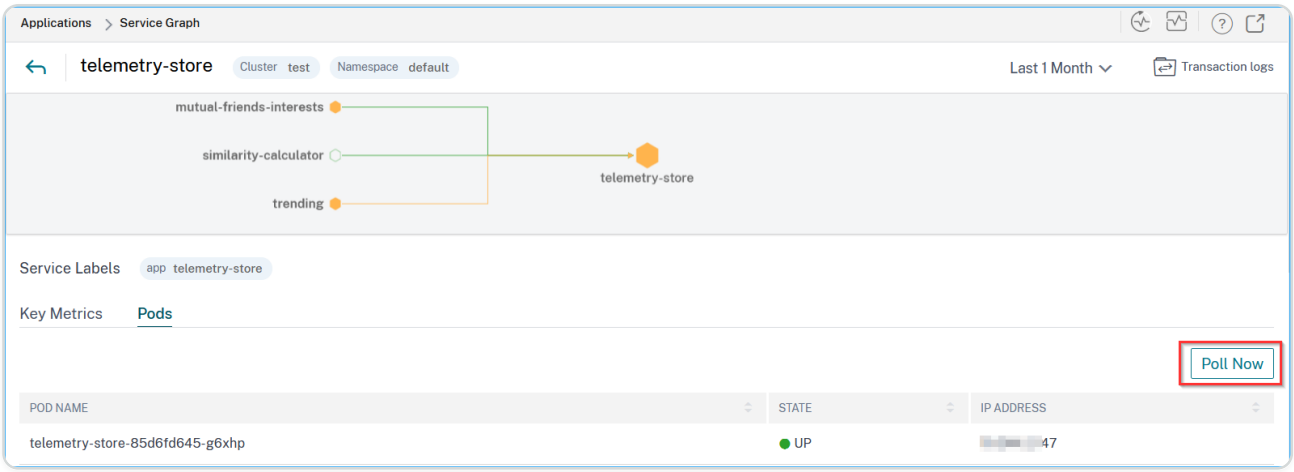
- **Pod name** – Denotes the pod name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Status** – Denotes if the pod is running (UP) or not (DOWN).
- **IP address** – Denotes the pod IP address

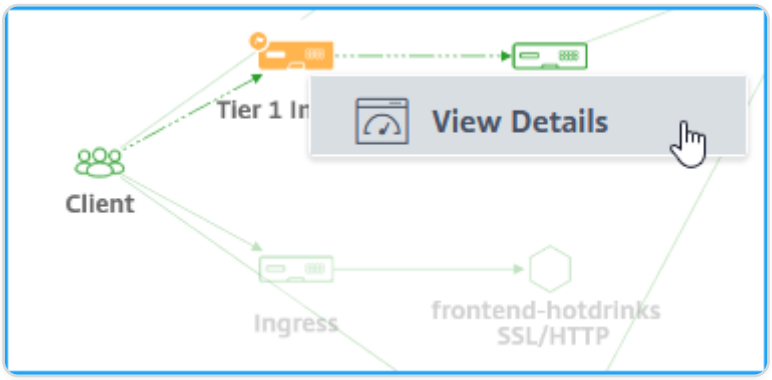
Use the Poll Now option to get the pod status

The **Poll Now** option fetches the latest pod status from the cluster.

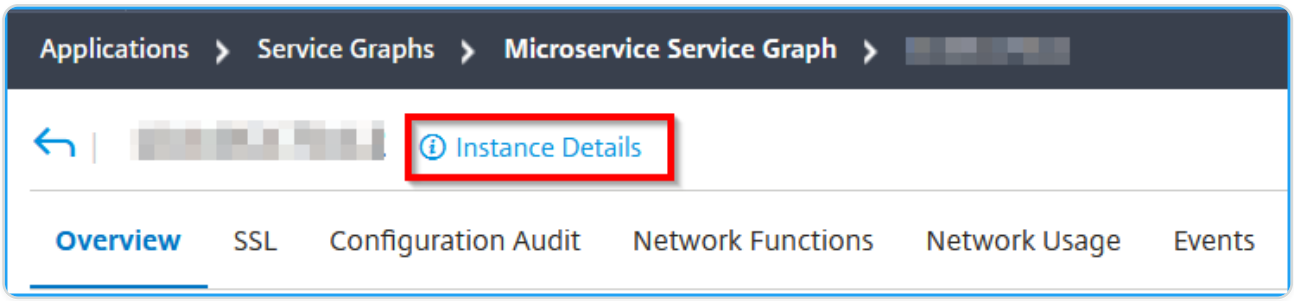


View ingress details for troubleshooting issues

In service graph, click the ingress and select **View Details** to visualize the details of NetScaler instance that is configured for the Kubernetes cluster.



Click **Instance Details** to view the details.



The following details are displayed:

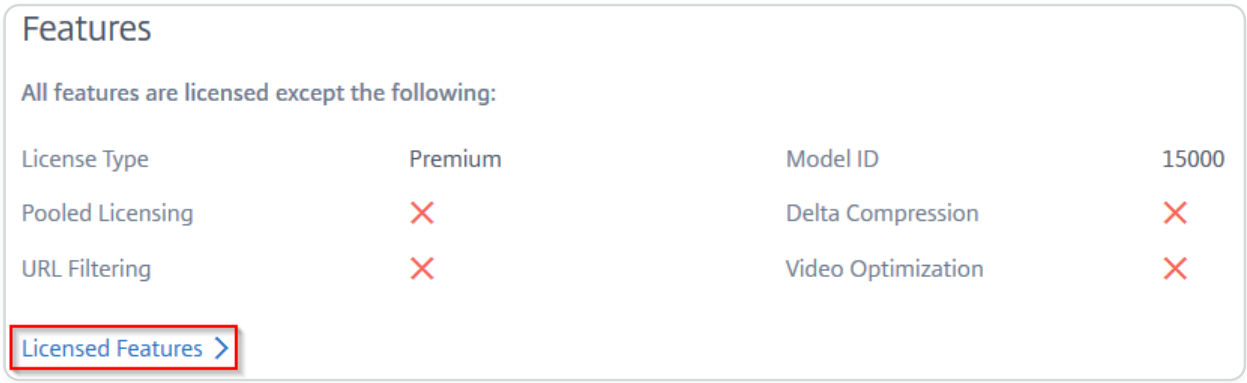
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Information** - Instance details such as instance type, deployment type, version, model, and so on.

Information

HOST NAME	217ns	MODEL ID	15000
SYSTEM IP ADDRESS	10.106.181.217	SYSTEM CUSTOM ID	Default
SYSTEM NAME	NetScaler	PACKET ENGINES	1
TYPE	Citrix ADC VPX	SSL CARDS	0
HA MASTER STATE	Primary	CPU	2099MHZ
NODE STATE	Up	VERSION	NetScaler NS11.1: Build 62.8.nc
PEER IP ADDRESS	--	HARDWARE VERSION	NetScaler Virtual Appliance
SECONDARY NODE STATUS	--	LOM VERSION	-NA-
HA SYNC STATUS	ENABLED	HOST ID	000c29e1c592
SYSTEM SERVICES	72	SERIAL NUMBER	HE2H81UJ47
NETMASK	255.255.255.0	ENCODED SERIAL NUMBER	891e0000cb254307ee9a
GATEWAY	10.106.181.1	CITRIX ADC UUID	--
ADMIN PROFILE	ns_nsroot_profile	LOCATION	POP (default)
HEALTH	--	CONTACT PERSON	WebMaster (default)
UPTIME	25 days, 19 hours, 42 minutes		
DESCRIPTION	--		

- **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



Features

All features are licensed except the following:

License Type	Premium	Model ID	15000
Pooled Licensing	✗	Delta Compression	✗
URL Filtering	✗	Video Optimization	✗

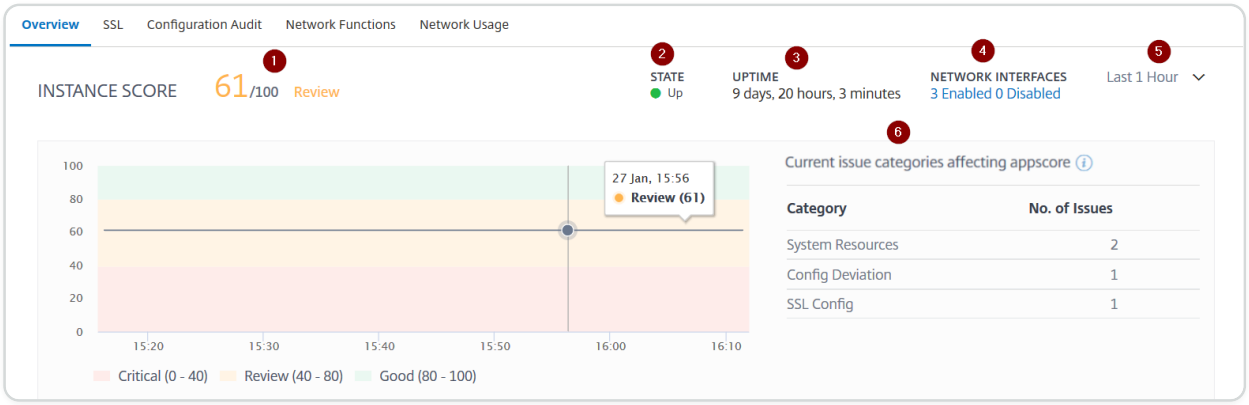
Licensed Features >

- **Modes** – By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**



1 – Indicates the current NetScaler instance score for the selected time duration. The final score is calculated as **100 minus total penalties**. The graph displays the score ranges for the selected time duration.

2 – Indicates the current status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 – Indicates the duration that the NetScaler instance is up and running.

4 – Indicates the total network interfaces enabled and disabled for the instance. Click to view the details such as network interface name and the status (enabled or disabled).

5 – Select the time duration from the list to view the instance details.

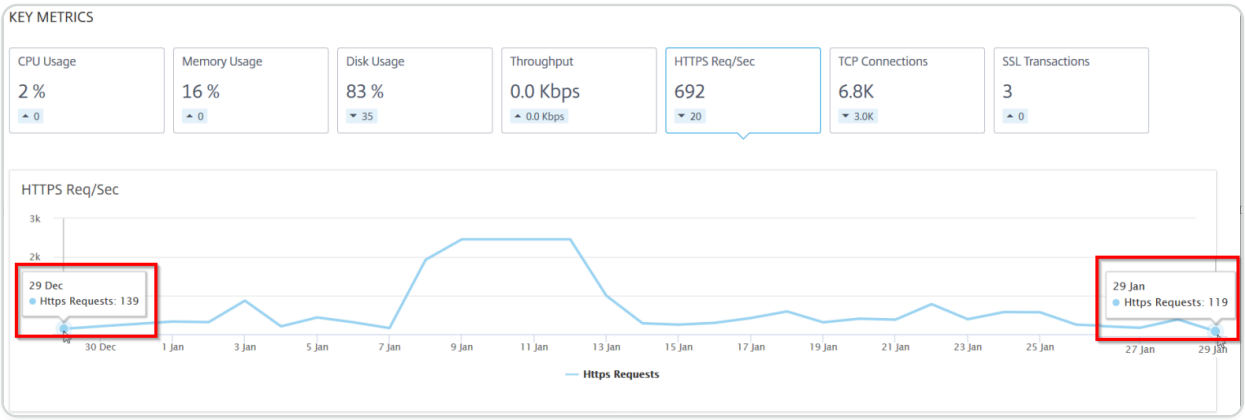
6 – Displays the total issues and issue category of the ADC instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Key Metrics**

  Click each tab to view the details. In each metric, you can view the average value and the difference value for the selected time.

  The following image is an example for HTTPS Req/Sec and the selected time duration is for last 1 month. The value **692** is the average HTTPS Req/Sec for the last 1-month duration and the value **20** is the difference value. In the graph, the first value is **139** and the last value is **119**. The difference value is **139 – 119 = 20**.



  You can view the following instance metrics in a graph format for the selected time duration:

  - **CPU Usage** – The average CPU % from the instance for the selected duration (displays for both packet CPU and for management CPU).
  - **Memory Usage** – The average memory usage % from the instance for the selected duration.
  - **Disk Usage** – The average disk space % from the instance for the selected duration.
  - **Throughput** – The average network throughput processed by the instance for the selected duration.
  - **HTTPS request/sec** – The average HTTPs requests received by the instance for the selected duration.
  - **TCP connections** – The average TCP connections established by the client and server for the selected duration.
  - **SSL transactions** – The average SSL transactions processed by the instance for the selected duration.

- **Issues**

  You can view the following issues that occur in NetScaler instance:

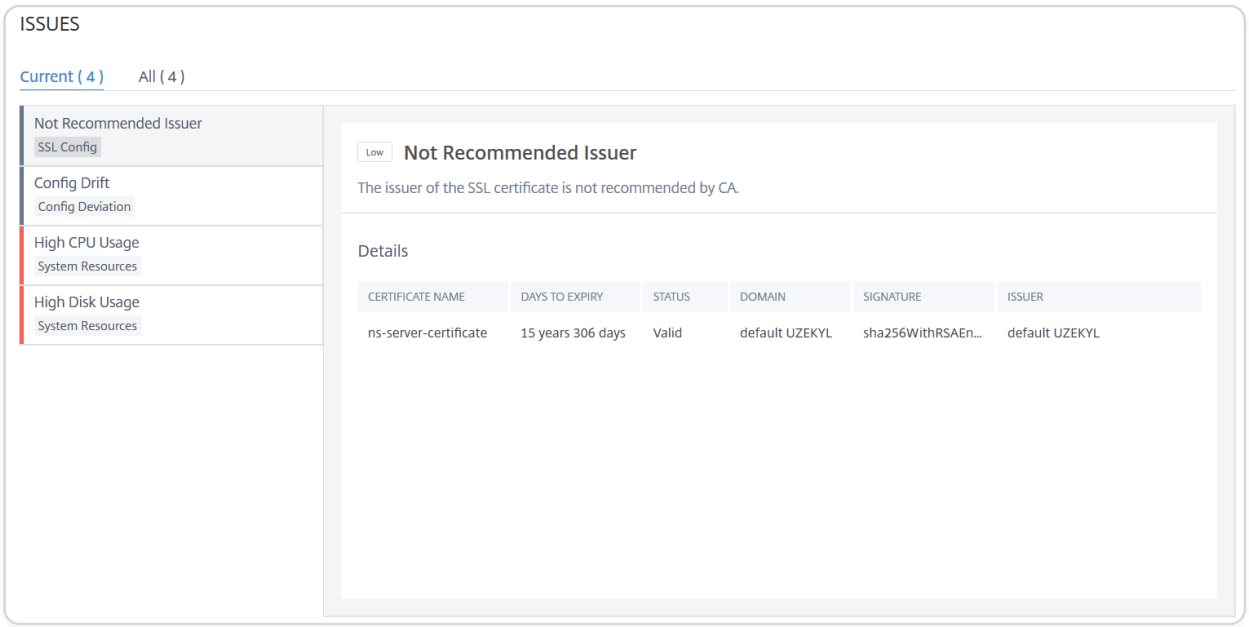
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage, and so on.	- High CPU Usage
		- High Memory Usage
		- High Disk Usage
		- SSL Card Failures
		- Power Failure
		- Disk Error
		- Flash Error
		- NIC Discards
SSL Config	Displays all issues related to the SSL configuration on the NetScaler instance.	- SSL Certs Expired
		- Not Recommended Issuer
		- Not Recommended Algorithm
		- Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in NetScaler instance.	- Config Drift
		- Running vs Template
Capacity issues	Displays ADC capacity issues. The ADM polls these events every five minutes	- Throughput Limit Reached

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
	from the ADC instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters.	
		- PE CPU Limit Reached
		- PPS Limit Reached
		- SSL Throughput Rate Limit
		- SSL TPS Rate Limit
Networking	Displays the operational issues that occur in the instances.	For more information, see Enhanced Infrastructure Analytics with new indicators.

Click each tab to analyze and troubleshoot the issue. For example, consider that an instance has the following errors for the selected time duration:



- The **Current** tab displays the current ADC operational issues that are affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Distributed tracing

In service graph, you can use the distributed tracing view to:

- Analyze the overall service performance.
- Visualize the communication flow between the selected service and its inter-dependent services.
- Identify which service indicates errors and troubleshoot the erroneous service
- View transaction details between the selected service and its each inter-dependent service.

Prerequisites

To view the trace information for the service, you must:

- Ensure that an application maintains the following trace headers, while sending any east-west traffic:

  - `x-request-id`
  - `x-b3-traceid`
  - `x-b3-spanid`
  - `x-b3-parentspanid`
  - `x-b3-sampled`
  - `x-b3-flags`
  - `x-ot-span-context`

- For **CIC builds earlier than 1.7.23**, update the CPX YAML file with `NS_DISTRIBUTED_TRACING` and value as `yes`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cpx-ingress
spec:
  selector:
    matchLabels:
      app: cpx-ingress
  replicas: 1
  template:
    metadata:
      name: cpx-ingress
      labels:
        app: cpx-ingress
      annotations:
    spec:
      serviceAccountName: cpx-ingress-k8s-role
      containers:
        - name: cpx-ingress
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
          securityContext:
             privileged: true
          env:
          - name: "EULA"
            value: "yes"
          - name: "KUBERNETES_TASK_ID"
            value: ""
          - name: "NS_MGMT_SERVER"
            value: "192.168.0.1"
          - name: "NS_MGMT_FINGER_PRINT"
            value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6D:97:3D:E2:5D"
          - name: "NS_HTTP_PORT"
            value: "9080"
          - name: "NS_HTTPS_PORT"
            value: 9443"
          - name: "LOGSTREAM_COLLECTOR_IP"
            value: "192.168.0.1"
          imagePullPolicy: Always
```

- For **CIC builds later than 1.7.23**, you must use a ConfigMap.

  ConfigMaps allow you to separate your configurations from your pods and make your workloads portable. Using ConfigMaps, you can easily change and manage your workload configurations and reduce the need to hardcode configuration data to pod specifications.

  With ConfigMap support, you can update the configuration automatically while keeping the NetScaler Ingress Controller pod running. You do not need to restart the pod after the update. For more information, see ConfigMap support for the ingress controller.

  Using the ConfigMap, you can enable or disable distributed tracing, events, audit logs, and so on. To use the ConfigMap:

  a. Create a YAML file using the required parameters.

     The following example YAML file has the distributed tracing enabled and other variables such as audit logs, events, and transactions disabled:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG:

    distributed_tracing:

      enable: 'true'

      samplingrate: 100

    endpoint:

      server: <ADM-AgentIP> / <ADM-AppserverIP>

    timeseries:

      port: 5563

      metrics:

        enable: 'true'

        mode: 'avro'

      auditlogs:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        enable: 'false'

      events:

        enable: 'false'

    transactions:

      enable: 'false'

      port: 5557
```

Note

> You can provide the values for `Samplingrate` between 0 and 100. NetScaler ADM displays the mentioned number of trace transactions.

b. Deploy the ConfigMap by using:

`kubectl create -f <configmap-yaml>.yaml`

c. Edit the CPX YAML file and use either `envFrom` or `args` to specify the following arguments:

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

OR

```
  args:
     - --configmap
       default/cic-configmap
```

d. If you want to change the value for any variable, edit the values in the ConfigMap. In this example, all other variables are changed from `false` to `true`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG:

    distributed_tracing:

      enable: 'true'

      samplingrate: 100

    endpoint:

      server: <ADM-AgentIP> / <ADM-AppserverIP>

    timeseries:

      port: 5563

      metrics:

        enable: 'true'

        mode: 'avro'

      auditlogs:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

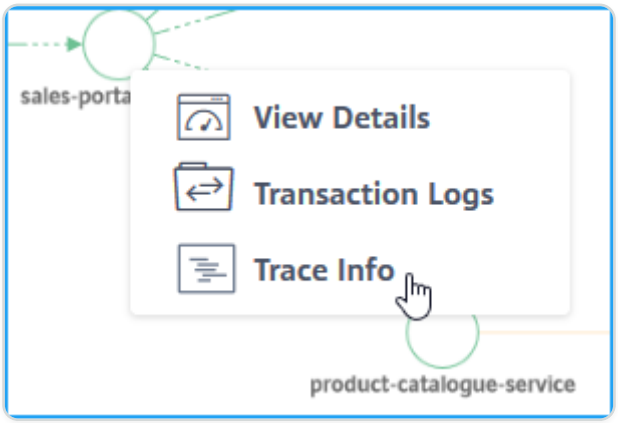
```
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
```

e. Reapply the ConfigMap using the following command:

```
kubectl apply -f <yaml-file>.yaml
```

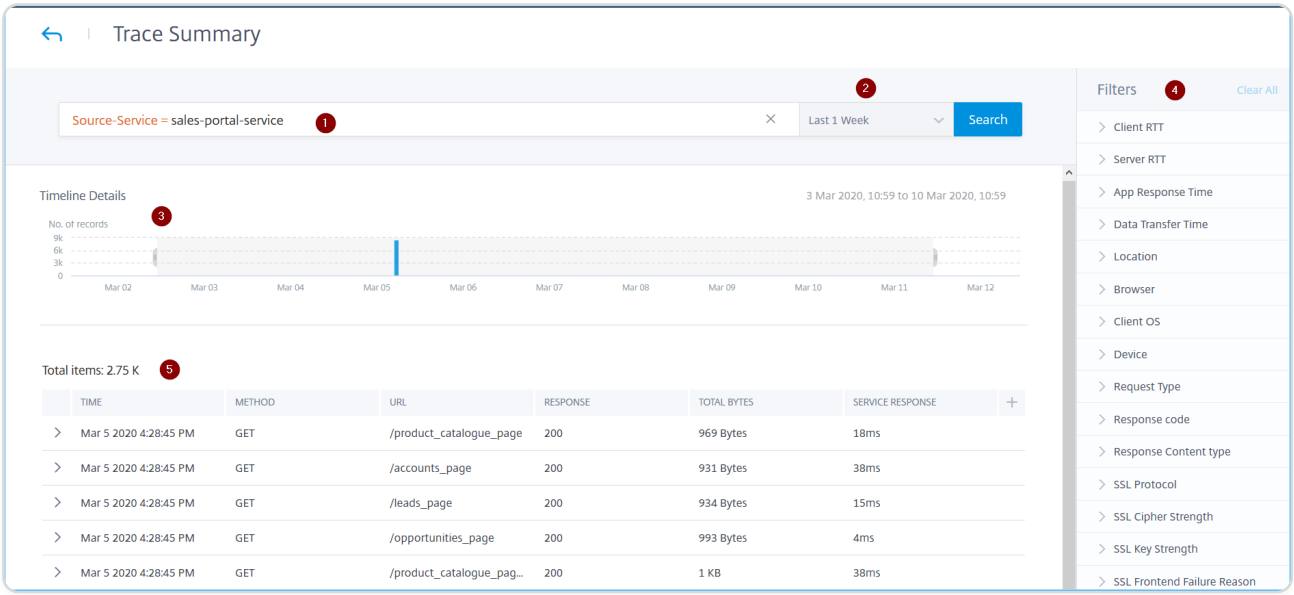
View service trace details

In service graph, click a service, and select **Trace Info**.



The Trace Summary page is displayed for the selected service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Trace Summary** displays:

- An advanced search that enables you to search through for transactions with suggestions and operators (1). For more information, see Advanced Search.
- The time duration list that enables you to select the time duration such as 1-hour, 12-hour, 1-day, 1-week, 1-month, and custom time (2).
- The Timeline Details graph that enables you to drag and select to display results for a specific time duration (3).
- The Filters panel that enables you to select options from each metric (4).
- The transaction details for the selected service (5).

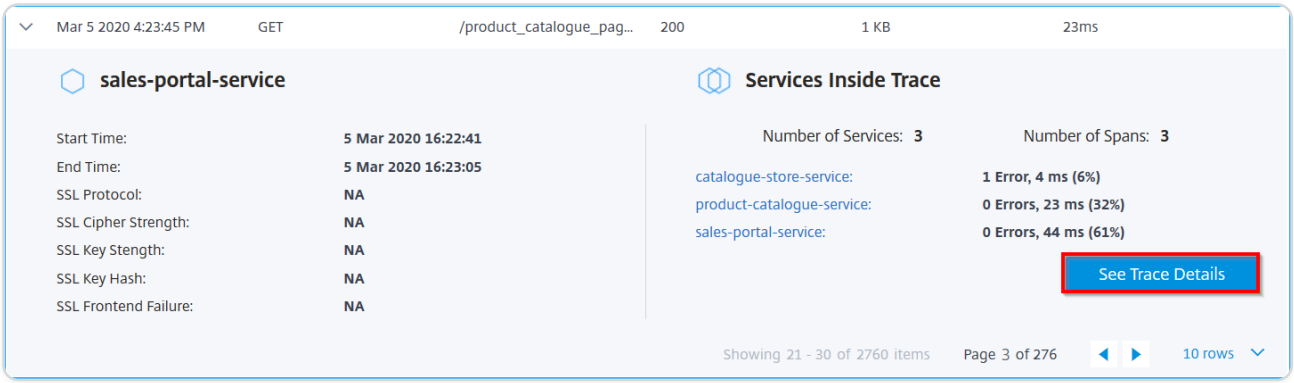
View the transaction details

Click a transaction to drill down for detailed information. You can view transaction details for the selected service such as:

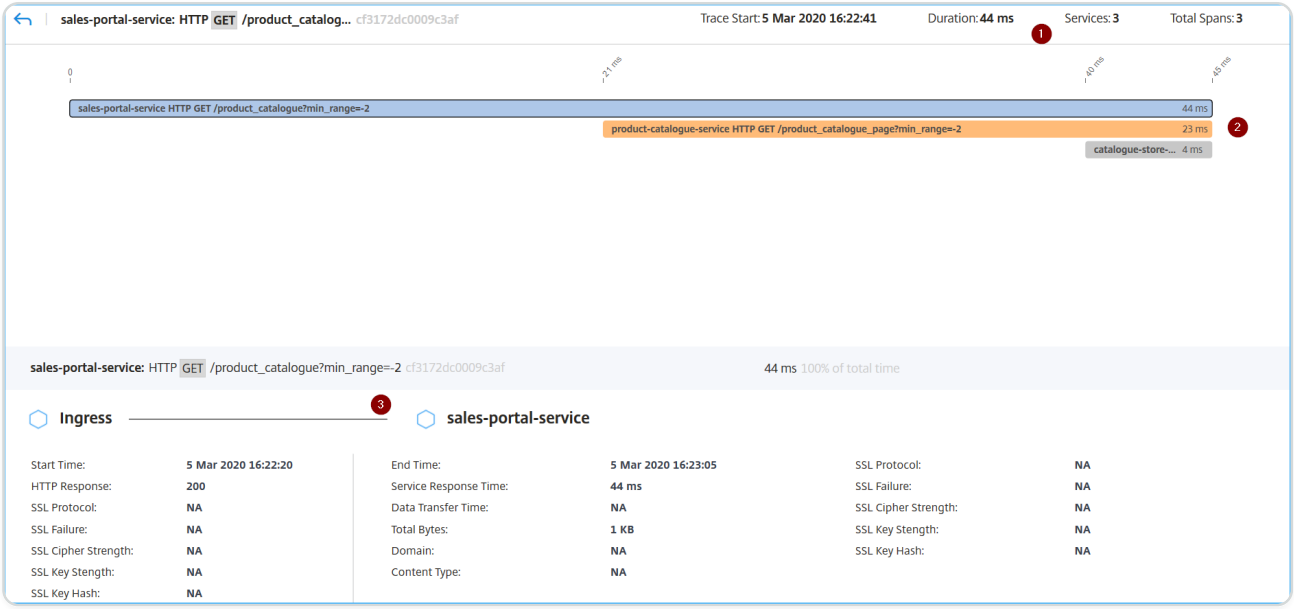
- Start time
- End time
- SSL metrics
- Communication with inter-dependent services (along with errors and response time with each service).

The following example indicates an error from `catalogue-store-service`. Click **See Trace Details** for further details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Trace Details page is displayed.



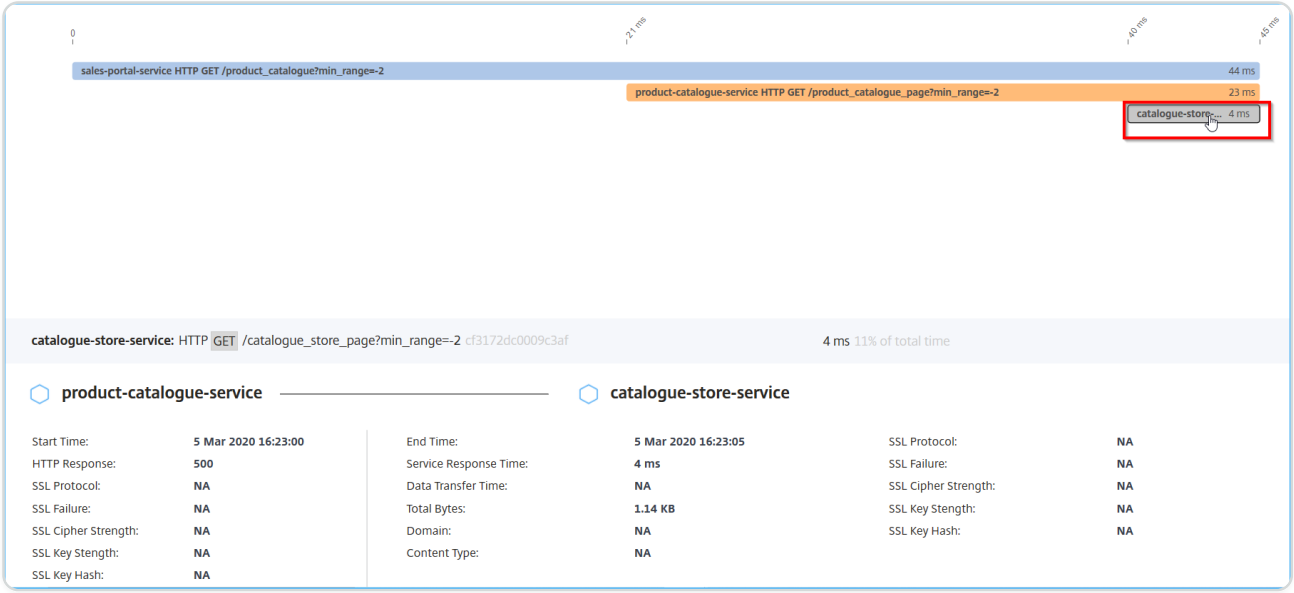
1 – Displays the start time, response time, total services, and total spans for the transaction.

2 – Displays the details for the selected service that has communicated with its inter-dependency services. You can click each transaction to view details.

3 – Displays the transaction details for each service.

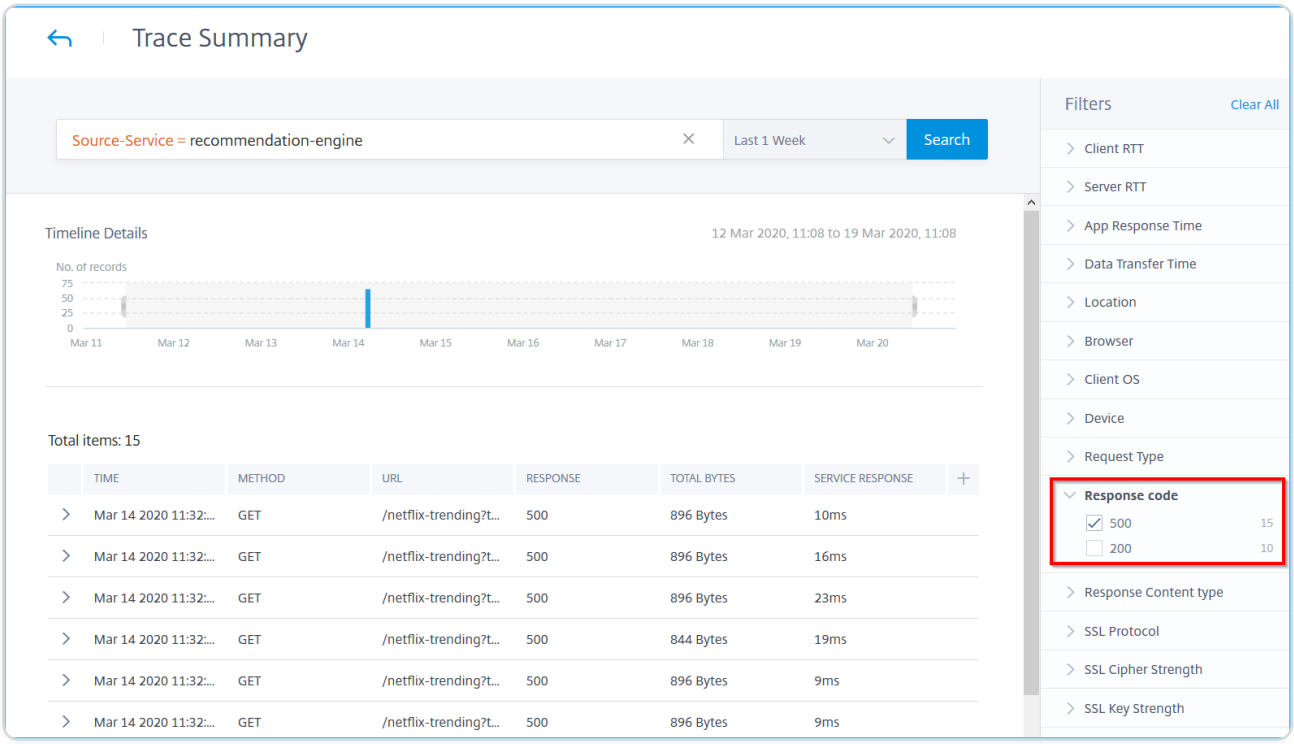
According to the example image, `catalogue-store-service` indicated an error. Click the transaction available for `catalogue-store-service`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The transaction details between `product-catalogue-service` and `catalogue-store-service` indicate HTTP response as 500. With these details, as an administrator, you can analyze the erroneous service and troubleshoot `product-catalogue-service` as a resolution.

You can also filter results by selecting options from each metric under the **Filters** panel. For example, if you want to view all 5xx transactions, click **Response code** and select **500**.



- **Client RTT**: The time duration for a packet to travel from the client.
- **Server RTT**: The time duration for a packet to travel from the server.
- **App Response Time**: The application average response time

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Data Transfer Time**: The data transfer size and the rate at which the transmit can happen from/to a service.
- **Location**: The client location
- **Browser**: The browser types used by the clients. For example: Chrome, Firefox.
- **Client OS**: The client OS based on the User Agent details from the browser.
- **Device**: The devices based on the User Agent details from the browser. For example: Tablet, Mobile.
- **Request Type**: The transaction request type. For example: GET.
- **Response code**: The response code received from the server. For example: 501, 404, 200.
- **Response content type**: The transaction content type. If the client request is for text/html, then the response from the server must be text/html.
- **SSL Protocol**: The SSL protocol version used by the clients. For example: SSLv3.
- **SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **SSL Front end Failure reason**: The front-end SSL handshake error message. For example: SSL CLIENTAUTH FAILURE

View diagnostic details for partial or no data in service graph

After you complete the required service graph configuration and add the Kubernetes cluster in NetScaler ADM, the service graph starts to populate data. In some scenarios, you might observe that service graph displays either partial data or no data. Some of the possible reasons for the partial data or no data in service graph are:

- Static route is not configured
- Kubernetes cluster status is down
- CPX registration is failed
- CPX virtual servers are not licensed
- The required analytics configuration is not set that prevents service graph to load all data

As an administrator, you might find it difficult to analyze the reasons when you see service graph displaying partial data or no data. The diagnostics information in service graph page enables you to see the possible reasons and required actions to troubleshoot the partial data or no data issue.

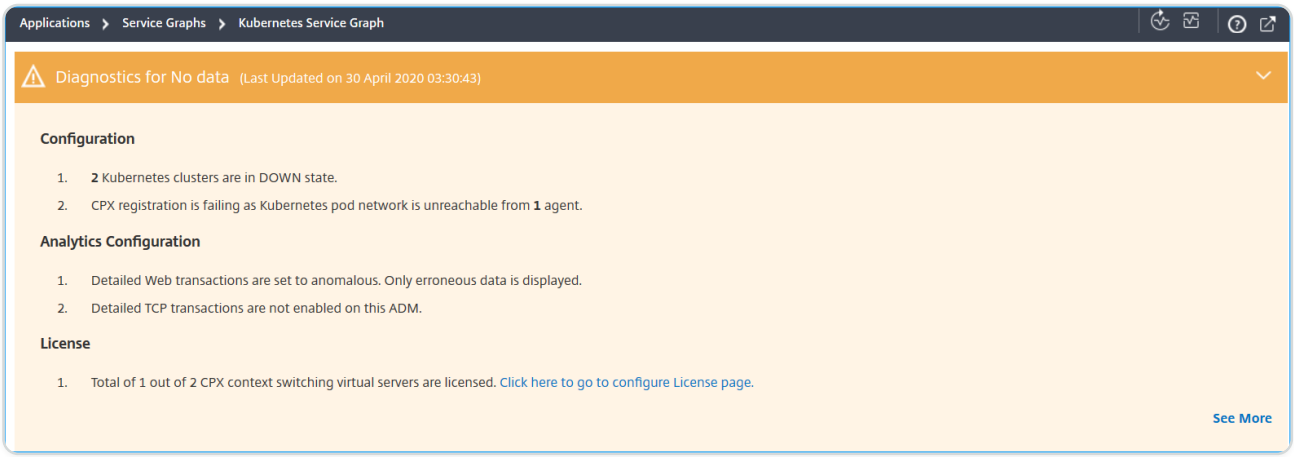
© 1997–2026 Citrix Systems, Inc. All rights reserved.

In NetScaler® ADM, navigate to **Applications** > **Service Graph** and click the **Microservices** tab.

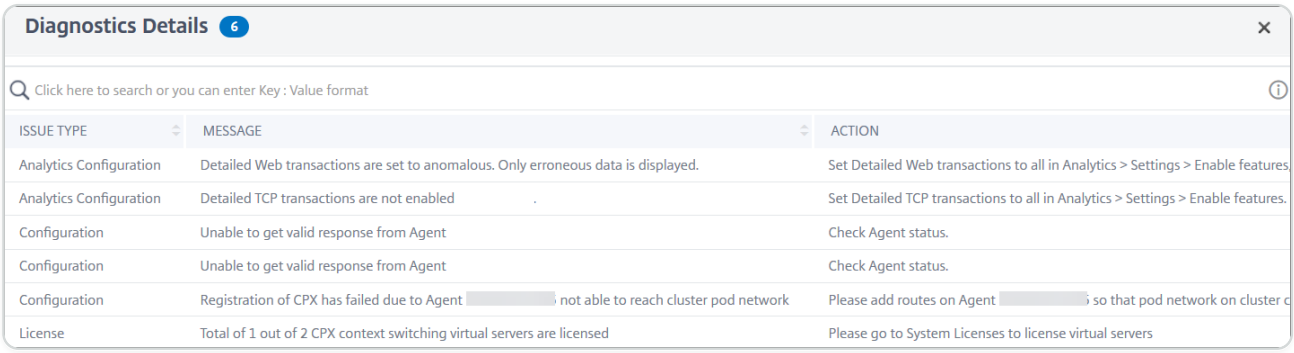
Diagnostics for no data

If service graph does not display any data, the following diagnostics message is displayed.

Click **>** to view details. You can view the possible reasons for service graph not displaying any data. The following image is an example for no data in service graph.



Click **See More** to view details for the issues.



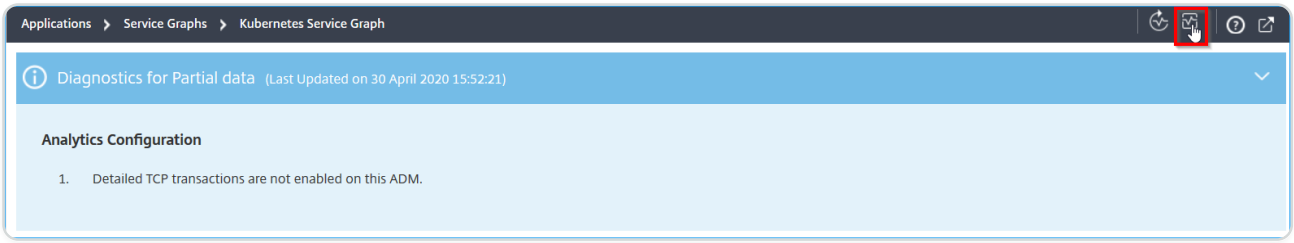
- **Issue Type** – Indicates if the issues occurring from configuration, analytics configuration, or licensing.
- **Message** – Indicates what has caused the issue.
- **Action** – Indicates what action must be performed to troubleshoot the issue.

Diagnostics for partial data

If service graph is displayed only with partial data, click the **Show Diagnostics** button to view the diagnostics information.

The following example indicates the TCP transactions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

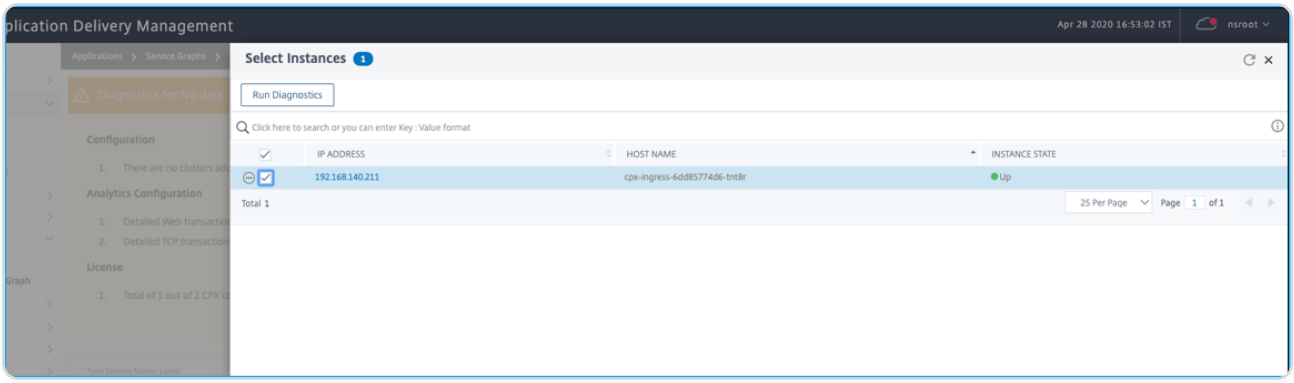


For this example, you must enable the **TCP Transaction Settings** to **All** by navigating to **Settings > Analytics Settings**.

Troubleshooting

As an administrator, using these diagnostics messages, you can validate these issues and try to troubleshoot these issues. After you troubleshoot, NetScaler ADM runs a periodic diagnostic check automatically at a regular interval. After the diagnostics check is complete, the partial data or no data in service graph issue will be resolved.

You can also click **Run Diagnostics**, select the **CPX instances**, and click **Run Diagnostics**.



For more troubleshooting scenarios, see the FAQs.

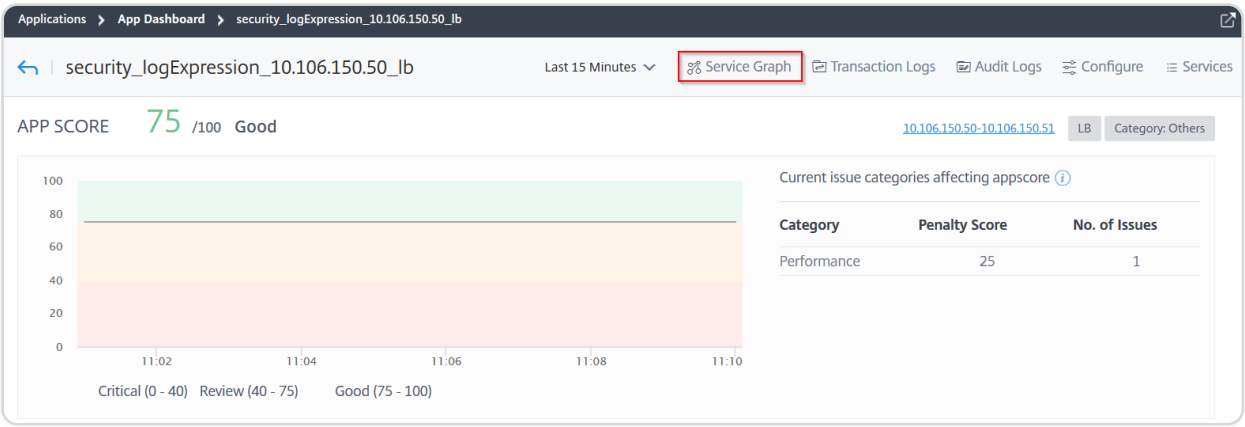
Service graph for applications

To view service graph for an application:

1. Navigate to **Applications** > **Dashboard**.
2. Select an application.

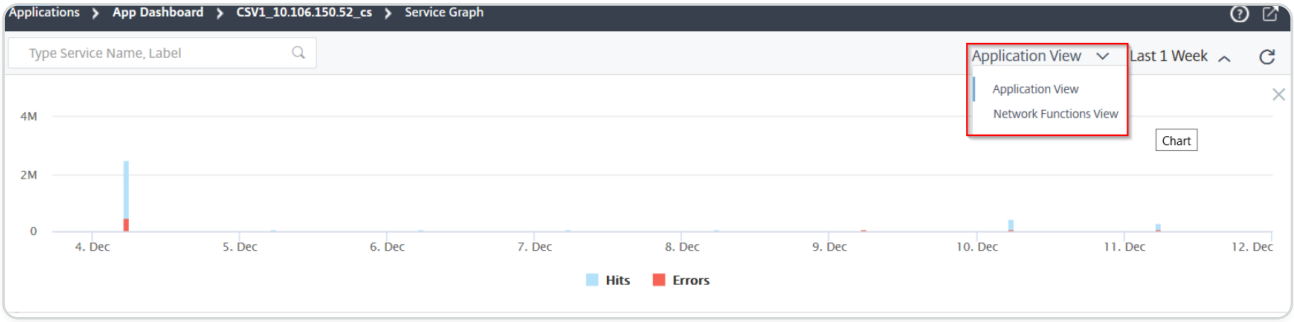
   The application details page is displayed.
3. Select the time duration and click **Service Graph**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

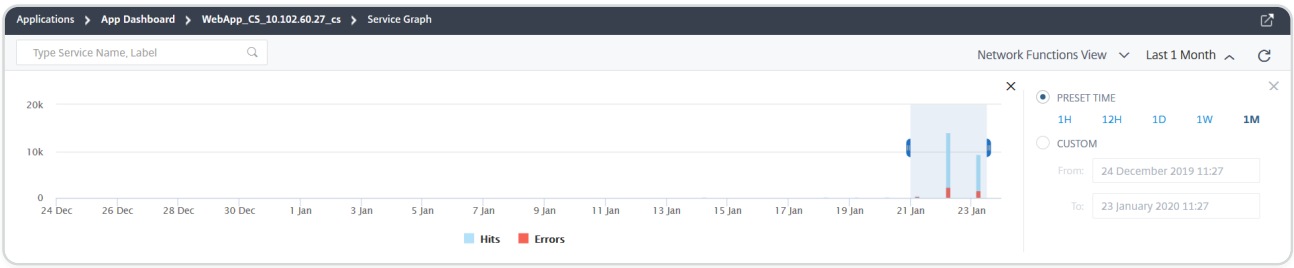


The service graph page is displayed for the selected application.

You can view service graph in **Application View** or in **Network Functions View**.



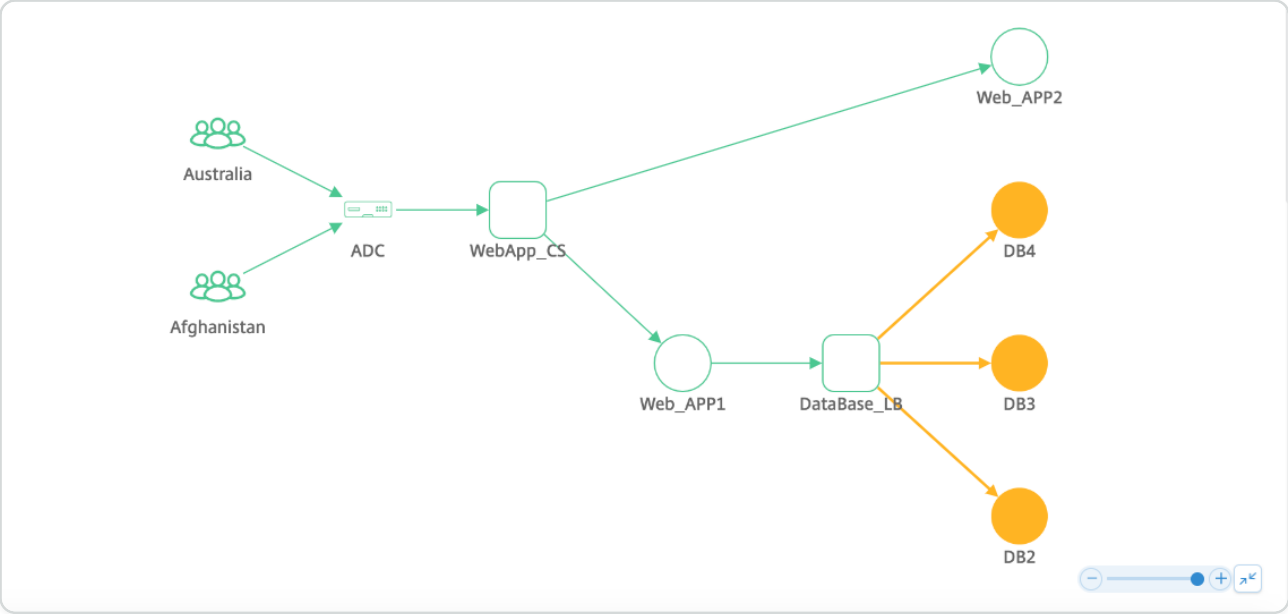
You can also drag and select the hits and errors to modify the results.



Application view

Displays the overview of the application configuration. In this view, you can visualize the communication between client, ADC, and web applications.

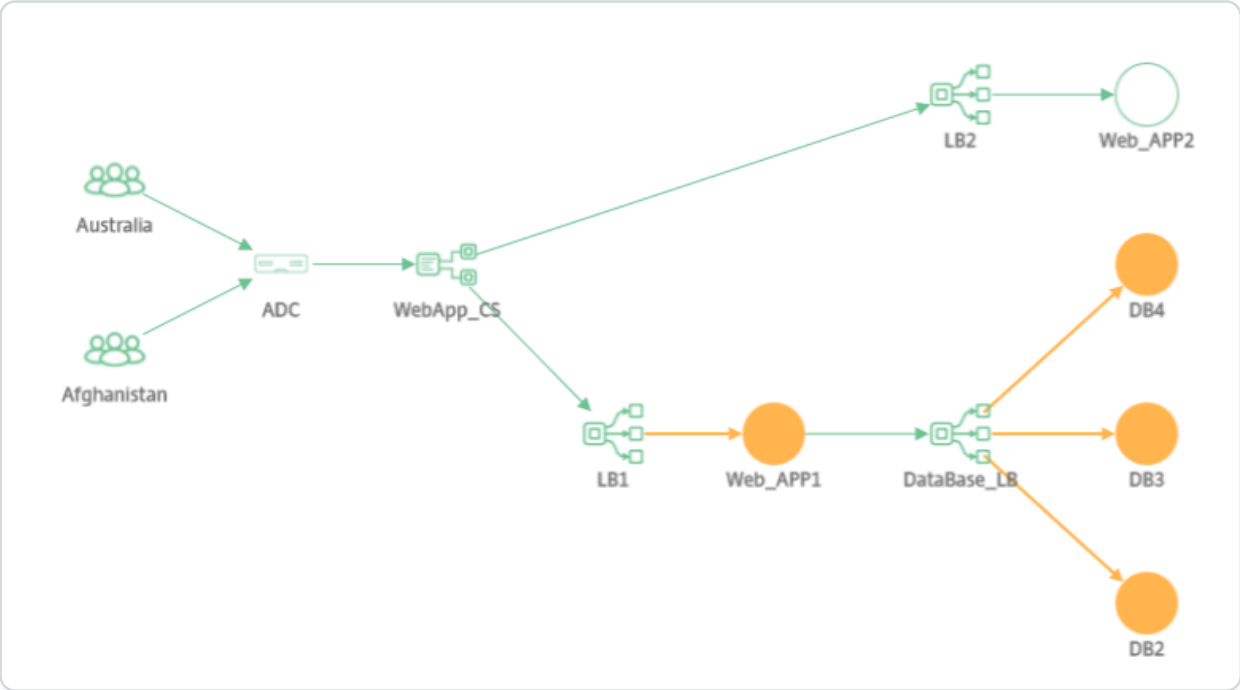
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Network functions view

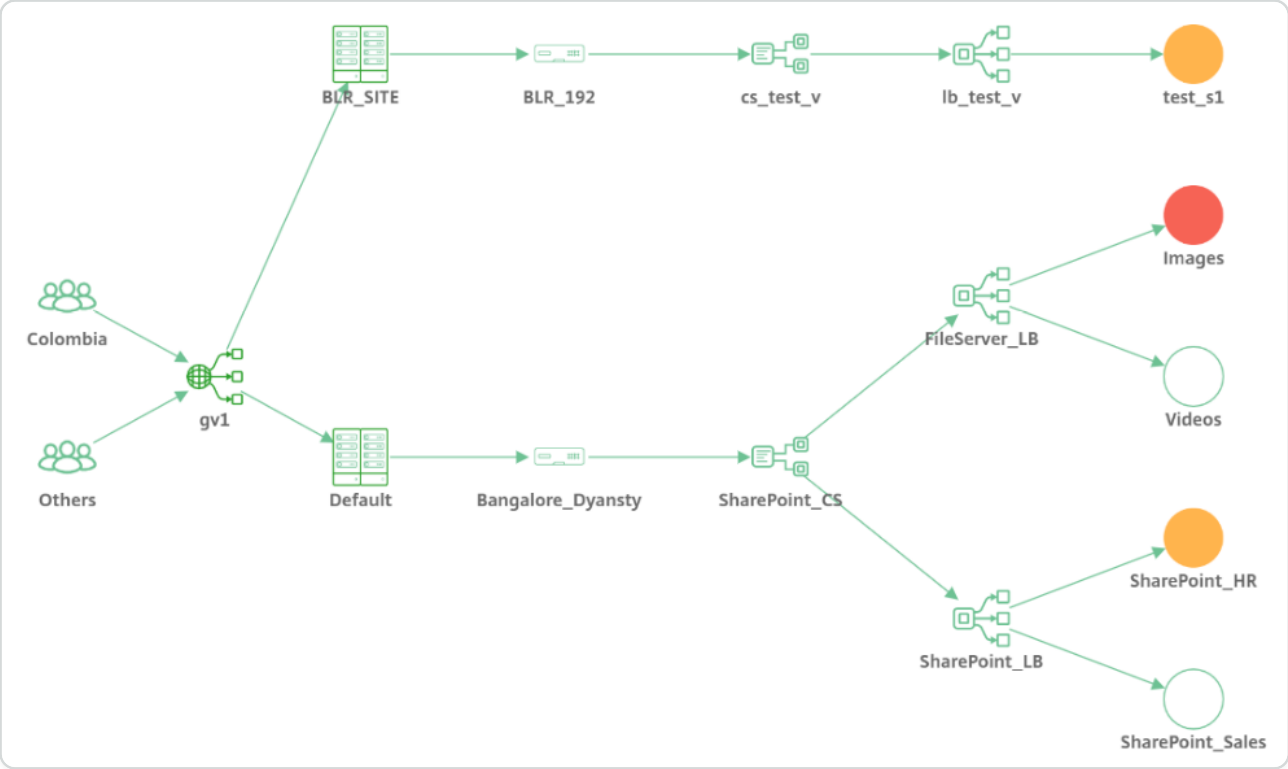
Displays the virtual servers associated with the application. In this view, you can visualize if the ADC is communicating with:

- Content Switching virtual server to access the application
- Load Balancing virtual server to access the application
- Both Content Switching and Load Balancing virtual servers to access the application



For GSLB application, the details are displayed along with the data center and NetScaler.

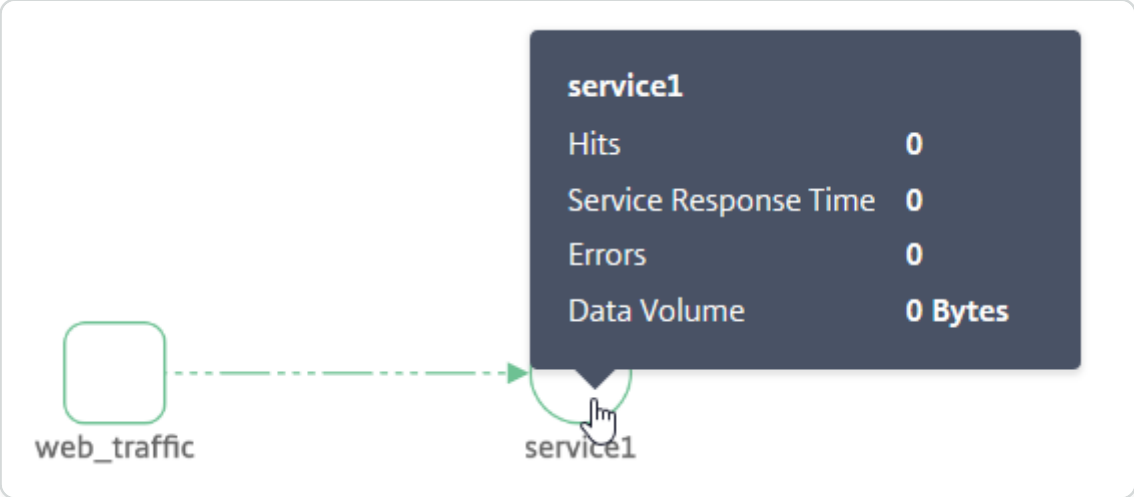
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Service graph view for no active transactions

If no active transactions occur between ADC and web application, Service graph displays only the basic configuration of the application (without client and ADC).

When you hover the mouse pointer on a service or virtual server, the details are displayed as 0 for all metrics because of no transactions.



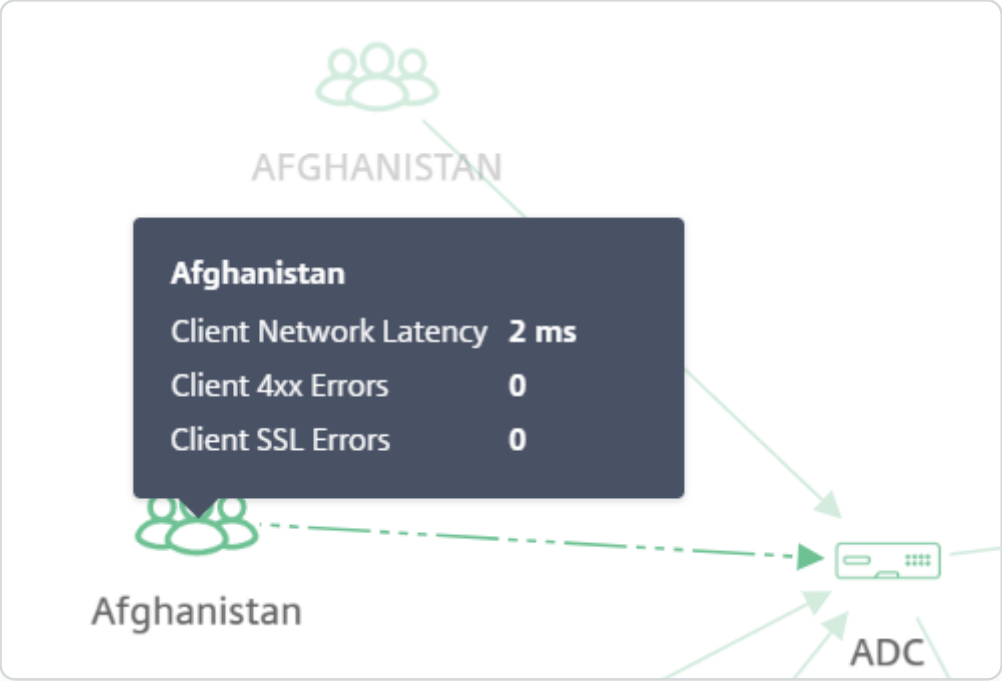
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyze metrics

Hover the mouse pointer on each service to view metrics details either in Application View or Network Function View.

Client metrics

Hover the mouse pointer on the client to view client metrics.

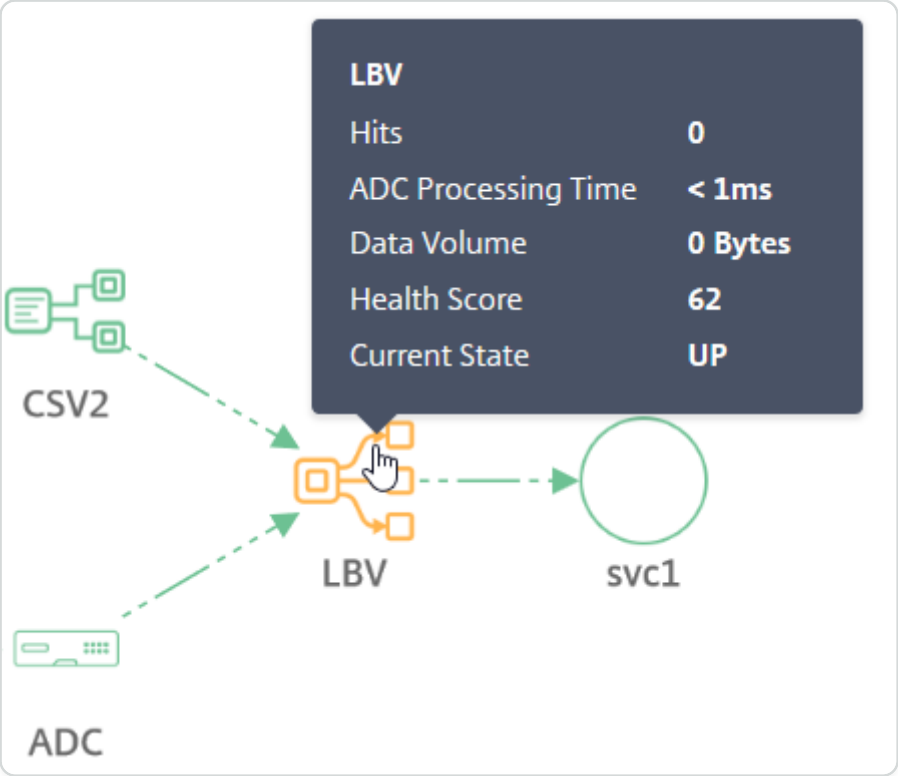


- **Client Network Latency** – Indicates the network latency from the client.
- **Client 4xx Errors** – Indicates the total number of 4xx errors occurred from the client.
- **Client SSL Errors** – Indicates the total number of SSL errors from the client.

Network function metrics

Hover the mouse pointer on a load balancing or content switching service to view the metrics details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

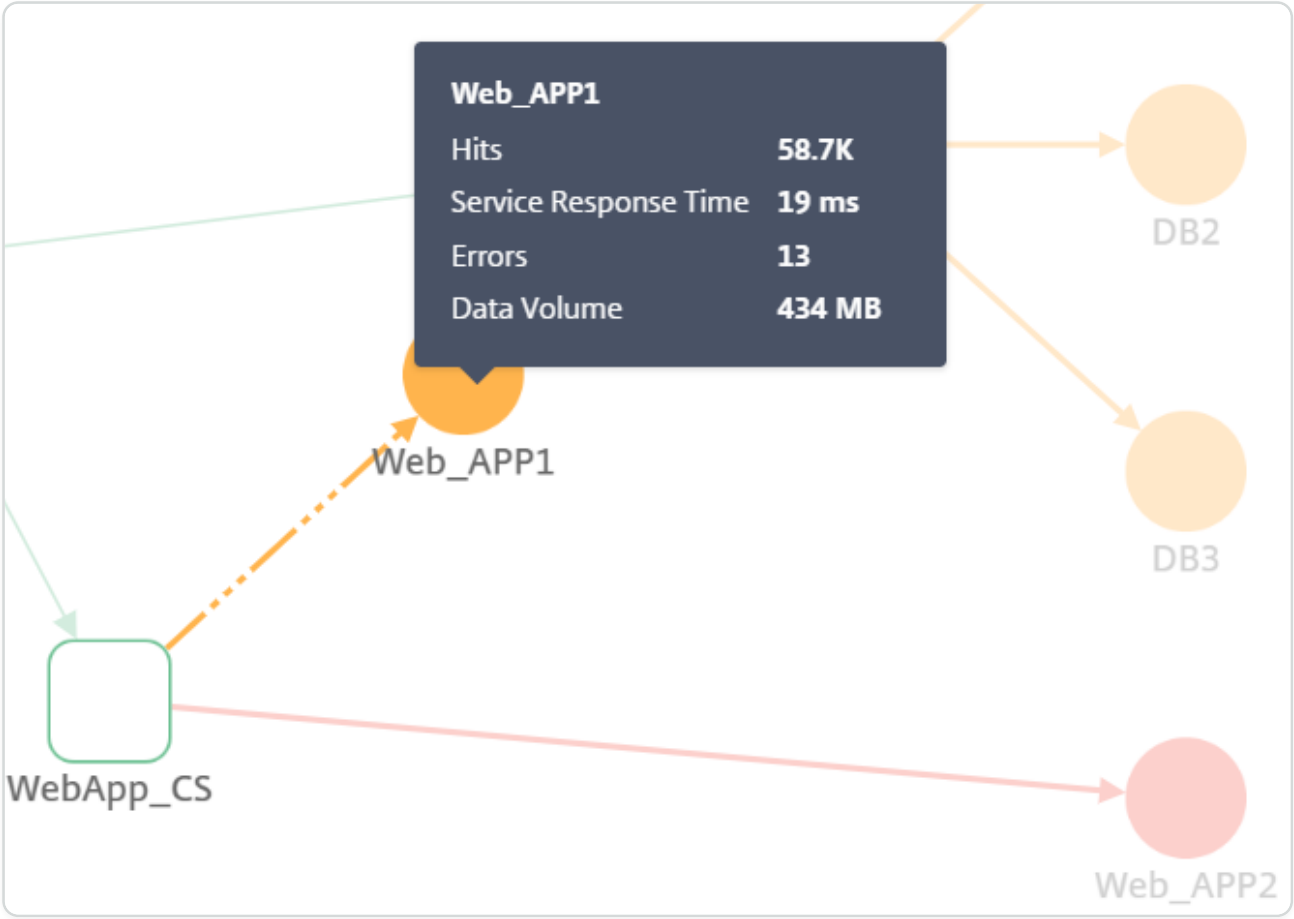


- **Hits** – Indicates the total number of hits received by the virtual server
- **ADC processing time** – Indicates the average processing time by the ADC instance
- **Data volume** – Indicates the total data volume processed by the virtual server
- **Health score** – Indicates the app score
- **Current state** – Indicates the current status of the virtual server

Service metrics

Hover the mouse pointer on a service (web application) to view the metrics

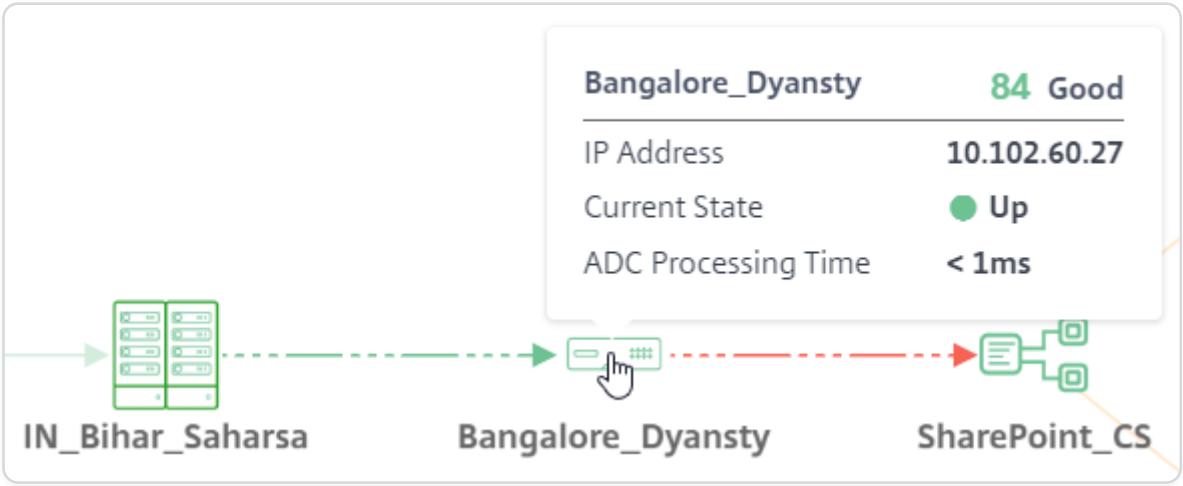
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Hits** – Indicates the total number of hits received by the service
- **Service response time** – Indicates the average response time from the service
- **Errors** – Indicates the total errors occurred from the service
- **Data Volume** – Indicates the total data processed by the service

NetScaler metrics (only for GSLB applications)

Hover the mouse pointer on the ADC to view the metrics.



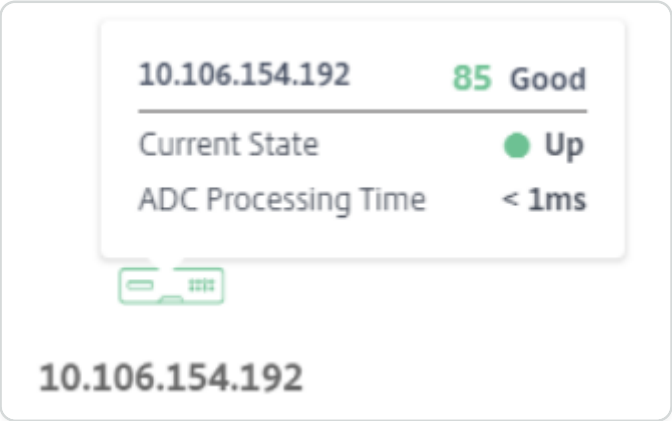
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Displays the host name and the current ADC score. The score is calculated based on the different NetScaler potential issues. For more information, see Instance score.
- **IP Address** – Denotes the NetScaler IP address
- **Current state** – Denotes the NetScaler status such as Up, Down, or Out of service
- **ADC Processing Time** – Denotes the average processing time by the ADC instance

NOTE

If a host name is not assigned to NetScaler:

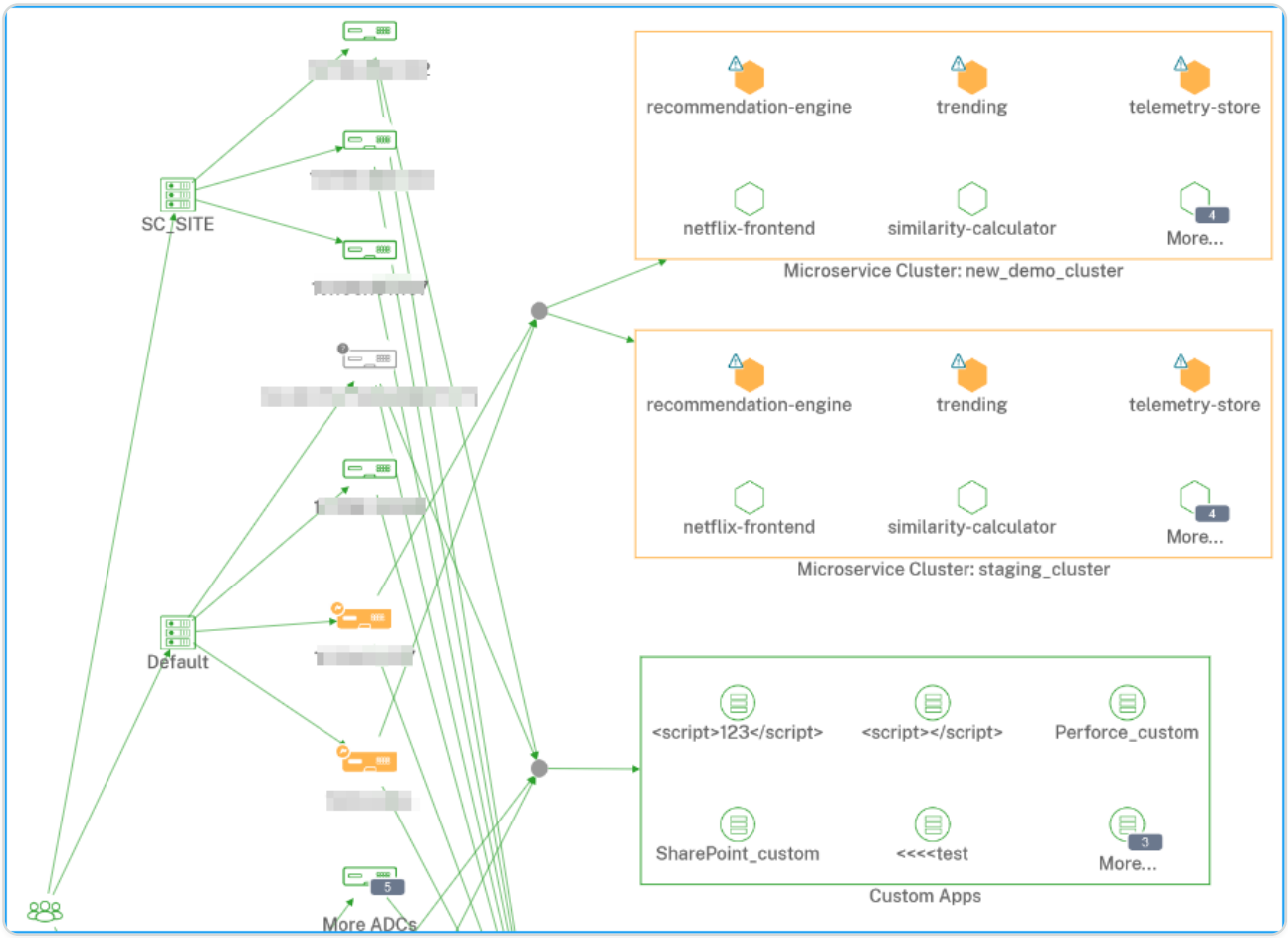
-NetScaler IP address is displayed instead of host name.
-In the metrics, the NetScaler IP address information is not displayed.



Holistic view of all applications in service graph

Navigate to **Applications** > **Service Graph** and then click **Global**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The service graph displays the following for the selected time duration:

- The region from where the users access the specific application

Data centers where the NetScaler instances are hosted

- The total discrete applications from all NetScaler instances

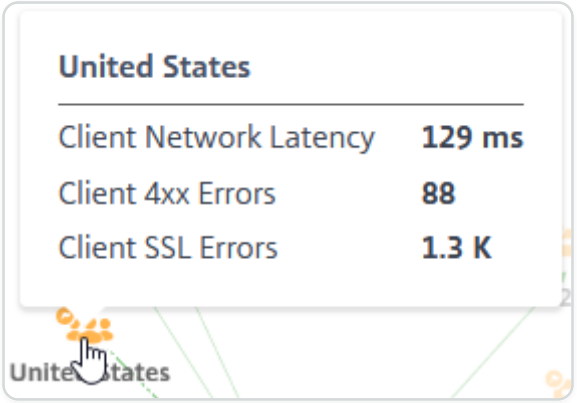
> **NOTE**
>
> If a NetScaler instance does not have discrete applications, the arrow edge towards the Discrete virtual server from the NetScaler instance is not visible

- The total custom applications from all NetScaler instances
- The total microservice applications from the NetScaler CPX instance

View client metrics

Hover the mouse pointer on a client region to view the metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Client Network Latency** - Indicates the average client network latency.
- **Client 4xx Errors** - Indicates the total client 4xx errors.
- **Client SSL Errors** - Indicates the total client SSL errors.

View NetScaler details

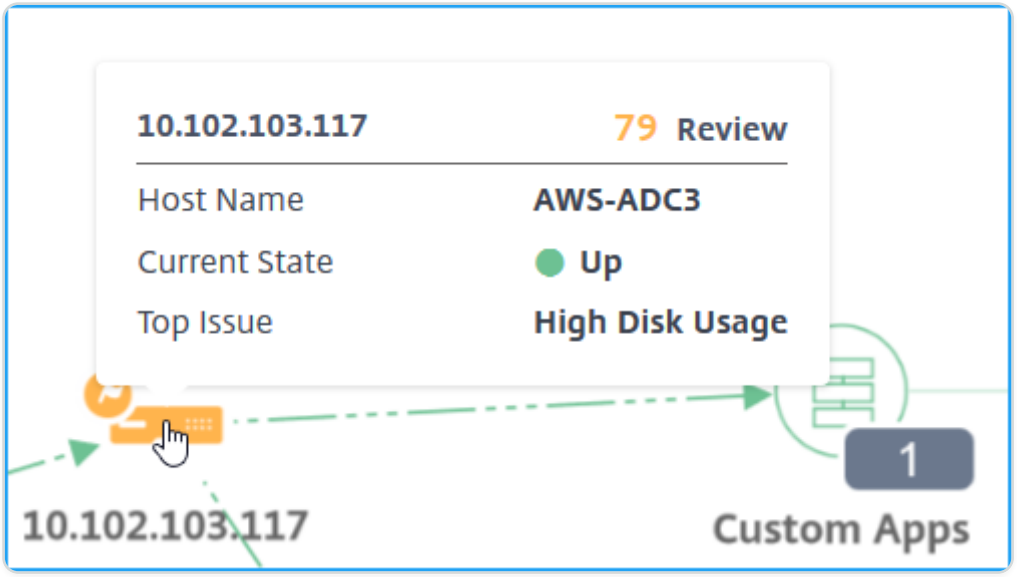
The service graph enables you to view:

- The data center grouped with its total NetScaler instances
- Only the top 4 low-scored NetScaler instances from each data center

Click **More ADCs** to view all NetScaler instances by selecting the respective status (Critical, Review, Good, and Not Applicable) tabs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hover the mouse pointer on a NetScaler instance to view the metrics.



You can view:

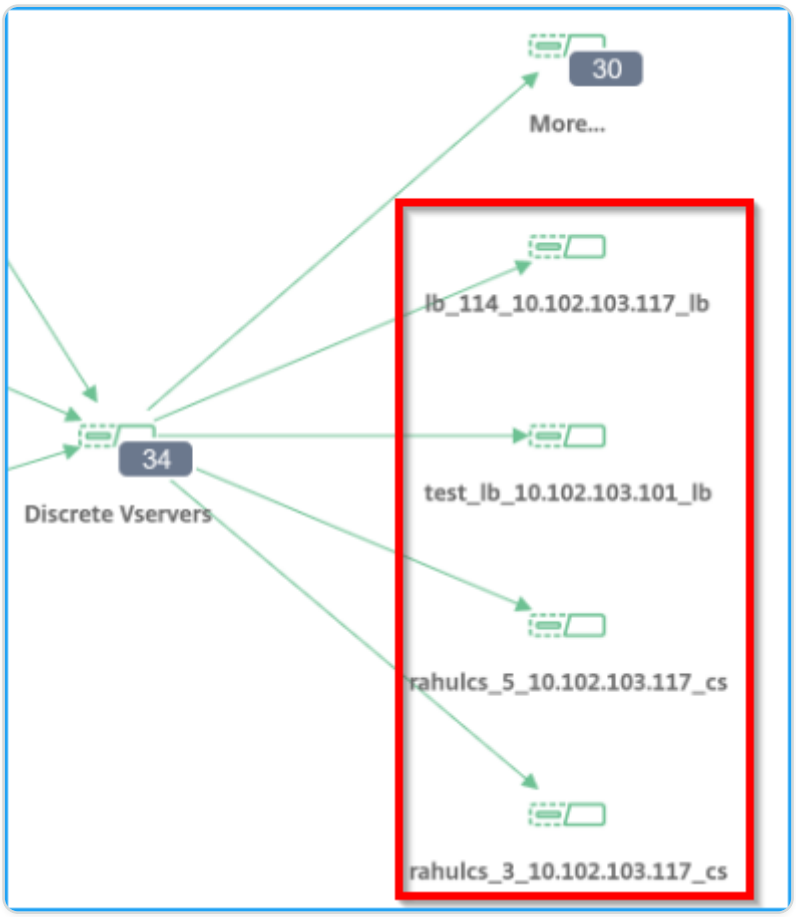
- NetScaler instance IP address and score
- **Host Name** – Indicates the host name that is assigned to the NetScaler instance
- **Current State** – Indicates the current status of the NetScaler instance such as Up, down, out-of-service.
- **Top Issue** – Indicates the top issue that affects the current NetScaler score

Click the **NetScaler instance** to view the instance details such as instance score, key metrics, and issues associated with the ADC instance. For more information, see View instance details in Infrastructure Analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View discrete applications

The service graph displays the top 4 low scored discrete applications.



Consider that you have the following discrete applications:

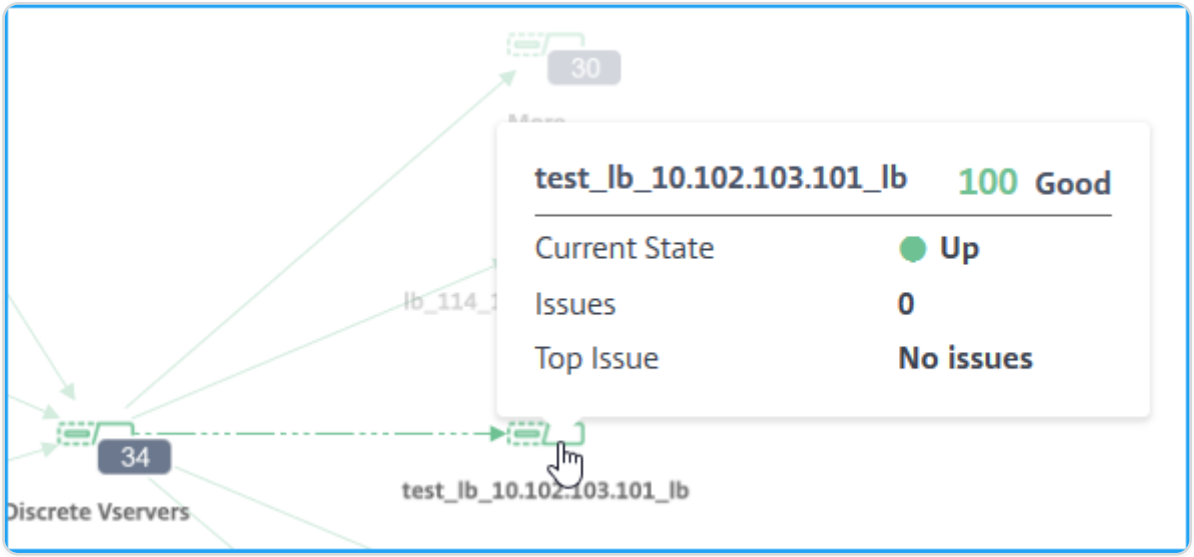
APP NAME	NETSCALER	APP SCORE	APP STATUS
App1	10.102.29.50	35 (Critical)	Up
App2	10.102.29.90	100 (Good)	Down
App 3	10.102.32.40	49 (Review)	Up
App4	10.102.113.208	92 (Good)	Down
App5	10.102.25.25	86 (Good)	Up
App6	10.102.29.41	77 (Good)	Up
App7	10.102.29.102	41 (Review)	Up

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this scenario, you can view App1, App3, App6, and App 7 as the top 4 low-scored applications in service graph.

Similarly, you can also view the top 4 low-scored applications for **Custom** and **Microservices** applications.

Hover the mouse pointer on a service to view the metrics information.

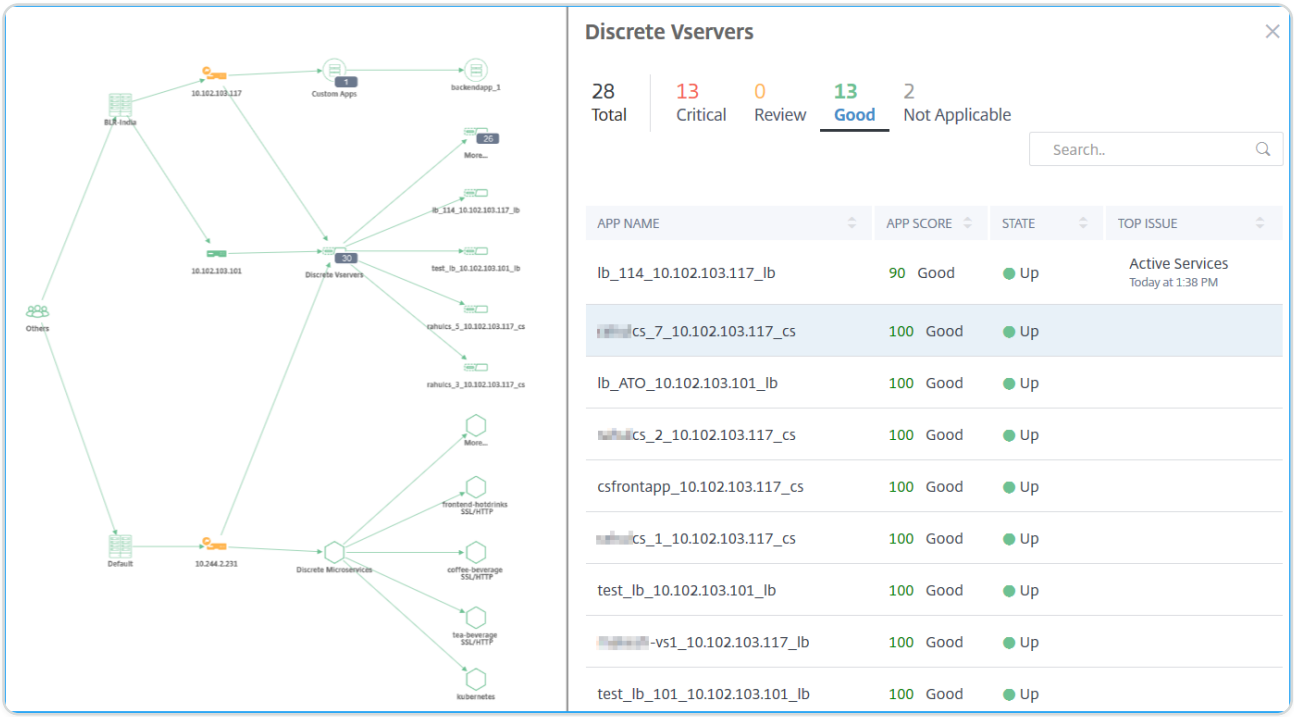


You can view:

- The application name and score
- **Current State** – Indicates the application current status such as Up or Down
- **Issues** – Indicates the total issues applicable for the application
- **Top Issue** – Indicates the top issue that impacts the overall application score

Click **More** to view all discrete applications. The Discrete virtual server page is displayed as shown in the following image:

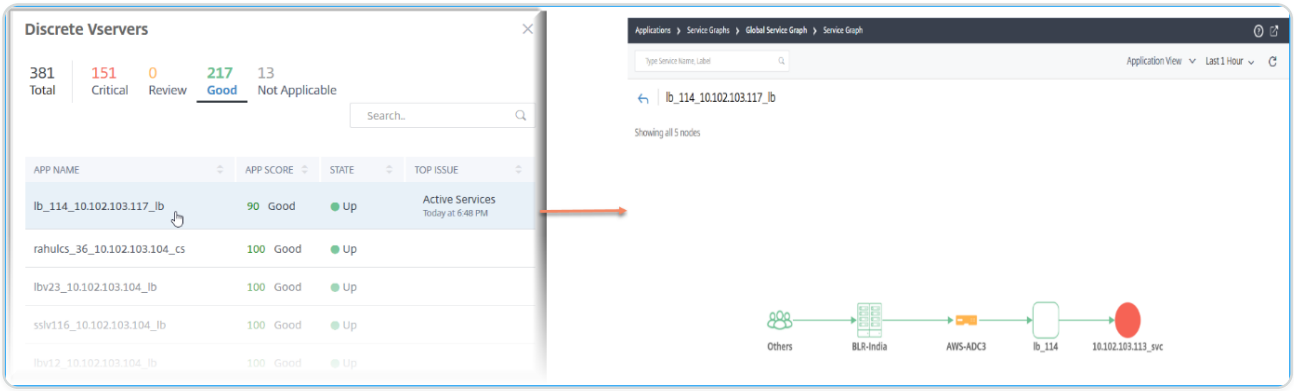
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The virtual servers are displayed according to the status.

- **Total** – Total discrete applications
- **Critical** – App score is between 0 and < 40
- **Review** – App score is between 40 and < 75
- **Good** – App score is > 75
- **Not Applicable** – App is not bound to any virtual server

You can click each tab to view the virtual servers. When you click an application, the service graph for the selected application is displayed.



For more information, see Service Graph for applications.

View microservice applications

The service graph also displays all microservice applications that belong to the Kubernetes clusters. Hover the mouse pointer on a service to view the metrics details.

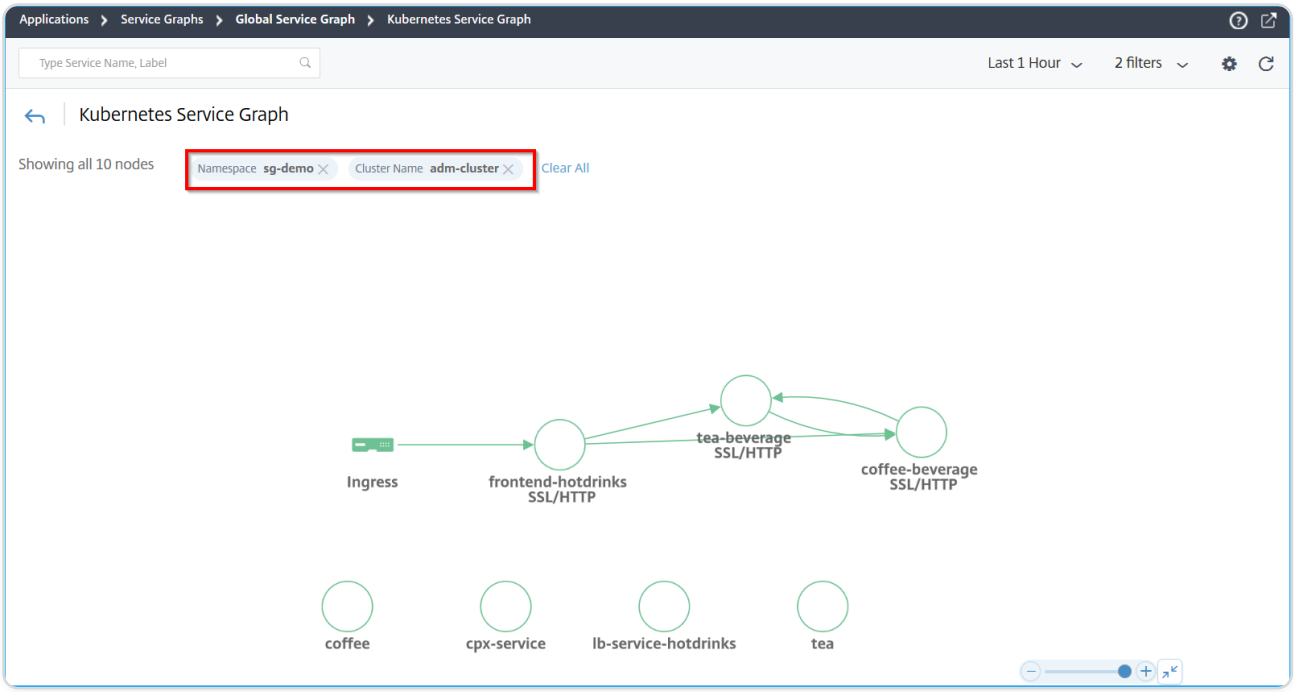
© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view:

- The service name
- The protocol used by the service such as SSL, HTTP, TCP, SSL over HTTP
- **Hits** – The total number of hits received by the service
- **Service Response Time** – The average response time taken from the service.

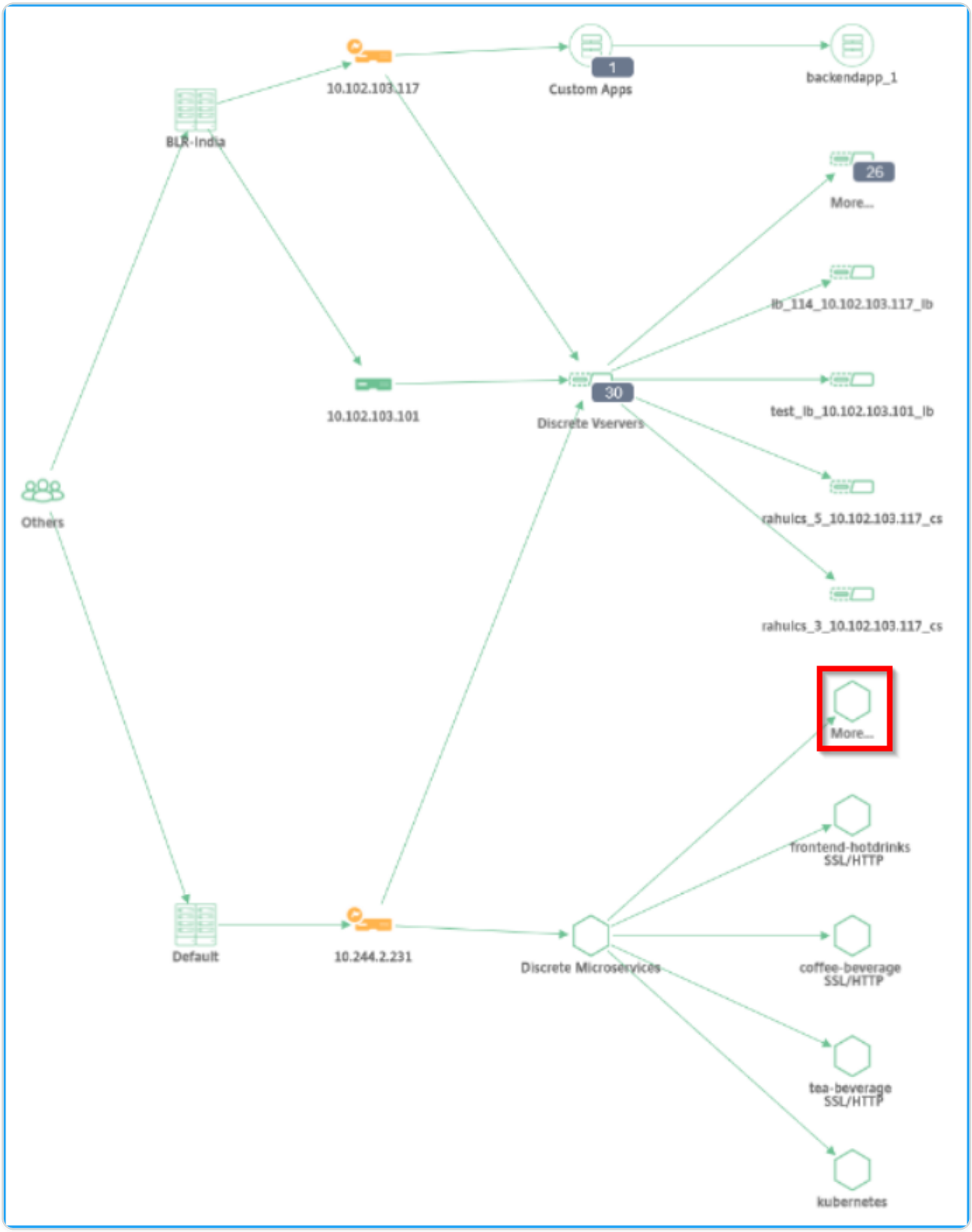
  (Response time = Client RTT + request last byte – request first byte)
- **Errors** – The total errors such as 4xx, 5xx, and so on
- **Data Volume** – The total volume of data processed by the service
- **Namespace** – The namespace of the service
- **Cluster Name** – The cluster name where the service is hosted
- **SSL Server Errors** – The total SSL errors from the service

When you click a service, the Kubernetes service graph for the selected service is displayed, along with the service namespace and cluster name filters applied.



Click **More** to view the Kubernetes service graph that has all services. For more information on Kubernetes service graph, see Service graph for cloud native applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



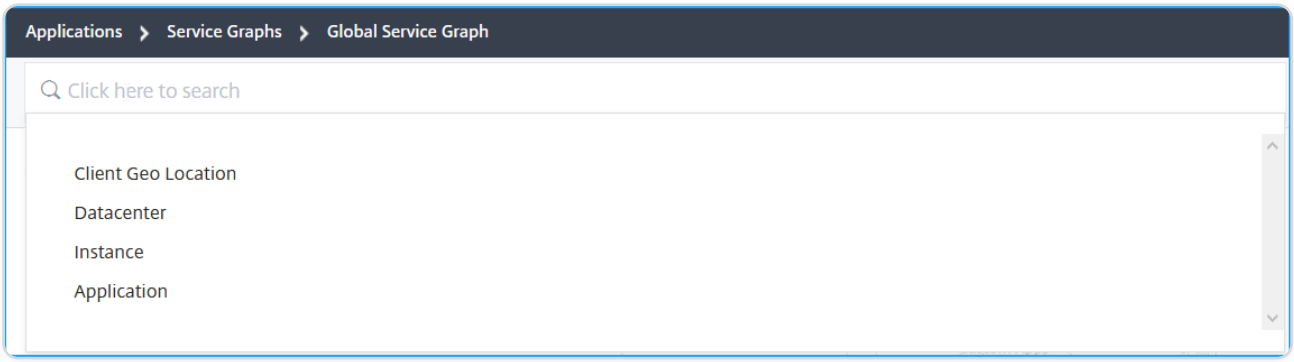
Search bar to filter results

You can use the search bar to filter results. As an administrator, this search bar enables you to narrow-down quickly to a particular instance/client/application/data center, when you have:

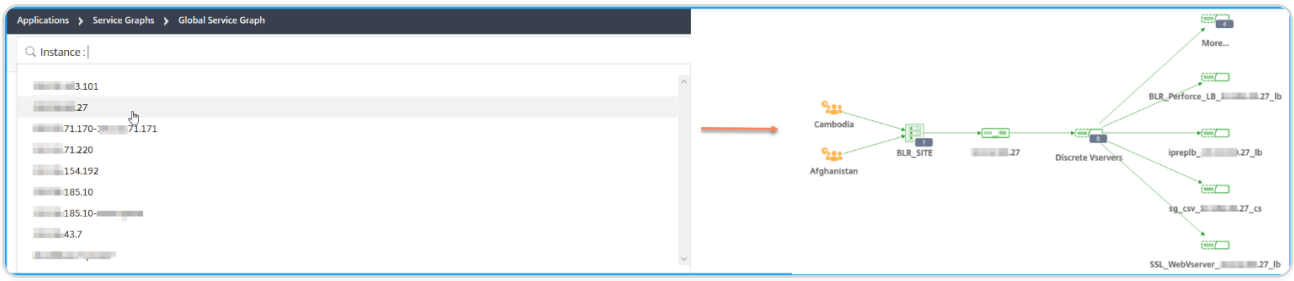
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A large enterprise with many data centers
- Configured many NetScaler instances for each data center
- Configured many applications deployed or accessed through each NetScaler instance
- Clients accessing the application from different locations

Place the mouse pointer on the search bar and select the category that you want to create the filter.



For example, if you want to view a particular ADC instance, select **Instance** from the search bar and select the instance IP address. The global service graph displays the selected instance and its associated applications, data centers, and client locations.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations. You can create a StyleBook for configuring a specific feature of NetScaler, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Lync.

StyleBooks fit in well with the principles of Infrastructure-as-code that is practiced by DevOps teams, where configurations are declarative and version-controlled. The configurations are also repeated and are deployed as a whole. StyleBooks offer the following advantages:

- **Declarative**: StyleBooks are written in a declarative rather than imperative syntax. Stylebooks allow you to focus on describing the outcome or the "desired state" of the configuration rather than the step-by-step instructions on how to achieve it on a particular NetScaler instance. NetScaler Application Delivery Management (ADM) computes the diff between existing state on a NetScaler and the desired state you specified, and makes the necessary edits to the infrastructure. Because StyleBooks use a declarative syntax, written in YAML, components of a StyleBook can be specified in any order, and NetScaler ADM determines the correct order based on their computed dependencies.
- **Atomic**: When you use StyleBooks to deploy configurations, the full configuration is deployed or none of it is deployed and this ensures that the infrastructure is always left in a consistent state.
- **Versioned**: A StyleBook has a name, namespace, and a version number that uniquely distinguishes it from any other StyleBook in the system. Any modification to a StyleBook requires an update to its version number (or to its name or namespace) to maintain this unique character. The version update also allows you to maintain multiple versions of the same StyleBook.
- **Composable**: After a StyleBook is defined, the StyleBook can be used as a unit to build other StyleBooks. You can avoid repeating common patterns of configuration. It also allows you to establish standard building blocks in your organization. Because StyleBooks are versioned, changes to existing StyleBooks results in new StyleBooks, therefore ensuring that dependent StyleBooks are never unintentionally broken.
- **App-Centric**: StyleBooks can be used to define the NetScaler configuration of a full application. The configuration of the application can be abstracted by using parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Therefore, users who create configurations from a StyleBook can interact with a simple interface consisting of filling a few parameters to create what can be a complex NetScaler configuration. Configurations that are created from StyleBooks are not tied to the infrastructure. A single configuration can thus be deployed on one or multiple NetScalers, and can also be moved among instances.

- **Auto-Generated UI**: NetScaler® ADM auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the NetScaler ADM GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.
- **API-driven**: All configuration operations are supported by using the NetScaler ADM GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

You can use one StyleBook to create multiple configurations. Each configuration is saved as a config pack. For example, consider that you have a StyleBook that defines a typical HTTP load balancing application configuration. You can create a configuration with values for the load balancing entities and execute it on a NetScaler instance. This configuration is saved as a config pack. You can use the same StyleBook to create another configuration with different values and execute it on the same or a different NetScaler instance. A new config pack is created for this configuration. A config pack is saved both on NetScaler ADM and on the NetScaler instance on which the configuration is executed.

You can either use default StyleBooks, shipped with NetScaler ADM, to create configurations for your deployment, or design your own StyleBooks and import them to NetScaler ADM. You can use the StyleBooks to create configurations either by using the NetScaler ADM GUI or by using APIs.

This document includes the following information:

- How to view StyleBooks
- Default StyleBooks
- Stylebooks developed for business applications
- Custom StyleBooks
- APIs in StyleBooks
- StyleBooks grammar

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook categories

There are two StyleBook categories in NetScaler® Application Delivery Management (ADM). They are the default StyleBooks and the custom StyleBooks. Whether it is a default or custom, a StyleBook is either a public or a private StyleBook. In NetScaler ADM, you can view all the StyleBooks that are present in the system, regardless of their type or visibility status. You can also view a graphical display of how StyleBooks are connected with each other.

This document explains the different types of StyleBooks. Also, it explains the following actions that you can perform on the StyleBooks from NetScaler ADM:

- Download a custom StyleBook and make modifications, or create a StyleBook based on an existing one.
- Hide ADM default StyleBooks.
- Delete a custom StyleBook from NetScaler ADM.
- Add tags to the StyleBooks.

Default and custom StyleBooks

- **Default StyleBooks** are the StyleBooks shipped with NetScaler ADM and they allow you to create configurations that you can deploy on your NetScaler instances. You cannot delete default StyleBooks, but you can hide them from the ADM GUI.
- **Custom StyleBooks** are your own StyleBooks that you imported in to NetScaler ADM.

Both default and custom StyleBooks can be either public or private.

Public and private StyleBooks

StyleBooks from which you can create configuration packs can be categorized as **public** StyleBooks. That is, they are all available for your direct usage to create configurations from the NetScaler ADM GUI and APIs.

But, some StyleBooks are used as building blocks for other StyleBooks. Such StyleBooks are marked as **private**. The private StyleBooks cannot be directly used to create configuration packs from the NetScaler ADM GUI. But, you can still display and view these StyleBooks on NetScaler ADM. To mark any of your custom StyleBooks as **private**, set the private attribute in the StyleBook to **true**. You can still use private StyleBooks to create configuration packs using the NetScaler ADM APIs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of a StyleBook marked as private

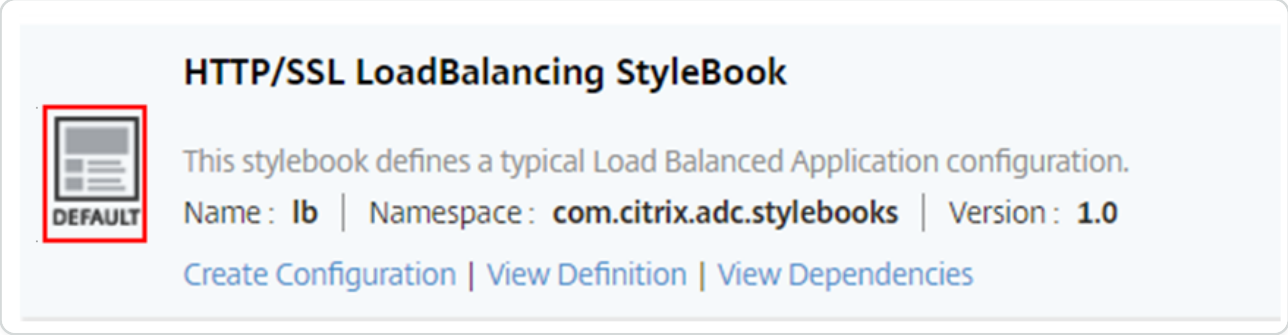
```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

View StyleBooks

The number of StyleBooks - both default and private are increasing in NetScaler 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.

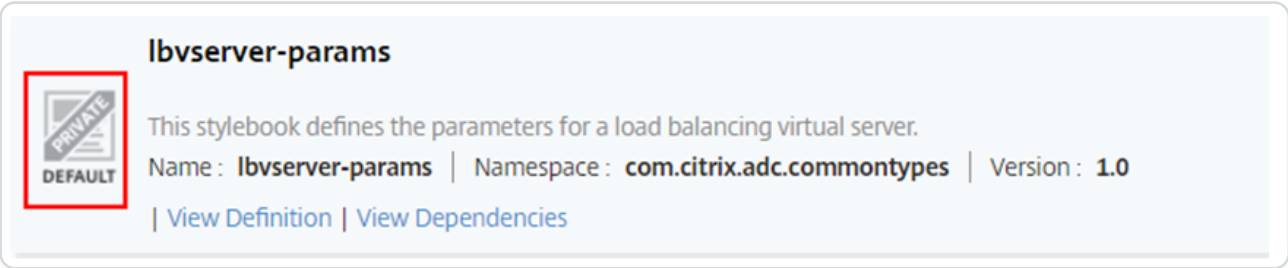
In NetScaler ADM, when you navigate to **Applications** > **StyleBooks**, you can view a list of StyleBooks that are present in the system.

A default public StyleBook has the following icon on its panel:



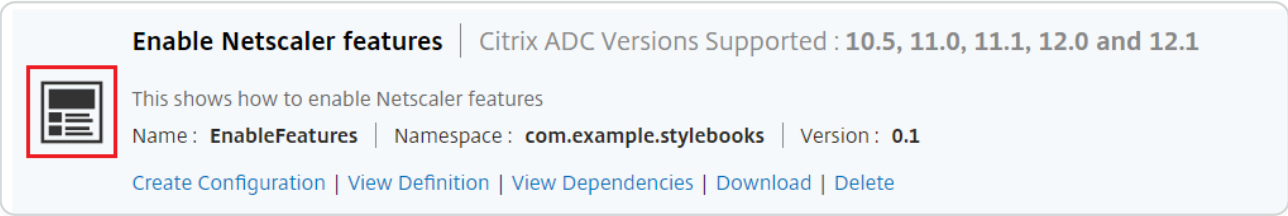
Whereas a default private StyleBook has an icon that declares it as a private StyleBook:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

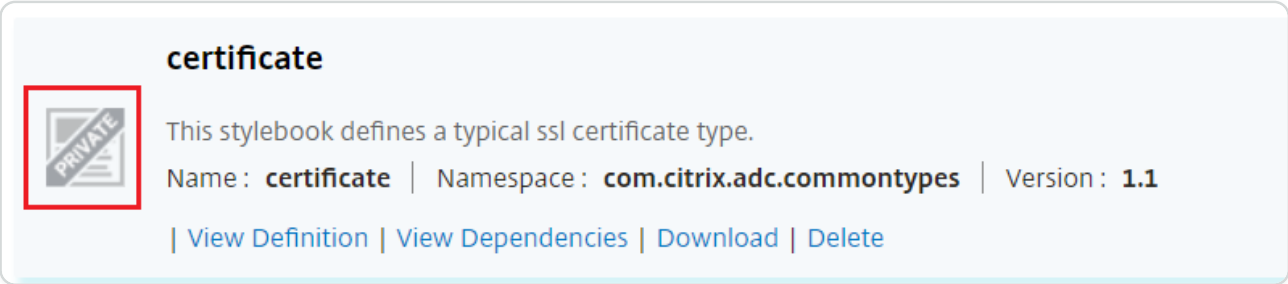


While you can view the definition and dependencies of a private StyleBook, you cannot create a configuration packs from a private StyleBook using the GUI. The main purpose of a private StyleBook is to use it as a building block for another StyleBook. Using the building-blocks-StyleBooks encourages the reuse of common configuration patterns.

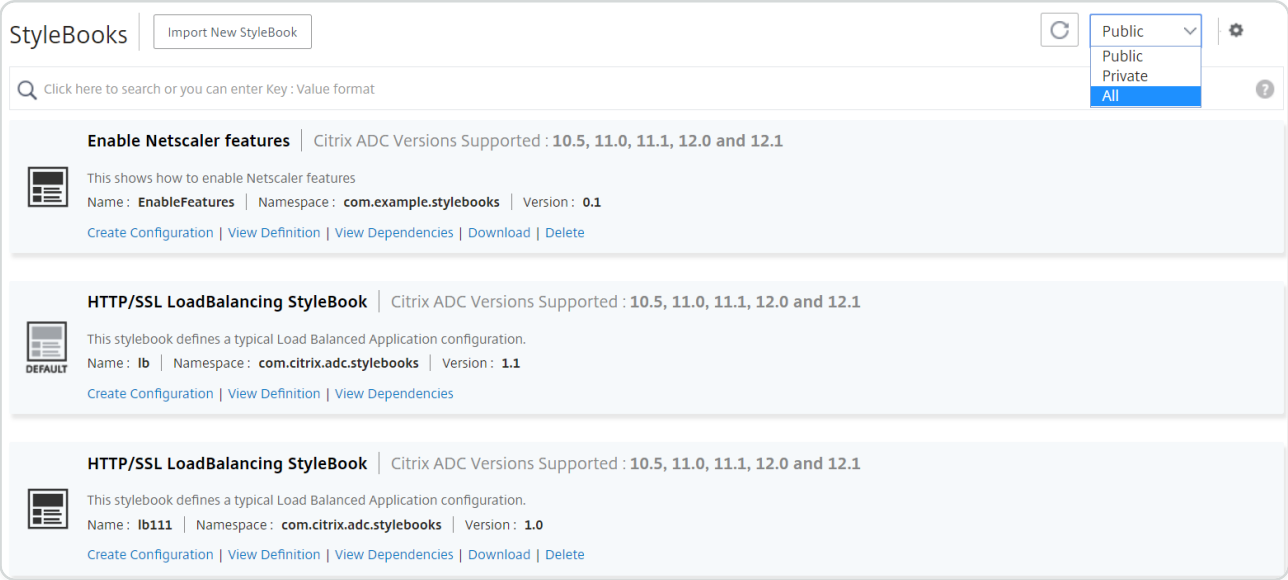
A custom public StyleBook has a different icon as shown in the following image:



While a custom private StyleBook appears with this icon:

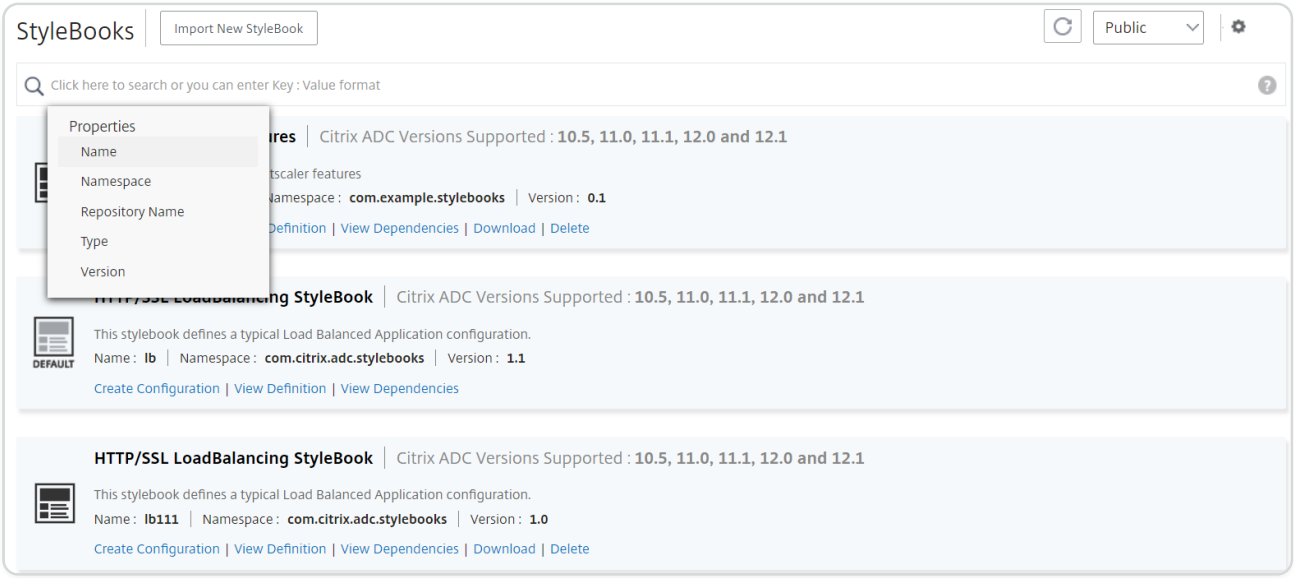


At the top right-side of the page, you can see an option to select the type of StyleBooks to view. There are three options - all, public, or private StyleBooks. Click one of the options.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also search for a particular StyleBook by clicking the search icon. You can search by name, namespace, and version attributes or a combination of these options. The search operation is not case-sensitive.



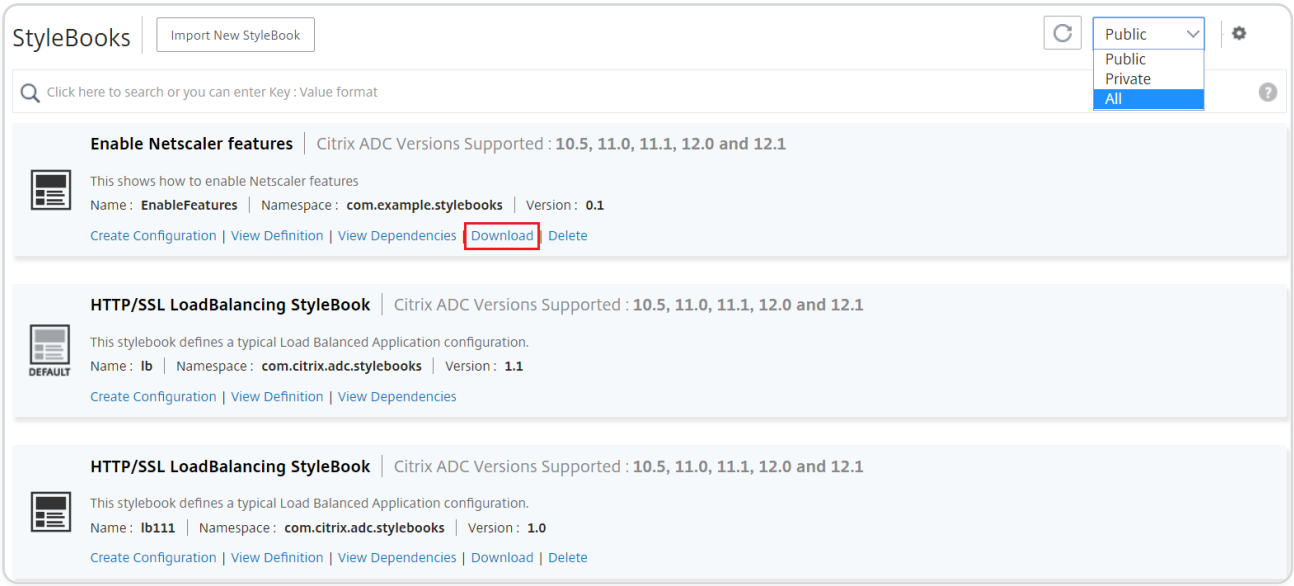
Download custom StyleBooks

To download the custom StyleBooks from NetScaler ADM, navigate to **Applications** > **StyleBooks** > **Configurations**. In the list of StyleBooks that are displayed on the right-side panel, check the option to download the custom-defined StyleBooks. Click **Download**. If the StyleBook has dependent custom StyleBooks, you can include the dependent StyleBooks in the downloaded bundle.

NOTE:

You can download custom StyleBooks that are marked as either public or private.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

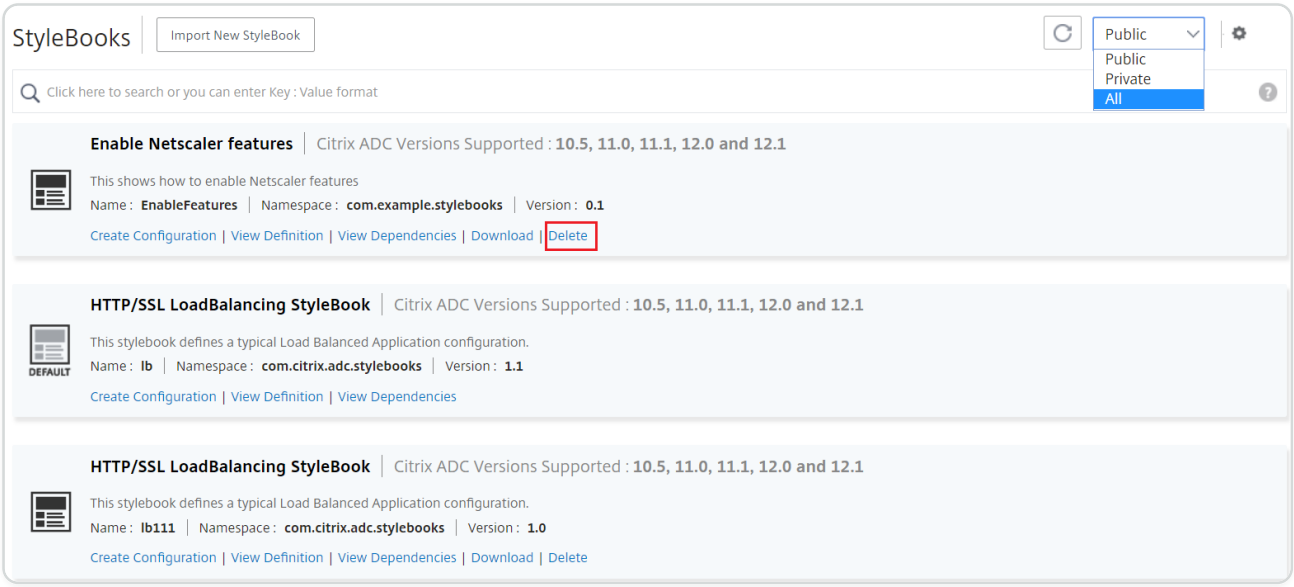


NOTE:

You cannot download NetScaler ADM default StyleBooks. You can view their definitions and dependencies. To do so, click **View Definition** and **View Dependencies** links on the StyleBook panel.

Delete custom StyleBooks

You can also delete a custom StyleBook by clicking the **Delete** button. A pop-up window prompts you to confirm if you want to remove the StyleBook from NetScaler ADM. If the StyleBook uses other custom StyleBooks, you can choose to remove such StyleBooks by selecting the check box.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Do not delete a custom StyleBook if it has dependent StyleBooks in NetScaler ADM. Otherwise, it would break the existing StyleBooks.

View StyleBook dependencies

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. You can study the existing default StyleBooks in NetScaler ADM to learn how one StyleBook can be built on top of another StyleBook.

NetScaler ADM allows you to view a graphical display of how StyleBooks are connected with each other. This representation is especially useful for complex StyleBooks that are built using other StyleBooks as building blocks. By looking at the dependency graph, it is possible to see the relationships and dependencies among multiple StyleBooks.

A StyleBook used by other StyleBooks cannot be removed from the system because it would break the existing StyleBooks. Using the dependency graph display, you can identify which StyleBooks are preventing the removal of a StyleBook.

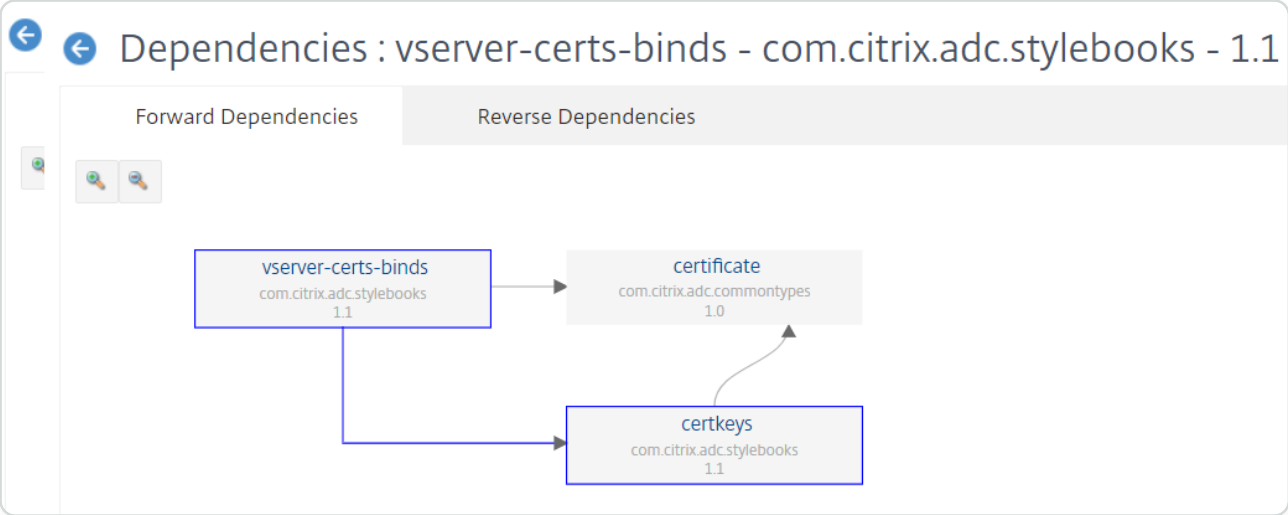
To view StyleBook dependencies

In NetScaler ADM, navigate to **Applications** > **StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler ADM. Scroll down and find your StyleBook. The **StyleBook** tile displays links to create a configuration, to view the StyleBook definition, and to view the StyleBook dependencies. Click **View Dependencies**.

Forward dependencies

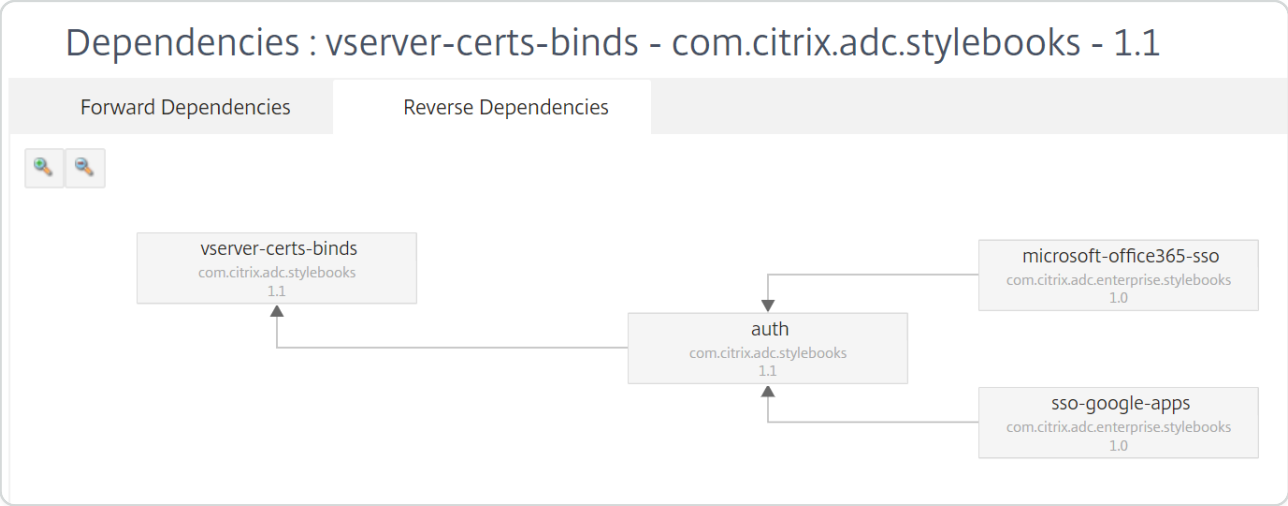
The **Forward Dependencies** tab allows you to view the different default StyleBooks that your StyleBook is using. Follow the arrows to find the StyleBook that a StyleBook is using. When you point your mouse to one of the arrows, the arrow and the StyleBooks that are connected to one another are highlighted. You can also click the StyleBook names to view the definition of that StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 the 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.



Audit ADC configuration against configuration pack

You can compare the changes made by a StyleBook configuration pack to the current ADC configuration. With this comparison, you can do the following:

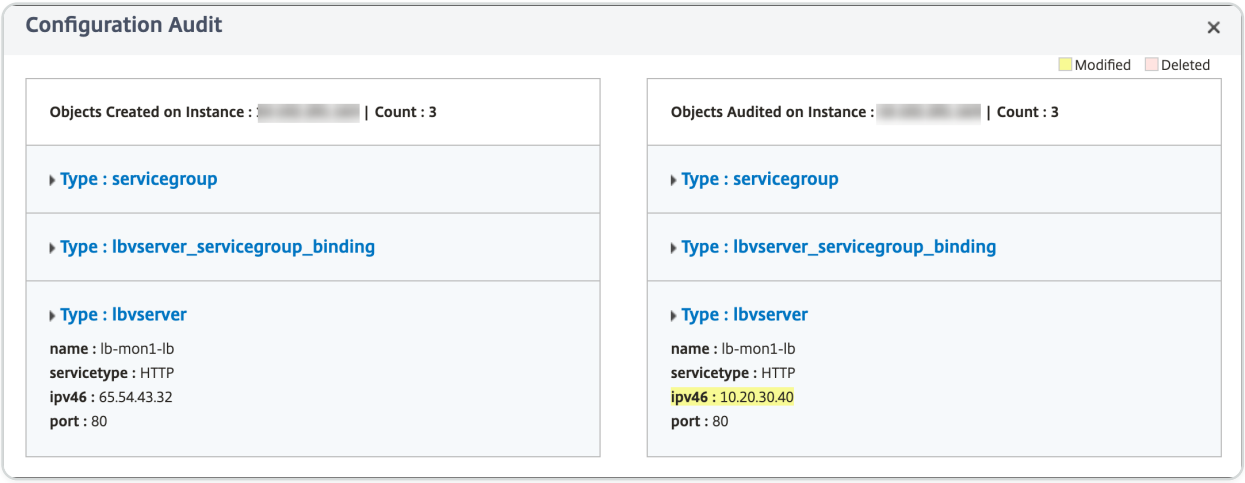
- Detect the configuration drift between StyleBook configuration pack and ADC configuration.
- Identify any modified and deleted objects on the ADC that do not reflect the changes made by the configuration pack.

To compare the configuration pack changes to the ADCs config, do the following.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Applications** > **StyleBooks** > **Configurations**.
2. Click **Configuration Audit**.

   The Configuration Audit page displays the objects created and audited.

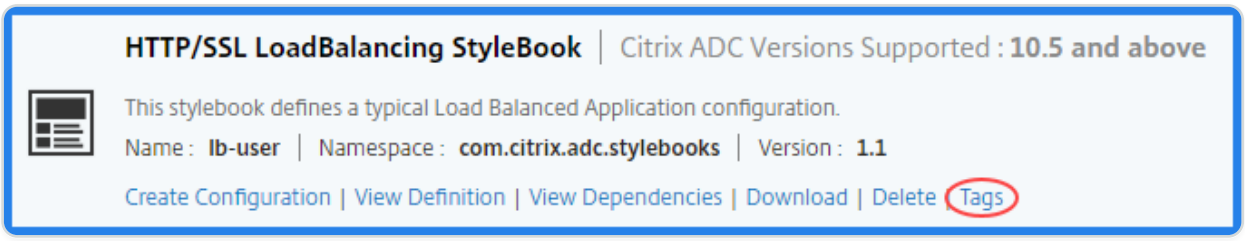


Create a tag for the StyleBook

You can add tags to any StyleBook in NetScaler ADM. Tags are key-value pairs that allow you to group StyleBooks using different criteria. You can use these tags while searching or filtering for StyleBooks in NetScaler ADM.

To add a tag to the StyleBook:

1. Navigate to **Applications** > **StyleBooks**.
2. Select **Tags** on the StyleBook for which you want to add tags.

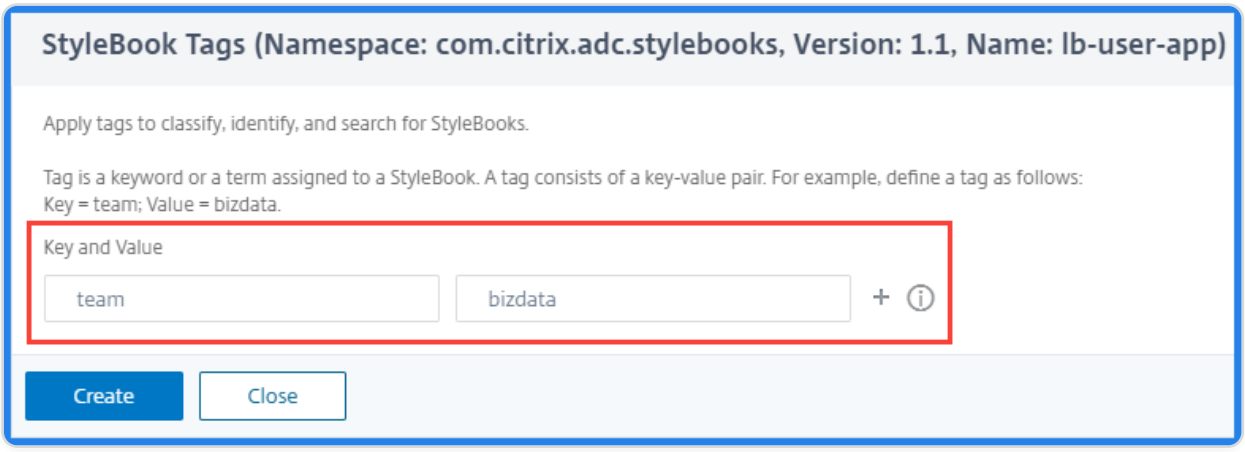


   You can add tags to all types of StyleBooks.

3. Specify the required **Key** and **Value** information that helps you filter the StyleBook.

   For example, Key=team and Value=bizdata

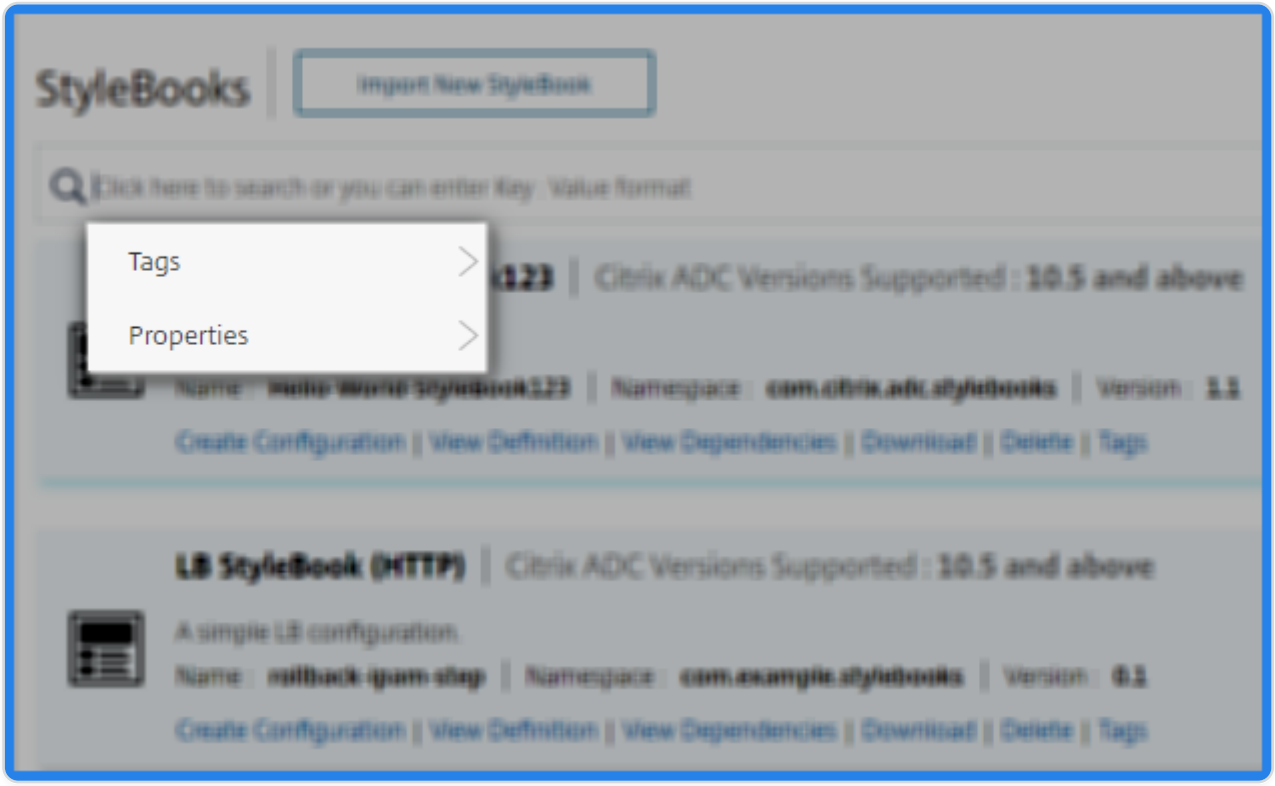
© 1997–2026 Citrix Systems, Inc. All rights reserved.



To add more tags, click **+**.

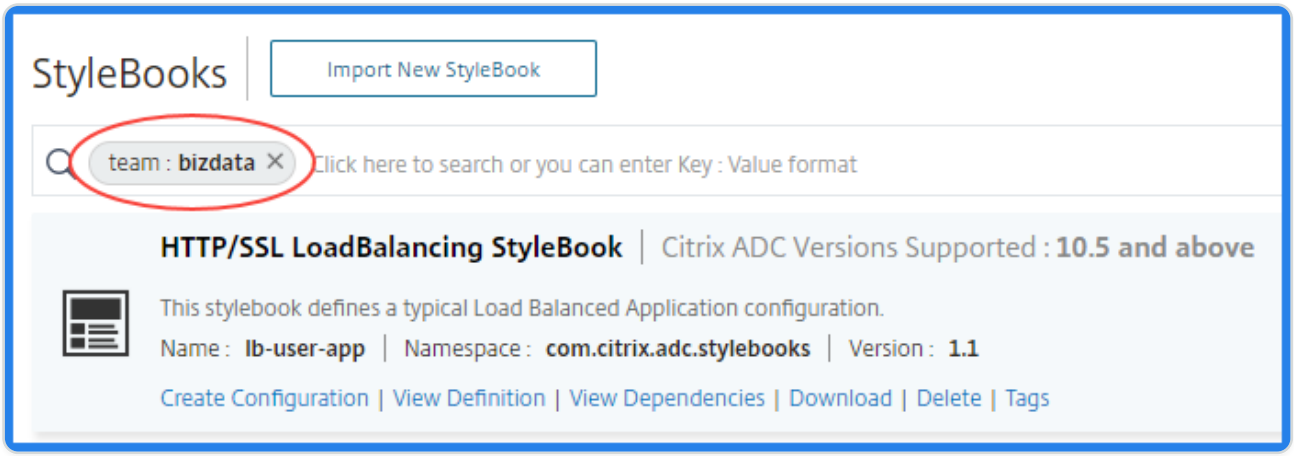
4. Click **Create**.

To filter StyleBooks using tags, in the search bar, click **Tags** and select key and value from the list. The StyleBooks that are matching the specified tag are displayed.



The following is an example search for the StyleBooks that have a tag where `key=team` and `value=bizdata`:

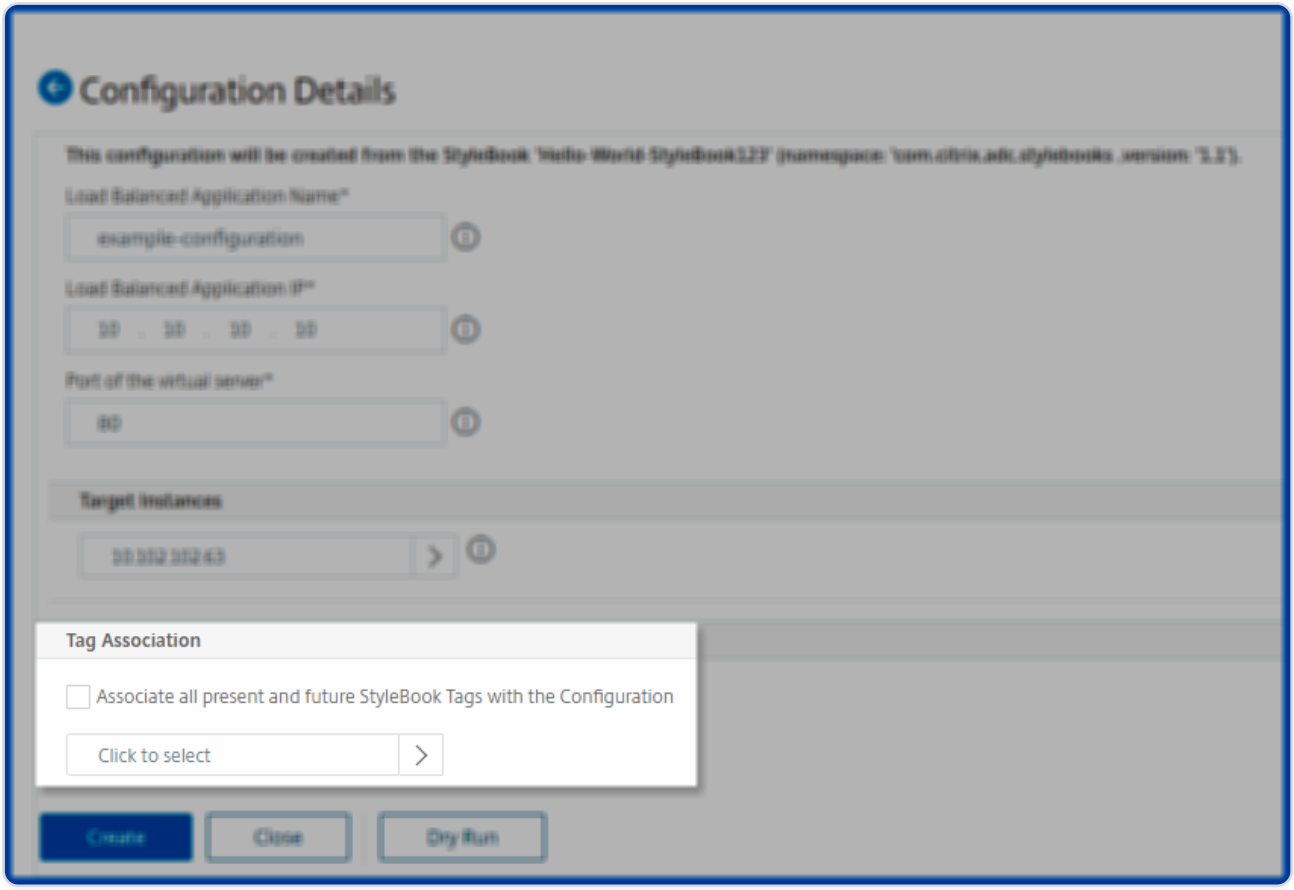
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can associate the StyleBook tags to its configuration pack. So, you can search the configuration packs using the StyleBook tags itself.

When you create a configuration pack, use one the following options in the **Tag Association** section:

- **Associate all present and future StyleBook tags with the configuration** – This option associates all the StyleBook tags to a configuration pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.
- **Select tags** – This option displays the tags of the selected StyleBook. You can select the required StyleBook tags and associate with a configuration pack.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure a StyleBook using CLI commands

If you want to configure any StyleBook using CLI commands, do the following:

- Run the `show ns runningConfig` command in NetScaler.
- In NetScaler ADM, create a configuration using either default StyleBooks, business application StyleBooks, or custom StyleBooks.
- Run the `show ns runningConfig` command in NetScaler again.

The difference between the two outputs displays the CLI commands that you can use to configure any StyleBook using the NetScaler CLI.

Import and synchronize StyleBooks from GitHub repository

Consider a scenario where you are using CI/CD processes for your development. Or, a scenario where you are managing all the application source code and deployment objects in GitHub.

In the GitHub repository, you might have created several StyleBooks for deploying the NetScaler configurations and managing these StyleBooks. These StyleBooks are also required in Citrix Applications and Delivery Management (ADM). Now, you can directly import these StyleBooks into NetScaler ADM. You don't need to manually copy them from GitHub and then upload them into NetScaler ADM or manually synchronize the files in both ADM and GitHub.

You can now define a repository in NetScaler® ADM that represents a GitHub repository. Provide the GitHub repository URL and your user name and password (or API token) created in GitHub. That means, only authorized users who have a valid account in GitHub can import and sync StyleBooks.

After creating the repository, you can sync NetScaler ADM with your GitHub repository. NetScaler ADM connects to GitHub and imports StyleBooks found in that repository. ADM then validates the StyleBooks and adds them to the list of StyleBooks in NetScaler ADM. StyleBooks are not added to NetScaler ADM if they fail validation. Correct the errors and commit updated versions into your GitHub repository. Later you can try importing them or syncing them again into NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- StyleBooks files can be imported and synchronized from any branch of a GitHub repository.
- You can import and synchronize StyleBooks that have dependent StyleBooks associated with them too.
- The synchronization of StyleBooks from a GitHub repository must be initiated manually from the NetScaler ADM GUI or API. That is, currently, importing and syncing of StyleBooks does not happen automatically based on GitHub commit activity.

Add a repository and import StyleBooks from GitHub repository

Before you begin, ensure you have a valid account in GitHub.

You can import StyleBook files to ADM from any folder in the GitHub repository.

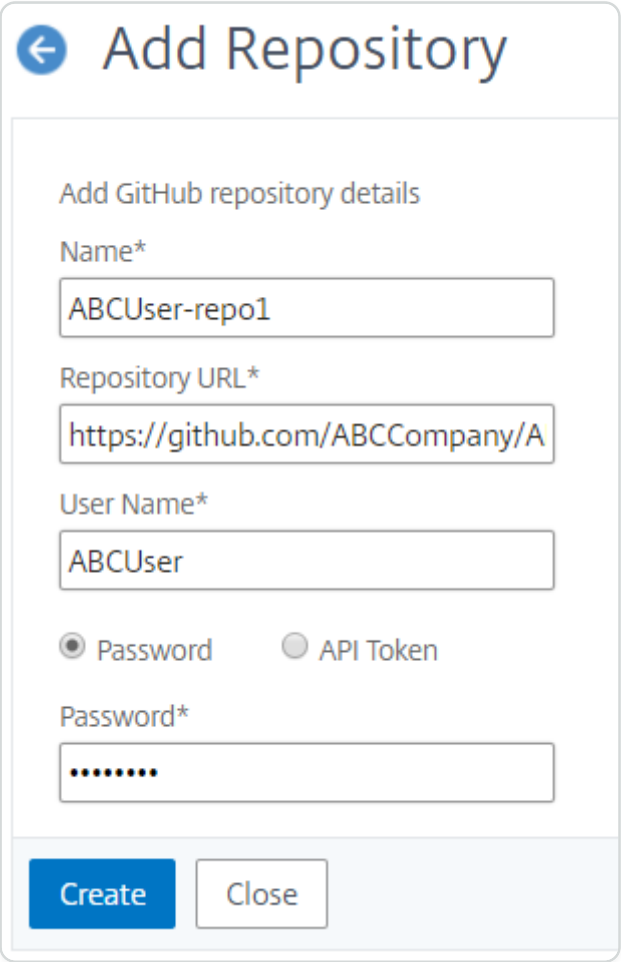
1. In NetScaler ADM, navigate to **Applications** > **StyleBooks** > **Repositories**.
2. Click **Add**. In the **Add Repository** window, enter the following parameters:
   - **Name**. Type the name of the repository. This name can be the same as the repository name in GitHub or a different one.
   - **Repository URL**. Type the GitHub repository URL.
   - **User name and password**. Type the user name and password with which you access the GitHub account.

   NOTE

   You can also provide the API token in place of a password. API tokens can be used instead of a password for GitHub over HTTPS. For information on how to create API tokens for your GitHub repository, see the GitHub documentation for creating personal access tokens.

3. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The repository is created in NetScaler ADM.

4. To import or sync StyleBooks, select the repository in the **Repositories** page, and click **Sync**.

The other actions that you can use here are:

- **Edit**. You can edit the repository URL, user name, and password (or API token).
- **Delete**. You can delete the repository along with all StyleBooks present in NetScaler ADM that were imported previously from that GitHub repository.

> **NOTE**
>
> You cannot delete a repository from NetScaler ADM if it has any StyleBooks that have ConfigPacks associated with them. First, delete all the configuration packs of these StyleBooks. You can later remove the repository from NetScaler ADM to clean up the StyleBooks from that repository.

- **Reset**. You can remove all StyleBooks in NetScaler ADM synced from that repository without actually deleting the repository entry from NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **List files**. You can see a list of all StyleBooks present in NetScaler ADM that originates from the GitHub repository.

Use default StyleBooks

A set of default StyleBooks are provided with NetScaler 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 NetScaler instances where you want to execute the configuration. After you submit the configuration, NetScaler ADM validates the parameter values you have specified, creates a graph of the configuration, connects to the NetScaler instances, and executes the configuration on the instances.

To create a configuration from a default StyleBook

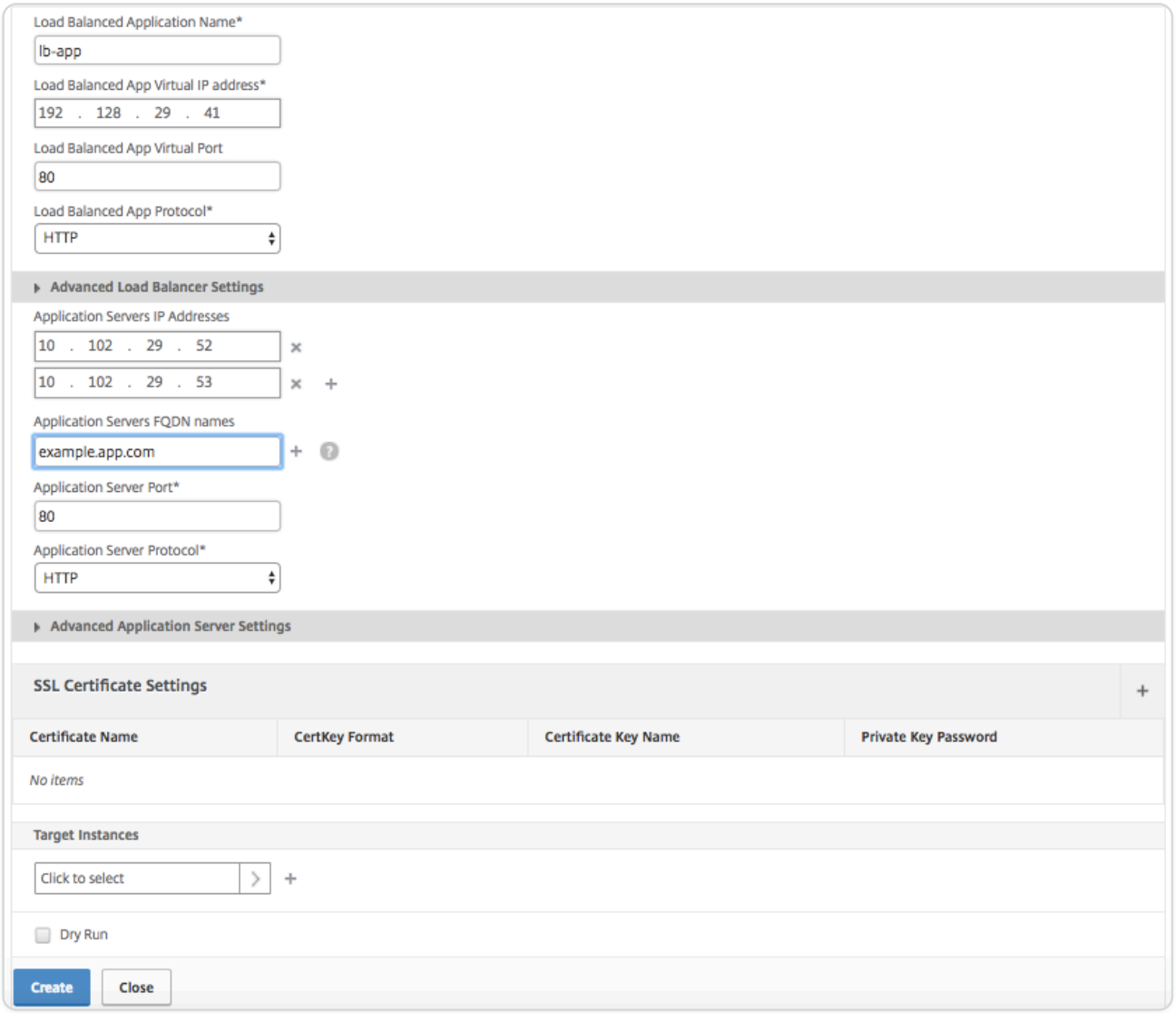
1.Navigate to **Applications** > **Configurations > StyleBooks**. The StyleBooks page displays all StyleBooks in NetScaler ADM. This list includes both default and custom StyleBooks. You can type the name of the StyleBook in the search field and press the **Enter** key. Else, you can scroll down the list to find the StyleBook.

2.Click **Create Configuration**. Specify the required values for the parameters.

Note:

> The configuration parameters and the values may differ based on the stylebook chosen.

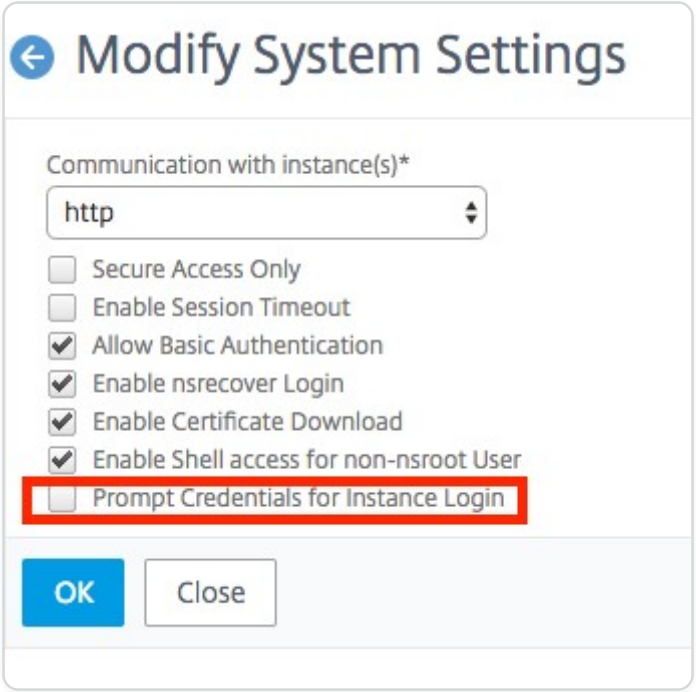
© 1997–2026 Citrix Systems, Inc. All rights reserved.



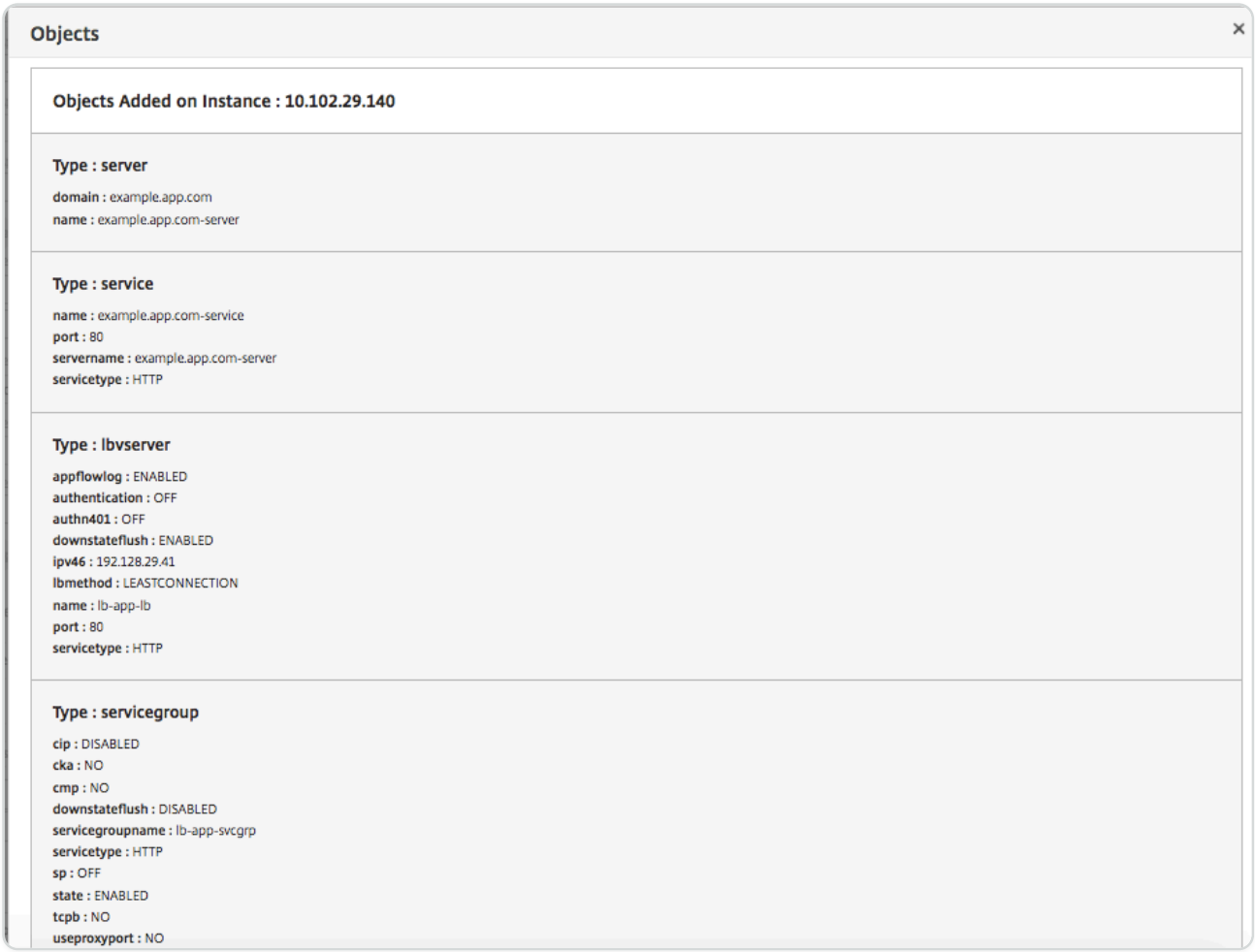
3.Under **Target Instances**, click and select the IP address of the NetScaler instance where you want to execute the configuration. If you want to execute this configuration on multiple instances, click "+" to add more instances.

If the **Prompt Credentials for Instance Login** option is enabled in **NetScaler ADM** > **Settings > Change System Settings** > **Modify System Settings**, you are prompted for your NetScaler instance credentials when you execute the configurations on the selected NetScaler instances. Else, NetScaler ADM uses the instance credentials stored in the instance profile for logging into the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you want to test or validate your configuration before executing it on the NetScaler 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4.Clear the **Dry Run** check box and click **Create** to create the configuration and execute the configuration on the NetScaler 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 NetScaler instances in NetScaler ADM to the available list of instances in this window.

You can now examine, update, or remove this configuration pack by using NetScaler® ADM.

Web application firewall StyleBook

NetScaler Web App Firewall is a web application firewall (WAF) that protects web applications and sites from both known and unknown attacks, including all application-layer and zero-day threats.

NetScaler ADM now provides a default StyleBook with which you can more conveniently create an application firewall configuration on NetScaler instances.

Deploying application firewall configurations

The following task assists you in deploying a load balancing configuration along with the application firewall and IP reputation policy on NetScaler instances in your business network.

To create an LB configuration with application firewall settings:

1. In NetScaler ADM, navigate to **Applications** > **Configurations** > **StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler ADM. Scroll down and find HTTP/SSL Load Balancing StyleBook with application firewall policy and IP reputation policy. You can also search for the StyleBook by typing the name as `lb-appfw`. Click **Create Configuration**.

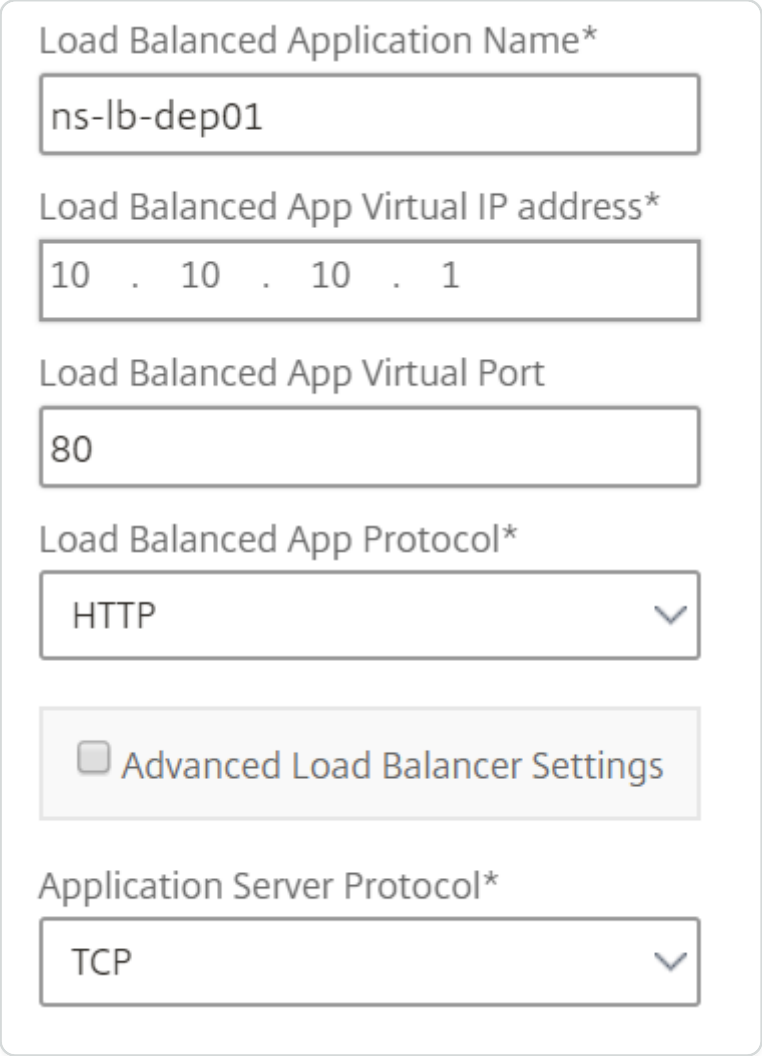
   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

2. Enter values for the following parameters:

   - **Load Balanced Application Name**. Name of the load balanced configuration with application firewall to deploy in your network.
   - **Load balanced App Virtual IP address**. Virtual IP address at which the NetScaler instance receives client requests.

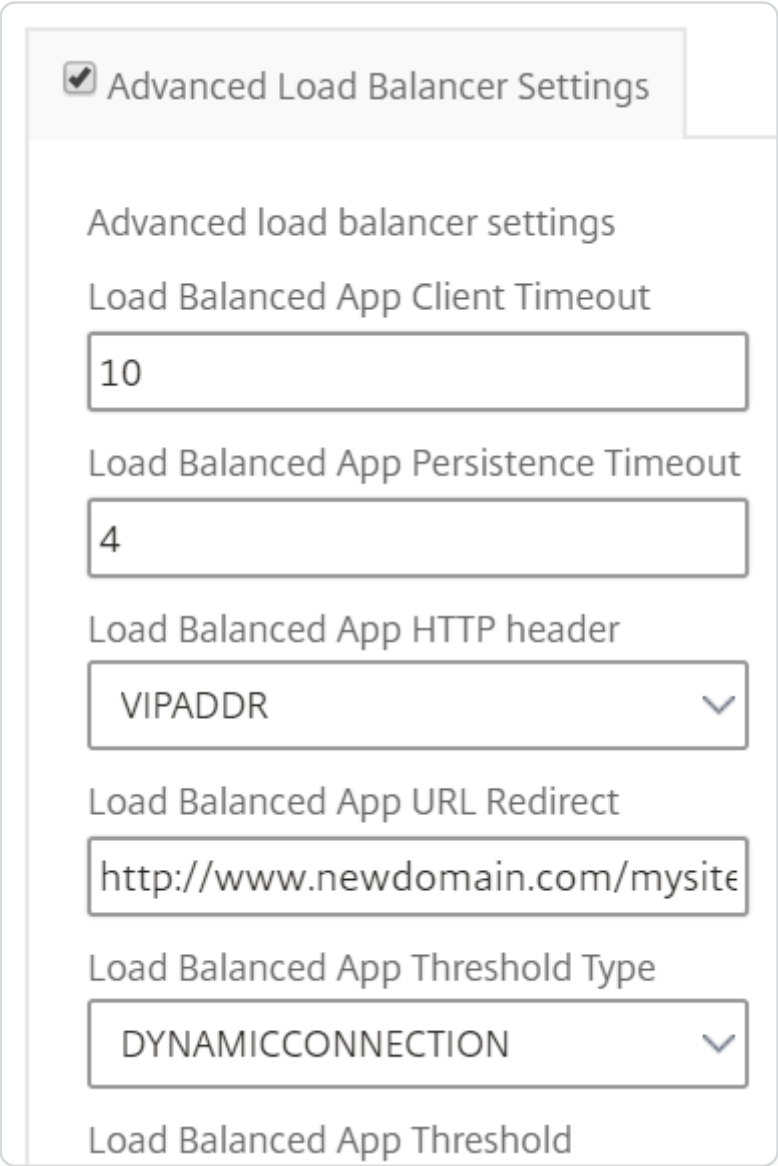
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Load Balanced App Virtual Port**. The TCP Port to be used by the users in accessing the load balanced application.
- **Load Balanced App Protocol**. Select the front-end protocol from the list.
- **Application Server Protocol**. Select the protocol of the application server.



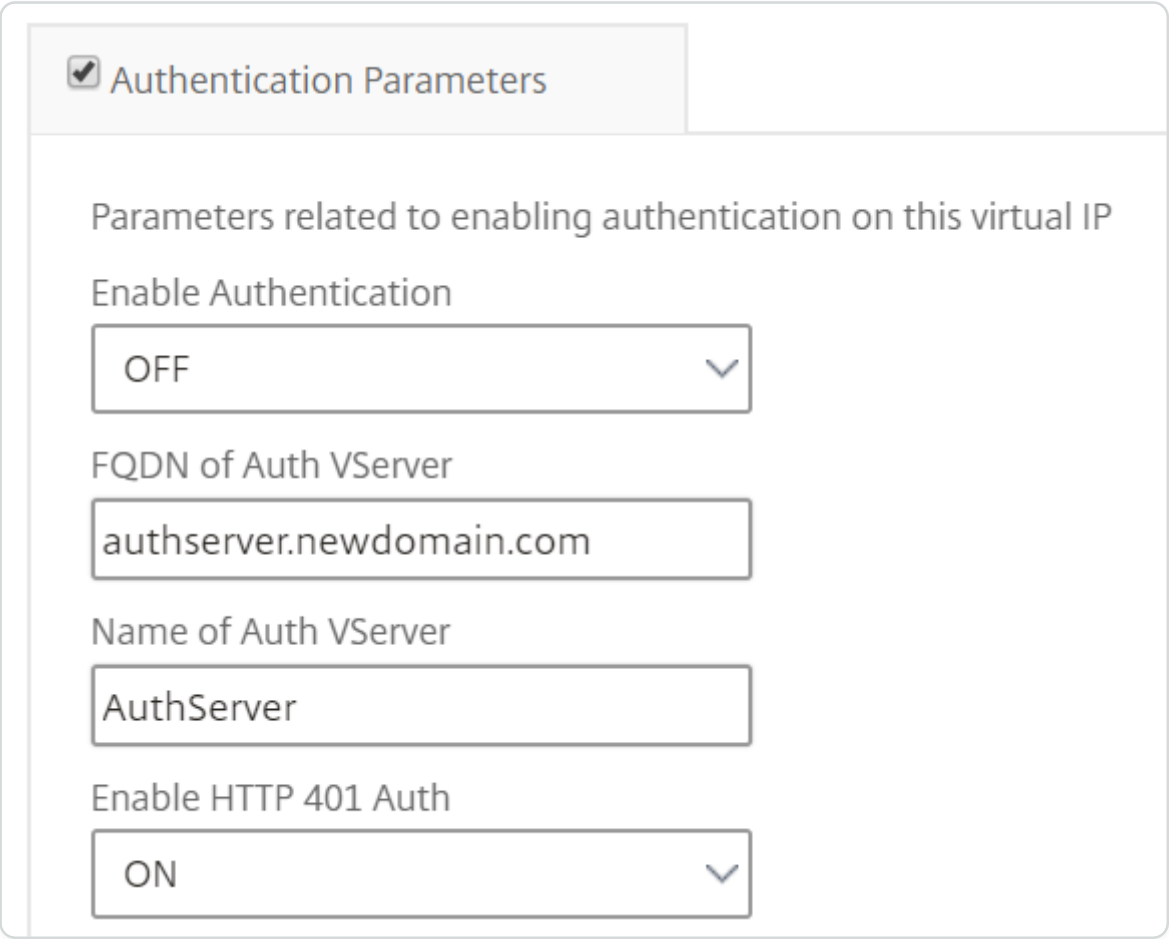
3. As an option, you can enable and configure the **Advanced Load Balancer Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

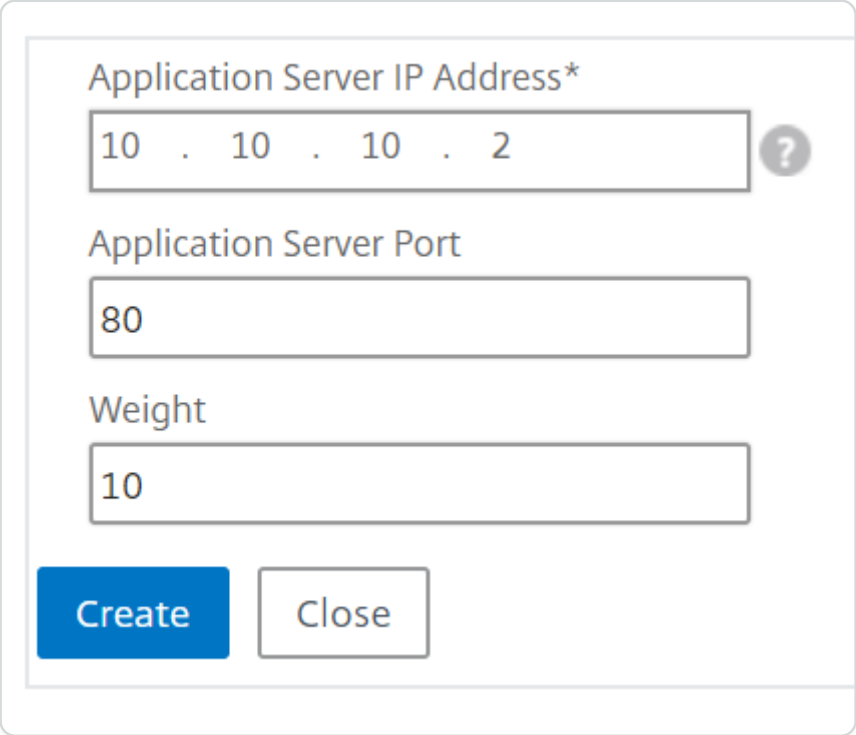


4. Optionally, you can also set up an authentication server for authenticating traffic for the load balancing virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

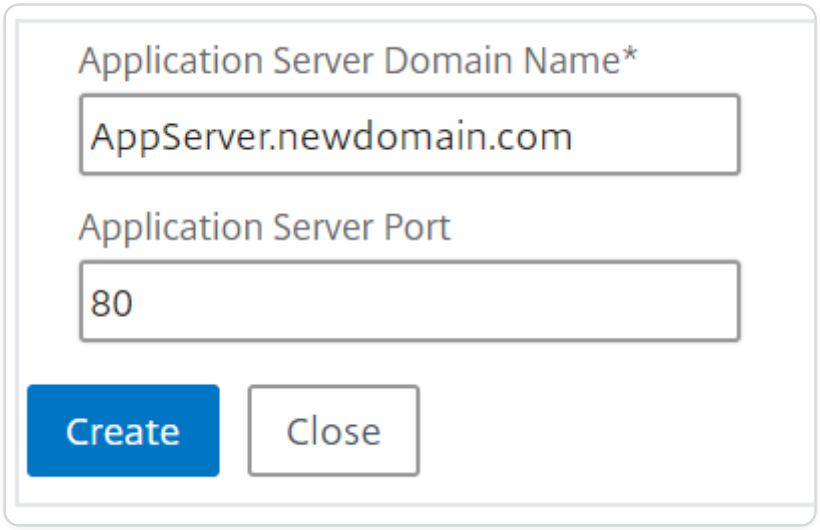


5. Click "+" in the server IPs and Ports section to create application servers and the ports that they can be accessed on.



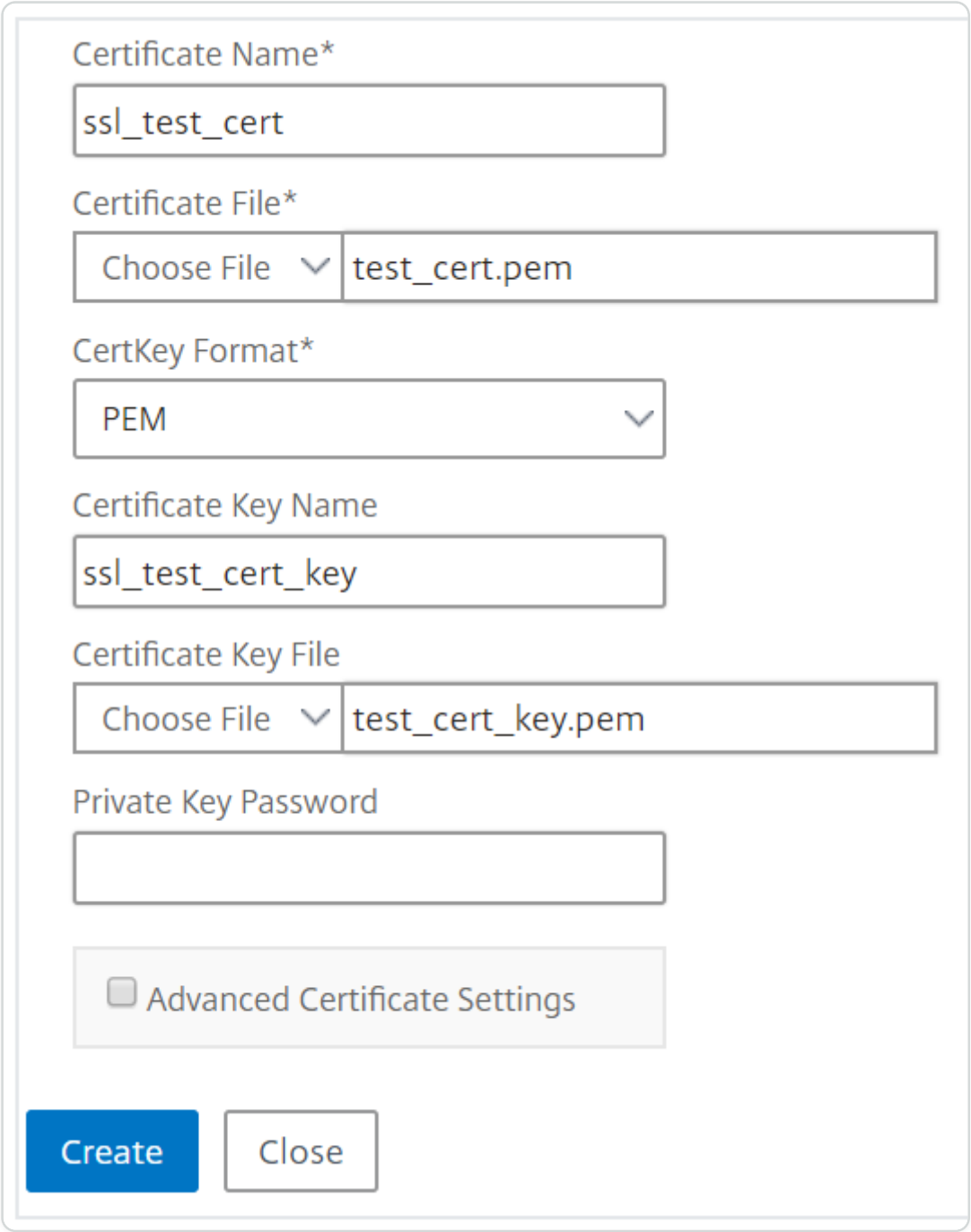
6. You can also create FQDN names for application servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



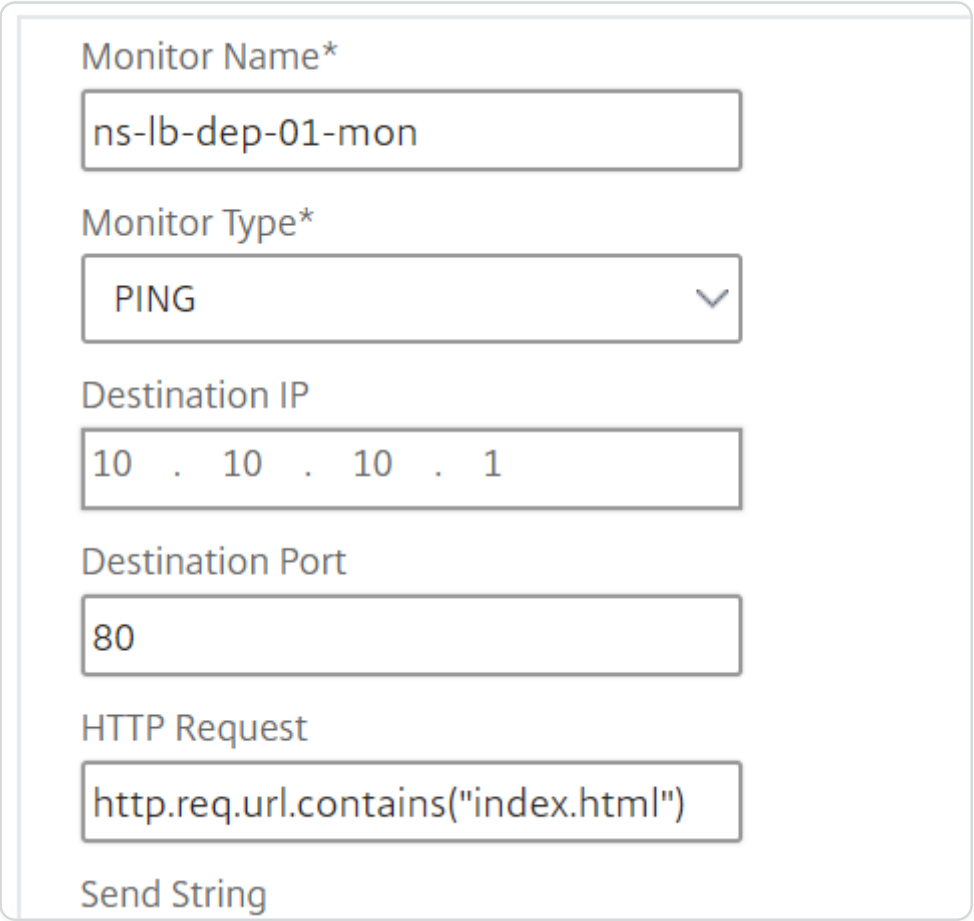
7. You can also specify the details of the SSL certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



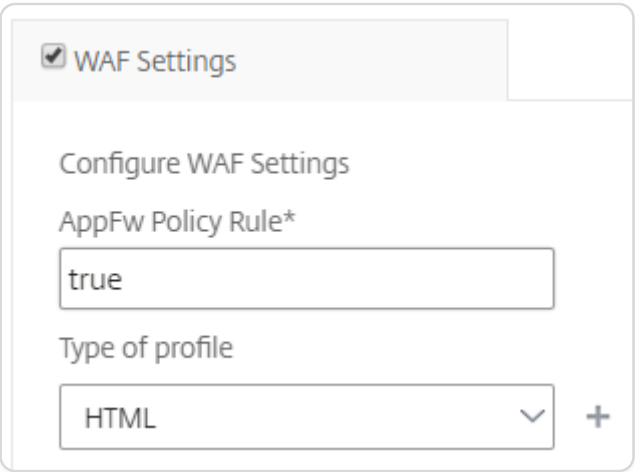
8. You can also create monitors in the target NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. To configure an application firewall on the virtual server, enable WAF Settings.

   Ensure that the application firewall policy rule is true if you want to apply the application firewall settings to all traffic on that VIP. Otherwise, specify the NetScaler policy rule to select a subset of requests to which to apply the application firewall settings. Next, select the type of profile that has to be applied - HTML or XML.



10. Optionally you can configure detailed application firewall profile settings by enabling the application firewall Profile Settings check box.

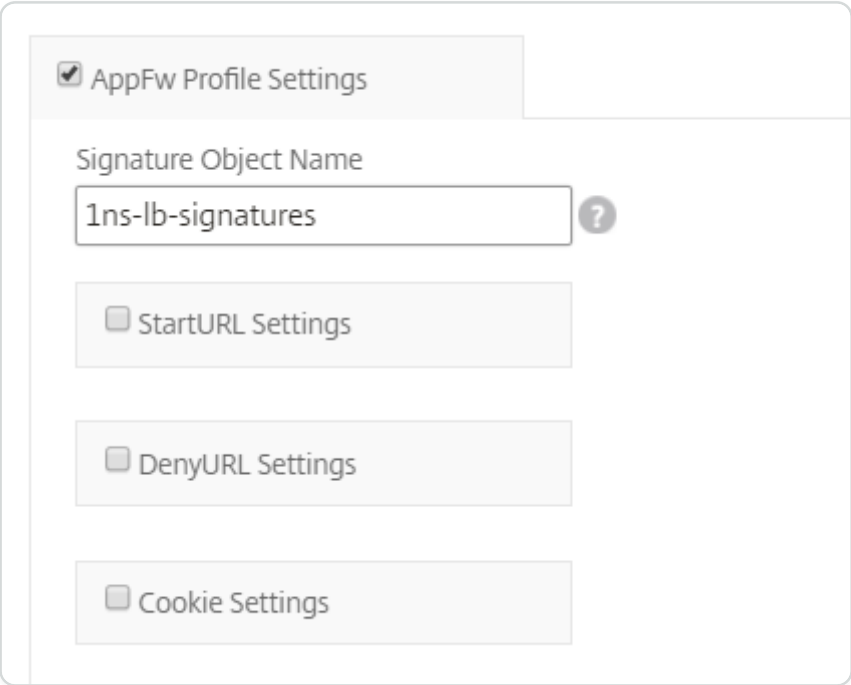
© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Optionally, if you want to configure application firewall signatures, enter the name of the signature object that is created on the NetScaler instance where the virtual server is to be deployed.

    NOTE

    You cannot create a signature object by using this StyleBook.

12. Next, you can also configure any other application firewall profile settings such as, StartURL settings, DenyURL settings and others.

    For more information on application firewall and configuration settings, see Application Firewall.

13. In the **Target Instances** section, select the NetScaler instance on which to deploy the load balancing virtual server with the application firewall.

    NOTE

    You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

14. You can also enable **IP Reputation check** to identify the IP address that is sending unwanted requests. You can use the IP reputation list to preemptively reject requests that are coming from the IP with the bad reputation.

15. Click **Create** to create the configuration on the selected NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

Citrix recommends that you select Dry Run to check the configuration objects that must be created on the target instance before you run the actual configuration on the instance.

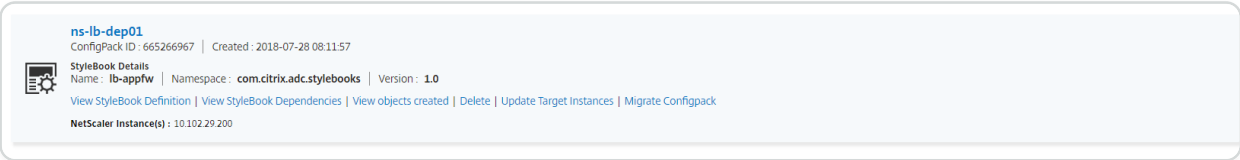
When the configuration is successfully created, the StyleBook creates the required load balancing virtual server, application server, services, service groups, application firewall labels, application firewall policies, and binds them to the load balancing virtual server.

The following figure shows the objects created in each server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

16. To see the ConfigPack created on NetScaler® ADM, navigate to **Applications** > **Configurations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create WAF and BOT profiles using StyleBook

When you can select a policy to an API resource in **API Gateway**, it allows you to define the traffic selection criteria to authenticate an API request. Also, it allows you to configure API security policies to the API traffic.

You can configure WAF and BOT policies to an API resource. Before you configure a policy, ensure to create its profile in NetScaler® Application Delivery Management (ADM). Use the following default StyleBooks to create a profile:

- API WAF Detection StyleBook
- API BOT Detection StyleBook

Create a WAF profile using the StyleBook

Perform the following to create a WAF profile:

1. In NetScaler ADM, navigate to **Applications** > **Configurations** > **StyleBooks**. Search for the StyleBook by typing the name as `api-waf-profile`. Click **Create Configuration**.

   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. Specify values for the following parameters:

   - **API WAF profile name** - A name to identify a WAF profile.
   - **Application Type** - Add application types to the profile. The WAF profile supports JSON and XML application types.
3. Optional, enable **Security Settings** to specify HTTP, JSON, or XML protection checks. You can also specify an Error URL to the NetScaler Web App Firewall. For more information, see Creating Web App Firewall profile.
4. Select the target NetScaler instance or instance group on which you want to deploy this configuration.
5. Click **Create**.

To configure a WAF policy, see Add policies to an API deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a BOT profile using the StyleBook

Perform the following to create a BOT profile:

1. In NetScaler ADM, navigate to **Applications** > **Configurations** > **StyleBooks**. Search for the StyleBook by typing the name as `api-bot-profile`. Click **Create Configuration**.

   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 **BOT Profile Name**, specify a name to identify a BOT profile.
3. Optional, enable the following options based on your requirements:

   - **Enable IP reputation check** - This option identifies the IP address that is sending unwanted requests. You can use the IP reputation list to preemptively reject requests that are coming from the IP with the bad reputation.
   - **Enable BOT Signatures** - Specify the BOT signature name. It blocks the requests from the specified signature.
   - **Allow List** - Specify IPv4 or subnet (CIDR) address. This option enables the BOT profile to bypass requests from the specified IPv4 or subnet address.
   - **Deny List** - Specify IPv4 or subnet (CIDR) address. This option enables the BOT profile to block requests from the specified IPv4 or subnet address.

4. Select the target NetScaler instance or instance group on which you want to deploy this configuration.
5. Click **Create**.

To configure a BOT policy, see Add policies to an API deployment.

Hide all default StyleBooks

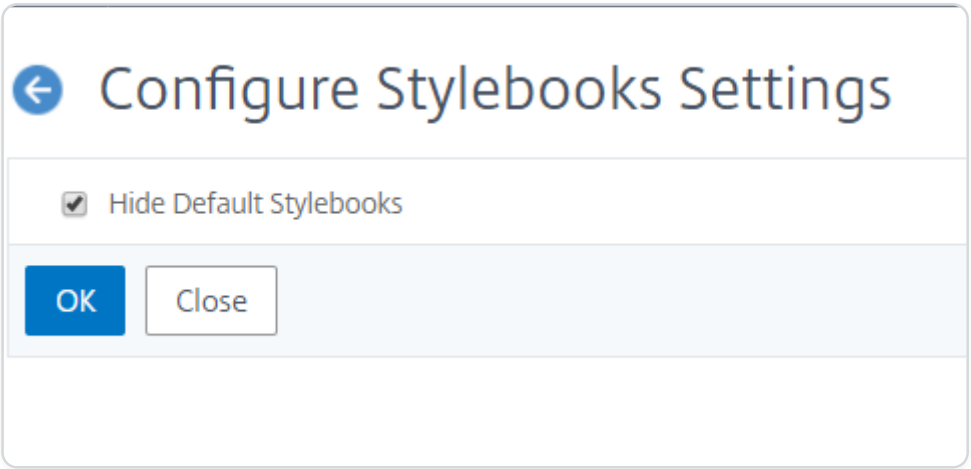
NetScaler® ADM lists all StyleBooks present in NetScaler ADM folder system. The list of StyleBooks includes default and custom StyleBooks that can be both private and public. As an administrator, you might want to hide all default StyleBooks. You can allow your users to view and access only custom StyleBooks built by you or by the users.

NetScaler ADM allows you to display your custom StyleBooks and hide all default StyleBooks that are shipped with NetScaler ADM. A new GUI option is provided where you can hide all default StyleBooks.

To hide all default StyleBooks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler 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.
4. On the **Configure StyleBook Settings** page, select **Hide Default StyleBooks** option.
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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate NetScaler application configuration using StyleBooks Configuration Builder

NOTE

This feature is in tech preview.

The StyleBooks Configuration Builder is used to create an application configuration StyleBook from an existing NetScaler configuration. This feature also automates the application configuration migration from one NetScaler instance to another instance.

Using Configuration Builder you can simplify the requirement to create a customized StyleBook. This feature enables you to create a StyleBook without in-depth knowledge of StyleBooks grammar and constructs. Otherwise, the knowledge of StyleBooks grammar and constructs is necessary to create a StyleBook.

The Configuration Builder also creates a ConfigPack that reflects the same ADC configuration on a new ADC instance. With this ConfigPack, the initial ADC configuration from one ADC instance can be duplicated to another ADC instance. The initial configuration source can be one of the following:

- **A NetScaler instance:** Specify the instance where the application configuration that you want to duplicate is hosted.

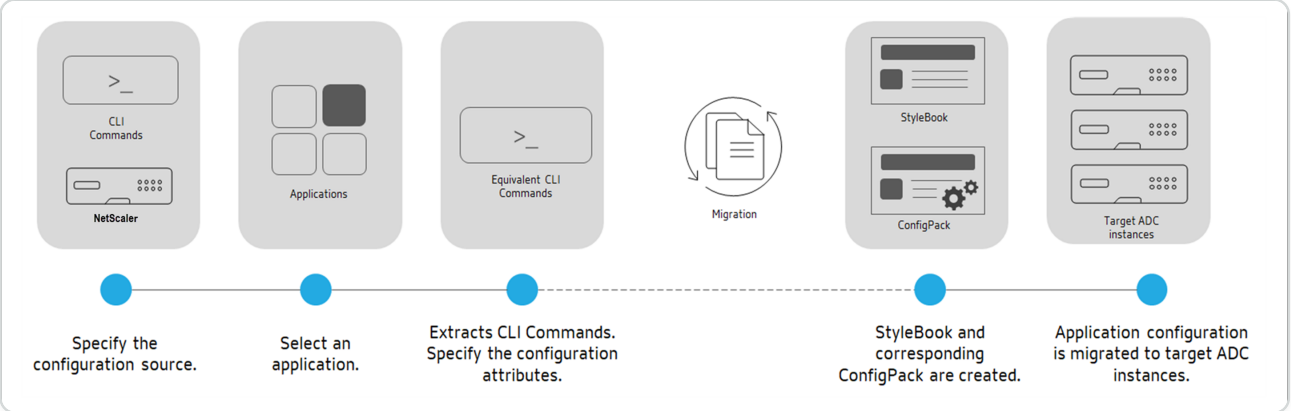
  The Configuration Builder converts the ADC configuration to a StyleBook and ConfigPack even if you do not specify the target instance. You can later use this configpack to migrate the ADC configuration to other ADC instances.
- **A set of CLI Commands:** Paste the configuration from `ns.conf` or `Application config`.

The Configuration Builder identifies the list of distinct applications embedded in the source configuration. When you select the application configuration of your interest, the Configuration Builder extracts the set of CLI commands for the selected application. These CLI commands are extracted from the source configuration. Also it identifies the deployment and configuration attributes that might require your input.

- **Deployment attributes** - You can view and edit the IP address and port of the virtual servers, services, service group members from the original configuration.
- **Configuration attributes** - These attributes can be passwords or certificates specified in the source configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After specifying the necessary information, start migrating or duplicating the application configuration on a target ADC instance.



After you complete application creation and migration, a ConfigPack is created in NetScaler® ADM along with its corresponding StyleBook. This ConfigPack represents the application configuration on the target ADC instance. To view the created ConfigPack, navigate to **Applications** > **StyleBooks** > **Configurations**.

Supported NetScaler Features

The StyleBook Configuration Builder recognizes and supports the following NetScaler features in the source configuration:

- Content Switching
- Load Balancing
- Monitoring
- SSL Offloading
- Rate limiting
- Rewrite
- Responder
- Web application firewall (WAF)

Create a StyleBook to migrate the NetScaler application configuration

The following procedure is to create a StyleBook that migrates the NetScaler application migration in NetScaler ADM:

1. Navigate to **Applications** > **StyleBooks** > **Configurations**.

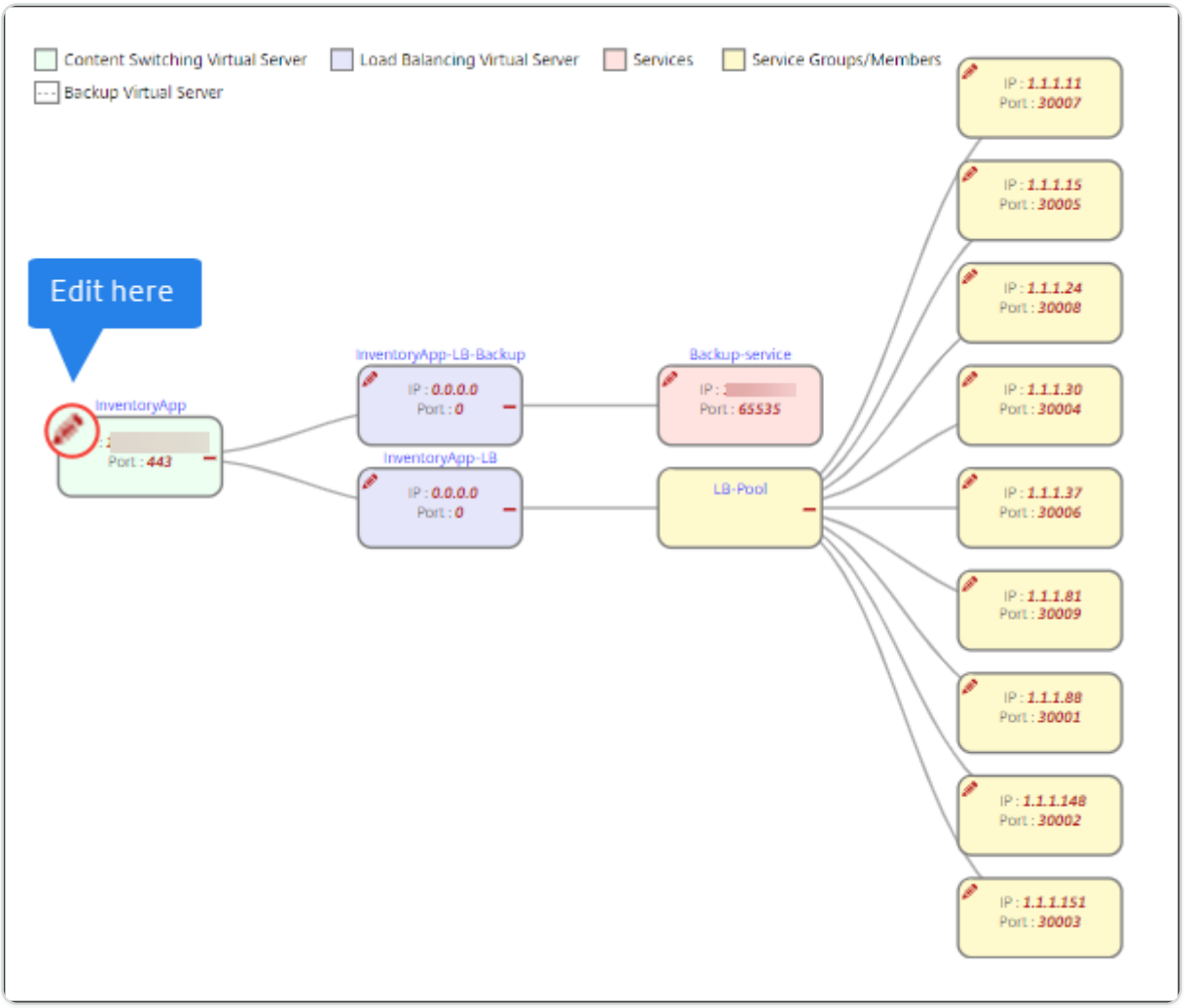
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Migrate ADC Configuration**.
3. Click **Get Started**.
4. In **Specify Configuration**, select the configuration source:
   - **Import from an ADC**: This option discovers the active applications on the selected ADC instance.
   - **Import using CLI Commands**: This option analyses the CLI commands and extracts the applications from the CLI commands.
5. Specify the **Source ADC Instance** from which you want to migrate or duplicate the application configuration.
6. Specify the **Target ADC Instance** to which you want to migrate or duplicate the application configuration.
7. In **Define Application**,
   a. In **Application Name**, specify the name of the application.
   b. Select the virtual servers that you want to migrate.
   c. Click **Next**.
8. In **Equivalent CLI Commands**, review the commands and click **Next**.

   These commands are specific to the selected application configuration.
9. In **Deployment Attributes**, you can view and edit the IP address and port of the virtual servers, services, and service group members.

   To edit the IP address and port, click the edit icon on the virtual server, service, or service group member in the flow diagram.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This tab appears only in the following cases:

- The source and target instances are different.
- Import configurations using CLI commands.

10. In **Configuration Attributes**, specify the necessary details and click **Next**.

    This tab lists the secrets such as keys to decrypt passwords and certificates.

> **NOTE**
>
> Before you start the migration, the missed or unsupported configurations are displayed in any of the following tabs:

Unsupported Configurations

Unsupported Global Configurations

To migrate these configurations successfully, you must apply the missed or unsupported configurations separately on the target instance. And, click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. In **Migrate**, specify the required StyleBook details. Click **Migrate**.

Limitations

- The named expressions and `responderhtmlpages` mentioned in the source instance are not identified. Make sure to configure the named expressions and `responderhtmlpages` on the target instance before migration.
- If the source has a configuration for `servicegroup` and monitor binding as follows:

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  The following error appears:

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  This error occurs because NetScaler saves the binding between Service Group and Monitor in an invalid format. This issue is fixed from NetScaler 12.1.52.15 build.

Business application StyleBooks

NetScaler® ADM provides the StyleBooks that helps you deploy an ADC configuration for specific business applications. For more information on such StyleBooks, see the following topics:

- SSO Google Apps StyleBook
- SSO Office 365 StyleBook
- Microsoft Skype for Business StyleBook
- Microsoft Exchange StyleBook
- Microsoft SharePoint StyleBook
- Microsoft ADFS proxy StyleBook
- Oracle e-business StyleBook
- Web application firewall StyleBook
- Create WAF and BOT profiles using StyleBook

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSO Google Apps StyleBook

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 NetScaler ADM SSO Google Apps StyleBook allows you to enable SSO for Google Apps through NetScaler instances. The StyleBook configures the NetScaler instance as a SAML identity provider for authenticating users to access Google Apps.

Enabling SSO for Google apps in a NetScaler 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 will also supports the higher versions of the same.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	Release 11.0, Advanced/Premium License

The following instructions assume that you have already created the appropriate external or internal DNS entries to route authentication requests to a NetScaler-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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To deploy SSO Google apps StyleBook

1. In NetScaler® ADM, navigate to **Applications** > **Configurations** > **StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler 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 authentication, authorization, and auditing virtual server to which the Google apps SAML IdP policy is bound.
   c. **SAML Rule Expression**. By default, the following NetScaler Policy (PI) expression is used: HTTP.REQ.HEADER("Referrer").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 Referrer header is coming from a Google domain.
4. The SAML IdP Settings section allows you to configure your NetScaler Instance as a SAML identity provider by creating the SAML IdP profile and policy that is used by the authentication, authorization, and auditing virtual server created in step 3.
   a. **SAML Issuer Name**. In this field, enter the public FQDN of your authentication virtual server. Example: `https://<NetScaler Auth VIP>/saml/login`
   b. **SAML Service Provider (SP) ID**. (optional) NetScaler identity provider accepts SAML authentication requests from an issuer name that matches this ID.
   c. **Assertion Consumer Service URL**. Enter the service provider's URL where NetScaler identity 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").

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 be compatible 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. NetScaler 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 NetScaler 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 NetScaler instance by using their corporate email 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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. LDAP server port that NetScaler connects to for authenticating users (default is 389).

iv. LDAP host name. 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 NetScaler 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 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 NetScaler 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 NetScaler. 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 NetScaler instance(s) on which to deploy this Google Apps SSO configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instance(s).

   NOTE

   You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also,

TIP

Citrix recommends that before running the actual configuration, you select **Dry Run** to visually confirm the configuration objects that are created on the target NetScaler instance(s) by the StyleBook.

SSO Office 365 StyleBook

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 NetScaler instances. You can now configure SAML authentication with NetScaler as the SAML Identity Provider (IdP) and Microsoft Office 365 as the SAML service provider.

Enabling SSO for Microsoft Office 365 in a NetScaler 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.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	11.0, Advanced/Premium License

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler-monitored IP address.

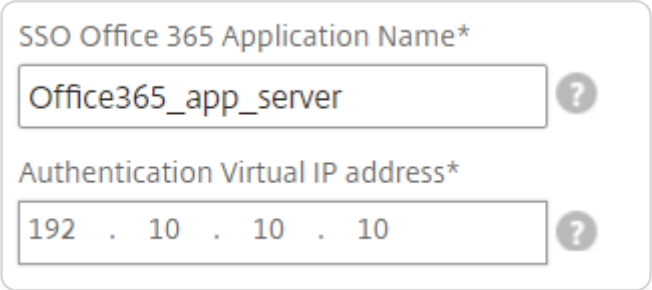
The following instructions assist you in implementing the SSO Office 365 StyleBook in your business network.

To deploy SSO Microsoft Office 365 StyleBook

1. In NetScaler® Application Delivery Management (ADM), navigate to **Applications** > **StyleBooks**. The **StyleBooks** page displays all the StyleBooks available for your use in NetScaler 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.



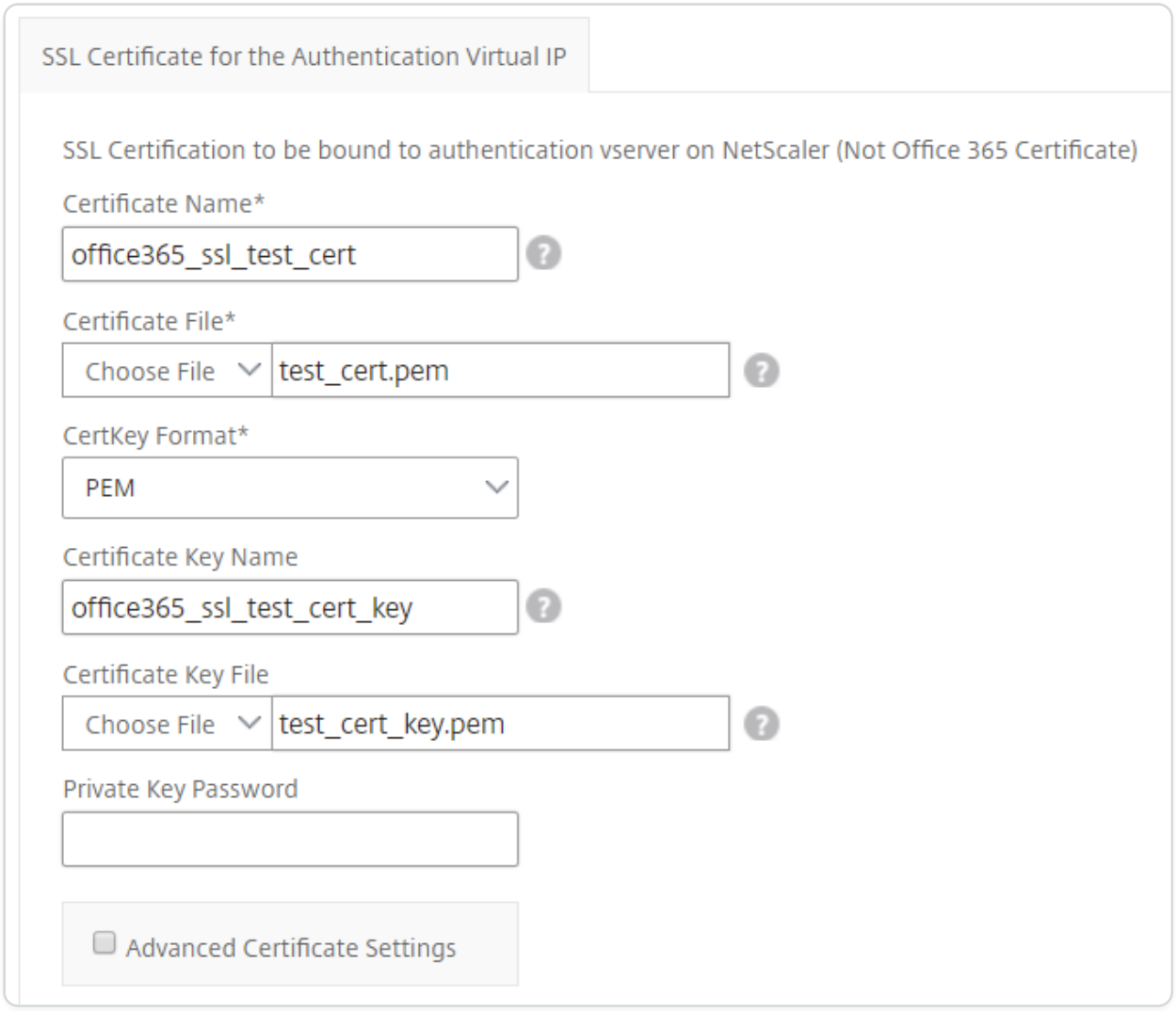
4. In **SSL Certificates Settings** section, enter the names of the SSL certificate and the certificate key.

   NOTE

   This is not the Office 365 service provider certificate. This SSL certificate is bound to the virtual authentication server on the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler. 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 NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

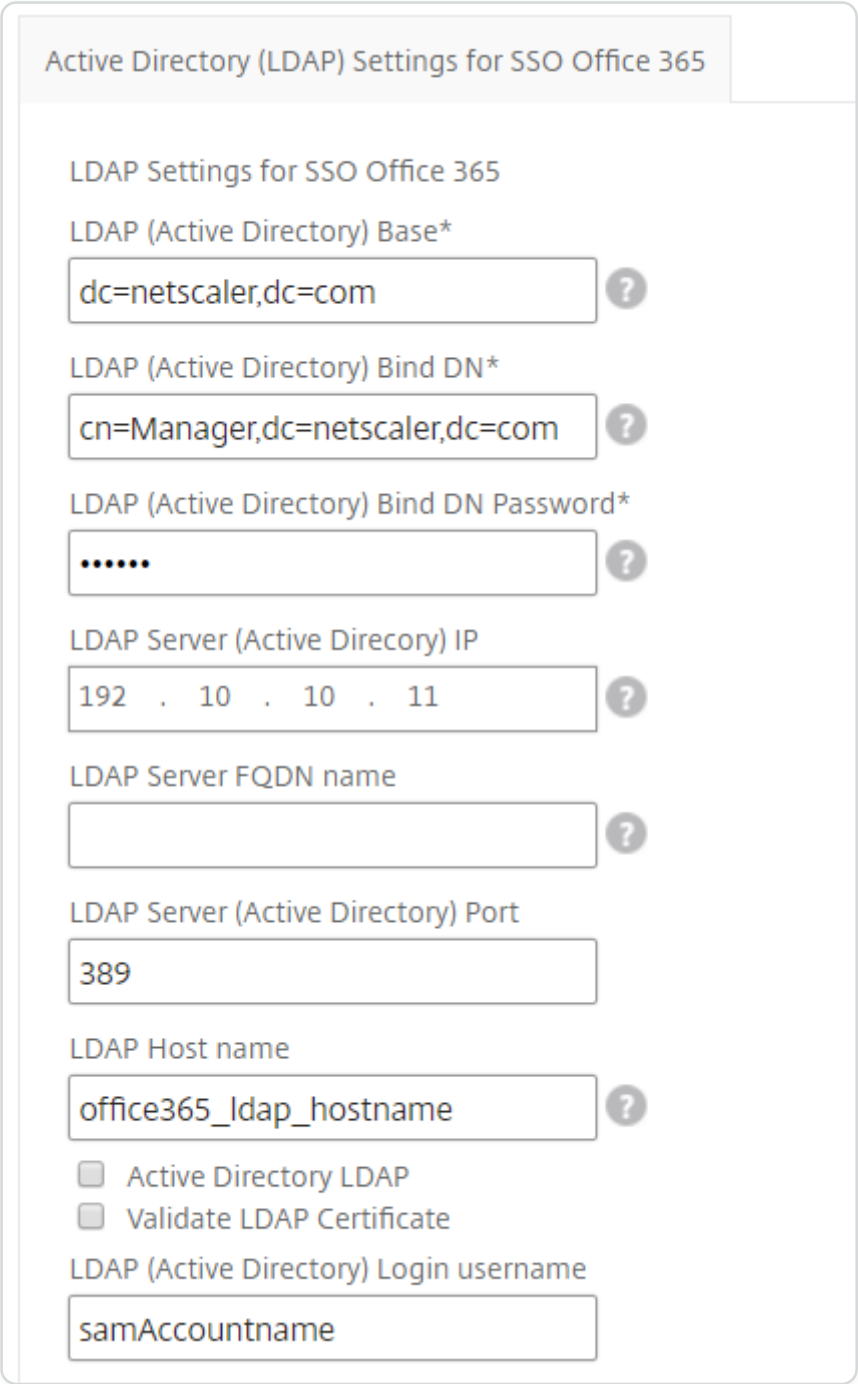
- **LDAP (Active Directory) Bind DN Password**. Enter the password of the domain account for authentication.
- A few other fields that you need to enter in this section are as follows:
  - LDAP server IP Address that NetScaler connects to for authenticating users.
  - LDAP server's FQDN name.

    NOTE

    You must specify at least one of the above two - the LDAP server IP address or the FQDN name.

  - LDAP server port that NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



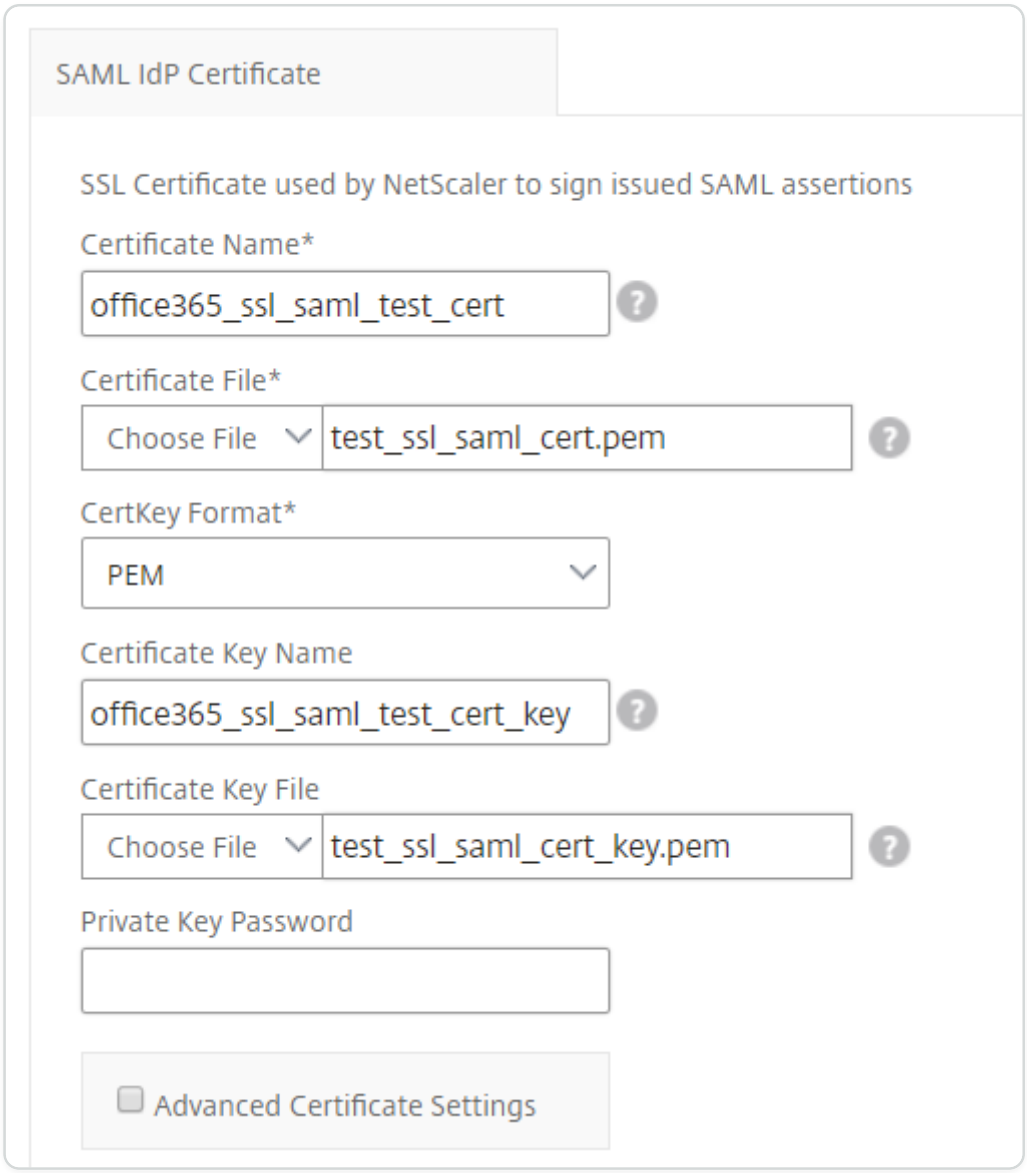
9. In **SAML IdP Certificate** section, you can specify the details of the SSL certificates used for SAML assertion.

   - **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

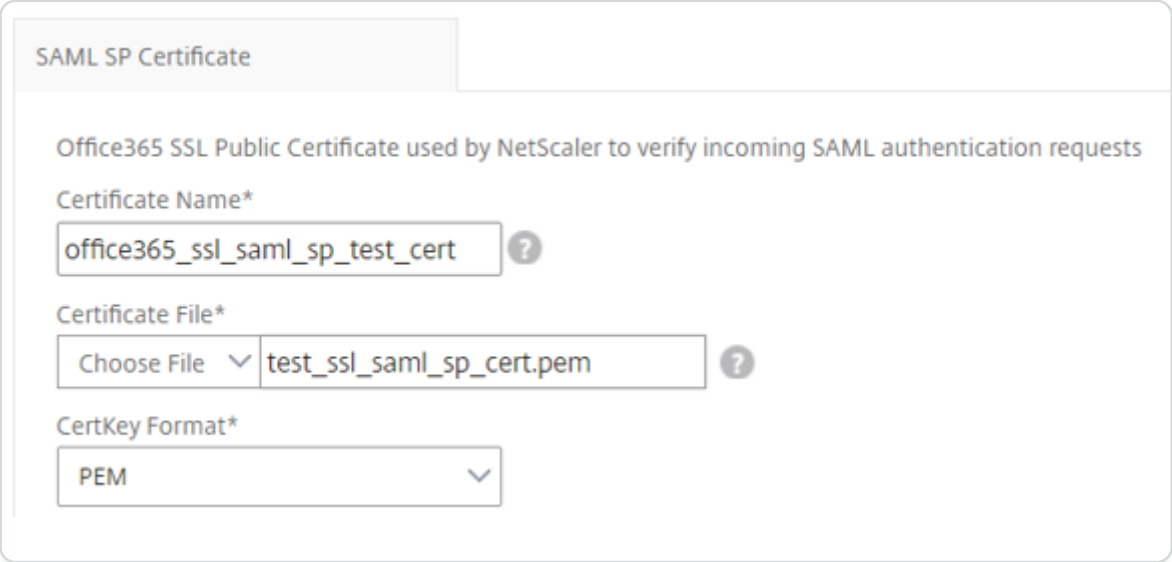


10. Optionally, you can select **SAML IdP CA Certificate** if the SAML IdP certificate entered above requires a CA public certificate to be installed on NetScaler. Make sure you select **Is a CA Certificate** in the above **Advanced Certificate Settings** section.
11. In the **SAML SP Certificate** section, enter the following details for the Office 365 SSL public certificate. This certificate is used by the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 NetScaler 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://<NetScaler Auth VIP>/saml/login`
    - **Name Identifier Expression**. Type in the NetScaler 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) NetScaler 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 NetScaler identity provider needs to send the SAML assertions after successful user authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The assertion consumer service URL can be initiated at the identity provider server site or the service provider site.

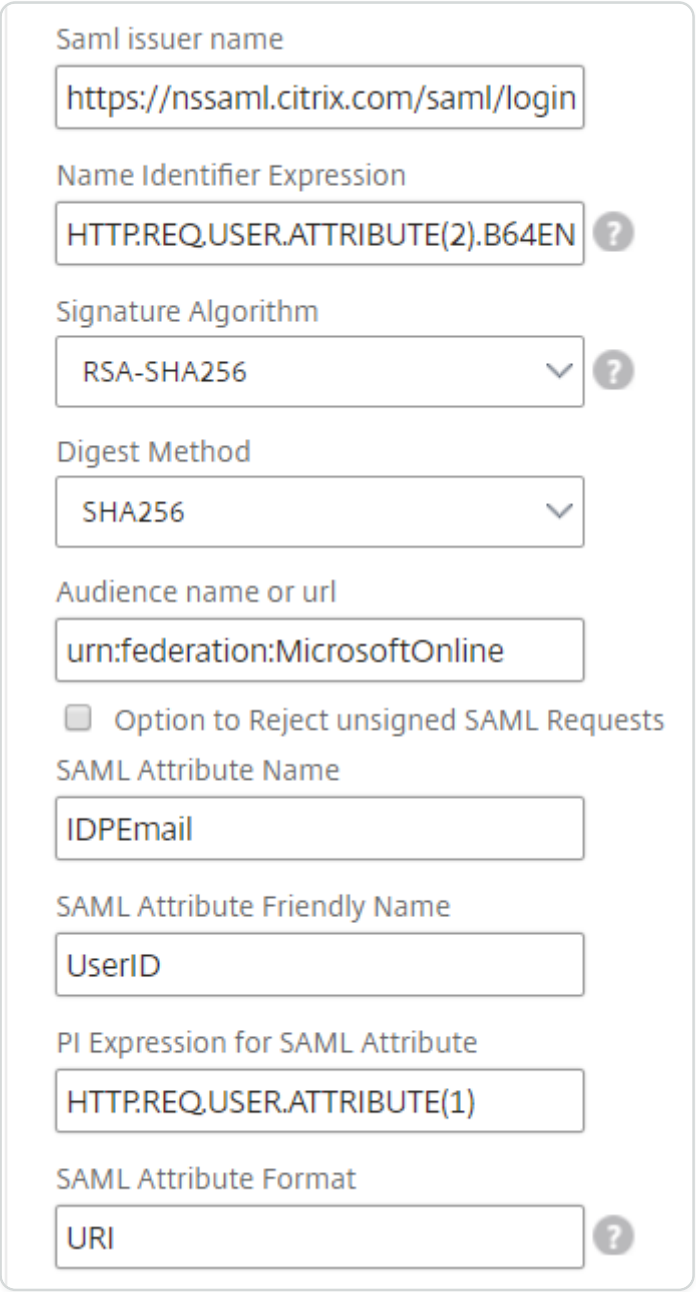
- There are other optional fields that you can enter in this section. For example, you can set the following options:
  - **SAML attribute name**. Name of user attribute sent in SAML Assertion.
  - **SAML attribute friendly name**. Friendly Name of the user attribute sent in SAML Assertion.
  - **PI expression for SAML attribute**. By default, the following NetScaler 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.

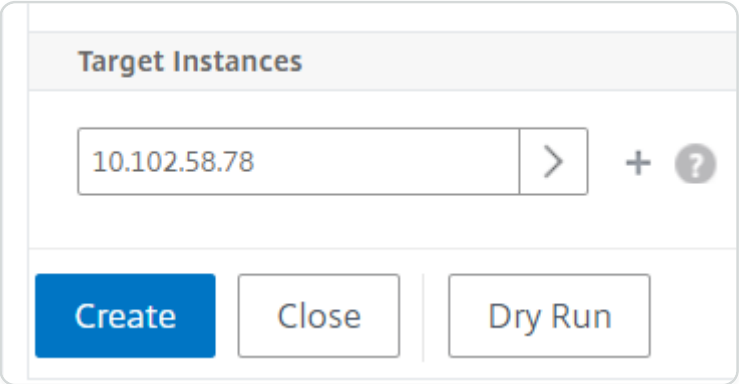
TIP

Citrix recommends that you retain the default settings as these settings have been tested to work with Microsoft Office 365 apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



13. Click **Target Instances** and select the NetScaler 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 NetScaler instance(s).



© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

Citrix recommends that before executing the actual configuration, you select **Dry Run** to view the configuration objects that are created on the target NetScaler instances by the StyleBook.

Microsoft Skype for Business StyleBook

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

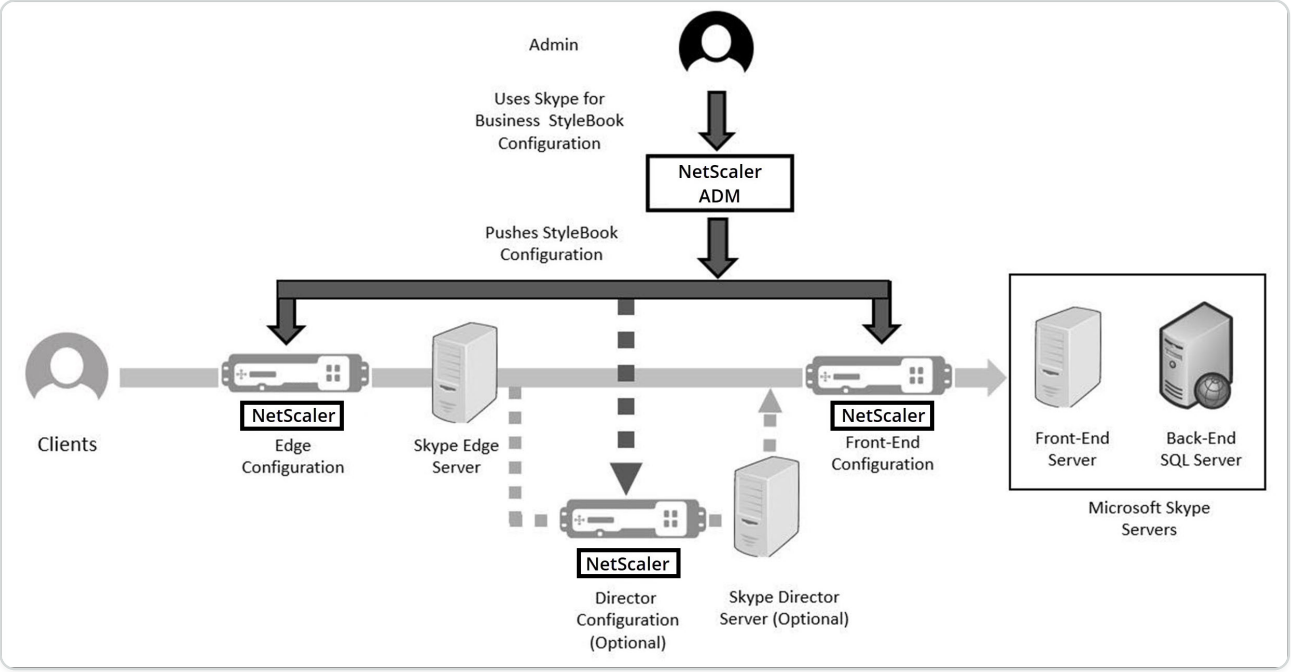
Director servers

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configuring NetScaler instances in an enterprise

The following table lists the IP addresses used in the sample configuration included in the instructions below:

SKYPE FOR BUSINESS SERVERS	VIRTUAL IP ADDRESS	SERVER IP ADDRESSES	NETSCALER INSTANCE
Edge Servers	External VIP - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	Internal VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	
Front-end Servers	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director Server	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

To configure front-end servers

1. In NetScaler® 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 NetScaler ADM. Scroll down and select **Microsoft Skype**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler instances for the three Skype servers.

The following table provides you a list of all default ports and protocols:

LABEL	PORT	PROTOCOL	DESCRIPTION
HTTP Port	80	HTTP	Used for communication from Front-End Servers to the web farm FQDNs when HTTPS is not used.
HTTPS Port	443	HTTPS	Used for communication from Front-End Servers to the web farm FQDNs.
AutoDiscover Internal Port	4443	HTTPS	HTTPS (from Reverse Proxy) and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
			HTTPS Front-End inter-pool communications for AutoDiscover sign-in.
RPC Port	135	DCOM and remote procedure call (RPC)	Used for DCOM based operations such as moving users, user replicator synchronization, and address book synchronization.
SIP Port	5061	TCP (TLS)	Used by Front-End servers for all internal SIP communications.
SIP Focus Port	444	HTTPS, TCP	Used for HTTPS communication between the Focus (the component that manages the Skype conference state) and the individual servers.
SIP Group Port	5071	TCP	Used for incoming SIP requests for the response group application.
SIP AppSharing Port	5065	TCP	Used for incoming SIP listening requests for application sharing.
SIP Attendant Port	5072	TCP	Used for incoming SIP requests for the attendant (that is, for dial-in conferencing).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
SIP Conf Announcement Port	5073	TCP	Used for incoming SIP requests for the Skype for Business server conferencing announcement service (that is, for dial-in conferencing).
SIP CallPark Port	5075	TCP	Used for incoming SIP requests for the CallPark application.
SIP Call Admission Port	448	TCP	Used for call admission control by the Skype for Business server bandwidth policy service.
SIP Call Admission TURN Port	5080	TCP	Used for call admission control by the bandwidth policy service for Audio/ Video Edge TURN traffic.
SIP Audio Test Port	5076	TCP	Used for incoming SIP requests for the audio test service.
HTTPS External Port	443	HTTPS	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
			media and A/V sessions.
HTTPS Internal Port	443	HTTPS	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.
SIP External Remote Access Port	5061	TCP	Used for external ports for SIP/MTLS communication for remote user access or federation.
SIP Internal Remote Access Port	5061	TCP	Used for internal ports for SIP/MTLS communication for remote user access or federation.
SIP External STUN UDP Port	3478	UDP	Used for external ports for STUN/ UDP inbound and outbound media communications.
SIP Internal STUN UDP Port	3478	UDP	Used for internal ports for STUN/UDP inbound and outbound media communications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
SIP Internal IM Port	5062		Used for internal ports for SIP/MTLS authentication of IM communications flowing outbound through the internal firewall.
HTTP Port	80	TCP	Used for initial communication from Directors to the web farm FQDNs.
HTTPS Port	443	HTTPS	Used for communication from Directors to the web farm FQDNs.
AutoDiscover Internal Port	4443	HTTPS	Used for HTTPS (from Reverse Proxy) and HTTPS Director inter-pool communications for AutoDiscover sign-in.
SIP Internal Port	5061	TCP	Used for internal communications between servers and for client connections.

6. In the **Target Instances** section, select the three different NetScaler instance on which to deploy the three Skype for Business servers.

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

7. Click **Create** to create the configuration on the selected NetScaler instances.

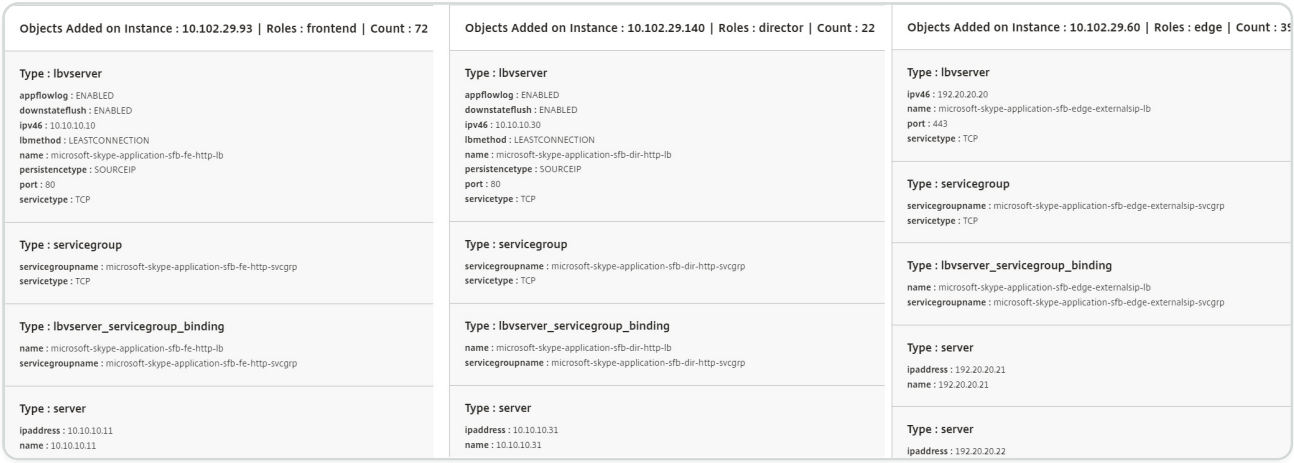
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

You can use the Microsoft Exchange 2016 StyleBook to deploy a NetScaler 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.

NetScaler features configured by using Microsoft Exchange StyleBook

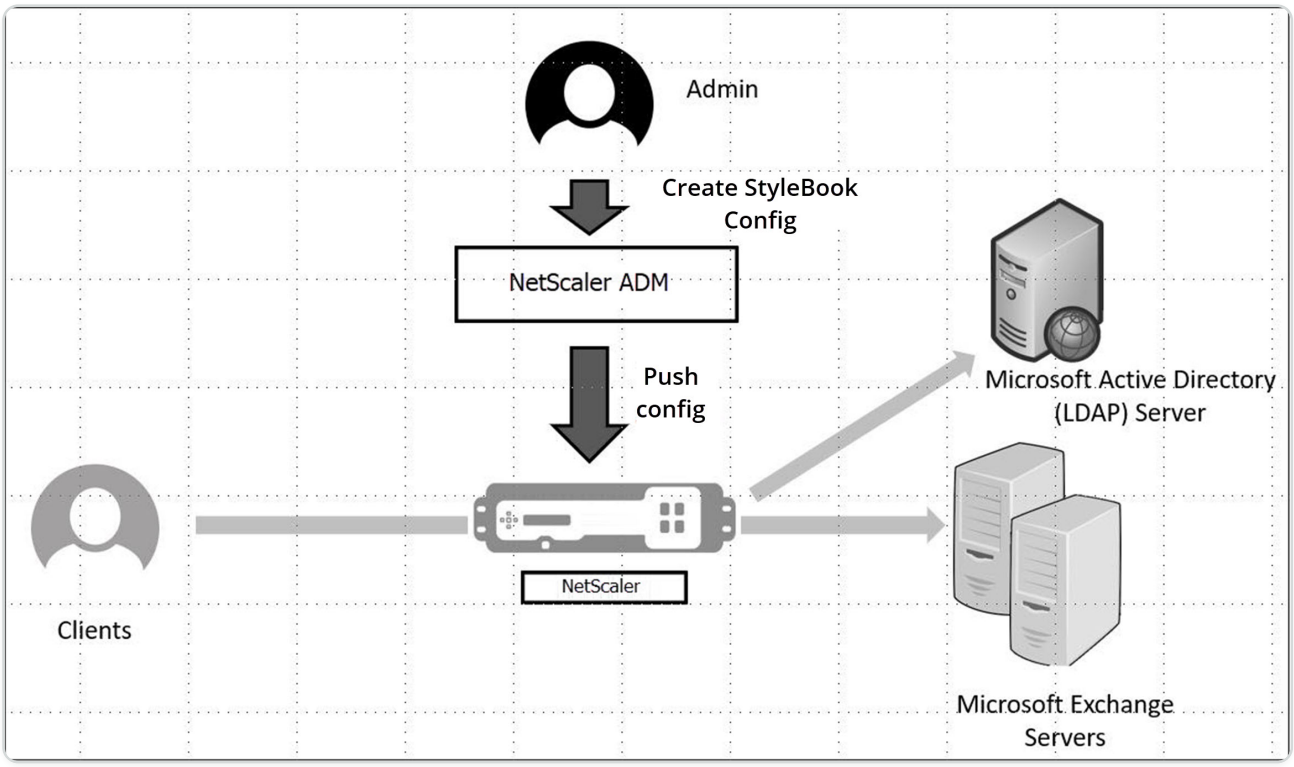
The Microsoft Exchange 2016 StyleBook enables and configures the following NetScaler features for Microsoft Exchange 2016 servers:

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rewrite - Redirects users to secure pages
- SSL offload - Offloads SSL processing to the NetScaler, 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 the Microsoft Exchange 2016 server.

Configuring a Microsoft Exchange StyleBook

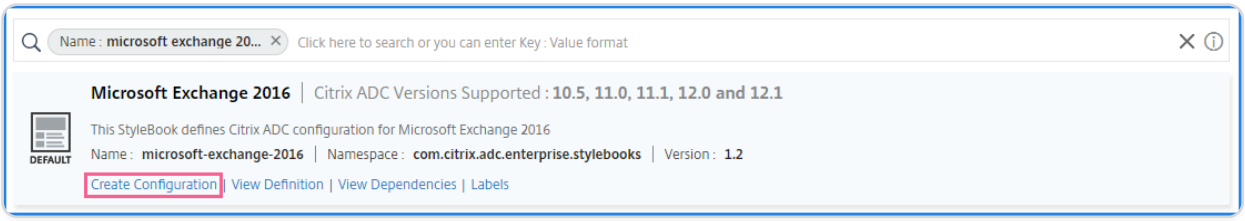
Configure the Microsoft Exchange StyleBook in your business enterprise to deploy the NetScaler configuration.

To configure a Microsoft Exchange application in NetScaler® ADM

1. In NetScaler ADM, navigate to **Applications** > **StyleBooks**.
2. Search for **Microsoft Exchange 2016 StyleBook** and click **Create Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler 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 NetScaler 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. NetScaler 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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 NetScaler 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-Attribute Name** - 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 NetScaler instance on which to deploy this Exchange configuration.

   NOTE

   If you want to view the recently discovered NetScaler instances, click the refresh icon.

7. Click **Create** to create the configuration file and run the configuration on the selected NetScaler instance.

   Citrix recommends that you first select **Dry Run** to check the configuration objects that are created on the target instance before running 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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can use the Microsoft SharePoint 2016 StyleBook to deploy a NetScaler configuration that optimizes and secures the Microsoft SharePoint 2016 enterprise application in your network.

Prerequisites

- Microsoft SharePoint 2016
- NetScaler ADM, version 12.0 and later
- NetScaler, version 10.5 and later

NetScaler features configured by the Microsoft SharePoint 2016 StyleBook

You can use the Microsoft SharePoint 2016 StyleBook to enable and configure the following NetScaler features for Microsoft SharePoint 2016:

- Load balancing
- Content Switching
- Responder
- Rewrite
- Compression
- Integrated Caching

Load balancing

NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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

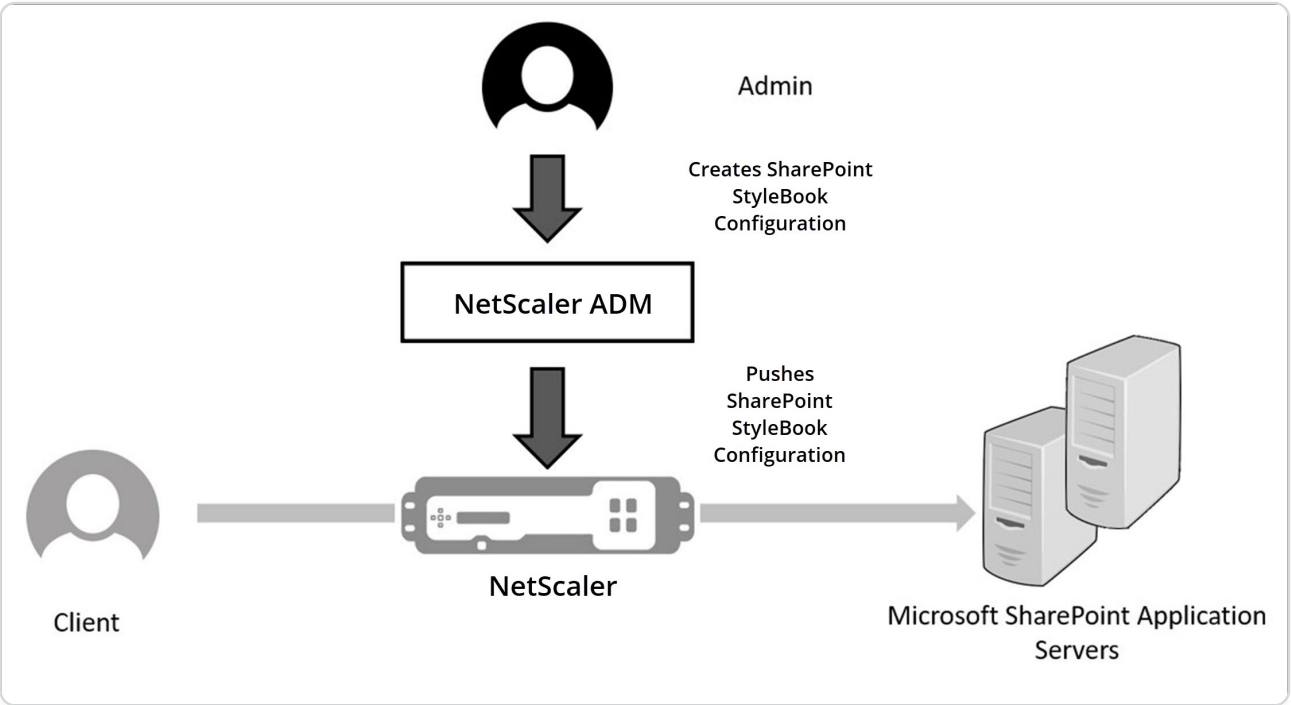
© 1997–2026 Citrix Systems, Inc. All rights reserved.

format. The major benefits of compressed traffic include reduced bandwidth costs, WAN latency reduction, and better server performance.

Integrated caching

The NetScaler 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 NetScaler instance on which NetScaler ADM is used to deploy a SharePoint StyleBook configuration.



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 NetScaler® ADM, navigate to **Applications** > **Administration** > **Configuration**, and click **Create New**.

   The **Choose StyleBook** page displays all the StyleBooks available for your use in NetScaler ADM.

2. Scroll down and select **Microsoft SharePoint 2016 StyleBook**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

In NetScaler 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 NetScaler 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.

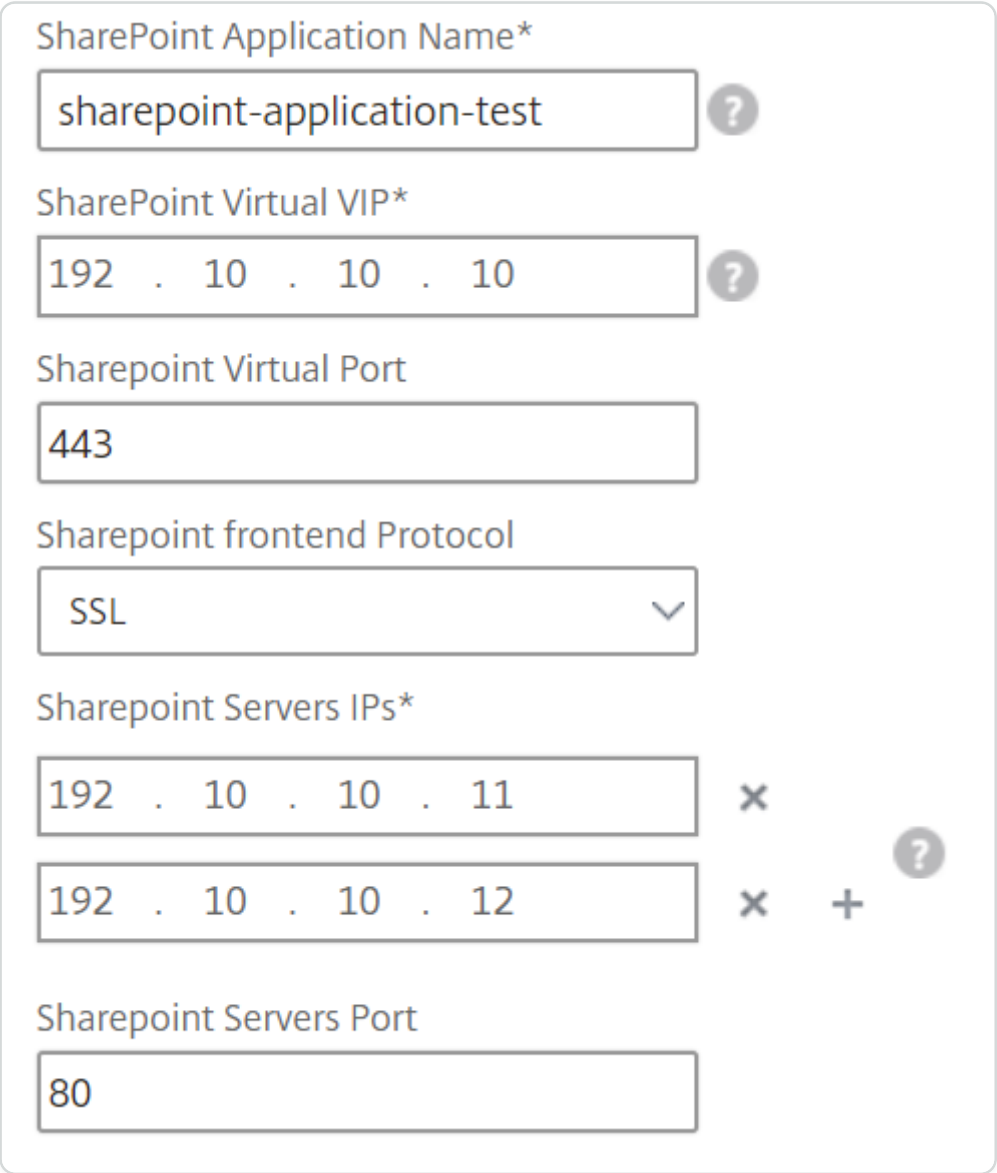
   NOTE

   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.

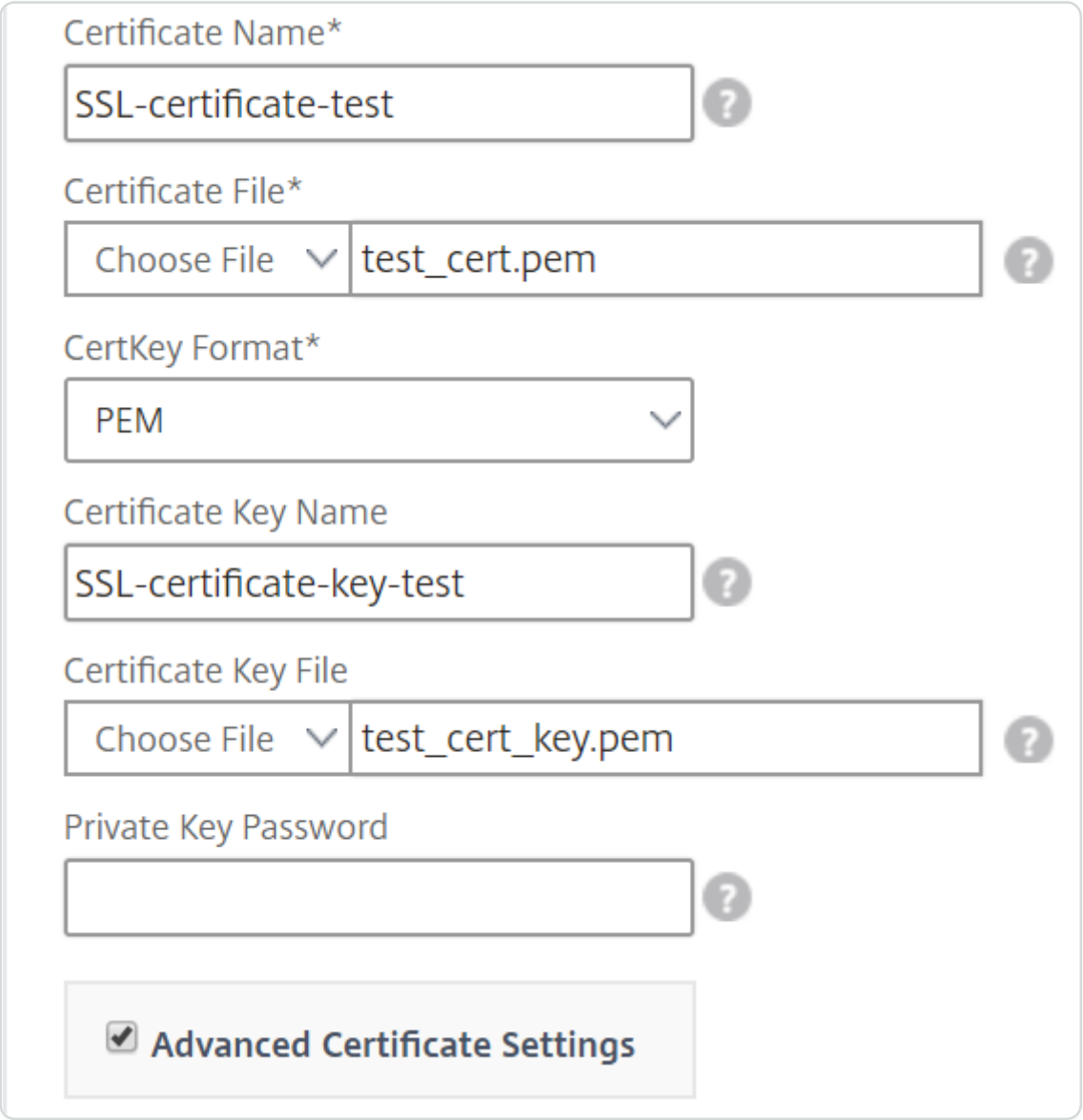
f. **SharePoint Servers Port**. TCP port number used by the SharePoint servers. By default, this is 80. You can edit this value if required, but make sure that this port is accessible on Microsoft SharePoint 2016 servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



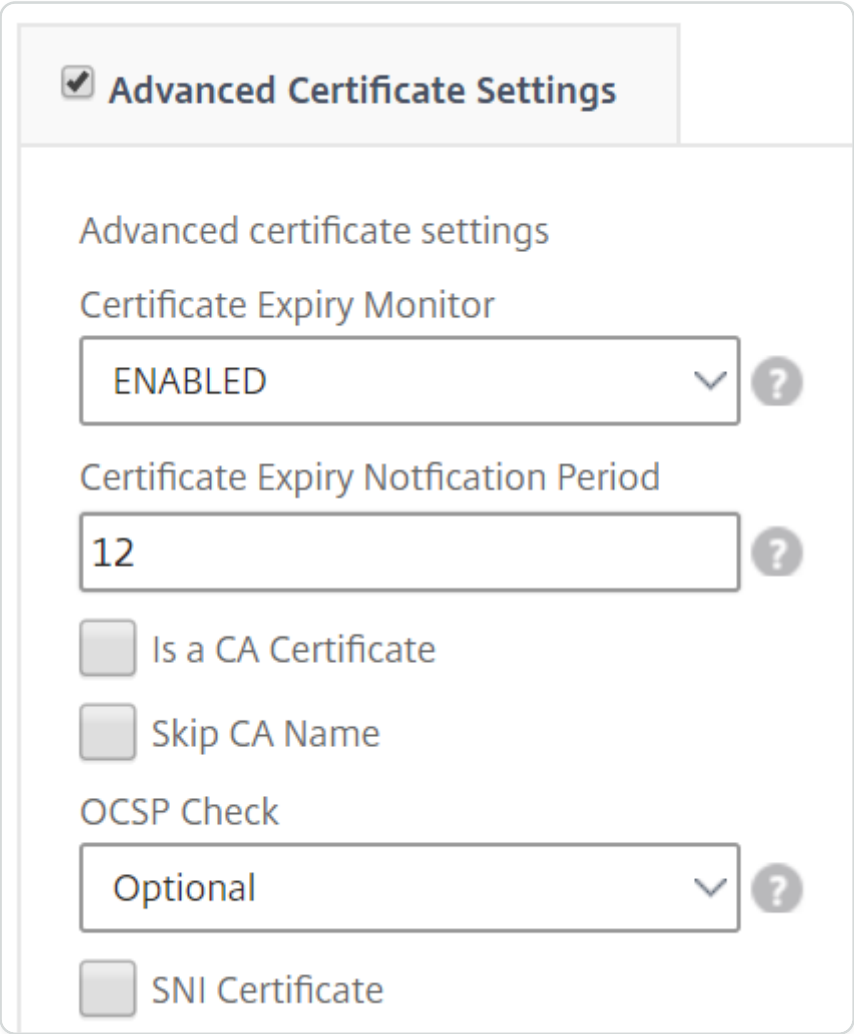
3. In the **SSL Certificates settings** section, click + to enter the name of the SSL certificate, the certificate key, and select the respective files from your local storage folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

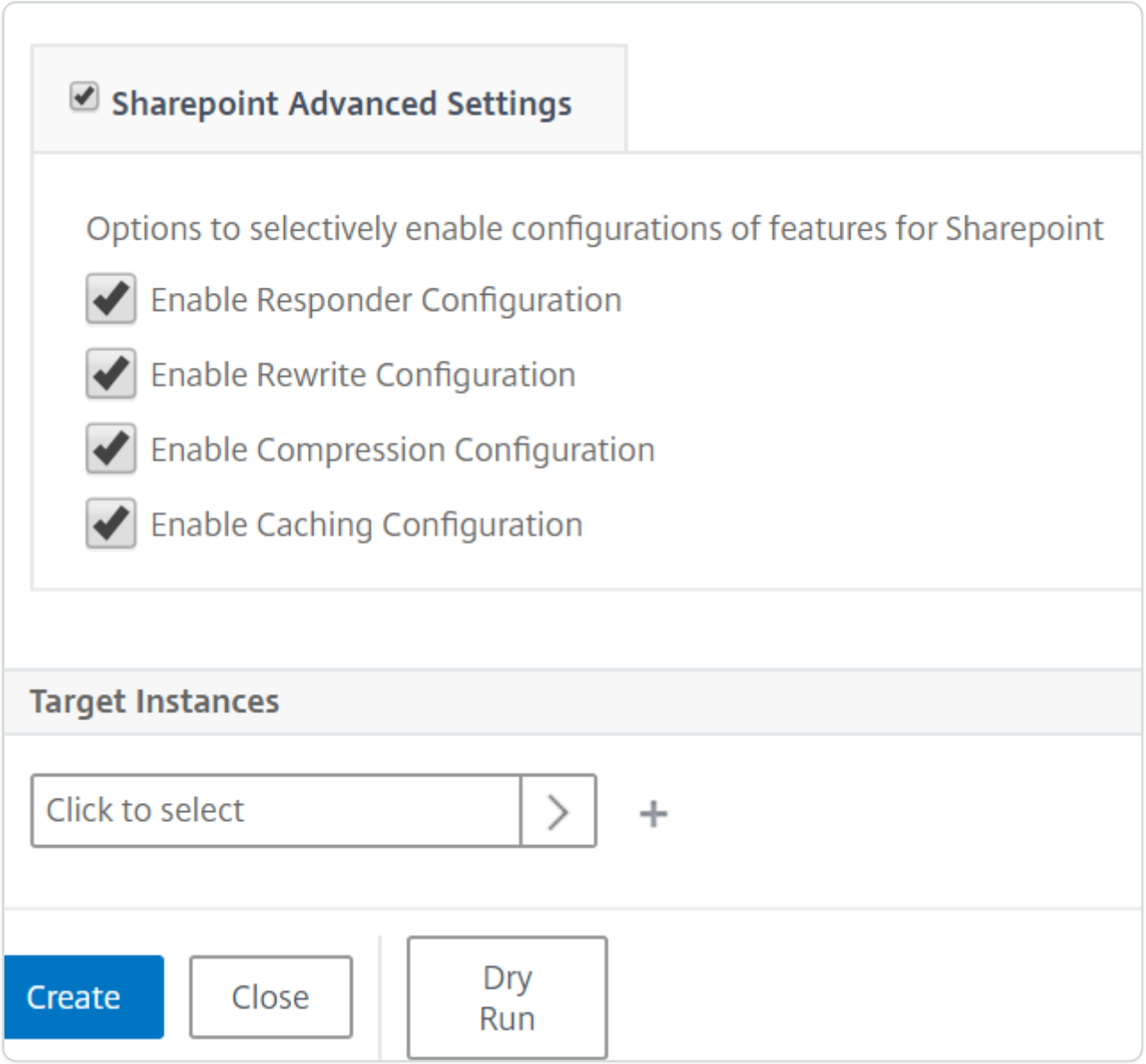


5. The SharePoint **Advanced Settings** section allows you to enable the NetScaler features that will be configured on the NetScaler instances. While the load balancing and content switching features are configured on the instances by default, you can choose the other features, that is, responder configuration, rewrite configuration, compression configuration, and integrated caching configuration, that you want to be configured on the instance.
6. Click **Target Instances** and select the NetScaler instance on which to deploy this SharePoint configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instance.

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Viewing the objects defined on the NetScaler instance

After the configuration pack is created on NetScaler ADM, you can view all the objects created on the NetScaler 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 NetScaler ADM."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : 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

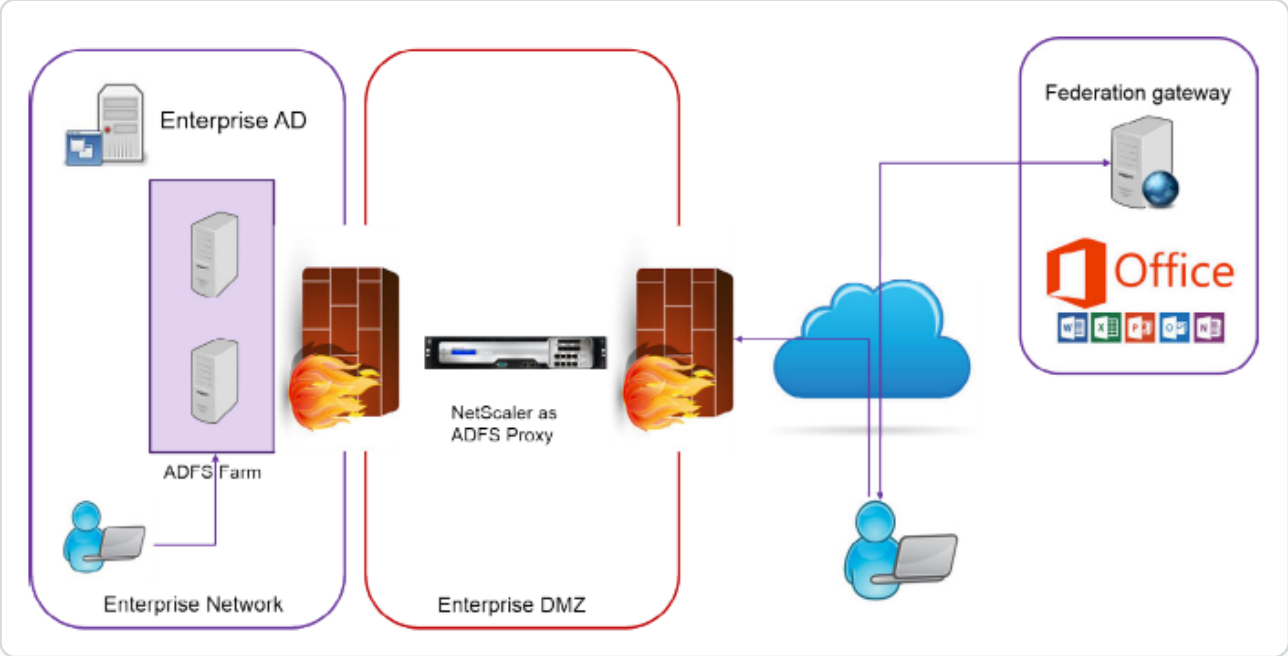
Microsoft ADFS proxy StyleBook

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.

NetScaler has the precise technology to enable secure connectivity, authentication, and handling of federated identity. Using NetScaler as ADFS proxy avoids the need to deploy an extra component in the DMZ.

The Microsoft ADFS Proxy StyleBook in NetScaler Application Delivery Management (ADM) allows you to configure an ADFS proxy server on a NetScaler instance.

The following image shows the deployment of a NetScaler instance as an ADFS proxy server in the enterprise DMZ.



Benefits of using NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   a. Examples of active protocol apps are – Microsoft Outlook, Microsoft Skype for Business
   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 NetScaler ADC features
   a. Content Switching
   b. SSL offload
   c. Rewrite
   d. Security (NetScaler 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). NetScaler 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 NetScaler AAA virtual server that handles the authentication for passive clients.

The StyleBook can also ensure that the DNS servers on the NetScaler are configured for ADFS.

The configuration section below describes how to set up NetScaler 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.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	11.0, Advanced/Premium License

The following instructions assume that you have already created the appropriate external and internal DNS entries.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploying Microsoft ADFS proxy StyleBook configurations from NetScaler® ADM

The following instructions assist you when implementing the Microsoft ADFS proxy StyleBook in your business network.

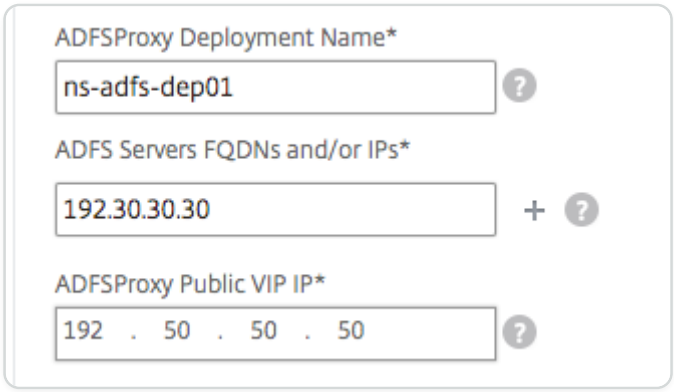
To deploy Microsoft ADFS proxy StyleBook

1. In NetScaler ADM, navigate to **Applications** \> **StyleBooks**. The **StyleBooks** page displays all the StyleBooks available for your use in NetScaler 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 NetScaler that performs as an ADFS proxy server.

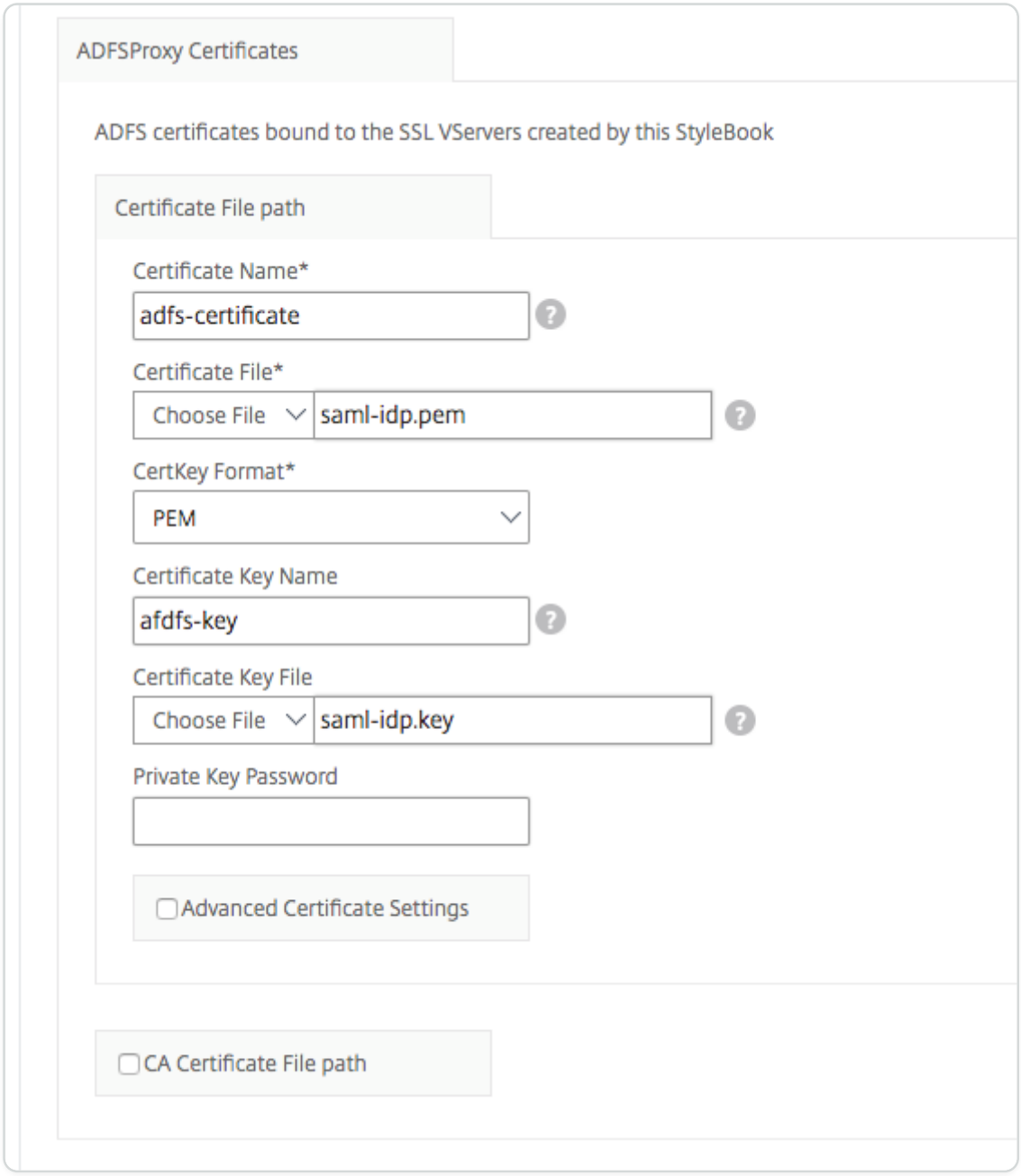


4. In the **ADFS Proxy Certificates** section, type the details of the SSL certificate and the certificate key.

   This SSL certificate is bound to all the virtual servers created on the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler. 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

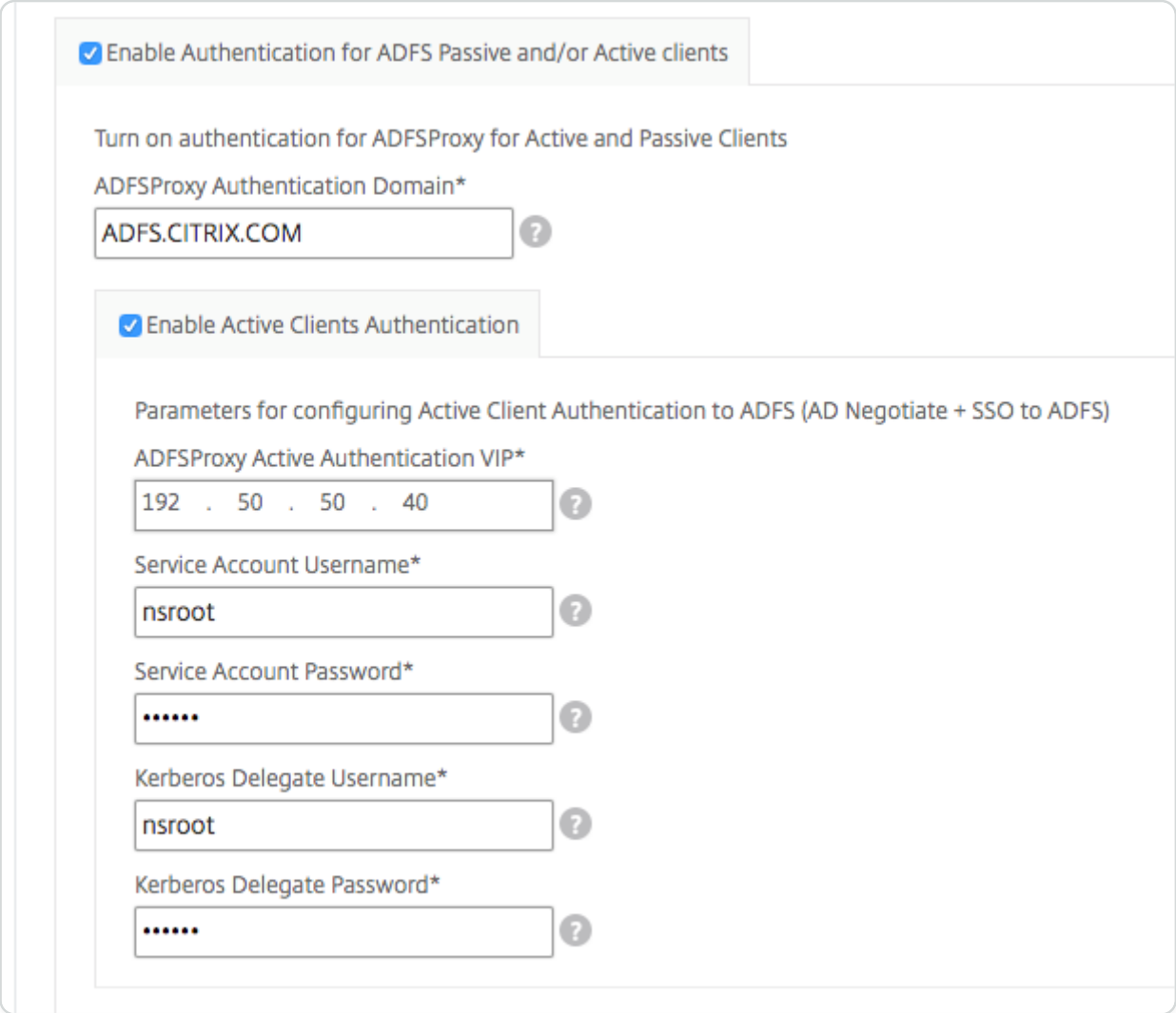
NOTE

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 NetScaler instance where the active clients are redirected for authentication.

b. **Service Account Username**. Type the service account user name used by NetScaler to authenticate your users to the active directory.

c. **Service Account Password**. Type the password used by NetScaler to authenticate your users to the active directory.



8. Configure authentication for passive clients by enabling the corresponding option and configuring the LDAP settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

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.

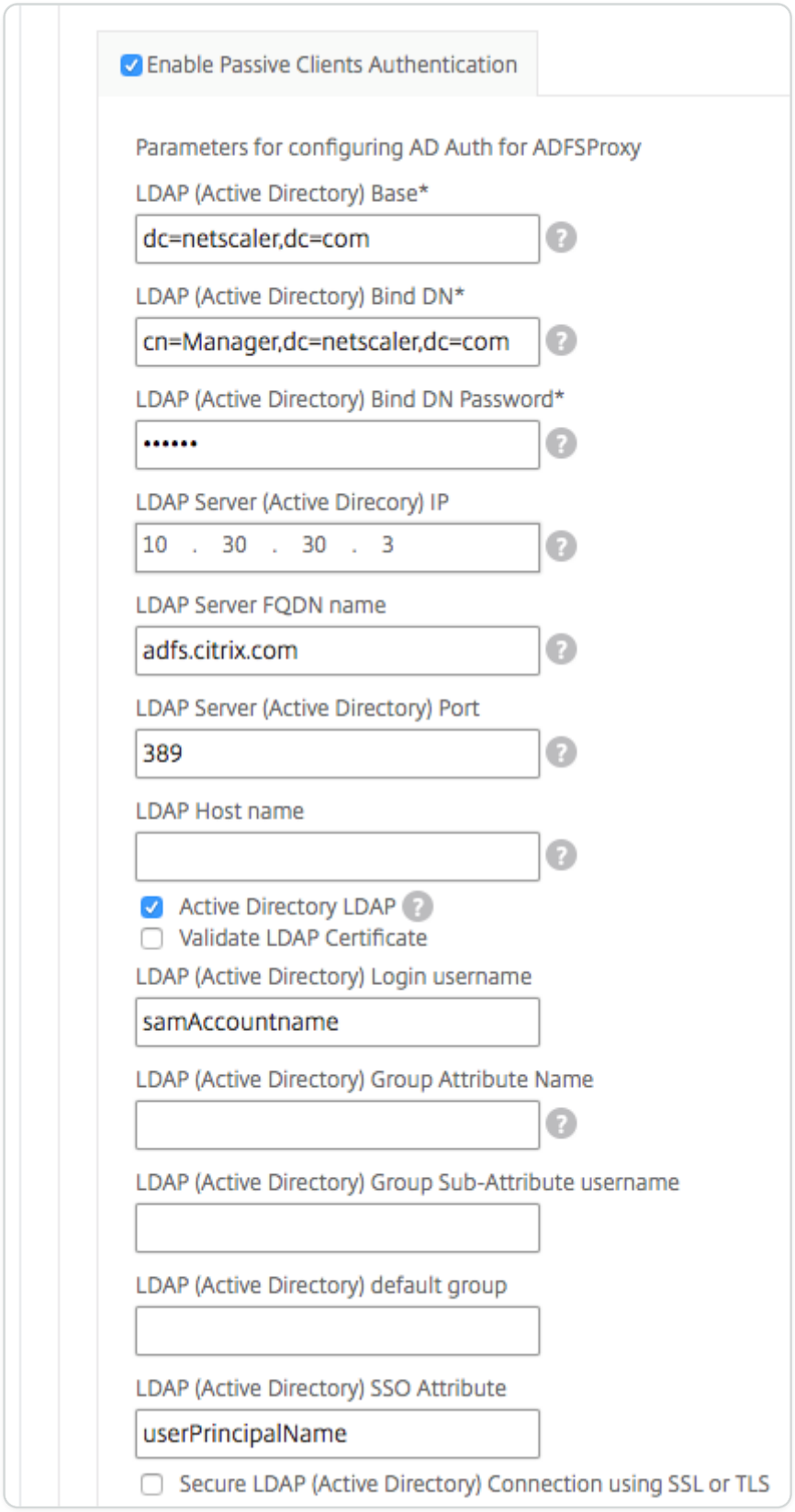
g. **LDAP (Active Directory) login username**. Type the username as "sAMAccountName."

h. **ADFS Proxy Passive Authentication VIP**. Type the IP address of the ADFS proxy virtual server for passive clients.

   NOTE

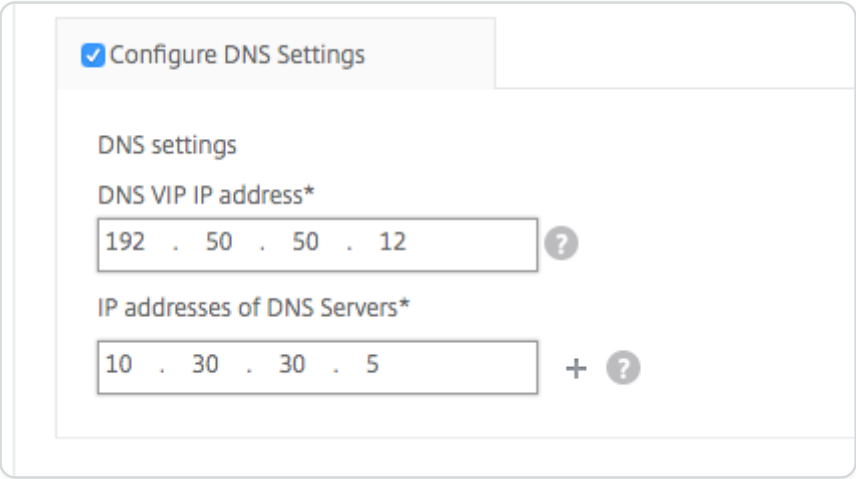
   The fields marked with "*" are mandatory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

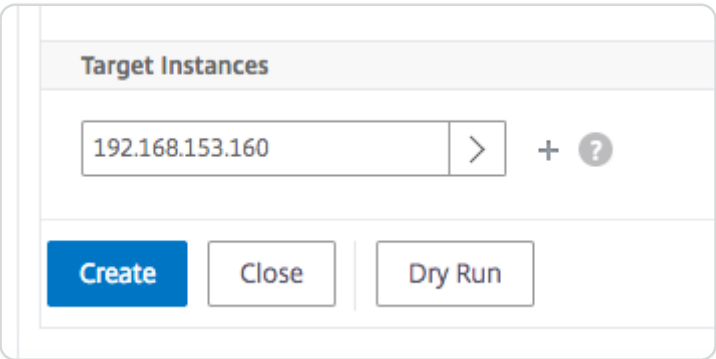


9. Optionally, you can also configure a DNS VIP for your DNS servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Click **Target Instances** and select the NetScaler instances to deploy this Microsoft ADFS proxy configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instances.



NOTE

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 NetScaler instances by the StyleBook. 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 NetScaler instance. The following image displays the list of objects created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURtVENDQW9HZ0F3SUJBZ0lCQXpBTkJna3Foa2lHOXcwQkFRc0ZB
VFHRXdKVlV6RW1NQ1FHQ1NxR1NjYjNEUUVKQVJZWApIVzkxWTJWbUxXTmhRR0ZqYldVdFkyOXljQzVqYjIweEZEQV
1URXlPVEExTVRrd05Wb1hEVEI5TVRFeU9EQTFNVGt3TlZvd2dZZ3gKR0RBV0JnTlZCQU1NRDNsdmRXTmxaaTF6WVcx
FRa0JGaGw1YjNWalpXWXRjMkZ0YkVCaFkyMWxMV052Y25BdVkyOXRNUkl3CkVBWURWUVFLREFsQlEwMUZMVU5
GQUFPQ0FROEFNSUlCQ2dLQ0FRRUF5L1gza0VCd2F0SEpoQmFXR2Z6WmwxQ1FkZ2JtbDFlYgpZT3hadG4xOHNpS
9kNXJCOHNmeG56K2RvbjJyaUhHaktEazVPYkFScmd2NVNHaGhmL3pvQVpDa3MybkVocjh6UElxOWoKQm8wc3NlTl
HV3VlpBakQxVitnNTVHSkdXMW9ubndyTlc0Q3ViTzMyRTFDNjh1WG1TZnIwdUlzTzIvRDF2ZnovSDh0QlM4CjFlV0Vla
0RBSkJnTlZIUk1FQWpBQU1Bc0dBMVVkRHdRRUF3SUY0REFOQmdrcWhraUc5dzBCQVFzRkFBT0NBUUVBbk1RSQpz
KOGc3CjNlUzlkbE15UkUveXh4N3V5SXpqR0ZaV1VBclMxL09PcUxGRHR2NEFZWXZ6UVhGL0pWM2phWjZnUkdMS0
zFRclNHdVYrdgoxRW1tMlNNcWxrbGVVclN5QXBuSlVWNHA0QTVDbTh6UTRVVDhtZjZQRkU2TFhRTHZCYzhWdUJvR
NBVEs1azE1NVZSd2UKaWt3OFYzR082MmdRc0hvV05RPT0KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=

fileencoding : BASE64

filelocation : /nsconfig/ssl

filename : saml-idp.pem

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBeS9YM2tFQndhdEhKaEJhV0dmelpsM
Q2eWJWY1NzajFiT0JEdU9CbVpnRS9LQS9kNXJCOHNmeG4Keitkb24ycmlIR2pLRGs1T2JBUnJndjVTR2hoZi96b0FaQ2t
BhTU1tV3dyQmN0OUhKdEJxcEpVUHV3VlpBakQxVitnNTVHCkpHVzFvbm53ck5XNEN1Yk8zMkUxQzY4dVhtU2ZyMH
h0bW1YT2tLb0JWaXdjREFRQUJBb0lCQUVtS1FGOEV2UVBtN0cveAo3T0VsNkJiRTk3RjJ2NEhtRnFJVjFpc1VoL2Q2Y2h2
WTUdnTHBZcDYvRS9DcFFQdkhyNEJSS3hiVXBvQkpaZ0g0eloKRHZjT1dadIjtc0hXYVBkUmoxVDNaaHdsd21aMEQ4U
wrSXBBRHJybkdOdUNHMId4NUorNHM3VG9aMXYzc1NtRThaK2pqdWtYCk5DTFBKcnh3dFJlSXc3ajRTenlDNWFCR1M
1RrZHhTc2ZPblF6THgwYUNQWnFWNCtQVkoycThzbkpvMXhJOWI1dE9mRlBNVApGRHZNYXZwKytHQnpWTyszRWI
wWDA2NWlSTnZVYnVrQklqWDgvYkhTNIlITjFWR2o2RVFYQmtrNmJmSXNDZ1lFQXpNQ2kKMkFhd0FTY3htT0Q1Zm
1PZTNPU2dVMWh4WmNDdjlUMGhNNEdWVVQyVFhqWkZNWWFBWk8yNjFwdWVKbTRkMXZqdDY3CjJrN0tVclhpY
iMzgxNW5tUmpyZTFrK21QN2tuL0xFQk1pVUVXV0tybXpFanRsbzhRTFhXVjZzU3ltVXJCVU11bnVLWgo1Y1B5bFdFTE
VCcUwwQjh5a0djUGVUbkRlS3dLQmdRQ0tBME1BMkNrazdkVkpsa08xb05jTDhrUGNYL0ZzckJURi8xL0QKRTcva1AxT
GR1Blb3NJK3FxQWw1aktiY3AxMFZYNUJ1cS9xbm9vREVkN2d0NGNFcEM0RTUvQW85VThGWVVGR3ZpcC9wdGwxC
EeloKUmllWXlWUnRkbkU5TE5kYU5STXdpTWFCYkhFazF4R1IxSDByQnFEYUE0M1B4Zm9FYjdndEdCaHE2azRUempa
otLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=

fileencoding : BASE64

filelocation : /nsconfig/ssl

filename : saml-idp.key

Type : sslcertkey

cert : saml-idp.pem

certkey : adfs-certificate

inform : PEM

key : saml-idp.key

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_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 : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-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-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
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-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : 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
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-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-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : rewritepolicylabel_rewritepolicy_binding

gotopriorityexpression : END
labelname : ns-adfs-dep01-request-rewritepolicylabel
policyname : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
priority : 10

Type : lbvserver_rewritepolicy_binding

bindpoint : REQUEST
gotopriorityexpression : END
invoke : true
labelname : ns-adfs-dep01-request-rewritepolicylabel
labeltype : policylabel
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
policyname : NOPOLICY-rewrite
priority : 10

Oracle e-business StyleBook

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 NetScaler 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

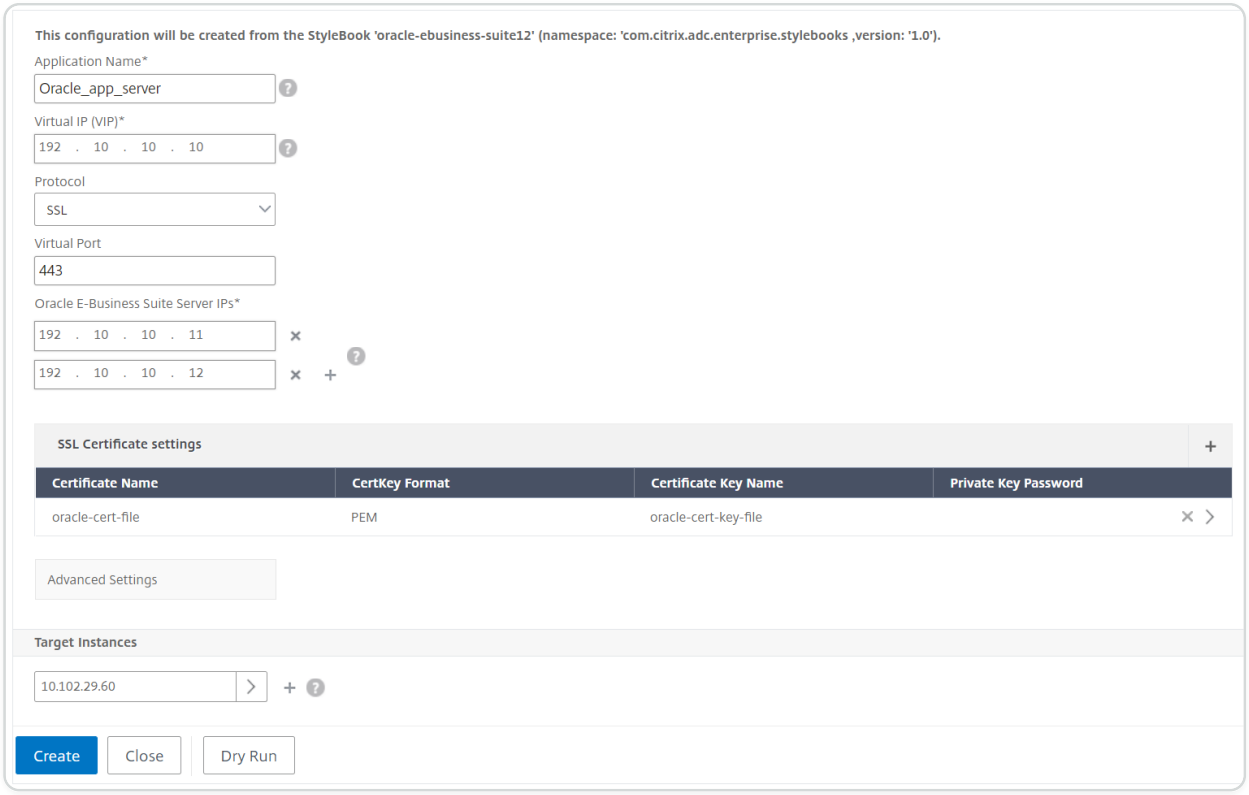
1. In NetScaler Application Delivery Management (ADM), navigate to **Applications** > **Configuration > StyleBooks**. The **StyleBooks** page displays all the StyleBooks that are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

available in your NetScaler 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 NetScaler instance on which the configuration must be created, and click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window. The refresh icon is currently available only on NetScaler ADM.

Citrix StoreFront™ StyleBooks

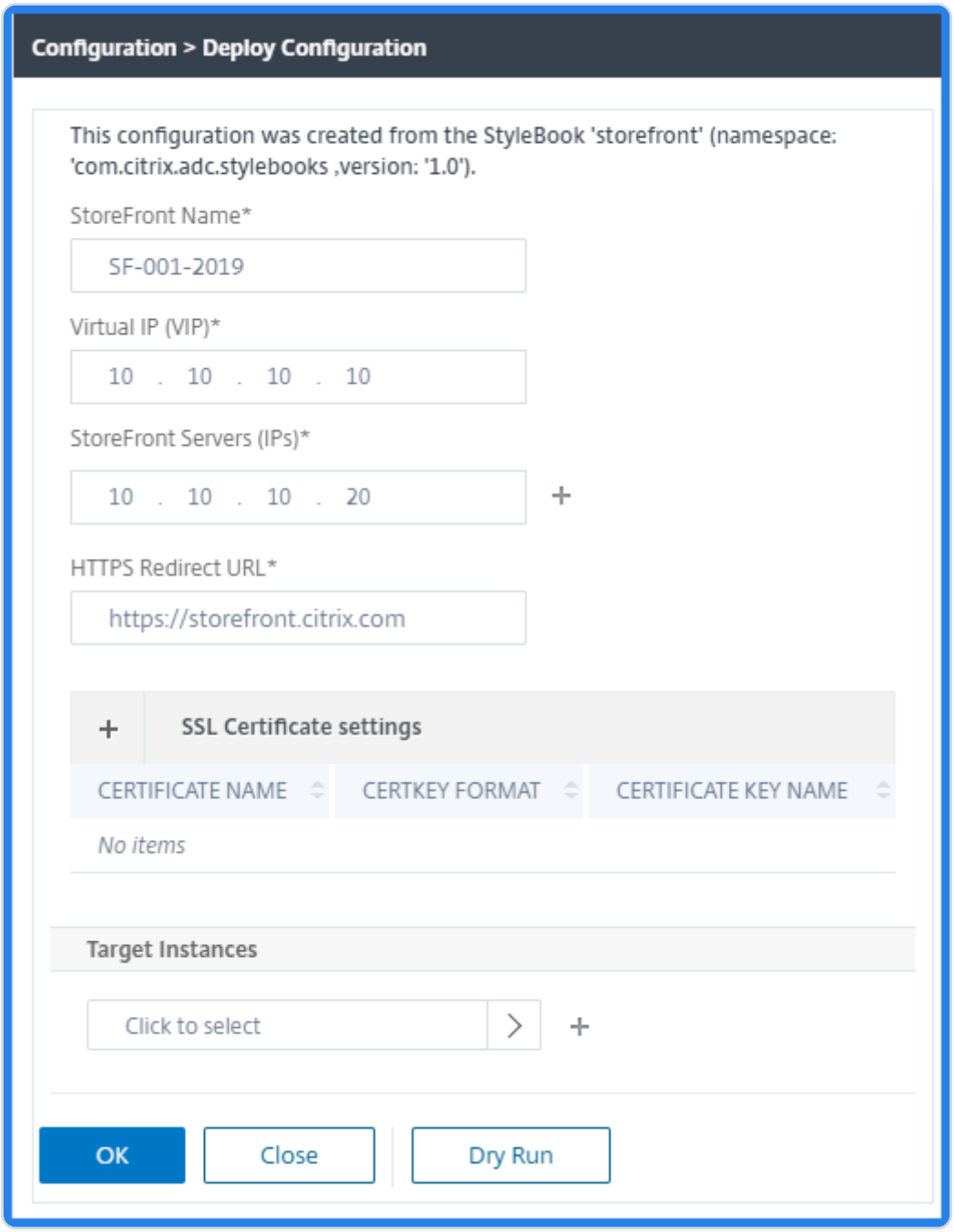
StoreFront is an enterprise app store that aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single store for users. StoreFront authenticates users to sites hosting resources and manages application stores and desktops that users access. It hosts your enterprise application store, which allows you give users self-service access to app and desktops you make available to them.

This StyleBook defines the NetScaler configurations for StoreFront servers. With this StyleBook, you can configure StoreFront servers to the desired NetScaler instances. You can choose encrypted communication by selecting SSL and providing the SSL files and key files from your local system.

Create configuration for Citrix StoreFront applications

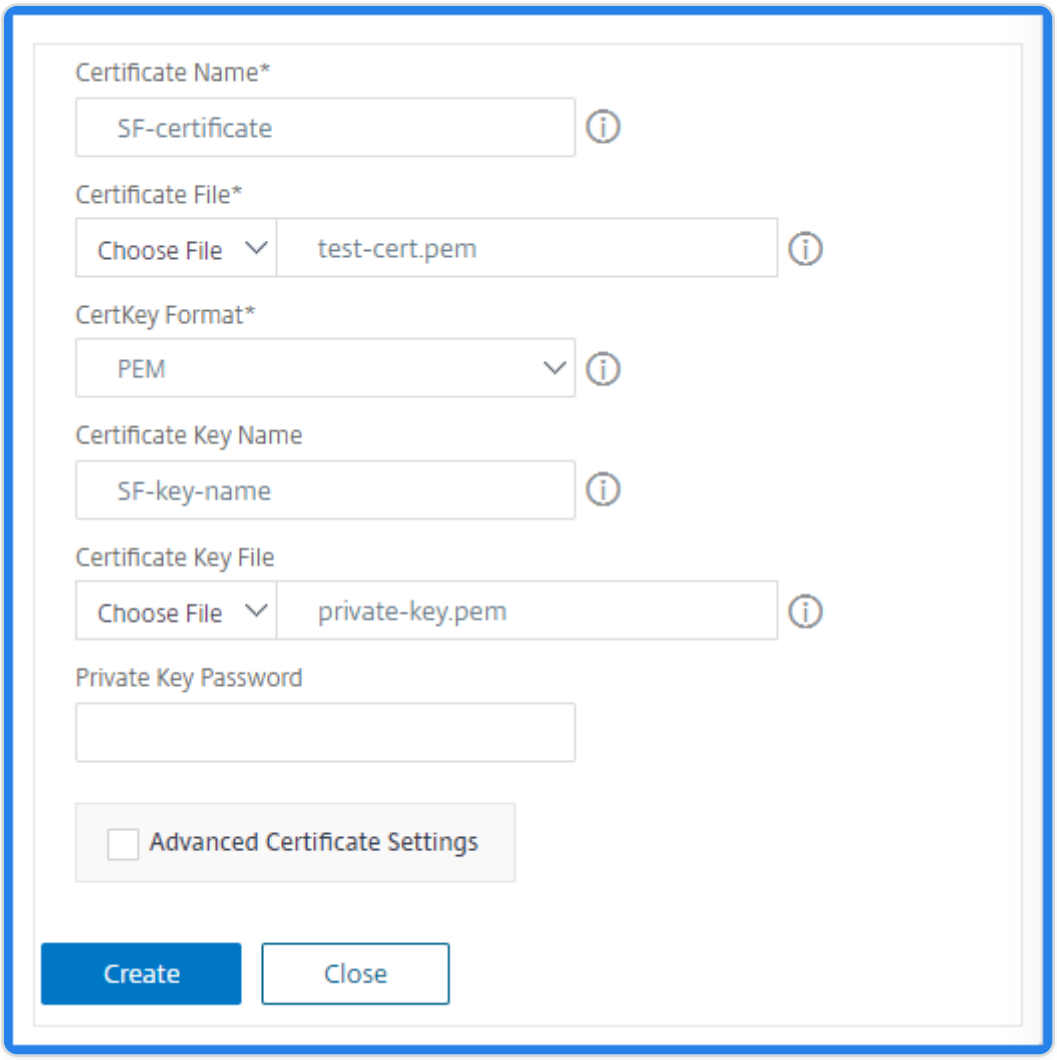
1. In the NetScaler® ADM GUI, navigate to **Applications > StyleBooks**.
2. In the search bar, use the **Name** properties and search `Citrix StoreFront`.
3. On the Citrix StoreFront StyleBook, click Create Configuration.
4. Specify the following details:
   - **StoreFront Name**: Specify the StoreFront name. The StoreFront ConfigPack is created with the same StoreFront name.
   - **Virtual IP (VIP)**: Specify the virtual IP address at which the NetScaler instance receives the client requests.
   - **StoreFront Servers**: Specify the IP addresses of the StoreFront servers that you want to configure with a NetScaler instance.
   - **HTTPS Redirect URL**: Specify the HTTPS url to which the HTTPS requests are redirected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. In **SSL Certificates Settings** section, enter the names of the SSL certificate and the certificate key.
6. Select the respective files from your local storage folder. You can also type in the private key password to specify the encrypted private keys in PEM format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 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.
8. Optional, select **SSL CA Certificate for the authentication virtual IP** check box if the SSL certificate requires a CA public certificate to be installed on NetScaler. Make sure you choose **Is a CA Certificate** in the **Advanced Certificate Settings** section.
9. Click **Create**.
10. Click **Target Instances** and select the NetScaler instances on which you want to configure the StoreFront servers.
11. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instances.

Create and use custom StyleBooks

You can write your own StyleBook for your deployment, import it to NetScaler® Application Delivery Management (ADM), and create configuration objects. You can also use API to create configurations from your StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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/OFF/Off/off, and TRUE/true/truthy/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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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 NetScaler 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 NetScaler ADM on any virtual server that is part of the StyleBook.

The following figure shows a simple outline of a StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: name
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
```

Header

Import StyleBooks

Parameters

Components

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

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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 NetScaler® ADM.
- **display-name**: A descriptive name for the StyleBook that appears on NetScaler 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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler 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 NetScaler 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 NetScaler NITRO version. A StyleBook that is based on Nitro version X can be used to configure any NetScaler that is version X or higher.

NOTE

To ensure that your StyleBooks can be used to configure any NetScaler 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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScalers 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:

```
parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Name of the application configuration.

  required: true



 -

  name: ip

  type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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 NetScaler 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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you import your StyleBook and use it, NetScaler 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 SyleBook.

For this example, you have to write the components section as follows:

```
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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 NetScaler ADM, or the default StyleBook that is shipped with NetScaler 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 NetScaler Nitro resources and their attributes, see the NetScaler 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 servicetype 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 NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: "Give a name to the application configuration."
    type: string
    required: true
  -
    name: vip-ipaddress
    label: "Load Balancer IP Address"
    description: "The Application VIP that clients access"
    type: ipaddress
    required: true
  -
    name: lb-alg
    label: LB Algorithm
    description: Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
     - ROUNDROBIN
     - LEAST-CONNECTION


  components:
   -
    name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler load balancing virtual server configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

To start using your StyleBook to create configurations, you have to import it to NetScaler 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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you have changed the name, the combination of name, namespace, and version creates a unique identifier for this StyleBook in the system.

```
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.

```
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.

```
parameters:

 -

 name: name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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:

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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 + "-svcgrp"
   servicetype: HTTP


components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver\_servicegroup\_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

 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 NetScaler 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
components:

 -

  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.svcg-comp.properties.name

 -

  name: lbvserver-svg-binding-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  type: ns::lbvserver\_servicegroup\_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
  name: $parameters.name + "-svcgrp"
  servicetype: HTTP
```

Here, all the components are at the same level (that is, they are not nested) but the result achieved (the NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      - 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

  -

    name: svcg-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP


 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.servicegroupname
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: 80
   servicegroupname: $components.svcg-comp.properties.servicegroupname
outputs:
-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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
```

To start using your StyleBook to create configurations, you have to import it to NetScaler 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

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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ipaddress

    label: Application Virtual IP (VIP)

    description: The Application VIP that clients access

    required: true

  -

    name: svc-servers

    type: ipaddress[]

    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true



  -

    name: response-code

    type: string[]

    label: List of Response Codes

    description: List of Response Codes - Provide a list of response codes
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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

          type: ns::servicegroup_lbmonitor_binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          properties:

            servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

            monitor_name: $parent.properties.monitorname
```

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 “lbmonitor” (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 NetScaler ADM. Then, import it to NetScaler 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

You can add GUI attributes in the parameters section of your StyleBook to make the fields intuitive when displayed on NetScaler® Application Delivery Management (ADM).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress

required: true
```

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.

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object

required: false

gui:

 collapse_pane: true

 columns: 2
```

Example. Some StyleBooks on NetScaler 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 NetScaler ADM GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: basic-lb-config

description: This stylebook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

private: true

schema-version: "1.0"

version: "0.1"
```

Import custom StyleBooks

After you have built your StyleBook, you have to import it to NetScaler® Application Delivery Management (ADM) to use it. NetScaler 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 NetScaler ADM system validates your StyleBooks on import. The StyleBook is now ready to be used for creating configurations.

NetScaler 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 the NetScaler 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 NetScaler 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 the YAML content.
- **YAML validation**. The content is validated for any YAML errors as you type in and any deviation is immediately highlighted. This validation allows you to write text that conforms to YAML guidelines even before you import the StyleBook in the ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Currently, the editor validates the content according to YAML guidelines. It does not validate for code correctness and typographical errors.

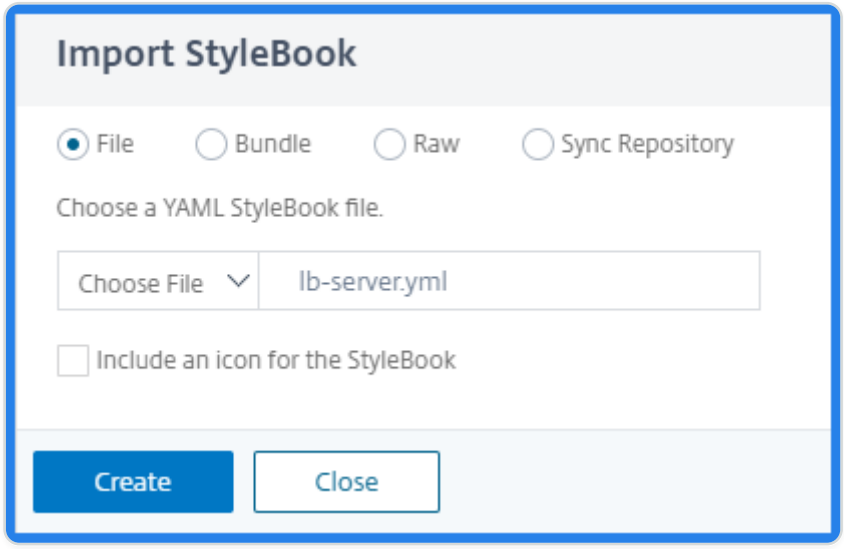
To import your StyleBook

1. In NetScaler ADM, navigate to **Applications** > **Configuration** > **StyleBooks**, and then click **Import New StyleBook**.
2. Click one of the following options to import a StyleBook.

   - **File** - select the required file or the bundle of files from your local storage.

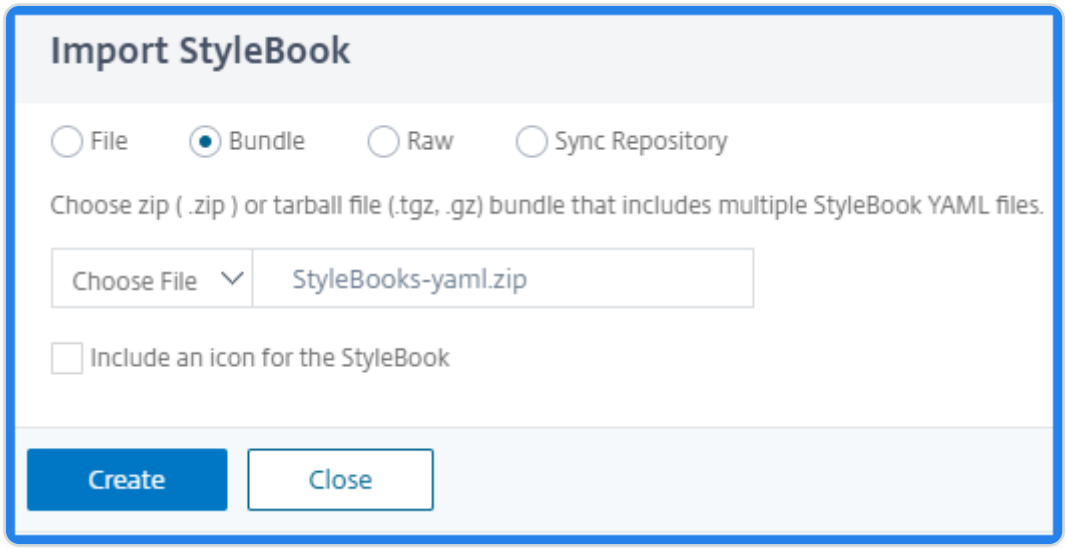
     NOTE

     In this example, import the `lb-vserver.yml` StyleBook that you had created in StyleBook to Create a Load Balancing Virtual Server.

   - **Bundle** - NetScaler ADM allows you to import multiple StyleBooks in YAML format. You can import more than one YAML StyleBook files that are compressed in a zip (.zip) format or tarball (.tgz, .gz) format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can now include icons to each StyleBook in the bundle. Ensure to have the resources folder that contains icons in the PNG, GIF, or JPEG formats. If the icon file name matches the StyleBook name, the icons are automatically mapped to the StyleBooks. Otherwise, do the following:

a. Add the `icon_mapping.json` file in the resources folder.

b. Map StyleBooks and icons in the `icon_mapping.json` file as follows:

```
<StyleBook file name> : <icon file name>
```

The following is an example StyleBook bundle:

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

The `resources` folder contains the required icons.

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

In this example, `sharepoint.yaml` and `skype.yaml` files are automatically mapped to `sharepoint.jpeg` and `skype.png` respectively.

To map `exchange.yaml` to `exch.png`, specify the following in the `icon_mapping.json` file:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

"exchange.yaml":"exch.png"

}
```

If you specify the `defaulticon` entry, the StyleBooks are mapped to the default icon unless they are mapped to a different icon.

```
defaulticon: <icon file name>
```

In **Applications > StyleBooks**, the imported StyleBooks appear with the mapped icons.

- **Raw** - Compose the content of your StyleBook in the YAML editor.

  You can validate the StyleBook contents to check the StyleBook grammar errors. To validate StyleBook contents, click **Validate Contents**.

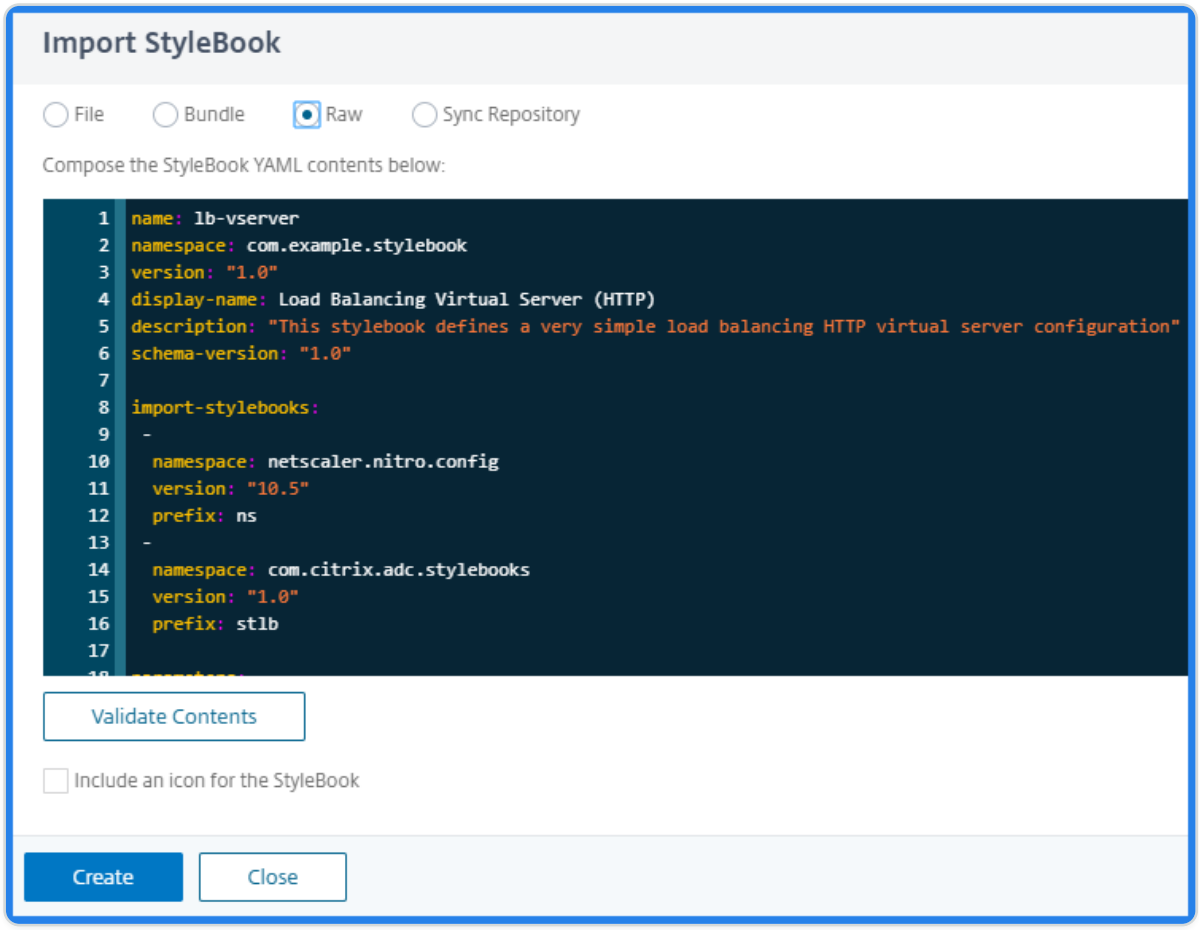
  NOTE

  While composing StyleBook, make sure to know the following concepts:

  - NITRO API
  - YAML

  For more information about how to write your own StyleBooks, see How to Create Your Own StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Sync Repository** - This option lists the repositories added to ADM. Select the repository that you want to synchronize with ADM.

NOTE

You can also copy and paste the content from a StyleBook YAML file to the YAML editor.

3. Optional, select an icon to a StyleBook.

   In **Applications > StyleBook**, the imported StyleBook appears with this icon.

4. Click **Create**.

   NetScaler ADM now validates your StyleBook for all syntactic and semantic errors according to the StyleBook grammar. Your StyleBook is not imported into NetScaler ADM if there are any errors.

   If there are no errors the StyleBook is successfully imported and 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If you are importing a bundle of files, NetScaler ADM decompresses the zipped folder and validates all the StyleBooks. The bundle is not imported even if one StyleBook file fails the validation test.

For more information on StyleBook grammar and syntax of the different constructs and attributes, see StyleBook Grammar.

5. Click the **Create Configuration** link to create configurations from this StyleBook.

   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

6. Specify the required values for the parameters.

   In the following example,

   a. Specify the **application name** and **load balancer IP address** mandatory fields.
   b. Select the **LoadBalancing Algorithm** from the list. By default, **ROUNDROBIN** is selected.

7. Under **Target Instances**, select the IP address of the NetScaler instance where you want to deploy the configuration.

   You can also deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.

8. If you want to test at the NetScaler (NITRO) configuration objects before you deploy the configuration, click **Dry Run**.

   If the configuration is valid, the configuration objects are created based on the specified values.

   In this example, the StyleBook creates only one object of type `lbvserver`. This load-balancing server was the only component defined in this basic example StyleBook.

   Later, click **Create** to deploy the configuration on the selected NetScaler instances.

After you deploy the configuration successfully, a new configuration pack appears in the **Configurations** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

Search custom StyleBooks

NetScaler 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 many default StyleBooks.

To search for custom StyleBooks

1. In NetScaler ADM, navigate to **Applications** > **Configurations** > **StyleBooks**.
2. Click the search icon at the top right side.
3. In the search bar, select **Type** and then select **Custom** from the sublist.
4. NetScaler ADM displays only the user-defined StyleBooks.

Create and edit a configuration pack

In NetScaler® Application Delivery Management (ADM), you can create a configuration pack from a StyleBook. And, the configuration pack is tied to the StyleBook from which it is created. The updates to the configuration pack are made through the StyleBook to which it is tied.

Create a configuration pack

Perform the following to create a configuration pack from a StyleBook:

1. Navigate to **Applications > StyleBooks > Configurations**.
2. Click **Add**.
3. In **Choose StyleBooks**, select the required StyleBooks from which you want to create a configuration pack.

   This page categorizes StyleBooks into default and custom StyleBooks. Select the respective tabs to find the required StyleBooks.
4. Specify the required details such as application name, IP address, port, or protocol type.

   The GUI fields differ from one StyleBook to another StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In **Target Instances**, select instances or instance groups where you want to run the configuration.

   NOTE

   You can deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.

6. Click **Dry Run**.

   The **Objects** page displays the objects that get created, modified, or removed from the NetScaler instances.

7. Click **Create**

   The configuration pack appears in the **StyleBook > Configurations** page.

If you want to edit the existing configuration packs, select the configuration pack and click **Edit**.

Change the StyleBook of a configuration pack

Sometimes, you need to update the StyleBook to add functionality or fix an issue. If you already have created configuration packs using the old StyleBook, you might want to update them to use the new updated StyleBook. To use a new StyleBook, change the existing StyleBook of the configuration pack.

Consider an example StyleBook **example-lb** that deploys a basic load balancer configuration on an ADC instance. And, you create a configuration pack CP1 from this StyleBook.

When you want to configure monitors with the basic load balancer configuration, you need a new StyleBook. Therefore, create **example-lb-mon** StyleBook that includes the ability to configure monitors along with the basic load balancer configuration.

After you create a StyleBook, update the existing configuration pack CP1 to add some monitors. To do so, perform the following:

1. Navigate to **Applications > StyleBooks > Configurations**.
2. Select the configuration pack for which you want to change the StyleBook.

   In this example, select CP1 from the list.

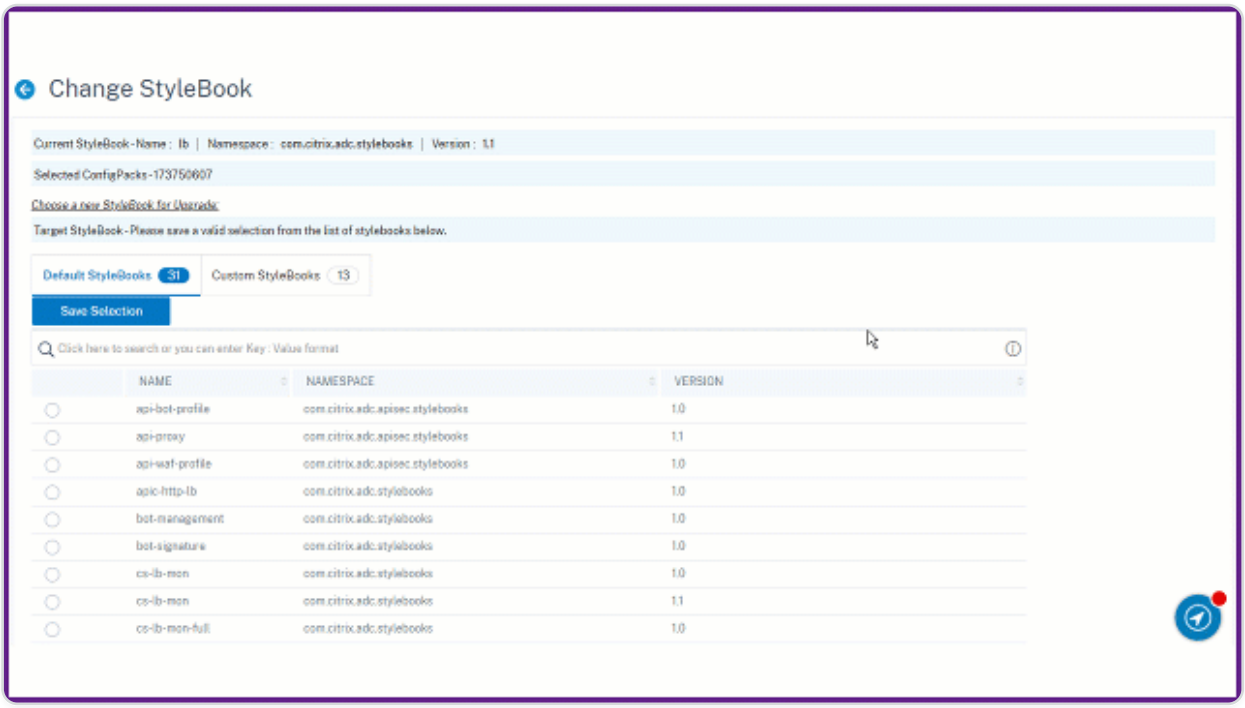
3. Click **Change StyleBook**.
4. Select the required StyleBook from the list. Then, click **Save Selection**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Change**.

   In this example, select **example-lb-mon** from the list.

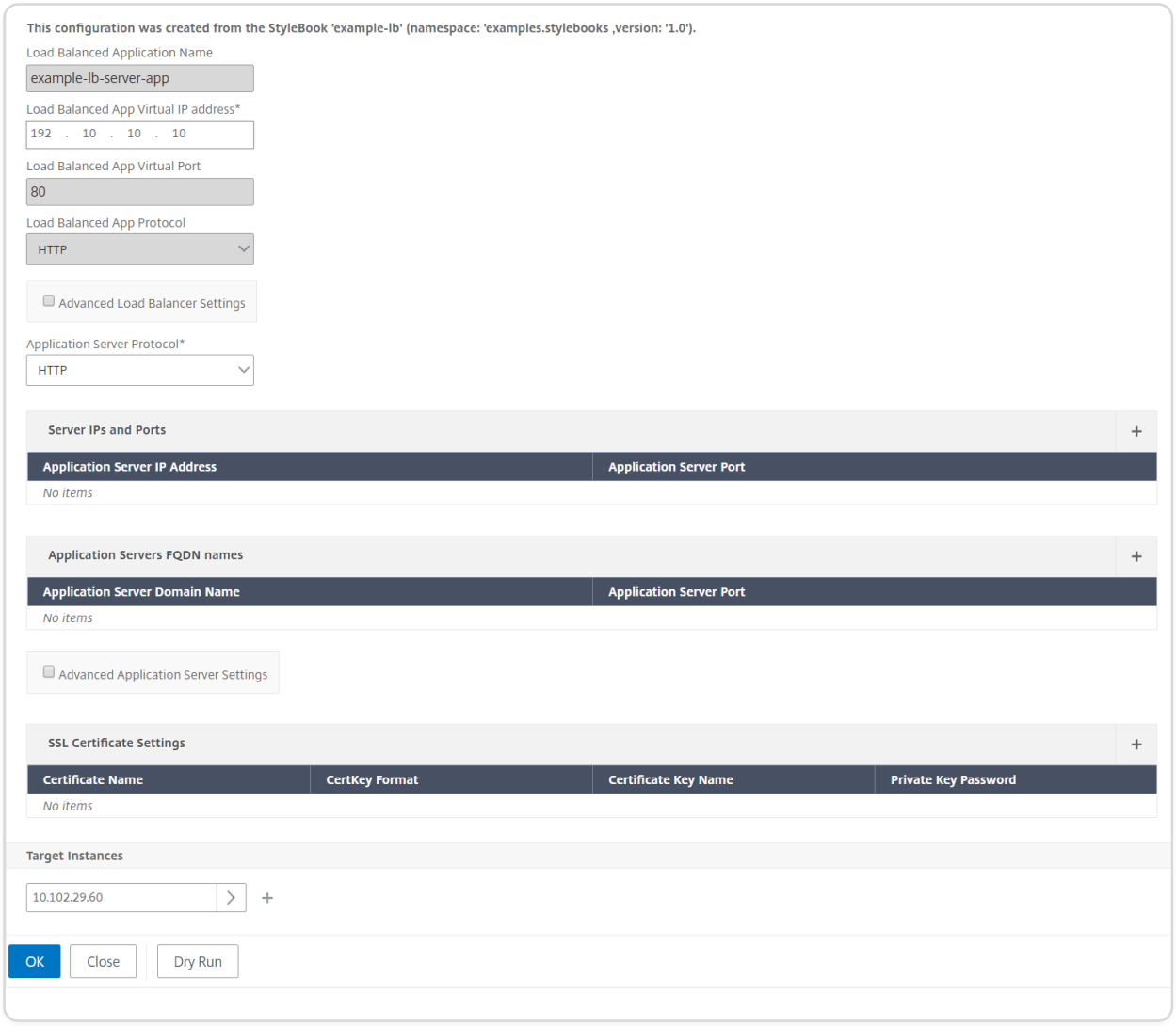
   When you change the StyleBook of a configuration pack, the parameters in the new StyleBook might have a different structure than the existing StyleBook. If the parameter structure is similar to the previous StyleBook, the parameters' values are automatically retained in their respective fields. Otherwise, only parameters that have the same structure between the two StyleBooks are transferred. For example, the same parameter name, type, parameter parent, and more.



   If new required parameters are added in the new StyleBook, after changing the StyleBook, you have to manually specify the values for such parameters.

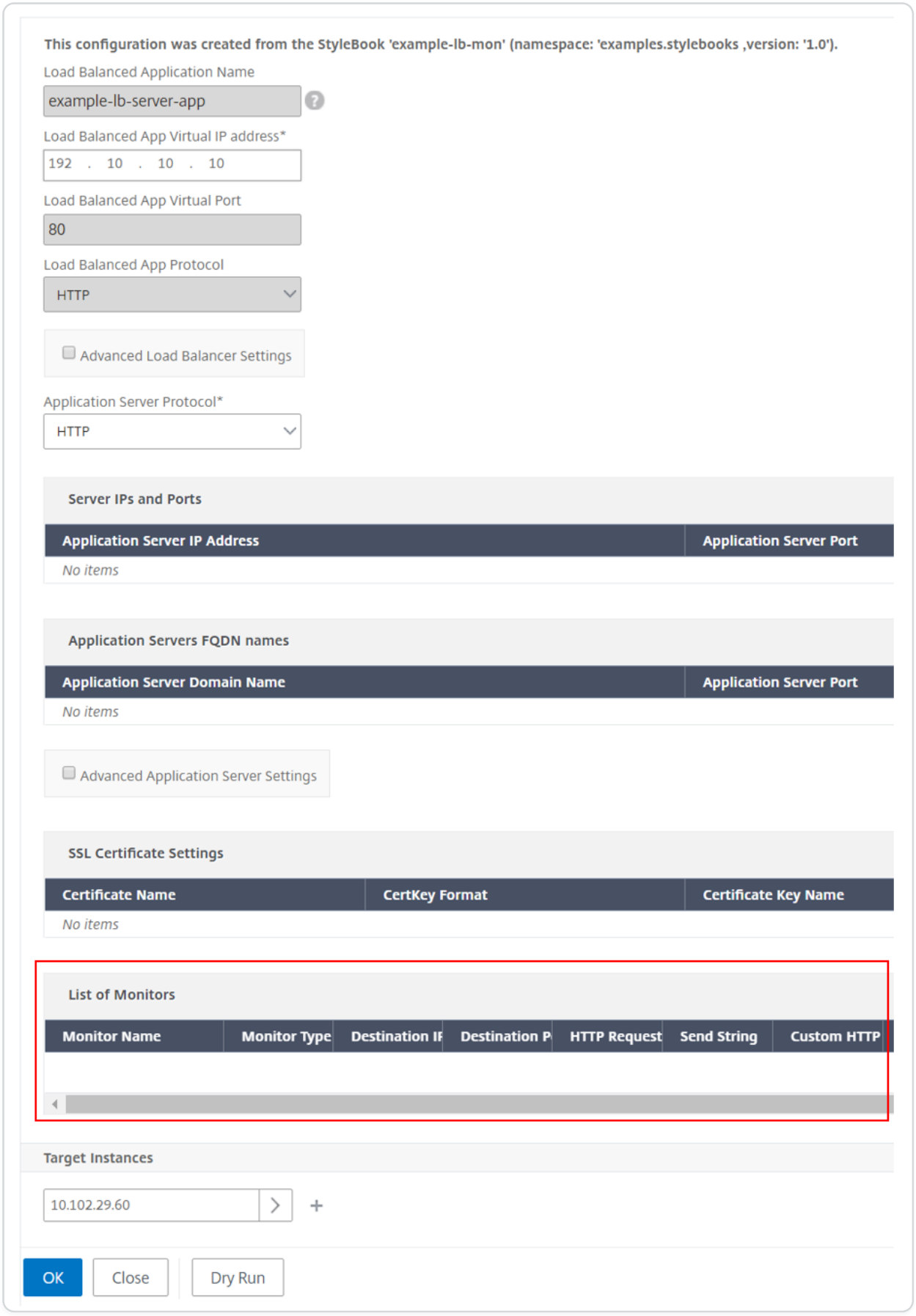
   In this example, the parameters that appear on the configuration page for the **example-lb** StyleBook are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The parameters that appear on the configuration page for the new **example-lb-mon** StyleBook are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this case, the StyleBooks retain the older values for the basic load balancer configuration because the new StyleBook hasn't changed existing parameters. And, it adds only the new parameters. For monitor parameters, manually specify the required values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In **Target Instances**, review the selected instances and update the list if necessary.
7. Click **Dry Run**.

   The **Objects** page displays the objects that get created, modified, or removed from the NetScaler instances.
8. Click **OK**.

   In the **StyleBook > Configurations** page, the **StyleBook Name** column displays the new StyleBook name for the selected configuration pack. In this case, it displays **example-lb-mon**.

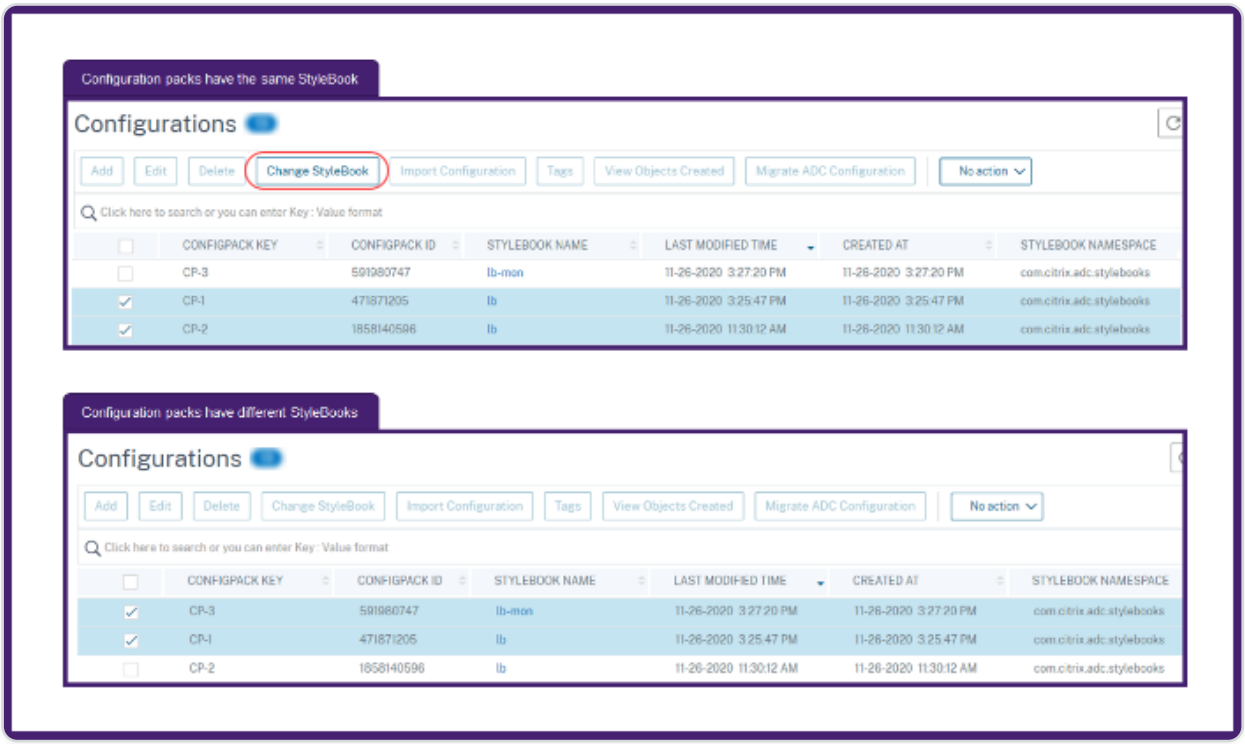
Change the StyleBook that has multiple configuration packs

When you change an existing StyleBook that has multiple configuration packs, do the following:

1. Import a new StyleBook to ADM.

   Typically, the new StyleBook has the same name and namespace with a higher version than the existing StyleBook. However, you can skip this step if the name, namespace, or version are different.
2. Change the StyleBook for the configuration packs that are associated with the existing StyleBook.

   You can select **Change StyleBook** only when the selected configuration packs are associated with the same StyleBook.

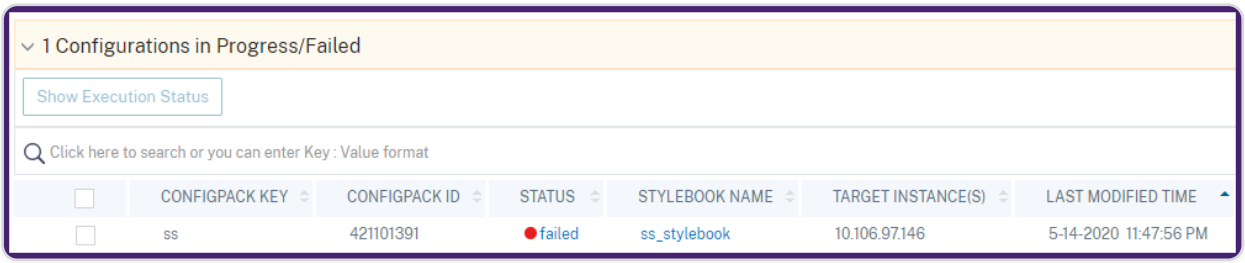


© 1997–2026 Citrix Systems, Inc. All rights reserved.

For the selected configuration packs, the ADM successfully changes the StyleBook when the following conditions are met:

- All the configuration parameters of the existing StyleBook must present in the selected StyleBook.
- The new parameters from the selected StyleBook are optional.

To see the progress of the selected configuration packs, select **Configurations in Progress/ Failed** in the **Configurations** page.



3. Remove the old StyleBook from ADM once all configuration packs are tied to the new StyleBook.

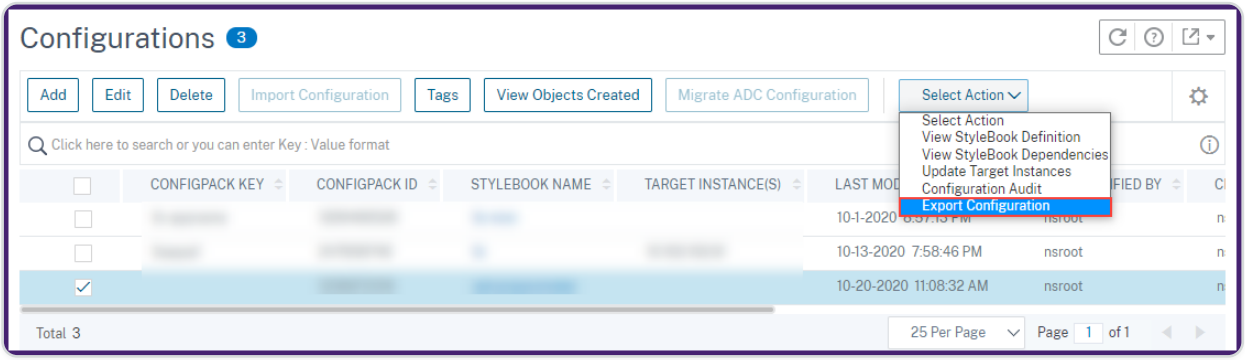
Export or import configuration packs

You can export or import a configuration pack like StyleBooks. With this feature, you can readily share the StyleBook configuration to another ADM server. When you export a configuration pack, a `tgz` or `zip` bundle downloads to your local computer. This bundle includes a JSON file with all the parameters defined in a configuration pack.

Export configuration

Do the following to export a configuration pack:

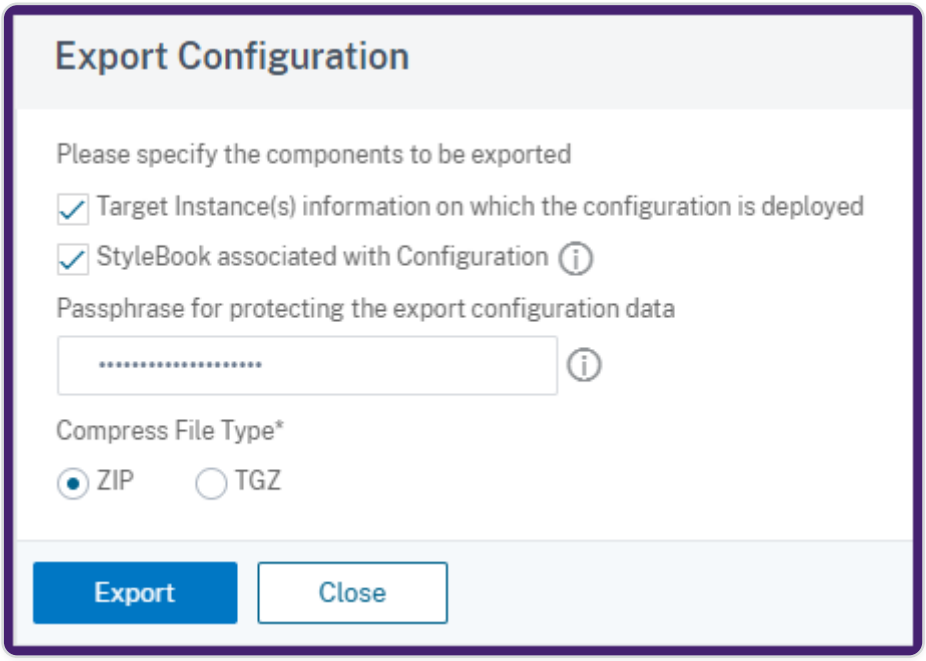
1. Navigate to **Applications > StyleBooks > Configurations**.
2. Select a configuration pack that you want to export.
3. In **Select Action**, select **Export Configuration**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the **Export Configuration** pane, specify the following:

   - **Target instance(s) information on which the configuration is deployed**: Select this option to include target instances' information with the export bundle.
   - **StyleBook associated with Configuration**: Select this option to include the StyleBook in the export bundle.
   - **Passphrase for protecting the export configuration data**: Specify a passphrase to encrypt the export bundle. This passphrase secures the sensitive data of a configuration pack.
   - **Compress file type**: Select either **ZIP** or **TGZ** file type.



5. Click **Export**.

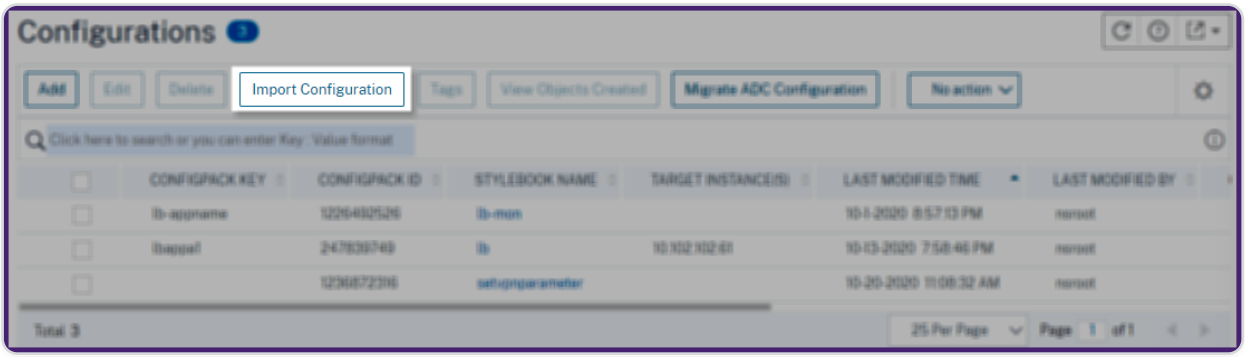
   Save the export bundle on your local computer.

Import configuration

You can import a configuration pack from your local computer to a different ADM server. To import a configuration pack, do the following:

1. Navigate to **Applications > StyleBooks > Configurations**.
2. Select **Import Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Choose the import file bundle from your computer.
4. Use the passphrase that you have specified during export.
5. Optional, in Advanced Options, select **Only allow creation of new configuration if all config objects already exist on ADC**.

   This option does not alter the objects that are already created on the ADC instance.

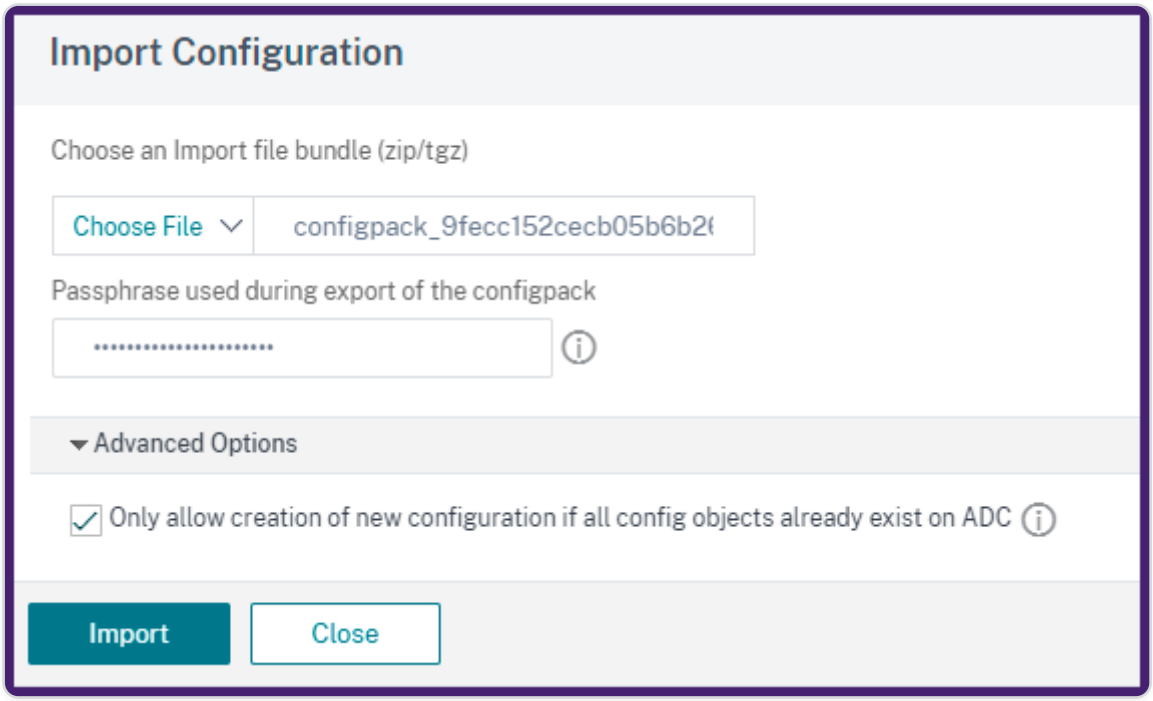
   Consider that you added the same ADC instance in two ADM servers. And, you want to migrate a configuration pack from one ADM server to another server. Use this option to import a configuration pack without altering its configuration objects on an ADC instance.

   IMPORTANT

   To use this option, ensure that the specified configuration bundle has the target instances information. See, Export configuration.

   This option only migrates the configuration if all the objects are present on the target instance.
6. Click **Import**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When you import a configuration pack, the ADM verifies the following:

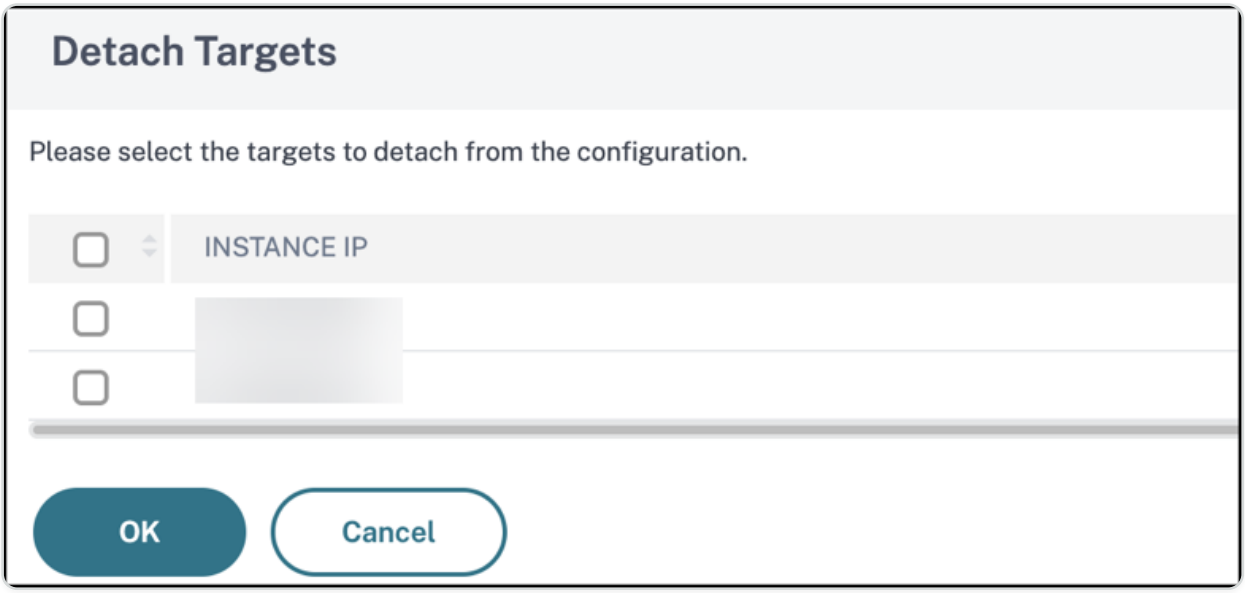
- **Associated StyleBook**: If the associated StyleBook is not in the ADM, it imports the StyleBook along with the configuration pack.
- **Target instances**: Check for target instances and deploys the configuration on the specified target instances. If the mentioned ADC instances are absent in the ADM, the configuration pack is imported without target instances.
- **Source ADM**: If you are importing a configuration pack on the same ADM server, the selected bundle updates the existing configuration pack.

Detach a target instance from a configuration pack

To detach a target instance from a configuration pack, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Select the configuration pack with a target instance that you want to remove.
3. In **Select Action**, select **Detach Targets**.
4. In the **Detach Targets** pane, select the target instance you want to remove from the configuration pack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **OK**.

A message displays, confirming the creation of a duplicate configuration pack with the target instance now removed.

Build your StyleBooks

The full content of **example-lb** StyleBook is provided for your reference as follows:

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

The full content of **example-lb-mon** StyleBook is provided for your reference as follows:

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

Create a StyleBook to upload files to NetScaler® ADM

NetScaler Application Delivery Management (NetScaler ADM) StyleBooks allow you to create NetScaler configurations that might include among other things while uploading files of any type from your local filesystem to the NetScaler instance, by using the NetScaler 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 NetScaler instance. The geo files are used typically in GSLB configurations for defining static-proximity based on the geo location:

Build your StyleBook -1

```
name: upload-geolocations

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
NetScaler

schema-version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import-stylebooks:

-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
ADM

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile

 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    filecontent: base64.encode($parameters.locationfile.contents)
```

NOTE

The parameter used in this example is of a type file. You can import this StyleBook in NetScaler ADM and use it to upload geolocation files.

This StyleBook requires the file to be already present in NetScaler ADM (for example, you would have already copied it to NetScaler ADM using a utility like scp). If you want to upload a file to NetScalers through NetScaler ADM without first copying it to the NetScaler ADM filesystem, you can build a StyleBook that has two "string" parameters, one is for specifying the file name to be used on the NetScaler 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

```
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
NetScaler

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "11.1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  prefix: ns


parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
filelocation: "/var/NetScaler/inbuilt_db/"

filecontent: base64.encode($parameters.filecontents)
```

Creating configurations to upload files

The following procedure creates a configuration on a selected NetScaler instance that would upload a geolocation file using the first StyleBook described above.

To create a configuration for uploading files:

1. In NetScaler ADM, navigate to **Applications** > **Configuration**, and click **Create New**. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler 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 NetScaler ADM the file is located under the current tenant's folder only. Use any file transfer protocol to copy the file to NetScaler ADM file system.
4. You might be asked to provide your user credentials before you access the target instances.
5. Select the target NetScaler 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 configuration pack is successful, the file is saved on the NetScaler instance file system under the location: /var/netscaler/inbuilt_db/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

Using the NetScaler ADM API to create a configuration pack

You can also use the NetScaler ADM API to create a configuration pack that uploads files to the selected NetScaler 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 NetScaler ADM

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 NetScaler ADM GUI. You can also use NetScaler ADM APIs to upload certificate files and key files that are already managed by NetScaler 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 NetScaler 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 NetScaler ADM. These are specified in the "parameters" section, as shown below:

```
parameters:

 -

  name: name

  type: string

  required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

   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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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 NetScaler 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 NetScaler 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 NetScaler 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 configuration pack.

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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 NetScaler ADM. The uploaded SSL certificate file is stored on NetScaler 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 NetScaler ADM.

Creating configurations to upload SSL files

The following procedure creates a basic load balancing virtual server configuration on a selected NetScaler 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 NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create a configuration for uploading files

1. In NetScaler ADM, navigate to **Applications** > **Configuration > StyleBooks**. The **StyleBooks** page displays all the StyleBooks that are available in your NetScaler 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 NetScaler ADM itself.
6. Select the target NetScaler instance on which the configuration needs to be created, and click **Create**.

NOTES:

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler ADM to the available list of instances in this window.

In NetScaler ADM, the following default StyleBooks, which are shipped as part of NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key
```

Using the NetScaler ADM API to create a configuration pack

You can also use the NetScaler ADM API to create a configuration pack that uploads Cert and Key files to the selected NetScaler instance. For more information on how to use APIs, see How to Use API to Create Configurations to Upload Cert and Key Files.

Viewing the objects defined on the NetScaler instance

After the StyleBook configuration pack is created on NetScaler ADM, click **View objects created** to display all the NetScaler objects created on the target NetScaler instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects

Objects Added on Instance : 10.102.29.200

Type : lbvserver

ipv46 : 10.10.10.1
lbmethod : ROUNDROBIN
name : vserver-1
port : 80
servicetype : SSL

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMzakNDQWtlZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREEvTVFzd0NRWURWUVFHRXdKVlV6RUwKTUFrR0ExVUVDQk1D
WTJFeEV6QVJCZ05WQkFjVENuTmhiblJoWTJ4aGNtRXhEakFNQmdOVkJBb1RCV0Z3Y0d4bApNQjRYRFRFMU1ERXhOekEyTURZMU5Gb1hEVEUyTURFeE56QTJNRFkxTkZvd1B6RUxNQ
WtHQTFVRUJoTUNWVk14CkN6QUpCZ05WQkFnVEFtTmhNUk13RVFZRFZRUUhFd3B6WVc1MFlXTnNZWEpoTVE0d0RBWURWUVFLRXdWaGNIQnMKWlRDQm56QU5CZ2txaGtpRzl
3MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXZFa2FoNjJFRnViTmVGUkNaQk9nN0pEZAo0dVQ1ZDBlM3UycUtaMTQrdzRjVkd5U053L1RxT2RhK1F3T0xiaU9OdDBhLzhKRDVyc096Q3N
CWHRldUsyZzRPCnhuNi8wc28zZFJKZTVKeFErNmNsT2VsVjdPbUpFTWVXZDd5WlJGbVFqZHgrZEROMjUxT25aa0pmeXN3NXdSVTUKSnpUQnRza3hRcjBQbnJ2S0tBa0NBd0VBQWFP
QjZUQ0I1akFkQmdOVkhRNEVGZ1FVam5XYVJsalF5N0pqNFozcwp0LzFIWmYvWUprZ3dad1lEVlIwakJHQXdYb0FVam5XYVJsalF5N0pqNFozc3QvMUhaZi9ZSmtpaFE2UkJNRDh4CkN6
QUpCZ05WQkFZVEFsVlRNUXN3Q1FZRFZRUUlFd0pqWVRFVE1CRUdBMVVFQnhNS2MyRnVkR0ZqYkdGeVlURU8KTUF3R0ExVUVDaE1GWVhCd2JHV0NBUUF3REFZRFZSMFRCQVV3
QXdFQi96QUxCZ05WSFE4RUJBTUNBUVl3RVFZSgpZSVpJQVliNFFnRUJCQVFEQWdFR01DNEdDV0NHU0FHRytFSUJEUVFoRmg5T1pYUlRZMkZzWlhJZ1IyVnVaWEpoCmRHVmtjRU5sY2
5ScFptbGpZWFjsTUEwR0NTcUdTSWIzRFFFQkN3VUFBNEdCQUs0RWY3aUFSRlRQUlo0b2pJWm0KTHlTeFhGaTE0SGxjK0VpMUNJejV3R09Db3pibWNXemZOZXVSSTdRQVlSSXQ3Wkh
hYWt0VGg0NXIvUHdPZXFLcgpSc2xNTzBnQ1hES3BtU2tXQ3VHdFhBbVhXU2xrTEt3bTFHL0pKdTBhSEFkdVhtRVkwNW52M016RWhTWW8xelhjCnFsYXJNcG9QUE14Qks0RmlBNWxs
QnAwTwotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : test_cert.pem

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlDWEFJQkFBS0JnUUM4U1JxSHJZUVc1czE0VkVKa0U2RHNrTjNpNVBsM1I3ZTdhb3BuWGo3RGdoVWJKSTNECjlPbzUxcjVEQTR0
dUk0MjNSci93a1BtdXc3TUt3RmUxNjRyYURnN0dmci9TeWpkMUVsN2tuRkQ3cHlVNTZWWHMKNllrUXg1WjN2SmxFV1pDTjNINTBNM2JuVTZkbVFsL0t6RG5CRlRrbk5NRzJ5VEZDdlEr
ZXU4b29DUUlEQVFBQgpBb0dBUUlENjZjaDBIRFJ0NSs5VjMxc3FJbUZ1NHJCM0Zub25ZN21ZT05sOHZ4WHRqU0wwdmxGRmZSTW9rMlMvCmU3Z0tjT040Rmo1VWk1N1gwN01aV1
dXY1o0aEhrMm5jMjlmOENLSW5oelhnYjFLQjRaMGp1TnUvNE1paVIyaHIKNkFROXluV0VMRlBDTjZWMHFQZWxGYXpVbnZJaHZpMFZGZCsyRUNBY0drVHg0Z0VDUVFEMklVODhGaU
kzVFJOYwpMcVJEMHh2ZVFWMkF6ZVBEYmFnTVFFRlNWZVZ3Yk11V3RJM2J0SkdwWXMxUkpIeitOdGw0dVprRGVQbnNJZE5ZCjNJWjNsNUp4QWtFQXc5WDdKTDJaNVpyaEVpM0Yzdj
YwU1U5RWM4Z01FdVhFZlhUendCc2puanJsckRIMUI0enYKR0hSU1lmUEdYeHh5cjRKVmc4Q25kczZVOHExN0N0SUxHUUpBS1FtT3UzYjVSMzByWURCS3BTQmF3aWpsM1NiMgo5Y3
VmdkVNdVlQci9ZVXBTZTVNcEg5dXdlYXlHalNQblR6OTM3UUFNK2g0K2xWZGlkS3Q0SkJKNmtRSkJBTHVSClRaUHBEV2UrcWVleGM1MmJzcTJzZ0ZHc3Z2T3lvam5QTkU5Qkx5STBJeH
FFVnIyK25KcDImeEpXWEI5b3JlZXcKRzV1dmdEWG9zdnlrYi83eklyRUNRRDMzV1lHeUw2MjJaRzZveHlxR1o1d1pCTFVtV1VyVE1zSngzOWZ5NUJoZgpkajNWcE10Y3plOFVKVmlPaGtyd
WNmb29tRlNPaUN4ZXhPQXM2MmVEZXNnPQotLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : test_cert_key.pem

Type : sslcertkey

cert : test_cert.pem
certkey : vserver-1-lb-cert
inform : PEM
key : test_cert_key.pem

Type : sslvserver_sslcertkey_binding

certkeyname : vserver-1-lb-cert
vservername : vserver-1

Enable analytics and configure alarms on a virtual server defined in a StyleBook

You can use the operations construct to configure NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -

      metric: "total_bytes"

      operator: "lessthan"

      value: 60

      period-unit: "day"
```

The attributes in the analytics section are used to instruct NetScaler 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 NetScaler policy expression to filter requests for which appflow records are collected on the virtual server.

When a configuration pack is created from this StyleBook, the NetScaler 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 configuration pack.

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 NetScaler ADM analytics GUI.

To learn how to view and analyze data collected on virtual servers that were created as part of a configuration pack, see the NetScaler ADM analytics documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance roles

In NetScaler Application Delivery Management (ADM), there might be a scenario where you have to configure multiple NetScaler 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 configuration pack and apply the same configuration on multiple NetScaler 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 configuration pack 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 configuration pack, each ADC instance in a configuration pack can be assigned a different role. This role determines the configuration objects of the configuration pack 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 configuration pack.

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.

```
target-roles:



  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: A

  name: B

    min-targets: 2

    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 configuration pack from this StyleBook, and max-targets specify the maximum number of ADC instances that can be assigned this role when creating a configuration pack 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 configuration pack, 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:

```
-

  name: C1

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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 NetScaler instances regardless of their role. You can use this feature effectively to create configuration objects that can be applied to all instances of a configuration pack.

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:

```
components:

  -

    name: C1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      name: lb3

      servicetype: HTTP

      ipv46: 13.13.13.13

      port: 80

  -

    name: C4

    type: ns::lbvserver

    roles:

      - default

    properties:

      name: lb4

      servicetype: HTTP

      ipv46: 14.14.14.14

      port: 80
```

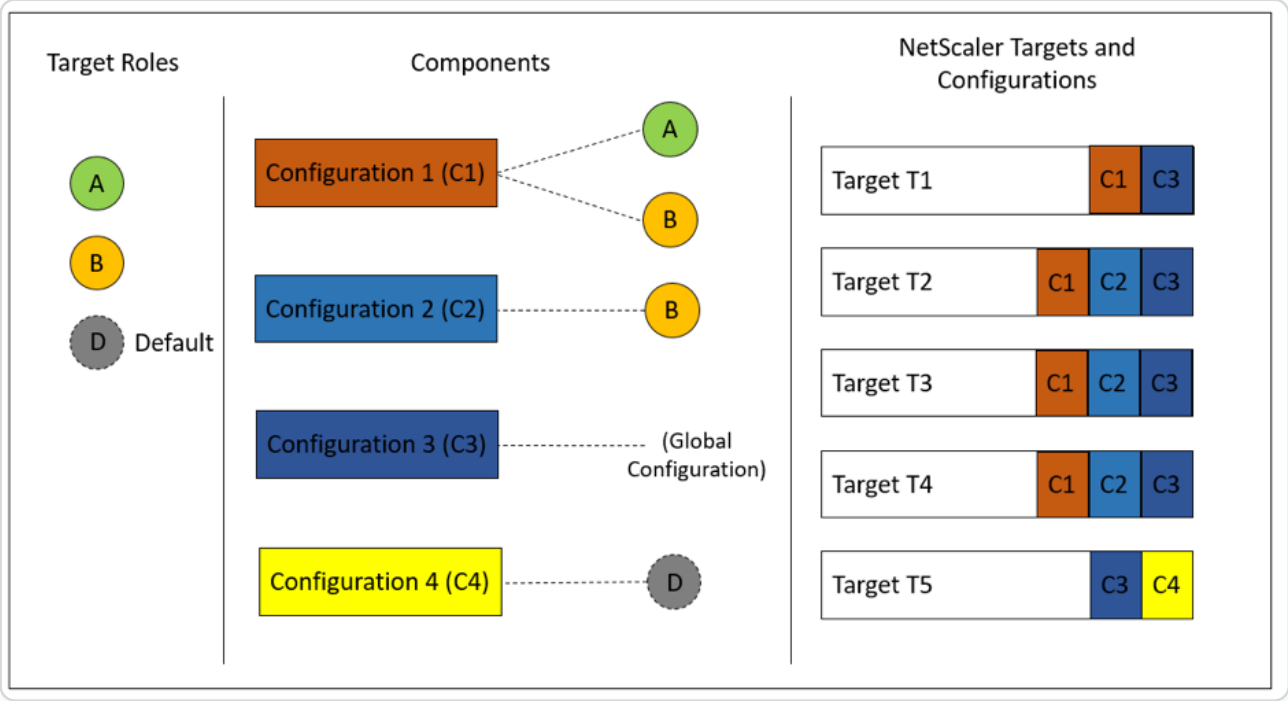
Note that the component C3 doesn't have a role defined, which means the component is deployed on all instances regardless of their role. On the other hand, component C4 has the role "default", which means it is applied to any instance that doesn't have an explicit role assigned to it.

Now, consider that you want to create a configuration pack 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

You can also use the “Dry Run” feature when creating a configuration pack 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:

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"

schema-version: "1.0"

import-stylebooks:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      - 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
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```

The following image shows the objects created for a sample configuration pack:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects created (9)

Instance : 10.102.102.136 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.135 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.62 | Roles : A, default | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 14.14.14.14
name : lb4
port : 80
servicetype : HTTP

Using APIs

When using the REST API, you can specify roles for each ADC instance when creating or updating the configuration pack as follows. In the “targets” block, specify the UUID of the specific NetScaler instance on which you want to deploy the individual components.

```
"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

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        {
          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a StyleBook to perform non-CRUD operations

StyleBooks manage NetScaler configurations by computing the necessary configuration objects on the NetScaler 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 NetScaler configuration objects support a few operations other than create, update or delete (CRUD operations). For example, a load balancer object (lbvserver) or a NetScaler feature object (nsfeature) can support the "enable" or "disable" operation. Similarly, NetScaler certkeys support the "link" and "unlink" operation to link or unlink a certificate to another certificate. These operations on NetScaler 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 NetScaler 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.

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  meta-properties

   action: enable

  properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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.

Migrate configuration pack of a StyleBook to another StyleBook

In NetScaler® Application Delivery Management (ADM), configuration packs are always bound to the StyleBook from which they are created. Any update to the configuration pack can be done only through the StyleBook that the configuration pack is bound to. NetScaler ADM now allows you to migrate an existing configuration pack to a new StyleBook. The new StyleBook can be a more original version of the current StyleBook that is bound to the configuration pack. Or, you can also migrate the configuration pack to an entirely different StyleBook.

For example, you created a StyleBook called **example-lb**. This StyleBook is used to deploy a basic load balancer configuration on a NetScaler instance. You created a configuration pack CP1 from this StyleBook on a NetScaler instance. Later, you realized that your StyleBook does not include a monitoring configuration. So, you now created a StyleBook called **example-lb-mon**. This

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook has the same load balancer configuration as example-lb StyleBook but adds the ability to configure monitors.

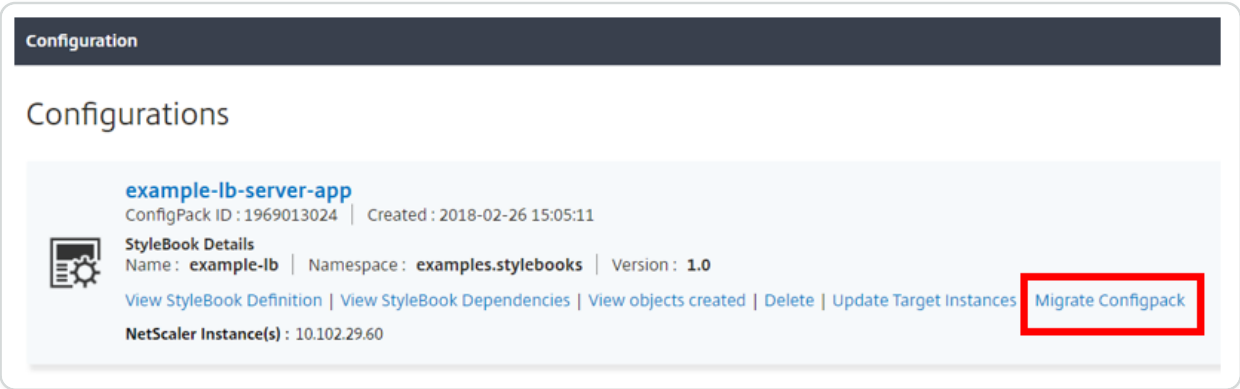
Now you want to update your existing configuration that was created in configuration pack CP1 to add some monitors. Previously, you had to delete the configuration pack CP1 and create a configuration pack CP2 from the new StyleBook to add monitors to your configuration. Deleting CP1 results in the removal of all the configuration created in configuration pack CP1 on one or more NetScaler instances. Earlier, you had to recreate a new configuration pack through the new StyleBook by typing values for all parameters.

Instead, you can now migrate the existing configuration pack CP1 to the new example-lb-mon StyleBook. Your new StyleBook can configure monitors monitor details. Only those monitor-related configuration objects are added to the NetScaler instances where the configuration pack was deployed. You have to provide just the monitor details now. The existing configuration deployed on the NetScaler instances that has not changed remains unaffected.

Migrate configuration pack

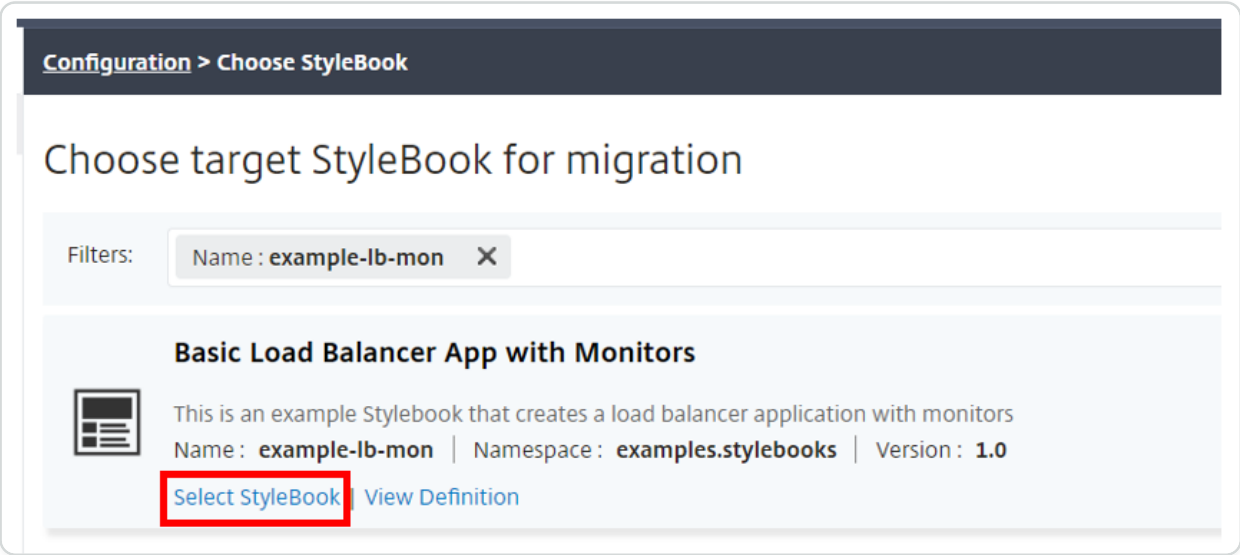
To migrate a configuration pack created using example-lb StyleBook to example-lb-mon StyleBook

1. In NetScaler ADM, navigate to **Applications** \> **Configurations**. The **Configurations** page displays all the configuration packs that are present in the system.
2. Scroll down to find the **example-lb** configuration pack that you would have created earlier, and click **Migrate Configpack**.



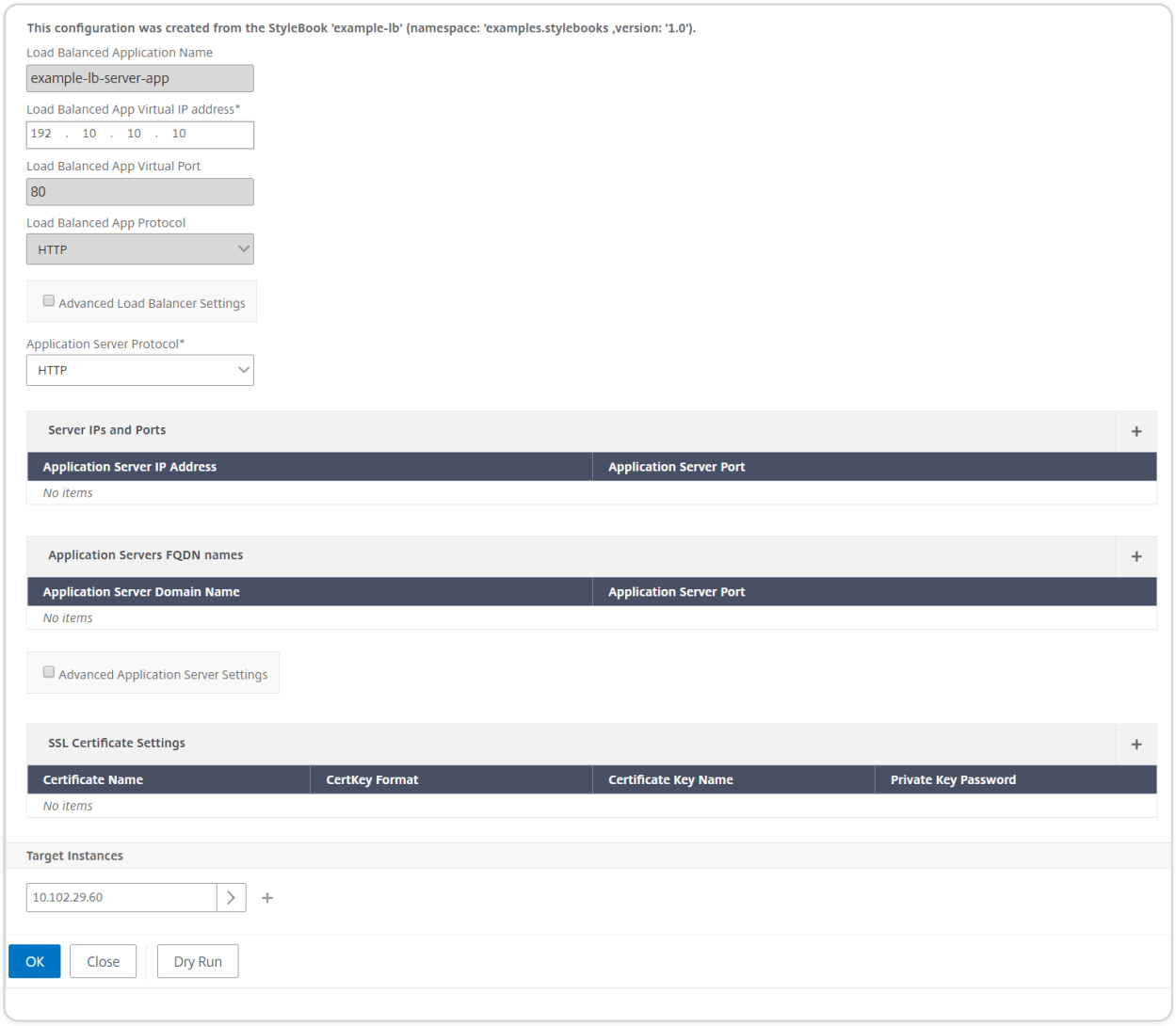
3. The **Choose target StyleBook for migration** page opens that lists all StyleBooks that available in NetScaler ADM. Scroll down to find the **example-lb-mon** StyleBook and click **Select StyleBook**. You can also search for the StyleBook by typing example-lb-mon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



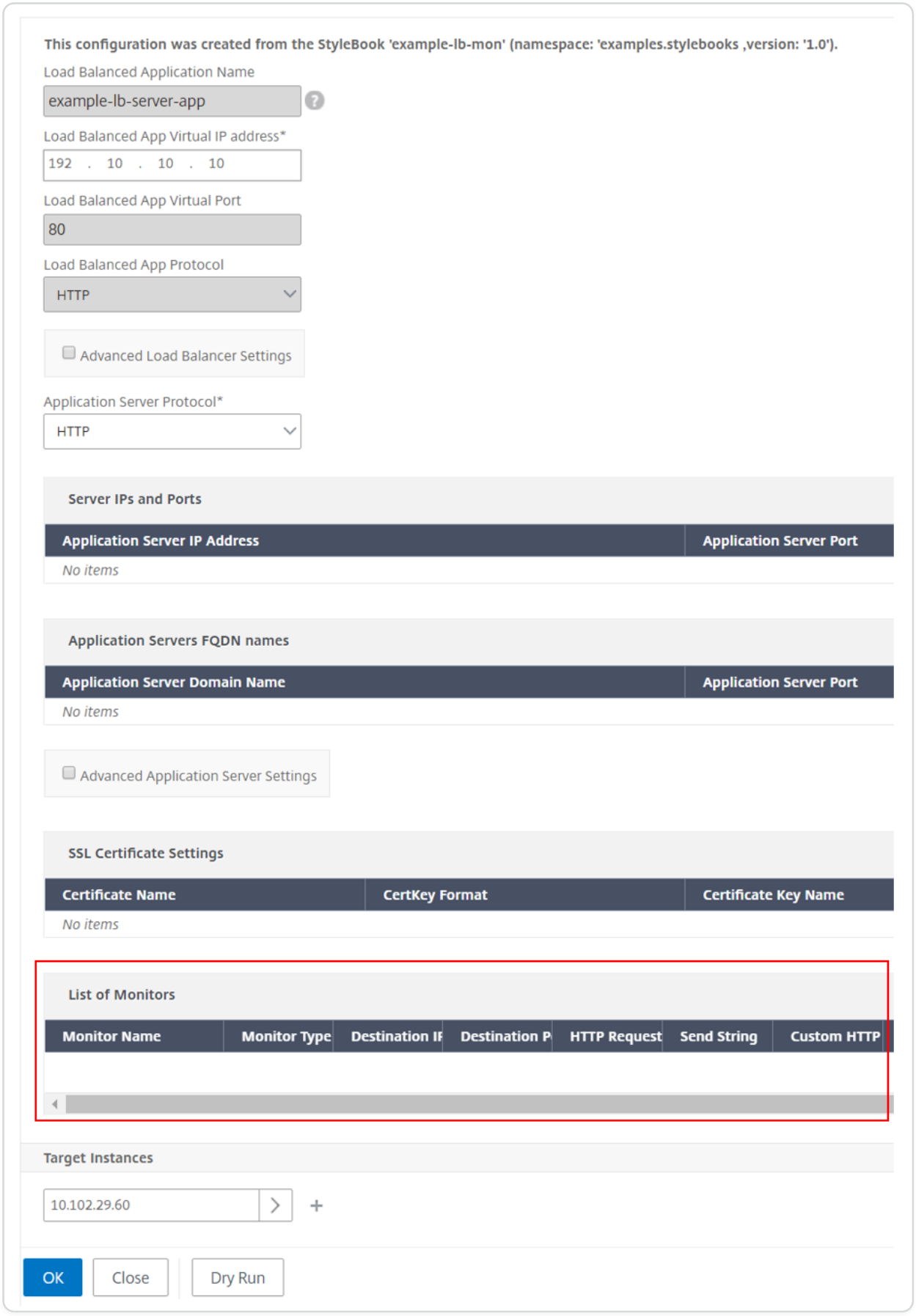
If you migrate from one StyleBook to another, all parameters in the two StyleBooks might not have the same structure. If the parameter structure is similar, the previous values are automatically retained in the parameter fields. A few of the parameters in the new StyleBook may be new, or there might be a change in their structure. In such a case, you must manually fill in in the values for the StyleBook parameters. For example, the following image shows the parameters of the example-lb StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following image shows the parameters after migrating the configuration pack to example-lb-mon StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this case, you can see that the StyleBooks retain the older values for the basic load balancer configuration. But, you must manually type the values for the monitor parameters.

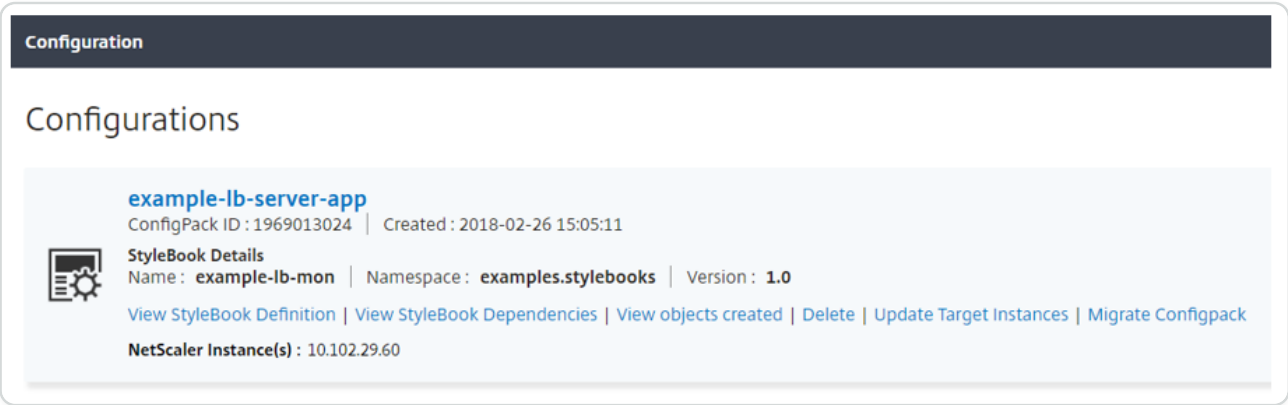
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Type in values for the new parameters used for creating monitors on the instance.
5. Under **Target Instances**, click and select the IP address of the NetScaler instance where you want to run the configuration. Note that you can deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.
6. Click **Dry Run**. The **Objects** page displays the objects that would be newly created, modified, or removed from the NetScaler instance(s).
7. Click **Create** to create or update the configuration of the selected instances. The configuration pack is created if the target instances are new. Else, the existing configurations deployed on the instances are updated.

> **NOTE**
>
> You can also click the refresh icon to add recently discovered NetScaler instances. So these instances are instantly available in the list of instances in this window. The refresh icon is currently available only on NetScaler ADM.

You can also migrate a configuration pack from one version of a StyleBook to the next version. Here also you might have to type the values of any new required parameters present in the new version. You can also migrate the configuration pack to an older version of the StyleBook. In this case, the extra parameters that are not present in the older StyleBook are removed. The **Objects** page displays any of the objects that are removed from the configuration.

After a successful migration, the ConfigPack is bound to the new StyleBook.



You can see that the name of the configuration pack and the configuration pack ID are same as earlier. But NetScaler ADM updates the StyleBook name to example-lb-mon from example-lb.

Build your StyleBooks

The full content of **example-lb** StyleBook is provided below for your reference:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

The full content of **example-lb-mon** StyleBook is provided below for your reference:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]

substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

Use API to create configurations from StyleBooks

After you have built your StyleBook, you have to import it to NetScaler® Application Delivery Management (ADM) to use it either by using the NetScaler ADM or by using NetScaler ADM APIs. NetScaler ADM validates your StyleBook when you import it, and if the validation is successful, your StyleBook appears on the NetScaler ADM catalog of StyleBooks, ready to be used for creating configurations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler 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 configuration pack from this StyleBook as follows:

```
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":

    [

      {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "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 NetScaler instance on which the load balancing virtual server lb1 with IP address 10.102.117.31 is created. The instance ID of the NetScaler instance is retrieved from NetScaler ADM.

To obtain the ID of an instance managed by NetScaler ADM, you can use NetScaler ADM APIs. For example, to retrieve the instance ID os a NetScaler instance whose IP address is 192.168.153.160, you can use the following API:

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address:192.168.153.160
```

```
Accept: application/json
```

The response contains the ID in the payload:

```
200

OK

Content-Type: application/json

{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "ns",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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 pack is successfully created, you receive the following HTTP response:

```
200 OK

Content-Type: application/json

{

  "configpack":

  {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "config_id": "1460806080"

  }

}
```

You have created your first configuration pack 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 pack and execute it on the same or different NetScaler 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 NetScaler instances.

The HTTP request is as follows:

```
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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "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 NetScaler instances represented by the ids "deecee30-f478-4446-9741-a85041903410" and "debecc60-d589-4557-8632-a74032802412".

On successful creation of the configuration pack, the following HTTP response is received:

```
200 OK

Content-Type: application/json

{

   "configpack":

  {

     "config_id": "1657696292"

  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

This new configuration pack has a different id 165769629. 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 configuration pack 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":

    {

      "name": "myapp",

      "ip": "10.70.122.25",

      "svc-servers":

      ["192.168.100.11","192.168.100.12"],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "svc-port": 8080

      },

      "target_devices":

      [

       {

        "id": "deecee30-f478-4446-9741-a85041903410"

       },

       {

        "id": "debecc60-d589-4557-8632-a74032802412"

       }

      ]

    }

  }
```

In this HTTP request, the load balancing configuration is executed on two NetScaler instances. You can log on to these NetScaler 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 configuration pack from this StyleBook as follows:

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/composite-example/configpacks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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"]

    },

    "target_devices":

    [

    {

      "id": "deecee30-f478-4446-9741-a85041903410"

    },

    {

      "id": "debecc60-d589-4557-8632-a74032802412"

    }

    ]

 }

}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this HTTP request, the configuration is created on two NetScaler instances represented by their IDs. If you log on to the NetScaler 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 configuration pack, 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 configuration pack as follows:

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
Content-Type: application/json

Accept: application/json

{

  "configpack": {

    "parameters": {

      "name": "myapp",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]

  },

  "target_devices":

  [

    {

    "id": "deecee30-f478-4446-9741-a85041903410"

    },

  {

    "id": "debecc60-d589-4557-8632-a74032802412"

  }

]

}

}
```

On successful update of the configuration pack, the following HTTP response is received:

```
200 OK

Content-Type: application/json

{

   "configpack": {

     "config-id": "4917276817"

  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Deleting a configuration

To delete this configuration (from all the NetScaler instances), you can use the API for deleting a configuration pack as follows:

```
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 configuration pack, the following HTTP response is received:

```
200 OK

Content-Type: application/json

{

   "configpack": {

     "config_id": "4917276817"

  }

}
```

You can log on to the NetScaler instance and verify that all the configuration objects that are part of this configuration pack have been removed.

If you want to remove the configuration from specific NetScaler instances instead of from all, use the update configuration pack operation described above and change the "target_devices" attribute in the JSON payload to remove the specific NetScaler instance IDs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use API to create configurations to upload certificate and key files

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 NetScaler® 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 NetScaler Console. Use REST API to create a configuration pack 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/jsonAccept: 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"        }

      ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "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
            }
        }
    ],
            "lb-advanced": {
                "flush-on-state-down": "ENABLED",
                "auth-params": {
                    "authentication": "OFF",
                    "authentication-http-401": "OFF"
        },
                "appflow-log": "ENABLED",
                "algorithm": "LEASTCONNECTION"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
           "svcg-advanced": {
               "svc-client-ip": "DISABLED",
               "svc-use-source-ip": "NO",
               "svc-use-proxy-port": "NO",
               "svc-surge-protection": "OFF",
               "svc-client-keepalive": "NO",
               "svc-tcp-buffering": "NO",
               "svc-compression": "NO",
               "svc-state": "ENABLED",
               "svc-downstate-flush": "DISABLED",
               "svc-enable-health-monitor": "NO"
      }
    },
       "targets": [
           {
               "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
      }
    ]
  }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

This configuration pack 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 configuration pack, the certificate and key files are uploaded to NetScaler ADM file system.

Use API to create configurations to upload any file type

You can also use the NetScaler Application Delivery Management (ADM) API to create a configuration pack that uploads files to the selected NetScaler instance.

Consider the StyleBook example you created to upload files of any type in How to Create a StyleBook to Upload Files to NetScaler MA Service. As in the example in the above topic, create a configuration pack and specify the value of the parameter "locationfile" as the file path of the location file on NetScaler ADM. Use REST API to create a configuration pack from this StyleBook as follows:

```
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": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        {

           "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"

      }

    ]

  }

}
```

Use API to import custom StyleBooks

You can now use the StyleBook APIs to import custom StyleBooks into NetScaler Application Delivery Management (ADM). Use REST API to create a configuration pack 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 NetScaler instance.

```
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>",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "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 NetScaler® ADM.

```
200 OK
```

Response Body:

```
{



  "stylebook":

{



    "name": "example-lb",



    "namespace": "com.example.stylebook",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "version": "1.0"



  }



}
```

Use API to download custom StyleBooks

You can download a custom StyleBook by providing the following StyleBooks REST API:

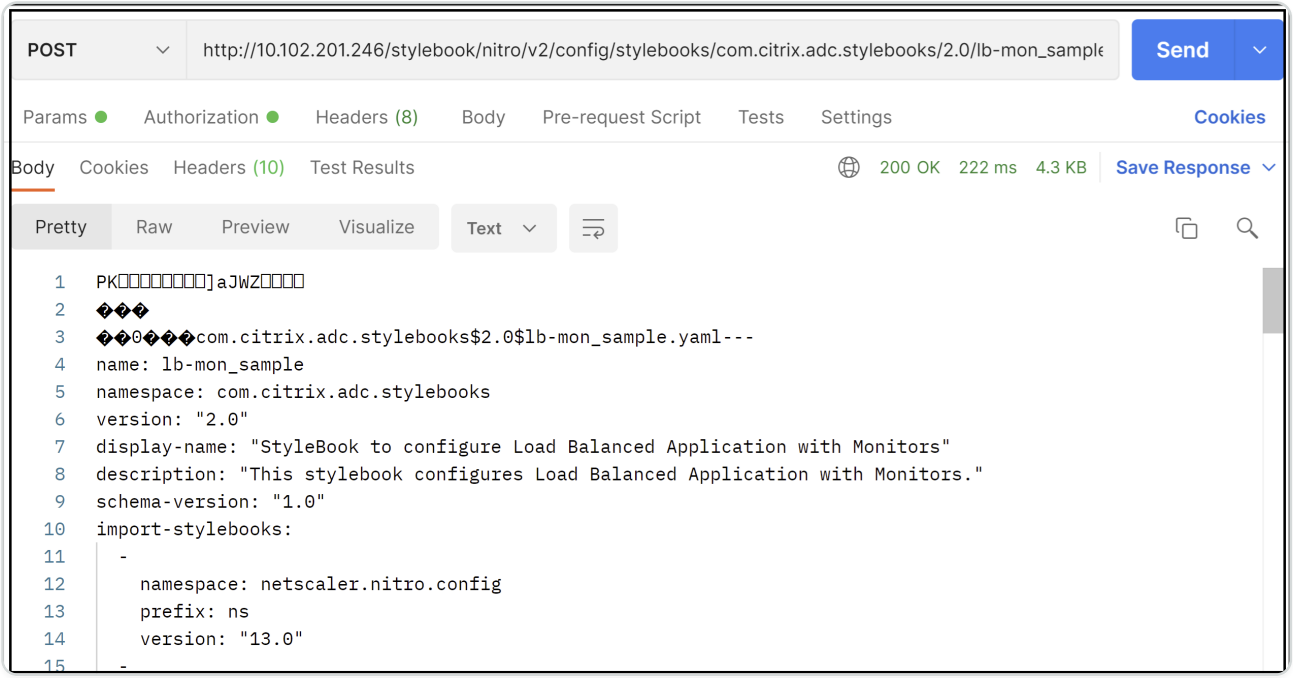
```
GET



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use API to delete custom StyleBooks

You can delete the custom StyleBook by providing the following StyleBooks REST API:

```
DELETE



https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>?dependencies=true
```

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).

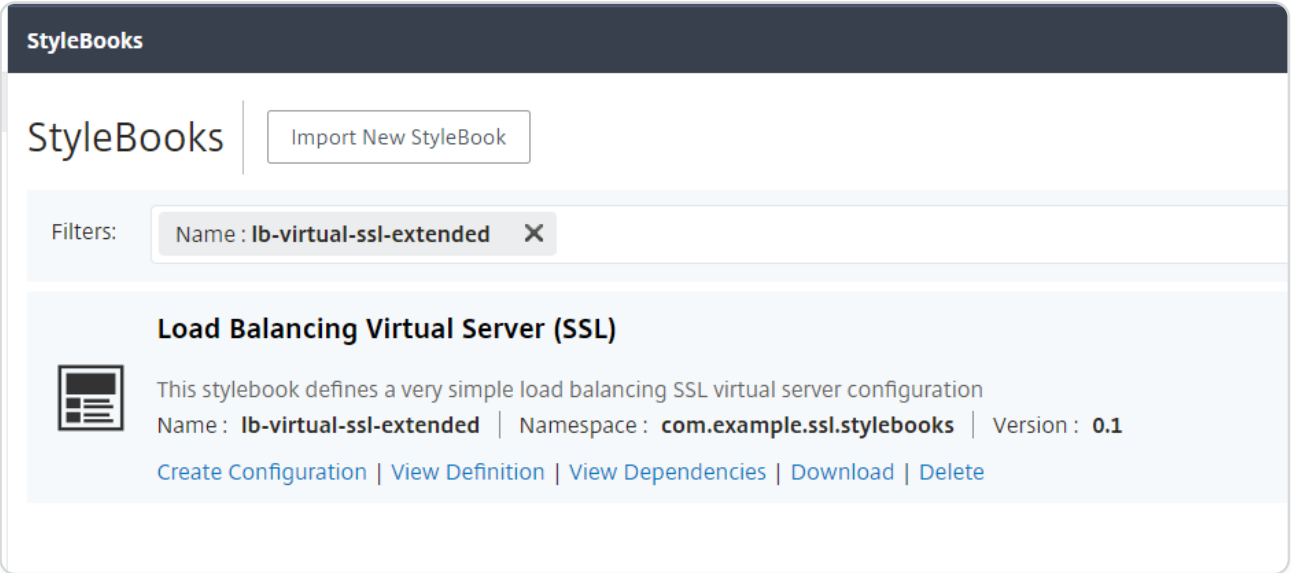
When you receive an HTTP response status code of 200, that means the custom StyleBook (and its dependencies) is successfully removed from NetScaler® ADM.

NOTE

You cannot delete a custom StyleBook that has other StyleBooks in MA Service that depend on it.

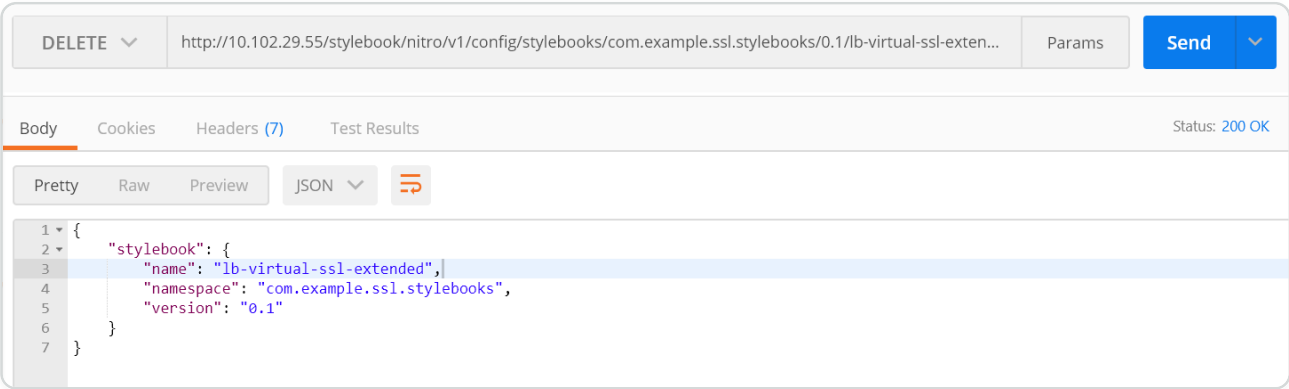
For example, assume that you had created a StyleBook named "lb-virtual-ssl-extended" in NetScaler ADM. You later decided to delete that StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

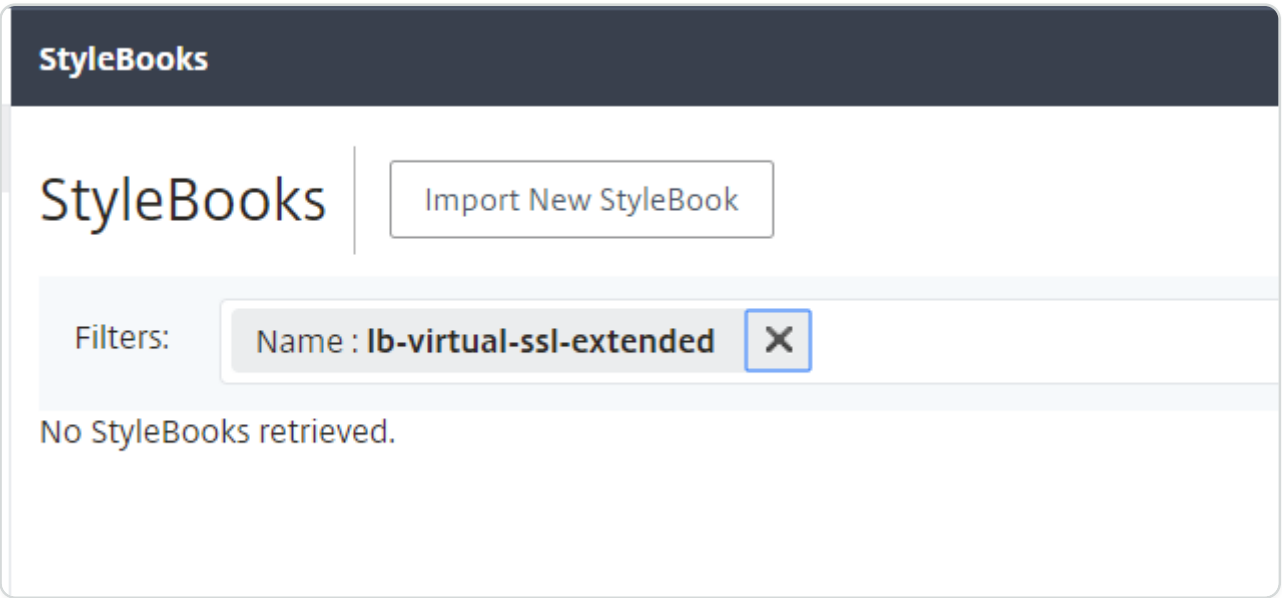


You can run the API in any tool such as the curl command line tool or the Postman chrome browser extension after making modifications to the IP address, name, version, and namespace fields.

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 NetScaler ADM.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks grammar

You can design your own StyleBooks, import them to NetScaler® Application Delivery Management (ADM), and then use them to create configurations either by using NetScaler 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.

Header	Import StyleBooks
Parameters	Parameters-default-sources construct
Substitutions	Components
Optional properties	Helper components
Properties default sources	Nested components
Condition construct	Repeat construct
Repeat-condition construct	Outputs
Nested repeats	Parent reference
Parameter reference	Substitutions reference
Components reference	Operations
Variable reference	Alarms
Analytics	Built-in functions
Expressions	Dependency detection
In-place interpolations	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, operations, analytics, alarms
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
- default
- roles, role, targets, target
- context, parent-context, parent_context

For information and examples about how to design your own StyleBooks, see How to Create Your Own StyleBooks.

Header

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:

ATTRIBUTE	DESCRIPTION
name	A name to identify the StyleBook. This attribute is mandatory.
display-name	A descriptive name for the StyleBook. This name appears on the NetScaler ADM GUI. This is an optional attribute.
description	A description text defines what this StyleBook do. This description appears on the ADM GUI. This is an optional attribute. **Note:** This is an HTML fragment and you can use HTML tags to customize headings or insert images using the `<img>` tag with URLs or embedded images.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
author	The author person or organization who creates the StyleBook. This is an optional attribute.
namespace	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: `<company>.<department>.<unit>.stylebooks`. This is a mandatory attribute.
version	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.
schema-version	The version of the StyleBooks schema. It takes the value "1.0" in the current release of NetScaler ADM. This is a mandatory attribute.
private	If this attribute is set to true, the StyleBook is not displayed on the NetScaler 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.

Example:

```
    name: lb

    description: "This stylebook defines a sample load balancing
configuration."
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
display-name: "Load Balancing StyleBook (HTTP)"

author: Mike Smith (ACME Infra team)

namespace: com.example.stylebooks

schema-version: "1.0"

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 NetScaler® 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

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 NetScaler NITRO types, such as lbvserver service or monitor. StyleBooks for NetScaler versions 10.5 and later are supported, which means that you can use your StyleBook to create and run configurations on any NetScaler 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:

```
import-stylebooks:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    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\>:: \<type-name\>**. 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 NetScaler.

Parameters

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 section is optional, most StyleBook might need one. You can consider the parameters section to define the fields for the users who use the StyleBook to create a configuration on a NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you import your StyleBook into NetScaler® ADM and use it to create a configuration, the GUI uses this section of the StyleBook to display a form. This form takes an input for the defined parameter values.

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 more alphabets, numbers, hyphen (-), or underscore (_).

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

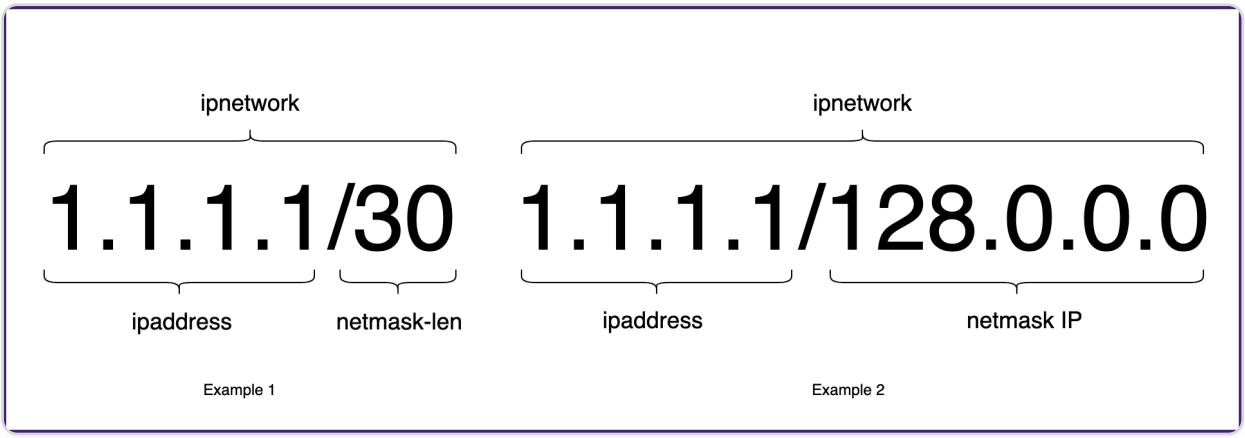
'type'

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `boolean`: Can be either true or false. YAML considers all the literals as booleans (for example, Yes or No).
- `ipaddress`: A string that represents a valid IPv4 or IPv6 address.
- `ipnetwork`: It has two parts. First part is the IP address and second part is the netmask.



The netmask consists of netmask length (`netmask-len`) or netmask IP address (`netmask_ip`). The netmask length is an integer between 0-32 and 0–128 for an IPv6 address. It is used to determine the IP addresses count in a network.

When creating or updating a configuration pack from the NetScaler ADM GUI, you can do one of the following actions:

- Enable Netmask Length and input the IP address and netmask length
- Disable Netmask Length and input the IP address and netmask IP address

In API, the netmask length and the netmask IP address is available as a single value as shown in the following example:

Example:

```
Content-Type: application/json

Accept: application/json

{

“configpack”:

{

      “stylebook”: {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        “namespace”: “com.example.stylebook”,

        “version”:“1.0”,

        “name”: “ipnetwork-example”,

        ..

        },

        “parameters”: {

           “name: “test-app”,

            “virtual-ip”: “212.100.30.0/255.255.255.0”,

        },

        “targets”:

        [

        ]

  }

  }
```

- `tcp-port`: A number between 0 and 65535 that represents a TCP or UDP port.
- `password`: Represents an opaque/secret string value. When the ADM GUI displays a value for this parameter, it is shown as asterisks (*****).
- `certfile`: Represents a certificate file. This value 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/\<tenant_path>/ns_ssl_certs` in ADM.

  The certificate file is added to the list of certificates managed by ADM.
- `keyfile`: Represents a certificate key file. This value allows you to upload the file directly from your local system when you are creating a StyleBook configuration using the ADM GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The uploaded certificate file is stored in the directory `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` in ADM.

The certificate key file is added to the list of certificate keys managed by ADM.

- `file`: Represents a file.
- `object`: This type is used when you want to group several related parameters under a parent element. 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 the list of types. To do so, add `[]` at 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

'network'

For `type: ipaddress`, you can specify the `network` attribute to auto-allocate an IP address from an ADM IPAM network.

ADM auto-allocates an IP address from the `network` attribute when you create a StyleBook configuration.

Example:

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

In this example, the `virtual-ip` field auto-allocates an IP address from `network-1`.The IP address is released back to the network when the configuration is deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'dynamic-allocation'

The `dynamic-allocation` attribute is added in the parameter definition of `type:ipaddress`. Use this attribute to dynamically list the ADM IPAM networks. This attribute can take either `true` or `false` as an input. For `type: ipaddress`, specify the `dynamic-allocation: true` attribute to dynamically list the ADM IPAM networks that are in ADM. In the configuration pack creation form, you can do the following:

1. Select the required IPAM network from the list.
2. Specify an IP address that you want to allocate from the selected IPAM network.

   If no IP address is specified, the ADM auto-allocates an IP address from the selected IPAM network.

Example:

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

In this example, the `virtual-ip` field lists the ADM IPAM networks that are in ADM. Select a network from the list to auto-allocate an IP address from the network. The IP address is released back to the network when the configuration is deleted.

'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 ADC instances), each configuration has a different/unique value for this parameter.

Default value is false.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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 ADM GUI, the user is prompted to select a parameter value from this list.

NOTE

If you want to display the list values as radio options, set the `layout` attribute.

Example 1:

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

Example 2:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      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. When a user creates a configuration without specifying a value, the default value is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The parameter takes no value if the following conditions are met:

- The parameter has no default value.
- A user does not provide a value for the parameter.

Example 1:

```
-

      name: timeout

      type: number

      default: 20
```

Example 2:

To list the default values of the parameter:

```
-

      name: protocols

      type: string[]

      default:

            -  TCP

            -  UDP

            -  IP
```

Example 3:

```
-

      name: timeout

      type: number
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: tcp-port

      min-value: 5000
```

The `min-value` of numbers can be negative. However, the `min-value` for `tcp-port` must be positive.

Mandatory? No

'max-value'

Use this attribute to define the maximum value for parameters of type `number` or `tcp-port`.

Ensure the maximum value is 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."

Ensure the minimum length of the characters defined as values are greater or equal to zero.

Example:

```
-

      name: appname

      type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      min-length: 3
```

Mandatory? No

'max-length'

Use this attribute to define the maximum length of values accepted for a parameter of type "string."

Ensure the maximum length of the values are 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.

Ensure the minimum number of items are greater or equal to zero.

Example:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2
```

Mandatory? No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'max-items'

Use this attribute to define the maximum number of items in a parameter that is a list.

Ensure the maximum number of items are 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 in the ADM GUI.

Mandatory? No

'columns'

This attribute is a subattribute of the `gui` attribute. Use this attribute to define the number of columns to display the `type: object[]` parameters in the ADM GUI.

Mandatory? No

'updatable'

This attribute is a subattribute of the `gui` attribute. Use this attribute to specify whether the parameter can be updated after the configuration is created. Set this attribute only on simple parameter types such as string, boolean, or number.

If the value is set to `false`, the parameter field is grayed out when you update the configuration.

Mandatory? No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'collapse_pane'

This attribute is a subattribute of the `gui` attribute. Use this attribute 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
```

Example of a complete parameters section:

```
parameters:

  -

    name: name

    label: Name

    description: Name of the application
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            default: ROUNDROBIN

        -

            name: enable-healthcheck

            label: Enable HealthCheck?

            type: boolean

            default: true
```

The following is an example that defines all the attributes of a list and the values explained in earlier sections:

```
        -

            name: features-list

            type: string[]

            min-length: 1

            max-length: 3
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            min-items: 1

            max-items: 3

            pattern: "\[A-Z\]+"

            allowed-values:

              - SP

              - LB

              - CS

            default:

              - LB
```

'layout'

This attribute is a subattribute of the `gui` attribute. Use this attribute to display the list values as radio buttons. Set the `layout` attribute to `radio` in the parameter section of a StyleBook definition. It applies to the parameter that has the `allowed-values` attribute. When you create a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuration pack, the ADM GUI displays the values in the `allowed-values` list as radio buttons.

Example:

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

The One, Two, and Three values appear as radio buttons in the ADM GUI.

'dependent-parameters'

This attribute is a subattribute of the `gui` attribute. It dynamically controls the parameter's appearance or its initial value in the StyleBook configuration form based on the value specified in another parameter.

Specify this attribute on a source parameter that controls the parameter's behavior on the form. You can include multiple conditions that control other parameters. For example, a source parameter `protocol` can have a dependent-parameter `certificate`, which only appears if the `protocol` parameter value is `SSL`.

Each condition can have the following attributes:

- **target-parameter**: Specify the target parameter to which this condition applies.
- **matching-values**: Specify the list of values of the source parameter that trigger the action.
- **action**: Specify one of the following actions on the targeted parameter:
  - `read-only`: The parameter is made read-only.
  - `show`: The parameter appears in the form if it is hidden.
  - `hide`: The parameter is removed from the form.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `set-value`: The parameter value is set to the value specified in the value attribute.

- **value**: The value of the target parameter if the action is `set-value`.

When a user input matches the specified values on the source parameter, the target parameter's appearance or value changes according to the specified action.

Example:

```
-

  name: lb-virtual-port

  label: "Load Balanced App Virtual Port"

  description: "TCP port representing the Load Balanced application"

  type: tcp-port

  gui:

    updatable: false

    dependent-parameters:

          -

            matching-values:

              - 80

            target-parameter: $parameters.lb-service-type

            action: set-value

            allowed-values:

            - HTTP

            - TCP

            - UDP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    default: 80
```

In this example, the dependent parameter is specified under the `lb-virtual-port` parameter (source parameter).

When the source parameter value is set to `80`, the `lb-service-type` parameter triggers the `set-value` action. As a result, a user is allowed to select one of the following options:

- HTTP
- TCP
- UDP

Parameters-default-sources construct

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.commontypes

    version: "1.0"

    description: This StyleBook defines a typical virtual IP config.

    private: true

    schema-version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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 NetScaler configuration for
Biz App

     schema-version: "1.0"

     import-stylebooks:

       -

           namespace: com.acme.commontypes

           prefix: cmtypes
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     version: "1.0"
parameters-default-sources:
      - cmtypes::vip-params
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            - 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:

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Substitutions are used to define shorthand names that can replace complex expressions in the StyleBook making the StyleBook more readable.

Substitutions are also useful when the same expression or value is used repeatedly in the StyleBook, for example, a constant value. Using a substitution name for a parameter allows you to update only the substitution value instead of updating all the occurrences of the parameter in the StyleBook which might be prone to errors.

Substitutions are also used for defining mappings between values.

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
```

You can specify a mnemonic name to a port number and 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 takes 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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          name: $parameters.name + "-lb"

          servicetype: HTTP

          ipv46: $parameters.ip

          port: **$substitutions.http-port**

          lbmethod: $parameters.lb-alg
```

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")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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 is-secure, or selects the check box corresponding to this parameter in the NetScaler 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 check box in the NetScaler ADM GUI, `servicetype` is assigned the value of **HTTP** and the port is assigned the value of **80**.

The following example shows how to use substitutions as a function. A substitution function can take one or more arguments. Arguments can be of simple type for example, string, number, IP address, boolean, and other types.

substitutions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

form-lb-name(name): $name + "-lb"

In this example, a substitution function "form-lb-name" is defined that takes a string argument called "name" **** and uses it to create a string that suffixes "-lb" to the string in the name argument. An expression using this substitution function is written as:

`$substitutions.form-lb-name("my")`

It 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 is shown as:

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname

         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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:

  slist:

    - a

    - b

    - c
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 can be used in condition, properties, repeat, and repeat-condition constructs.

The following example of a component shows how a substitution can be used to specify the properties:

```
  properties:
    a: $substitutions.slist
    b: $substitutions.sdict
    c: $substitutions.slistofdict
    d: $substitutions.sdictoflist
```

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. As all the load balancing virtual servers tied to the same content switching virtual server might have an identical configuration, use a substitution list and dictionary to build the configuration to avoid repeating the same configuration for every load balancing virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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" specifies the properties of the load balancing virtual servers associated with the ccontent switching 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 the `cs-pools` component, you can assign the value of this substitution to the `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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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 csvserver_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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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.

```
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

$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 doesn't return any value

Iterate through substitution lists

In the following example, the StyleBook iterates through a substitution list called `apps` to create a set of `lbvserver` components and their corresponding service groups and bound servers.

```
substitutions:

  apps:

    -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lb1
    vip: 1.2.3.4
    vport: 80
    protocol: HTTP
    servers:
      -
        ip: 10.8.11.11
        port: 8080
      -
        ip: 10.8.11.12
        port: 8080
  -
    name: lb2
    vip: 1.2.3.5
    vport: 81
    protocol: HTTP
    servers:
      -
        ip: 10.9.11.28
        port: 8080
      -
        ip: 10.9.11.29
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          port: 8181
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    repeat: $substitutions.apps
    repeat-item: app
    properties:
      name: $app["name"]
      ipv46: $app["vip"]
      port: $app["vport"]
      servicetype: $app["protocol"]
    components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        properties:
          servicegroupname: $parent.properties.name + "-svg"
          servicetype: HTTP
        components:
          -
            name: servers-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: ns::server

            repeat: $app["servers"]

            repeat-item: server

            properties:

              name: $server["ip"]

              ipaddress: $server["ip"]

            components:

              -

                name: servicegroup-servicegroupmember-binding-comp

                type: ns::servicegroup_servicegroupmember_binding

                properties:

                  servicegroupname:
$parent.parent.properties.servicegroupname

                  servername: $parent.properties.name

                  port: $server["port"]
```

Components

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
name	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 (_).
description	A description of the role of this component in the StyleBook.
type	The type determines what properties this component provides. Components have two kind of 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." When a component has a built-in type attribute, it creates a configuration object of that type on the NetScaler. For example, if a component refers to the built-in type “lbvserver,” this component creates a load balancing virtual server on the NetScaler instance that is the target of the configuration. **Composite type**: This type refers to an existing StyleBook that you created and imported into NetScaler ADM. When a component has a composite type attribute, it creates all the configuration objects, which are specified in the referenced StyleBook, on the NetScaler 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 Create a Composite StyleBook.
properties	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
	another StyleBook, that is, a composite type, the properties correspond to the parameters defined in that StyleBook.

Example:

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 NetScaler instance.

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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

       port: 80

       lbmethod?: $parameters.lb-advanced.algorithm
```

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:

```
components
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    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

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.

```
parameters:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46

      port: $parameters.lb.port

      servicetype: $parameters.lb.servicetype

      lbmethod: $parameters.lb.lbmethod
```

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.

```
parameters:

  -

    name: lb

    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
```

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -

              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:

                      repeat-list: $parameters.svc-servers

                      repeat-item: srv

                    properties:

                      ip: $srv

                      port: str($parameters.svc-port)

                      servicegroupname: $parent.properties.name
```

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 NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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:

```
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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following example builds the configuration object of NITRO type ns::systemfile if the condition is evaluated to true.

Example:

```
     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

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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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:

                        -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        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:

                          repeat-list: $parameters.svc-servers

                          repeat-item: srv

                        properties:

                               ip: $srv

                               port: $parameters.svc-port

                               servicegroupname: $parent.properties.name
```

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

name: members-svcg-comp

type: ns::servicegroup_servicegroupmember_binding

repeat:

  repeat-list: $parameters.svc-servers

properties:

       ip: $repeat-item

       port: $parameters.svc-port

       servicegroupname: $parent.properties.name
```

In addition to being able to refer to the current item white 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:

```
   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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
    -

            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
```

Repeat-condition construct

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:

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      repeat-list: $parameters.certificates

      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

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:

```
parameters:

  -

      name: vips
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Outputs

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.

ATTRIBUTE	DESCRIPTION	MANDATORY
name	The name of the output corresponding to the configuration object you want to expose.	Yes
description	A text string describing the output.	No
value	This attribute specifies how to extract the value that is returned by a StyleBook.	Yes

Example:

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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

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:

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parent reference

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:

```
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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Components reference

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:

```
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

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If a substitution is a map, you can refer to an element in the map as `$substitutions.<substitutions-name>[<map-key>]`. For example, `$substitutions.protocol-map[$parameters.port]`.

Variable reference

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:

```
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:

      -

         name: service-members-comp

         type: ns::service
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        properties:

          name: $server-name + "-service"

          servername: $parent.properties.name

          servicetype: $parameters.svc-service-type

          port: $parameters.svc-server-port
```

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 `$\<varname\>`.

Operations

Operations is an optional section in a StyleBook. In this section, you can configure NetScaler Application Delivery Management (ADM) analytics to collect AppFlow records on all or some of the traffic transactions. The virtual server created on a NetScaler instance by using the StyleBook handles these traffic transactions. In this section, you can also configure NetScaler ADM to trigger alarms when certain traffic conditions are met on a virtual server.

You can configure NetScaler® ADM through StyleBooks to collect traffic statistics from various NetScaler ADM Insights that are listed as follows:

- Web Insight
- WAF Security Violations
- HDX™ Insight
- NetScaler Gateway Insight.

The virtual servers supported are load balancing, content switching, and VPN virtual servers.

Enable both Web Insight and WAF Security Violations 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 NetScaler Gateway Insight or one of them.

Any NetScaler ADM Insight enabled on NetScaler instances through StyleBooks uses the IPFIX protocol (AppFlow) to send the data from the instances to NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also, when you enable Web Insight, Client-Side Measurements is enabled on the load balancing and the content switching virtual servers. With client side measurements enabled, ADM captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

Example 1:

The following example shows how to write the operations section in a StyleBook to enable both HDX Insight and NetScaler Gateway Insight on a VPN virtual server:

```
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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following example shows how to write the operations section in a StyleBook to enable both Web Insight and WAF Security Violations 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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

Each element in the analytics section is used to configure the NetScaler® ADM analytics feature for one or more virtual servers created in StyleBooks.

An element in the analytics section has the following attributes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
name	Name of the analytics element.	Yes
description	A text string describing what this element is.	No
condition	A boolean expression. When this condition evaluates to false, the entire analytics element is skipped.	No
repeat	Iterates over a list.	No
repeat-condition	A boolean expression. If the expression evaluates to false, the current iteration is skipped.	No
repeat-item	Name of the item in the current iteration.	No
repeat-index	Name of the index value of the current iteration.	No
properties	The list of properties of analytics.	Yes
target	One of the properties in the list. The target expression is the name of a virtual server, configured on the NetScaler, for which analytics is collected.	Yes
filter	One of the properties in the list. The value of this attribute is a NetScaler advanced policy expression that is used to filter the requests on the virtual server for which analytics is collected. By default, the analytics data is	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
	collected on all the traffic passing through the virtual server.	
insights	One of the properties in the list. The value of this attribute is the type of insight data to be collected from the target virtual server.	No

Example 1: Configuring analytics for a single virtual server

```
operations:



  analytics:

    -

    name: lbvserver-ops-comp

    properties:

        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        insights:

          -

            type: webinsight

          -

            type: securityinsight
```

Example 2: Configuring analytics for a list of VPN virtual servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        insights:

          -

            type: hdxinsight

          -

            type: gatewayinsight
```

Each attribute in the analytics section configures the NetScaler instances to collect AppFlow records on the virtual server identified by the target property.

The target virtual servers and the corresponding allowed insight types are as follows:

TARGET VIRTUAL SERVER	INSIGHT TYPE
lbvserver	webinsight, securityinsight
csvserver	webinsight, securityinsight
vpnserver	hdxinsight, gatewayinsight

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

IPFIX is the default transport mode used to configure analytics for virtual servers in StyleBooks.

Alarms

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:

ATTRIBUTE	DESCRIPTION	MANDATORY
target	An expression that evaluates to the name of a virtual server, configured on the NetScaler, for which alarms are configured.	Yes
email-profile	Name of an email profile that is defined in the NetScaler ADM Analytics feature and contains a list of email addresses that you want to notify when the alarm is triggered.	No (either an email-profile or an sms-profile must be defined)
sms-profile	Name of an SMS profile that is defined in the NetScaler ADM Analytics feature and contains a list of phone numbers that you want to notify when the alarm is triggered.	No (either an email-profile or an sms-profile must be defined)
rules	A list of rules that define the conditions that would trigger an alarm for the virtual server defined by the target property.	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
metric	An attribute of rule. The name of a metric you want to track pertaining to the NetScaler virtual server.	Yes
operator	An attribute of rule. The operator to use to compare the metric to the value. Valid operators are "greaterthan" and "lessthan."	Yes
value	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.	Yes
period-unit	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).	Yes

The following table provides a list of metrics that are tracked pertaining to the NetScaler virtual server.

Counters|Description|Detailed Desription|NetScaler ADM Calculation

For a VPN virtual server			

app_count	VPN App Launch Count	Total number of unique VPN applications on this	Monotonically increasing counter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

		VPN virtual server launched during a time interval specified by the user.	on each new application launch
app_launch_duration	VPN App Launch Duration	Average time taken to launch an application (in milliseconds)	Average value calculated across the launch time durations of all VPN applications launched on this VPN virtual server
Other virtual servers (CS, LB, Auth, GSLB)			
total_requests	Number of requests	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.	Monotonically increasing counter, incremented on each new request to this virtual server.
total_bytes	Bytes	Total bytes transferred from the virtual server to NetScaler ADM over the specified time interval.	Monotonically increasing counter to account for the total number of bytes served by this virtual server.
application_response_time	Response Time	Average response time of the virtual server.	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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of an alarms section in a StyleBook:

```
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

        -

          metric: "total_bytes"

          operator: "lessthan"

          value: 1024

          period-unit: day
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expressions

One of the most powerful features of a StyleBook is the use of expressions. You can use StyleBooks expressions in various scenarios to compute dynamic values. The following example is an expression to concatenate a parameter value with a literal string.

Example:

```
$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 (+)
- Subtraction (-)
- 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 (+)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

- Concatenate two lists: $parameters.external-servers + $parameters.internal-servers
- If `$parameters.ports-1` is and `$parameters.port-2` is , the `$parameters.ports-1 + $parameters.ports-2` displays as a list .

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 expressions - boolean

- **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 the opposite way.
- **in**: Tests whether the first argument is a substring of the second argument

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **in**: Tests if an item is part of a list

NOTE

You can type-cast expressions where strings are converted into numbers and numbers are converted to strings. Similarly, you can cast `tcp-port` to a number, and an IP address can be cast to a string.

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`

Verbatim string expressions

You can use verbatim strings when special characters in a string have to take their literal form. These strings can contain escape characters, backslash, quotes, parentheses, whitespaces, brackets, and so on. In verbatim strings, the special characters' usual interpretation is skipped. All the characters in the string are preserved in their literal form.

In StyleBooks, you can include NetScaler Policy Expressions in their literal form using verbatim strings. The Policy Expressions typically contain special characters. Without verbatim strings, you have to escape special characters by breaking strings into substrings.

To create a verbatim string, encapsulate a string between special characters as follows:

```
~{string}~
```

You can use verbatim strings anywhere in the StyleBook.

NOTE

Do not use the sequence of characters `}~` in an input string because this sequence indicates the end of a verbatim string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

Target expressions

In a StyleBook definition, you can use the `$current-target` expression to refer to the current target ADC instance. To specifically refer to the IP address of the target ADC instance, use this expression as follows:

```
$current-target.ip
```

Example:

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

In this example, the name of the `lbvserver` is constructed with the IP address of the target ADC instance.

Expression Type Validation

StyleBook engine 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of Type Checks:

In the following example, the expected type of port property of `lbvserver` StyleBook is `tcp-port`. In NetScaler Application Delivery Management (ADM), the 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 displays an error and fails to import or migrate a StyleBook.

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: str("80")

      servicetype: HTTP
```

To successfully compile this StyleBook, declare the following as a number in the compiler:

`port: 80`

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 NetScaler® ADM. Now if this StyleBook is imported to NetScaler ADM, the compiler identifies such invalid expressions and flag it. As a result, the StyleBook fails to import to NetScaler 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 NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

kind of error is identified during import and the StyleBook is not imported to NetScaler ADM. Manually correct such errors and import the StyleBooks.

```
Components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: $components.lbvserver-comp.properties.lbvservername

servicegroupname: $components.sg-comp.properties.servicegroupname
```

Indexing Lists

Items of a list can be accessed now by indexing them directly:

Expression	Description
`$components.test-lbs[0]`	Refers to the first item in test-lbs component
`$components.test-lbs[0].properties.p1`	Refers to property p1 of the first item in test-lbs component
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Refers to property `servicegroupname` of the second item in `servicegroups` component, which is an output from the first item of `lbcomps` component

In-place interpolations

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 **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, "jpeg".

For this, you write a policy expression as follows: "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:

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

If $parameter.url-object is assigned "csv", the above expression will evaluate to "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:

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

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.

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 lb-%{$parameters.appname}%-%{$parameters.vip}% returns "lb-app1-1.1.1.1", if $parameters.appname is "app1" and $parameters.vip is "1.1.1.1"

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 "%{lb-%{$parameters.port + 1}%}%"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The internal string, "**%{$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

EXPRESSION	RESULT
lb-%{$parameters.appname}%-def	lb-lb1-def

Automatic type conversions

EXPRESSION	RESULT
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Sequential interpolations

EXPRESSION	RESULT
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nested interpolations

EXPRESSION	RESULT
%{abc-%{$parameters.n1 + 1}%}%	abc-2
str("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%")	bc-1-3

Interpolations with quotewrap

EXPRESSION	RESULT
str("%{quotewrap(abcd)}%")str("%{quotewrap(`https://)}%+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	"abcd"<`https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL`

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:

CATEGORY	EXPRESSION	RESULT
Escaping interpolations	str("%{str($parameters.n1) + }\%}%")	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	"%{str($parameters.n1) + \"\}\%\"}%"	1}%

Built-in functions

Expressions in StyleBooks can make use of built-in functions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

- The `"set-" + str(10)` function returns `"set-10"`.
- The `str(10)` function returns `10`.
- The `str(1.1.1.1)` function returns `1.1.1.1`.
- The `str(T rue)` function returns `"T rue"`.
- The `str(ADM)` function returns `"mas"`.

int()

The `int()` function takes a string, number, IP address, or `tcpport` as an argument and returns an integer.

Examples:

- The `int("10")` function returns `10`.
- The `int(10)` function returns `10`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `int(ip('0.0.4.1'))` function returns `1025`.

bool()

The `bool()` function takes any type as an argument. If the argument value is `false`, empty, or absent, this function returns `false`.

Otherwise, it returns `true`.

Examples:

- The `bool(true)` function returns `true`.
- The `bool(false)` function returns `false`.
- The `bool($parameters.a)` function returns `false` if the `$parameters.a` is `false`, empty, or absent.

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"]`

The `len($substitutions.items)` function returns `3`

Example 2:

The `len("NetScaler ADM")` function returns `10`.

Example 3:

If `$parameters.vips` has values `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, the `len($parameters.vips)` function returns `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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `min(80, 100, 1000)` function returns `80`.
- The `min(-20, 100, 400)` function returns `-20`.
- The `min(-80, -20, -10)` function returns `-80`.
- The `min(0, 100, -400)` function returns `-400`.

Examples with a list of numbers/tcp-ports:

- Support `$parameters.ports` is a list of `tcp-ports` and has values: `[80, 81, 8080]`.

  The `min($parameters.ports)` function 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:

- The `max(80, 100, 1000)` function returns `1000`.
- The `max(-20, 100, 400)` function returns `400`.
- The `max(-80, -20, -10)` function returns `-10`.
- The `max(0, 100, -400)` function returns `100`.

Examples with a list of numbers/tcp-ports:

- Support `$parameters.ports` is list of `tcp-ports` and has values: `[80, 81, 8080]`.

  The `max($parameters.ports)` function 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:

The `bin(100)` function returns `0b1100100`.

oct()

The `oct()` function takes a number as an argument, and returns a string that represents the number in octal format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Examples of expressions:

The `oct(100)` function 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:

The `hex(100)` function returns `0x64`.

lower()

The `lower()` function takes a string as an argument and returns the same string in the lowercase.

Example:

The `lower("ADM")` function returns `adm`.

upper()

The `upper()` function takes a string as an argument and returns the same string in uppercase.

Example:

The `upper("NetScaler ADM")` function returns `NetScaler ADM`.

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]
```

The `sum($substitutions.list-of-numbers)` function returns `88`.

Example 2:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If `$parameters.ports` is `[80, 81, 82]`, the `sum($parameters.ports)` function 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:

The `pow(3,2)` function returns `9`.

ip()

The `ip()` function takes an integer, string, or an IP address as an argument and returns the IP address based on the input value.

Examples:

- Specify an IP address in the `ip` function:

  The `ip(3.1.1.1)` function returns `3.1.1.1`.
- Specify a string in the `ip` function:

  The `ip('2.1.1.1')` function returns `2.1.1.1`
- Specify an integer in the `ip` function:
  - The `ip(12)` function returns `0.0.0.12`.
  - When you specify an integer as string in the `ip` function, it returns an equivalent IP address of the input.

    The `ip('1025')` function returns `0.0.4.1`.

  This function also supports the integer addition and subtraction operations and returns a resultant IP address.

  - Addition: The `ip(1025) + ip(12)` function returns `0.0.4.13`.
  - Subtraction: The `ip('1025') - ip(12)` function returns `0.0.3.245`.
  - Combine addition and subtraction: The `ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` returns `2.2.2.0`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

base64.encode()

The `base64.encode()` function takes a string argument and returns the base64 encoded string.

Example:

The `base64.encode("abcd")` function returns `YWJjZA==`.

base64.decode()

The `base64.decode` function takes a base64 encoded string as an argument and returns the decoded string.

Example:

The `base64.decode("YWJjZA==")` function 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 `$parameters.monitor` is an optional parameter. If you provide a value to this parameter when creating a configuration pack, exist the `($parameters.monitor)` function 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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]`.

The `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`.

Example 1:

The `if-then-else($parameters.servicetype == HTTP, 80, 443)` function returns `80` if `$parameters.servicetype` has value `HTTP`. Otherwise, the function returns `443`.

Example 2:

The `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` function returns the value of `$parameters.hport` if `$parameters.servicetype` has value `HTTP`.

Otherwise, the function returns the value of `$parameters.sport`.

Example 3:

The `if-then-else($parameters.servicetype == HTTP, 80)` returns `80` if `$parameters.servicetype` has value `HTTP`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Otherwise, the function does not return any value.

join()

The `join()` function takes two arguments:

Argument 1: list of numbers, `tcp-ports`, strings, or IP addresses

Argument 2: delimiter string (optional)

This 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 the elements in the list are joined as one string.

Example:

- `$parameters.ports` is `[81, 82, 83]`.
  - With delimiter argument:

    The `join($parameters.ports, '-')` function returns `81-82-83`.
  - Without delimiter argument:

    The `join($parameters.ports)` function returns `818283`.

split()

The `split()` function splits an input string into multiple lists depending on the specified separators. If no or blank (`''`) separator is specified, this function considers space as a separator and splits the string into lists.

Examples:

- The `split('Example_string_split', 's')` function returns `['Example_','tring_','plit']`.
- The `split('Example string split')` function returns `['Example','string','split']`.
- The `split('Example string split', '')` function returns `['Example','string','split']`.
- The `split('Example string')` function returns `['Example','string']`.

  This function considers continuous spaces as one space.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

  The `map(str, $parameters.nums)` function 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:

    The `map($substitutions.add-10, $parameters.nums)` function 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)`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

quotewrap()

The `quotewrap()` function takes a string as an argument and returns a string after adding a double quote character before and after the input value.

Example:

The `quotewrap("ADM")` function returns `"mas"`

replace()

The `replace()` function takes three arguments:

Argument 1: string

Argument 2: string or list

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 an empty string).

Replace a substring with another substring:

- The `replace('abcdef', 'def', 'xyz')` function returns `abcxyz`.

  All occurrences of `def` are replaced with `xyz`.
- `replace('abcdefabc', 'def')` returns `abcabc`.

  As there is no third argument, `def` is removed from the resulting string.

Specify the characters list that you want to replace in a string.

`$parameters.spl_chars = ['@', '#', '!', '%']`

This list contains the values that have to be replaced in an input string.

The `replace('An#example@to%replace!characters', $parameters.spl_chars, '_')` function returns `An_example_to_replace_characters`.

The output string has underscore (`_`) instead of characters specified in the `$parameters.spl_chars` list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

trim()

The `trim()` function returns a string where the leading and trailing whitespaces are stripped from the input string.

Example:

The `trim(' abc ')` function 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:

The `truncate('NetScaler ADM', 6)` returns `Citrix`.

distinct()

The `distinct()` function extracts unique items from a list input.

Examples: If `$parameters.input_list` is `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`, the `distinct($parameters.input_list)` function returns `['ADM', 'ADC', 'VPX', 'CPX']`.

url.encode()

The `url.encode()` function returns a string where characters are transformed using the ASCII character set according to RFC 3986.

Example:

The `url.encode("a/b/c")` function returns `a%2Fb%2Fc`.

url.decode()

The `url.decode()` function returns a string where the URL encoded argument is decoded in to a regular string according to RFC 3986.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

The `url.decode("a%2Fb%2Fc")` function returns `a/b/c`.

is-ipv4()

The `is-ipv4()` function takes an IP address as an argument and returns the boolean `True` if the IP address is of the IPv4 format.

The `is-ipv4(10.10.10.10)` function returns `True`

is-ipv6()

The `is-ipv6()` function takes an IP address as an argument and returns the boolean `True` if the IP address is of the IPv6 format.

The `is-ipv6(2001:DB8::)` function returns `True`

startswith()

The `startswith()` function determines whether a string begins with a given prefix. This function requires two mandatory string arguments.

`startswith(str, sub_str)`

This function returns `True` when the string (`str`) starts with the substring (`sub_str`).

Examples:

- The `startswith('Citrix', 'Ci')` function returns `True`.
- The `startswith('Citrix', 'iC')` function returns `False`
- The `startswith('Citrix', 'Ab')` function returns `False`

endswith()

The `endswith()` function determines whether a string ends with a given suffix. This function requires two mandatory string arguments.

`endswith(str, sub_str)`

This function returns `True` when the string (`str`) ends with the substring (`sub_str`).

Examples:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `endswith('Citrix', 'ix')` function returns `True`.
- The `endswith('Citrix', 'Ix')` function returns `False`.
- The `endswith('Citrix', 'ab')` function returns `False`.

contains()

The `contains()` function determines whether a string contains a given substring. This function requires two mandatory string arguments.

`contains(str, sub_str)`

This function returns `True` when the substring (`sub_str`) is contained anywhere inside the string (`str`).

Example:

- The `contains('Citrix', 'tri')` function returns `True`.
- The `contains('Citrix', 'Ci')` function returns `True`.
- The `contains('Citrix', 'ti')` function returns `False`

substring()

Use the `substring()` function to extract a substring from a string.

`substring(str, start_index, end_index)`

This function requires the two mandatory arguments and one optional integer argument.

- `str` (Mandatory)
- `start_index` (Mandatory)
- `end_index` (Optional)

This function returns the substring from the string (`str`) that is between the specified index positions. If you do not specify the end index position, the function extracts the substring from the start index to the end of the string.

NOTE

When you specify `end_index`, the substring excludes the character at the `end_index` position.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

- The `substring('Citrix', 2)` function returns `trix`
- The `substring('Citrix', 10)` function returns (`"`)

  In this example, the function returns a blank string because it has an invalid `start_index` position.
- The `substring('Citrix', 2, 4)` function returns `tr`

  In this example, the function extracts the characters between 2 and 4 index positions.
- The `substring('Citrix', -3)` function returns `rix`

  If you want to extract characters that are at the end of the string, specify a negative value for the `start_index` argument.

  In this example, the function extracts the substring that includes the last three characters in the string.

Dependency detection

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.name

      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
     name: mylb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: $components.lbvserver-comp.properties.servicetype
```

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 NetScaler® ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security

NetScaler Console security analytics help you monitor, detect, and mitigate threats to your applications. The following topics help you view and act on security insights:

- Application security dashboard
- Security violations
- Integration with Splunk
- Integration with New Relic

Application Security Dashboard

The **App Security** dashboard provides you the overview of security metrics for the discovered/licensed applications. This dashboard displays the security attack information for the discovered/licensed applications, such as sync attacks, small window attacks, DNS flood attacks, and so on.

To view the security metrics on app security dashboard:

1. Navigate to **Security** > **Security Dashboard**.
2. Select the instance IP address from the Instance list.

   The reports include the following information for each application:

   - **Threat index**. A single-digit rating system that indicates the criticality of attacks on the application. The more critical the attacks on an application, the higher the threat index for that application. The values range from 1 through 7.

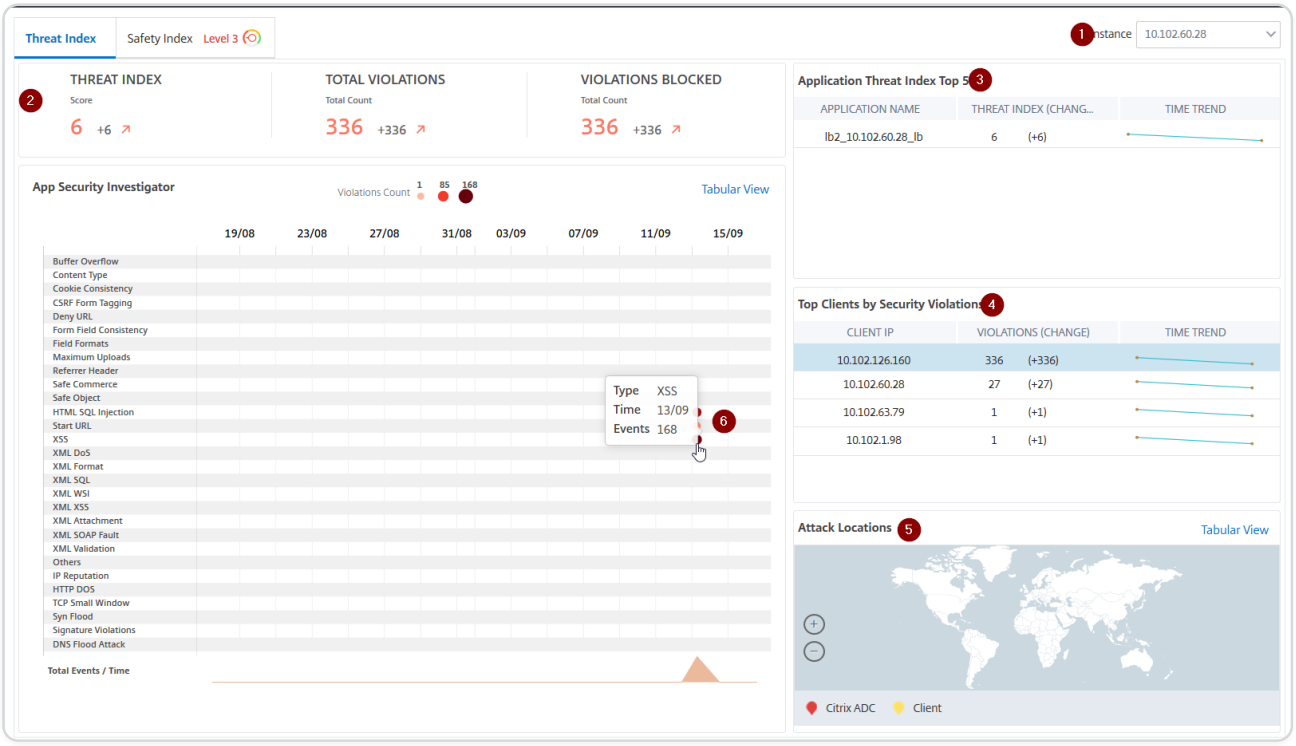
     The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives an insight into the attacks on the application. Violation information is sent to NetScaler® ADM only when a violation or attack occurs. A large number of breaches and vulnerabilities lead to a high threat index value.
   - **Safety index**. A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. The values range from 1 through 7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The safety index considers both the application firewall configuration and the NetScaler system security configuration. For a high safety index value, both configurations must be strong. For example, if rigorous application firewall checks are in place, but NetScaler system security measures, such as a strong password for the `nsroot` user is not provided, then applications are assigned a low safety index value.

You can view the discrepancies reported on the **App Security Investigator**.

Threat index details



1 - Displays the NetScaler instance IP address for which you can view details.

2 - Displays details such as threat index score, total violations occurred, and total violations blocked.

3 - Displays the virtual server of the selected instance.

4 - Displays the security violations based on clients. The App Security Investigator graph is displayed for each client. You can click each client IP to view the results.

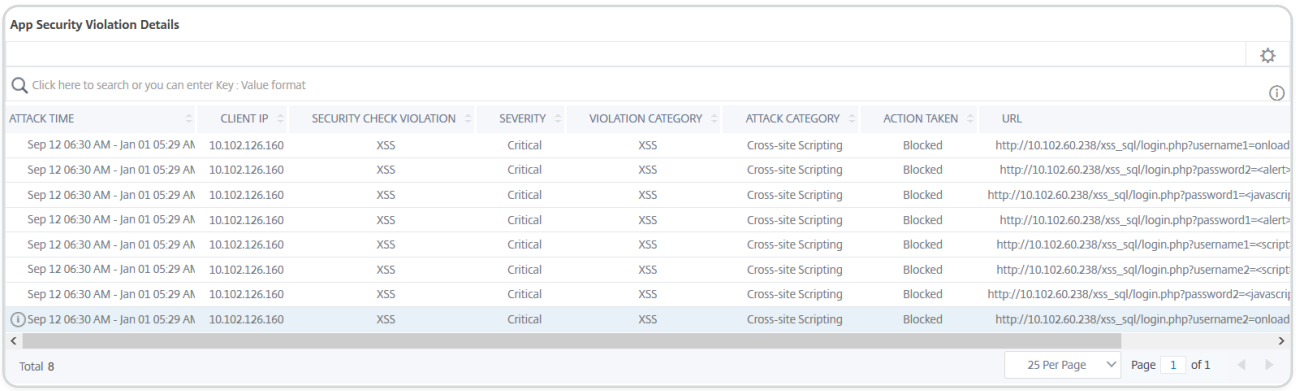
5 - Displays the violations in map view and tabular view.

6 - Displays the violation details. When you hover the mouse pointer on the graph, the details such as violation type, time of the attack, and total events are displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you click a bubble graph, the details are displayed in the **App Security Violation Details** page. For example, if you want to further view details for cross-site scripting (cross-site script) violation, click the graph populated for **XSS** in **App Security Investigator**.

The **App Security Violation Details** is displayed with violation details such as attack time, attack category, severity, URL, and so on.



You can also click the **Settings** option to select the options that you want to get it displayed.

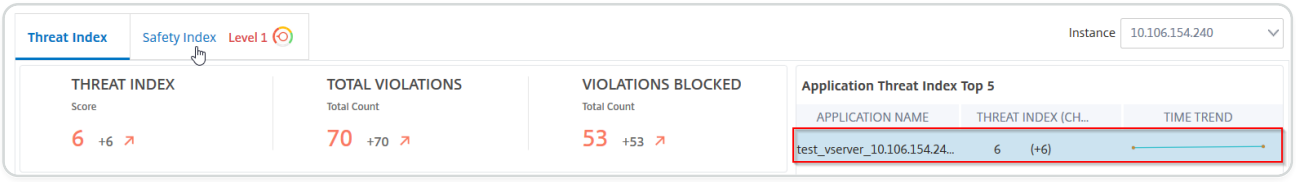
Safety index details

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application safety index summary.

The safety index summary gives you information about the effectiveness of the following security configurations:

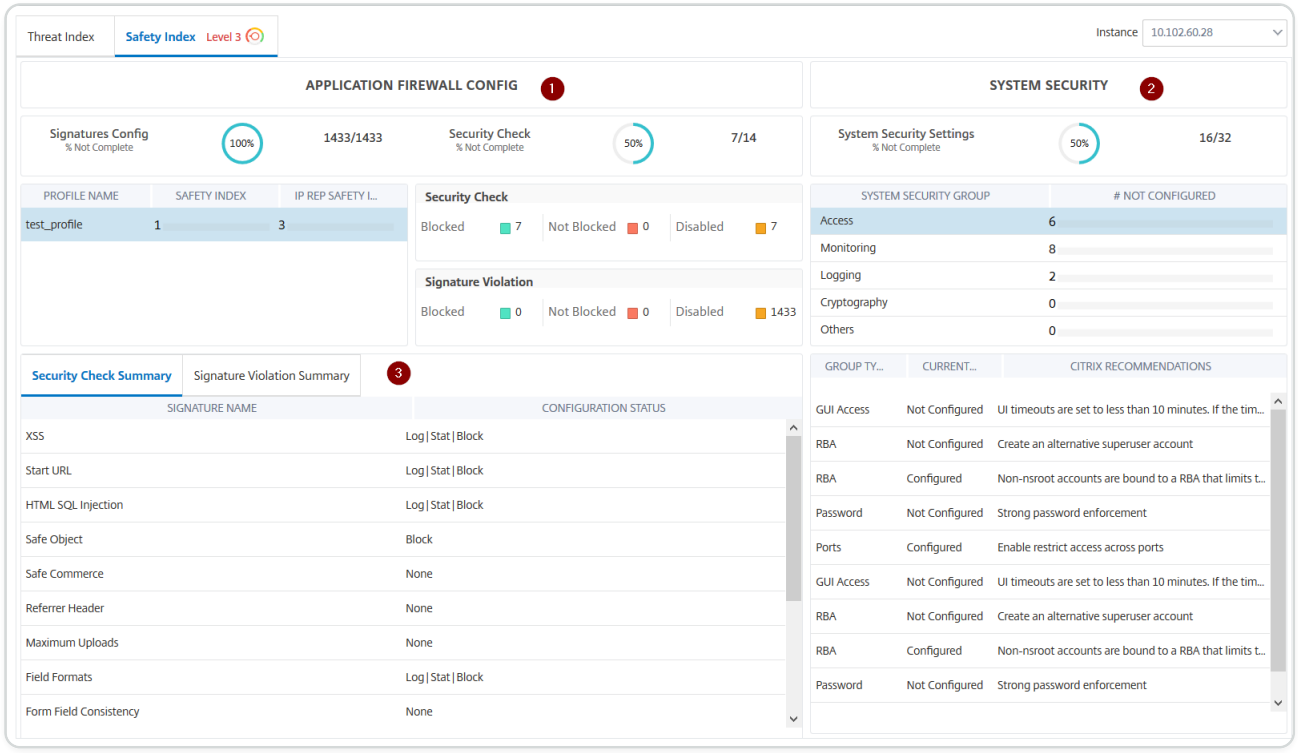
- **Application Firewall Configuration**. Shows how many signature and security entities are not configured.
- **NetScaler ADM System Security**. Shows how many system security settings are not configured.

To view the **Safety Index** details, select a virtual server/application and click the **Safety Index** tab.



The details are displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 - Displays the detailed information for Application Firewall configurations.

2 - Displays the detailed information for System Security. Click each security group to get details on current status and Citrix recommendations.

3 - Displays the summary for Security Check and Signature Violation.

You can also view summary of the threat environment by enabling the **WAF Security Violations** for virtual servers and then navigating to **Security** > **Security Violations**.

View application security violation details

Web applications that are exposed to the internet have become vulnerable to attacks drastically. NetScaler® ADM enables you to visualize actionable violation details to protect applications from attacks. Navigate to **Security** > **Security Violations** for a single-pane solution to:

- Visualize applications with full visibility into the threat details associated in both WAF Security Violations and Bot Security Violations
- Access the application security violations based on its categories such as **Network**, **Bot**, and **WAF**
- Take corrective actions to secure the applications

The **Security Violations** page has the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Application Overview** – Displays an overview with applications that have total violations, total WAF and Bot violations, violation by country, and so on. For more information, see Application overview.
- **All Violations** – Displays the application security violation details. For more information, see All violations.

Prerequisite

Ensure if **Metrics Collector** is enabled. By default, **Metrics Collector** is enabled on the NetScaler instance. For more information, see Configure Intelligent App Analytics.

Integration with Splunk

You can now integrate NetScaler® ADM with Splunk to view analytics for:

- WAF violations
- Bot violations
- SSL Certificate Insights

Splunk add-on enables you to:

- Combine all other external data sources.
- Provide greater visibility of analytics in a centralized place.

NetScaler ADM collects Bot, WAF, SSL events, and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an administrator, using the CIM compatible data, you can view the events in the Splunk dashboard.

For a successful integration, you must:

- Configure Splunk to receive data from NetScaler ADM
- Configure NetScaler ADM to export data to Splunk
- View dashboards in Splunk

Configure Splunk to receive data from NetScaler ADM

In Splunk, you must:

1. Setup the Splunk HTTP event collector endpoint and generate a token

© 1997–2026 Citrix Systems, Inc. All rights reserved.

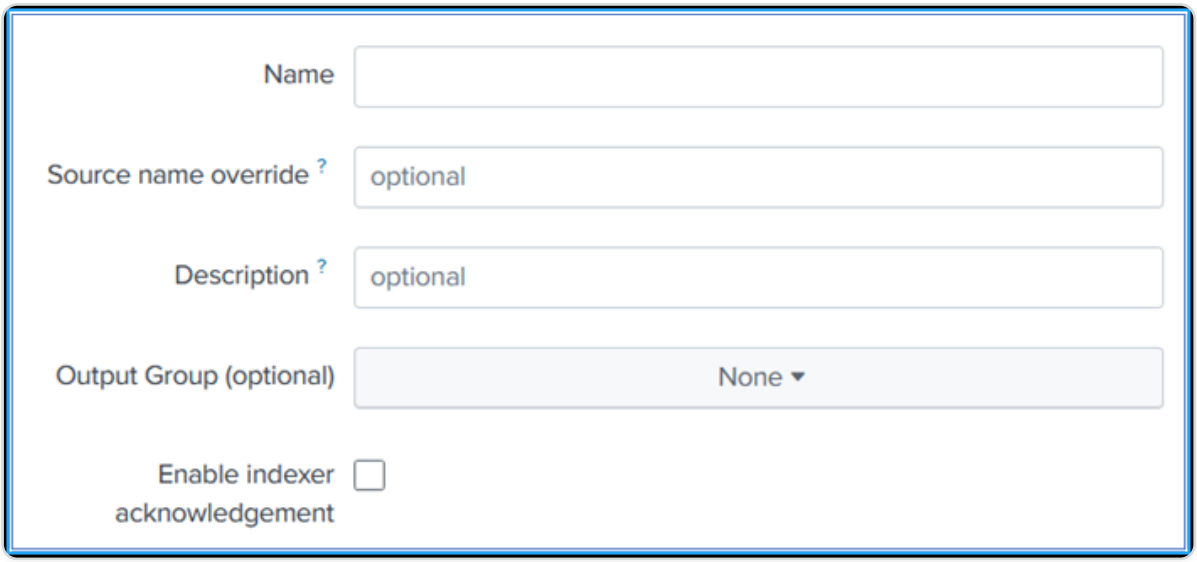
2. Install the Splunk Common Information Model (CIM) add-on
3. Prepare a sample dashboard in Splunk

Setup the Splunk HTTP event collector endpoint and generate a token

You must first setup the HTTP event collector in Splunk. This setup enables the integration between the ADM and Splunk to send the data. Next, you must generate a token in Splunk to:

- Enable authentication between ADM and Splunk.
- Receive data through the event collector endpoint.

1. Log on to Splunk.
2. Navigate to **Settings > Data Inputs > HTTP event collector** and click **Add new**.
3. Specify the following parameters:
   a. **Name**: Specify a name of your choice.
   b. **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector.
   c. **Description (optional)**: Specify a description.
   d. **Output Group (optional)**: By default, this option is selected as None.
   e. **Enable indexer acknowledgement**: By default, this option is not selected.

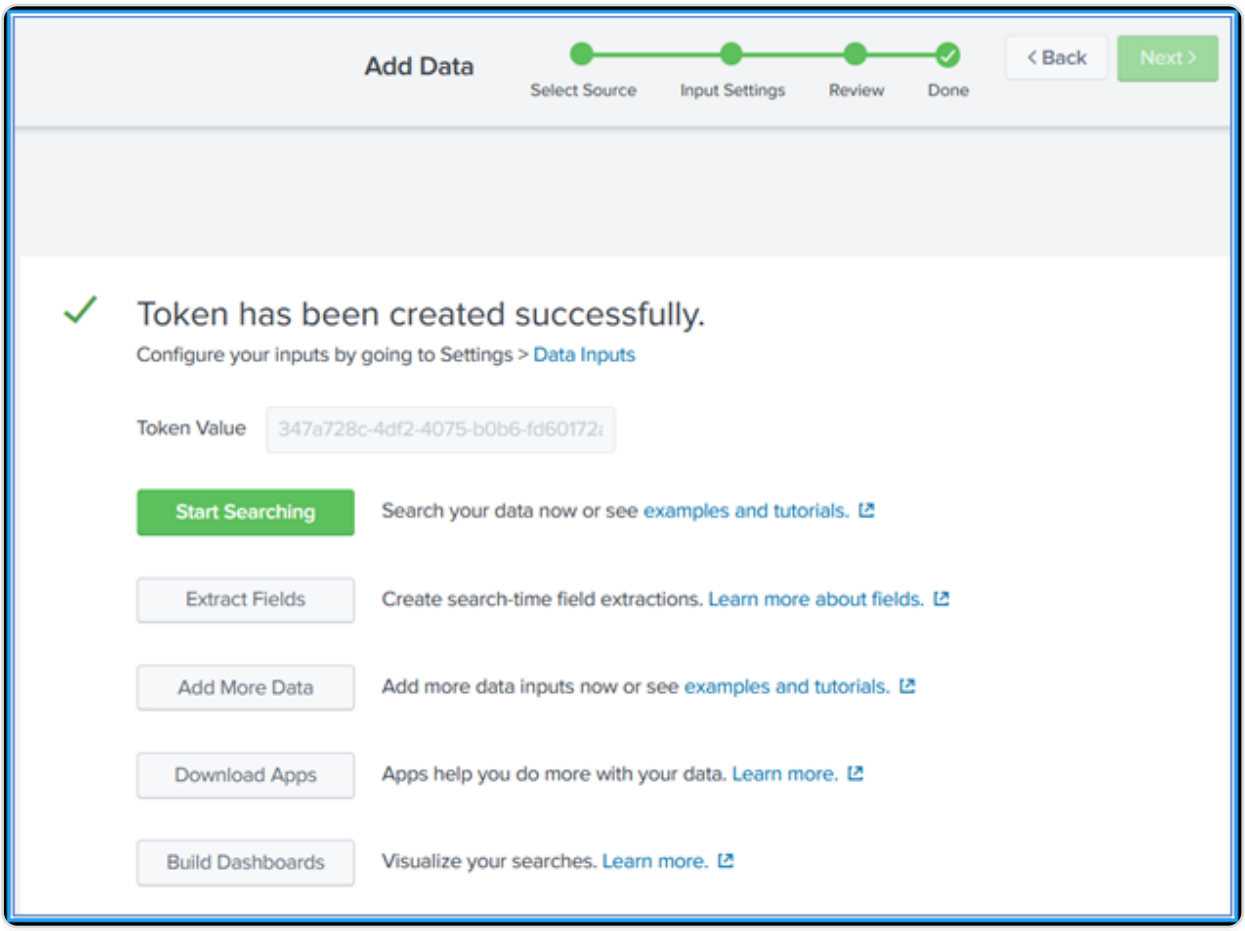


4. Click **Next**.
5. Optionally, you can set additional input parameters in the **Input Settings** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Click **Review** to verify the entries and then click **Submit**.

   A token gets generated. You must use this token when you add details in NetScaler ADM.

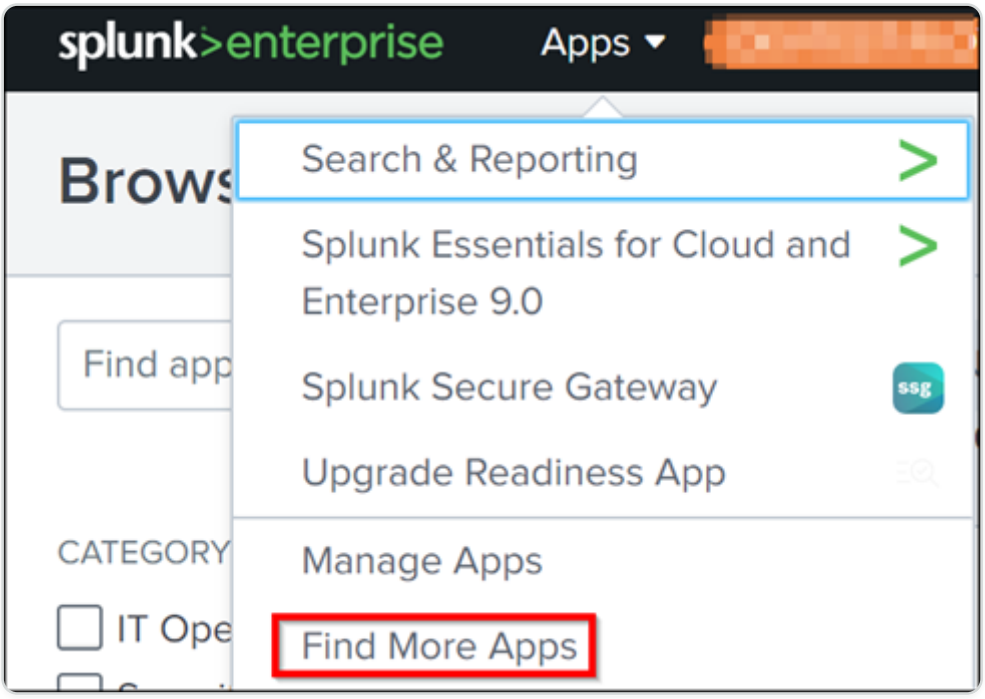


Install the Splunk Common Information Model

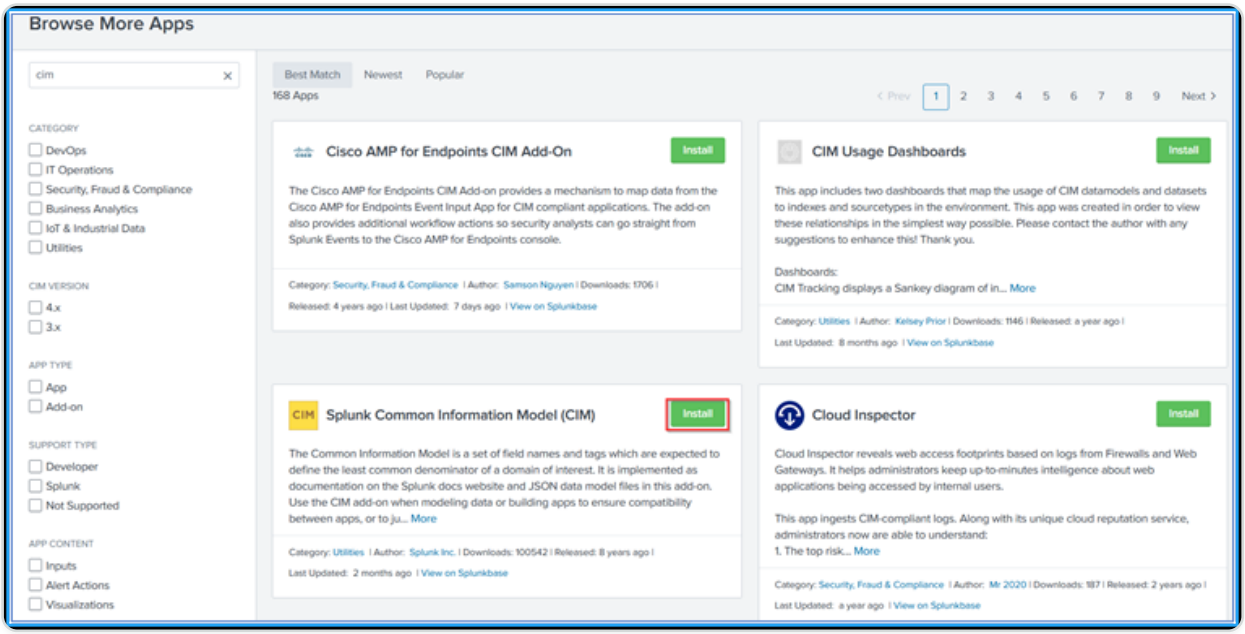
In Splunk, you must install the Splunk CIM add-on. This add-on ensures that the data received from NetScaler ADM to normalize the ingested data and match a common standard using the same field names and event tags for equivalent events.

1. Log on to Splunk.
2. Navigate to **Apps > Find More Apps**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Type **CIM** in the search bar and press **Enter** to get the **Splunk Common Information Model (CIM)** add-on, and click **Install**.



Prepare a sample dashboard in Splunk

After you install the Splunk CIM, you must prepare a sample dashboard using a template for WAF and Bot, and SSL Certificate Insights. You can download the dashboard template (`.tgz`) file, use any editor (for example, notepad) to copy its contents, and create a dashboard by pasting the data in Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

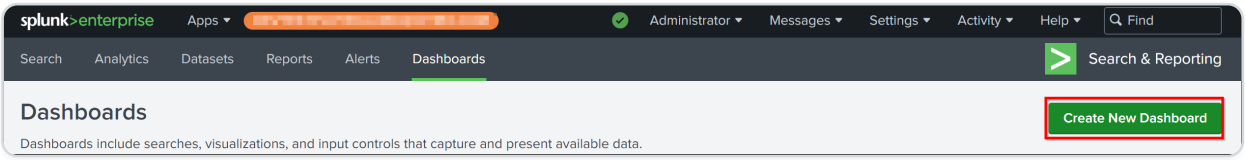
The following procedure to create a sample dashboard is applicable for both WAF and Bot, and SSL Certificate Insights. You must use the required `json` file.

1. Log on to Citrix downloads page and download the sample dashboard available under Observability Integration.
2. Extract the file, open the `json` file using any editor, and copy the data from the file.

   NOTE:

   After you extract, you get two `json` files. Use `adm_splunk_security_violations.json` to create the WAF and Bot sample dashboard, and use `adm_splunk_ssl_certificate.json` to create the SSL certificate insight sample dashboard.

3. In the Splunk portal, navigate to **Search & Reporting > Dashboards** and then click **Create New Dashboard**.



4. In the **Create New Dashboard** page, specify the following parameters:

   a. **Dashboard Title** - Provide a title of your choice.

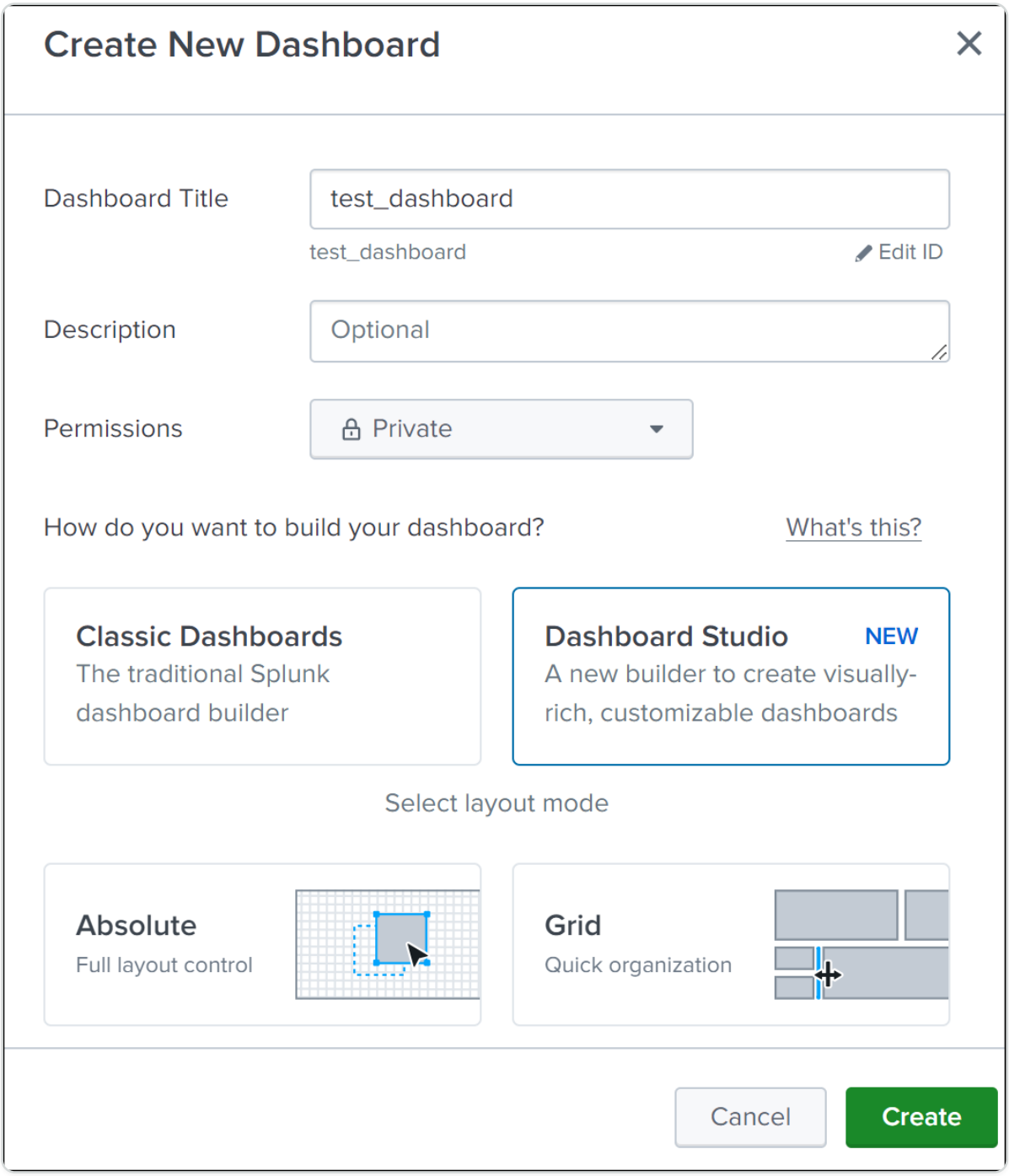
   b. **Description** - Optionally, you can provide a description for your reference.

   c. **Permission** - Select **Private** or **Shared in App** based on your requirement.

   d. Select **Dashboard Studio**.

   e. Select any one layout (**Absolute** or **Grid**), and then click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

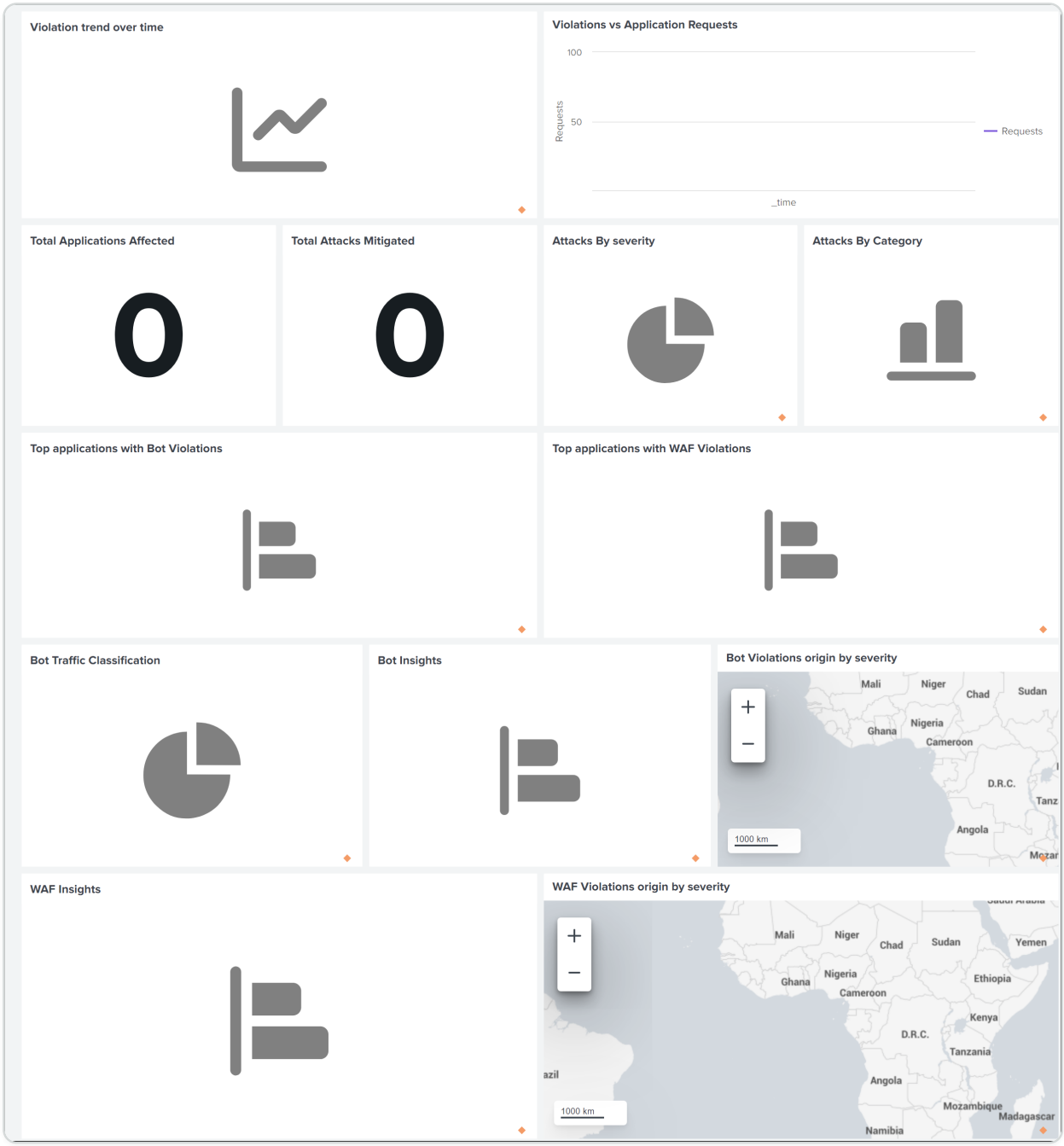


After you click **Create**, select the **Source** icon from the layout.

5. Delete the existing data, paste the data that you copied in step 2, and click **Back**.
6. Click **Save**.

   You can view the following sample dashboard in your Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure NetScaler ADM to export data to Splunk

You now have everything ready in Splunk. The final step is to configure NetScaler ADM by creating a subscription and adding the token.

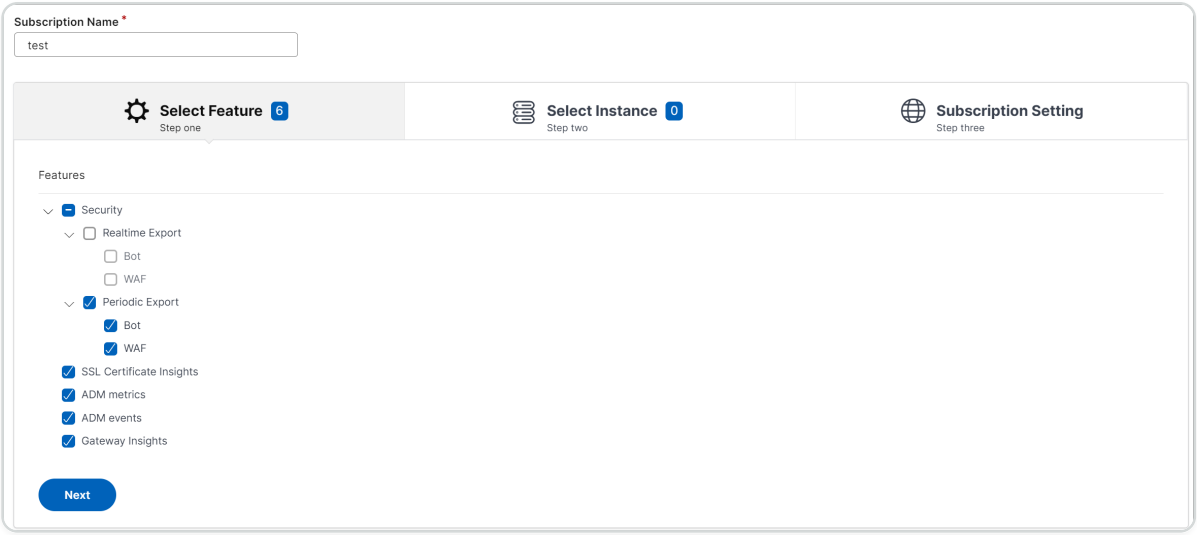
Upon completion of the following procedure, you can view the updated dashboard in Splunk that is currently available in your NetScaler ADM:

1. Log on to NetScaler ADM.
2. Navigate to **Settings > Ecosystem Integration**.
3. In the **Subscriptions** page, click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the **Select features to subscribe** tab, select the features that you want to export and click **Next**.

   - **Realtime Export** - The selected violations are exported to Splunk immediately.
   - **Periodic Export** - The selected violations are exported to Splunk based on the duration you select.



5. In the **Specify export configuration** tab:

   a. **End Point Type** – Select **Splunk** from the list.

   b. **End Point** – Specify the Splunk end point details. The end point must be in the `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` format.

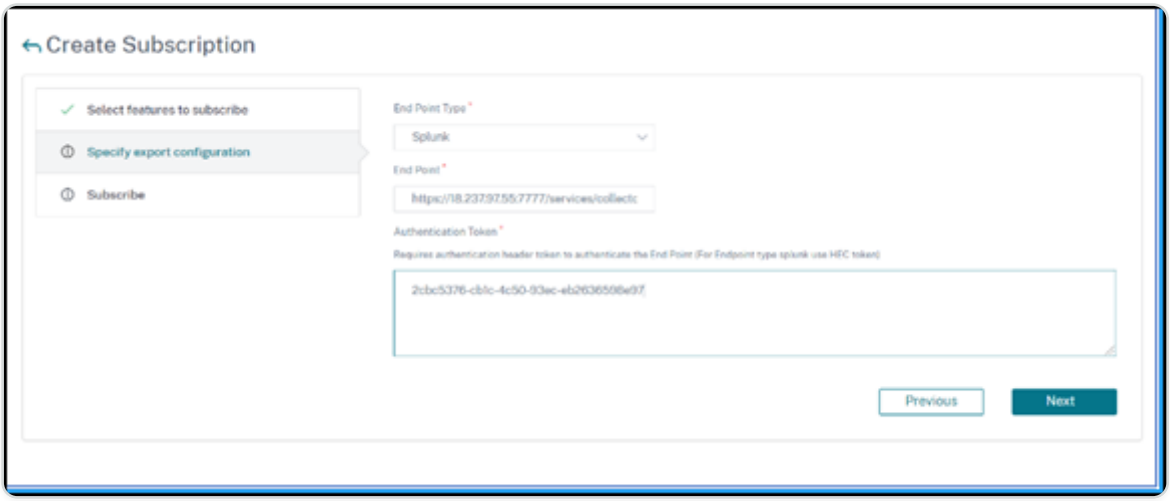
   > **NOTE**
   >
   > It is recommended to use HTTPS for security reasons.

   - **SPLUNK_PUBLIC_IP** – A valid IP address configured for Splunk.
   - **SPLUNK_HEC_PORT** – Denotes the port number that you have specified during the HTTP event endpoint configuration. The default port number is 8088.
   - **Services/collector/event** – Denotes the path for the HEC application.

   c. **Authentication token** – Copy and paste the authentication token from the Splunk page.

   d. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. In the **Subscribe** page:

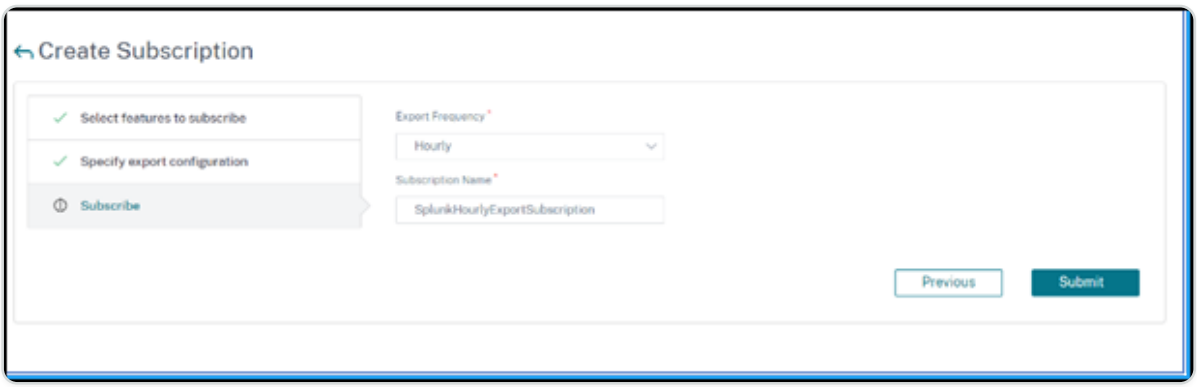
   a. **Export Frequency** – Select Daily or Hourly from the list. Based on the selection, NetScaler ADM exports the details to Splunk.

   > **NOTE:**
   >
   > Applicable only if you have selected violations in **Periodic Export**.

   b. **Subscription Name** – Specify a name of your choice.

   c. Select the **Enable Notifications** check box.

   d. Click **Submit**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- When you configure with **Periodic Export** option for the first time, the selected features data get pushed to Splunk immediately. The next export frequency happens based on your selection (daily or hourly).
- When you configure with **Realtime Export** option for the first time, the selected features data pushed to Splunk immediately when the violations are detected in NetScaler ADM.

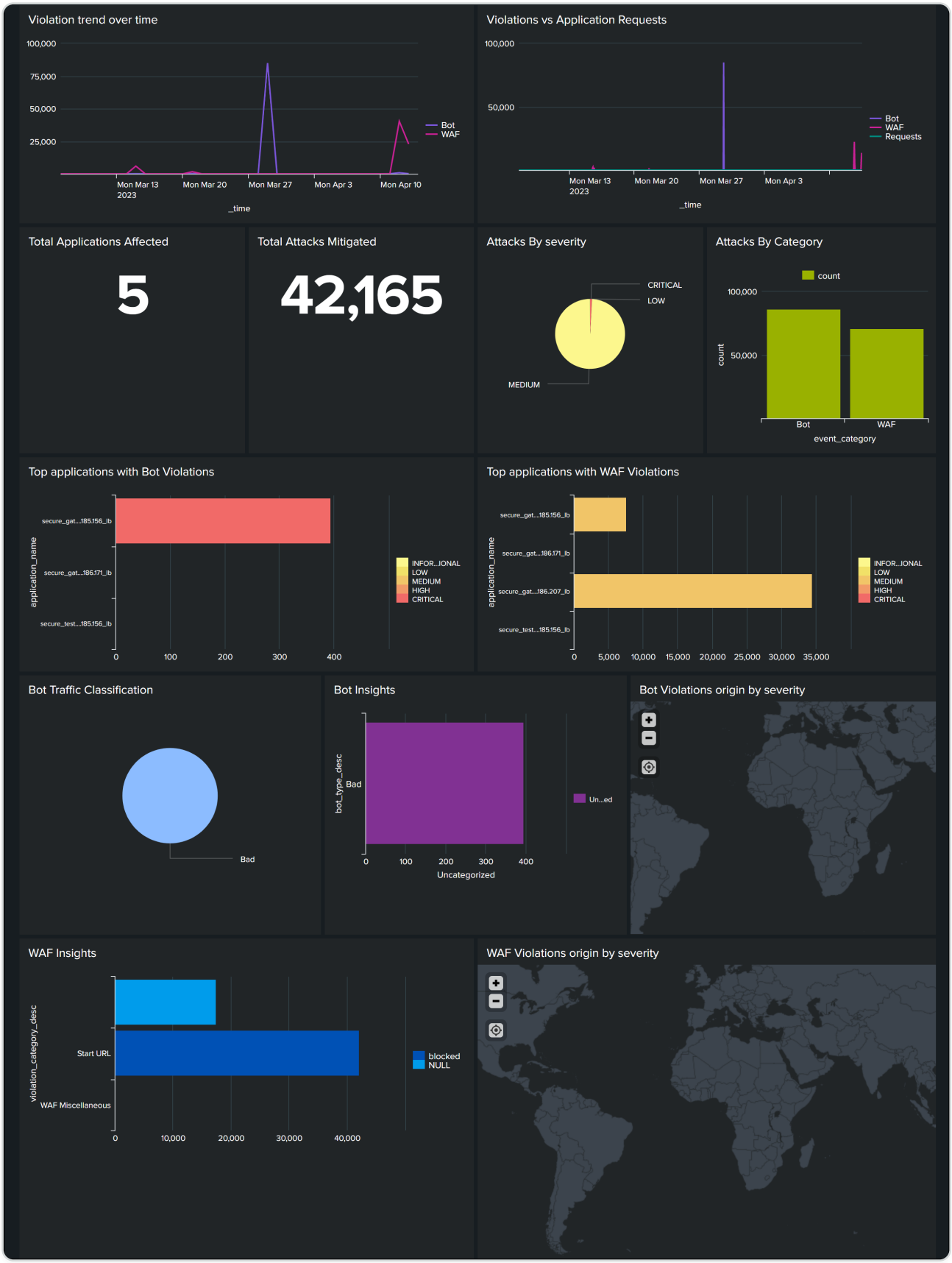
View dashboards in Splunk

After you complete the configuration in NetScaler ADM, the events appear in Splunk. You are all set to view the updated dashboard in Splunk without any additional steps.

Go to Splunk and click the dashboard that you have created to view the updated dashboard.

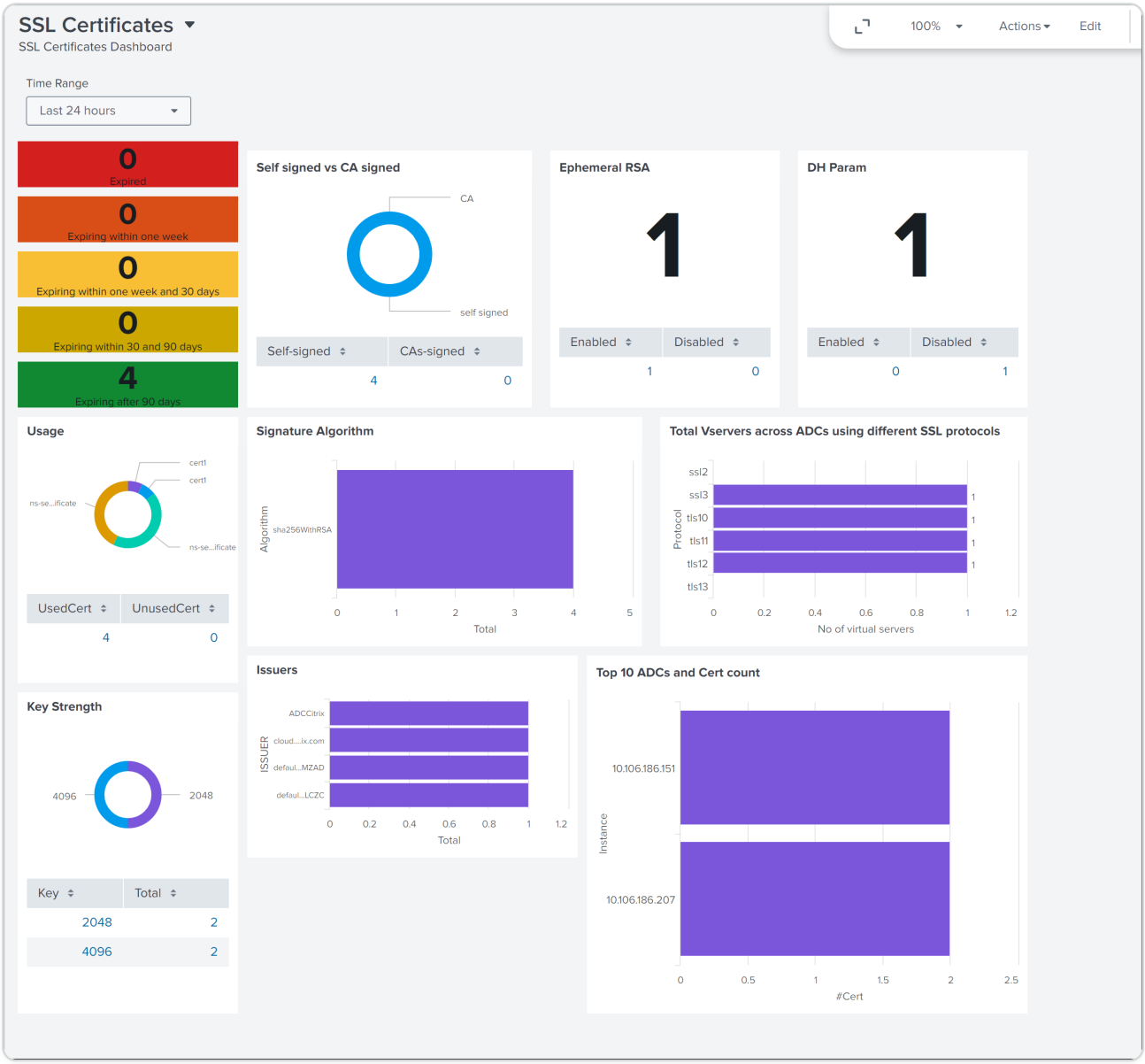
The following is an example for the updated WAF and Bot dashboard:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following dashboard is an example for the updated SSL Certificate Insights dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Integration with New Relic

You can now integrate NetScaler® ADM with New Relic to view analytics for WAF and Bot violations in your New Relic dashboard. With this integration, you can:

- Combine all other external data sources in your New Relic dashboard.
- Get visibility of analytics in a centralized place.

NetScaler ADM collects Bot and WAF events, and sends them to New Relic either in real time or periodically based on your choice. As an administrator, you can also view the Bot and WAF events in your New Relic dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

For a successful integration, you must:

- Obtain a New Relic event endpoint in the following format:

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```

  For more information on configuring an event endpoint, see New Relic documentation.

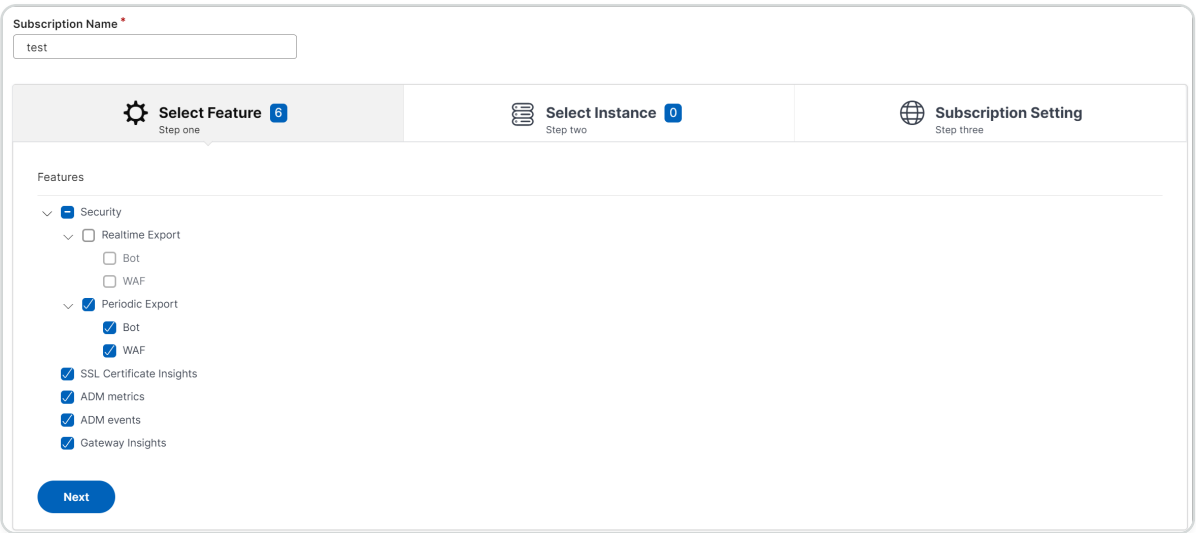
  For more information on getting an account ID, see New Relic documentation.
- Obtain a New Relic key. For more information, see New Relic documentation.
- Add the key details in NetScaler ADM

Add the key details in NetScaler ADM

After you generate a token, you must add details in NetScaler ADM to integrate with New Relic.

1. Log on to NetScaler ADM.
2. Navigate to **Settings > Ecosystem Integration**.
3. In the **Subscriptions** page, click **Add**.
4. In the **Select features to subscribe** tab, select the features that you want to export and click **Next**.

   - **Realtime Export** - The selected violations are exported to New Relic immediately.
   - **Periodic Export** - The selected violations are exported to New Relic based on the duration you select.



5. In the **Specify export configuration** tab:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

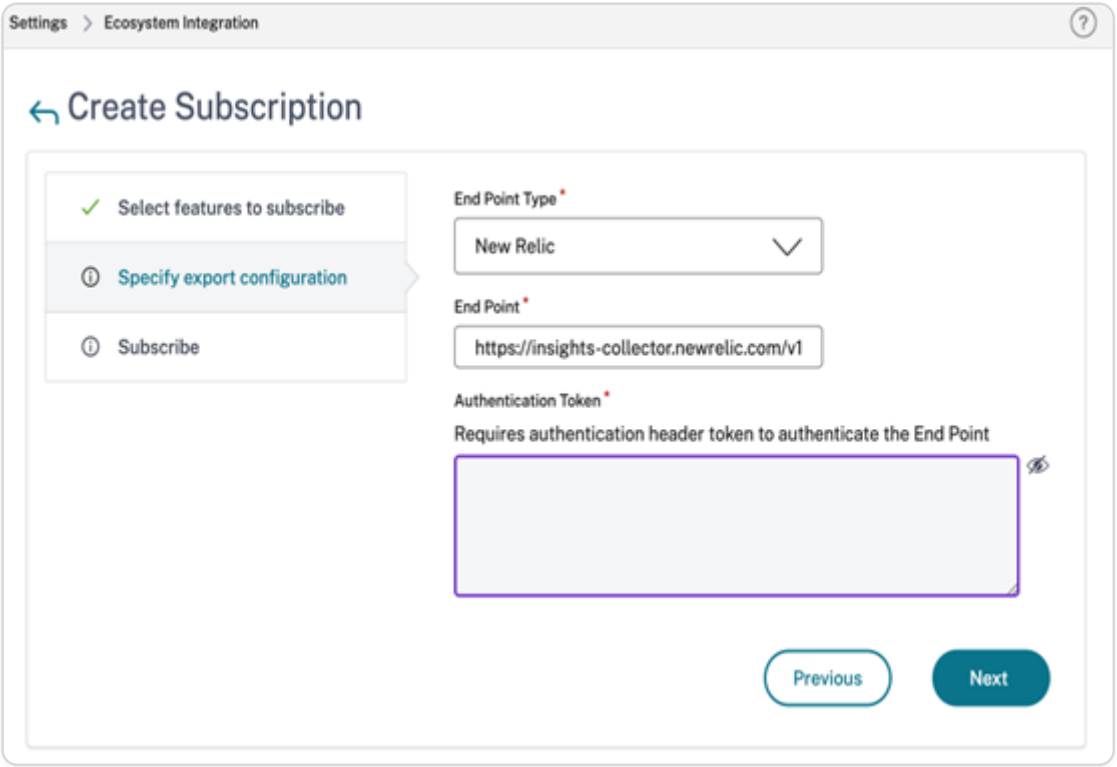
a. **End Point Type** – Select **New Relic** from the list.

b. **End Point** – Specify the New Relic end point details. The end point must be in the `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` format.

> **NOTE**
>
> It is recommended to use HTTPS for security reasons.

c. **Authentication token** – Copy and paste the authentication token from the New Relic page.

d. Click **Next**.



6. In the **Subscribe** page:

a. **Export Frequency** – Select Daily or Hourly from the list. Based on the selection, NetScaler ADM exports the details to New Relic.

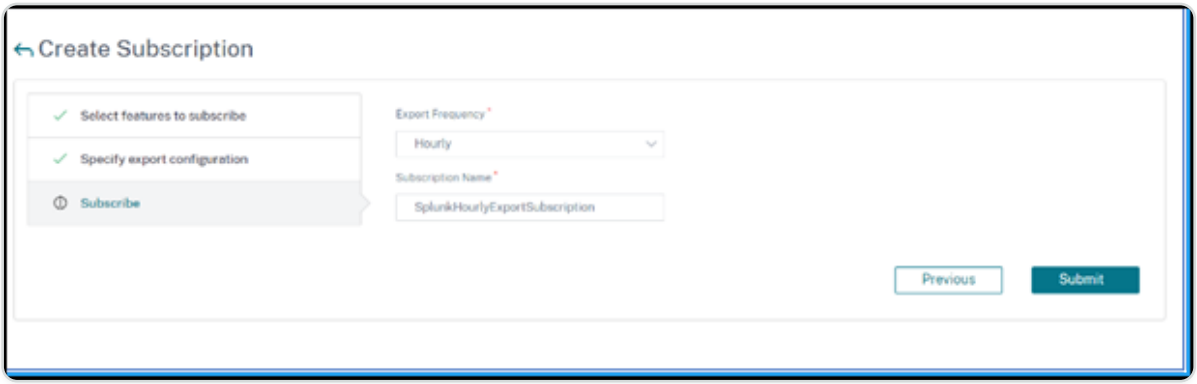
> **NOTE**
>
> Applicable only if you have selected violations in **Periodic Export**.

b. **Subscription Name** – Specify a name of your choice.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Select the **Enable Notifications** check box.

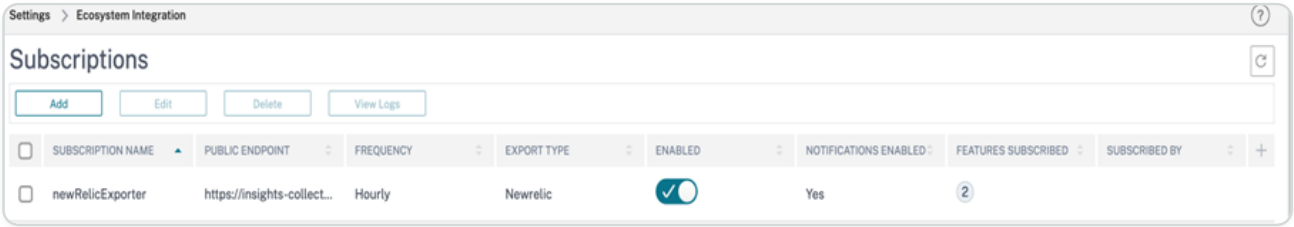
d. Click **Submit**.



NOTE

- When you configure with **Periodic Export** option for the first time, the selected features data get pushed to New Relic immediately. The next export frequency happens based on your selection (daily or hourly).
- When you configure with **Realtime Export** option for the first time, the selected features data pushed to New Relic immediately as soon as the violations are detected in NetScaler ADM.

The configuration is complete. You can view details in the **Subscriptions** page.



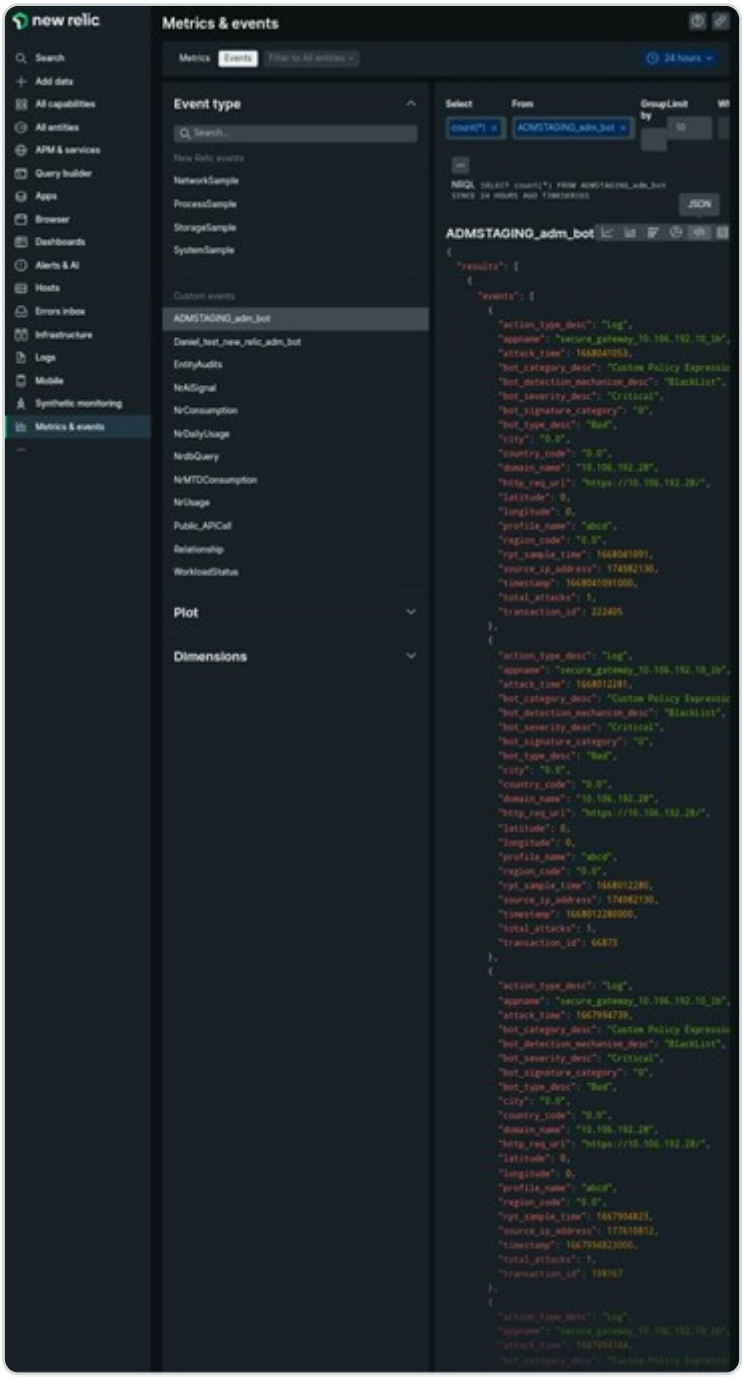
New Relic dashboard

When the events are exported in New Relic, you can view event details under **Metrics & events** in the following JSON format:

`<subsription_name>_adm_<event name>` where event name can be Bot, WAF, and so on.

In the following example, ADMSTAGING is the `<subscription_name>` and bot is the `<event_name>`.

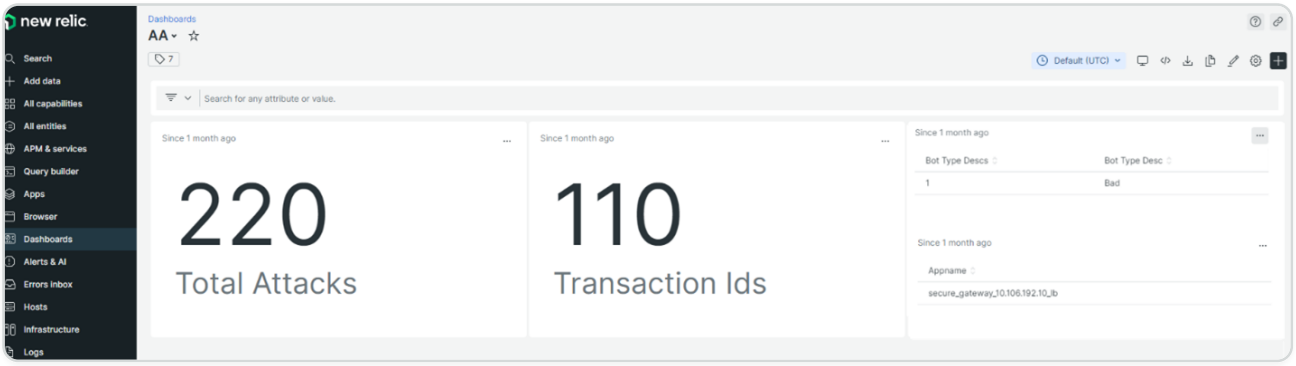
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once you get the JSON data ingested into your New Relic dashboard, as an administrator, you can use the NRQL (New Relic Query Language) and create a custom dashboard with facets and widgets based on your choice by constructing queries around the ingested data. For more information, see `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

The following is an example dashboard created using the NRQL:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To create this dashboard, the following queries are required:

- Widget 1: Total Unique Attacks in events table

  `SELECT count(total_attacks) from <event_name> since 30 days ago`

- Widget 2: Unique Transaction IDs in event table

  `SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago`

- Widget 3: Total Unique Bot Types and their counts

  `SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago`

- Widget 4: Total unique App Names seeing Bot Violations

  `SELECT uniques(appname) from <event_name> since 30 days ago`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway

NetScaler Console provides gateway analytics that give you visibility into the performance and user experience of traffic served through NetScaler Gateway. The following topics help you monitor and troubleshoot gateway traffic:

- Gateway Insight
- HDX Insight

Gateway Insight

In a NetScaler Gateway deployment, visibility into a user's access details is essential for troubleshooting access failure issues. As a network administrator, you want to know when a user is not able to log on to NetScaler Gateway, and you want to know the user activity and the reasons for logon failure. This information is typically not available unless the user sends a request for resolution.

Gateway Insight provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway. You can view a list of all available users, number of active users, number of active sessions, and bytes and licenses used by all users at any given time. You can view the end-point analysis (EPA), authentication, single sign-on (SSO), and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

Gateway Insight also provides visibility into the reasons for application launch failure for virtual applications. This enhances your ability to troubleshoot any kind of logon or application launch failure issues. You can view the number of applications launched, the number of total and active sessions, the number of total bytes, and the bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All log messages are stored in the NetScaler® ADM database, so you can view error details for any time period. You can also view a summary of the logon failures and determine at what stage of the logon process a failure has occurred.

Points to note

- Gateway Insight is supported on the following deployments:
  - Access Gateway
  - Unified Gateway
- The NetScaler ADM release and build must be the same or later than that of the NetScaler Gateway appliance.
- One hour of Gateway Insight reports can be viewed for NetScaler instances with Advanced license. A Premium license is a must view Gateway Insight reports beyond one hour.

Limitations

- NetScaler Gateway does not support Gateway Insight when the authentication method is configured as certificate-based authentication.
- For Gateway Insight reporting, geo location information is not provided from the NetScaler appliance.
- Successful user logons, latency, and application-level details for virtual ICA applications and desktops are visible only on the HDX™ Insight Users dashboard.
- In a double-hop mode, visibility into failures on the NetScaler Gateway appliance in the second DMZ is not available.
- Remote Desktop Protocol (RDP) desktop access issues are not reported.
- Gateway Insight is supported for the following authentication types. If other authentication type is used other than these, you might see some discrepancies in Gateway Insight.
  - Local
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Native OTP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- OAuth-OpenID Connect

  For the OAuth-OpenID Connect authentication, NetScaler can act as an OAuth-OpenID connect relying party (RP) or OAuth-OpenID connect identity provider (IdP). When the authentication succeeds, the user name is reported under the Users tab in the Gateway Insight report. However, you cannot identify whether the session was created at IdP or RP.

  Note: OAuth-OpenID Connect authentication is supported from NetScaler ADM release 13.1 build 4.xx and later.

Enable Gateway Insight

To enable Gateway Insight for your NetScaler Gateway appliance, you must first add the NetScaler Gateway appliance to NetScaler ADM. You must then enable AppFlow for the virtual server representing the VPN application. For information about adding device to NetScaler ADM, see Adding Devices.

NOTE

To view end-point analysis (EPA) failures in NetScaler ADM, you must enable AppFlow authentication, authorization, and auditing user name logging on the NetScaler Gateway appliance.

The following procedure to enable gateway insight is applicable if your NetScaler ADM is **13.0 Build 36.27**:

1. Navigate to **Infrastructure > Instances**, and select the instance for which you want to enable AppFlow.
2. From the **Select Action** list, select **Configure Analytics**.
3. In the **Configure Insight** page, under **Configure Analytics**, select **NetScaler Gateway**.
4. Select the virtual server and then click **Enable AppFlow**.
5. On the **Enable AppFlow** screen, in the **Select Expression** list, click true.
6. Next to **Transport Mode**, select the **Logstream** check box.

   NOTE

   You can choose either **IPFIX** or **Logstream** as transport mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

7. Click **OK**.

For NetScaler ADM version 13.0 Build 41.x or later

1. Navigate to **Infrastructure > Instances**, and select the instance.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the virtual server and click **Enable Analytics**.
4. Under **Advanced Options**:
   a. Select **Logstream**
   b. Select **NetScaler Gateway**
5. Click **OK**.

Enable AppFlow authentication, authorization, and auditing user name logging on a NetScaler Gateway appliance by using the GUI

1. Navigate to **Configuration > System > AppFlow > Settings**, and then click **Change AppFlow Settings**.
2. In the **Configure AppFlow Settings** screen, select **AAA Username**, and then click **OK**.

Viewing Gateway Insight reports

In NetScaler ADM, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the **Overview** section, you can view the EPA, SSO, Authentication, and Application Launch failures. You can also view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.

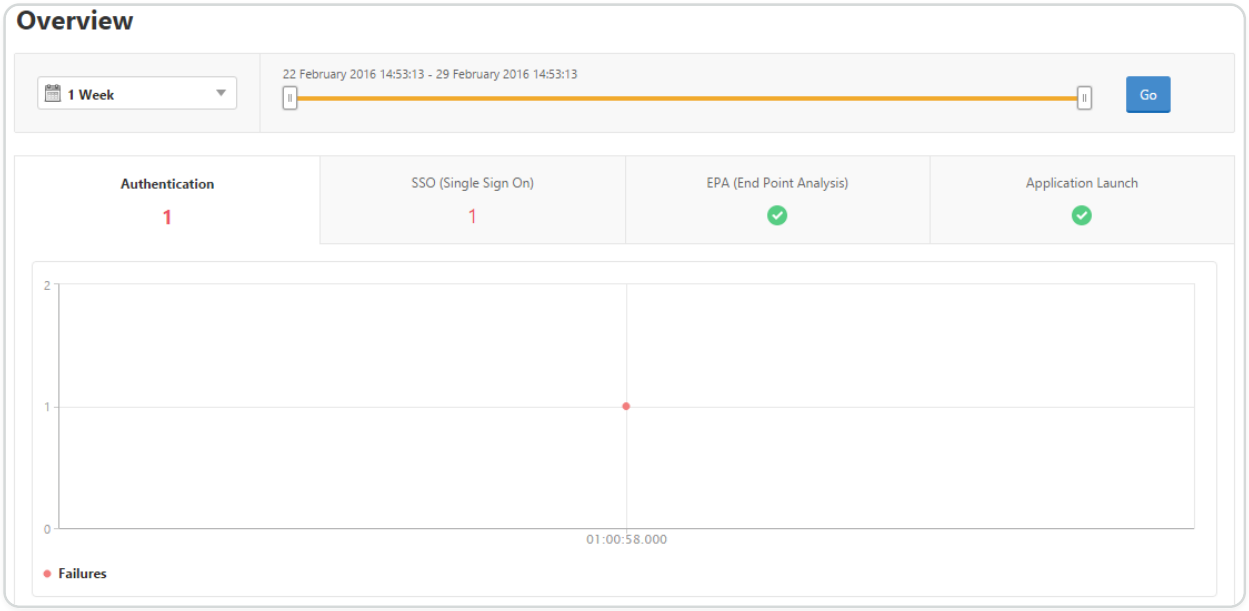
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

To view EPA, SSO, authentication, authorization, and application launch failures

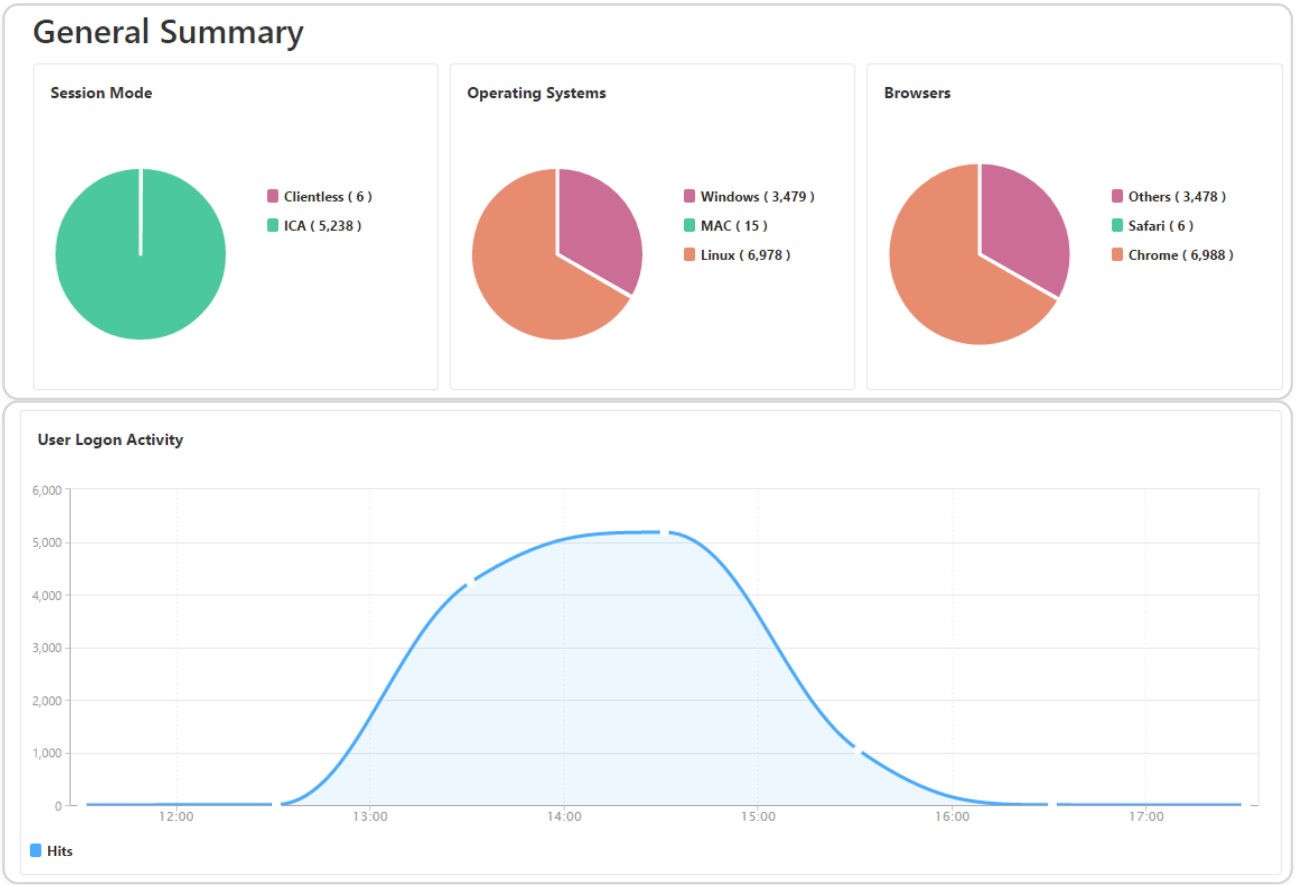
1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.



To view a summary of session modes, clients, and the number of users

In NetScaler ADM, navigate to **Gateway > Gateway Insight**, scroll down to view the reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Viewing Gateway Insight reports for users

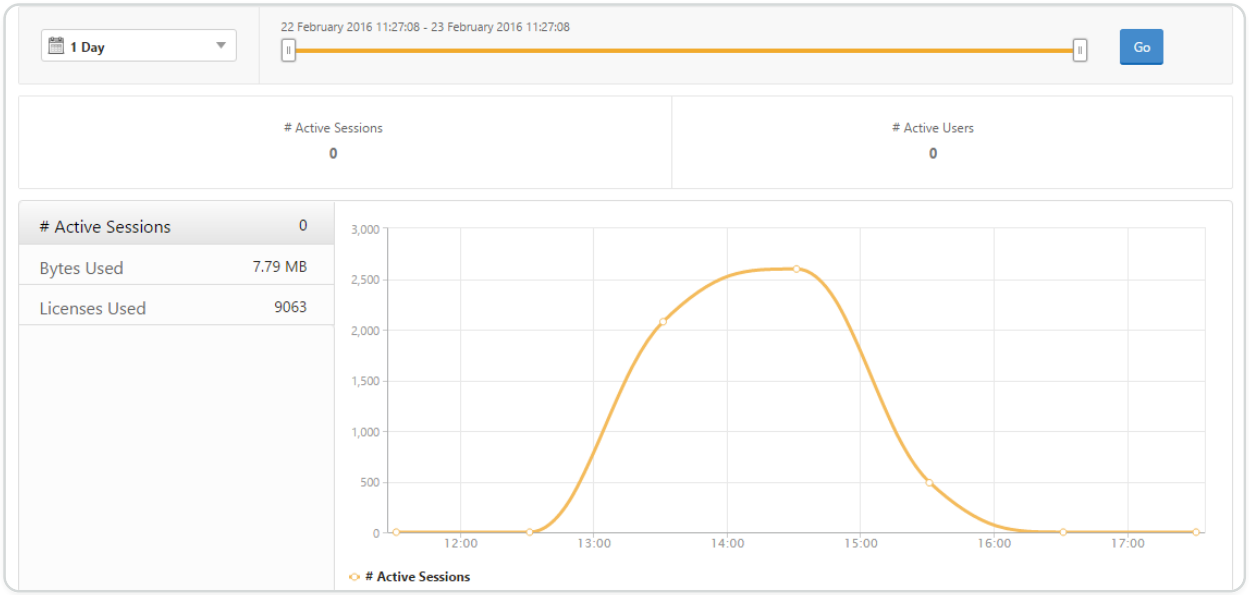
You can view the reports for:

- All users associated with the NetScaler Gateway appliances.
- The EPA, authentication, SSO, and application launch failures for a user.
- The details of active and terminated sessions for a user.
- The types of session modes such as Full Tunnel, clientless VPN, and ICA® Proxy.

To view user details

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight > Users**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. You can view the number of active users, number of active sessions, bytes, and licenses used by all users during the time period.

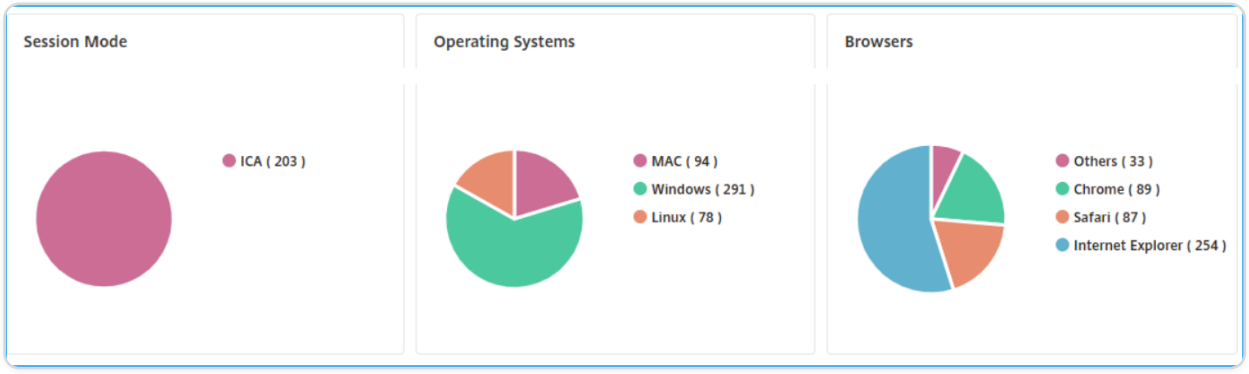
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Scroll down to view a list of available users and active users.

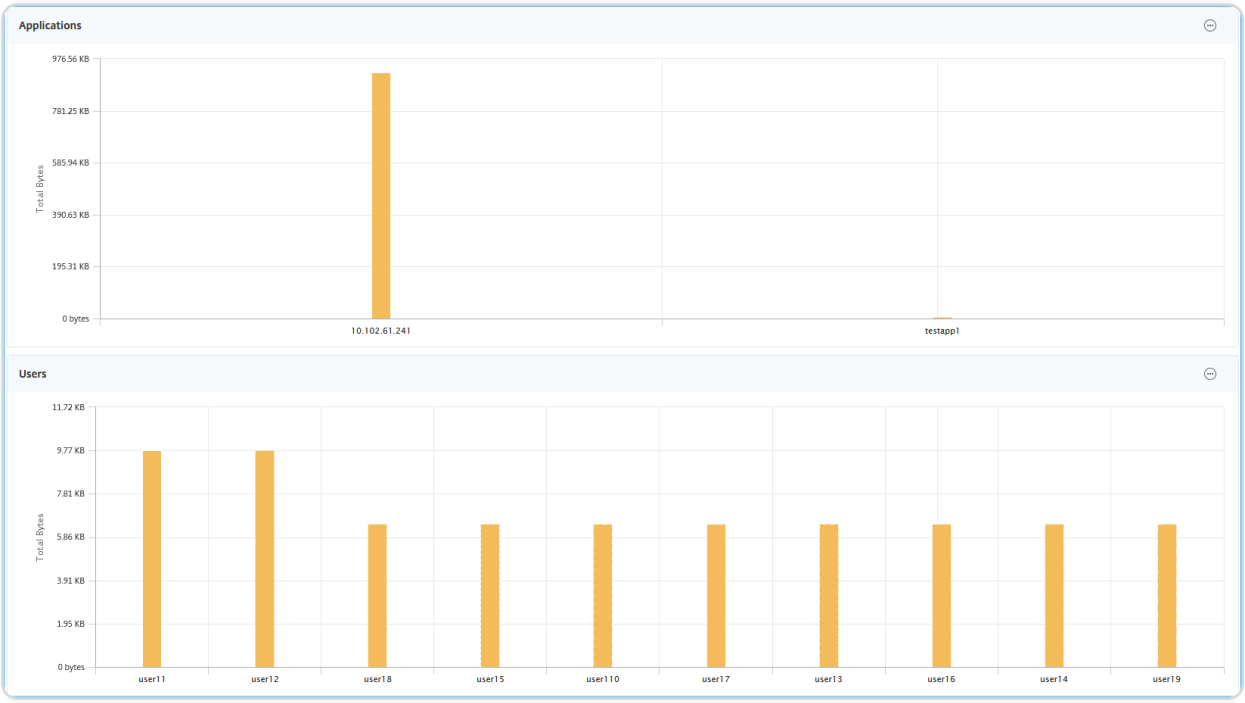
On the **Users** or **Active Users** tab, click a user to view the following user details:

- **User details** - You can view insights for each user associated with the ADC Gateway appliances. Navigate to **Gateway** > **Gateway Insight** > **Users** and click a user to view insights for the selected user such as Session Mode, Operating System, and Browsers.

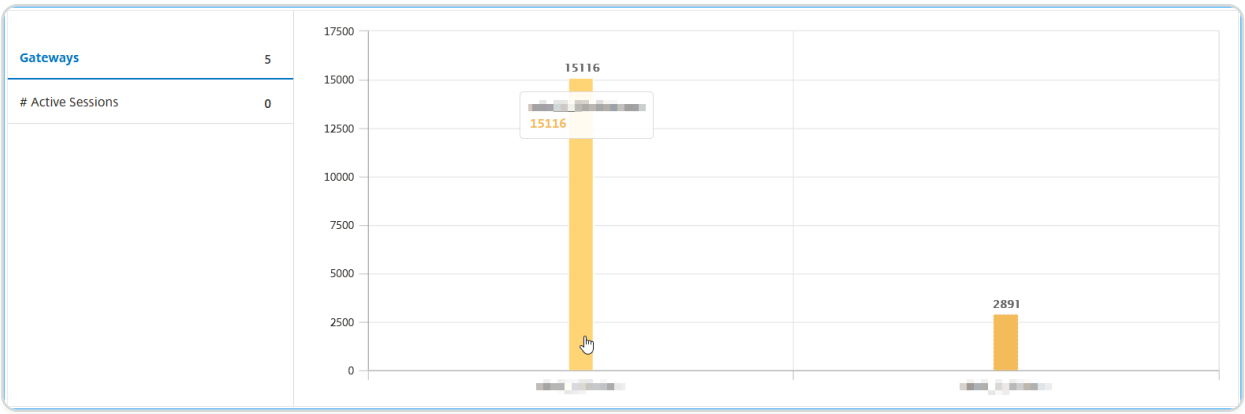


- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.

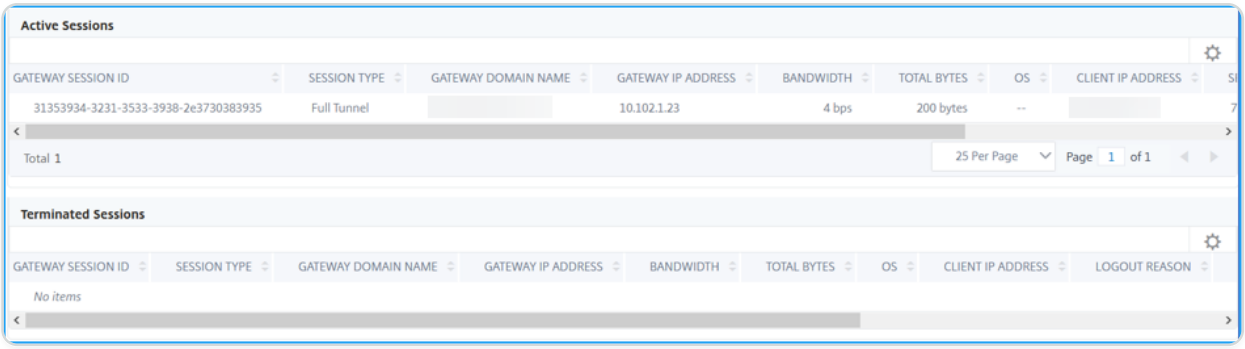
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **View more option for applications and users** – For more than 10 applications and users, you can click the more icon in Applications and Users to view all users and applications details that are associated with the selected gateway.
- **View details by clicking the bar graph** – When you click a bar graph, you can view the relevant details. For example, navigate to **Gateway > Gateway Insight > Gateway** and click the gateway bar graph to view the gateway details.

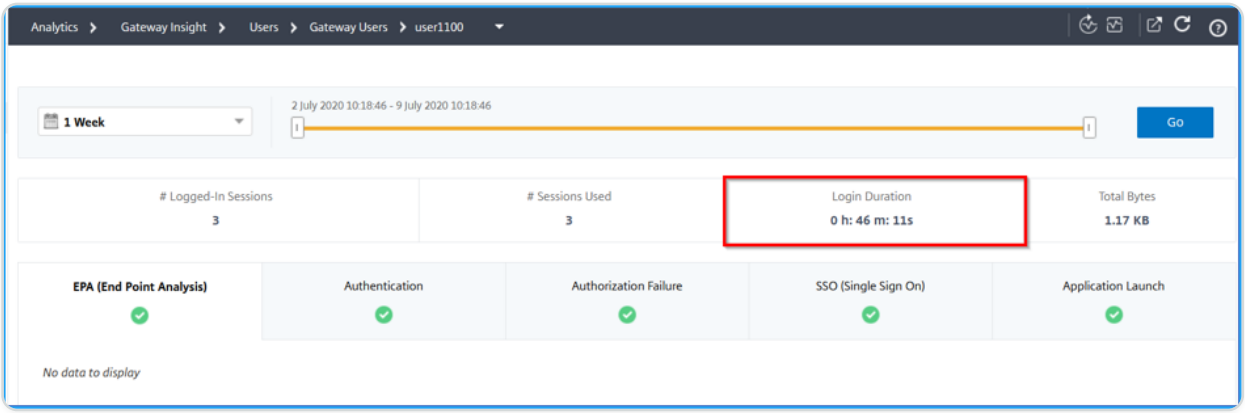


- The user **Active Sessions** and **Terminated Sessions**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The gateway domain name and gateway IP address in **Active Sessions**.
- The user login duration.



- The reason for the user logout session. The logout reasons can be:
  - Session timed out
  - Logged out because of internal error
  - Logged out because of inactive session timed out
  - User has logged out
  - Administrator has stopped the session

Viewing Gateway Insight reports for applications

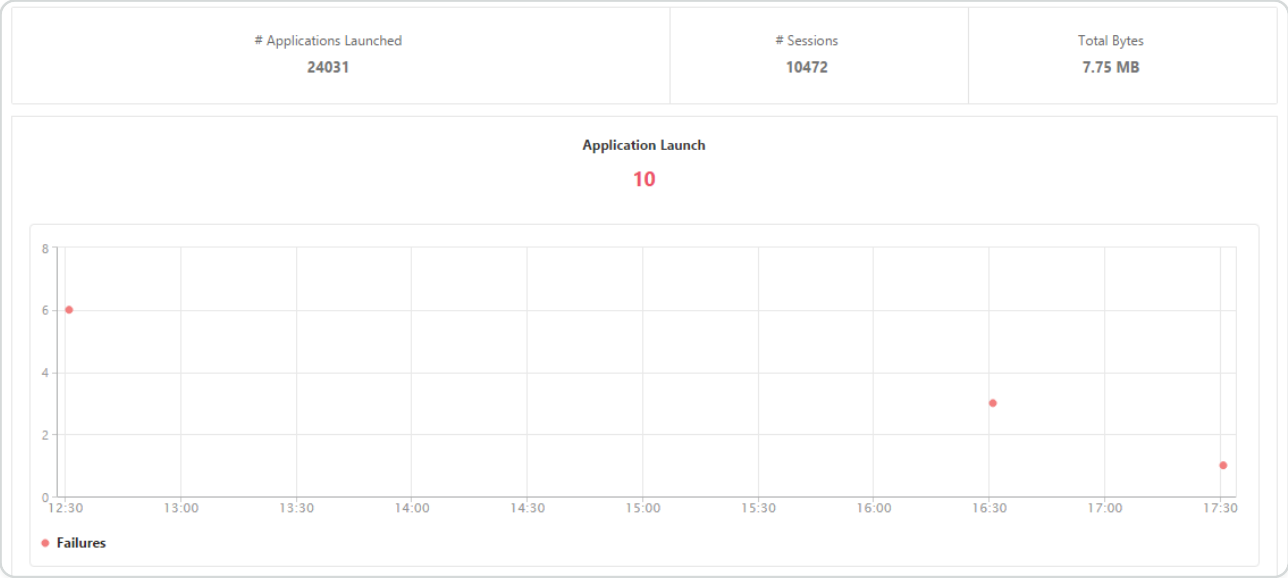
You can view the number of applications launched, the number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

To view application details

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight > Applications**.
2. Select the time period for which you want to view the application details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of applications launched, the number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Scroll down to view the numbers of sessions, bandwidth, and total bytes consumed by ICA and other applications.

ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

On the **Other Applications** tab, you can click an application in the **Name** column to display details of that application.

Viewing Gateway Insight reports for gateways

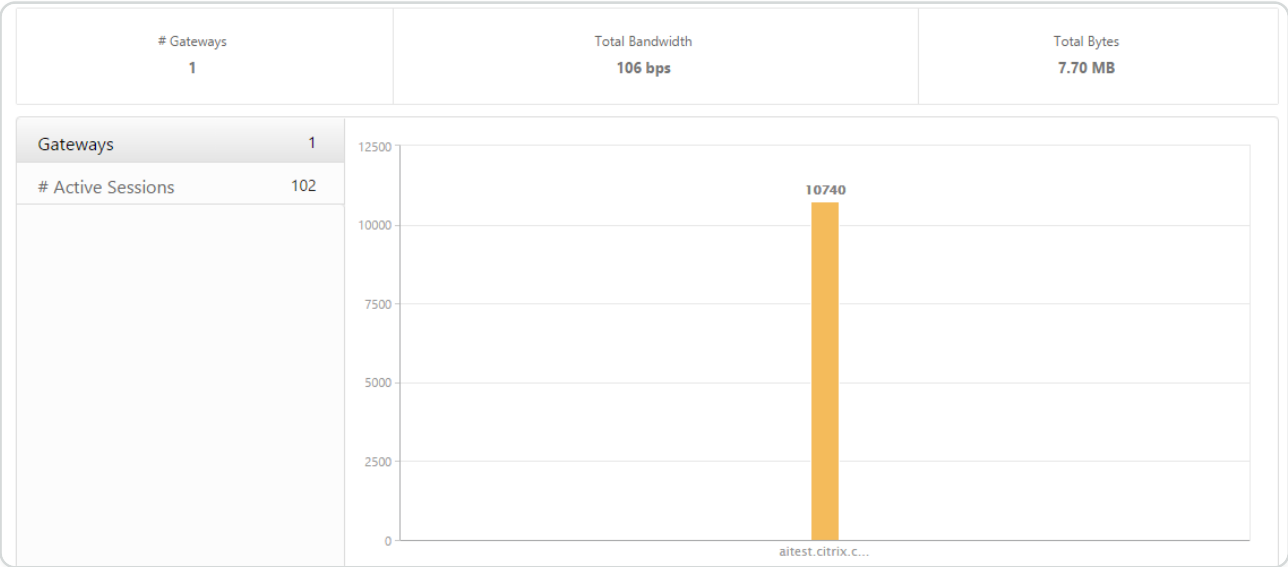
You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

To view gateway details

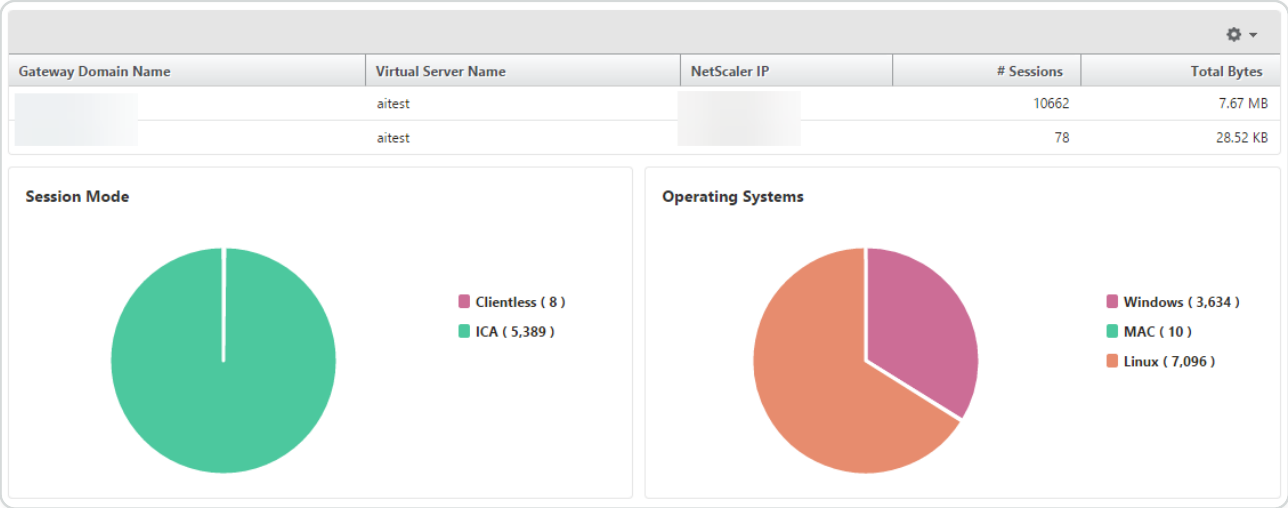
1. In **NetScaler ADM**, navigate to **Gateway > Gateway Insight > Gateways**.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click **Go**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can now view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time.



Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, NetScaler IP address, session modes, and Total Bytes.



You can click a gateway in the **Gateway Domain Name** column to display the EPA, authentication, single sign-on, and application launch failures and other details for a gateway.

Exporting reports

You can save the Gateway Insight reports with all the details shown in the GUI in PDF, JPEG, PNG, or CSV format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- Users with read only access cannot export reports.
- Geo map reports are exported only if the NetScaler ADM has internet connectivity.

To export a report

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select the required format, and then click **Export**.

To schedule export:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Schedule Export**, specify the details and click **Schedule**.

To add an email server or an email distribution list:

1. On the **Configuration** tab, navigate to **Settings > Notifications > Email**.
2. In the right pane, select **Email Server**, to add an email server, or select **Email Distribution list** to create an email distribution list.
3. Specify the details and click **Create**.

To export the entire Gateway Insight dashboard:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select **PDF** format, and then click **Export**.

Gateway Insight use cases

The following use cases show how you can use Gateway Insight to gain visibility into users' access details, applications, and gateways on NetScaler Gateway appliances.

A user is not able to log in to the NetScaler Gateway appliance or to the internal web servers

You are a NetScaler Gateway administrator monitoring NetScaler Gateway appliances through NetScaler ADM, and you want to see why a user is unable to log in, or at what stage of the login process the failure has occurred.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM enables you to view the user login error details in the following stages of the login process:

- Authentication
- End-point analysis (EPA)
- Single sign-on

In NetScaler ADM, you can search for a particular user and then view all the details for that user.

To search for a user:

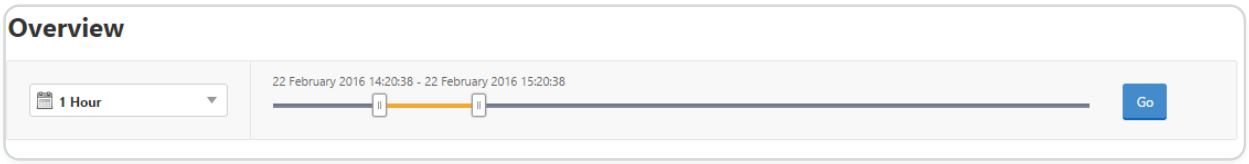
In NetScaler ADM, navigate to **Gateway > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

Authentication failures

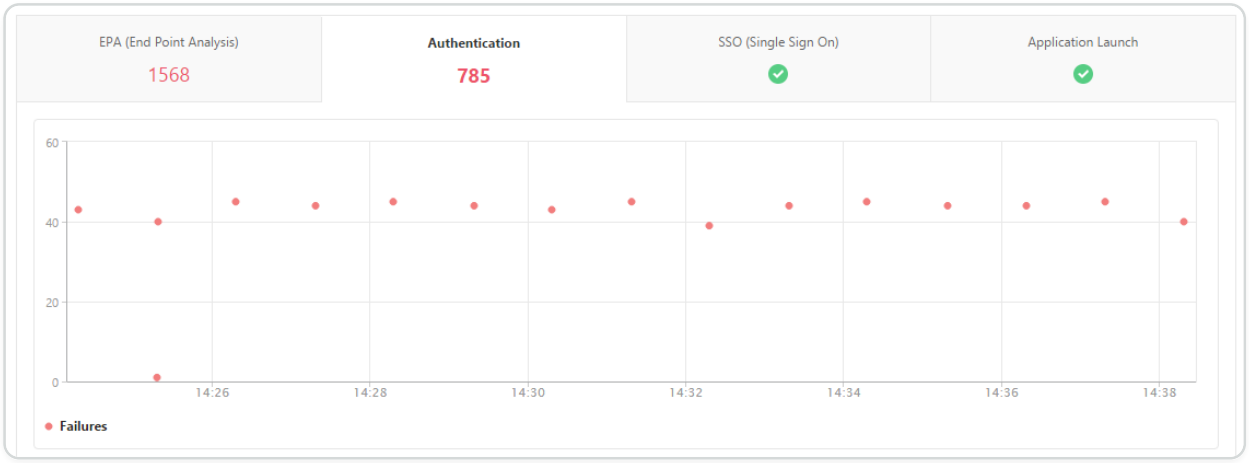
You can view authentication errors such as incorrect credentials or no response from the authentication server. You can also see the factor at which the authentication failed.

To view the authentication failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the authentication errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scroll down to view details of each authentication error such as **Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address**, and more from the table on the same tab. The **Error Description** column in the table displays the reason for the logon failure, and the **State** column displays the nth factor at which the failure occurred.

IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
5.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

You can click a user in the **Username** column to display the authentication errors and other details for that user. You can customize the table to add or delete columns by using the settings icon.

IMPORTANT:

If OAuth-OpenID Connect authentication fails, the user name is displayed as **NA** in the Gateway Insight report for some of the failures, for example "Token verification failure". In this failure, the user names are not available for authentication failure due to "Token verification failure" at the OAuth-OpenID connect relying party.

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-				gitest.citrix.com		Relying party: Token verification failed
-NA-				gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token decryption failure

EPA failures

You can view EPA failures at the pre-authentication or post-authentication stage.

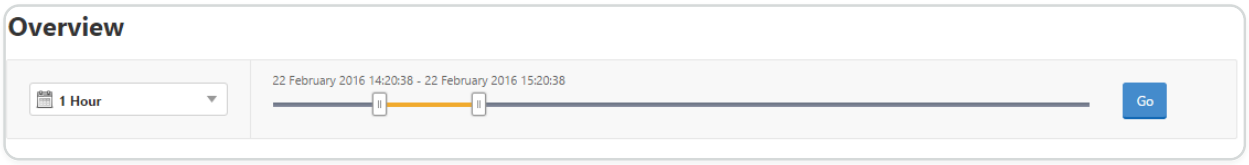
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

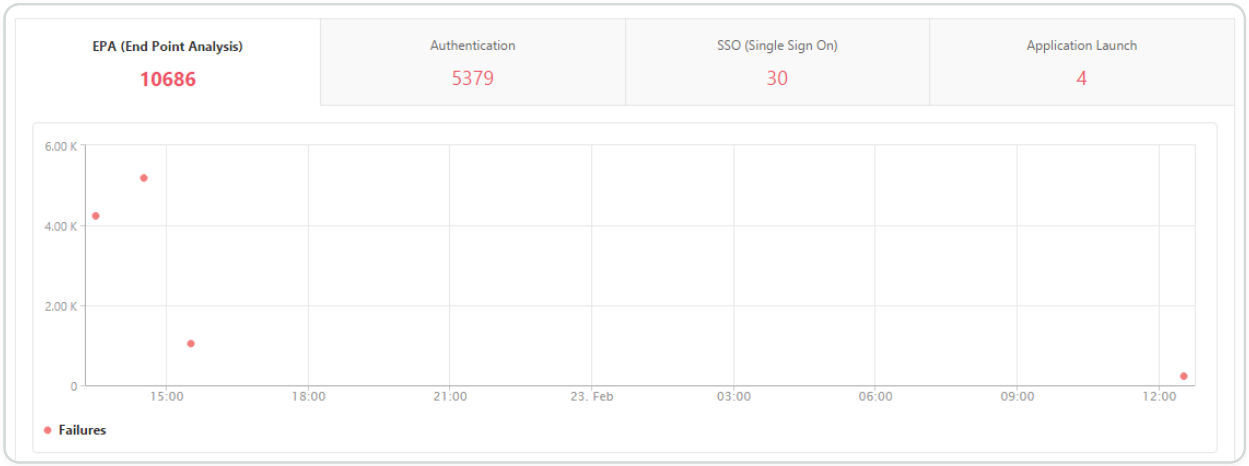
- EPA failures are reported only when classic expressions are configured.
- EPA failures are not reported if advanced expression is configured in the pre-authentication or post-authentication policy.
- EPA failures are not reported if EPA is configured as one of the factors in an nFactor authentication flow.

To view EPA failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **EPA (End Point Analysis)** tab. You can view the number of EPA errors at any given time in the **Failures** graph.



Scroll down to view details of each EPA error such as **Username, NetScaler IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name** and more from the table on the same tab. The **Error Description** column in the table displays the reason for the EPA failure, and the **Policy Name** column displays the policy that resulted in the failure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

You can click a user in the **Username** column to display the EPA errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

NOTE

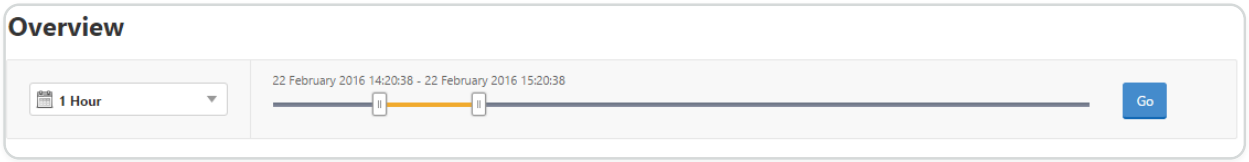
NetScaler Gateway doesn't report the EPA failures when the "clientSecurity" expression is configured as a VPN session policy rule.

SSO failures

You can view the all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

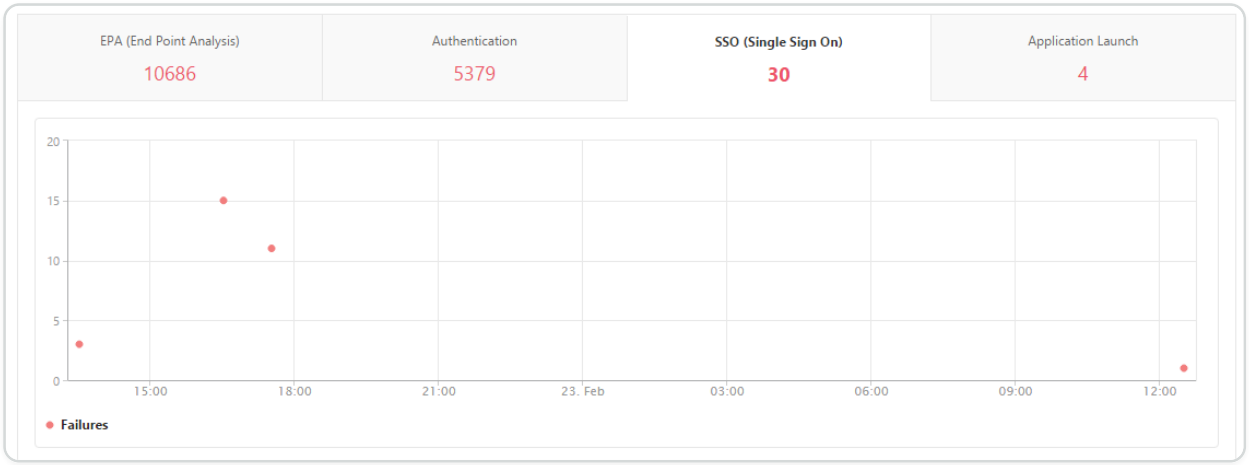
To view the SSO failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Scroll down to view details of each SSO error such as **Username, NetScaler IP Address, Error Time, Error Description, Resource Name** and more from the table on the same tab.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

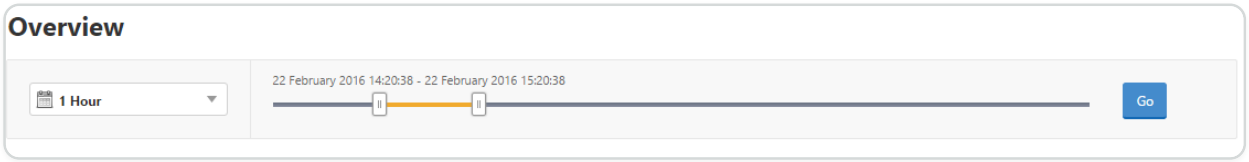
You can click a user in the **Username** column to display the SSO errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

After successfully logging on to NetScaler Gateway, a user is not able to launch any virtual application

For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or Citrix Virtual App server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

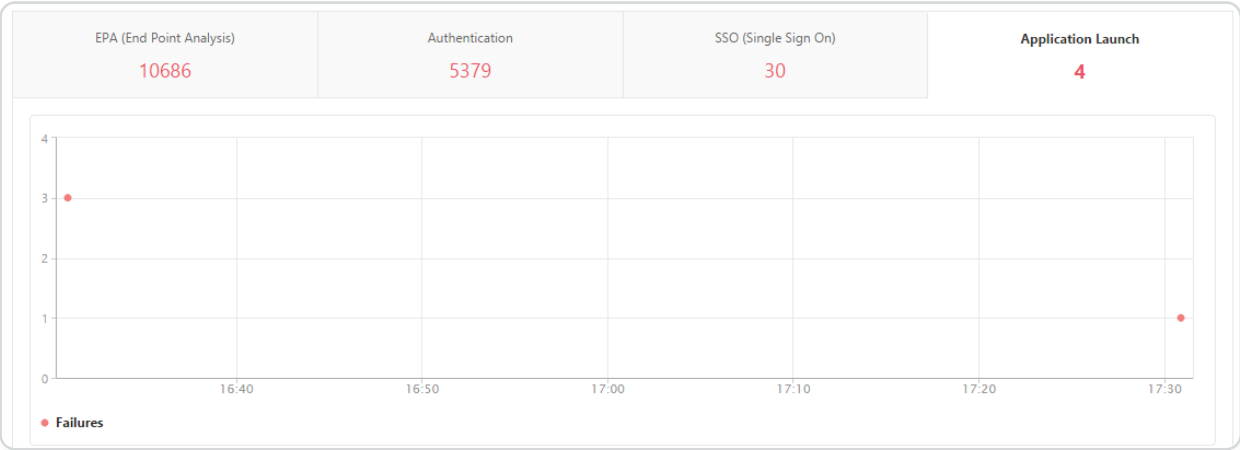
To view the application launch failure details:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click the **Application Launch** tab. You can view the number of application launch failures at any given time in the **Failures** graph.



Scroll down to view details of each application launch error, such as **NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, and more, from the table on the same tab. The **Error Description** column in the table displays the IP address of the STA server and the **Resource Name** column displays the details of the resource for which the STA validation has failed.

IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

You can click a user in the **Username** column to display the application launch errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

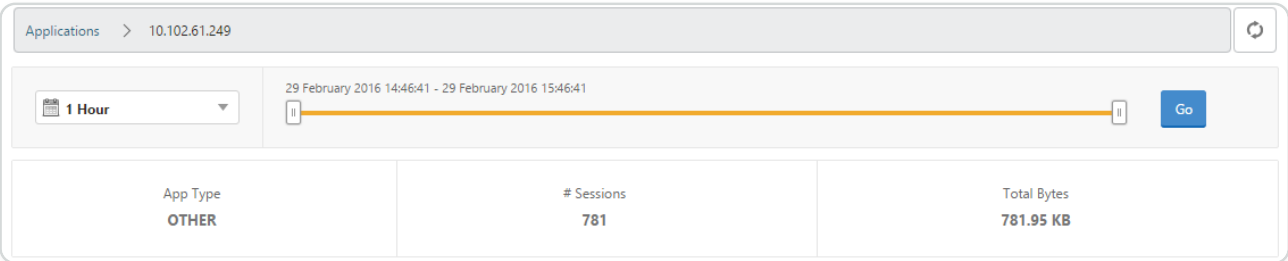
After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application

After you have successfully launched a new application, in NetScaler ADM, you can view the total bytes and bandwidth consumed by that application.

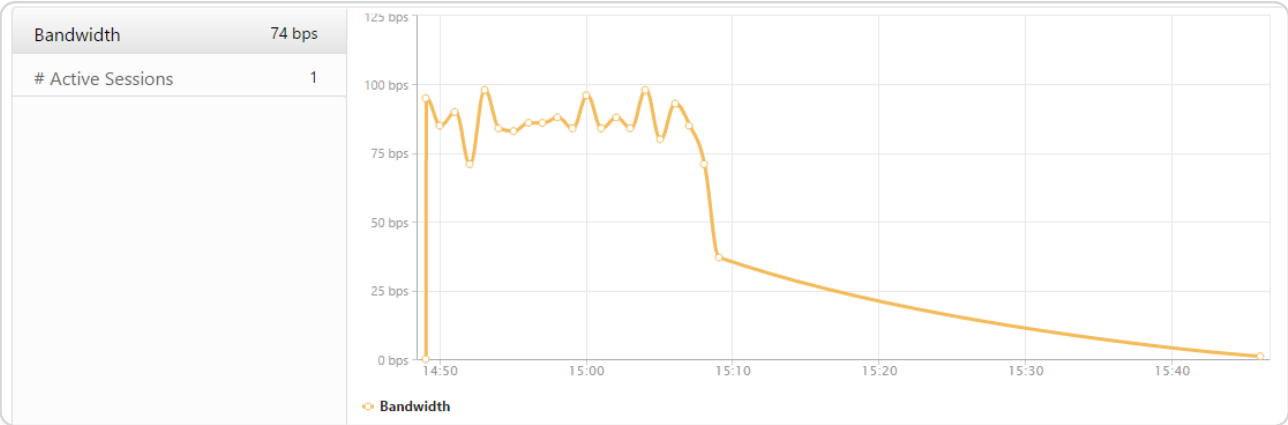
To view total bytes and bandwidth consumed by an application:

In NetScaler ADM, navigate to **Gateway > Gateway Insight > Applications**, scroll down and, on the **Other Applications** tab, click the application for which you want to view the details.

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network

With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

To view user access for resources:

1. In NetScaler ADM, **navigate to Gateway > Gateway Insight > Applications**.
2. On the screen that appears, scroll down, and on the **Other Applications** tab, select the application to which the user was unable to log on.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

3. Scroll down and in the **Users** table, all the users that have access to that application are displayed.

Different users might be using different NetScaler Gateway deployments or might log on to NetScaler Gateway through different access modes. The administrator must be able to view details about the deployment types and access modes

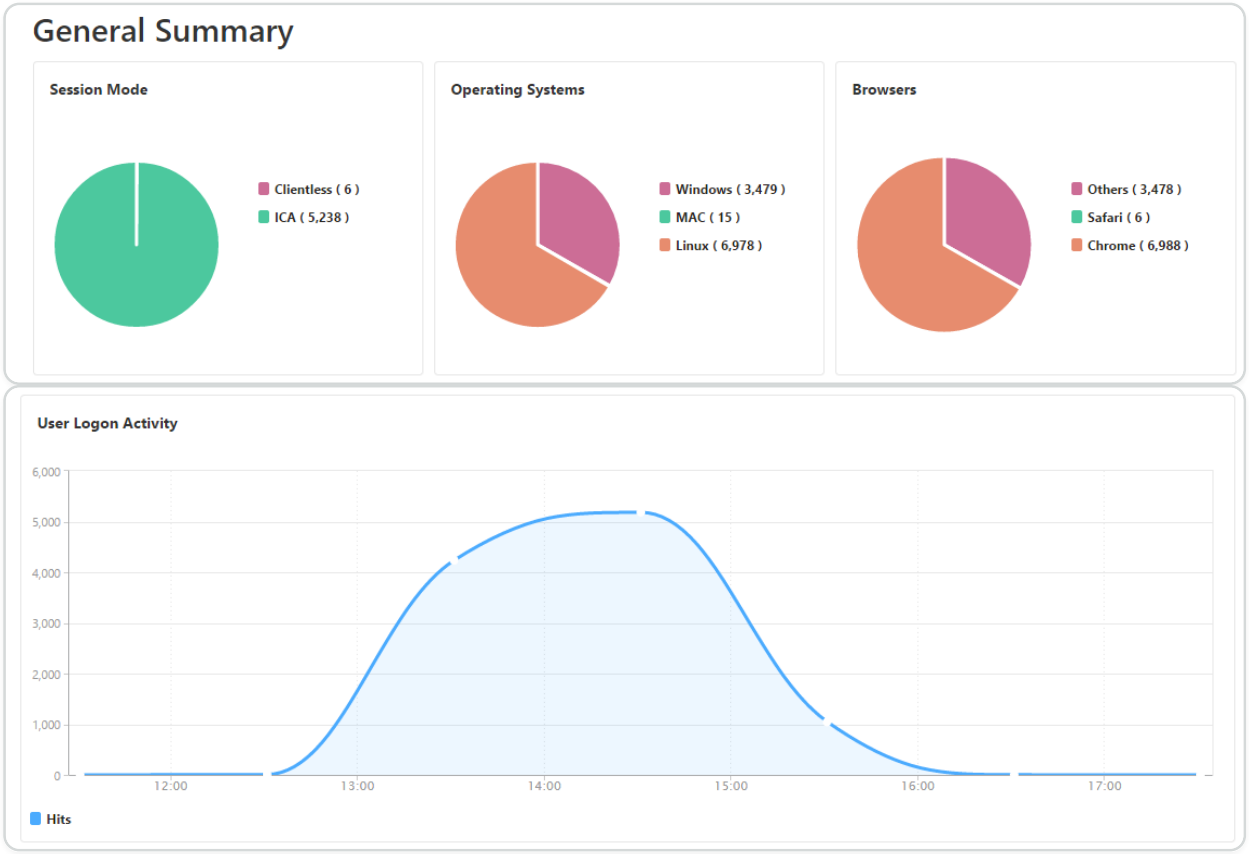
With Gateway Insight, you can view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour. You can also determine whether a user's deployment is a unified gateway or classic NetScaler Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

To view the summary of session modes, type of clients, and number of users logged on:

1. In NetScaler ADM, navigate to **Gateway > Gateway Insight**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In the **Overview** section, scroll down to view the **Session Mode, Operating Systems, Browsers**, and **User Logon Activity** charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.



Troubleshoot Gateway Insight issues

If the Gateway Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- Gateway Insight configuration.
- Connectivity issue between NetScaler and NetScaler ADM.
- Record generation in NetScaler.
- Validations in NetScaler® ADM.

Gateway Insight configuration checklist

- Make sure that the AppFlow feature is enabled in the NetScaler appliance. For details, see Enabling AppFlow.
- Check the Gateway Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the Gateway Insight configuration. Make sure that the bind type is REQUEST. For example;

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
```

Bind type OTHERTCP_REQUEST is also required for Gateway Insight.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
OTHERTCP_REQUEST
```

- For single-hop, Access Gateway, or Unified Gateway deployment, make sure that Gateway Insight AppFlow policy is bound to the VPN virtual server, where VPN traffic is flowing. For details, see Enabling HDX Insight data collection.
- For double-hop, Gateway Insight must be configured on both the hops.
- Check `appflowlog` parameter in NetScaler Gateway/VPN virtual server. For details, see Enabling AppFlow for Virtual Servers.

Connectivity between NetScaler and NetScaler ADM checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check Gateway Insight AppFlow® policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation in NetScaler checklist

- Run the `nsconmsg -d stats -g ai_tot` command and check for the stats increments in NetScaler.
- Capture `nstrace logs` and check for CFLOW packets to confirm NetScaler exports AppFlow records.

NOTE:

The `nstrace logs` are required only for IPFIX. For Logstream, nstrace logs do not confirm if the ADC appliance exported the AppFlow records.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validation of records in NetScaler ADM

- Run the `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` command to check the logs to confirm NetScaler ADM is receiving AppFlow records.
- Make sure that the NetScaler instance is added to the NetScaler ADM.
- Make sure that the NetScaler Gateway/VPN virtual server is licensed in NetScaler ADM.

Validation of Logstream logs in NetScaler ADM

Validation of Logstream data received by NetScaler ADM can be done using the following methods:

- **Enabling data record logging in NetScaler ADM**

  Once enabled, the logs can be seen in the /var/mps/log/mps_afdecoder.log

- **Enabling ULFD library logging**

  Run the command `/mps/decoder_enable_debug`

  The logs are captured in `/var/ulflog/libulfd.log`

  You can disable logging by using the command `/mps/decoder_disable_debug`

Gateway Insight counters

The following Gateway Insight counters are available.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

AppFlow records in NetScaler log

Starting from release 13.0 build 71.x, you can check the NetScaler logs to confirm if the AppFlow records are exported. The default log level of `syslogparams` captures all the error and information logs. In case you do not find a clue about the errors, enable all log levels including DEBUG in `syslogparams` to capture even the DEBUG logs.

Sample logs

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "GwInsight:
Sent auth record Func=ns_sslvpn_export_auth_data Username=<name>
Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid> Gwip=<ip>:443
StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<vpnfqdn> Authtype=3
EPAid=(null) AuthStage=1 AuthDuration=309 AuthAgent=<auth_server_ip>
Groupname= Policyname=<name> CurfactorPolname=<name> NextfactorPolname=
CSecExpr= Devicetype=16777219 Deviceid=0 email="

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight:
Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is zero"

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight:
Func=update_session_appflow_collector pcb or session is NULL"

<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record Username=<>
Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=1 Sessid=<sessid>
Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn>
SSOAuthMethod=0 SessState=2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/
Citrix/Store

Web BackendServername= SSOurl= email="

SSO logs:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=1 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=3 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=2 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:443 SessSeq=c
Sessid=<sessid> Gwip=<ip>:443 StatusCode=155 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=6 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

Contact Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler ADM versions.
- Tech support bundle for NetScaler and NetScaler ADM.
- `nstrace` capture during the issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known Issues

Refer ADC release notes for known issues on Gateway Insight.

HDX™ Insight

HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktop passing through NetScaler. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables NetScaler Application Delivery Management (ADM) to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your NetScaler Gateway virtual servers. AppFlow can be delivered by the IPFIX protocol or the LogStream method.

NOTE

To allow ICA® round trip time calculations to be logged, enable the following policy settings:

- ICA Round Trip Calculation
- ICA Round Trip Calculation Interval
- ICA Round Trip Calculation for Idle Connections

If you click an individual user, you can see each HDX session, active or terminated, that the user made within the selected time frame. Other information includes several latency statistics and bandwidth consumed during the session. You can also get bandwidth information from individual virtual channels such as audio, printer mapping, and client drive mapping.

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

You can also navigate to **Gateway > HDX Insight > Applications** and click **Launch Duration** to view the time taken for the application to launch. You can also view the user agent of all connected users by navigating to **Gateway > HDX Insight > Users.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

HDX insight supports Admin Partitions configured in NetScaler instances running on software version 12.0.

The following Thin Clients support HDX Insight:

- WYSE Windows-based Thin Clients
- WYSE Linux-based Thin Clients
- WYSE ThinOS-based Thin Clients
- 10ZiG Ubuntu-based Thin Clients

Identifying the root cause of slow performance issues

Scenario 1

User is experiencing delays while accessing Citrix Virtual Apps and Desktops.

The delays might be due to latency on the server network, ICA traffic delays caused by the server network, or latency on the client network.

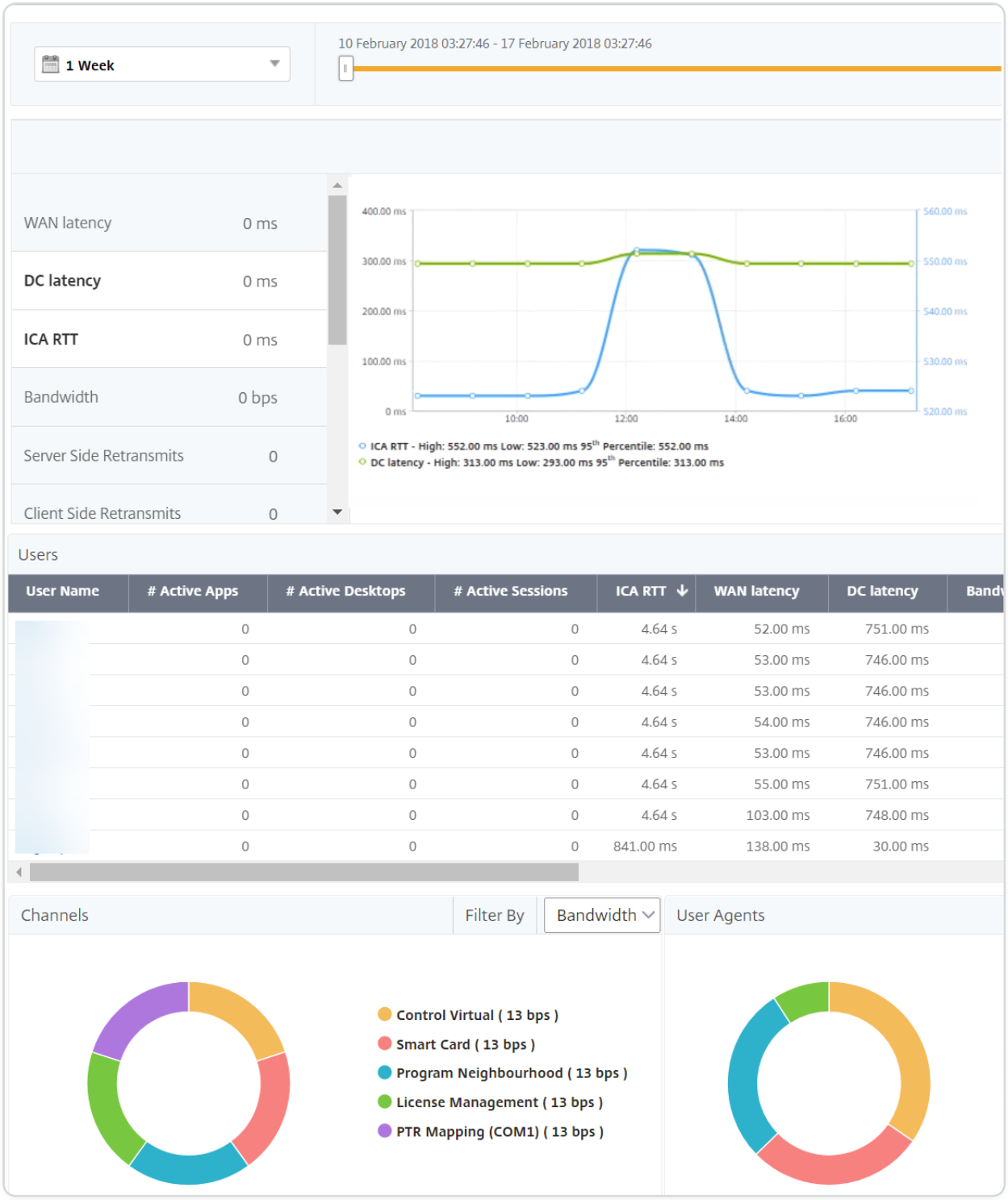
To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

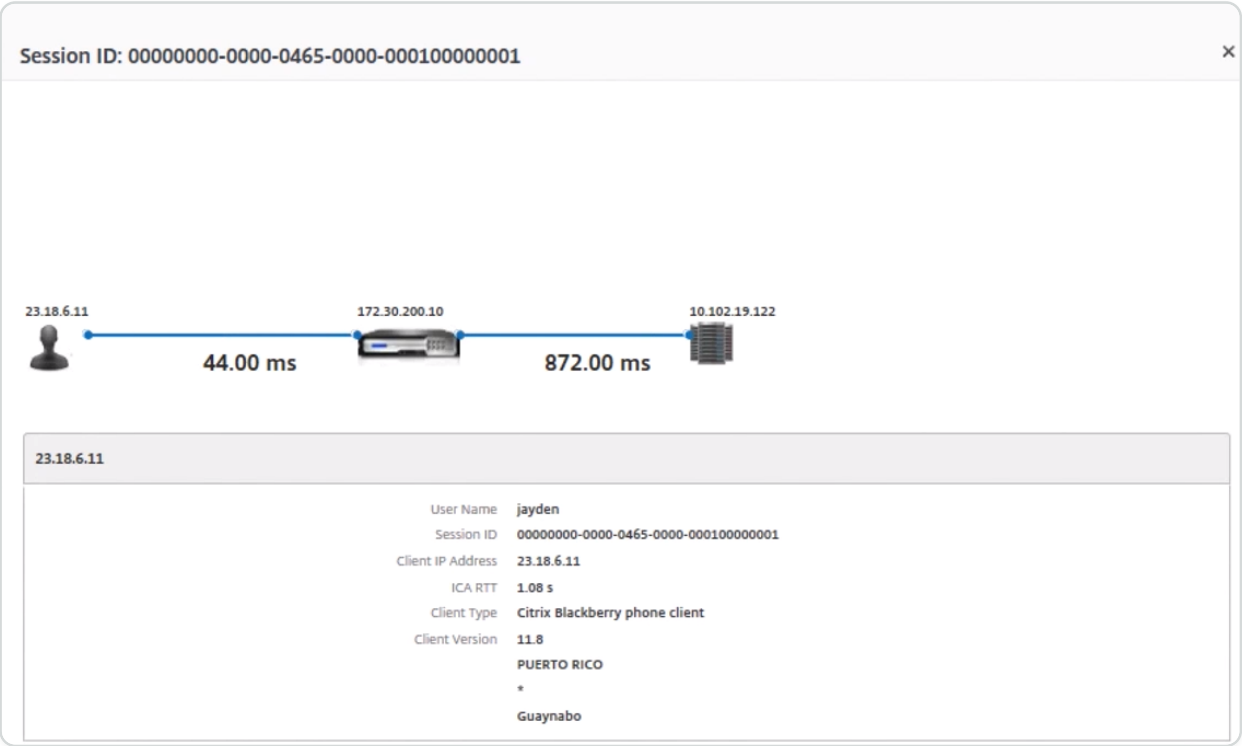
1. Navigate to **Gateway > HDX Insight> Users**.
2. Scroll down and select the user name and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Summary

In this example, the **DC Latency** is 751 milliseconds, the **WAN latency** is 52 milliseconds, and **Host Delays** is 6 seconds. This indicates that the user is experiencing delay due to average latency caused by the server network.

Scenario 2

User is experiencing delay while launching an application on Citrix Virtual App or Desktop

The delay might be due to latency on the server network, ICA-traffic delays caused by the server network, latency on the client network, or time taken to launch an application.

To identify the root cause of the issue, analyze the following metrics:

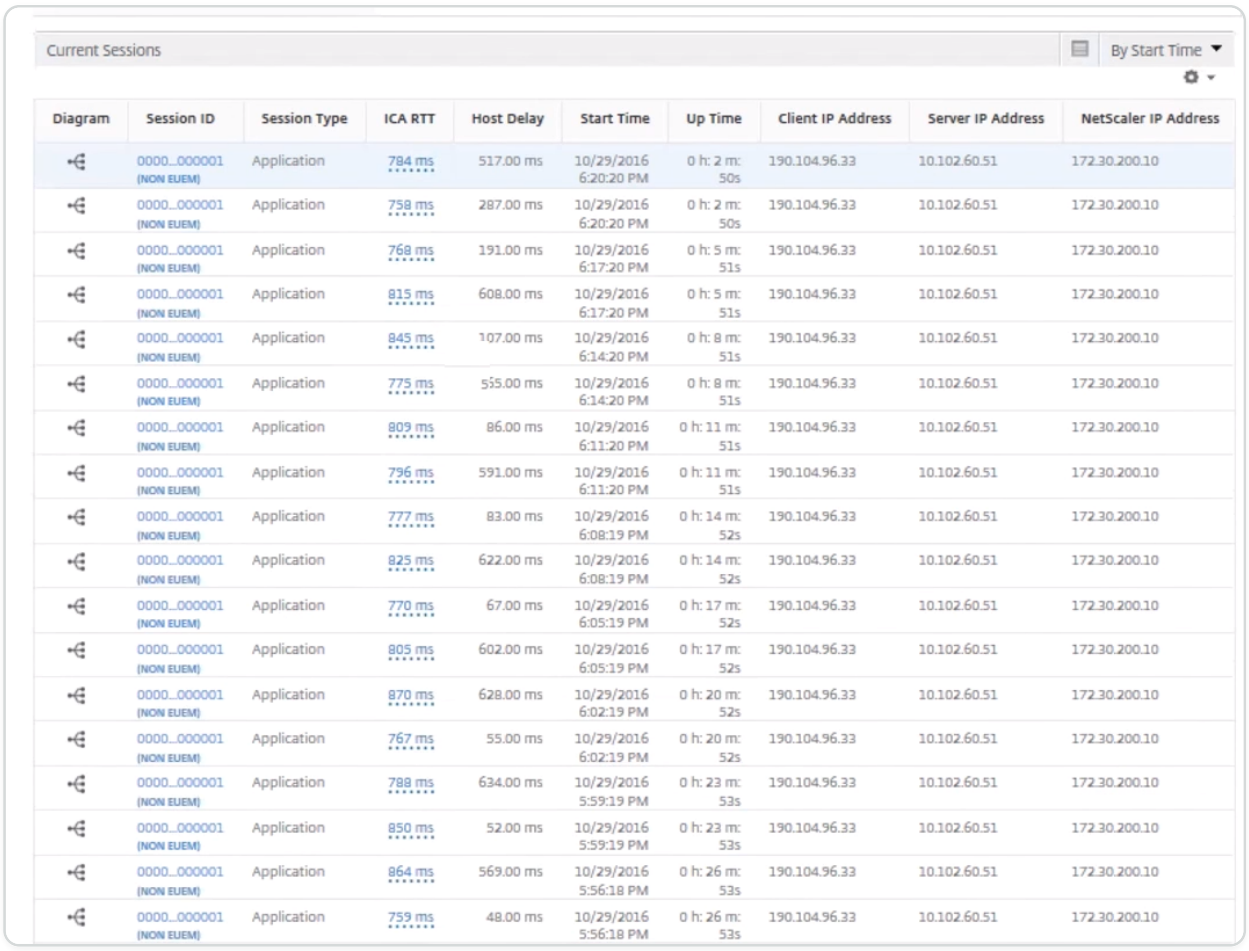
- WAN latency
- DC latency
- Host delay

To view the user metrics:

1. Navigate to **Gateway > HDX Insight > Users.**
2. Scroll down and click the user name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the graphical representation, note the WAN Latency, DC Latency, and RTT values for the particular session.
4. In the **Current Sessions** table, note that the host delay is high.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Summary

In this example, the **DC Latency** is 1 millisecond, the **WAN latency** is 12 milliseconds, but the **Host Delay** is 517 milliseconds. High RTT with low DC and WAN latencies indicates an application error on the host server.

Note HDX Insight also displays more user metrics, such as WAN jitter and Server Side Retransmits if you are using NetScaler ADM running software 11.1 build 51.21 or later. To view these metrics, navigate to **Gateway > HDX Insight > Users**, and select a user name. The user metrics appear in the table next to the graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geomaps for HDX Insight

The NetScaler® ADM geomaps functionality displays the usage of applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage across various geographical locations.

You can configure NetScaler ADM to display the geomaps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

You can also view the historical and active users' details from the geo location maps in HDX Insight. Navigate to **Gateway > HDX Insight**, and in the **World** section of the map, click the country or region for which you want to see the details. You can further drill down to view information by city and state.

To configure a geomap for data centers:

Navigate to **Settings > Analytics Settings > IP Blocks** to configure geomaps for a particular location.

Use case

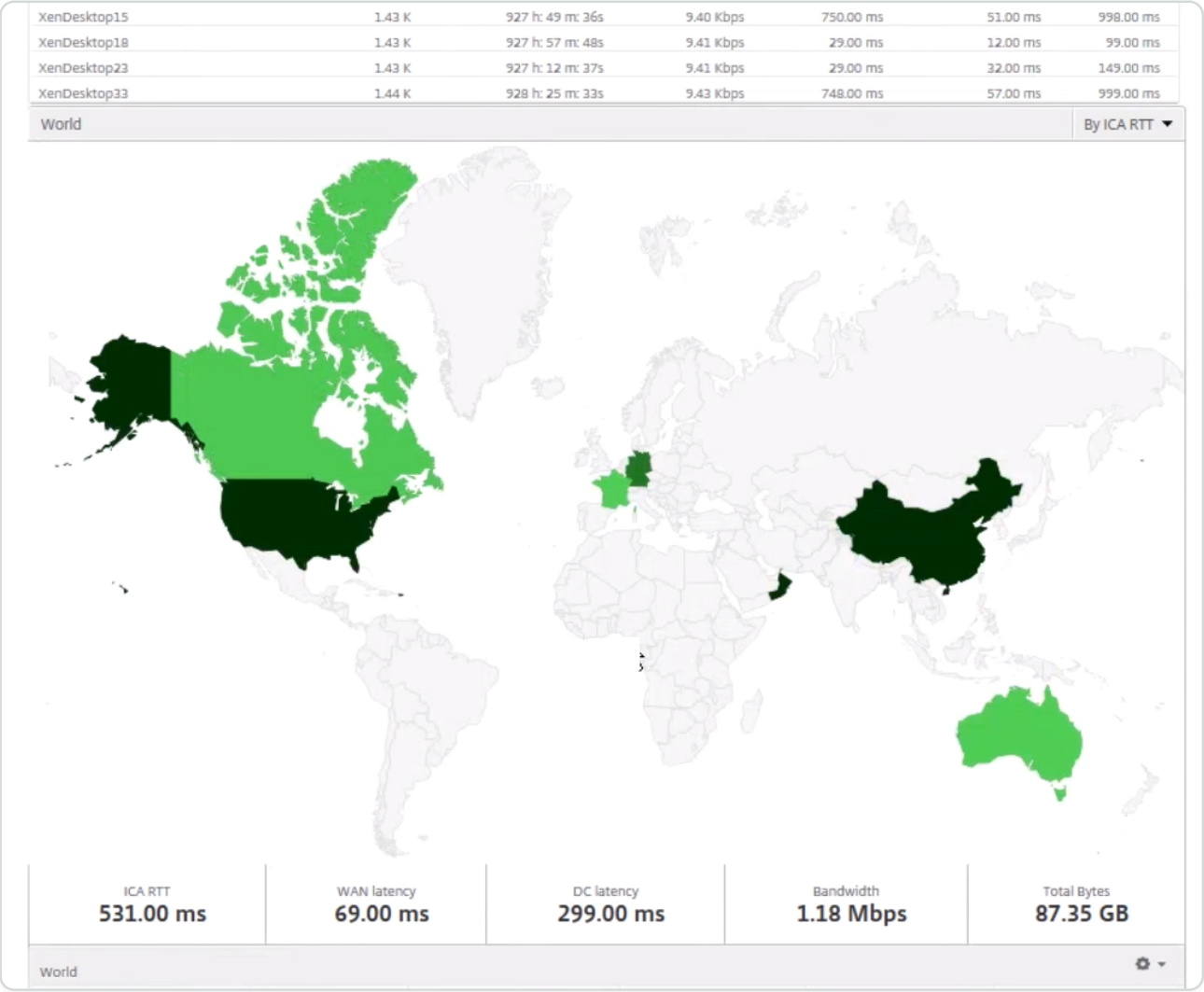
Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.

The Santa Clara users use the NetScaler Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the NetScaler Gateway appliance at India.x.com to access VPN traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

During a particular time-interval, say 10 AM to 5 PM, the users in Santa Clara connect to SClara.x.com to access VPN traffic. Most of the users access the same NetScaler Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

A NetScaler administrator analyzing the traffic can use the geo map functionality to show the traffic in Santa Clara office. The map shows that the response time in the Santa Clara office is high, because the Santa Clara office has only one NetScaler Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another NetScaler Gateway, so that users have two local NetScaler Gateway appliances through which to access the VPN.



Limitations

If NetScaler instances have Advanced license, thresholds set on NetScaler ADM for HDX Insight will not be triggered since analytical data is collected for only 1 hour.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling HDX™ Insight data collection

HDX Insight enables IT to deliver an exceptional user experience by providing unprecedented end-to-end visibility into the ICA traffic that passes through the NetScaler instances and is a part of NetScaler Application Delivery Management (ADM) Analytics. HDX Insight delivers compelling and powerful business intelligence and failure analysis capabilities for the network, virtual desktops, applications, and application fabric. HDX Insight can both instantly triage on user issues, collects data about virtual desktop connections, and generates AppFlow records and presents them as visual reports.

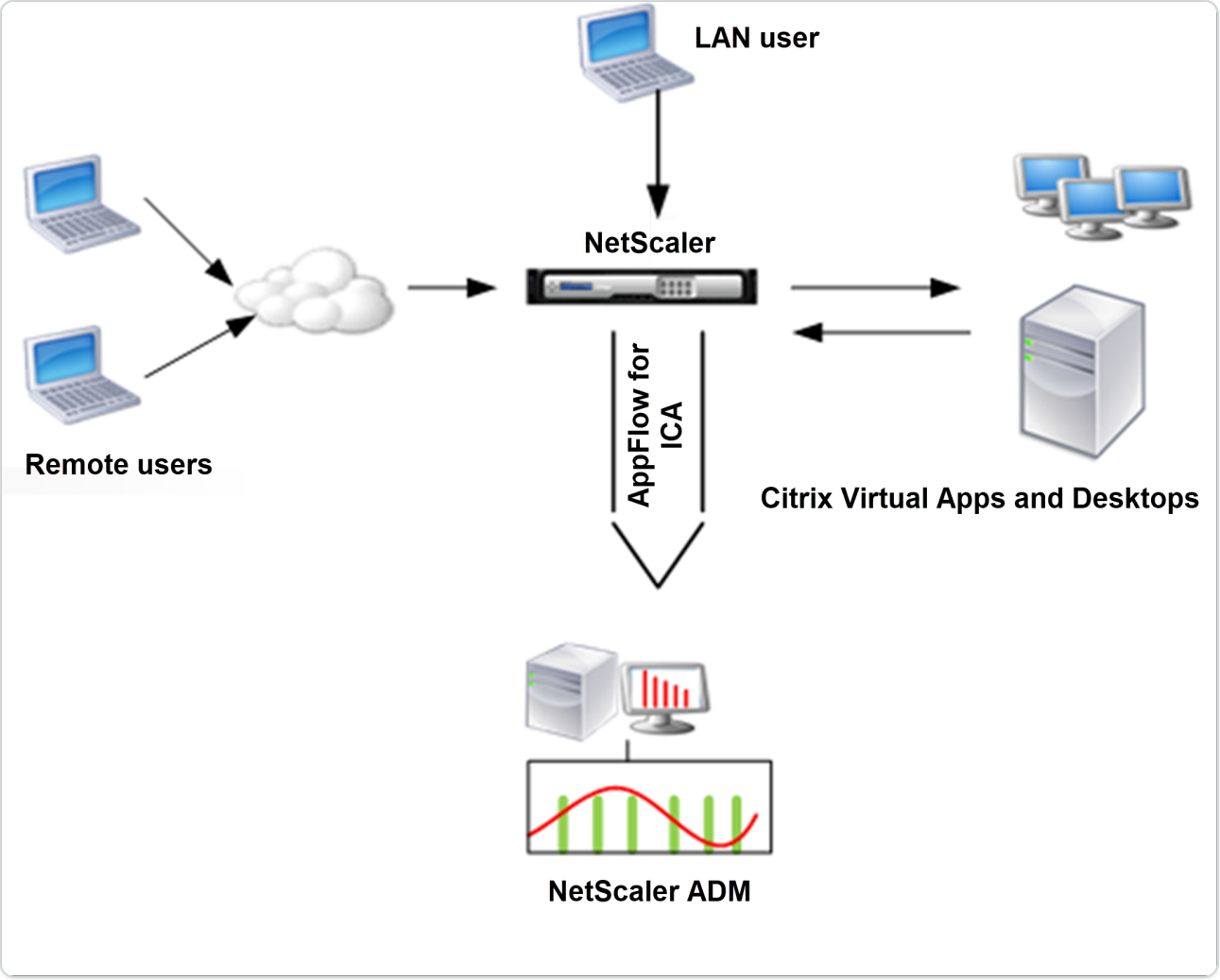
The configuration to enable data collection in the NetScaler differs with the position of the appliance in the deployment topology.

Enabling data collection for monitoring NetScalers deployed in LAN user mode

External users who access Citrix Virtual App and Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual App and Desktop applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

NetScaler ADM and NetScaler Gateway appliance reside in the same subnet.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow, and then view the reports on the dashboard.

After you add the NetScaler appliance to the NetScaler ADM inventory, you must enable AppFlow for data collection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- On an ADC instance, you can navigate to **Settings > AppFlow > Collectors**, to check if the collector (that is, NetScaler ADM) is up or not. NetScaler instance sends AppFlow records to NetScaler ADM using NSIP. But the instance uses its SNIP to verify connectivity with NetScaler ADM. So, ensure that the SNIP is configured on the instance.
- You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler ADM configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

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 NetScaler Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]



add vpn trafficPolicy <name> <rule> <action>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Add NetScaler ADM as an AppFlow collector on the NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

NOTE

The value of type must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA® traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

Example:

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration. Type: `save ns config`

Enabling data collection for NetScaler Gateway appliances deployed in single-hop mode

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization. In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler Application Delivery Management (ADM) inventory and enable AppFlow on ADM.

To enable the AppFlow feature from NetScaler® ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, `<http://192.168.100.1>`).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA**.
7. Click **OK**.

NOTE

when you enable AppFlow in single-hop mode, the following commands run in the background. These commands are explicitly specified here for troubleshooting purposes.

```
-  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>
```

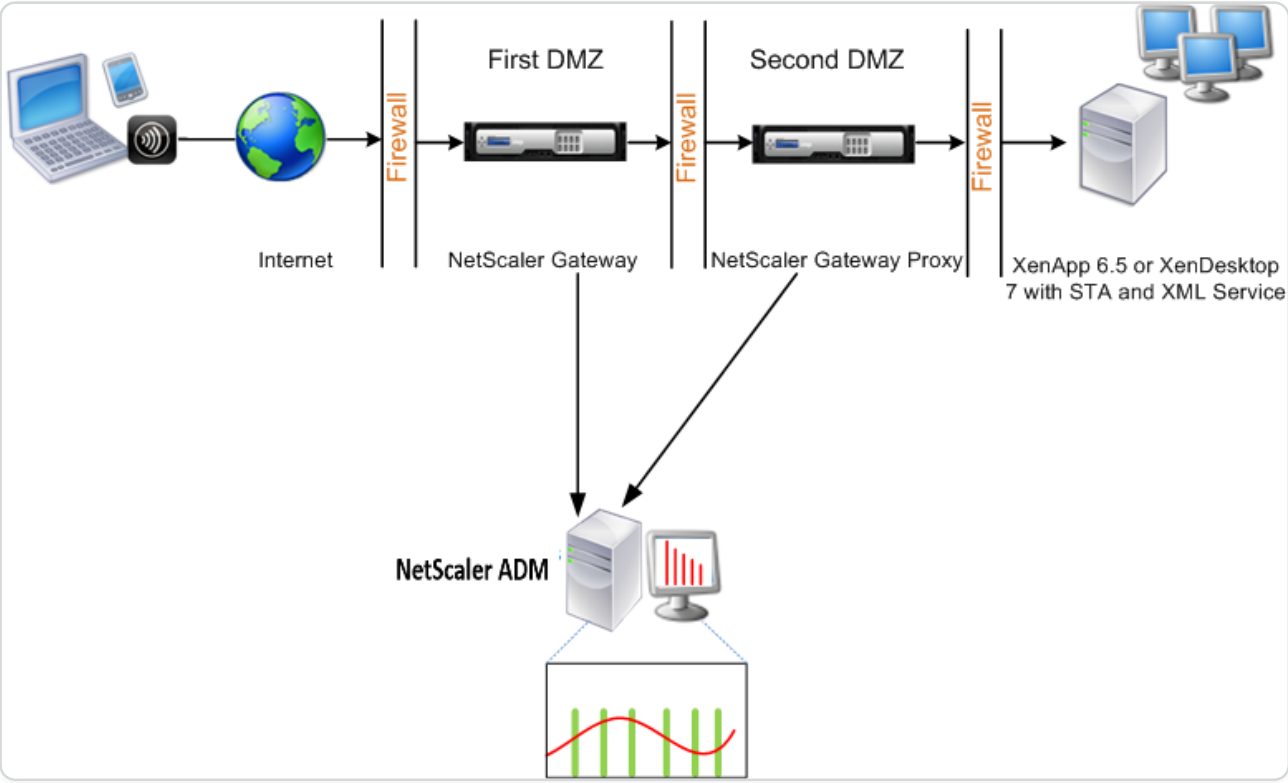
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  set vpn vserver <name> -appflowLog ENABLED



-  save ns config
```

EUEM virtual channel data is part of HDX Insight data that the NetScaler ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

Enabling data collection for NetScaler Gateway appliances deployed in double-hop mode

The NetScaler Gateway double-hop mode provides additional protection to an organization's internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler ADM so that the NetScaler Gateway appliances report these vital statistics.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler ADM can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler ADM and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler ADM collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler ADM inventory and enable data collection, each of the appliances exports the reports by keeping track of the hop count and connection chain ID.

For NetScaler ADM to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of NetScaler Gateway appliances through which the traffic flows from a client to the servers. The connection chain ID represents the end- to end connections between the client and server.

NetScaler ADM uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler ADM inventory, enable AppFlow on NetScaler ADM, and then view the reports on the NetScaler ADM dashboard.

Configure HDX Insight on virtual servers used for Optimal Gateway

Steps to configure HDX Insight on virtual servers used for Optimal Gateway:

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the VPN virtual server configured for authentication, and click **Enable Analytics**.
4. Select **HDX Insight** and then select **ICA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select other advanced options as required.
6. Click **OK**.
7. Repeat steps 3 through 6 on the other VPN virtual server.

Enable data collection on NetScaler ADM

If you enable NetScaler ADM to start collecting the ICA details from both the appliances, the details collected are redundant. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first NetScaler Gateway appliances, and then enable AppFlow for TCP on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow feature from NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, `<http://192.168.100.1>`).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.
5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA** or **TCP** for ICA traffic or TCP traffic respectively.

   NOTE

   If AppFlow logging is not enabled for the respective services or service groups on the NetScaler appliance, the NetScaler ADM dashboard does not display the records, even if the Insight column shows Enabled.

7. Click **OK**.

Configuring NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler Gateway appliances to export the reports to NetScaler ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

Configure NetScaler Gateway Using the Command Line Interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON or
OFF)] [-imgGifToPng]



add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

```
bind vpn vserver <name> -nextHopServer <name>



bind vpn vserver vs1 -nextHopServer nh1
```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
 appflowLog ( ENABLED or DISABLED )]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]



set vpn vserver vs -authentication OFF
```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
OTHERTCP_REQUEST
```

6. Enable the other NetScaler Gateway appliance to export ICA records:

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA_REQUEST
```

7. Enable connection chaining on both the NetScaler Gateway appliances:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]



set appflow param -connectionChaining ENABLED
```

Configure NetScaler Gateway using Configuration Utility:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the Advanced group, expand **Published Applications**.
   c. Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.
2. Enable double hop on the NetScaler Gateway in the second DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand more, select **Double Hop** and click **OK**.
3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand **More**, and clear **Enable Authentication**.
4. Enable one of the NetScaler Gateway appliances to export TCP records.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.
   c. Click the + icon and from the **Choose Policy** list, select **AppFlow**, and from the **Choose Type** list, select **Other TCP Request**.
   d. Click **Continue**.
   e. Add a policy binding, and click **Close**.
5. Enable the other NetScaler Gateway appliance to export ICA records:
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Advanced** group, expand **Policies**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   c. Click the + icon and from the **Choose Policy** list, select AppFlow, and from theChoose Type list, select **Other TCP Request**.
   d. Click **Continue**.
   e. Add a policy binding, and click **Close**.

6. Enable connection chaining on both the NetScaler Gateway appliances.
   a. On the **Configuration** tab, navigate to **System** > **Appflow**.
   b. In the right Pane, in the **Settings** group, double-click **Change Appflow Settings**.
   c. Select **Connection Chaining** and Click **OK**.

7. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.
   a. On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Advanced group**, expand **Published Applications**.
   c. Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

8. Enable double hop on the NetScaler Gateway in the second DMZ.
   a. On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand More, select **Double Hop**, and click **OK**.

9. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.
   a. On the Configuration tab expand NetScaler Gateway and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand **More**, and clear **Enable Authentication**.

10. Enable one of the NetScaler Gateway appliances to export TCP records.
    a. On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. In the right pane, double-click the virtual server, and in the Advanced group, expand **Policies**.

c. Click the **+** icon and from the Choose Policy list, select AppFlow, and from the **Choose Type** list, select **Other TCP Request**.

d. Click **Continue**.

e. Add a policy binding, and click **Close**.

11. Enable the other NetScaler Gateway appliance to export ICA records.

a. On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b. In the right pane, double-click the virtual server, and in the Advanced group, expand **Policies**.

c. Click the **+** icon and from the **Choose Policy** list, select AppFlow, and from the **Choose Type** list, select **Other TCP Request**.

d. Click **Continue**.

e. Add a policy binding, and click **Close**.

12. Enable connection chaining on both the NetScaler Gateway appliances.

Enable data collection for monitoring NetScalers deployed in transparent mode

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a Citrix Virtual Apps and Desktop environment, the ICA traffic is not transmitted over a VPN.

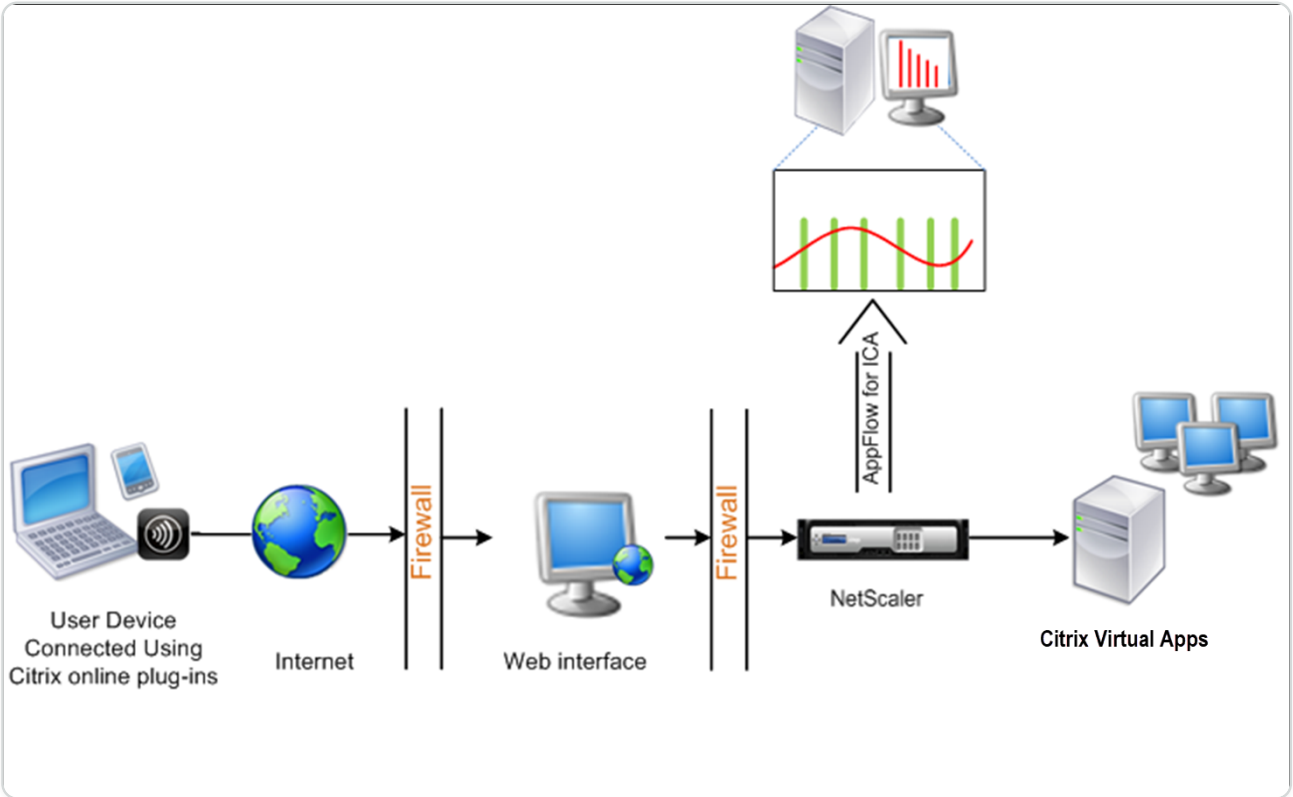
After you add the NetScaler to the NetScaler ADM inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler ADM as an AppFlow collector on each NetScaler appliance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- You cannot enable data collection on a NetScaler deployed in transparent mode by using the NetScaler ADM configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

The following figure shows the network deployment of a NetScaler ADM when a NetScaler is deployed in a transparent mode:



To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

```
set ns param --icaPorts <port>...
```

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

```
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.

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global <policyname> <priority> -type <type>
```

Example:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

NOTE

The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

Example:

```
set appflow param -flowRecordInterval 60
```

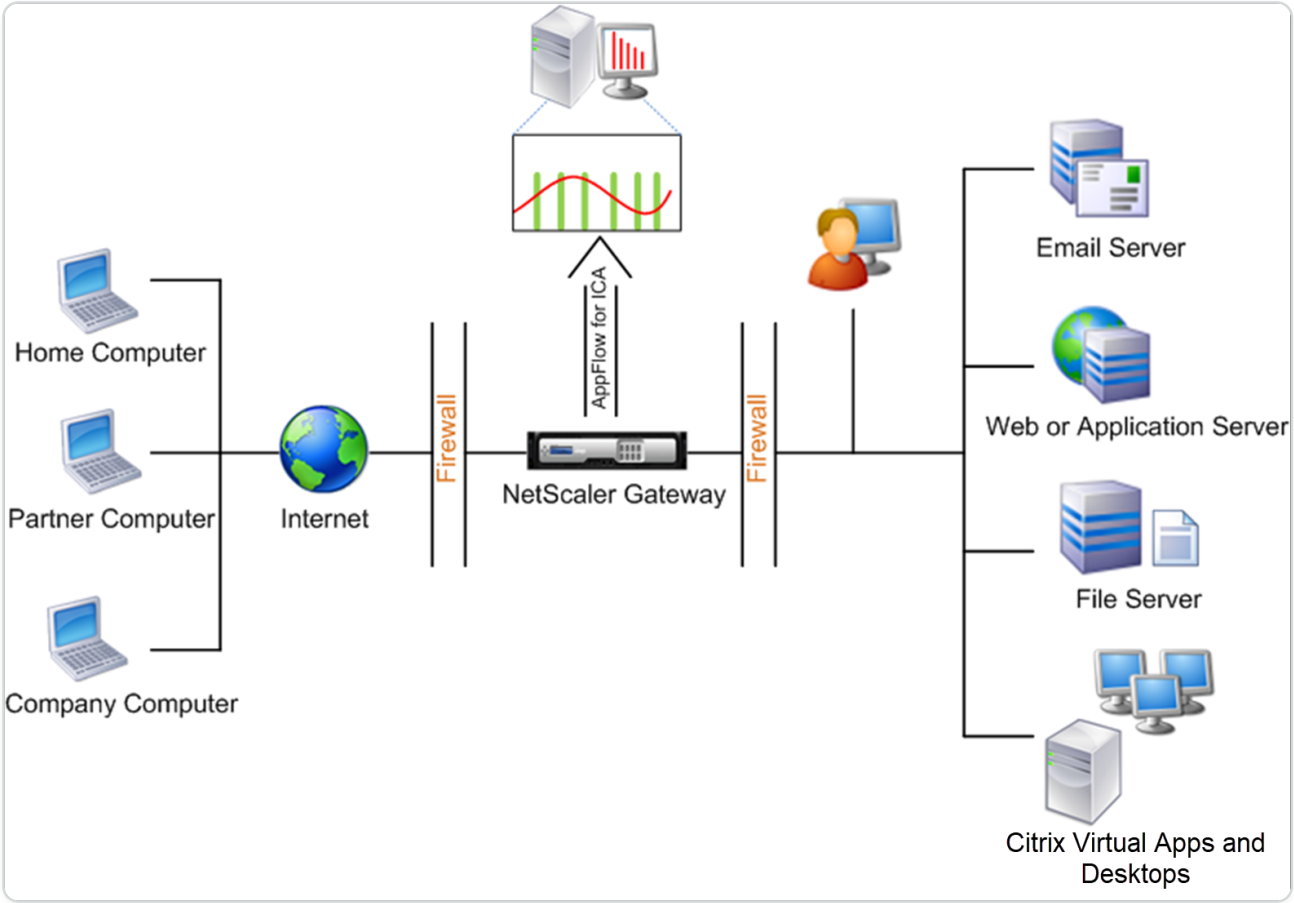
8. Save the configuration. Type: `save ns config`

Enable data collection for NetScaler Gateway appliances deployed in single-hop mode

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop mode provides security if an external user tries to access the internal network in an organization. In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler Application Delivery Management (ADM) inventory and enable AppFlow on ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To enable the AppFlow® feature from ADM:

1. Navigate to **Infrastructure** \> **Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Action** list, select **Enable/Disable Insight**.
3. Select the **VPN virtual servers**, and click **Enable AppFlow**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA®**.
5. Click **OK**.

NOTE

When you enable AppFlow in single-hop mode, the following commands run in the background. These commands are explicitly specified here for troubleshooting purposes.

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

EUEM virtual channel data is part of HDX Insight data that the NetScaler® ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

Enable data collection to monitor NetScalers deployed in transparent mode

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler is deployed in transparent mode in a Citrix Virtual Apps and Desktops environment, the ICA traffic is not transmitted over a VPN.

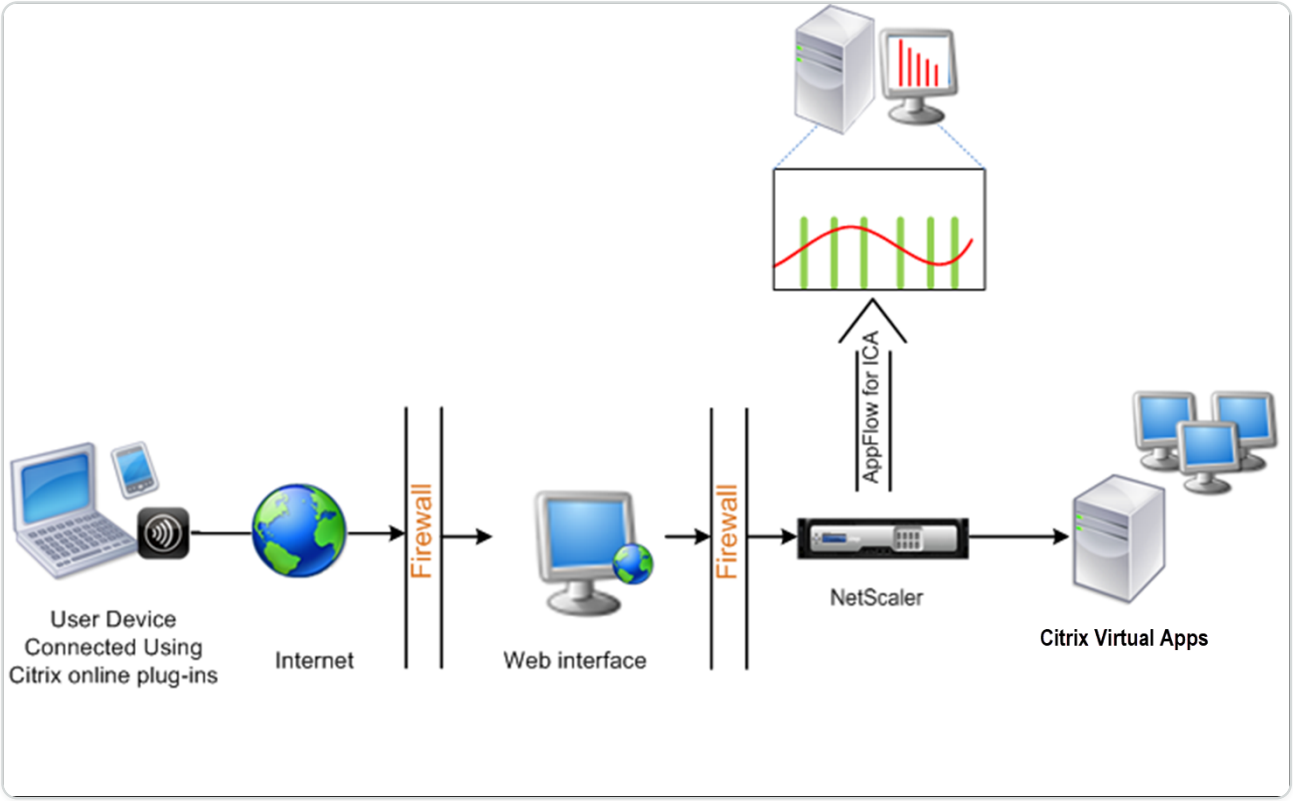
After you add the NetScaler to the NetScaler ADM inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler ADM as an AppFlow collector on each NetScaler instance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

NOTE

- You cannot enable data collection on a NetScaler deployed in transparent mode by using the NetScaler ADM configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

The following figure shows the network deployment of a NetScaler ADM when a NetScaler is deployed in a transparent mode:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

   ```
   set ns param --icaPorts \<port\>...
   ```

   Example:

   ```
   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 instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

Note To view the AppFlow collectors configured on the NetScaler instance, use the **show appflow collector** command.

4. Create an AppFlow® action and associate the collector with the action.

```
add appflow action <name> -collectors <string> ...
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA® traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

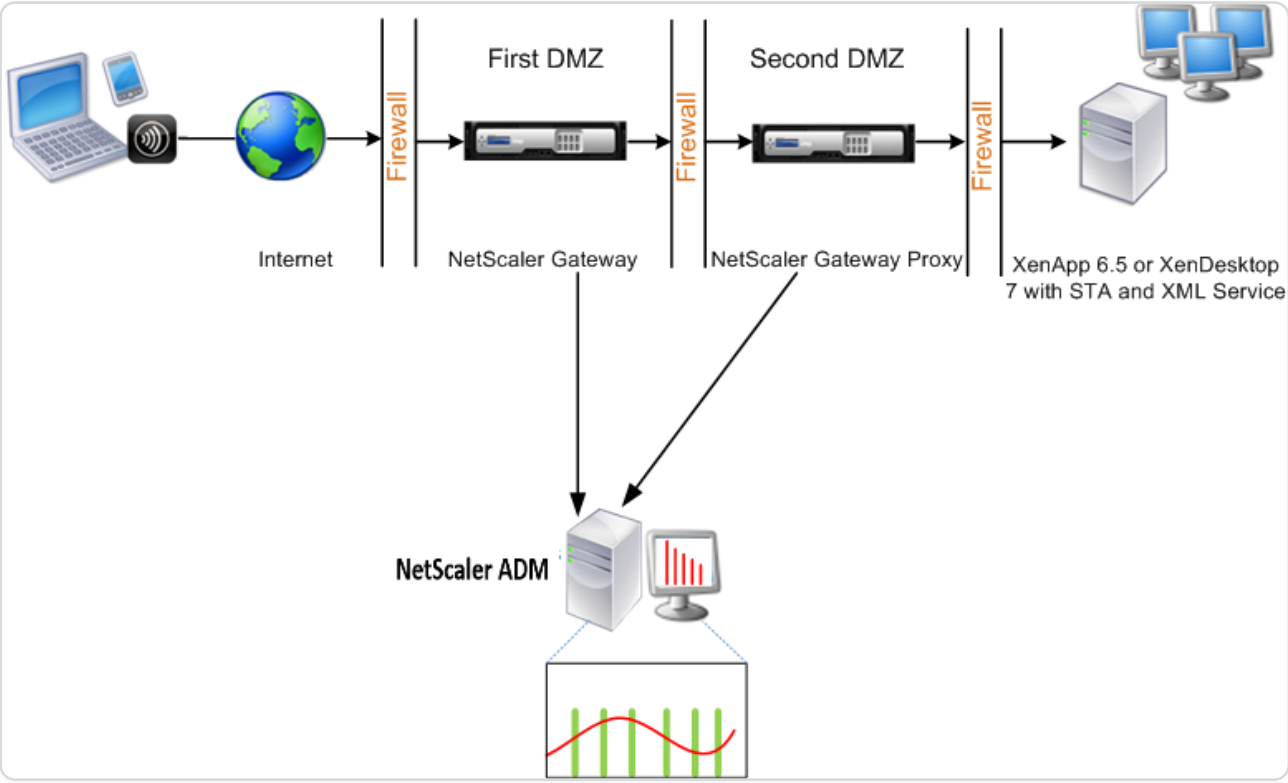
```
save ns config
```

Enable data collection for NetScaler Gateway appliances deployed in double-hop mode

The NetScaler Gateway double-hop mode provides extra protection to an organization's internal network, because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler ADM, so that the NetScaler Gateway appliances report these vital statistics.

Figure 3. NetScaler® ADM deployed in double-hop mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler ADM can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler ADM and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler ADM collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler ADM inventory and enable data collection, each appliance exports the reports by keeping track of the hop count and connection chain ID.

For NetScaler ADM to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of NetScaler Gateway appliances through which the traffic flows from a client to the servers. The connection chain ID represents the end- to end connections between the client and server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler ADM inventory, enable AppFlow on NetScaler ADM, and then view the reports on the NetScaler ADM dashboard.

Enable data collection on NetScaler ADM

If you enable NetScaler ADM to start collecting the ICA details from both the appliances, the details collected are redundant. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for TCP on one of the first NetScaler Gateway appliances, and then enable AppFlow for ICA on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow® feature from NetScaler ADM:

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Action** list, select **Enable/Disable Insight**.
3. Select the VPN virtual servers, and click **Enable AppFlow**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA/TCP** for ICA traffic a TCP traffic respectively.

   NOTE

   If AppFlow logging is not enabled for the services or service groups on the NetScaler appliance, the NetScaler ADM dashboard does not display the records, even if the Insight column shows Enabled.

5. Click **OK**.

Configure NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler Gateway appliances to export the reports to NetScaler ADM:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

Configure NetScaler Gateway using the command line interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

   add vpn nextHopServer \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure**(ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

   bind vpn vserver \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

   set vpn vserver \<name\> \[**- doubleHop** (ENABLED |DISABLED)\] \[**- appflowLog** (ENABLED |DISABLED)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

   set vpn vserver\<name\> \[**-authentication** (ON|OFF)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Enable one of the NetScaler Gateway appliances to export TCP records.

   bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \ [**-type**\<type\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. Enable the other NetScaler Gateway appliance to export ICA records:

   bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \ [**-type**\<type\>\]

   ```
   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA\_REQUEST
   ```

7. Enable connection chaining on both the NetScaler Gateway appliances:

   set appFlow param \[**-connectionChaining** (ENABLED|DISABLED)\]

   ```
   set appflow param -connectionChaining ENABLED
   ```

Configuring NetScaler Gateway using configuration utility:

1. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.

   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

   b. In the right pane, double-click the virtual server, and in the Advanced group, expand **Published Applications**.

   c. Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

2. Enable double hop on the NetScaler Gateway in the second DMZ.

   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   c. Expand **More** , select **Double Hop** and click **OK**.

3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.

   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand **More**, and clear **Enable Authentication**.

4. Enable one of the NetScaler Gateway appliances to export TCP records.

   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.
   c. Click the + icon and from the **Choose Policy** list, select **AppFlow**, and from the **Choose Type** drop-down list, select **Other TCP Request**.
   d. Click **Continue**.
   e. Add a policy binding, and click **Close**.

5. Enable the other NetScaler Gateway appliance to export ICA records:

   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Advanced** group, expand **Policies**.
   c. Click the + icon and from the **Choose Policy** drop-down list, select **AppFlow**, and from theChoose Type drop-down list, select **Other TCP Request**.
   d. Click **Continue**.
   e. Add a policy binding, and click **Close**.

6. Enable connection chaining on both the NetScaler Gateway appliances.

   a. On the **Configuration** tab, navigate to **Settings > Appflow**.
   b. In the right Pane, in the **Settings** group, click **Change Appflow Settings**.
   c. Select **Connection Chaining** and Click **OK**.

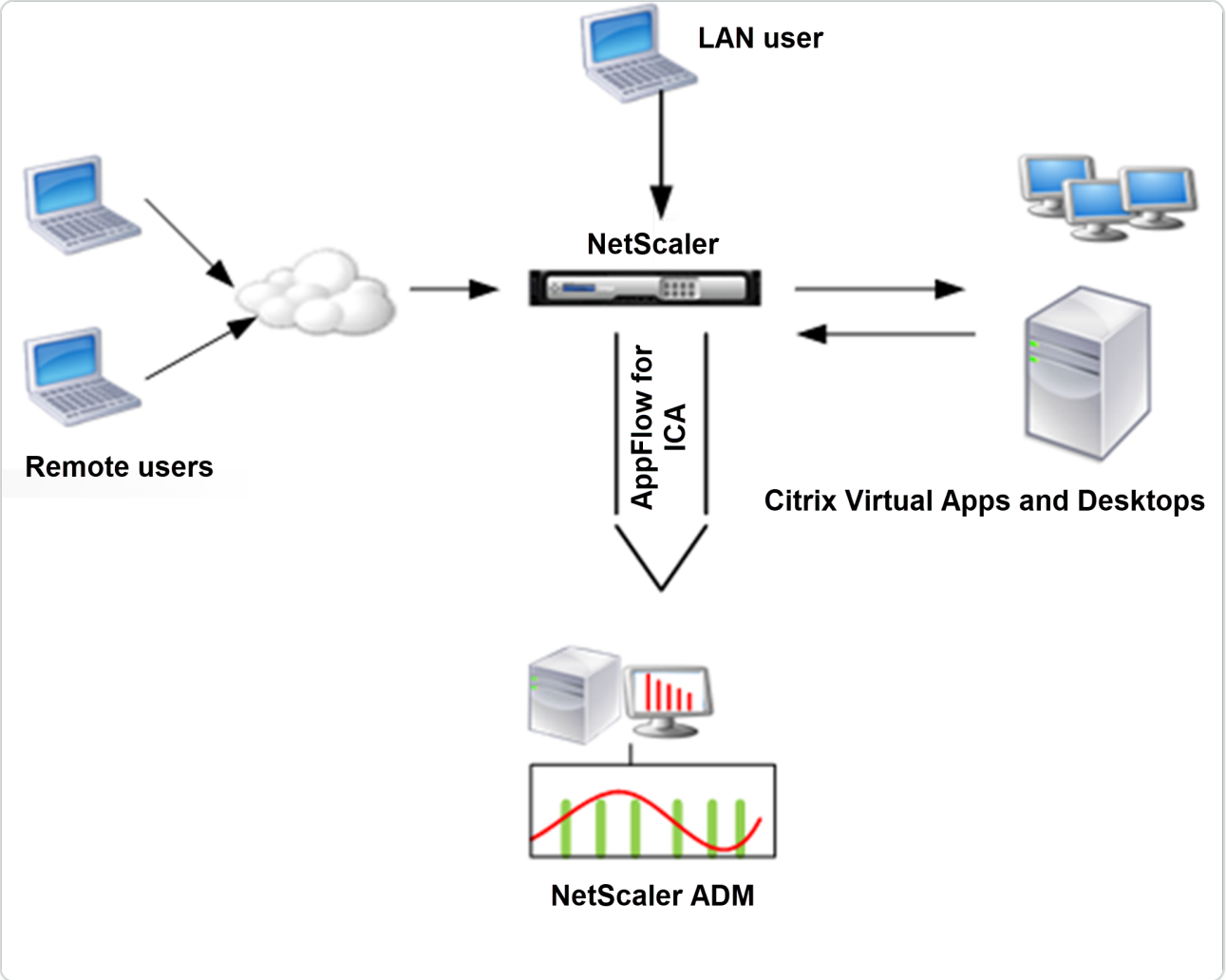
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable data collection to monitor NetScalers deployed in LAN user mode

External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual Apps and Desktops applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

Figure 4. NetScaler® ADM deployed in LAN User Mode



Note NetScaler ADM and NetScaler Gateway appliance reside in the same subnet.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow, and then view the reports on the dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you add the NetScaler appliance to the NetScaler ADM inventory, you must enable AppFlow for data collection.

NOTE

- You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler ADM configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

   ```
   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
   <cachetype>] [ - cltTimeout <secs>]
   ```

   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 NetScaler Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

   ```
   add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



   add vpn trafficPolicy** \<name\> \<rule\> \<action\>
   ```

   Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Add NetScaler ADM as an AppFlow collector on the NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
```

NOTE

The value of type must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

Example:

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

```
save ns config
```

Create thresholds and configure alerts for HDX™ Insight

HDX Insight on NetScaler Application Delivery Management (ADM) allows you to monitor the HDX traffic passing through NetScaler instances. NetScaler ADM allows you to set thresholds on various counters used to monitor the Insight traffic. You can also configure rules and create alerts in NetScaler ADM.

HDX traffic type is associated with various entities such as applications, desktops, gateways, licenses, and users. Every entity can contain different metrics associated with them. For example, application entity is associated with various hits, bandwidth consumed by the application, and response time of the server. A user entity can be associated with WAN latency, DC latency, ICA® RTT, and bandwidth consumed by a user.

The threshold management for HDX Insight in NetScaler® ADM allowed you to proactively create rules and configure alerts whenever the thresholds set are breached. Now, this threshold management is extended to configure a group of threshold rules. You can now monitor the group instead of individual rules. A threshold rule group comprises one or more user-defined threshold rules for metrics chosen from entities such as users, applications, and desktops. Each rule is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

monitored against an expected value that you enter when you create the rule. In case of users entity, the threshold group can be associated with a geolocation as well.

An alert is generated on NetScaler ADM only if all the rules in the configured threshold group are breached. For example, you can monitor an application on total session launch count and also on application launch count as one threshold group. An alert is generated only if both rules are breached. This allows you to set more realistic thresholds on an entity.

A few examples are listed as follows:

- Threshold rule1: ICA RTT(metric) for users(entity) must be \<= 100 ms
- Threshold rule2: WAN Latency (metric) for users(entity) must be \<= 100 ms

An example of threshold group can be: {Threshold rule 1 + Threshold rule 2}

To create a rule, you must first select the entity that you want to monitor. Then choose a metric while creating a rule. For example, you can select applications entity and then select Total Session Launch count or App Launch Count. You can create one rule for every combination of an entity and a metric. Use the comparators provided (\>, \<, \>=, and \<=) and type a threshold value for each metric.

NOTE

If you do not want to monitor multiple entities in a single group, you must create a separate threshold rule group for each entity.

When the value of a counter exceeds the value of a threshold, NetScaler ADM generates an event to signify a threshold breach, and an alert is created for every event.

You must configure how you receive the alert. You can enable the alert to be displayed on NetScaler ADM and/or receive the alert as an email or as an SMS on your mobile device. For the last two actions, you must configure the email server or the SMS server on NetScaler ADM.

Threshold groups can also be bound to Geolocations for geo-specific monitoring for user entity.

Example Use cases

ABC Inc. is a global firm and has offices in over 50 countries. The firm has two data centers, one in Singapore and other in California that host the Citrix Virtual Apps and Desktops. Employees of the firm access the Citrix Virtual Apps and Desktops throughout the globe using NetScaler Gateway and Citrix GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wants to track the user experience for all their offices to optimize the apps and desktop delivery for anywhere, anytime access. Eric also wants to check the user-experience-metrics like ICA RTTs, latencies, and raise any deviations proactively.

The users of ABC Inc. have a distributed presence. Some users are located close to the data center, while a few are located at further away from the data center. As the user base is distributed widely, the metrics and the corresponding thresholds also vary among these locations. For example, the ICA RTT for a location near to the data center can be 5–10 ms whereas the same for a remote location can be around 100 ms.

With threshold rule group management for HDX Insight, Eric can set geo-specific threshold rule groups for each location and be alerted through email or SMS for breaches per area. Eric is also able to combine tracking of more than one metric within a threshold rule group and narrow down the root cause to capacity issues if any. Eric is now able to proactively track any deviation without having to worry about the complexity of manually looking through all Citrix Virtual Apps and Desktops portfolio metrics.

To create a threshold rule group and configure alerts for HDX Insight using NetScaler ADM:

1. In NetScaler ADM, navigate to **Settings > Analytics Settings > Thresholds**. On **Thresholds** page that opens, click **Add**.
2. On the **Create Thresholds and Alerts** page, specify the following details:

    a. **Name**. Type in a name for creating an event for which NetScaler ADM generates an alert.

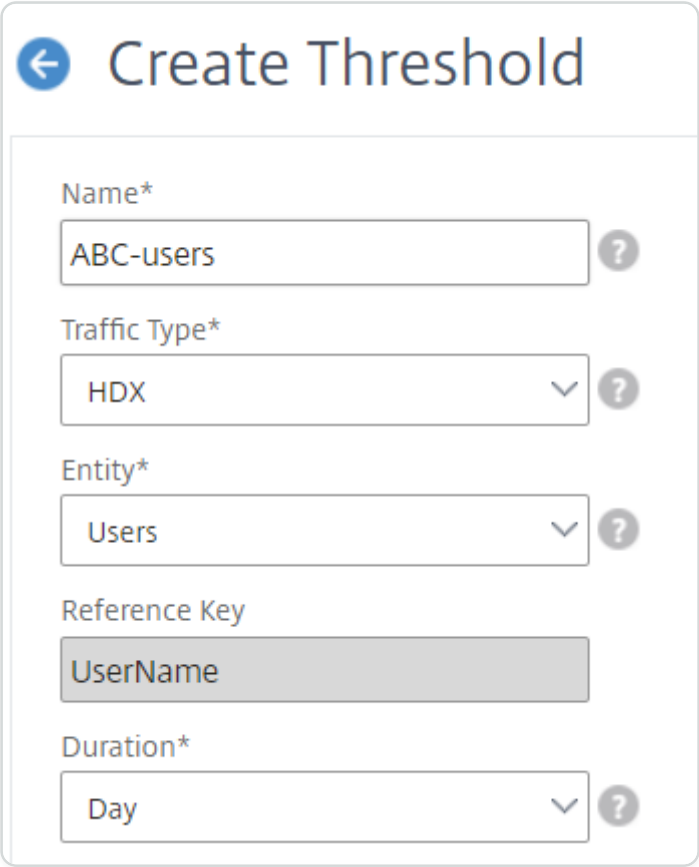
    b. **Traffic Type**. From the list box, select HDX.

    c. **Entity**. From the list box, select the category or the resource type. The entities differ for each traffic type that you have selected earlier.

    d. **Reference Key**. A reference key is automatically generated based on the traffic type and entity that you have selected.

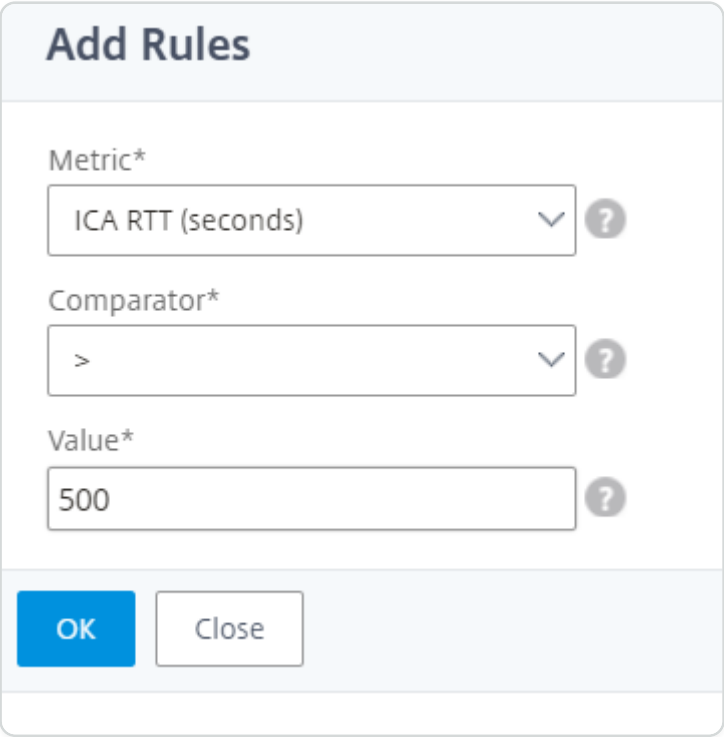
    e. **Duration**. From the list box, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



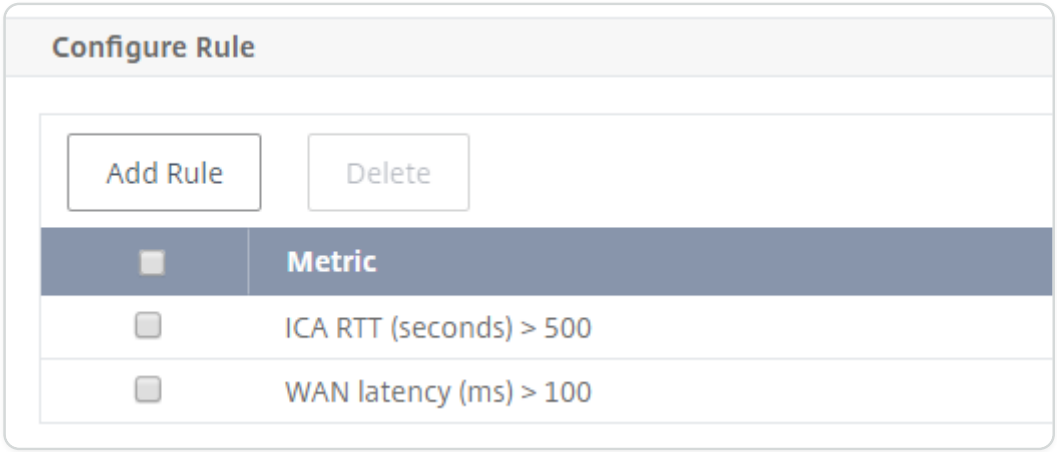
3. Creating threshold rules group for all entities:

   For HDX traffic, you must create a rule by clicking **Add Rule. E**nter the values in the **Add Rules** pop-up window that opens.



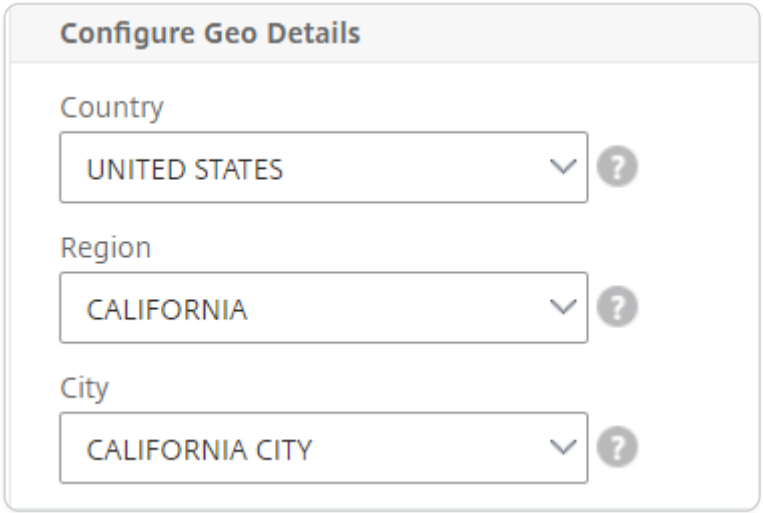
© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can create multiple rules to monitor each entity. Creating multiple rules in one single group allows you to monitor the entities as a group of threshold rules instead of individual rules. Click **OK** to close the window.



4. Configuring Geolocation tagging for Users entity

   Optionally, you can create a location-based alert for the user entity in the **Configure Geo Details** section. The following image shows an example of creating a geolocation based tagging to monitor WAN latency performance for users on the west coast of the United States.



5. Click **Enable Thresholds** to allow NetScaler ADM to start monitoring the entities.
6. Optionally, configure actions such as email notifications and SMS notifications.
7. Click **Create** to create a threshold rule group.

Viewing HDX™ Insight reports and metrics

HDX insight provides complete visibility of the reports and metrics pertaining to HDX traffic on your NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view the HDX metrics for any selected entity. The views include the following categories of entities:

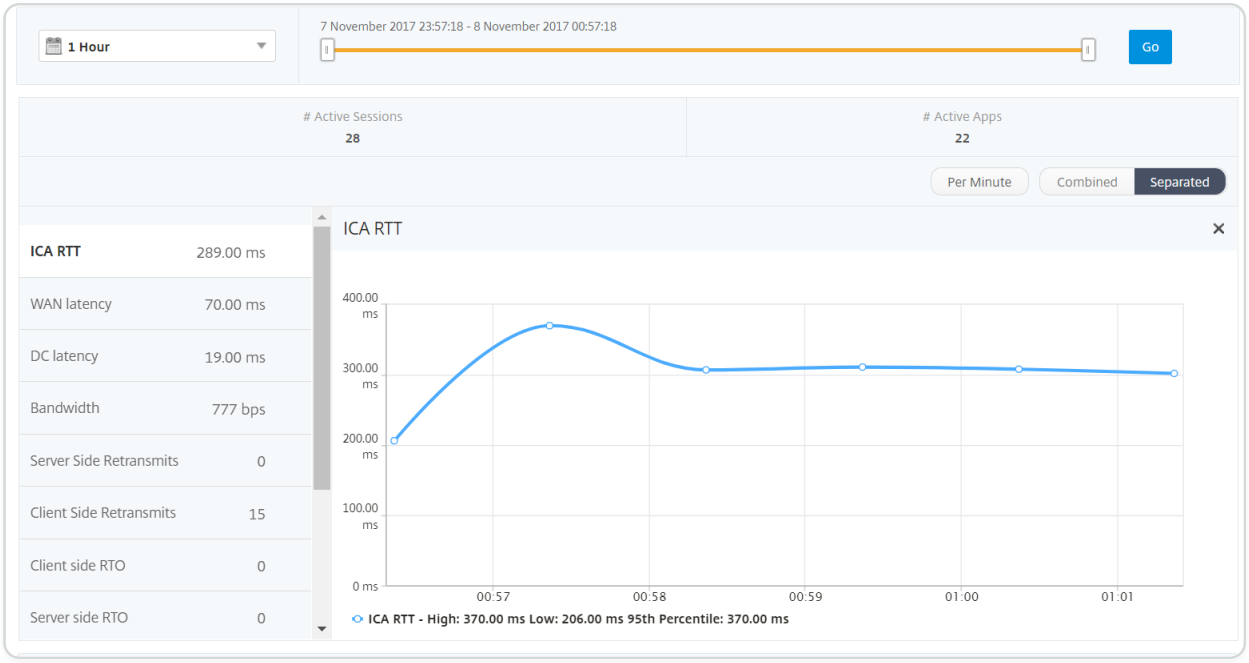
- **Users**: Displays the reports for all the users accessing the Citrix Virtual App or Desktop within the selected time interval.
- **Applications:** Displays the reports for total number of applications, and all related relevant information like the total number of times the applications were launched within the specified time interval.
- **Instances**: Displays the reports on the NetScaler instances that act as gateways for incoming traffic.
- **Desktops**: Displays the reports for the desktops used in the selected time frame.
- **Licenses**: Displays the reports for total SSL VPN licenses used within the specified time slot.

User view reports and metrics

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktops user.

To navigate to the users view:

1. Navigate to **Gateway > HDX Insight > Users**



User view reports and metrics consist of the following sections:

- Summary View
- Per User View

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Per User Session View

Summary view

The summary view displays the reports for all the users that have logged in during the selected timeline. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

To change the selected time period:

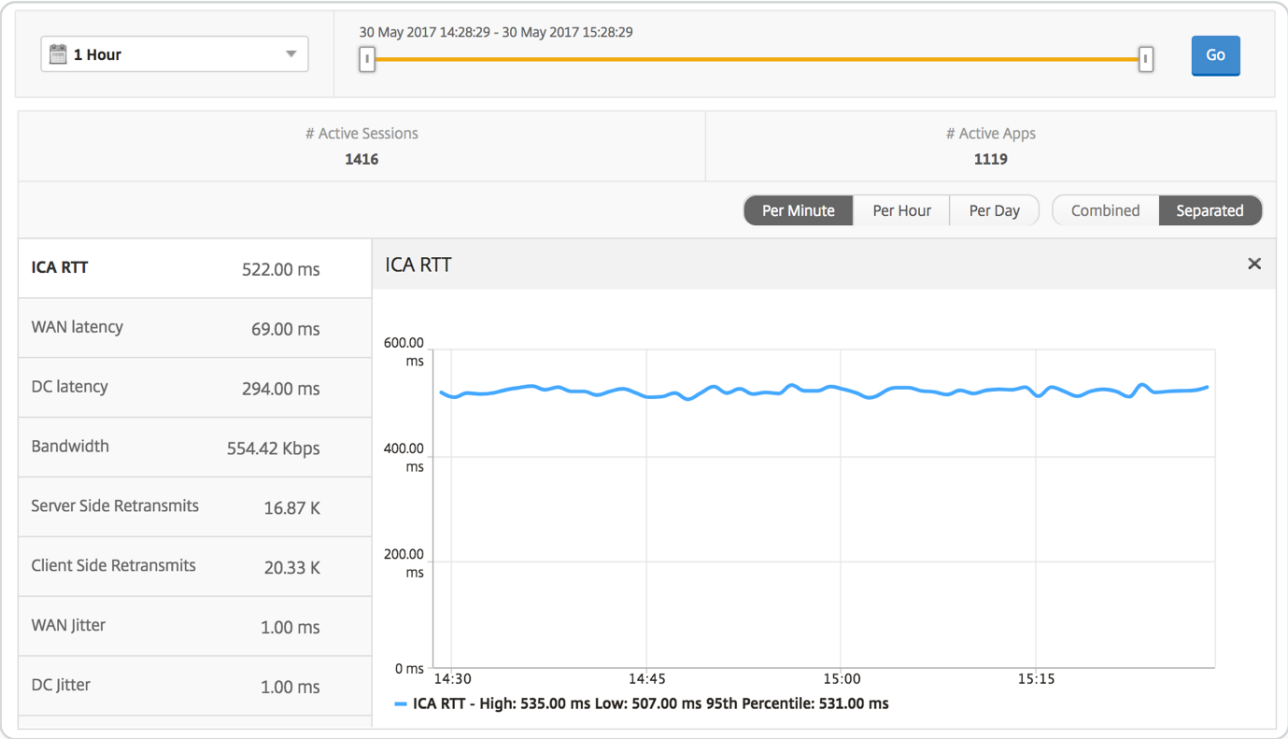
1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI OR CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

User summary report

Following are the metrics that are specific to this report.

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

Users

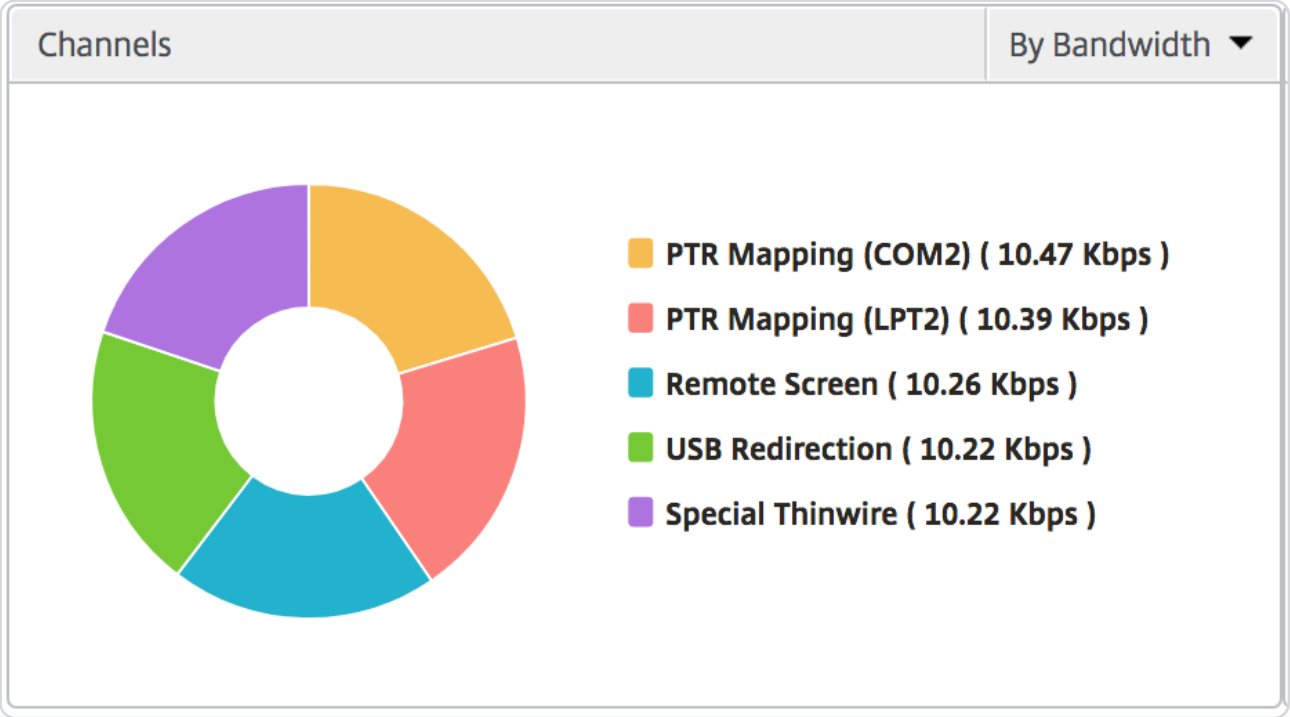
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

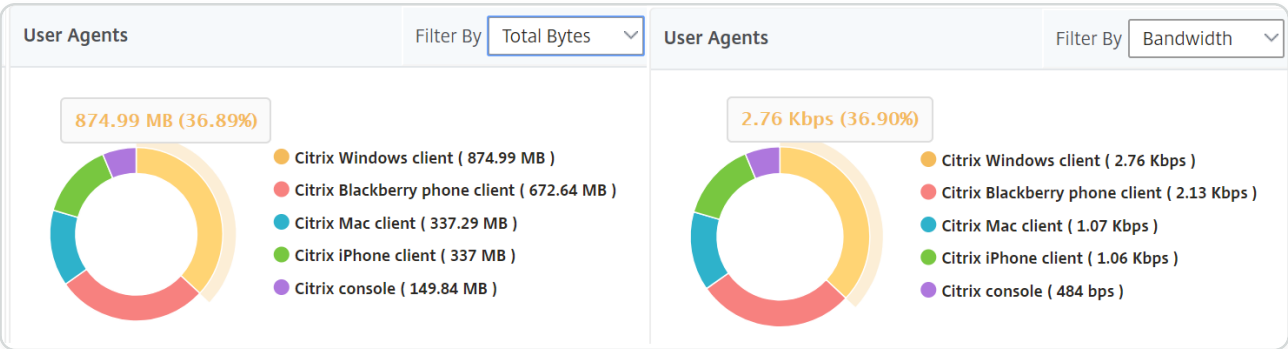
Channels

Channels represent the overall bandwidth or the total bytes consumed by each ICA® virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

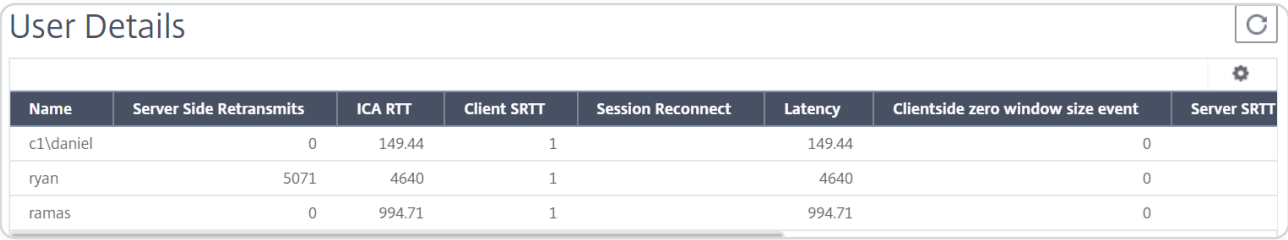


User agents

User agents represent the overall bandwidth/total bytes consumed by each workspace client in the form of a doughnut chart. Each colored segment in the chart represents one workspace client. The length of the segment depends on the number of users launching their applications on that workspace client. You can also sort the metrics by bandwidth, or total bytes.



Click each segment to view the details of the users using that workspace client.



Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Thresholds breach count

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period.

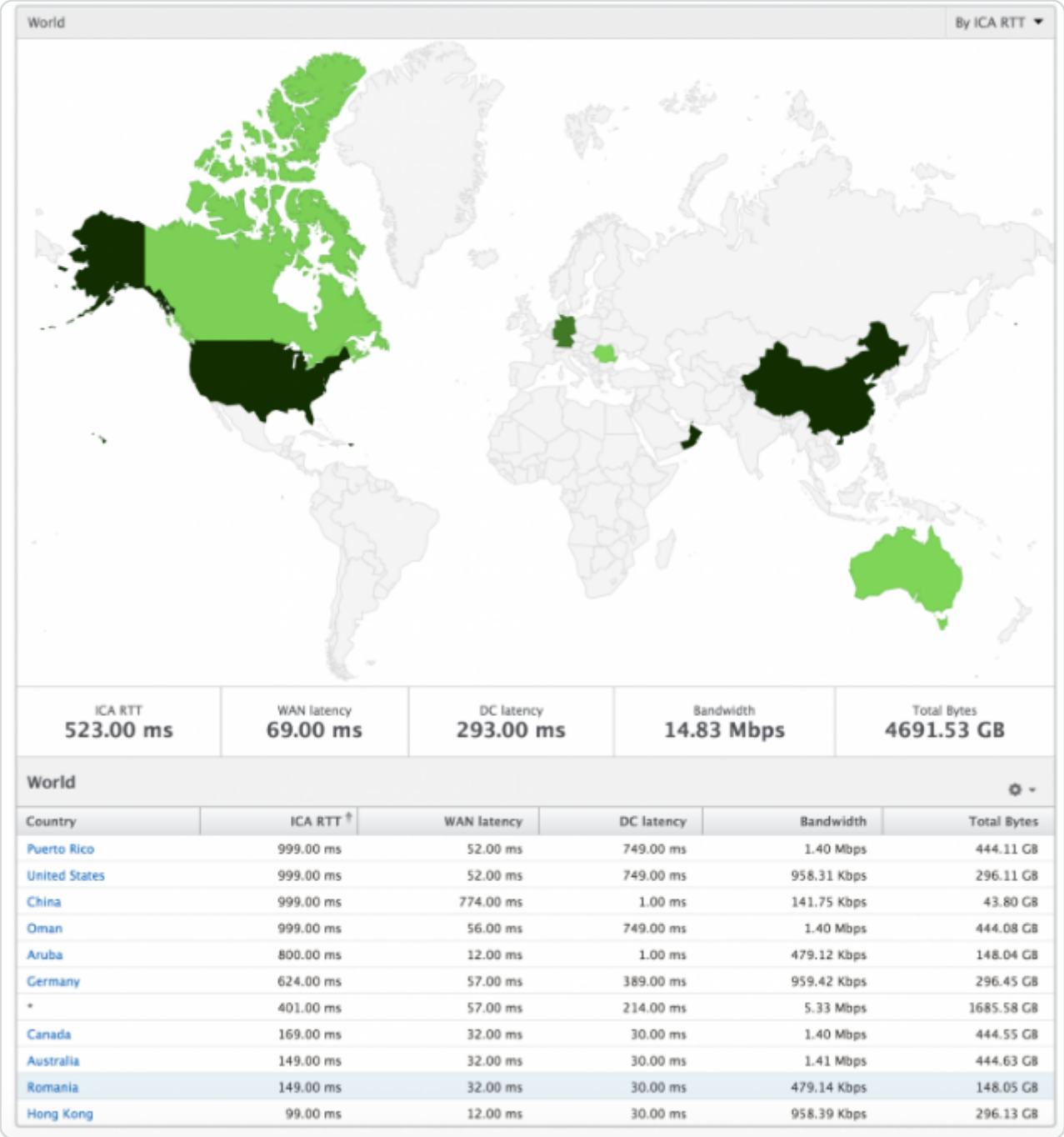
World map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per User view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Log on to your NetScaler® ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the Users summary report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.

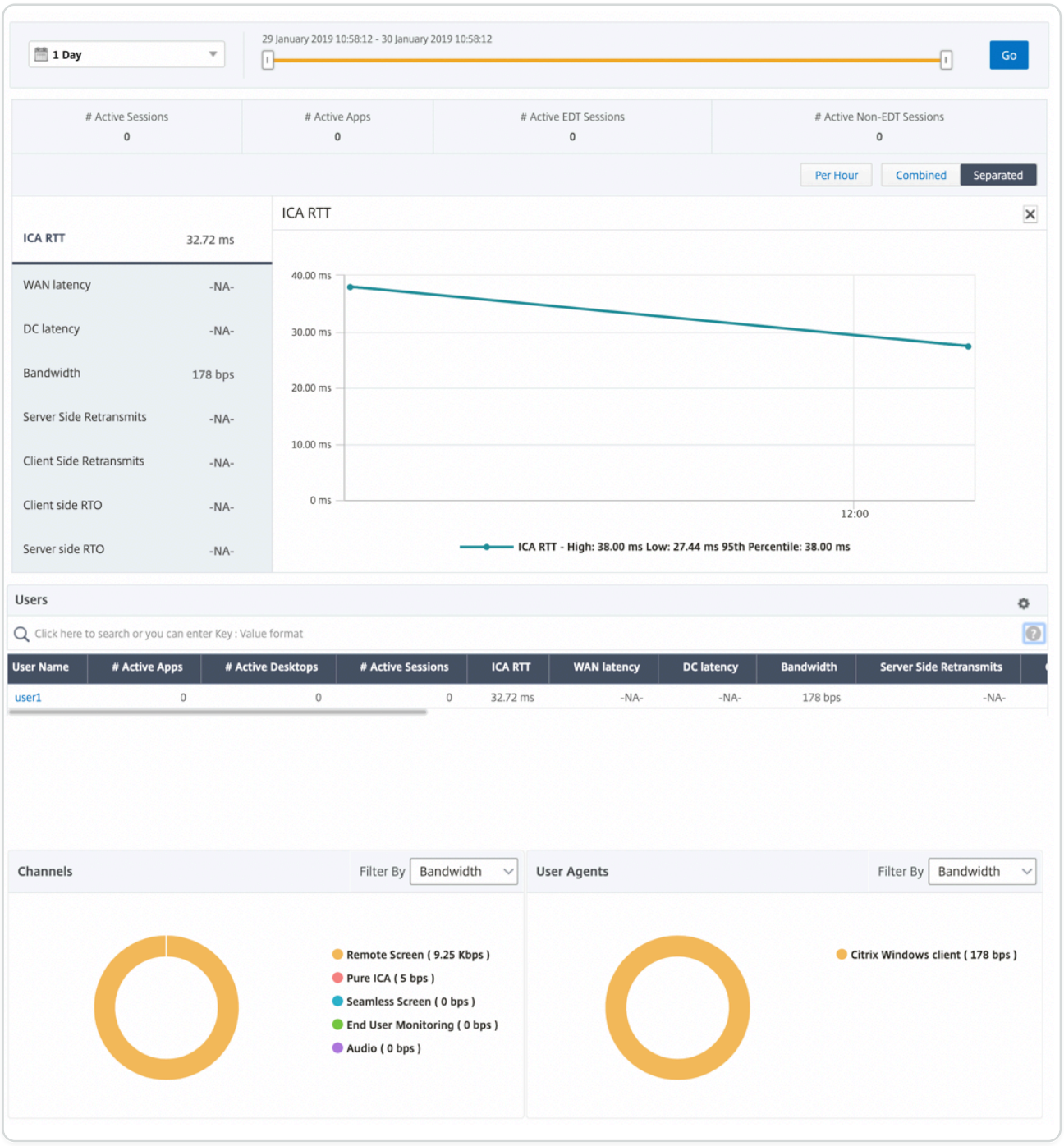
Support for EDT in HDX insight

NetScaler Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

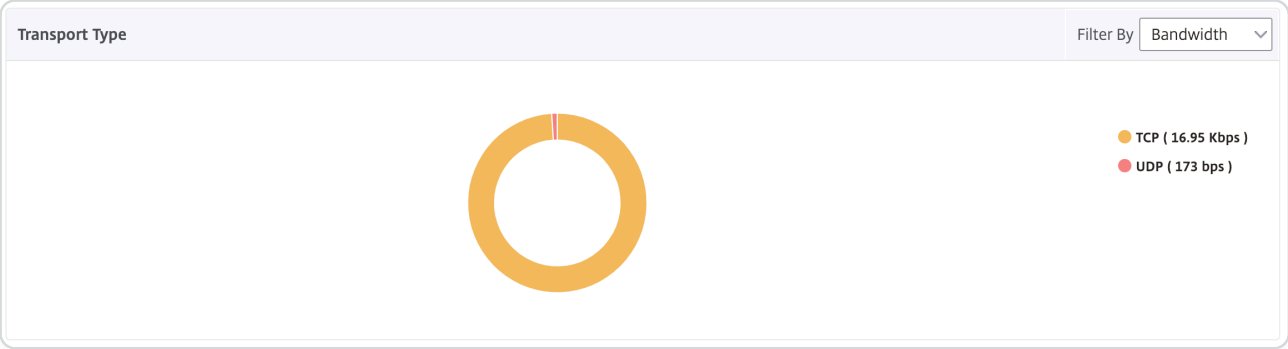
EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".



A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

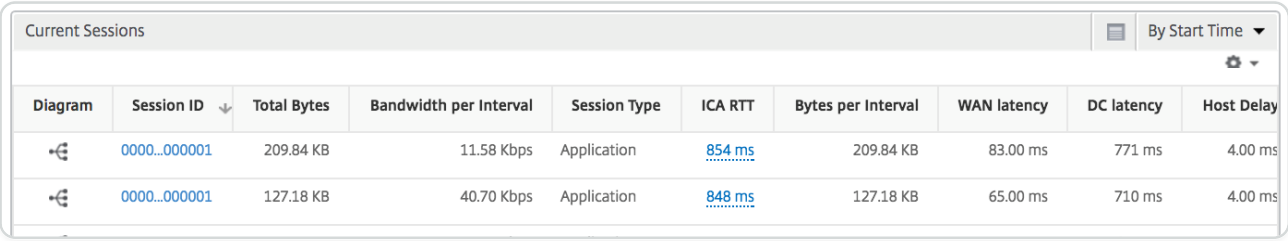


NOTE

EDT in HDX Insight is supported on NetScaler ADM from release 12.1 build 50.28 and is available on ADC instances from release 12.1 build 49.23.

HDX Insight metrics available from NetScaler ADM 12.0 and later:

L7 CLIENT-SIDE LATENCY	THE AVERAGE L7 LATENCY OBSERVED BETWEEN THE ICA CLIENT AND THE NETSCALER INSTANCE. THIS METRIC IS USEFUL IN CASE OF NON-CITRIX DEVICES BEING PRESENT IN THE DELIVERY PATH.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Terminated Sessions — By Start Time

Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB

Desktop users

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

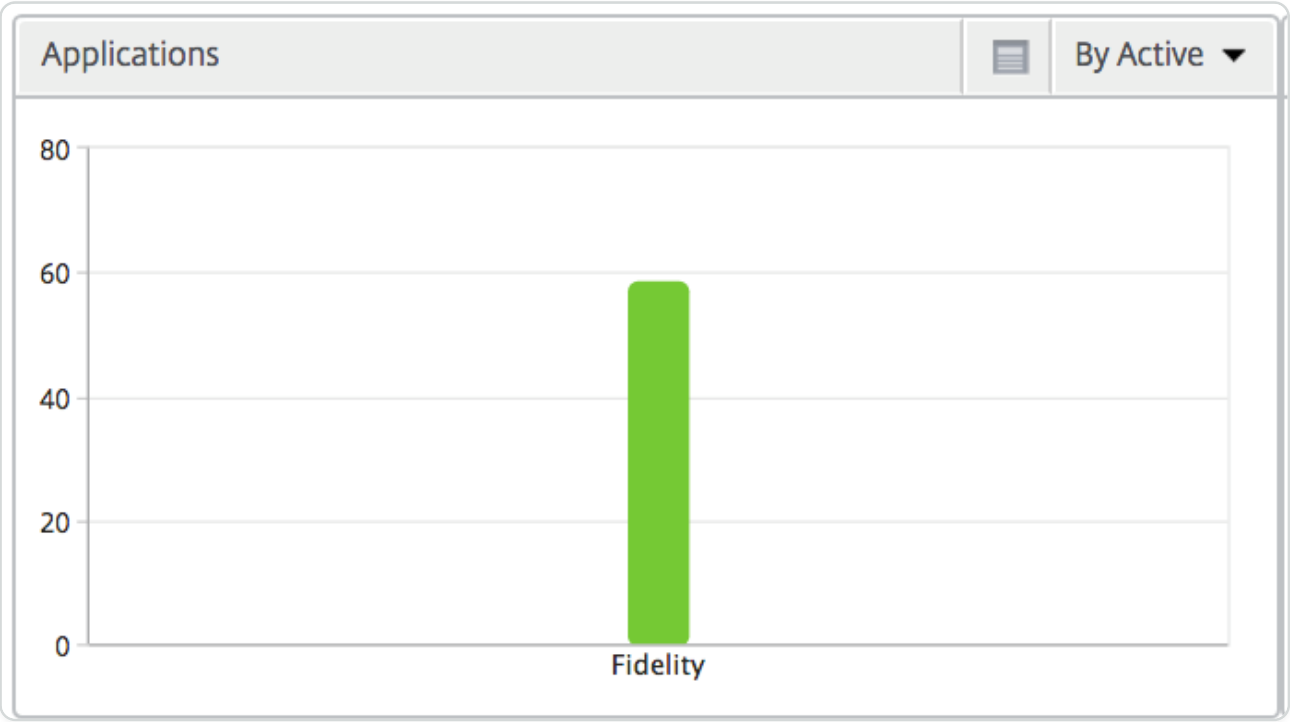
Desktop Users — By Desktop Launch Count

Name	Desktop Launch Count	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

Applications

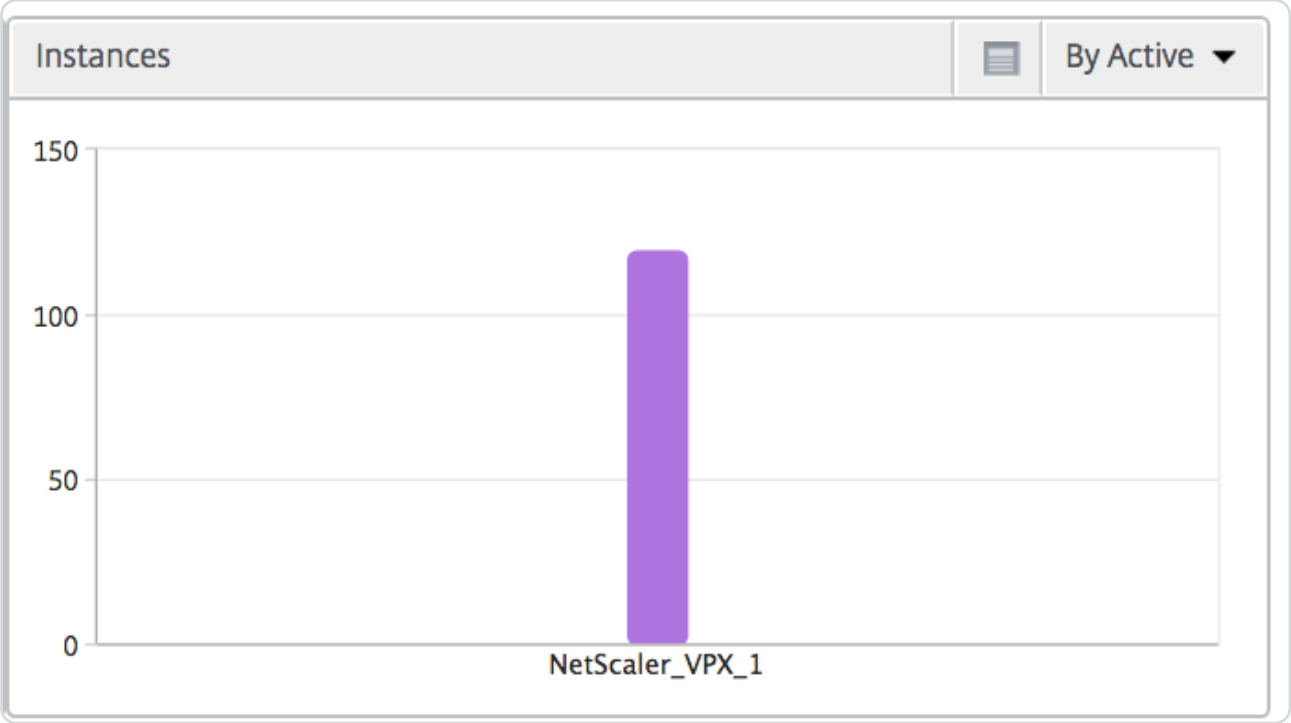
A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Instances

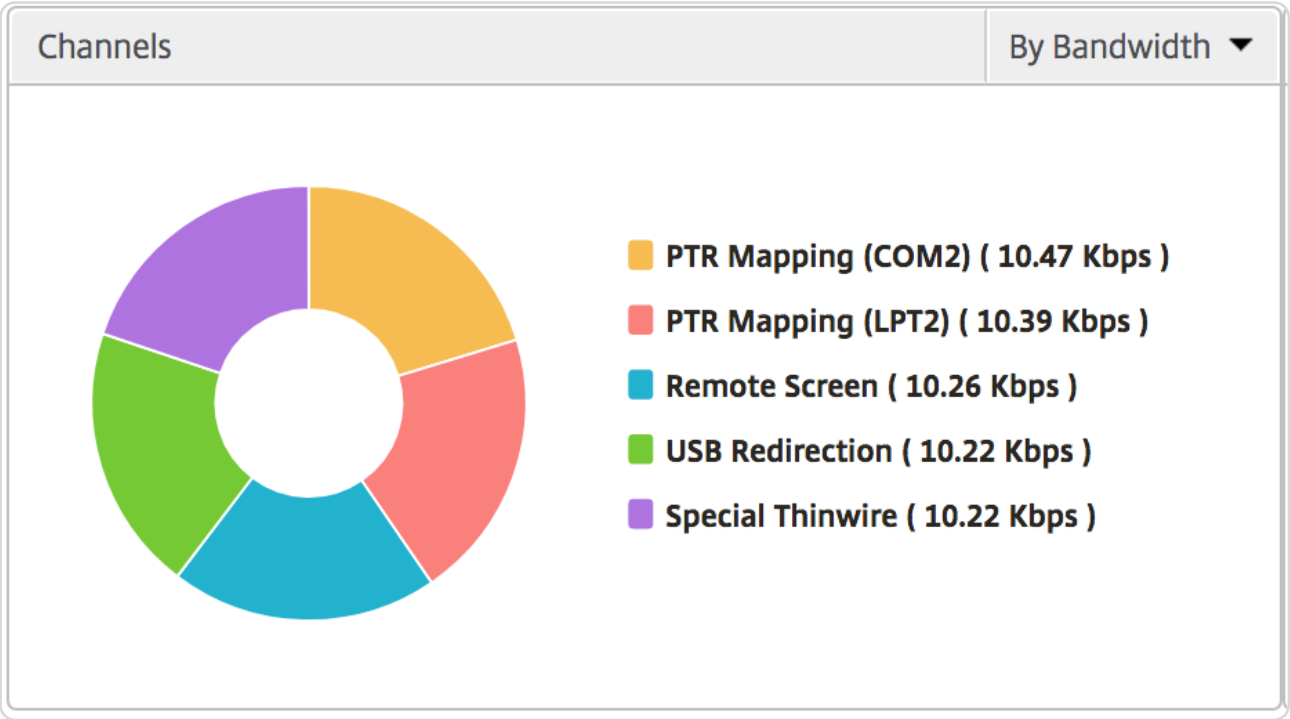
A bar graph representing NetScaler instances sorted by Active and total apps



Channels

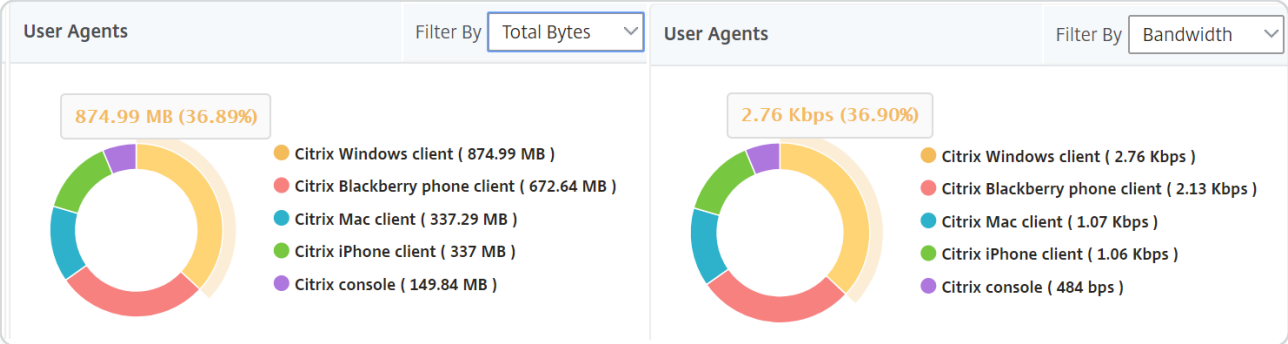
Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Per User session view

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

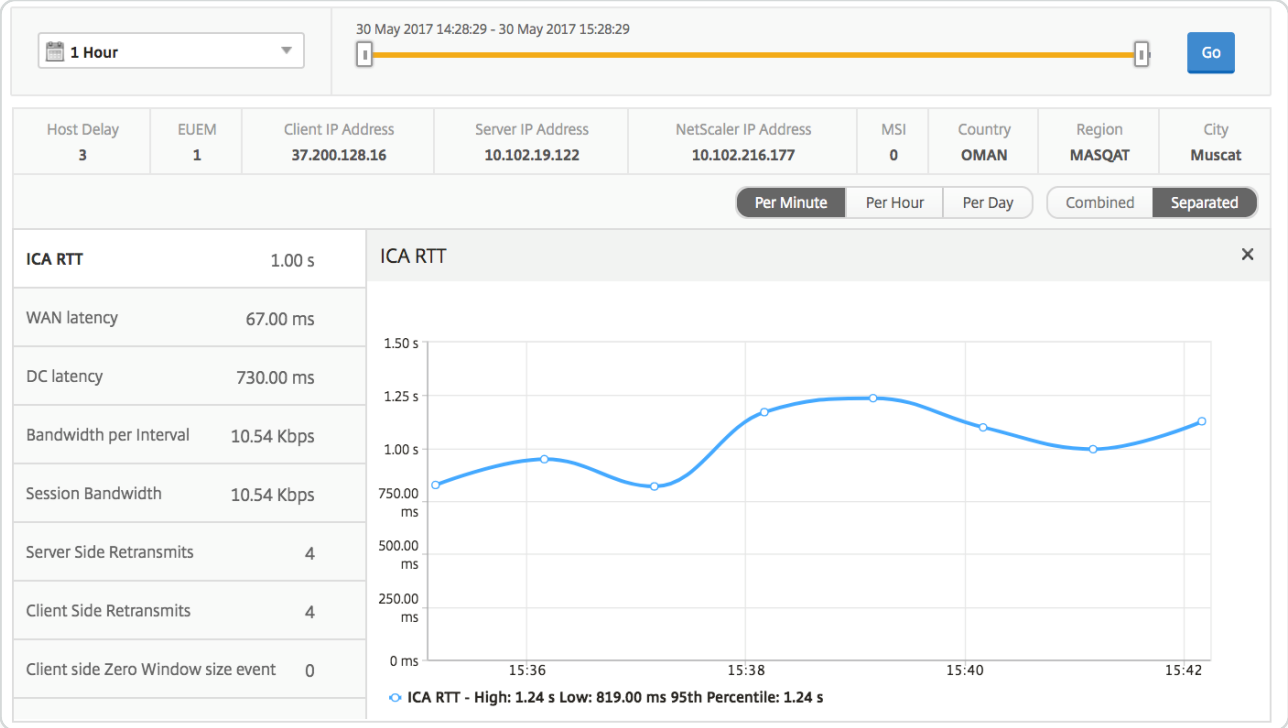
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Timeline chart

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.

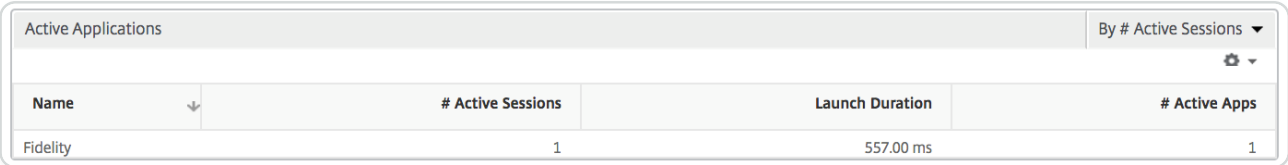
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



Active application

The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions

The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Related Sessions | By Common Server

Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

Application view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX Insight > Applications**.

Summary view

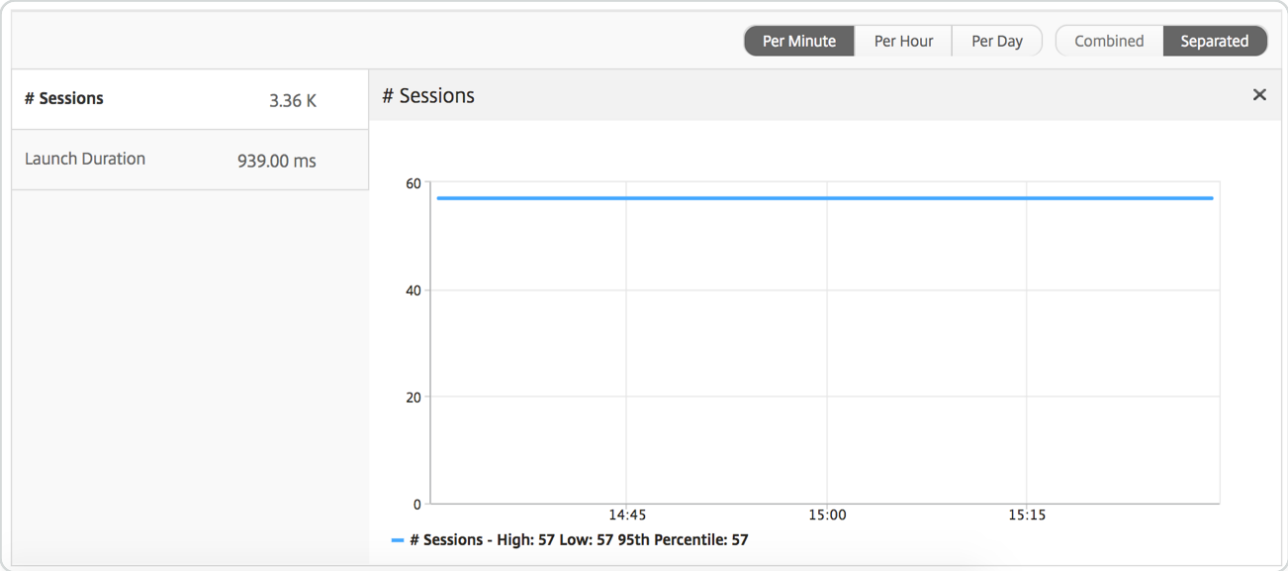
The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

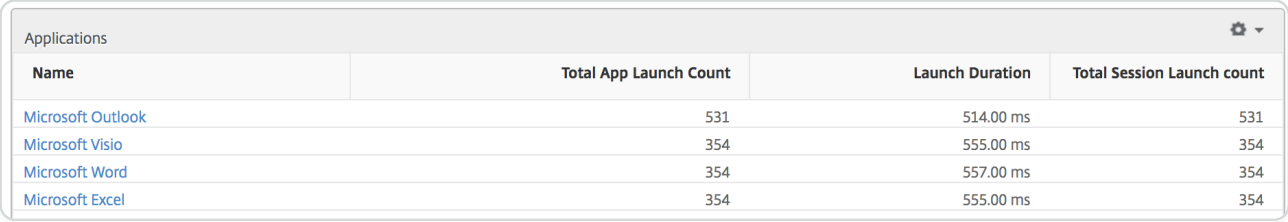
METRICS	DESCRIPTION
# Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Applications summary report

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.
Launch Duration	Average time taken to launch the Citrix Virtual App.



Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

Active application report

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive

© 1997–2026 Citrix Systems, Inc. All rights reserved.

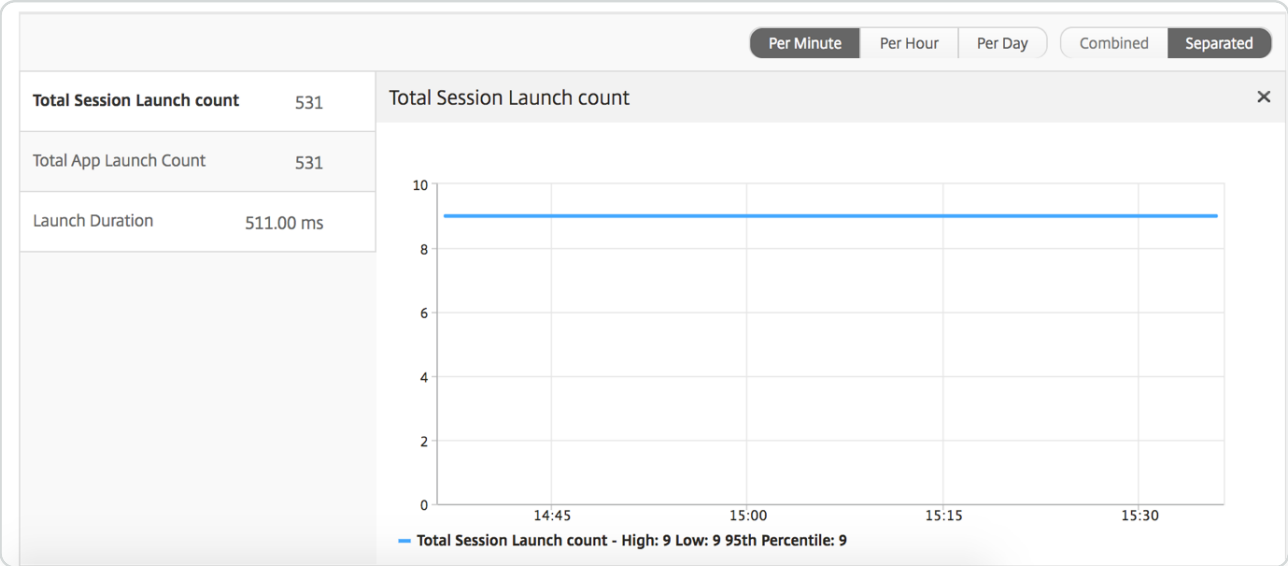
METRICS	DESCRIPTION
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.

Threshold report

The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Current sessions report

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

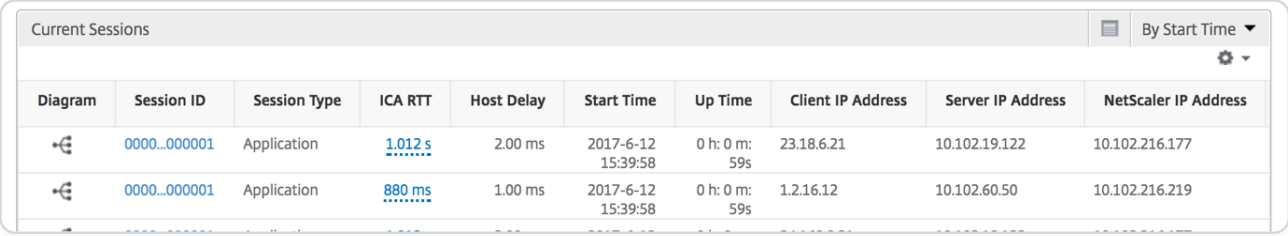
METRICS	DESCRIPTION
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.



Per application session view

The per application session view displays reports for a particular selected application session.

To view the Session reports:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Applications**.
3. Select a particular user from the Application Summary Report.
4. Selected a session from current sessions report.

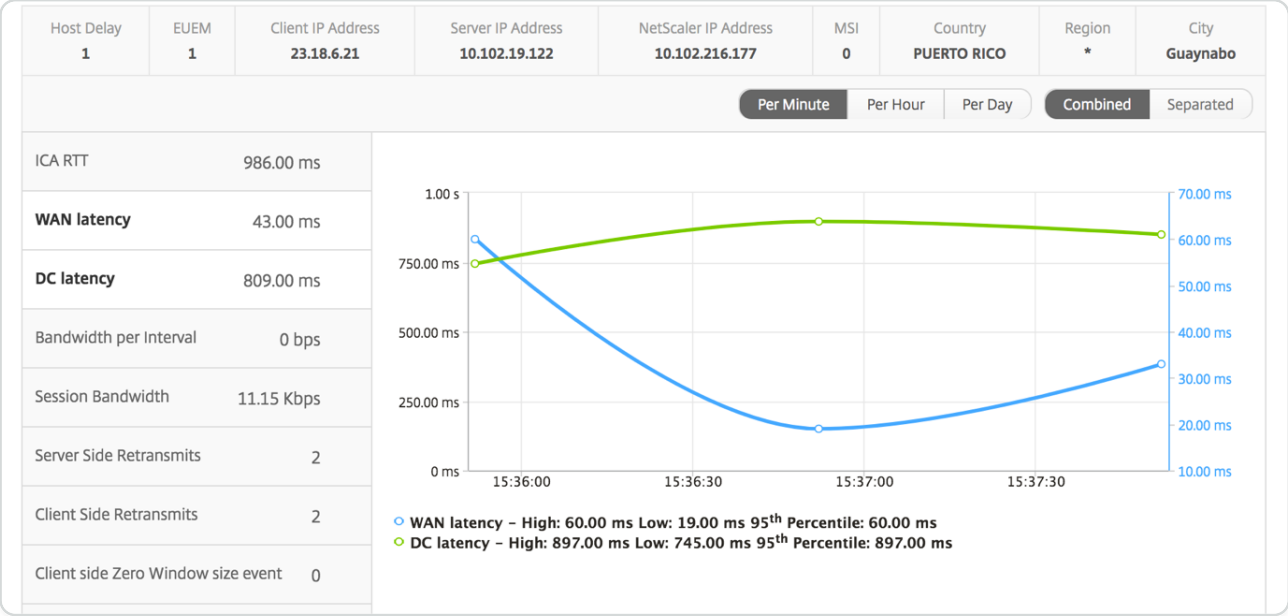
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart

METRICS	DESCRIPTION
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

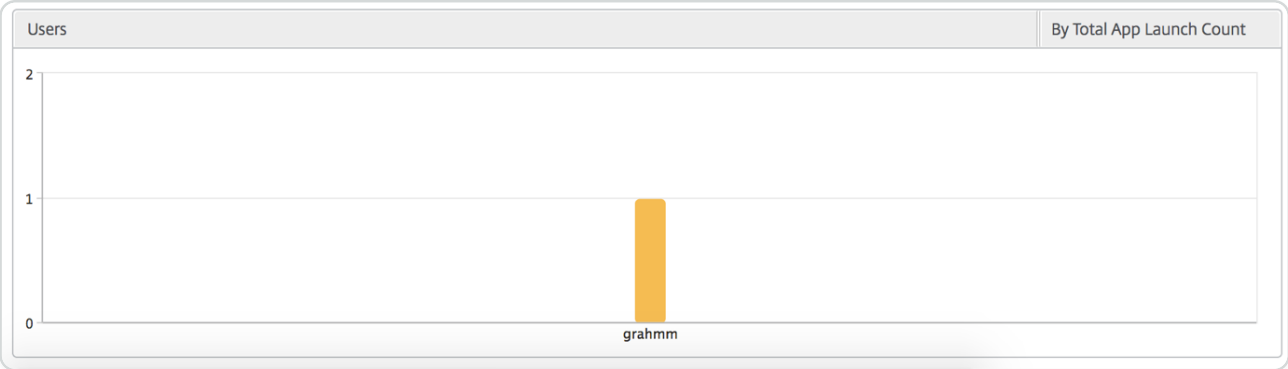
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



User bar graph

The User's bar graph represents the users logged into this particular app.



Desktop view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Log on to your NetScaler ADM using a supported web browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigate to **Gateway > HDX Insight > Desktop**.

Summary view

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless

© 1997–2026 Citrix Systems, Inc. All rights reserved.

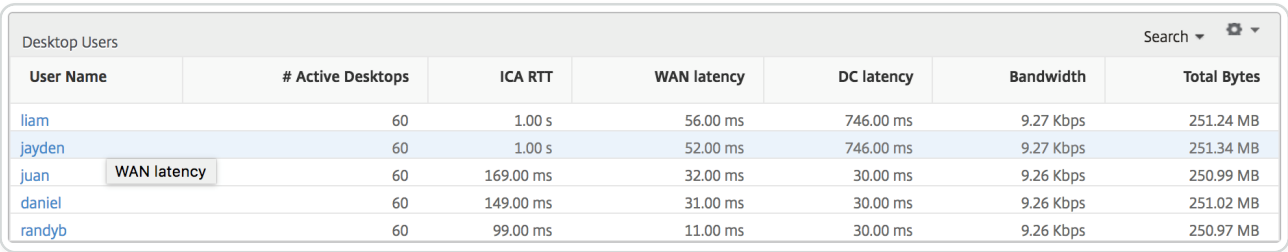
METRICS	DESCRIPTION
	but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

Desktop summary report

METRICS	DESCRIPTION
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.


Desktop Users

Search

User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

WAN latency

Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period. For more information, see how to create thresholds.

Per Desktop view

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

To navigate to the particular Desktop view:

1. Log on to your NetScaler ADM using a supported web browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

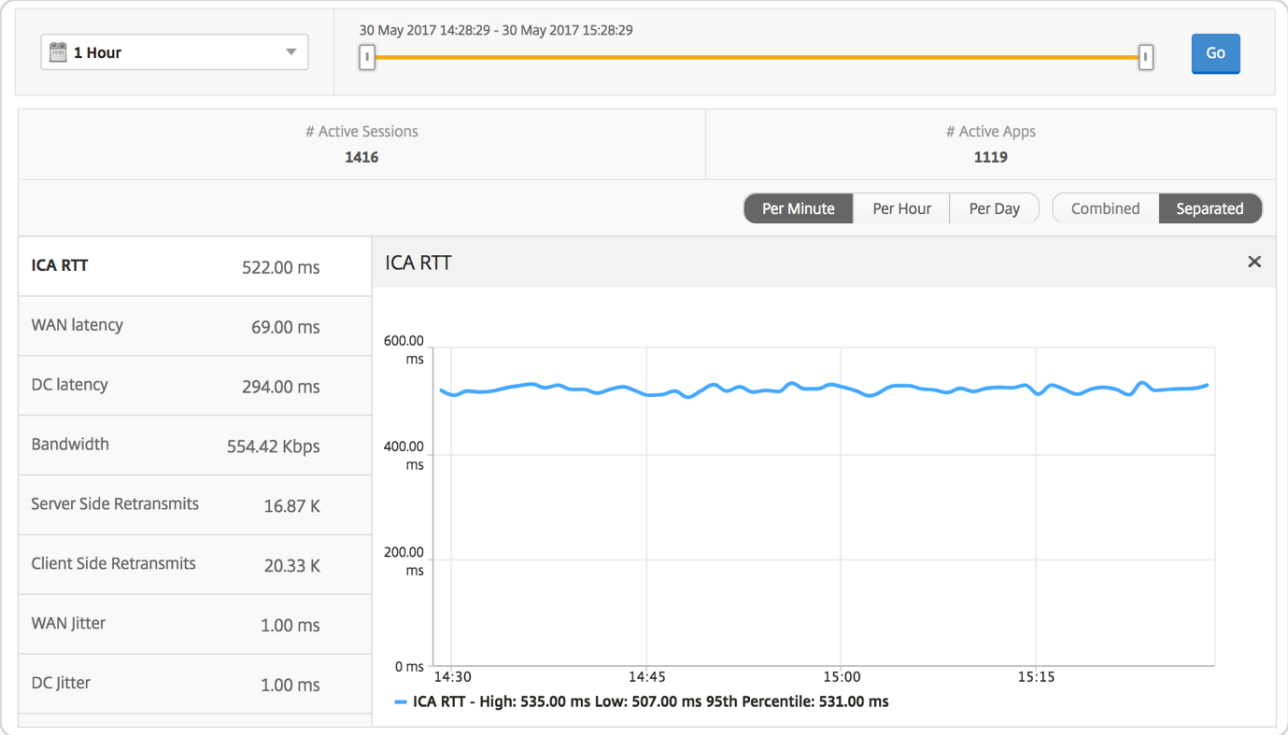
2. Navigate to **Analytics \> HDX Insight \> Desktop**.
3. Select a particular **Desktop** from the **Desktop Summary Report**.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



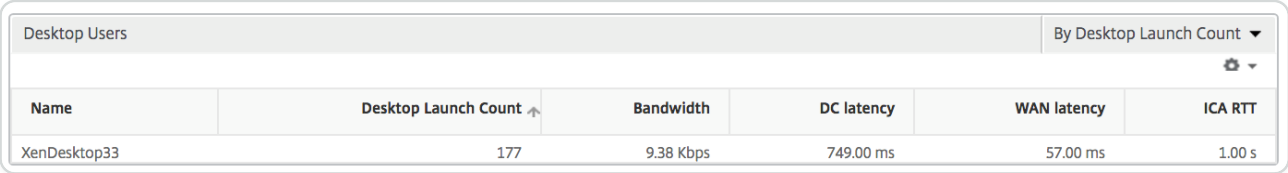
Desktop Users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



User Desktops Active/Inactive report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

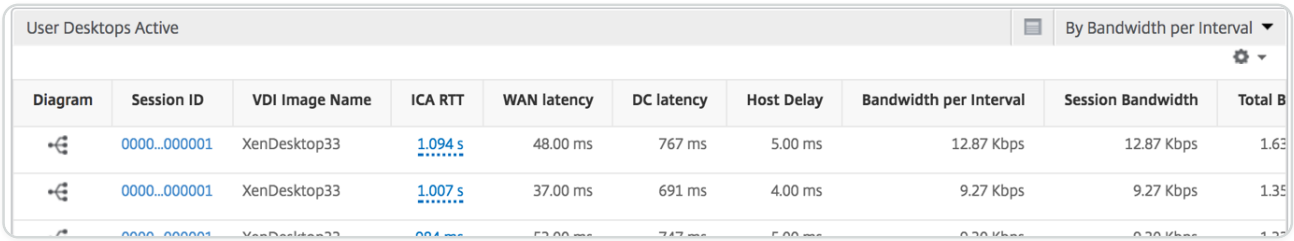
METRICS	DESCRIPTION
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per Desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics \> HDX Insight \> Desktop**.
3. Select a particular desktop from the **Desktop Summary Report**.
4. Select a session from current sessions report.

Timeline chart

The per user session view provides reporting for a particular selected user's session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

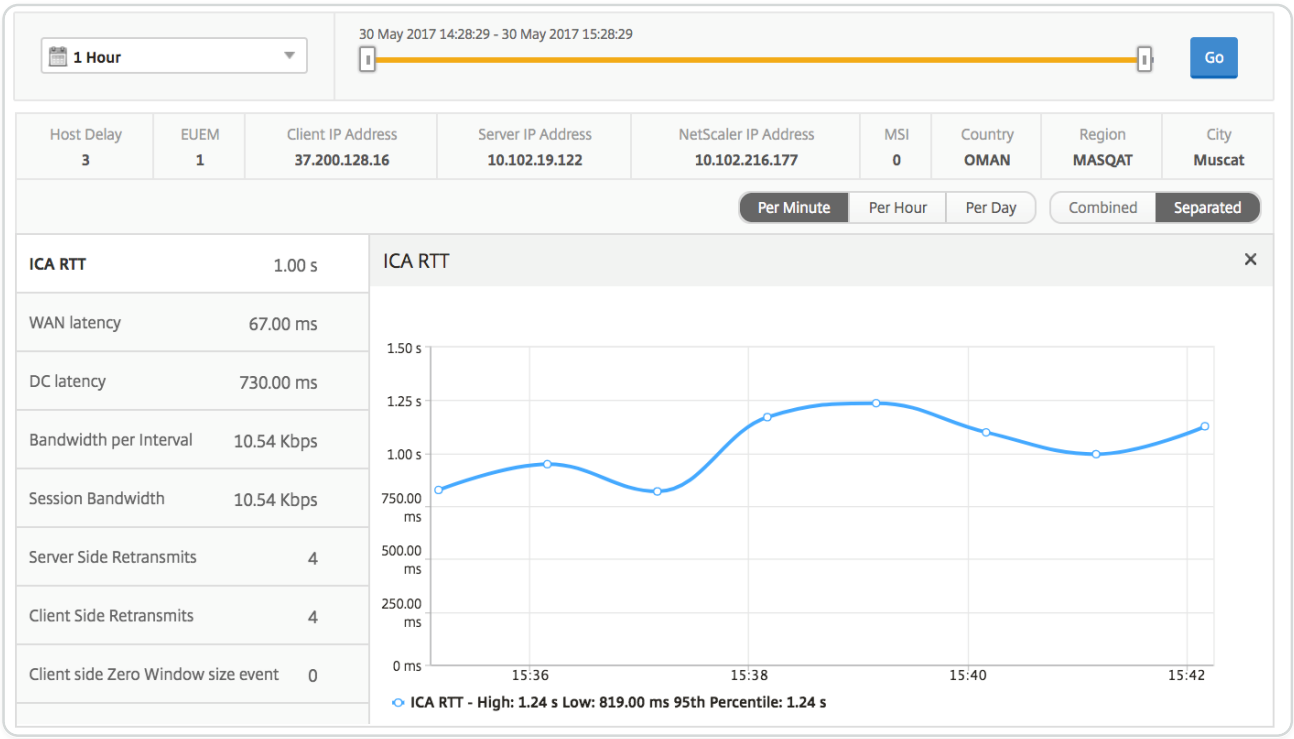
To view the metrics for a selected user's session:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the **User Summary Report** section.
4. Select a session from **Current Sessions** or **Terminated Sessions** column.

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



Related Desktop sessions report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

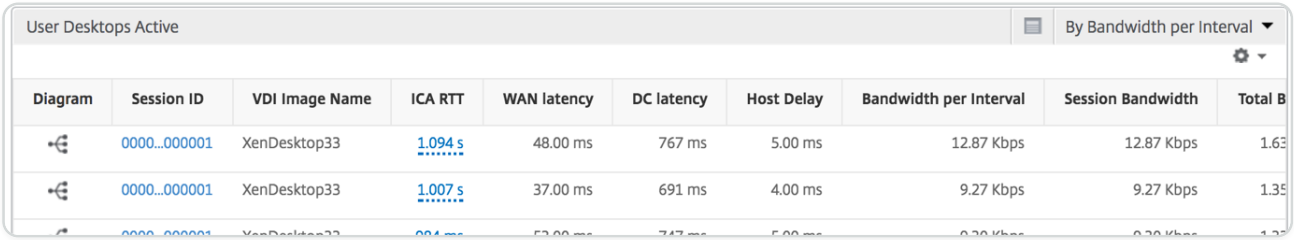
METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.



Instance view reports and metrics

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the Instance view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics \> HDX Insight \> Instances**.

Instance view reports and metrics consist of the following sections:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Instance Summary View
- Per Instance View

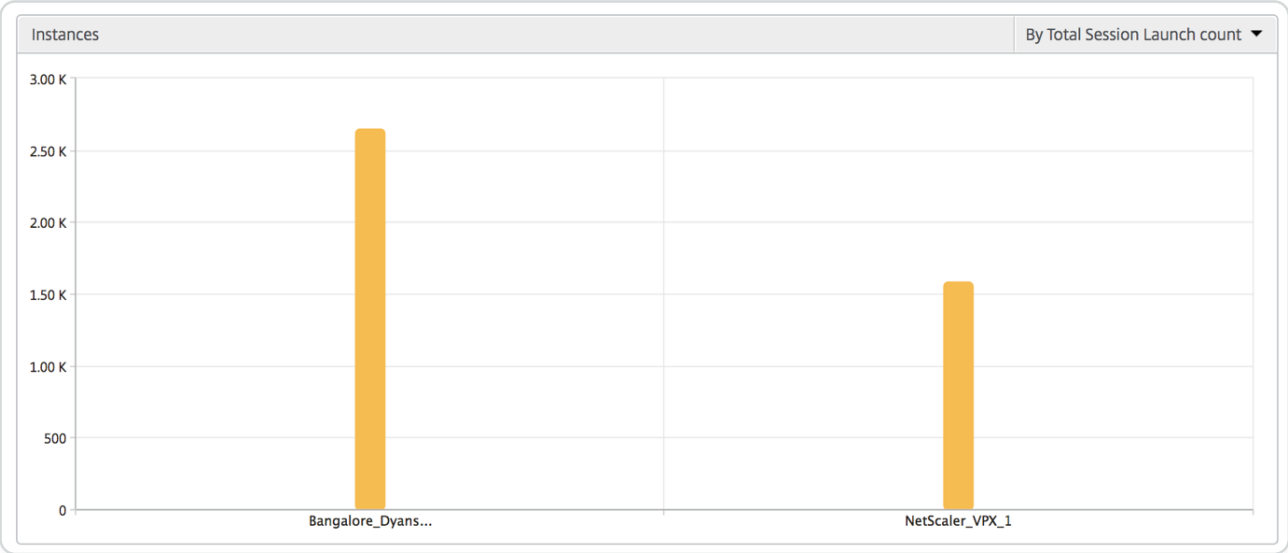
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler ADM.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

Instance bar graph

This graph displays the instance vs the Total Session Launch count | Total Apps which can be selected from the list on the top right on the graph canvas.



Instance/Active instances summary report

METRICS	DESCRIPTION
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Type	N/A

Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Threshold report

Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds.

Skipped flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type and so on This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.

Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

World view

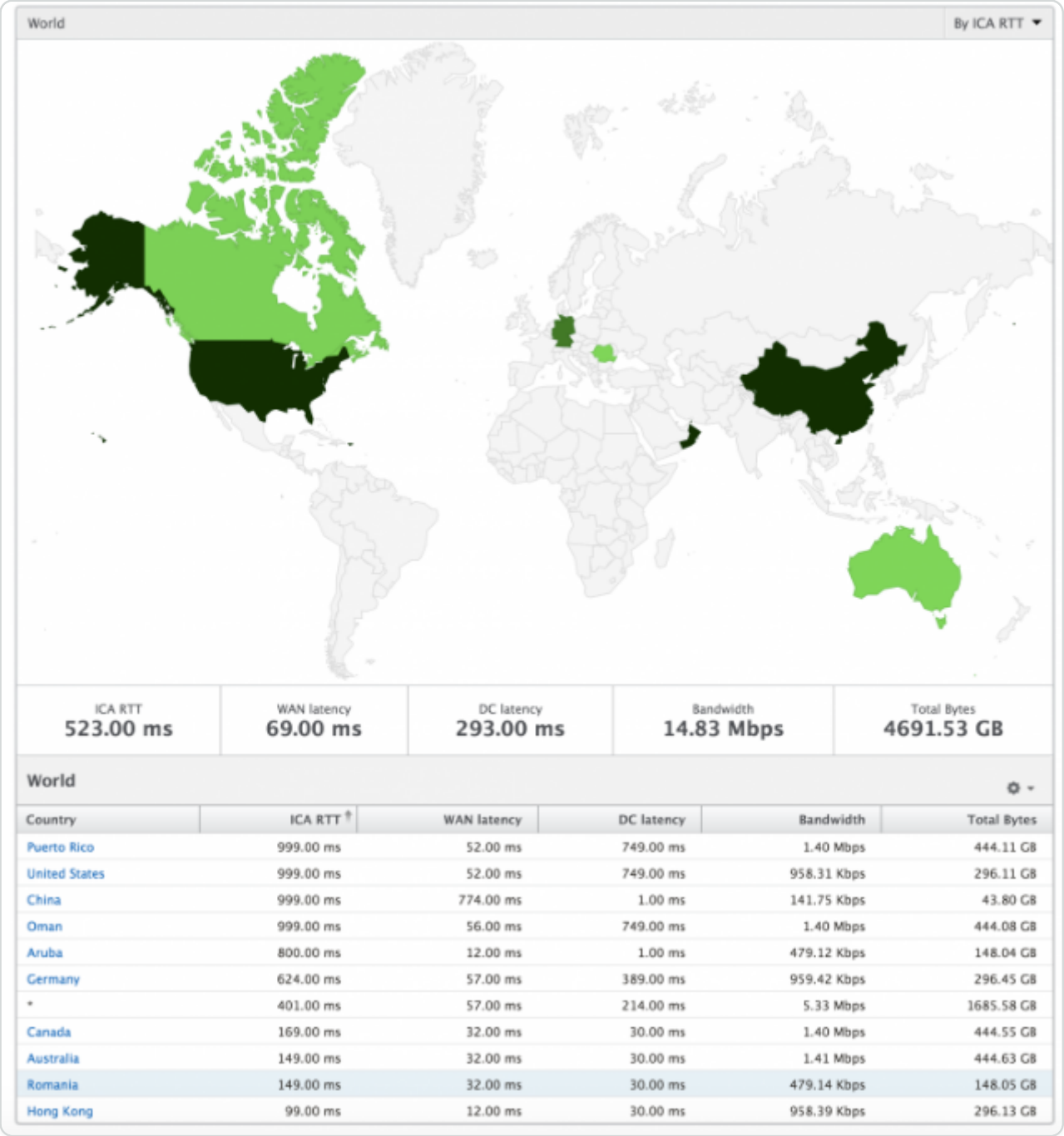
The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per instance view

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

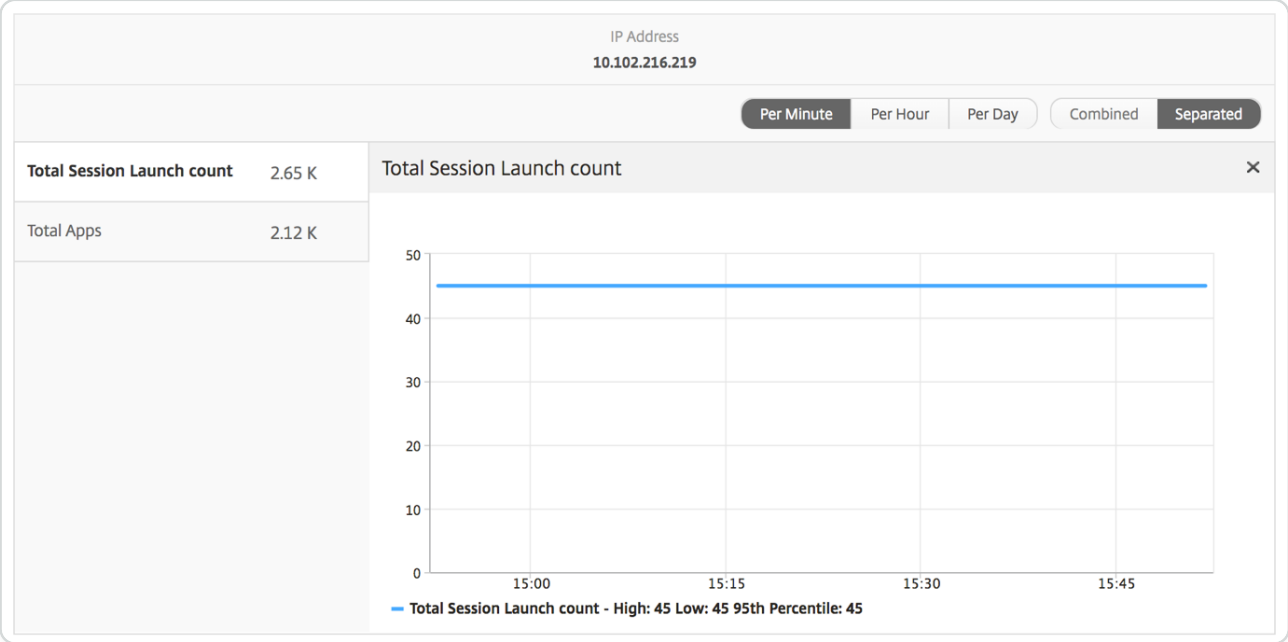
To navigate to the instance view:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics \> HDX Insight \> Instances**.
3. Select a particular instance from the **Instance Summary Report**.

Line chart

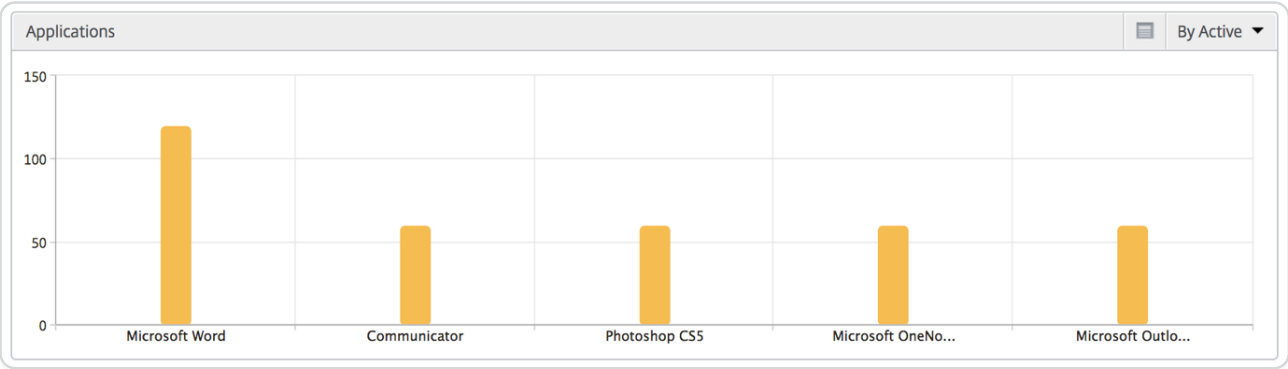
METRICS	DESCRIPTION
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



Applications bar graph

Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.

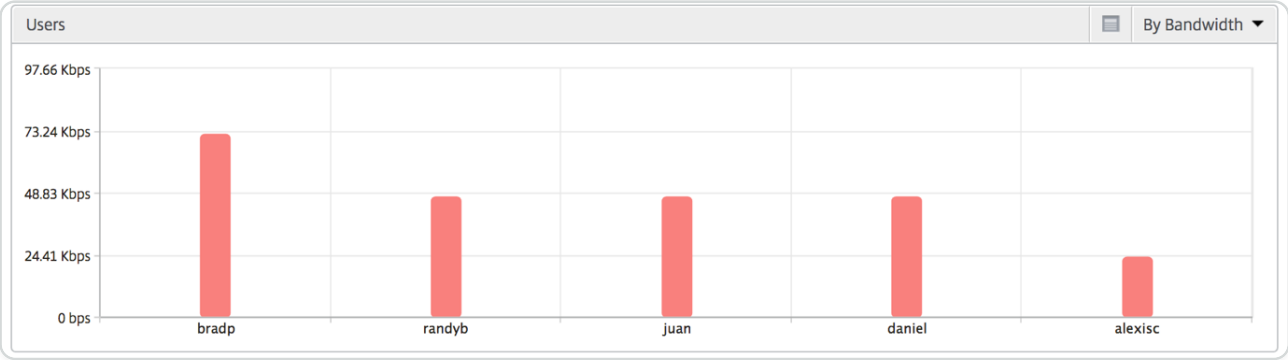
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Users bar graph

The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT



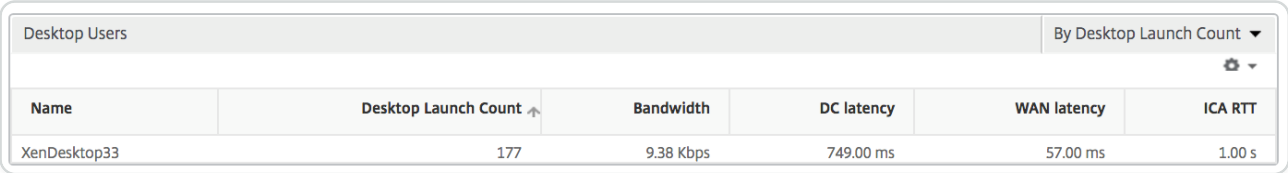
Desktop Users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



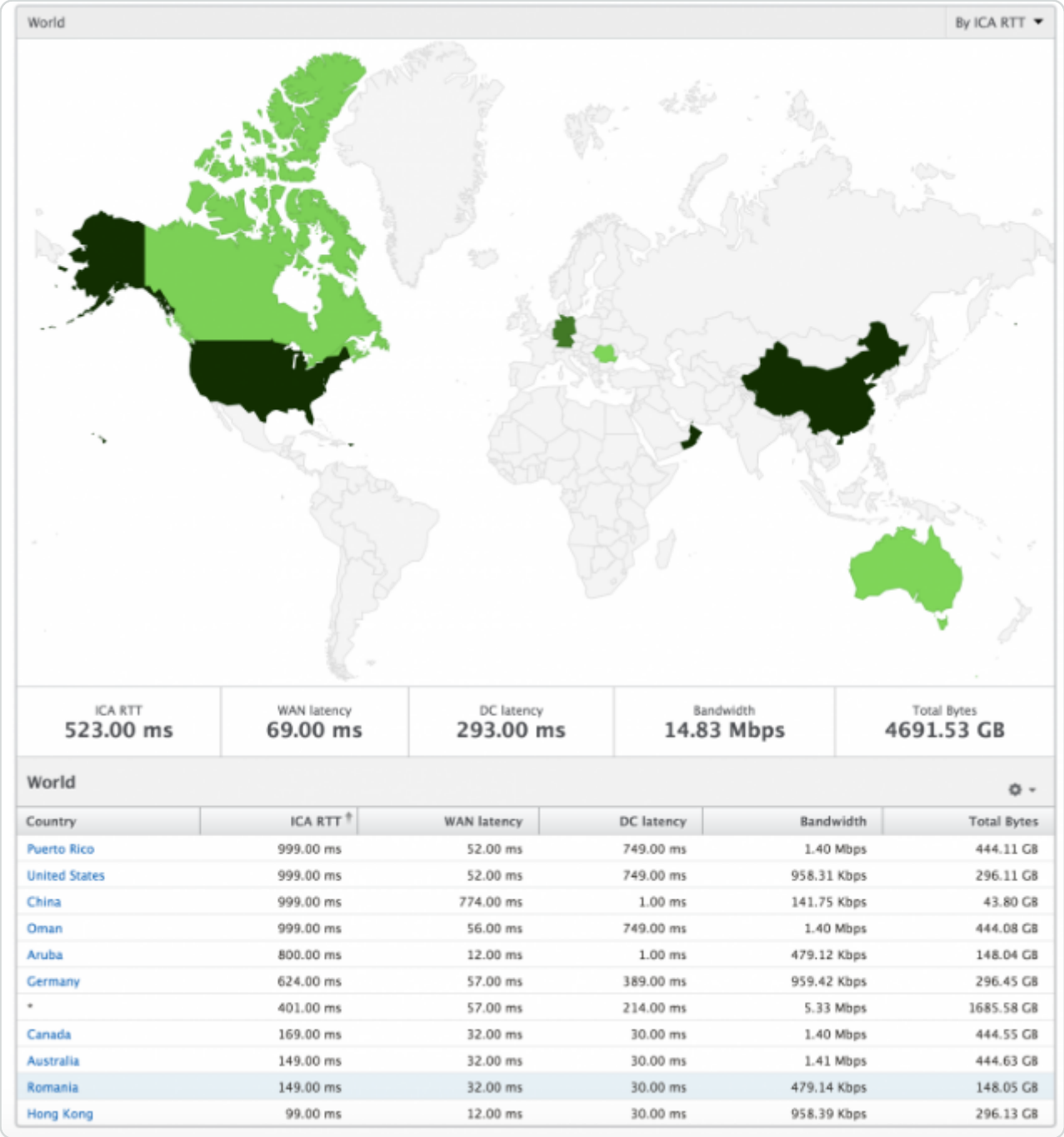
World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License view reports and metrics

The license view gives details on the NetScaler Gateway license information.

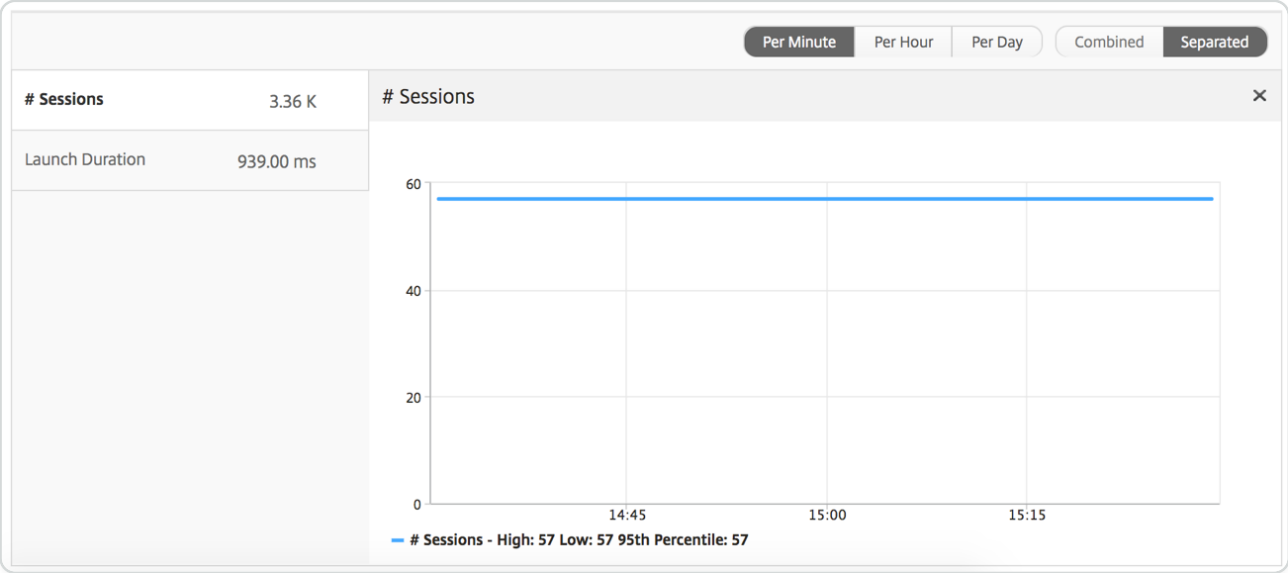
To navigate to the License view:

1. Log on to your NetScaler ADM using a supported web browser.
2. Navigate to **Analytics \> HDX Insight \> Licenses**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart

METRICS	DESCRIPTION
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds.

Application View Reports and Metrics

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX™ Insight > Applications**.

Summary view

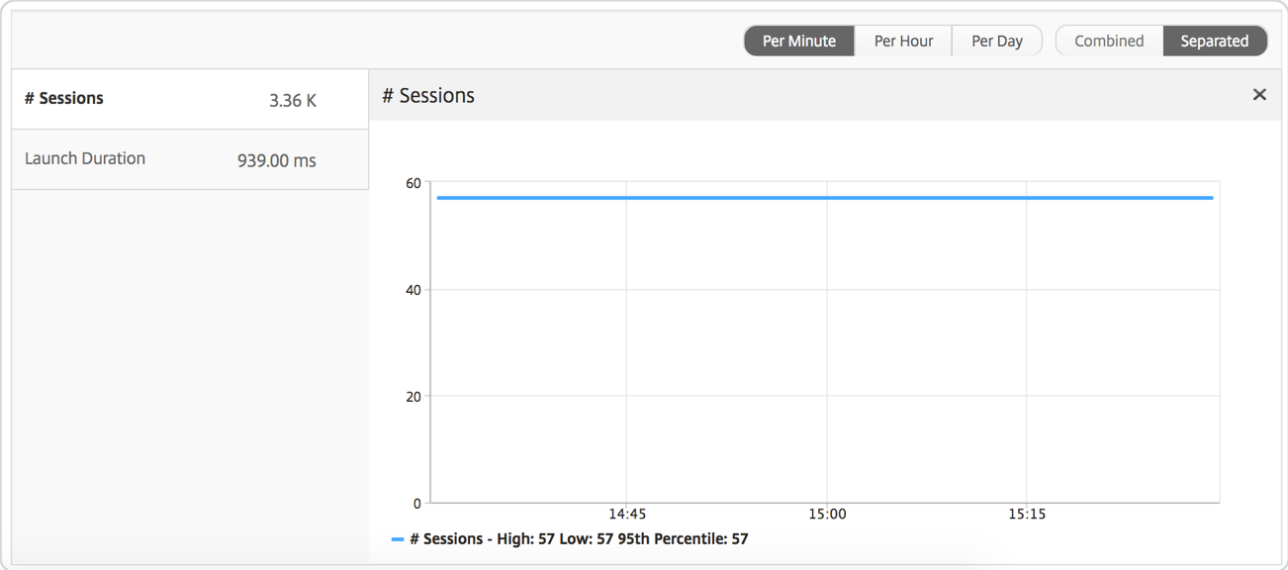
The summary view displays the reports for all the applications that are logged in during the selected timeline.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

METRICS	DESCRIPTION
# Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.



Applications summary report

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.
Launch Duration	Average time taken to launch the Citrix Virtual App.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

Active application report

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.

Active Applications

Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

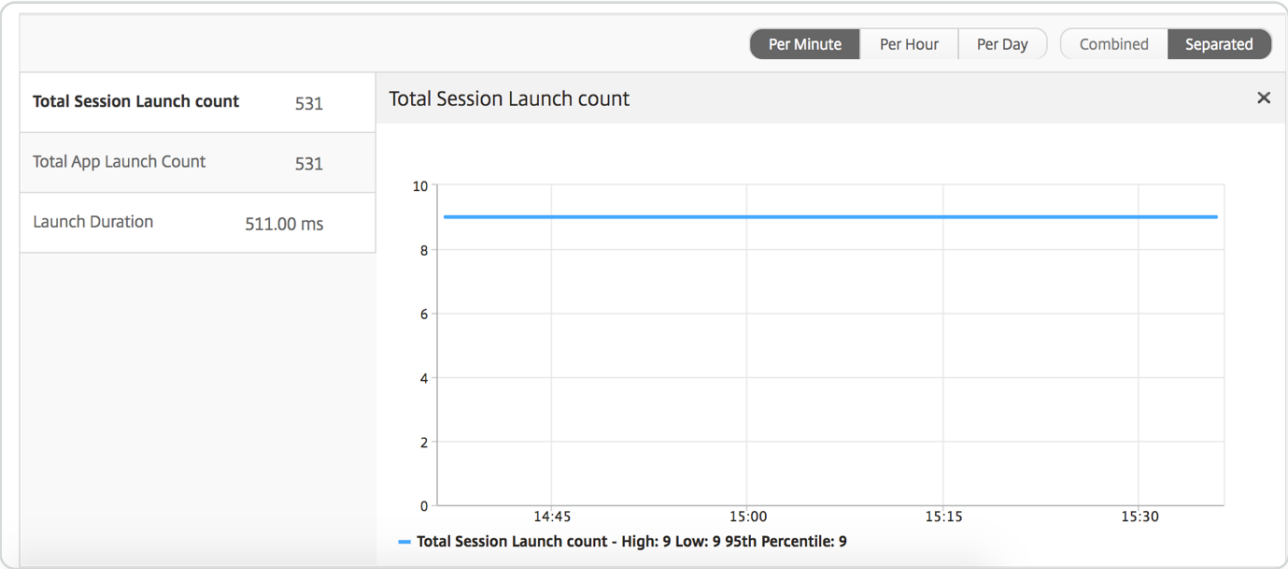
Threshold report

The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds and alerts.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Current sessions report

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

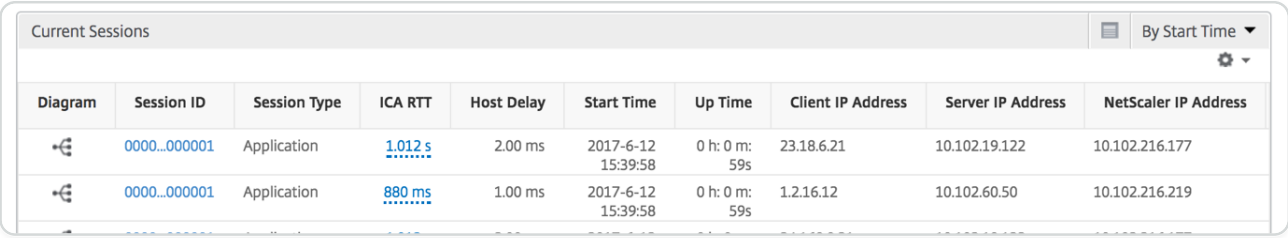
METRICS	DESCRIPTION
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in non-Citrix devices being present in the delivery path.



Per Application session view

The per application session view displays reports for a particular selected application session.

To view the Session reports:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

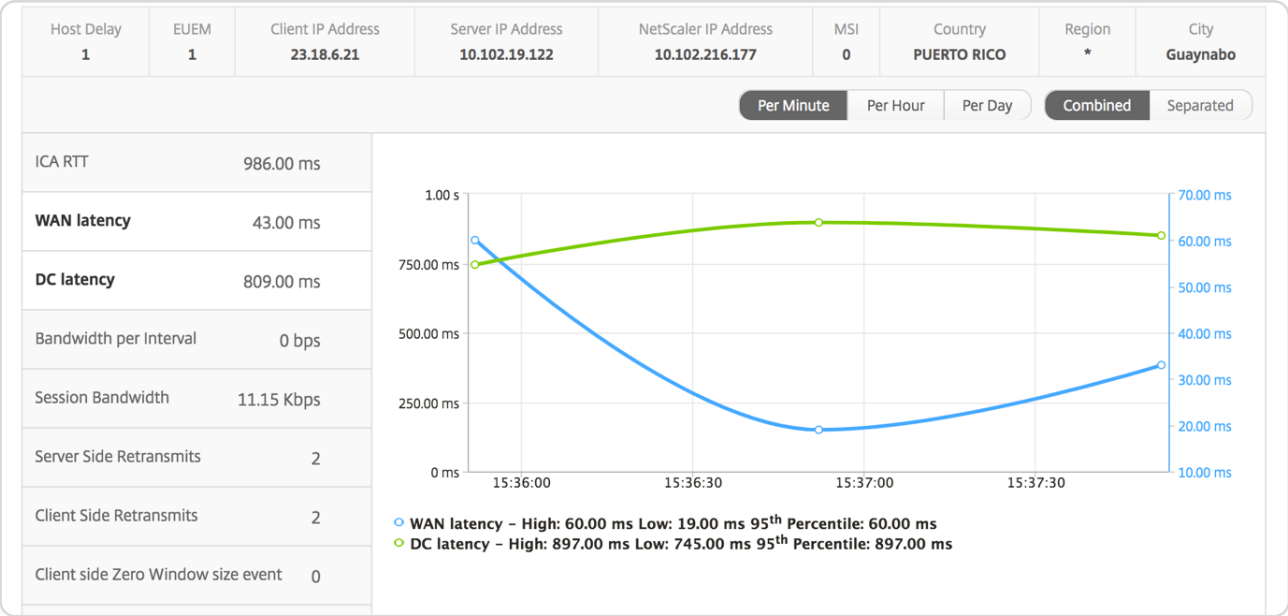
1. Navigate to **Gateway > HDX Insight > Applications**.
2. Select a particular user from the Application Summary Report.
3. Selected a session from current sessions report.

Line chart

METRICS	DESCRIPTION
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.

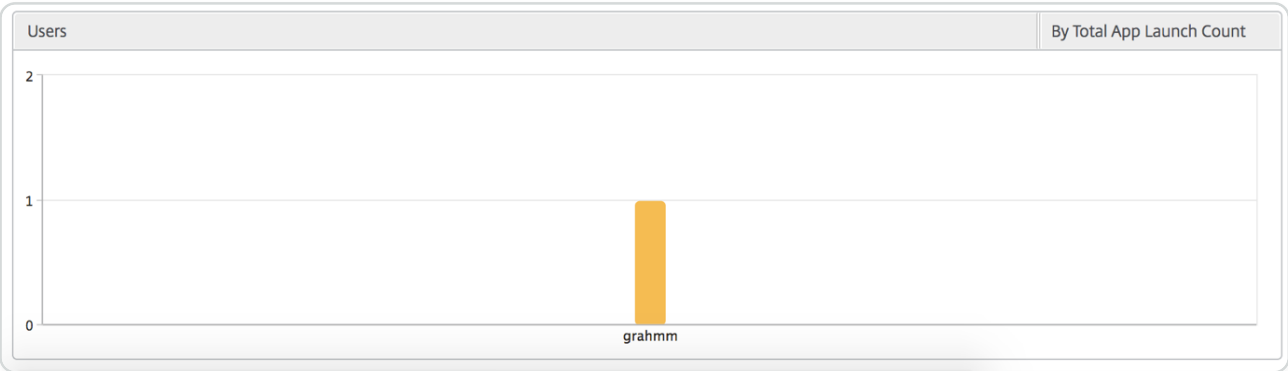
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



User bar graph

The User's bar graph represents the users logged into this particular app.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop View Reports and Metrics

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Navigate to **Gateway > HDX™ Insight > Desktop**.

Summary view

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

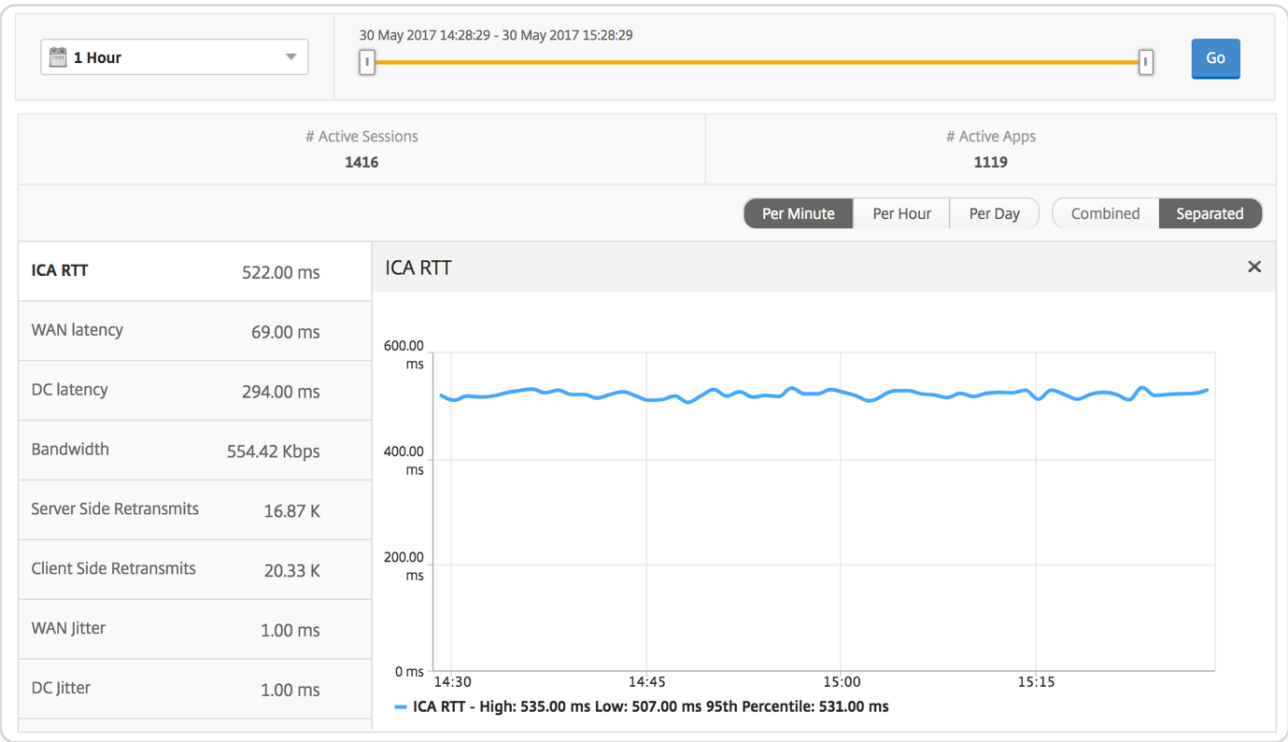
All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

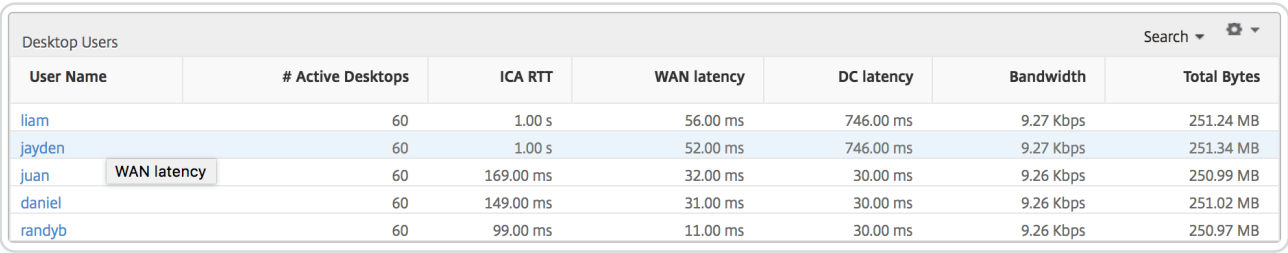
METRICS	DESCRIPTION
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop summary report

METRICS	DESCRIPTION
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.



User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To navigate to the particular Desktop view:

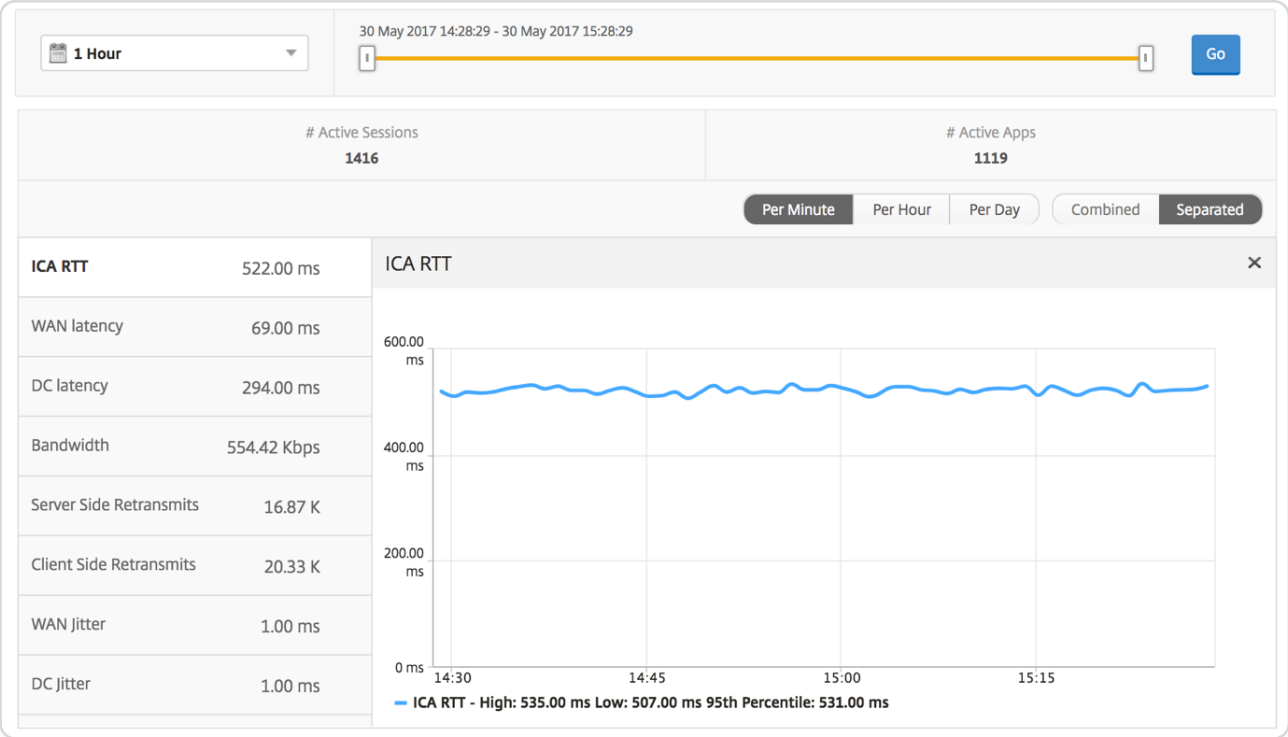
1. Navigate to **Analytics \> HDX Insight \> Desktop**.
2. Select a particular **Desktop** from the **Desktop Summary Report**.

Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



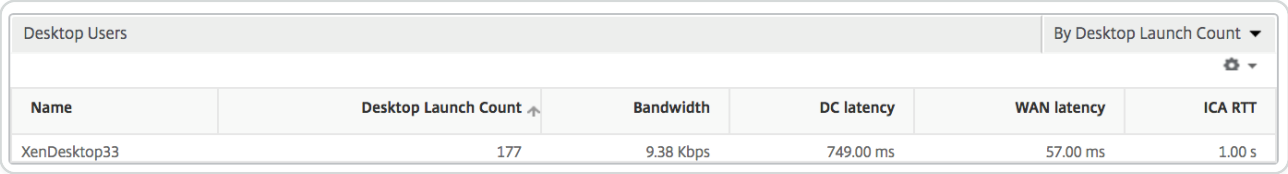
Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



User desktops active/inactive report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

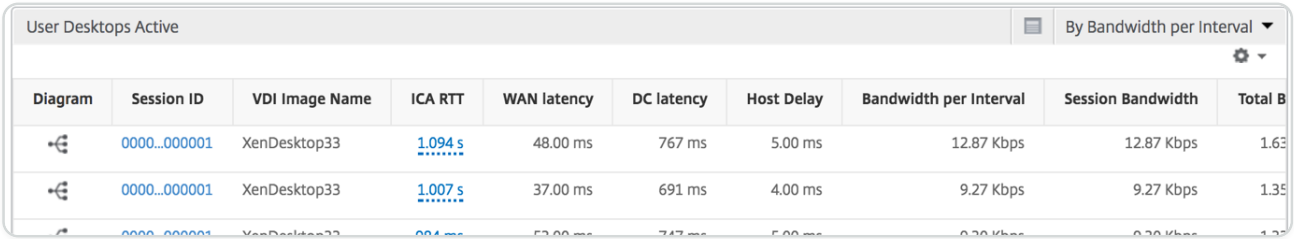
METRICS	DESCRIPTION
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
	but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Navigate to **Gateway > HDX Insight > Desktop**.
2. Select a particular desktop from the **Desktop Summary Report**.
3. Select a session from current sessions report.

Timeline chart

The per user session view provides reporting for a particular selected user's session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

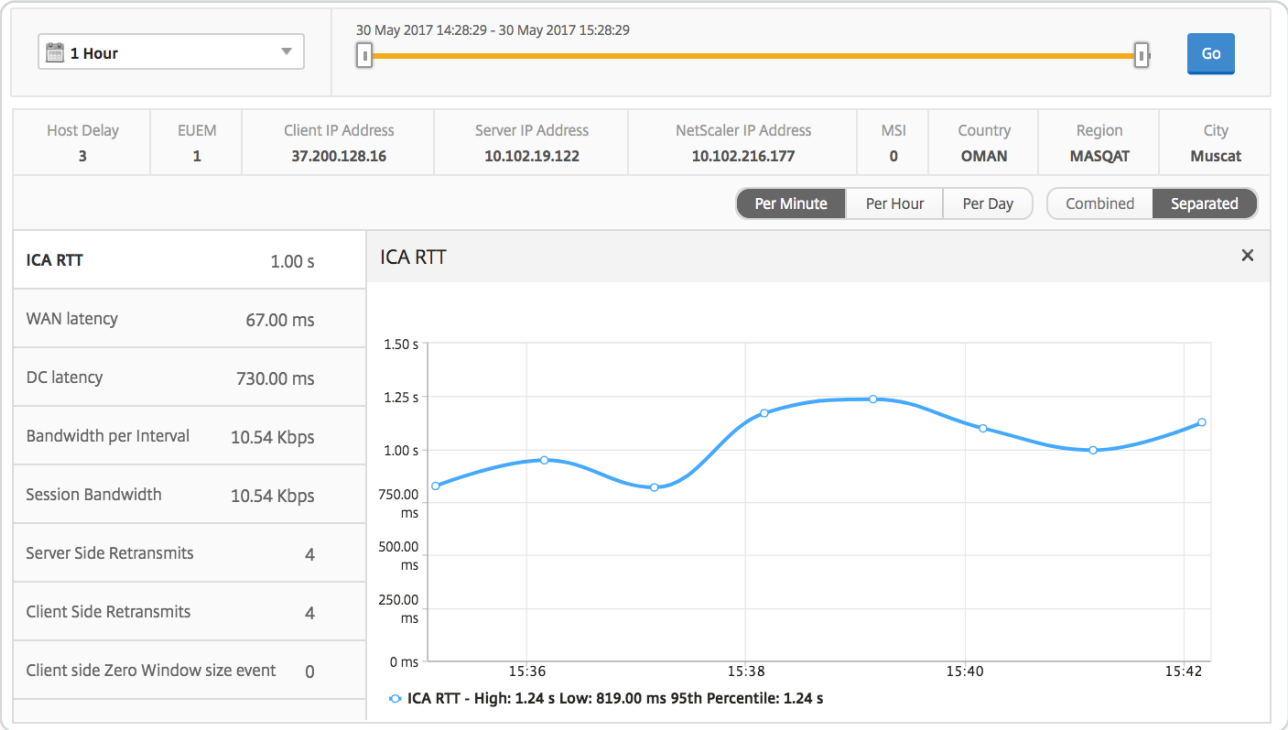
To view the metrics for a selected user's session:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App and Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



Related desktop sessions report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

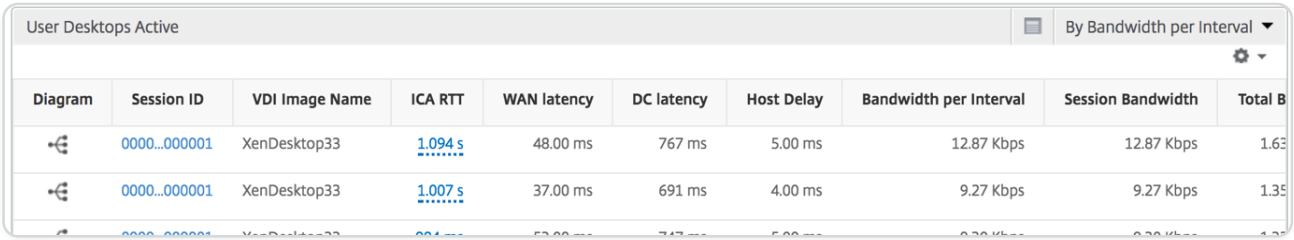
METRICS	DESCRIPTION
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Receiver type- Citrix Windows Client and so on
Client Version	Receiver version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected



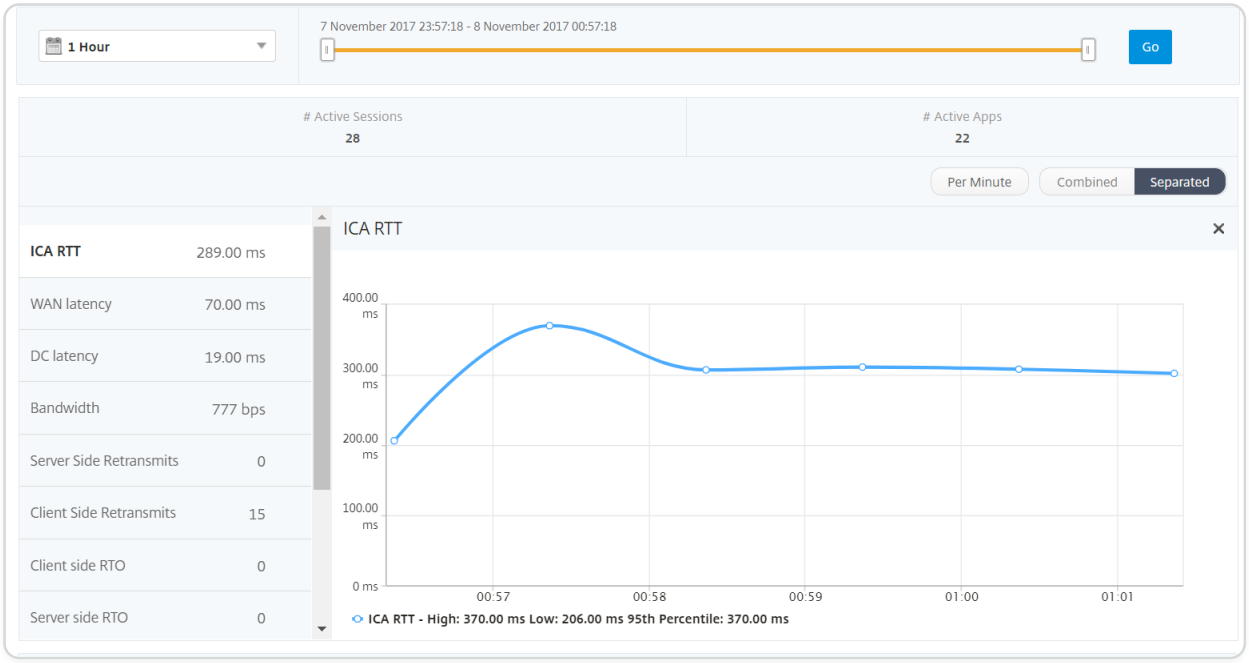
User View Reports and Metrics

The reports and metrics in this view are displayed per Citrix Virtual Apps™ and Desktop users.

To navigate to the Users view:

1. Navigate to **Gateway > HDX™ Insight > Users**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Summary view

The summary view displays the reports for all the users that have logged in during the selected timeline. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

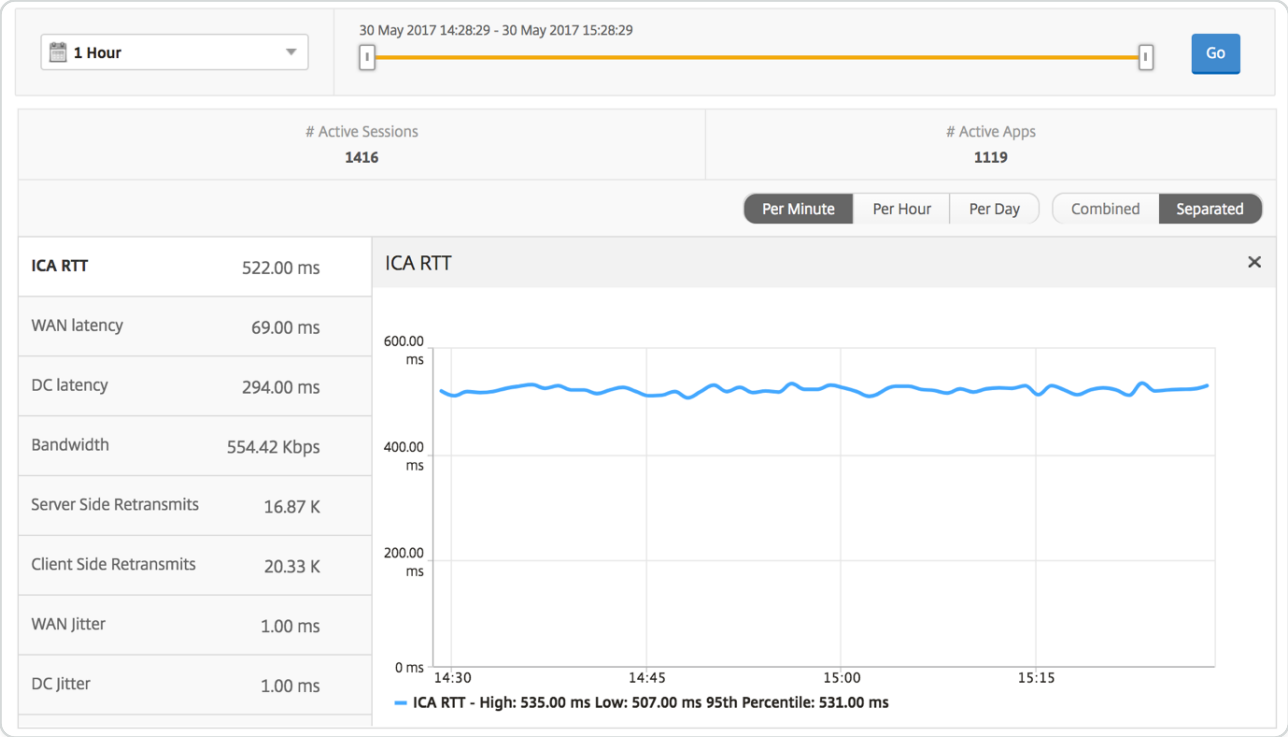
Line chart

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



User summary report

Following are the metrics that are specific to this report.

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

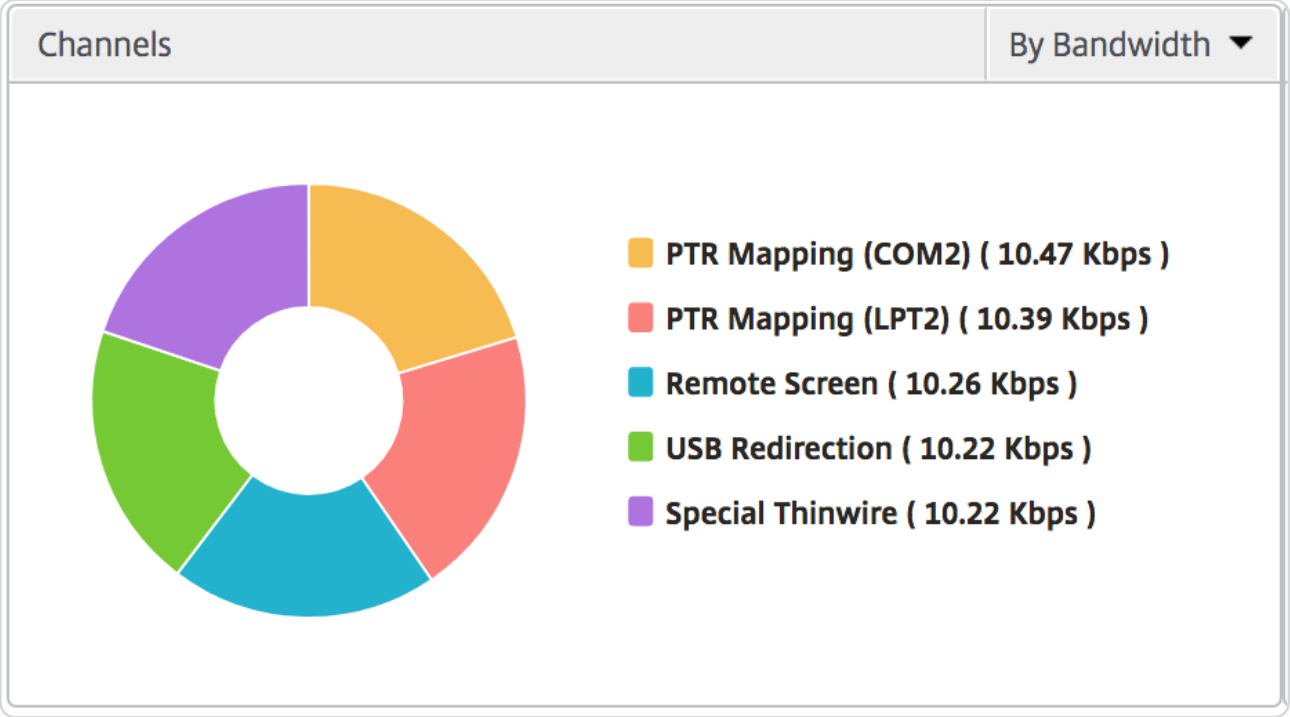
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

Channels

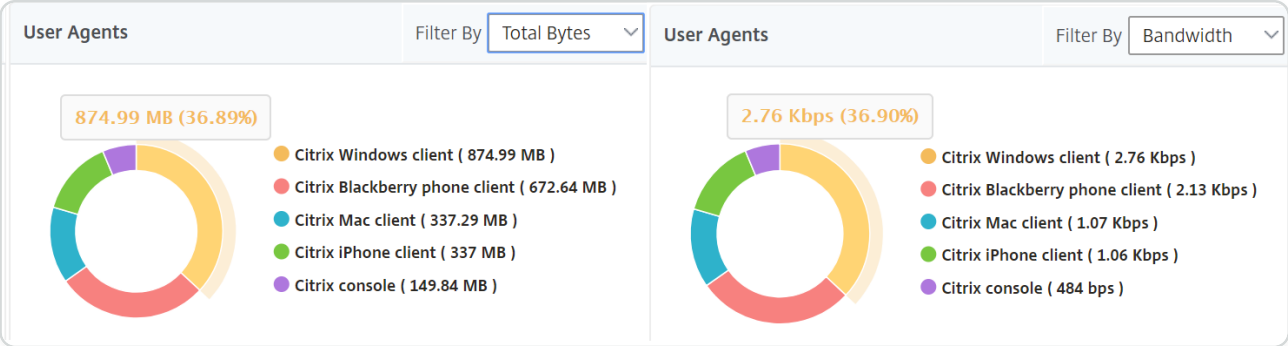
Channels represent the overall bandwidth or the total bytes consumed by each ICA® virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Thresholds breach count

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period. For more information, see how to create thresholds and alerts.

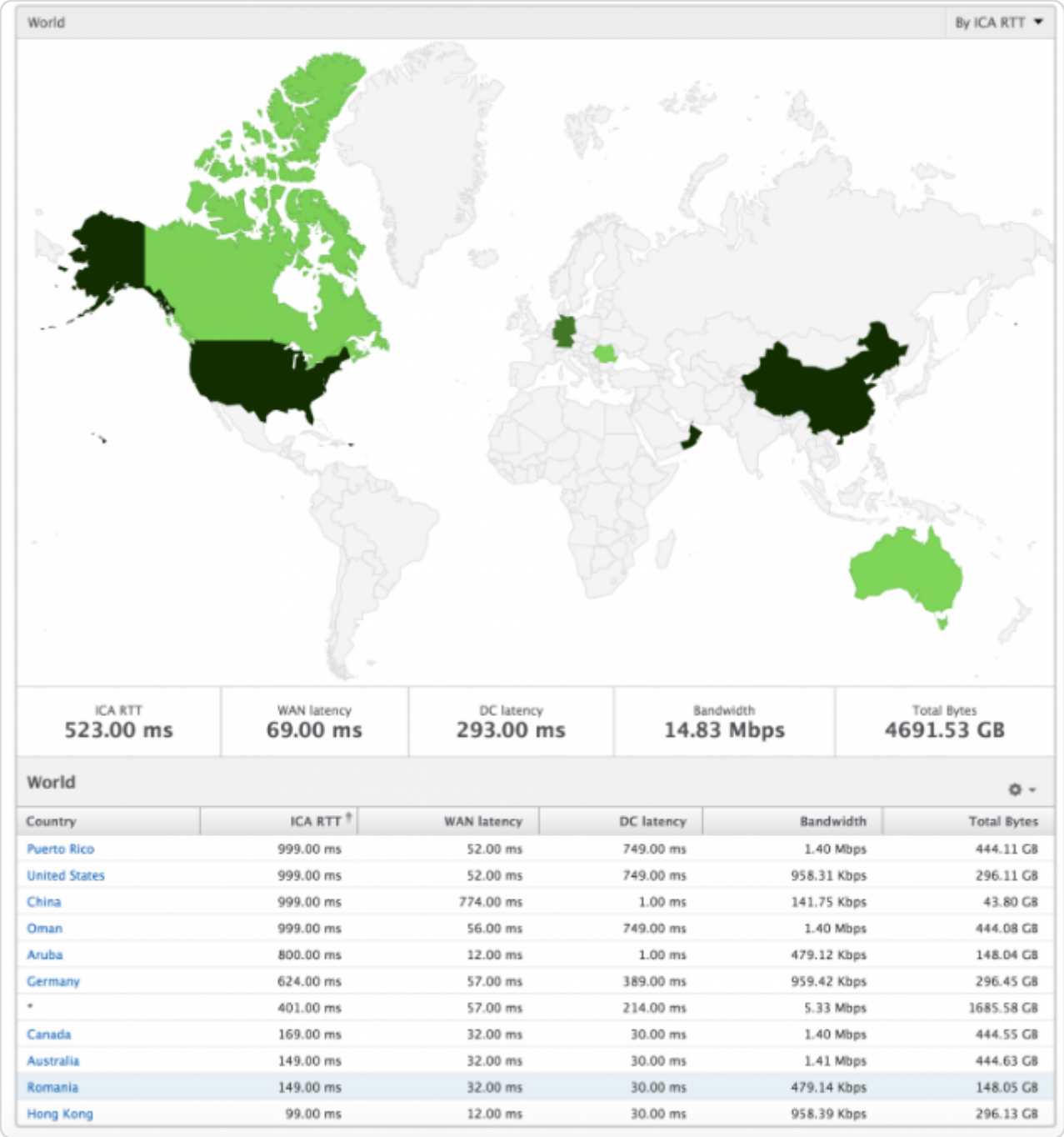
World map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per user view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the Users summary report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler ADCs caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

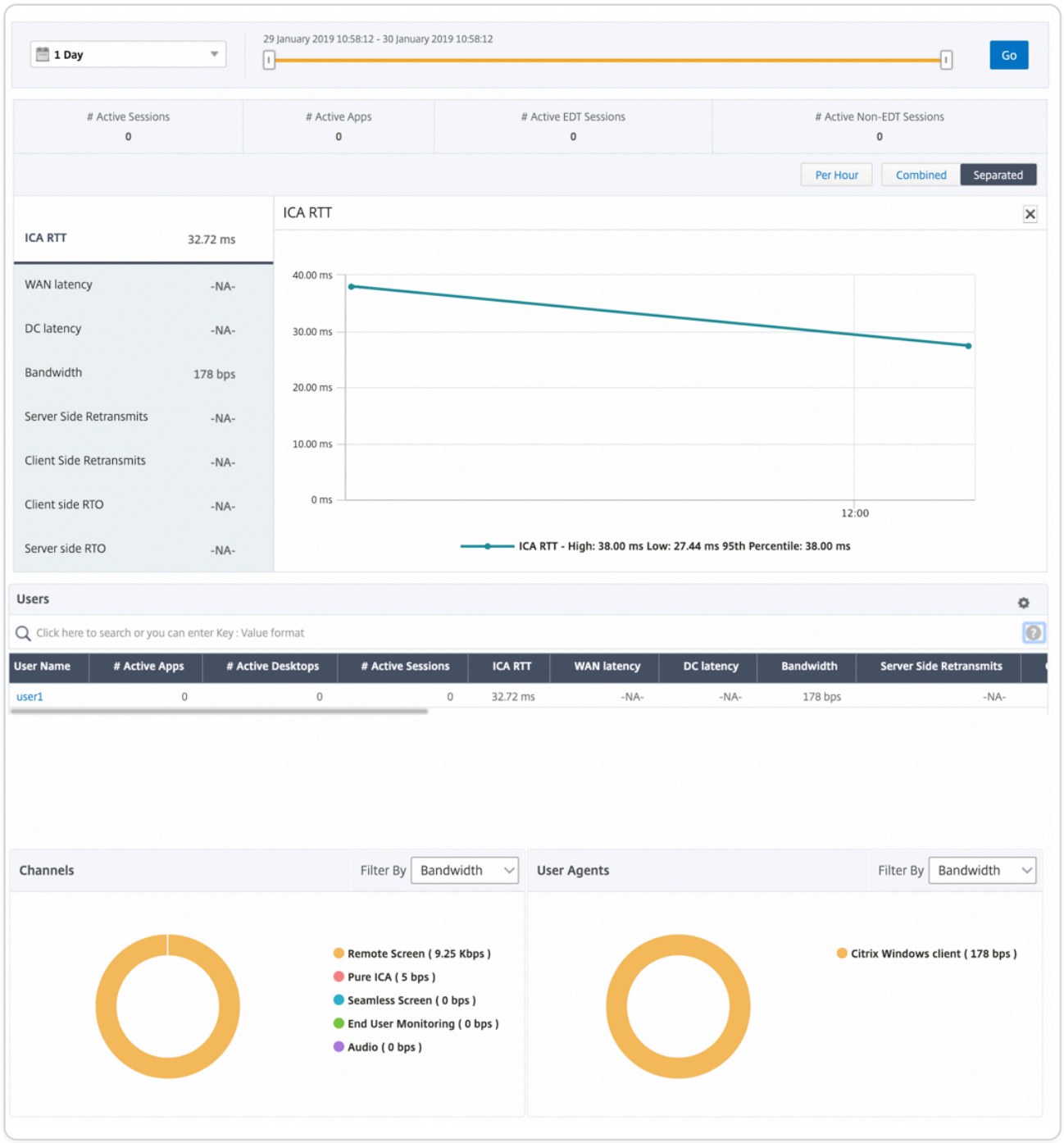
Support for EDT in HDX insight

NetScaler Application Delivery Management (ADM) now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, ADM now supports both UDP and TCP protocol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

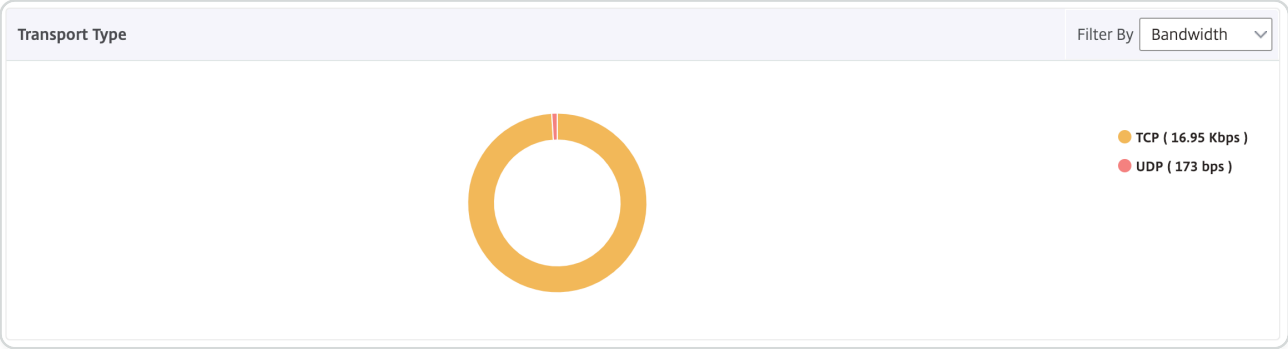
EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, and RTOs. Some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".



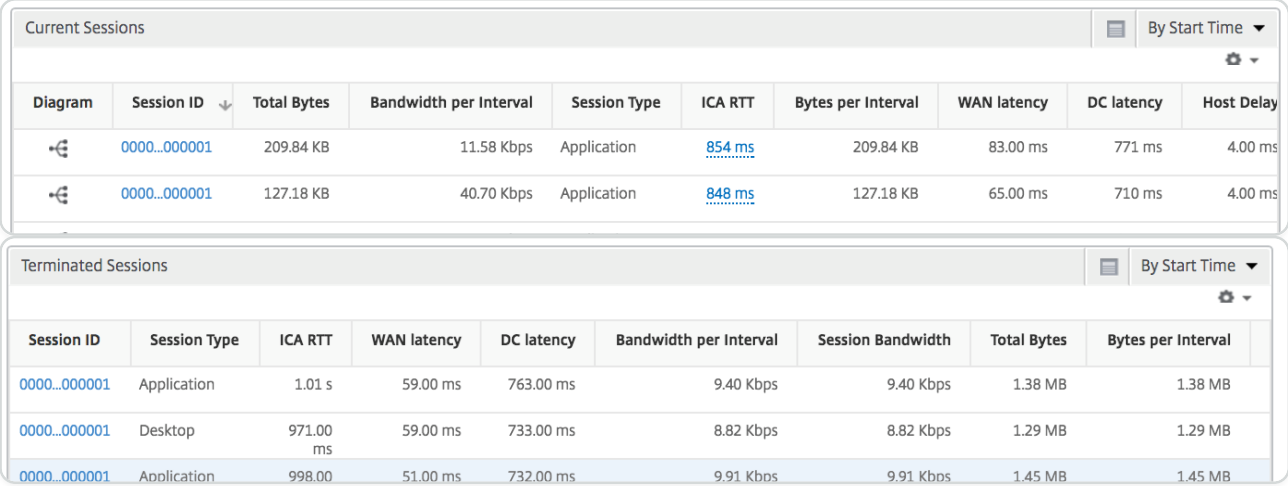
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HDX Insight metrics available from NetScaler ADM 12.0 and later:

L7 CLIENT-SIDE LATENCY	THE AVERAGE L7 LATENCY OBSERVED BETWEEN THE ICA CLIENT AND THE NETSCALER INSTANCE. THIS METRIC IS USEFUL IN CASE OF NON-CITRIX DEVICES BEING PRESENT IN THE DELIVERY PATH.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.

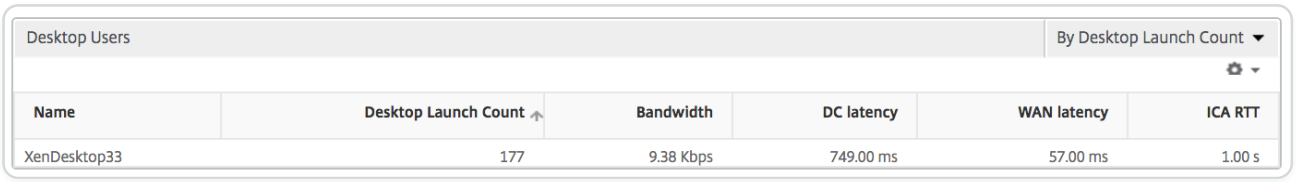


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop Users

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

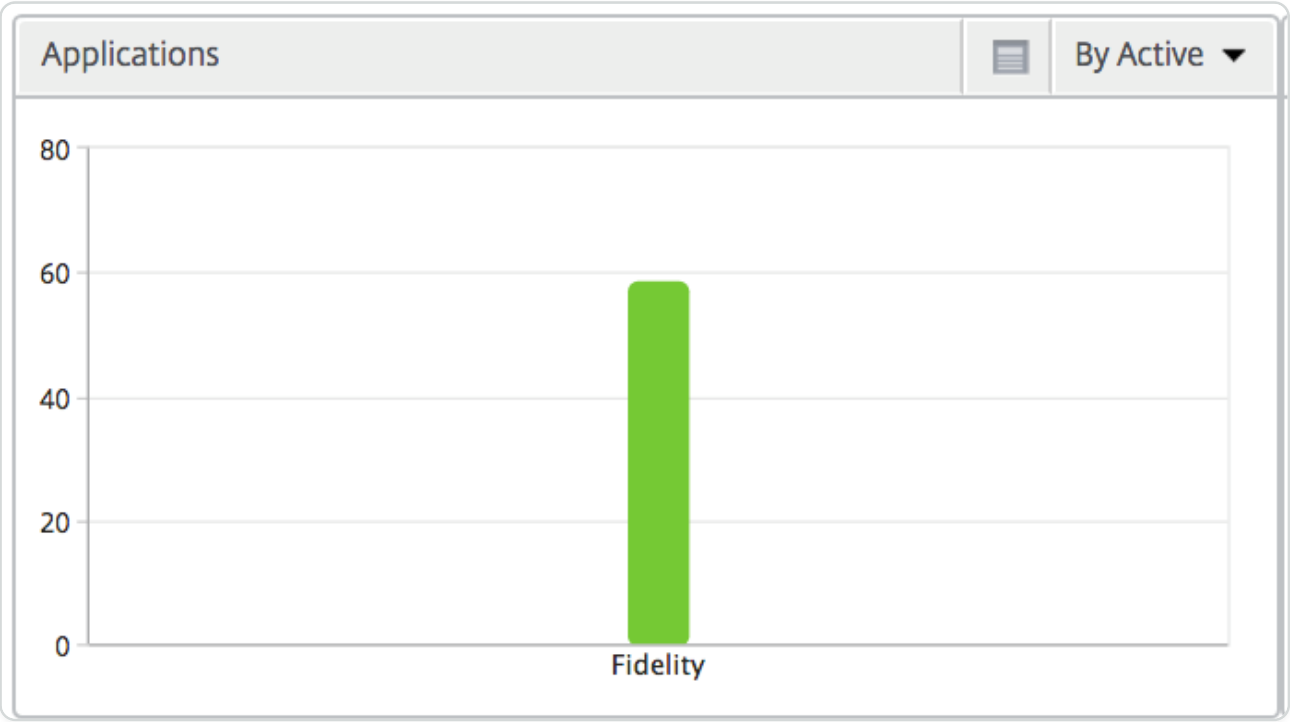
METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



Applications

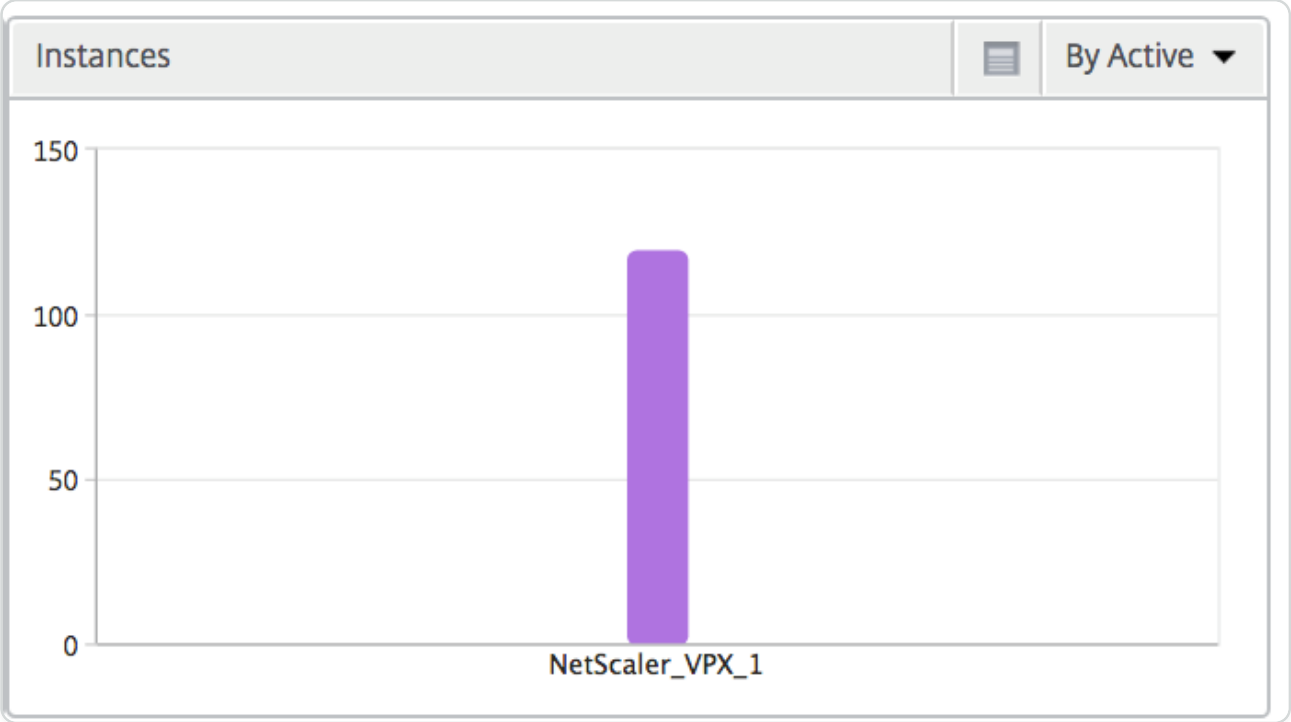
A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Instances

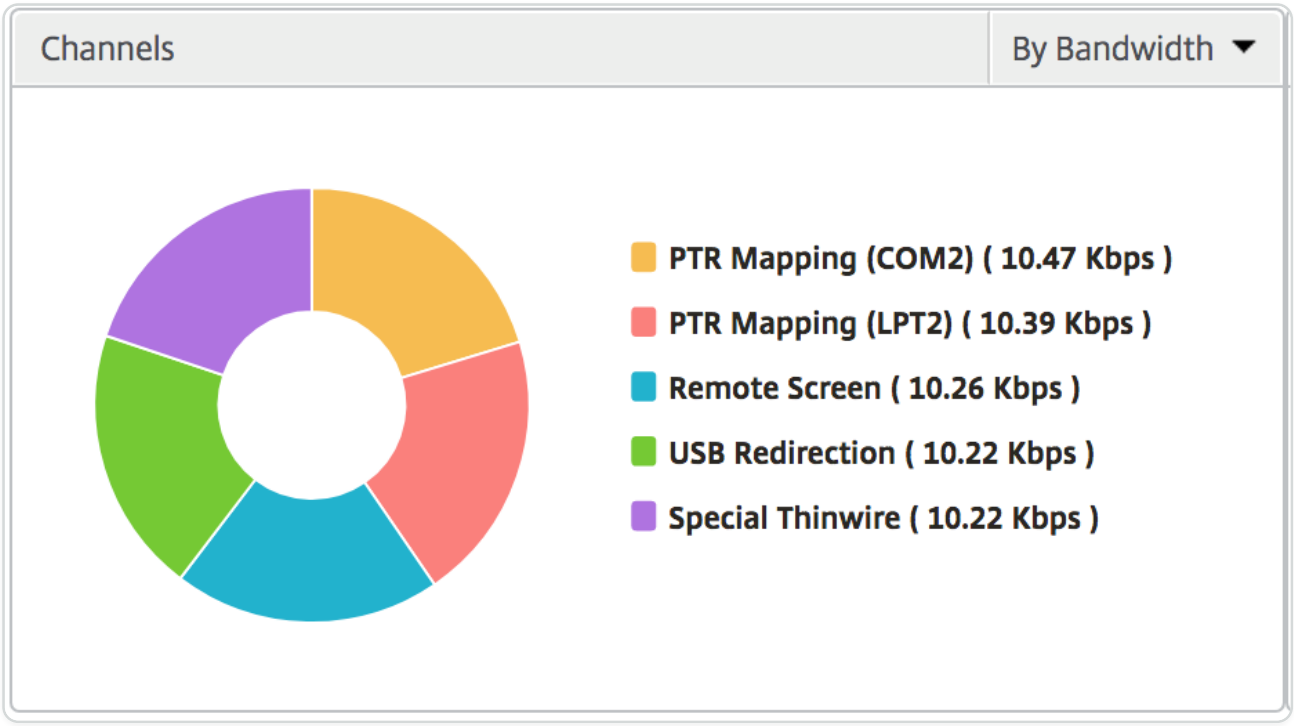
A bar graph representing NetScaler Instances sorted by Active and total apps



Channels

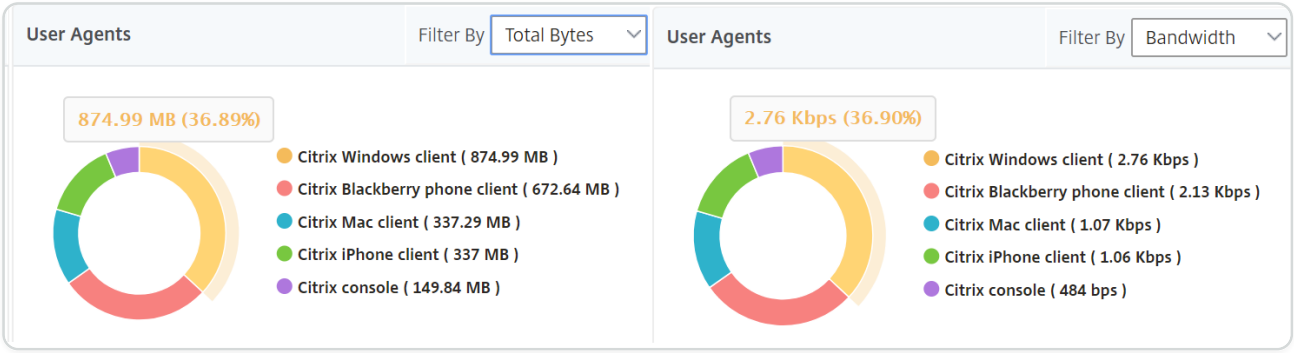
Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Per User session view

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

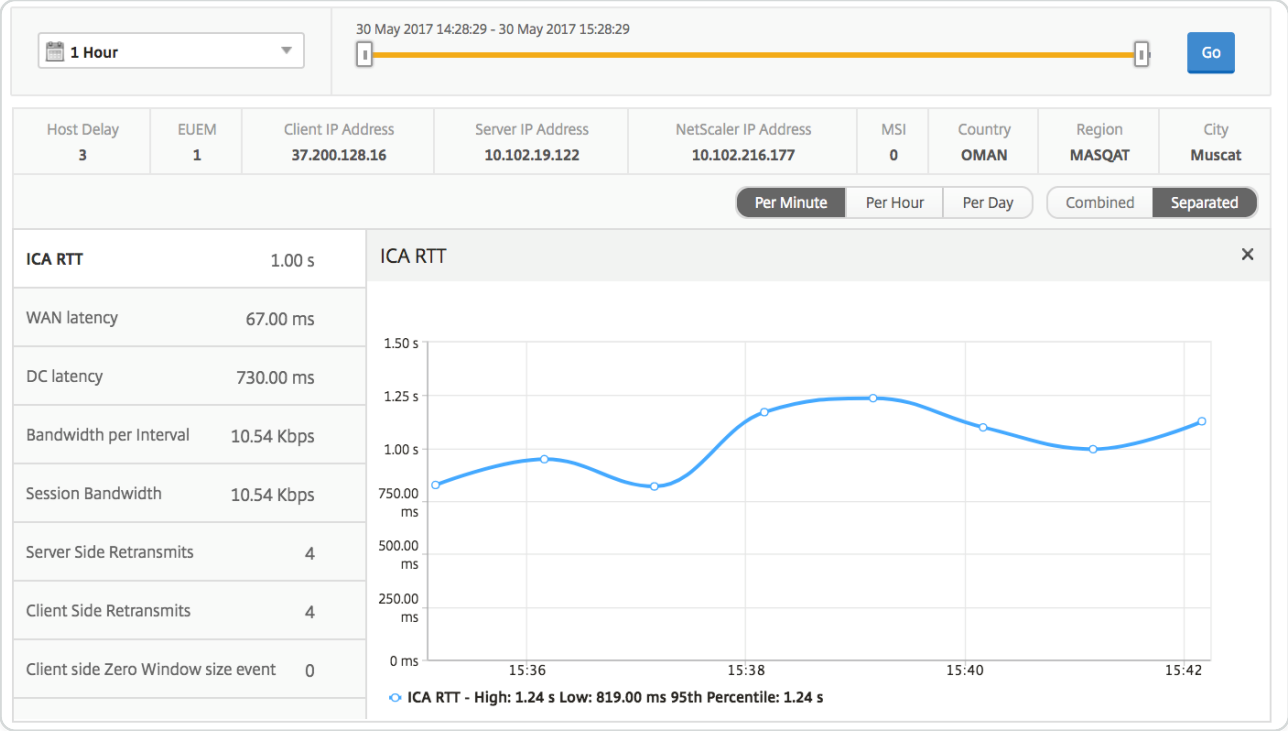
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Timeline chart

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

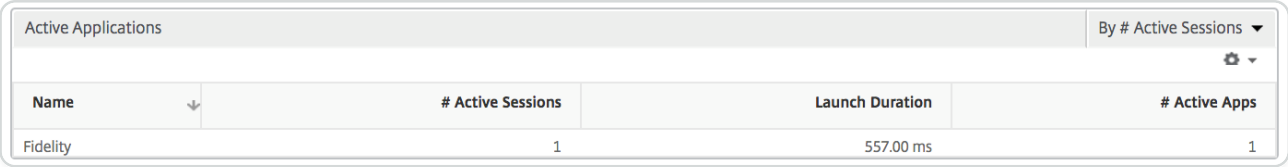
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



Active application

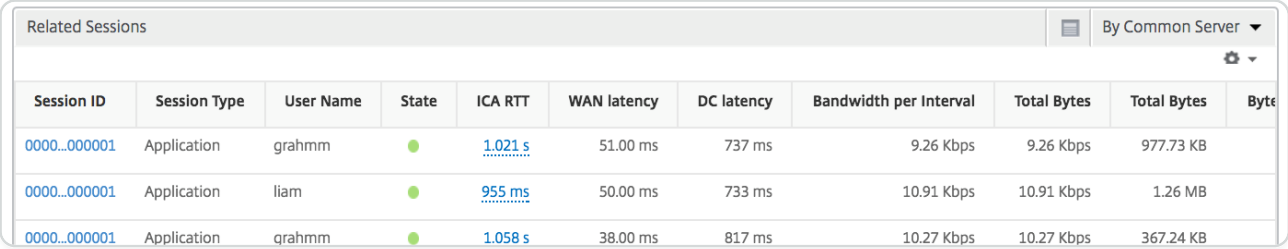
The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions

The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

Instance View Reports and Metrics

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the instance view:

1. Navigate to **Gateway > HDX™ Insight > Instances**.

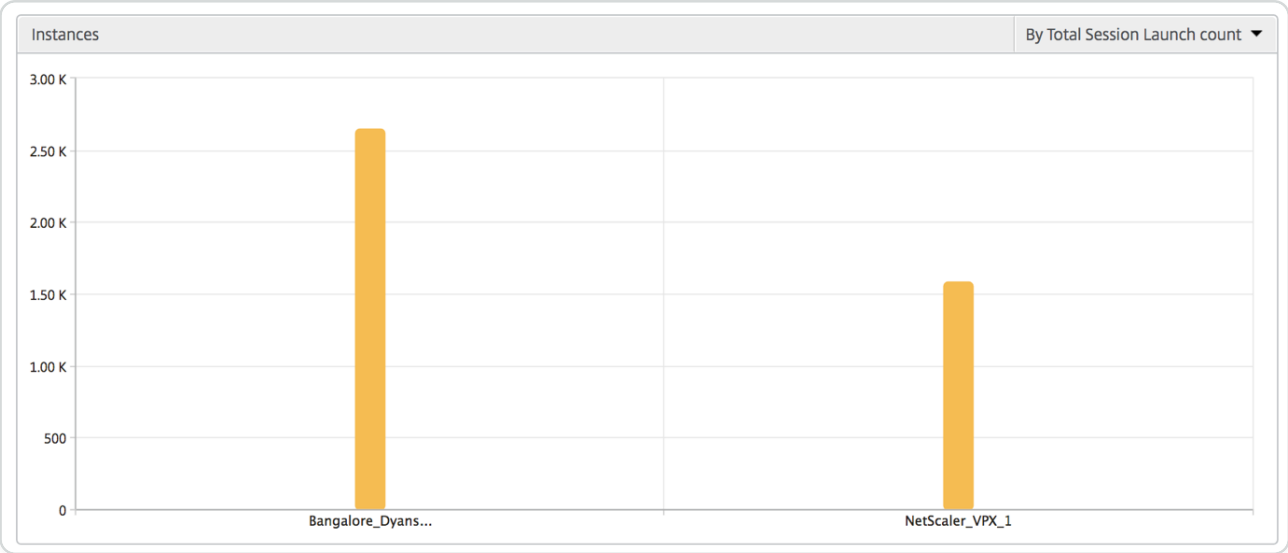
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler ADM.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

Instance bar graph

This graph displays the instance vs the Total Session Launch count and Total Apps which can be selected from the list on the top right on the graph canvas.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance/Active instances summary report

METRICS	DESCRIPTION
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A

Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Threshold report

Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds and alerts.

Skipped flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type, and so on. This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.

See **Error\! Hyperlink reference not valid** for more details on issues related to ICA parsing.

Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

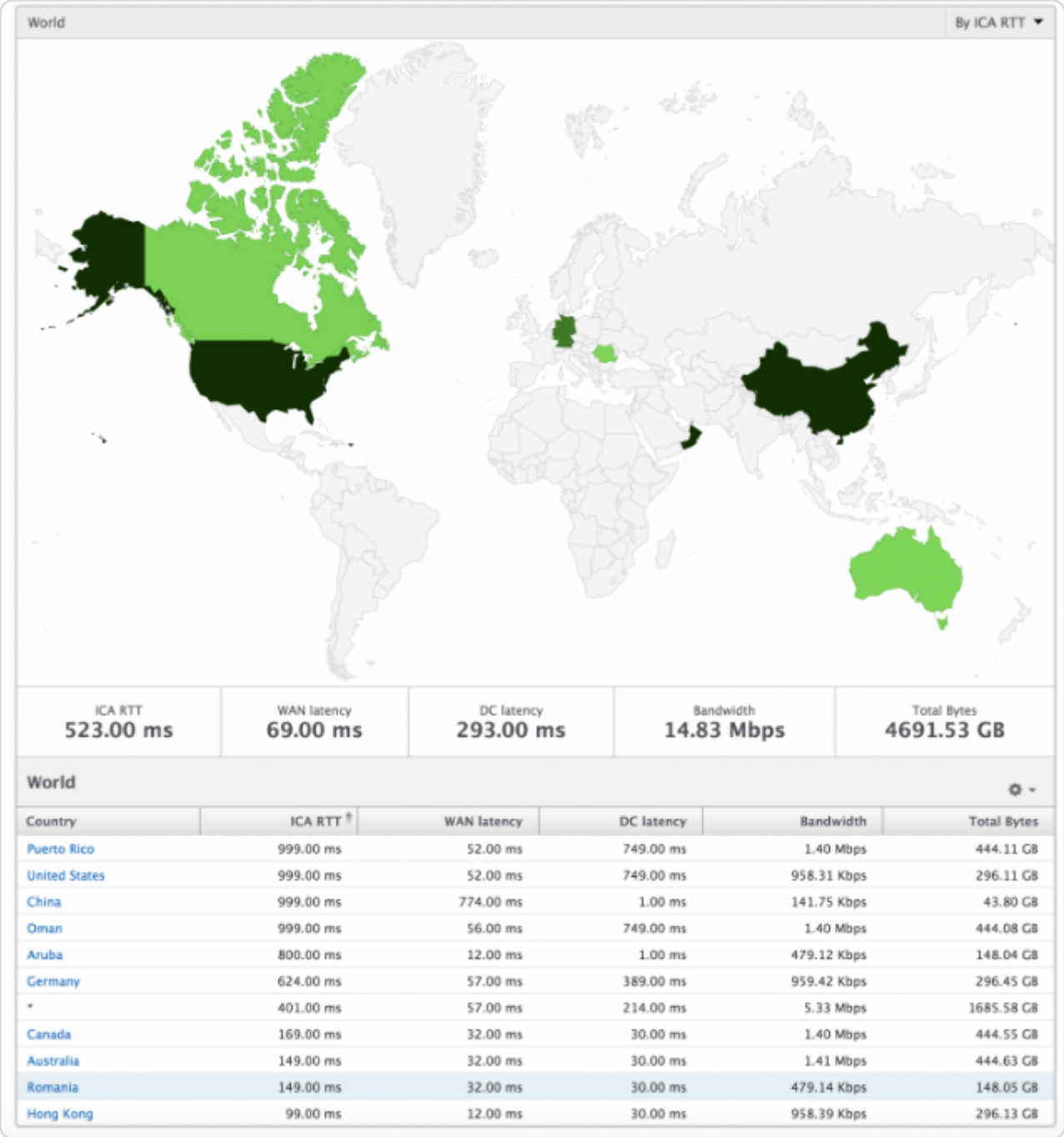
World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA® RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per instance view

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

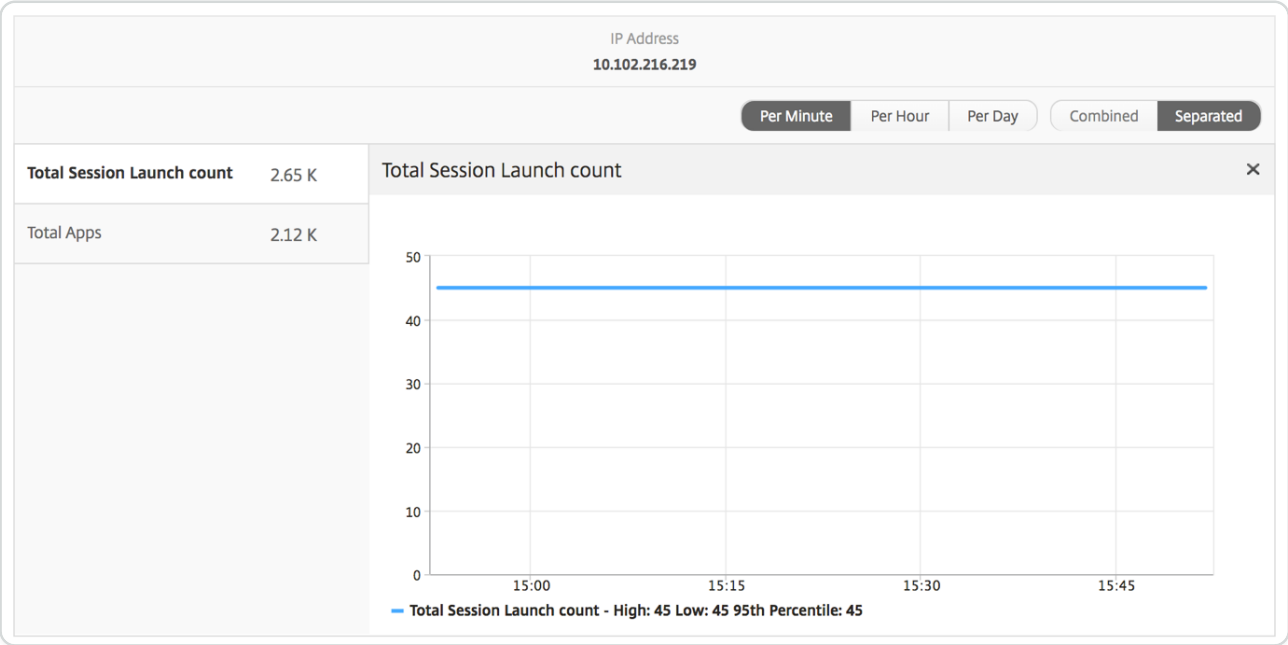
To navigate to the instance view:

1. Navigate to **Gateway > HDX Insight > Instances**.
2. Select a particular instance from the **Instance Summary Report**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

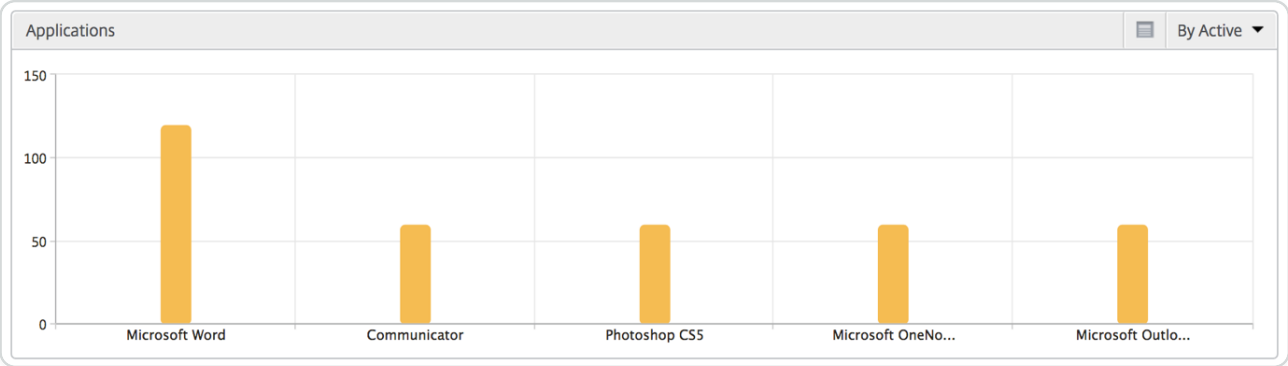
Line chart

METRICS	DESCRIPTION
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



Applications bar graph

Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.

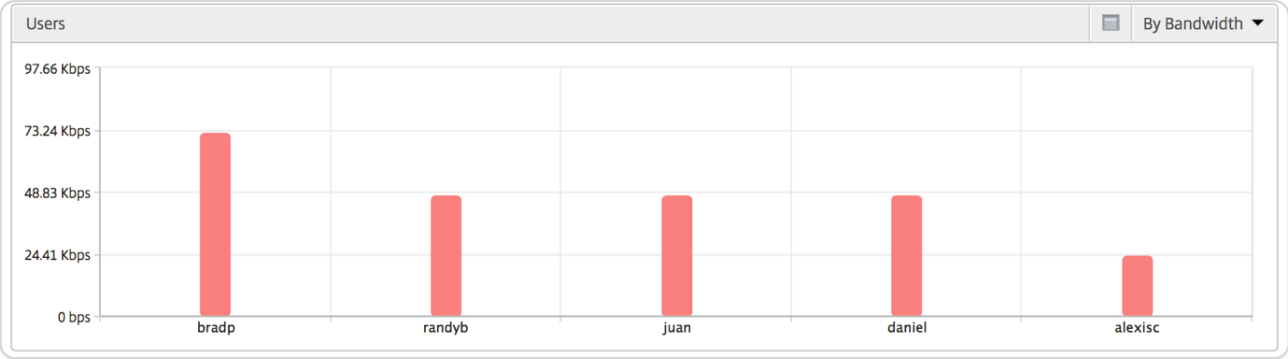


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Users bar graph

The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT



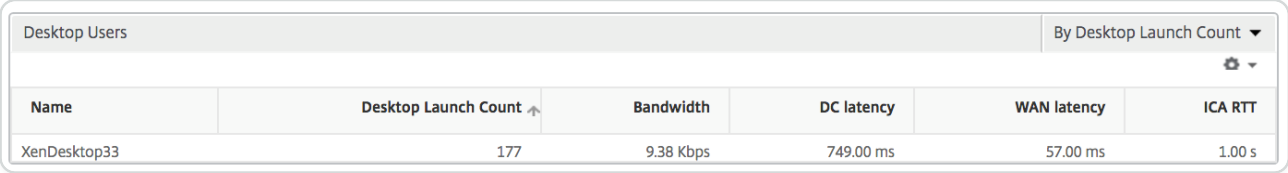
Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
	application or desktop hosted on Citrix Virtual App or Desktop respectively.



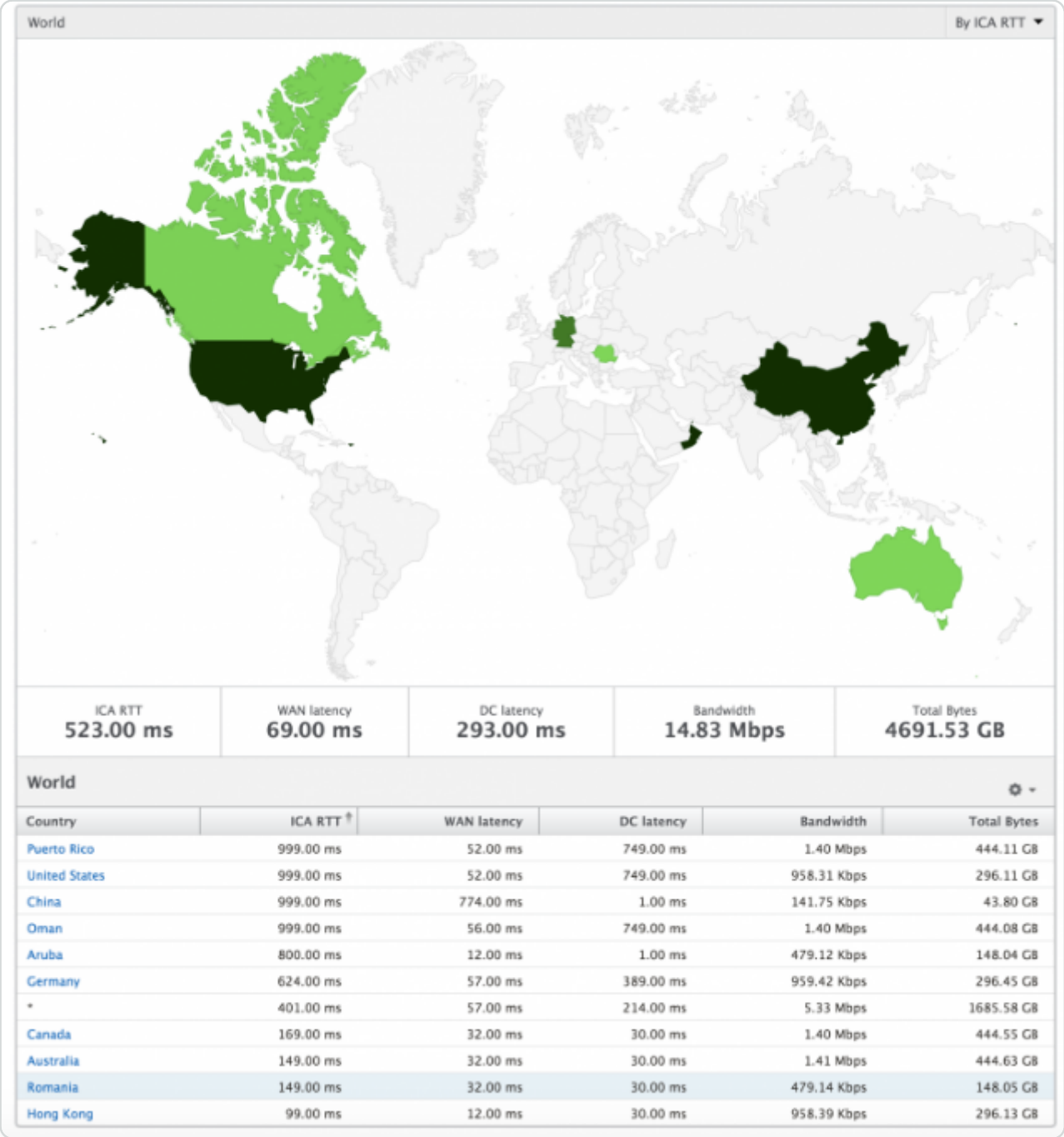
World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler ADM version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License View Reports and Metrics

The license view gives details on the NetScaler Gateway license information.

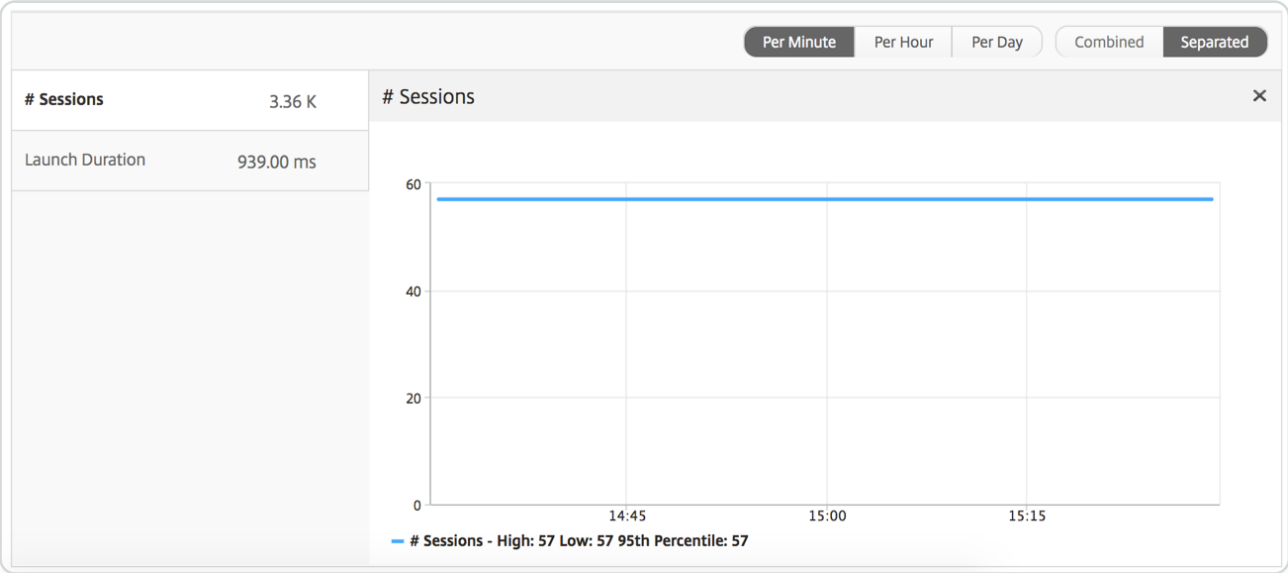
To navigate to the license view:

1. Navigate to **Gateway > HDX™ Insight > Licenses**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Line chart

METRICS	DESCRIPTION
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds and alerts.

Troubleshoot HDX™ Insight issues

If the HDX Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- HDX Insight configuration.
- Connectivity between NetScaler and NetScaler ADM.
- Record generation for HDX/ICA traffic in NetScaler.
- Population of records in NetScaler® ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX Insight configuration checklist

- Make sure that the AppFlow feature is enabled in NetScaler. For details, see Enabling AppFlow.
- Check HDX Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the HDX Insight configuration. Make sure that the bind type is ICA REQUEST. For example;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type ICA_REQUEST
  ```

  For transparent mode, the bind type must be ICA_REQ_DEFAULT. For example;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- For single-hop/Access Gateway or double-hop deployment, make sure that HDX Insight AppFlow policy is bound to the VPN virtual server, where HDX/ICA traffic is flowing.
- For Transparent mode or LAN user mode make sure the ICA® ports 1494 and 2598 are set.
- Check `appflowlog` parameter in NetScaler Gateway or VPN virtual server is enabled for Access Gateway or double-hop deployment. For details, see Enabling AppFlow for Virtual Servers.
- Check “Connection Chaining” is enabled in double-hop NetScaler. For details see, Configuring NetScaler Gateway appliances to export data.
- After HA Failover if the HDX Insight details are Skip parsed, check ICA param “enableSRonHAFailover” is enabled. For details, see Session Reliability on NetScaler High Availability Pair.

Connectivity between NetScaler and NetScaler ADM checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check HDX Insight AppFlow® policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.

- Validate any firewall blocking AppFlow ports 4739 or 5557.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Record generation for HDX/ICA traffic in NetScaler checklist

Run the command `tail -f /var/log/ns.log | grep -i "default ICA Message"` for log validation. Based on the logs that are generated, you can use this information for troubleshooting.

- Log: **Skipped parsing ICA connection - HDX Insight not supported for this host**

  Cause: Unsupported Citrix Virtual Apps and Desktops versions

  Workaround: Upgrade the Citrix Virtual Apps and Desktops servers to a supported version.

- Log: **Client type received 0x53, NOT SUPPORTED**

  Cause: Unsupported version of Citrix Workspace

  Solution: Upgrade Citrix Workspace to a supported version. For details, see Citrix Workspace app.

- Log: **Error from Expand Packet - Skipping all hdx processing for this flow**

  Cause: Issue with uncompressing ICA traffic

  Solution: No reports are available for this ICA session until a new session is established.

- Log: **Invalid transition: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Cause: Issue with parsing the ICA handshake

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Missing EUEM ICA RTT**

  Cause: Unable to parse End-User Experience Monitoring channel data

  Solution: Make sure End-User Experience Monitoring service in started on the Citrix Virtual Apps and Desktops servers. Make sure you are using the supported versions of Citrix Workspace App.

- Log: **Invalid Channel Header**

  Cause: Unable to identify channel header

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Skip code**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you see any of the following values for skip code, then the Insight details are skip parsed.

Skip code 0 indicates that the record is successfully exported from NetScaler.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
100	NS_ICA_ERR_NULL_FRAG	Error handling ICA fragments, likely due to memory conditions
101	NS_ICA_ERR_INVALID_HS_CMD	Invalid handshake command received
102	NS_ICA_ERR_REDUC_PARAM_CNT	Invalid parameter specified for V3 expander initialization
103	NS_ICA_ERR_REDUC_INIT	Unable to initialize the V3 expander correctly
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Insufficient bytes to assign a coder to a channel
105	NS_ICA_ERR_INVALID_CHANNEL	Invalid ICA channel number
106	NS_ICA_ERR_INVALID_DECODER	Invalid decoder specified for a channel
107	NS_ICA_ERR_INVALID_TW_PARAM	Invalid parameter count specified on Thinwire channel
108	NS_ICA_ERR_INVALID_TW_DECODER	Invalid decoder for Thinwire channel
109	NS_ICA_ERR_REDUC_NO_DECODER	No decoder defined for channel
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Expander error: Bytes consumed more than bytes available

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
112	NS_ICA_ERR_REDUC_BYTES_OOR	Error: Uncompressed data overrun
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefined Expander command
114	NS_ICA_ERR_CGP_FILL_HOLE	Error while handling split CGP frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB allocation error – due to low memory conditions
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Memory allocation error for expander context
117	NS_ICA_ERR_ICA_OLD_SERVER	Old server, capability blocks not supported
118	NS_ICA_ERR_PIR_MANY_FRAG	Packet Init request is fragmented, unable to process
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA capability initialization error
120	NS_ICA_ERR_NO_MSI_SUPPORT	Host does not support MSI feature. Indicates for XenApp version lower than 6.5 or XenDesktop versions lower than 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Invalid CGP command encountered
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Insufficient bytes over channel
123	NS_ICA_ERR_CHANNEL_DATA	Incorrect data on EUEM, CONTROL, or SEAMLESS channel

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
124	NS_ICA_ERR_INVALID_PURE_CMD	Invalid command received while processing pure ICA channel data
125	NS_ICA_ERR_INVALID_PURE_LEN0	Invalid length encountered while processing pure ICA channel data
126	NS_ICA_ERR_INVALID_PURE_LEN	Invalid length encountered while processing PURE ICA channel data
127	NS_ICA_ERR_INVALID_CLNT_DATA	Invalid data length received from client
128	NS_ICA_ERR_MSI_GUID_SZ	Error in MSI GUID size
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Detected invalid channel header
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Retrieval of reconnected session failed
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Error in disabling SR
132	NS_ICA_ERR_REDUC_NOT_V3	Unsupported ICA Reducer version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression disabled, not honored by host
134	NS_ICA_ERR_IDENT_PROTO	Unable to identify ICA or CGP protocol, seen with incorrect workspaces
135	NS_ICA_ERR_INVALID_SIGNATURE	Incorrect ICA signature or magic string

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
136	NS_ICA_ERR_PARSE_RAW	Error while parsing the ICA handshake packet
137	NS_ICA_ERR_INCOMPLETE_PKT	Incomplete packet received in handshake
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA frame is too large, exceeds 1460 bytes
139	NS_ICA_ERR_FORWARD	Error while forwarding the ICA data
140	NS_ICA_ERR_MAX_HOLES	Unable to process CGP command as it is split beyond supported limit
141	NS_ICA_ERR_ASSEMBLE_FRAME	Unable to reassemble ICA frame correctly
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Skipped ICA parsing for this workspace (client) as it is not in the allow list
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Unable to detect parsing state for client reconnect cookie
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Invalid reconnect cookie length detected post client reconnect
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects cookie missed the needed constraint
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Invalid workspace version string received from client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Invalid product ID received from client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Invalid channel length post expansion
149	NS_ICA_ERR_SPECIAL_THINWIRE	Decompression error
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Encountered insufficient bytes for seamless command
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Encountered insufficient bytes for EUEM command
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Invalid event for seamless channel parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Invalid event for CTRL channel parsing
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Invalid event for EUEM channel parsing
155	NS_ICA_ERR_USB_INVALID_EVENT	Invalid event for USB channel parsing
156	NS_ICA_ERR_PURE_INVALID_EVENT	Invalid event for pure channel parsing
157	NS_ICA_ERR_VCP_INVALID_EVENT	Invalid event for virtual channel parsing
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Invalid event for ICA data parsing
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Invalid event for CGP data parsing
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Invalid state for a crypt command in basic encryption
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Invalid crypt command in basic encryption

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Invalid state for a crypt command in RC5 encryption
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Invalid crypt command in RC5 encryption
164	NS_ICA_ERR_ADVCRYPT_ENC	Error in RC5 encryption/ decryption
165	NS_ICA_ERR_ADVCRYPT_DEC	Error in RC5 encryption/ decryption
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA does not support Reducer Version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace does not support Reducer Version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unexpected number of bytes in ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Higher CGP resumption sequence number from peer post reconnects
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Unable to restore ICA parsing state post reconnect
171	NS_ICA_ERR_NSAP_PARSING	Error while parsing Insight channel data
172	NS_ICA_ERR_NSAP_APP	Error while parsing app details from Insight channel data
173	NS_ICA_ERR_NSAP_ACR	Error while parsing ACR details from Insight channel data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
174	NS_ICA_ERR_NSAP_SESSION_END	Error while parsing session end details from Insight channel data
175	NS_ICA_ERR_NON_NSAP_SN	Skipped ICA parsing on service node due to the absence of Insight channel support
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP is not supported by client
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP is not supported by VDA
178	NS_ICA_ERR_NSAP_NEG_FAIL	Error while NSAP data negotiation
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Error in fetching service reconnects ticket in service node
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Error when receiving higher reconnect sequence number in service node
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Error while disabling HDX Insight for non-NSAP connections

Sample logs:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Error counters

Various counters are captured ICA parsing. The following table lists the various counters for ICA parsing. Run the command `nsconmsg –g hdx –d statswt0` for viewing the counter details.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/DIAGNOSTICS)
hdx_tot_ica_conn	Indicates total number of Pure ICA connections detected by NS. Incremented whenever an ICA connection based on the ICA signature on a client PCB is detected.	Stats
hdx_tot_cgp_conn	Indicates total number of CGP connections detected by NS (Session Reliability ON). Incremented whenever a CGP connection based on the CGP signature on a client PCB is detected.	Stats
hdx_dbg_tot_udt_conn	Indicates total number of UDP ICA connections detected by NS	Stats
hdx_dbg_tot_nsap_conn	Indicates total number of NSAP supported connections detected by NS	Stats
hdx_tot_skip_conn	Indicates how many ICA connections were skipped by	Stats

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/DIAGNOSTICS)
	parser due to invalid ICA or CGP signature.	
hdx_dbg_active_conn	Total Active EDT/CGP/ICA connections at that instant.	Stats
hdx_dbg_active_nsap_conn	Total Active EDT/CGP/ICA NSAP connections at that instant.	Stats
hdx_dbg_skip_appflow_disabled	Total number of instances where AppFlow was detached from a session because of disabling AppFlow	Stats/Diagnostics
hdx_dbg_transparent_user	Total number of transparent user access	Stats/Diagnostics
hdx_dbg_ag_user	Total number of Access Gateway user access	Stats/Diagnostics
hdx_dbg_lan_user	Total number of LAN user mode access	Stats/Diagnostics
hdx_basic_enc	Indicates the number of ICA connections using basic encryption	Stats/Diagnostics
hdx_advanced_enc	Indicates the number of ICA connections using advanced RC5 based encryption	Stats/Diagnostics
hdx_dbg_reconnected_session	Total number of reconnect requests from client without any NetScaler error	Stats/Diagnostics
hdx_dbg_host_rejected_ns_reconnect	Total number of hosts rejected reconnects requests by client	Stats/Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/DIAGNOSTICS)
hdx_euem_available	Indicates the number of connections having the End User Experience Monitoring channel available. End User Experience Monitoring channel is required to collect statistics such as ICA RTT.	Stats/Diagnostics
hdx_err_disabled_sr	Session Reliability is disabled using `nsapimgr` knob. Session does not work for this session.	Error
hdx_err_skip_no_msi	XA/XD server is Missing MSI capability. This indicates an older server version and HDX Insight skips this connection.	Error
hdx_err_skip_old_server	Old unsupported server version	Error
hdx_err_clnt_not_whitelist	Client workspace not in allow list, HDX Insight skips this connection	Error
hdx_sm_ica_cam_channel_disabled	Total number of NS_ICA_CAM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_usb_channel_disabled	Total number of NS_ICA_USB_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_clip_channel_disabled	Total number of NS_ICA_CLIP_CHANNEL disabled via SmartAccess policy	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/DIAGNOSTICS)
hdx_sm_ica_ccm_channel_disabled	Total number of NS_ICA_CCM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cdm_channel_disabled	Total number of NS_ICA_CDM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com1_channel_disabled	Total number of NS_ICA_COM1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com2_channel_disabled	Total number of NS_ICA_COM2_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cpm_channel_disabled	Total number of NS_ICA_CPM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_lpt1_channel_disabled	Total number of NS_ICA_LPT1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_lpt2_channel_disabled	Total number of NS_ICA_LPT2_CHANNEL disabled via SmartAccess policy	Diagnostics
dx_dbg_sm_ica_msi_disabled	Total number of cases where MSI is disabled via SmartAccess policy	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/DIAGNOSTICS)
hdx_sm_ica_file_channel_disabled	Total number of NS_ICA_FILE_CHANNEL is disabled via SmartAccess policy	Diagnostics
hdx_dbg_usb_accept_device	Total number of USB devices accepted	Diagnostics
hdx_dbg_usb_reject_device	Total number of USB devices rejected	Diagnostics
hdx_dbg_usb_reset_endpoint	Total number of USB endpoints reset	Diagnostics
hdx_dbg_usb_reset_device	Total number of USB devices reset	Diagnostics
hdx_dbg_usb_stop_device	Total number of USB devices stopped	Diagnostics
hdx_dbg_usb_stop_device_response	Total number of responses from stopped USB devices	Diagnostics
hdx_dbg_usb_device_gone	Total number of USB devices gone	Diagnostics
hdx_dbg_usb_device_stopped	Total number of USB devices stopped	Diagnostics

nstrace validation

Check for CFLOW protocol to see all AppFlow records going out of NetScaler.

Population of records in NetScaler ADM checklist

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` and check logs to confirm NetScaler ADM is receiving AppFlow records.
- Confirm NetScaler instance is added to NetScaler ADM.
- Validate NetScaler Gateway/VPN virtual server is licensed in NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Make sure multi-hop parameter setting is enabled for double-hop.
- Make sure NetScaler Gateway is cleared for second-hop in double-hop deployment.

Before contacting Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler ADM versions.
- Citrix Virtual Apps and Desktops server versions.
- Client Workspace versions.
- Number of Active ICA sessions when the issue occurred.
- Tech support bundle captured by running the `show techsupport` command at the NetScaler command prompt.
- Tech support bundle captured for NetScaler ADM.
- Packet traces captured on all NetScaler. To start a packet trace, type, `start nstrace -size 0'` To stop a packet trace, type, `stop nstrace`
- Collect entries in the system's ARP table by running the `show arp` command.

Known Issues

Refer ADC release notes for known issues on HDX Insight.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

NetScaler ADM provides infrastructure management and analytics capabilities to discover, monitor, and manage your NetScaler instances. The following topics help you manage your NetScaler infrastructure:

- Infrastructure Analytics
- Instance management
- SSL certificate management
- Events
- Network functions
- Network reporting
- Configuration
- Upgrade jobs
- Orchestration
- Video Insight

Infrastructure Analytics

A key goal for network administrators is to monitor NetScaler instances. ADC instances offer interesting insights into usage and performance of applications and desktops accessed through it. Administrators must monitor the ADC instance and analyze the application flows processed by each ADC instance. They can be able to remediate any probable issues in configuration, setup, connectivity, certificates, and others which might impact application usage or performance. For example, a sudden change in the application traffic pattern can be due to change in SSL configuration like disabling of an SSL protocol. Administrators must be able to quickly identify the correlation between these data points to ensure the following:

- Application availability is in an optimal state
- There are no resource consumption, hardware, capacity, or configuration change issues
- There are no unused inventories
- There are no expired certificates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure Analytics feature simplifies the process of data analysis by correlating multiple data sources and quantifying it to a measurable score that defines the health of an instance. With this feature, the administrators get a single touch point to understand if there is a problem, the origin of the problem, and probable remediations that they can perform.

Infrastructure analytics

The NetScaler Application Delivery Management (ADM) Infrastructure analytics feature collates all the data gathered from the NetScaler instances and quantifies it into an **Instance Score** that defines the health of the instances. The instance score is summarized over a tabular view or as circle pack visualization. The Infrastructure Analytics feature helps you to visualize the factors that resulted or might result in an issue on the instances. This visualization also helps you to determine the actions that must be performed to prevent the issue and its recurrence.

Instance score

Instance score indicates the health of an ADC instance. A score of 100 means a perfectly healthy instance without any issues. Instance score captures different levels of potential issues on the instance. It is a quantifiable measurement of instance health and multiple "health indicators" contribute to the score.

Health indicators are the building blocks of the instance score, where the score is computed periodically for a predefined "monitoring period," based on all detected indicators in that time window. Currently, Infrastructure analytics calculates the instance score once every hour based on the data collected from the instances. An indicator can be defined as any activity (an event or an issue) that belongs to one of the following categories on the instances.

- System resource indicators
- Critical events indicators
- SSL configuration indicators
- Configuration deviation indicators

Health indicators

- System resources indicators

  The following are the critical system resource issues that might occur on NetScaler instances and monitored by NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **High CPU usage**. The CPU usage has crossed the higher threshold value in the NetScaler instance.
- **High memory usage**. The memory usage has crossed the higher threshold value in the NetScaler instance.
- **High disk usage**. The disk usage has crossed the higher threshold value in the NetScaler instance.
- **Disk errors**. There are errors on hard disk 0 or hard disk 1 on the hypervisor where the ADC instance is installed.
- **Power failure**. The power supply has failed or disconnected from the ADC instance.
- **SSL card failure**. The SSL card installed on the instance has failed.
- **Flash errors**. There are Compact Flash Errors seen on the NetScaler instance.
- **NIC discards**. The packets discarded by the NIC card have crossed the higher threshold value in the NetScaler instance.

For more information on these system resources errors, see The instance dashboard.

- Critical events indicators

  The following critical events are identified by the events under event management feature of ADM that are configured with critical severity.

  - **HA sync failure**. Configuration sync between the ADC instances in high availability has failed on the secondary server.
  - **HA no heartbeats**. The primary server in a pair of ADC instances in high availability is not receiving heart beats form the secondary server.
  - **HA bad secondary state**. The secondary server in a pair of ADC instances in high availability is in Down, Unknown, or Stay secondary state.
  - **HA version mismatch**. The version of the ADC software images installed on a pair of ADC instances in high availability does not match.
  - **Cluster sync failure**. Configuration sync between the ADC instances in cluster mode has failed.
  - **Cluster version mismatch**. The version of the ADC software images installed on the ADC instances in cluster mode does not match.
  - **Cluster propagation failure**. Propagation of configurations to all instances in a cluster has failed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE**
>
> You can have your list of critical SNMP events by changing the severity levels of the events. For more information on how to change the severity levels, see Modify the reported severity of events that occur on NetScaler instances.

For more information on events in NetScaler ADM, see Events.

- SSL configuration indicators
  - **Not recommended key strength**. The key strength of the SSL certificates is not as per NetScaler® standards
  - **Not recommended issuer**. The issuer of the SSL certificate is not recommended by Citrix.
  - **SSL certs expired**. The SSL certificate installed in the ADC instance has expired.
  - **SSL certs expiry due**. The SSL certificate installed in the ADC instance is about to expire in the next one week.
  - **Not recommended algorithms**. The signature algorithms of SSL certificates installed in the ADC instance are not as per NetScaler standards.

For more information on SSL certificates, see SSL dashboard.

- Configuration deviation indicators
  - **Config drift template**. There is a drift (unsaved changes) in configuration from the audit templates that you have created with specific configurations you want to audit on certain instances.
  - **Config drift default**. There is a drift (unsaved changes) in configuration from the default configuration files.

For more information on configuration deviations and how to run audit reports to check configuration deviation, see View audit reports.

View ADC Capacity issues

When an ADC instance has consumed most its available capacity, packet-drop may occur while processing the client traffic. This issue causes low performance in an ADC instance. By understanding such ADC capacity issues, you can allocate additional licenses proactively to steady the ADC performance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view ADC capacity issues,

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Expand the instance for which you want to view capacity issues.

The ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters:

- **Throughput Limit Reached** – The number of packets dropped in the instance after the throughput limit is reached.
- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** – The number of packets dropped in the instance after PPS limit is reached.
- **SSL Throughput Rate Limit** – The number of times the SSL throughput limit reached.
- **SSL TPS Rate Limit** – The number of times the SSL TPS limit reached.

The ADM calculates the instance score on the defined capacity threshold.

- Low threshold – 1 packet drop or rate-limit counter increment
- High threshold – 10000 packets drop or rate-limit counter increment

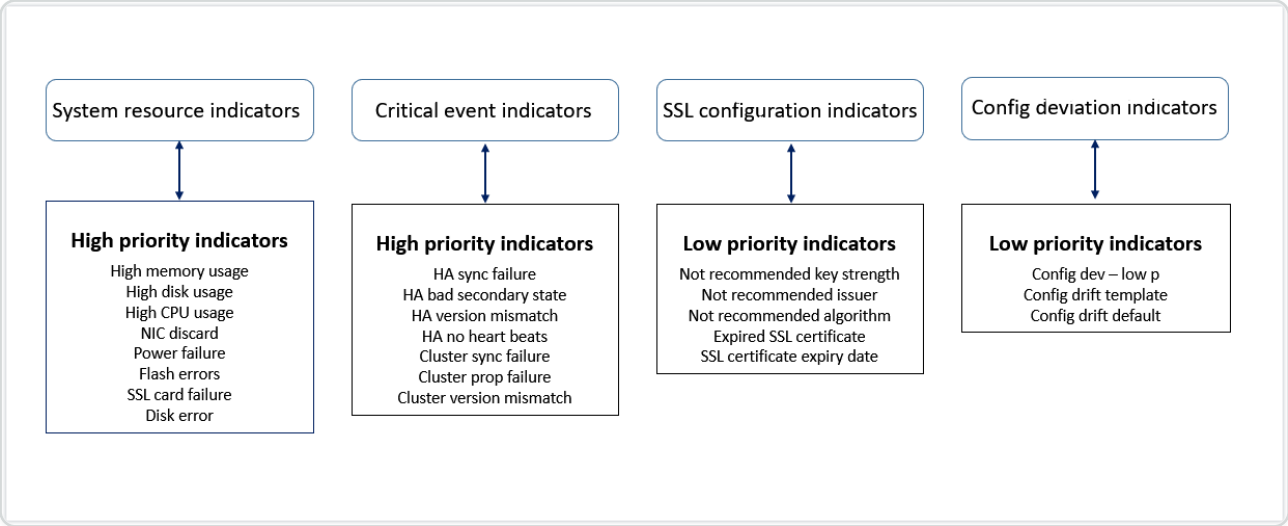
Therefore, when an ADC instance breaches the capacity threshold the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the `ADCCapacityBreach` category. To view these events, navigate to **Accounts > System Events**.

Value of health indicators

The indicators are classified into high priority indicators and low-priority indicators based on their values as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The health indicators within the same group of indicators have different weights assigned to them. One indicator might contribute more to lowered instance score than another indicator. For example, high memory usage brings down the instance score more than high disk usage, high CPU usage, and NIC discard. If an instance has a greater number of indicators detected on it, the lesser is the instance score.

The value of an indicator is calculated based on the following rules. The indicator is said to be detected in one of the following three ways:

1. **Based on an activity**. For example, a System resource indicator is triggered whenever there is a power failure on the instance, and this indicator reduces the value of the instance score. When the indicator is cleared the penalty is cleared, and the instance score increases.
2. **Based on the threshold value breach**. For example, a System resource indicator is triggered when the NIC card discards packets and the threshold level is breached.
3. **Based on the low and high threshold value breach**. Here, an indicator can be triggered in two ways:
   - When the value of the indicator is between low and high thresholds, in which case a partial penalty is levied on the instance score.
   - When the value crosses the high threshold, in which case a full penalty is levied on the instance score.
   - No penalty is levied on the instance score if the value falls below a low threshold.

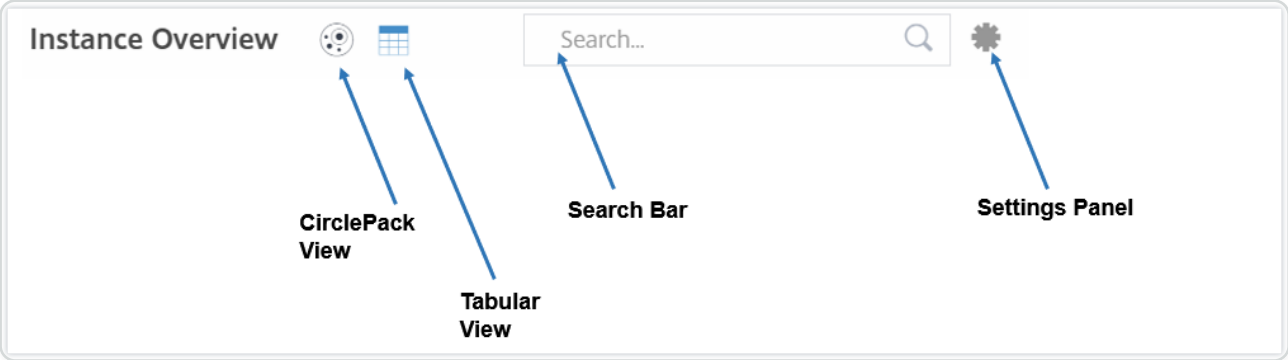
For example, CPU usage is a system resource indicator triggered when the usage value crosses the low threshold and also when the value crosses the high threshold.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure analytics dashboard

Navigate to **Infrastructure > Infrastructure Analytics**.

The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.

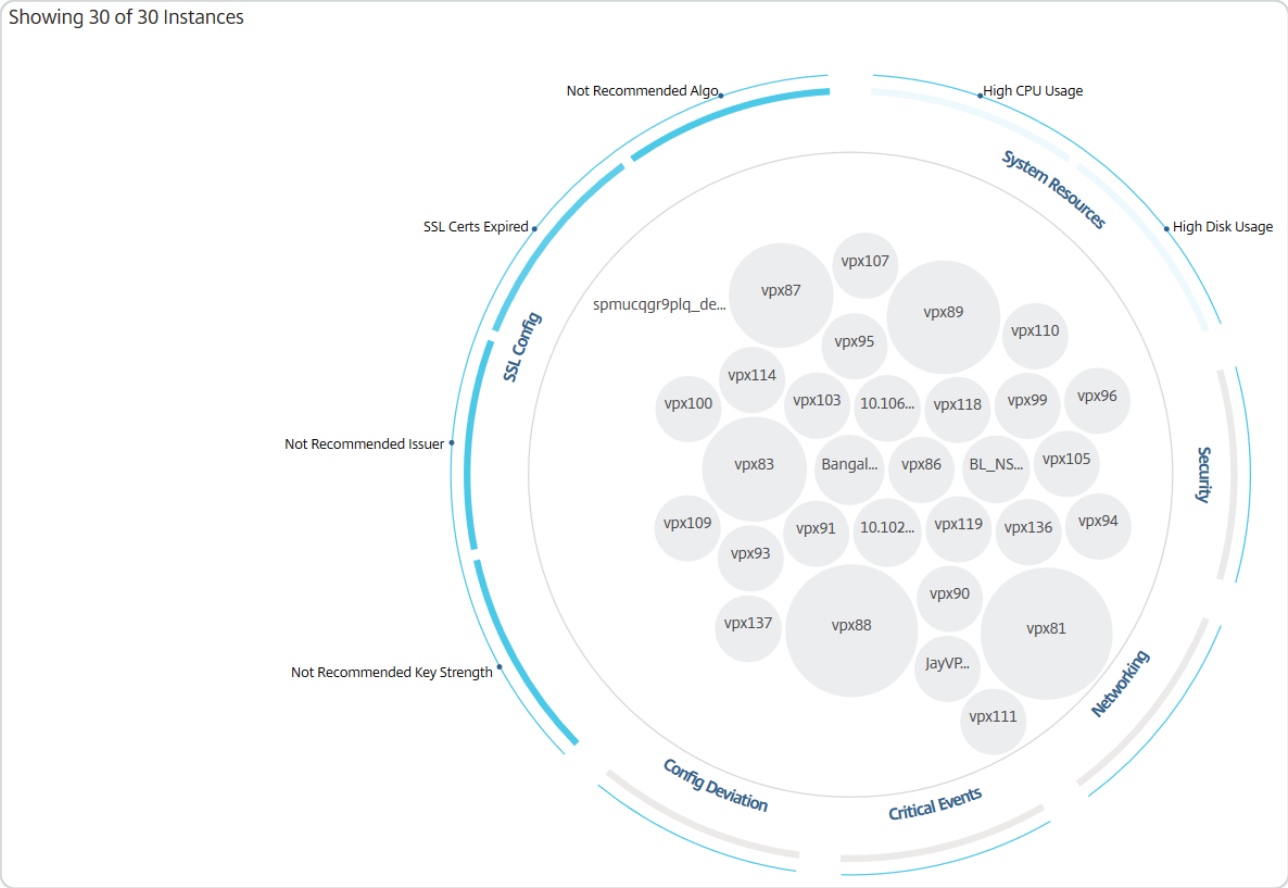


- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view formats, the Summary Panel displays details of all the instances in your network.

Circle pack view

Circle packing diagrams show instance groups as tightly organized circles. They often show hierarchies where smaller instance groups are either colored similarly to others in the same category, or nested within larger groups. Circle packs represent hierarchical data sets and shows different levels in the hierarchy and how they interact with each other.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

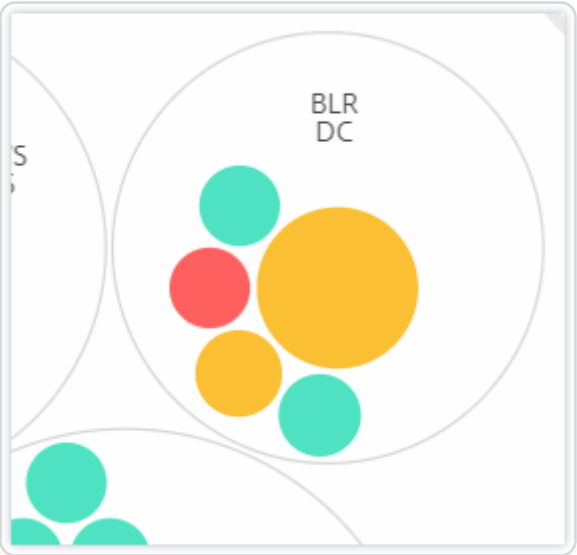


Instance circles

Color. Each instance is represented in Circle Pack as a colored circle. The color of the circle indicates the health of that instance.

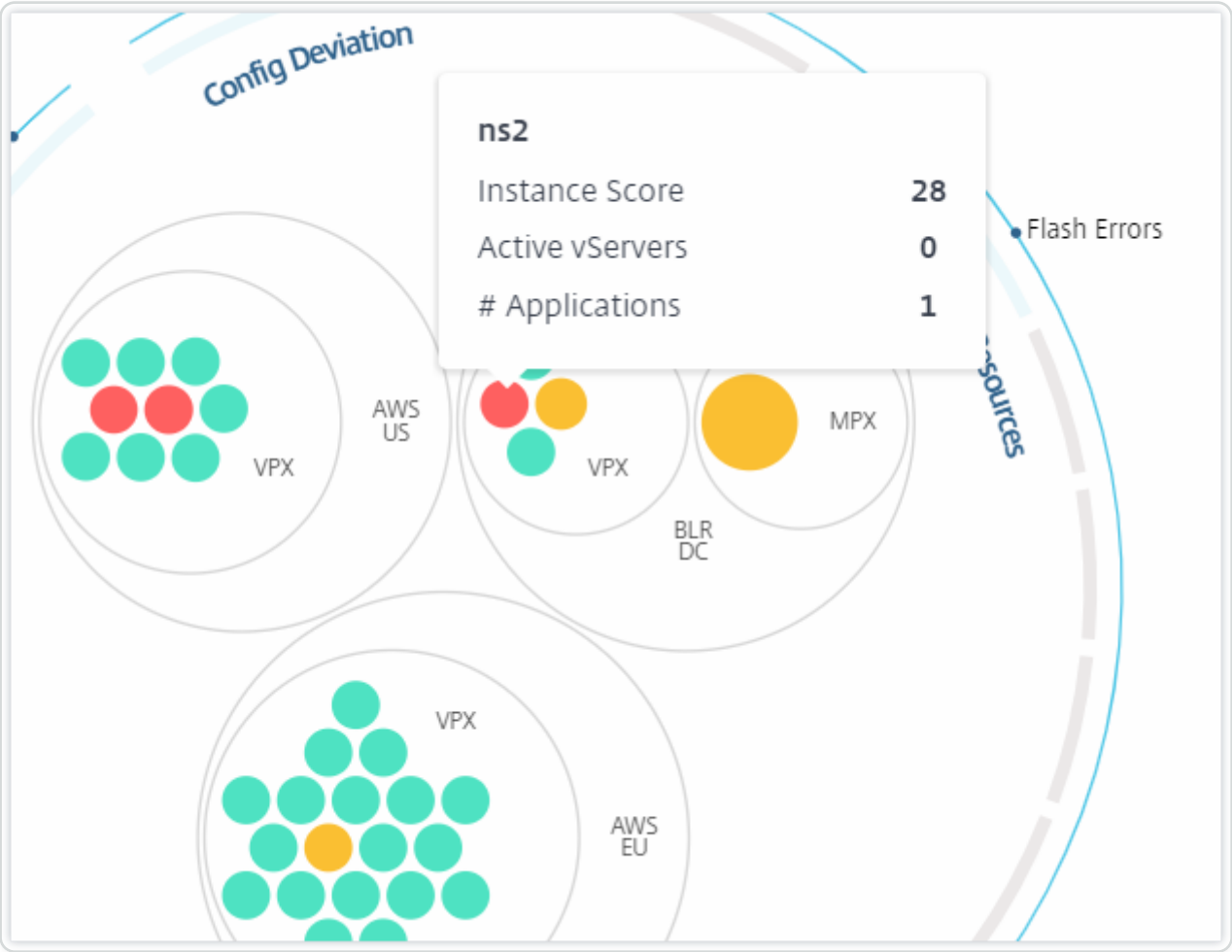
- **Green** - instance score is between 100 and 80. The instance is healthy.
- **Yellow** - instance score is between 80 and 50; some issues have been noticed and in need of review.
- **Red** - instance score is below 50. The instance is in a critical stage as there are multiple issues noticed on that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Size. The size of these colored circles indicates the number of virtual servers configured on that instance. A bigger circle indicates that there are a greater number of virtual servers.

You can hover the mouse pointer on each of the instance circles (colored circles) to view a summary. The hover tool tip displays the host name of the instance, the number of active virtual servers and the number of applications configured on that instance.



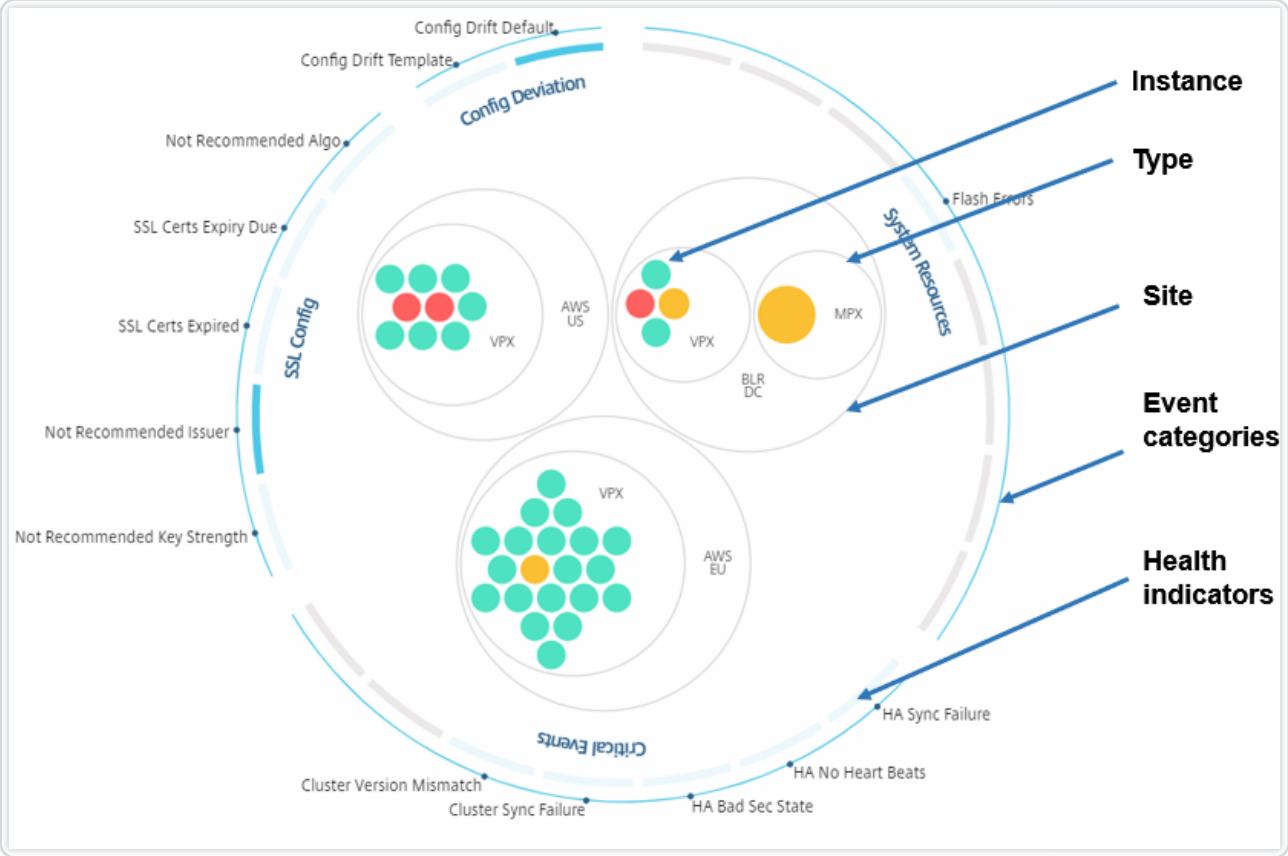
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Grouped instance circles

The Circle Pack at the outset, comprises instance circles that are grouped, nested, or packed inside another circle based on the following criteria:

- the site where they are deployed
- the type of instances deployed - VPX, MPX, SDX, and CPX
- the virtual or physical model of the ADC instance
- the ADC image version installed on the instances

The following image shows a Circle Pack where the instances are first grouped by the site or data center where they are deployed, and then they are further grouped based on their type, VPX, and MPX.



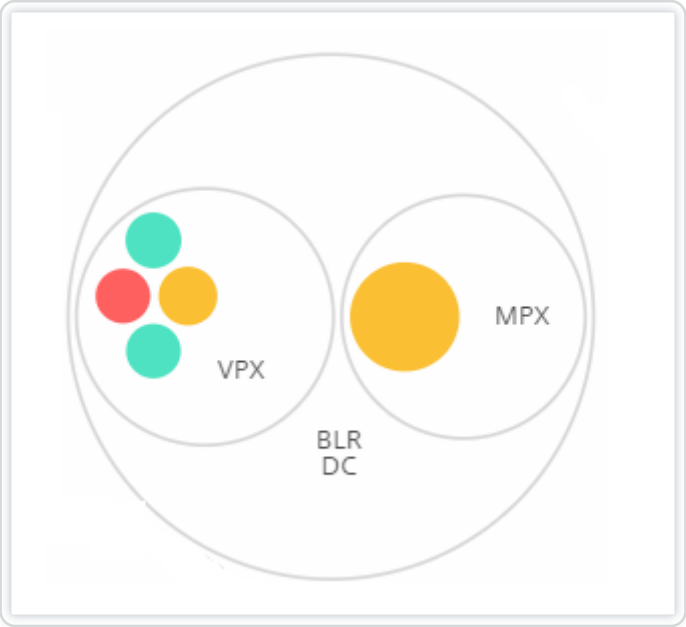
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the NetScaler ADM (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

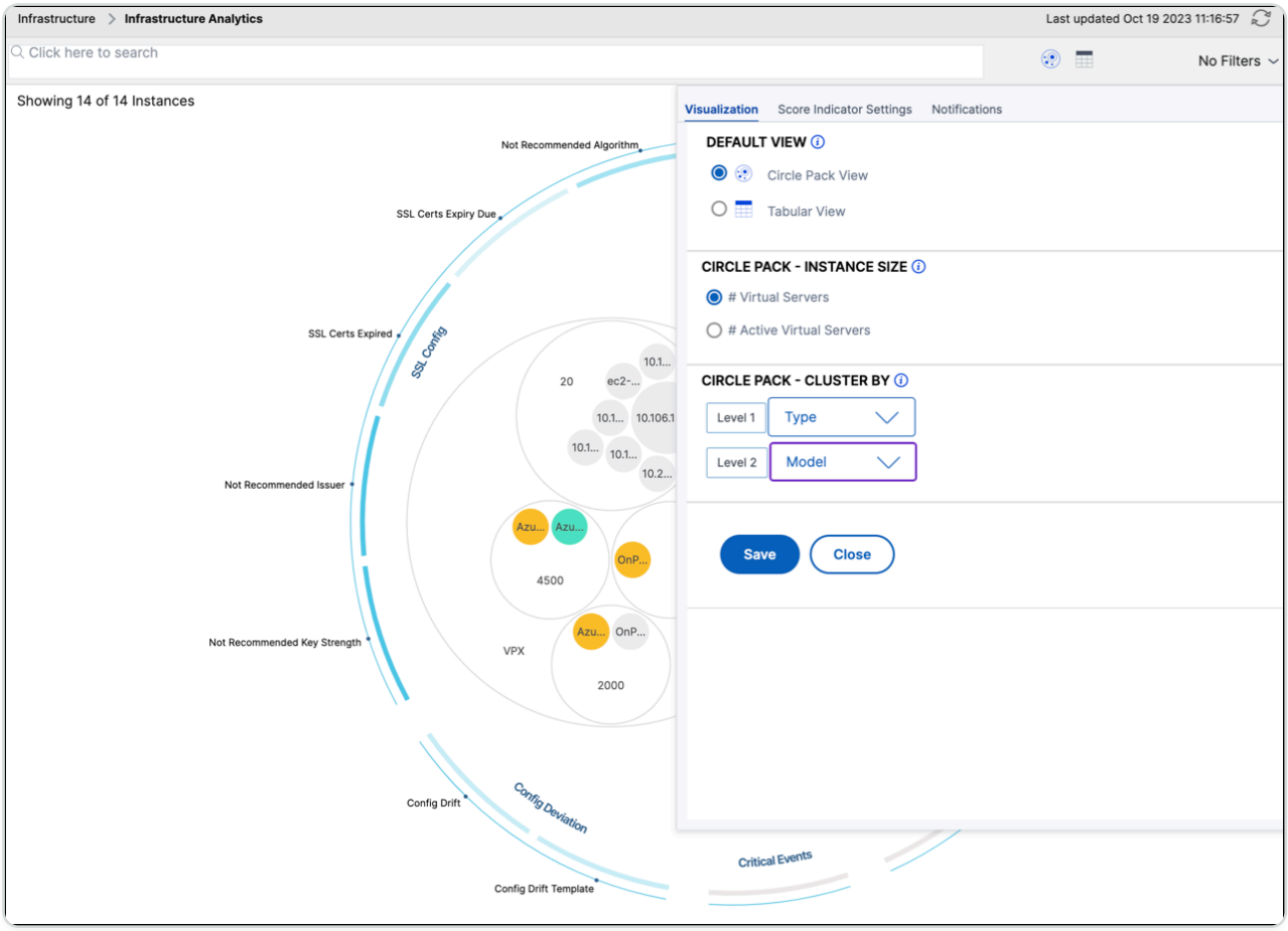
Clustered instance circles

NetScaler ADM monitors many instances. To ease the monitoring and maintenance of these instances, Infrastructure Analytics allows you to cluster them at two levels. That is, the instance groupings can be nested within another grouping.

For example, the BLR data center has two types of ADC instances - VPX and MPX, deployed in it. You can first group the ADC instances by their type and then group all instances by the site where they are grouped. You can now easily identify how many types of instances are deployed in the sites that you are managing.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

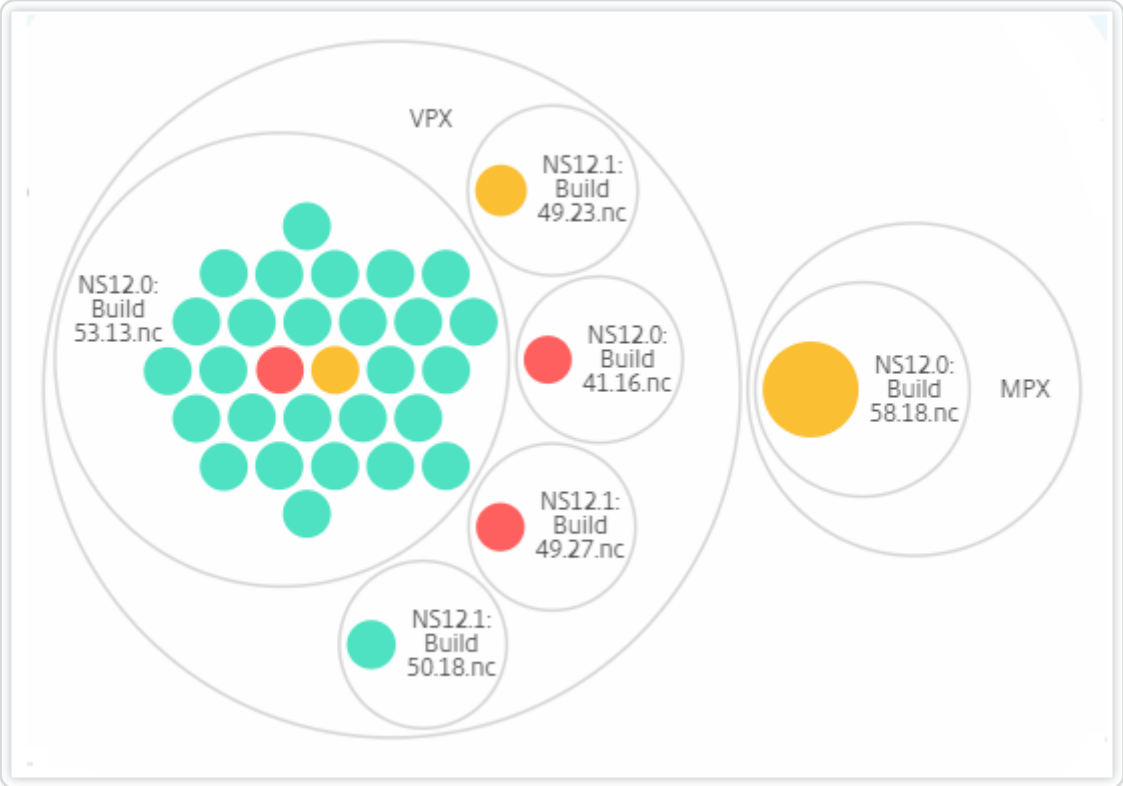


A few more examples of two-level clustering are as follows:

Site and model:

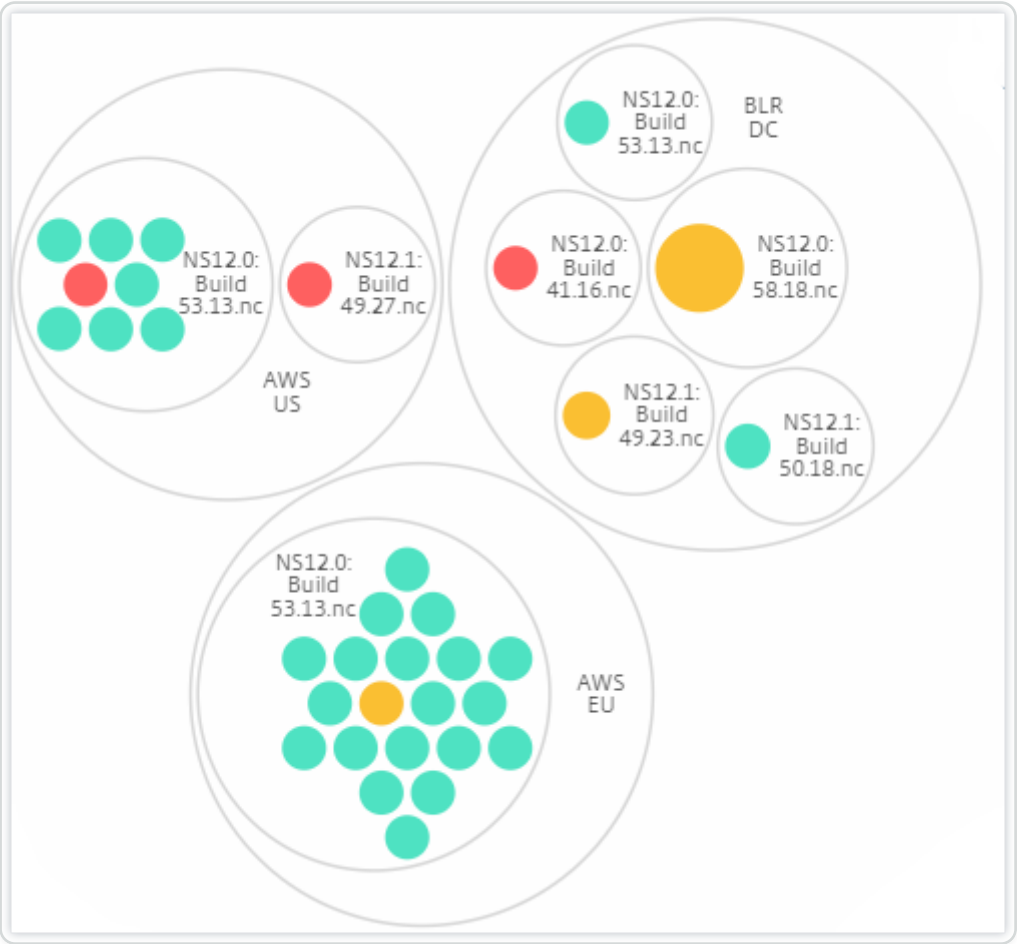
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type and version:



Site and version:

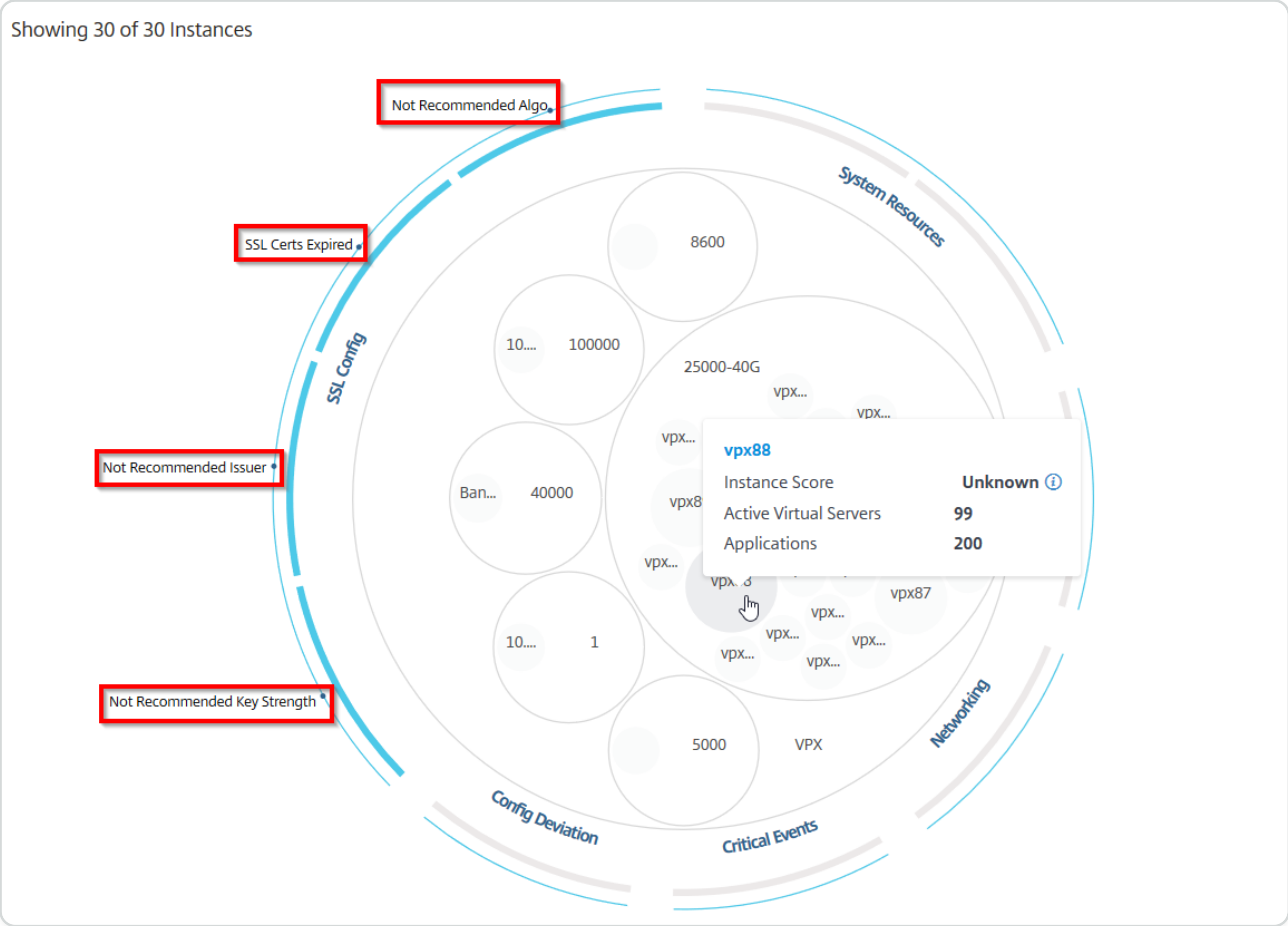
© 1997–2026 Citrix Systems, Inc. All rights reserved.



How to use Circle Pack

Click each of the colored circle to highlight that instance.

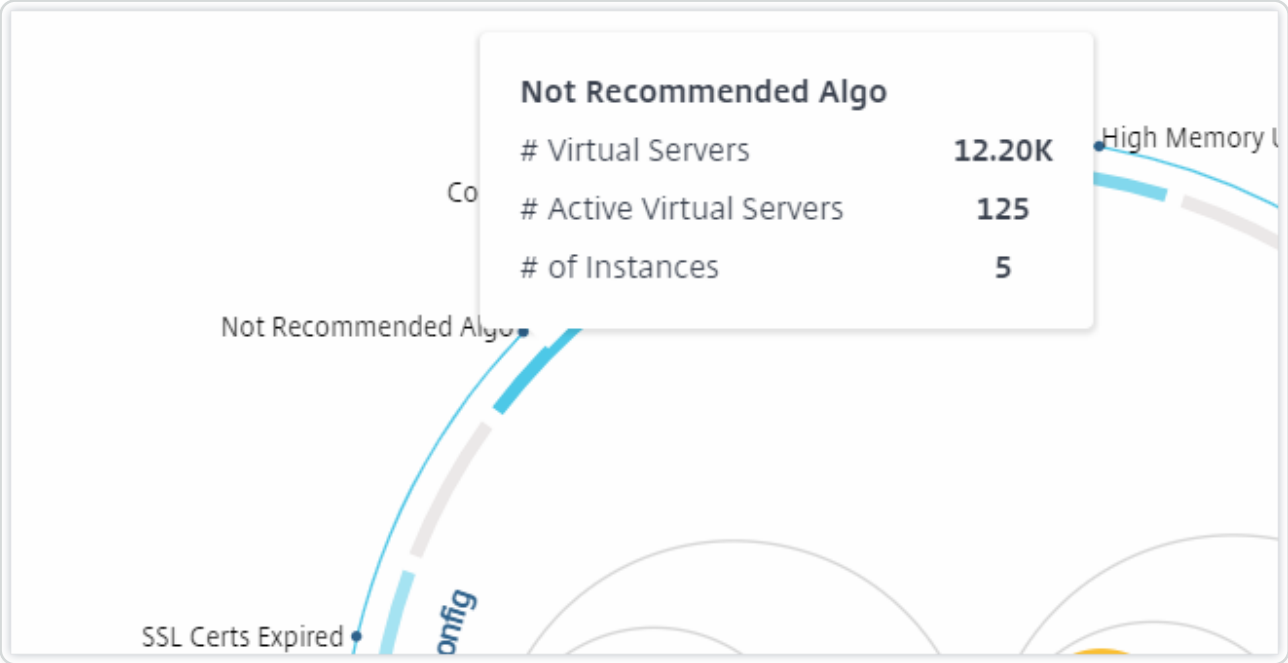
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.

You can also click the health indicators to get more details on the number of instances that have reported that risk indicator. For example, click `Not recommended Algo` to view the summary report of that risk indicator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



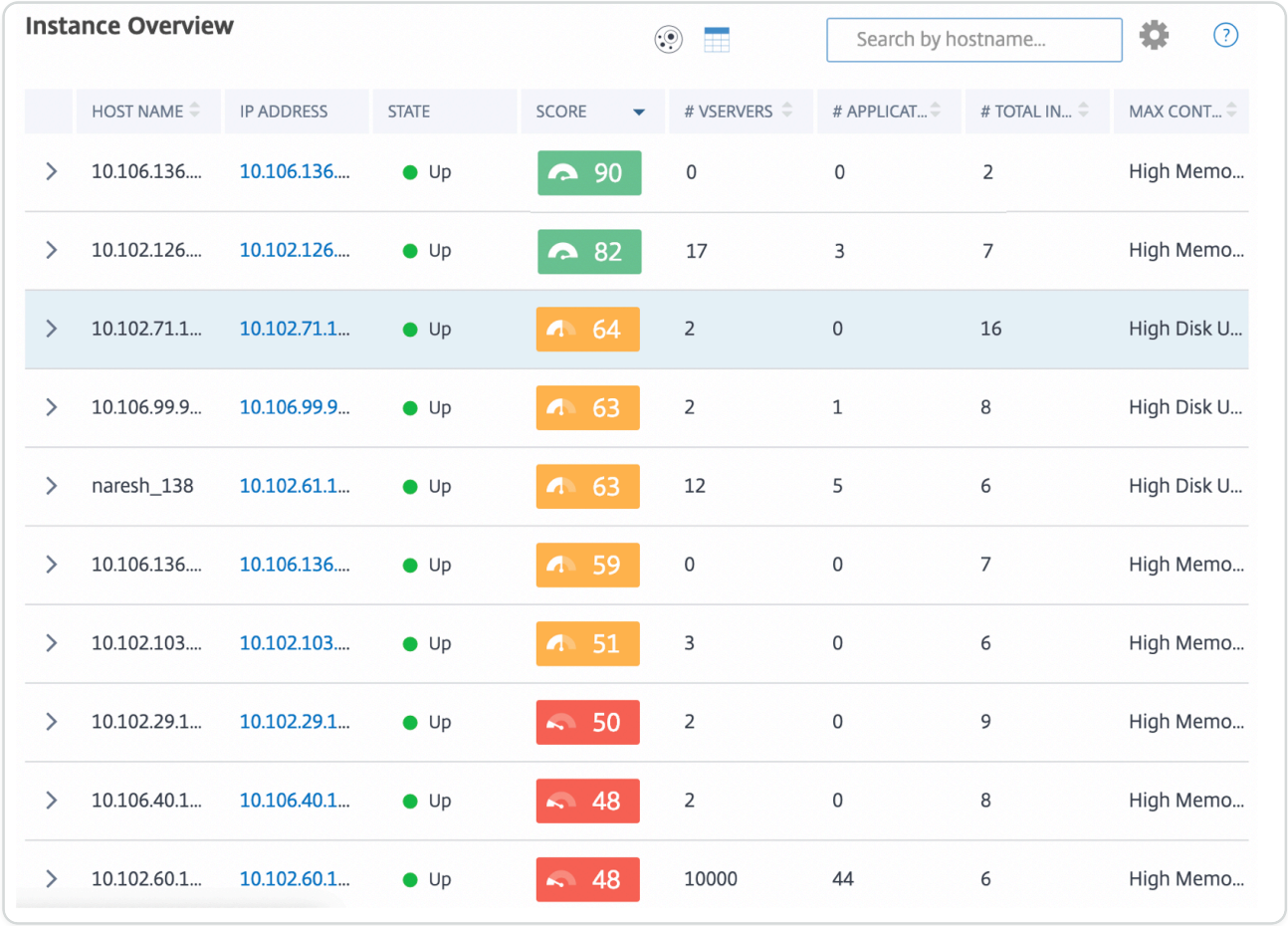
Tabular view

The tabular view displays the instances and the details of those instances in a tabular format. The details that are displayed are as follows:

- Host name of the instance
- The IP address of the instance
- State of the instance
- Instance score
- Number of virtual servers configured on that instance
- Number of applications configured on that instance
- Total number of risk indicators
- The event that is contributing more to a lowered instance score

The instances that are in the critical state are at the top of the table, followed by the instances that need to be reviewed and then the healthier instances.

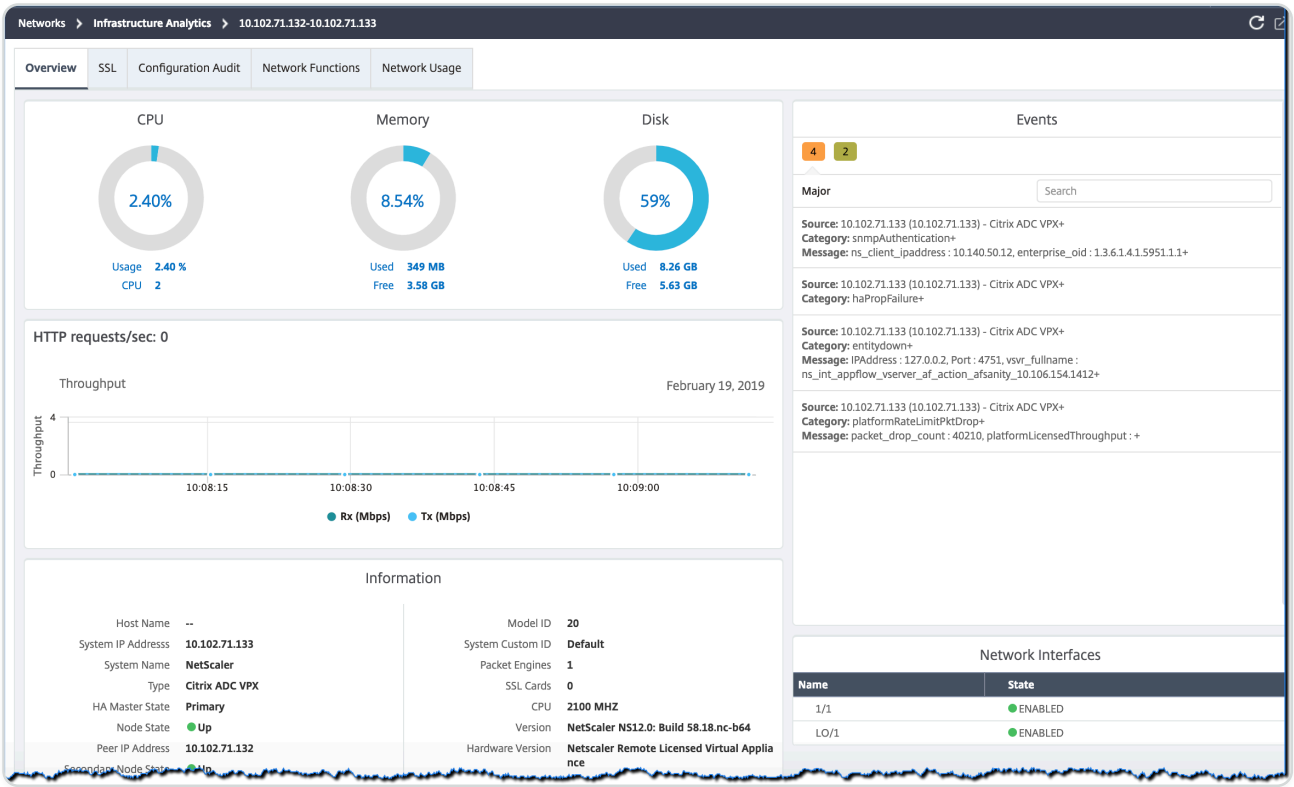
© 1997–2026 Citrix Systems, Inc. All rights reserved.



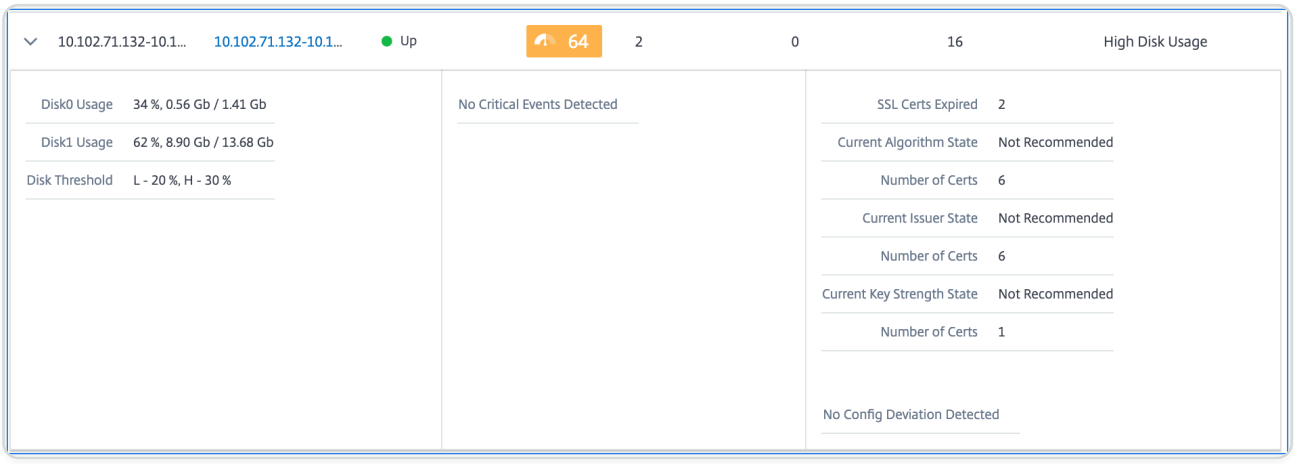
HOST NAME	IP ADDRESS	STATE	SCORE	# VSERVERS	# APPLICAT...	# TOTAL IN...	MAX CONT...
10.106.136....	10.106.136....	Up	90	0	0	2	High Memo...
10.102.126....	10.102.126....	Up	82	17	3	7	High Memo...
10.102.71.1...	10.102.71.1...	Up	64	2	0	16	High Disk U...
10.106.99.9...	10.106.99.9...	Up	63	2	1	8	High Disk U...
naresh_138	10.102.61.1...	Up	63	12	5	6	High Disk U...
10.106.136....	10.106.136....	Up	59	0	0	7	High Memo...
10.102.103....	10.102.103....	Up	51	3	0	6	High Memo...
10.102.29.1...	10.102.29.1...	Up	50	2	0	9	High Memo...
10.106.40.1...	10.106.40.1...	Up	48	2	0	8	High Memo...
10.102.60.1...	10.102.60.1...	Up	48	10000	44	6	High Memo...

Click the instance IP address in the tabular view to see more details of that instance as a dashboard display. The instance dashboard presents an overview of the instance where you can see the CPU, memory, and the disk usage of the instance. You can also see details related to SSL certificate management, config audit, network functions, and a network report that shows detailed network usage of the instance. Scroll down further to see the list of the features and the modes enabled on this instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also click the arrow at the beginning of each row to expand the row for more details.



The expanded table row displays the errors that have occurred on the instance for all the categories. In the example above, you can view that there have been errors in system resources, SSL configuration, and deviations in configuration files. But there are no critical events reported from the instance.

How to use the summary Panel

The **Summary Panel** assists you in efficiently and quickly focuses on the instances that are in need of review or critical state. The panel is divided into three tabs - overview, instance info, and traffic profile. The changes you make in this panel modifies the display in both Circle Pack and Tabular view formats. The following sections describe these tabs in more detail. The examples in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the following sections assist you to use the different selection criteria efficiently to analyze the issues reported by the instances.

Overview:

The **Overview** tab allows you to monitor the instances based on the hardware errors, usage, expired certificates and similar indicators that can occur in the instances. The indicators that you can monitor here are as follows:

- CPU usage
- Memory usage
- Disk usage
- System failures
- Critical events
- SSL certificates expiry

The following examples illustrate how you can interact with the **Overview** panel to isolate those instances that are reporting errors.

Example 1: View instances that are in a review state:

Select **Review** check box to view only those instances that are not reporting critical errors, but still needs attention.

The Histograms in the **Overview** panel represent an aggregated number of instances based on high CPU usage, high memory usage, and high disk usage events. The Histograms are graded at 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, and 100%. Hover your mouse pointer on one of the bar charts. The legend at the bottom of the chart displays the usage range and the number of instances in that range. You can also click the bar chart to display all the instances in that range.

Example 2: View instances that are consuming between 10% and 20% of the allocated memory:

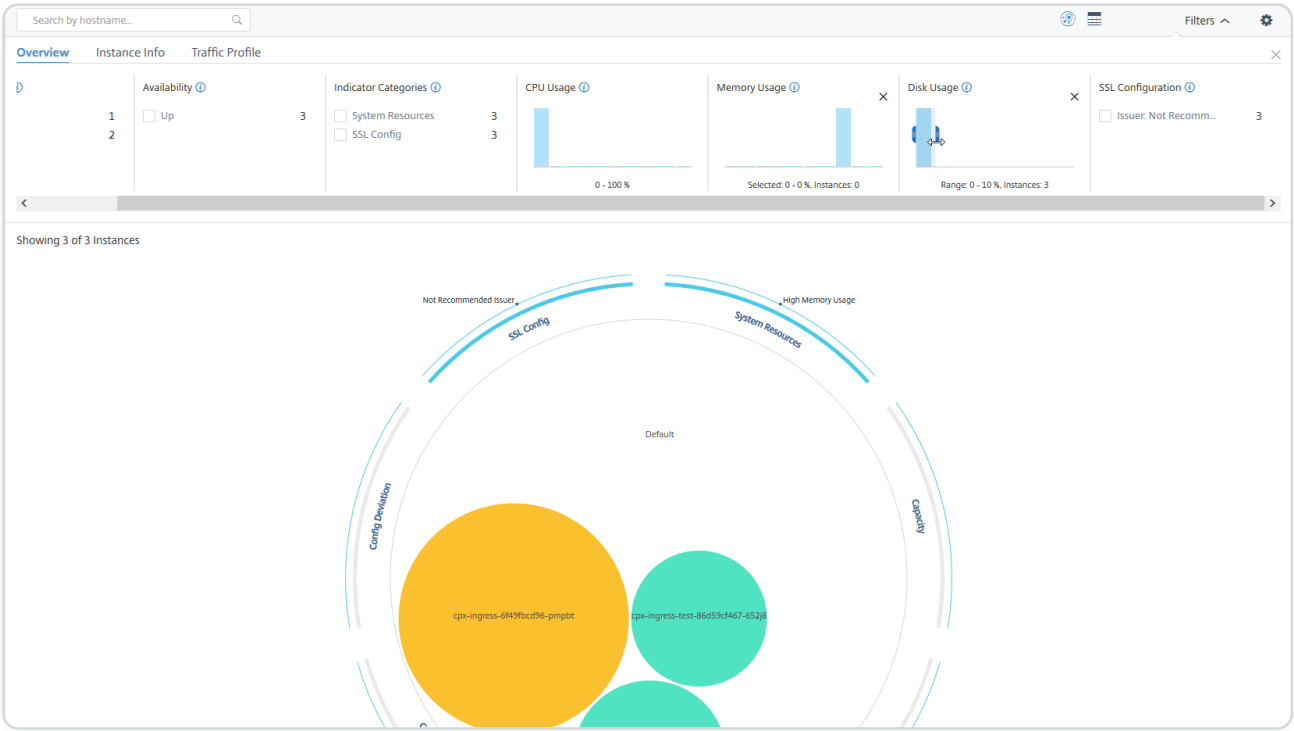
In the memory usage section, click the bar chart. The legend shows that the selected range is 10–20% and there are 29 instances operating in that range.

You can also select multiple ranges in these histograms.

Example 3: View instances that are consuming high disk space in multiple ranges:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view instances that have consumed disk space between 0 and 10%, drag the mouse pointer over the two ranges.



NOTE

Click "X" to remove the selection. You can also click **Reset** to remove multiple selections.

The horizontal bar charts in the **Overview** panel indicate the number of instances that report system errors, critical events, and expiry status of the SSL certificates. Select the check box to view those instances.

Example 4: View instances for expired SSL certificates:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1 - Click the **Filter** list.

2 - In the **SSL certificates expiry** section, select **Expired** check box to view the instances.

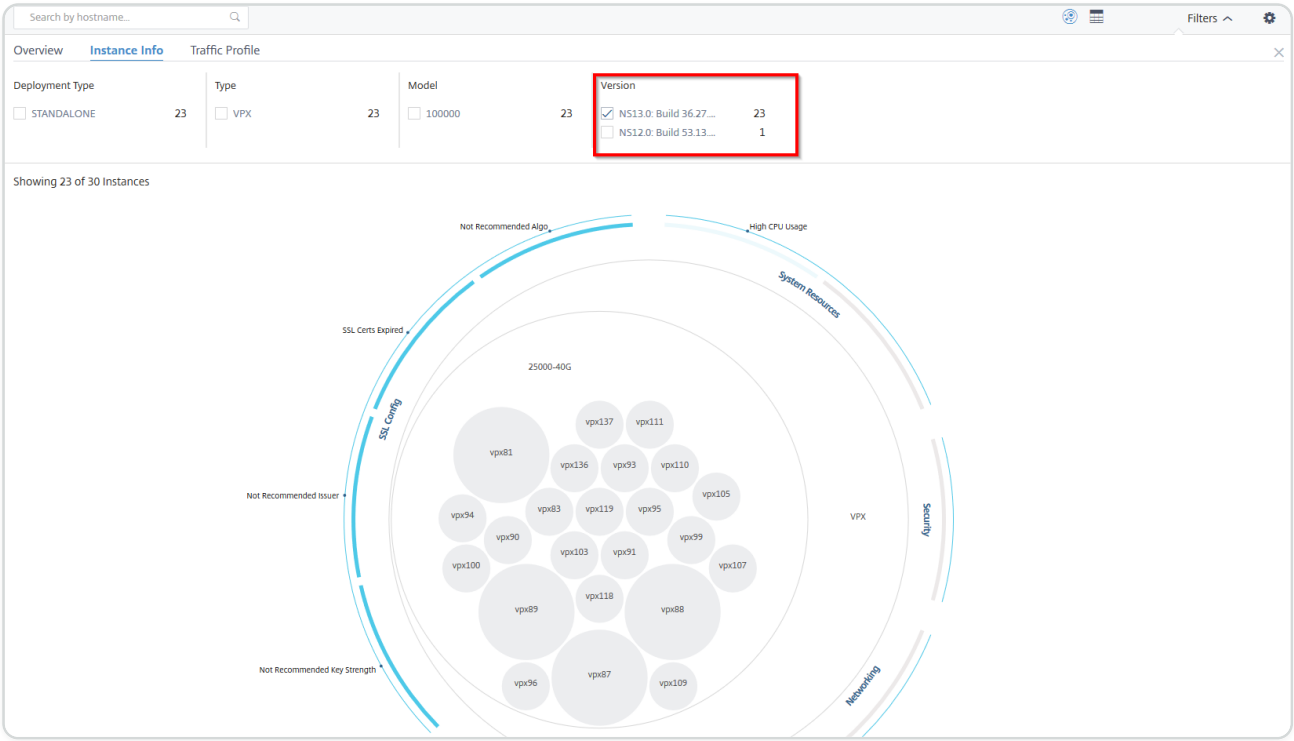
Instance info

The **Instance Info** panel allows you to view instances based on the type of deployment, instance type, model, and software version. You can select multiple check boxes to narrow down your selection.

Example 5: View NetScaler VPX instances with specific build number:

Select the version that you want to view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



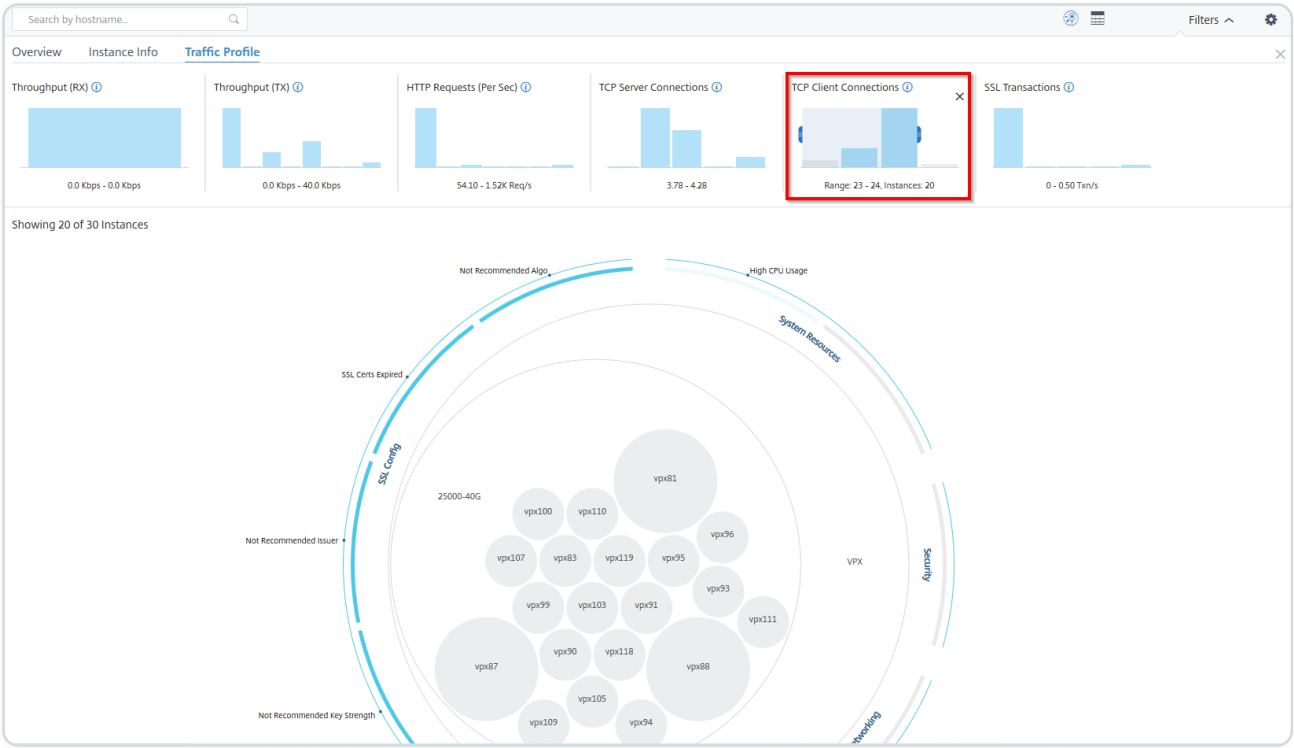
Traffic profile

The Histograms in the **Traffic profile** panel represent an aggregated number of instances based on the licensed throughput on the instances, number of requests, connections, and transactions handled by the instances. Select the bar chart to view instances in that range.

Example 6: View instances supporting TCP connections:

The following image shows the number of instances supporting TCP connections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



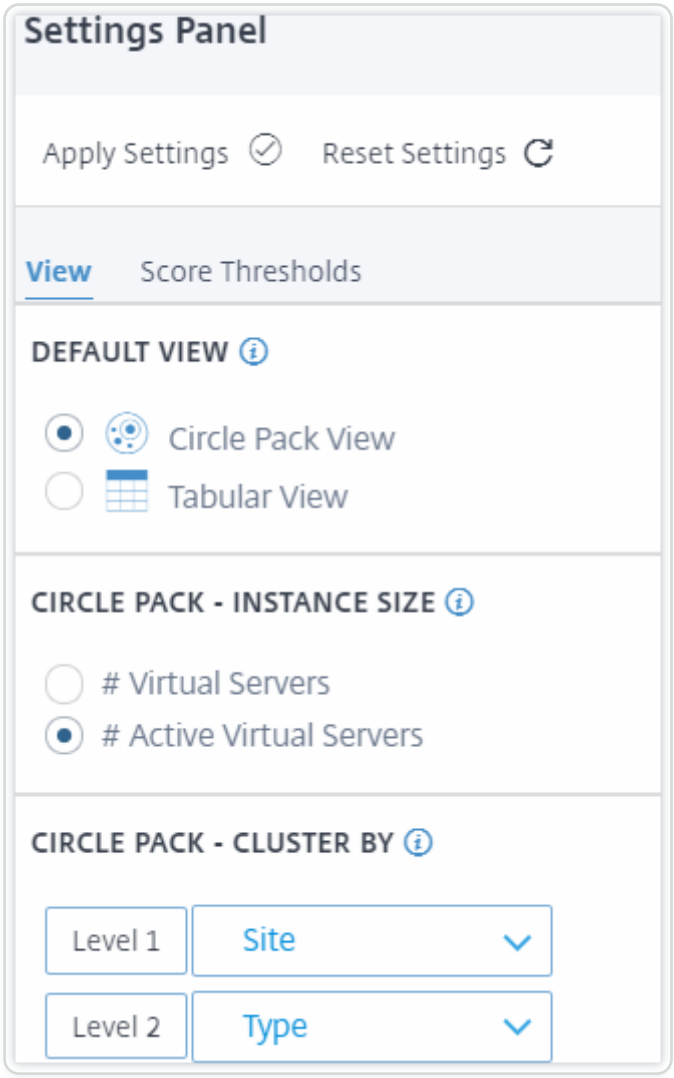
How to use the settings panel

The **Settings** panel allows you to set the default view of the Infrastructure Analytics. It also allows you to set the low and high threshold values for high CPU usage, high disk usage, and high memory usage. The settings panel is divided into two tabs - View and Score Thresholds.

View

- **Default View**. Select **Circle Pack** or Tabular format as the default view on the analytics page. The format you select is what you see whenever you access the page in NetScaler ADM.
- **Circle Pack - Instance Size**. Allow the size of the instance circle to by either the number of virtual servers or the number of active virtual servers.
- **Circle Pack - Cluster By**. Decide the two-level clustering of the instance circles. For more information on instance clustering, see Clustered instance circles.

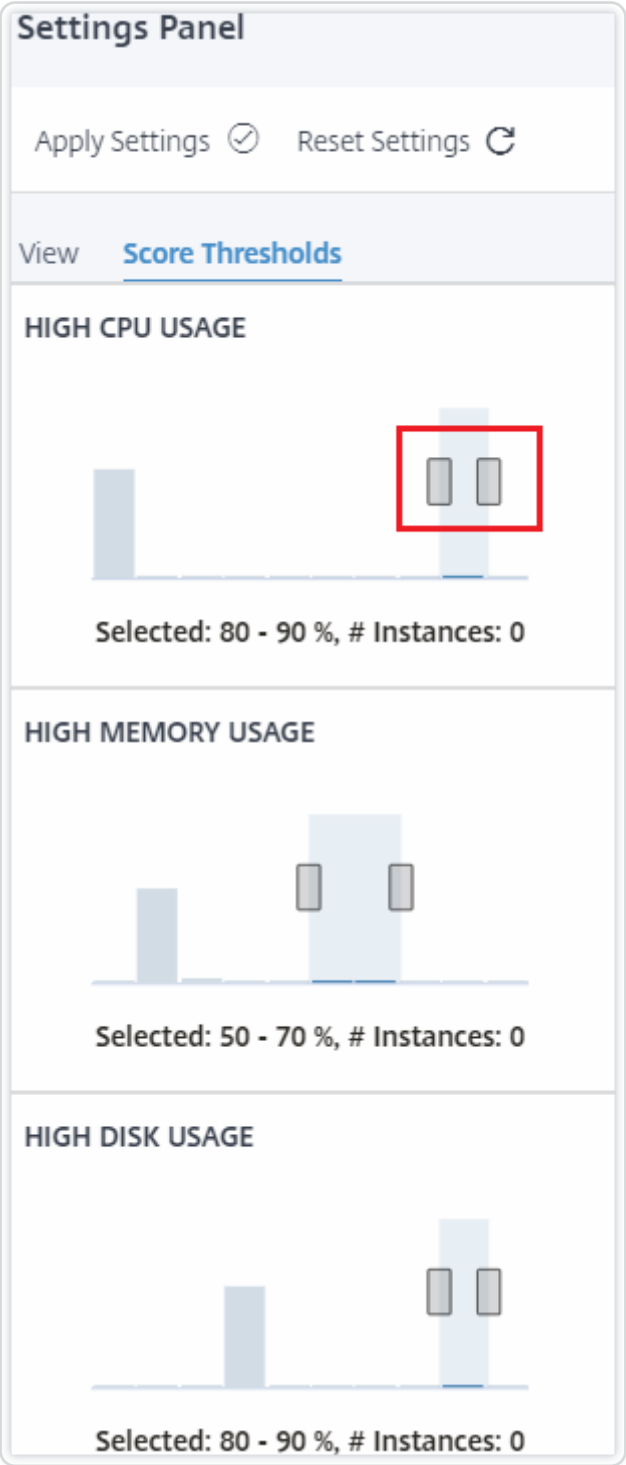
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Score thresholds

You can modify the low and high threshold values for high CPU, memory, and disk usage depending on the traffic requirements in your organization. Drag the handles in each of the selection Histogram to set the values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

Click **Apply Settings** to apply these changes, or click **Reset** to remove all changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to visualize data on the dashboard

Using Infrastructure Analytics, network admins can now identify instances needing the most attention within a few seconds. To understand data visualization in more detail, let us consider the case of Chris, a network admin of ExampleCompany.

Chris maintains many NetScaler instances in the organization. A few of the instances process high traffic, and Chris needs to monitor them closely. Chris notices that a few high-traffic instances are no longer processing the full traffic passing through them. To analyze this reduction, earlier, Chris had to read multiple data reports coming in from various sources. Chris had to spend more time trying to correlate the data manually and ascertain which instances are not in optimal state and need attention.

Chris uses the Infrastructure Analytics feature to see the health of all instances visually.

The following two examples illustrate how Infrastructure Analytics assists Chris in maintenance activity:

Example 1 - To monitor the SSL traffic:

Chris notices on the Circle Pack that one instance has a low instance score and that instance is in "Critical" state. Chris clicks that instance to see what the issue is. The instance summary displays that there is an SSL card failure on that instance and the instance is unable to process SSL traffic (the SSL traffic has reduced). Chris extracts that information and sends a report to the team to look into the issue immediately.

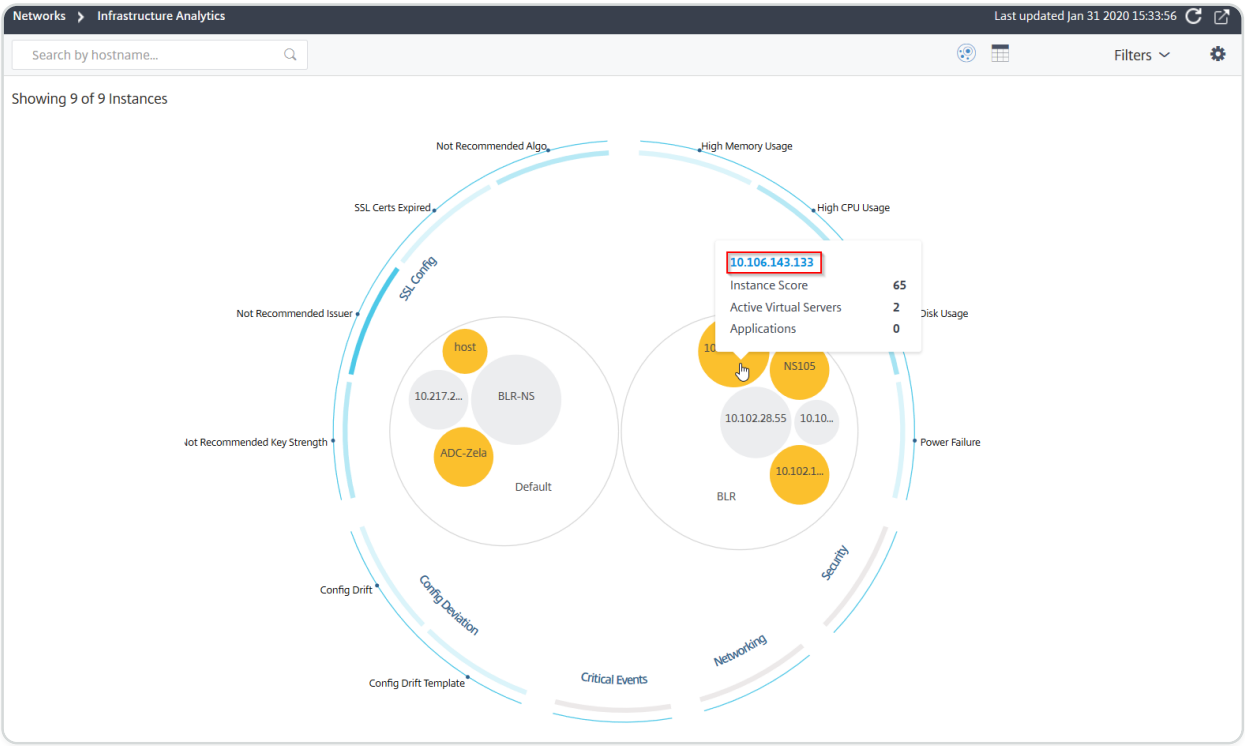
Example 2 - To monitor configuration changes:

Chris also notices that another instance is in "Review" state and that there has been a config deviation recently. When Chris clicks the config deviation risk indicator, Chris notices that RC4 Cipher, SSL v3, TLS 1.0, and TLS 1.1 related configuration changes have been made which might be due to security concerns. Chris also notices that the SSL transaction traffic profile for this instance has gone down. Chris exports this report and sends it to the admin to inquire further.

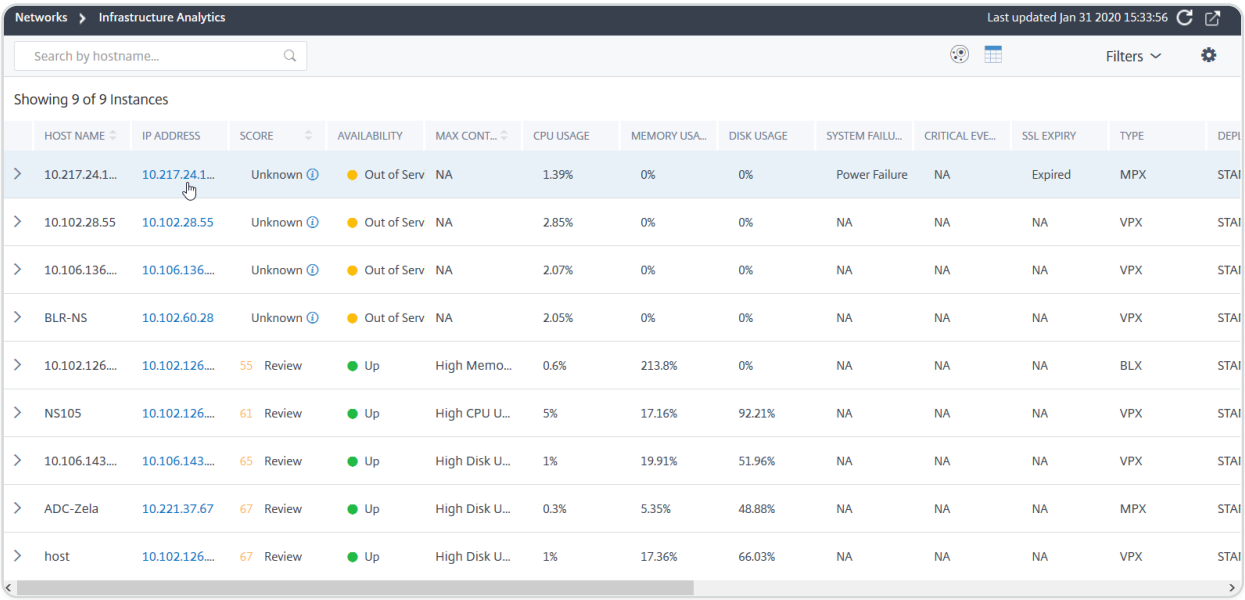
View instance details in Infrastructure Analytics

1. Navigate to **Infrastructure > Infrastructure Analytics**
2. Click the circle pack view and select the IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also click an IP address from the table view.



HOST NAME	IP ADDRESS	SCORE	AVAILABILITY	MAX CONT...	CPU USAGE	MEMORY USA...	DISK USAGE	SYSTEM FAILU...	CRITICAL EVE...	SSL EXPIRY	TYPE	DEPL
10.217.24.1...	10.217.24.1...	Unknown	Out of Serv	NA	1.39%	0%	0%	Power Failure	NA	Expired	MPX	STAI
10.102.28.55	10.102.28.55	Unknown	Out of Serv	NA	2.85%	0%	0%	NA	NA	NA	VPX	STAI
10.106.136....	10.106.136....	Unknown	Out of Serv	NA	2.07%	0%	0%	NA	NA	NA	VPX	STAI
BLR-NS	10.102.60.28	Unknown	Out of Serv	NA	2.05%	0%	0%	NA	NA	NA	VPX	STAI
10.102.126....	10.102.126....	55 Review	Up	High Memo...	0.6%	213.8%	0%	NA	NA	NA	BLX	STAI
NS105	10.102.126....	61 Review	Up	High CPU U...	5%	17.16%	92.21%	NA	NA	NA	VPX	STAI
10.106.143....	10.106.143....	65 Review	Up	High Disk U...	1%	19.91%	51.96%	NA	NA	NA	VPX	STAI
ADC-Zela	10.221.37.67	67 Review	Up	High Disk U...	0.3%	5.35%	48.88%	NA	NA	NA	MPX	STAI
host	10.102.126....	67 Review	Up	High Disk U...	1%	17.36%	66.03%	NA	NA	NA	VPX	STAI

- **Host name** – Denotes the host name assigned to the ADC instance
- **IP address** – Denotes the IP address of the ADC instance
- **Score** – Denotes the ADC instance score and the status such as Critical, Good, and Fair
- **Availability** – Denotes the status of the ADC instance such as **Up**, **Down**, or **Out of service**.
- **Max Contribution** – Denotes the issue category that the ADC instance has the maximum error counts.
- **CPU usage** – Denotes the current CPU % used by the instance
- **Memory usage** – Denotes the current memory % used by the instance

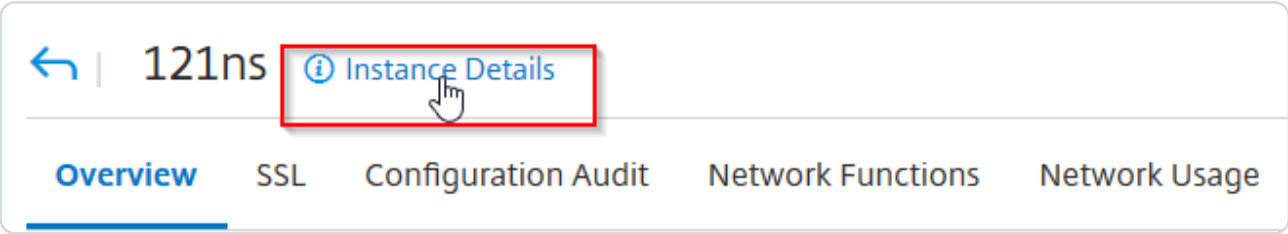
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Disk usage** – Denotes the current disk % used by the instance
- **System Failure** – Denotes the total number of errors for the instance system
- **Critical Events** – Denotes the event category that the NetScaler instance has the maximum events
- **SSL expiry** – Denotes the status of the SSL certificate installed on the ADC instance
- **Type** – Denotes the ADC instance type such as VPX, SDX, MPX, or CPX
- **Deployment** – Denotes if the ADC instance is deployed as a standalone instance or HA pair
- **Model** – Denotes the ADC instance model number
- **Version** – Denotes the ADC instance version and build number
- **Throughput** – Denotes the current network throughput from the ADC instance
- **HTTPS request/sec** – Denotes the current HTTPS requests/sec received by the ADC instance
- **TCP connection** – Denotes the current TCP connections established
- **SSL transaction** – Denotes the current SSL transactions processed by the ADC instance
- **Site** – Denotes the name of the site that the ADC instance is deployed.

NOTE

For every 5 minutes, the current values for CPU usage, memory usage, disk usage, throughput, and so on are updated.

Click **Instance Details** to view the details.



The following details are displayed:

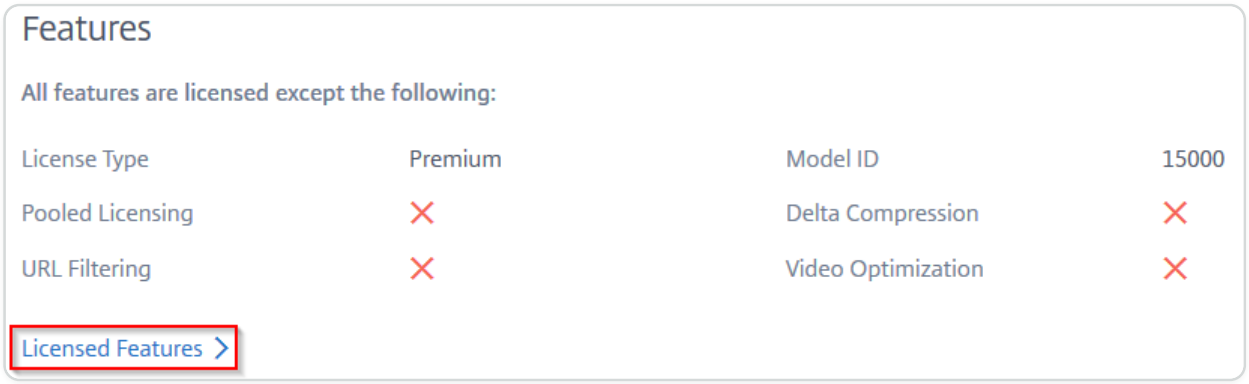
- **Information** - Instance details such as instance type, deployment type, version, model.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Information

HOST NAME	217ns	MODEL ID	15000
SYSTEM IP ADDRESS	10.106.181.217	SYSTEM CUSTOM ID	Default
SYSTEM NAME	NetScaler	PACKET ENGINES	1
TYPE	Citrix ADC VPX	SSL CARDS	0
HA MASTER STATE	Primary	CPU	2099MHZ
NODE STATE	Up	VERSION	NetScaler NS11.1: Build 62.8.nc
PEER IP ADDRESS	--	HARDWARE VERSION	NetScaler Virtual Appliance
SECONDARY NODE STATUS	--	LOM VERSION	-NA-
HA SYNC STATUS	ENABLED	HOST ID	000c29e1c592
SYSTEM SERVICES	72	SERIAL NUMBER	HE2H81UJ47
NETMASK	255.255.255.0	ENCODED SERIAL NUMBER	891e0000cb254307ee9a
GATEWAY	10.106.181.1	CITRIX ADC UUID	--
ADMIN PROFILE	ns_nsroot_profile	LOCATION	POP (default)
HEALTH	--	CONTACT PERSON	WebMaster (default)
UPTIME	25 days, 19 hours, 42 minutes		
DESCRIPTION	--		

- **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



Features

All features are licensed except the following:

License Type	Premium	Model ID	15000
Pooled Licensing	✕	Delta Compression	✕
URL Filtering	✕	Video Optimization	✕

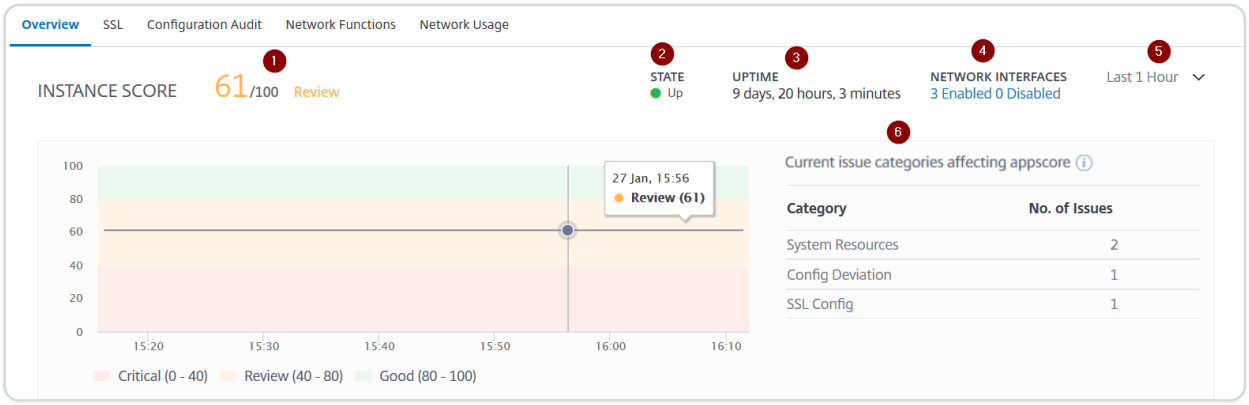
Licensed Features >

- **Modes** – By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**



1 – Indicates the current NetScaler instance score for the selected time duration. The final score is calculated as **100 minus total penalties**. The graph displays the score ranges for the selected time duration.

2 – Indicates the status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 – Indicates the duration that the NetScaler instance is up and running.

4 – Indicates the total network interfaces enabled and disabled for the instance. Click to view the details such as network interface name and the status (enabled or disabled).

5 – Select the time duration from the list to view the instance details.

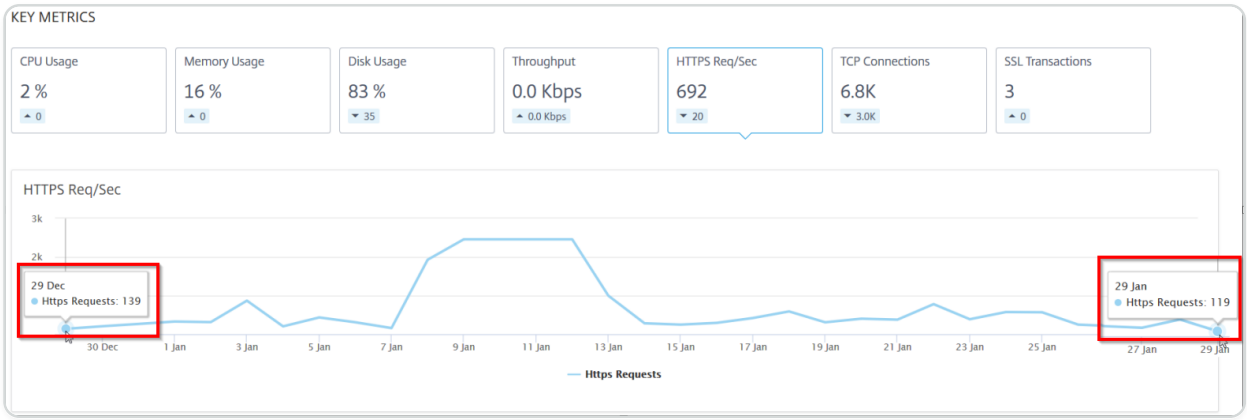
6 – Displays the total issues and issue category of the ADC instance.

- **Key Metrics**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click each tab to view the details. In each metric, you can view the average value and the difference value for the selected time.

The following image is an example for HTTPS Req/Sec and the selected time duration is 1 hour. The value **692** is the average HTTPS Req/Sec for the 1-month duration and the value **20** is the difference value. In the graph, the first value is **139** and the last value is **119**. The difference value is **139 – 119 = 20**.



You can view the following instance metrics in a graph format for the selected time duration:

- **CPU Usage** – The average CPU % from the instance for the selected duration (displays for both packet CPU and for management CPU).
- **Memory Usage** – The average memory usage % from the instance for the selected duration.
- **Disk Usage** – The average disk space % from the instance for the selected duration.
- **Throughput** – The average network throughput processed by the instance for the selected duration.
- **HTTPS request/sec** – The average HTTPs requests received by the instance for the selected duration.
- **TCP connections** – The average TCP connections established by the client and server for the selected duration.
- **SSL transactions** – The average SSL transactions processed by the instance for the selected duration.

- **Issues**

  You can view the following issues that occur in NetScaler instance:

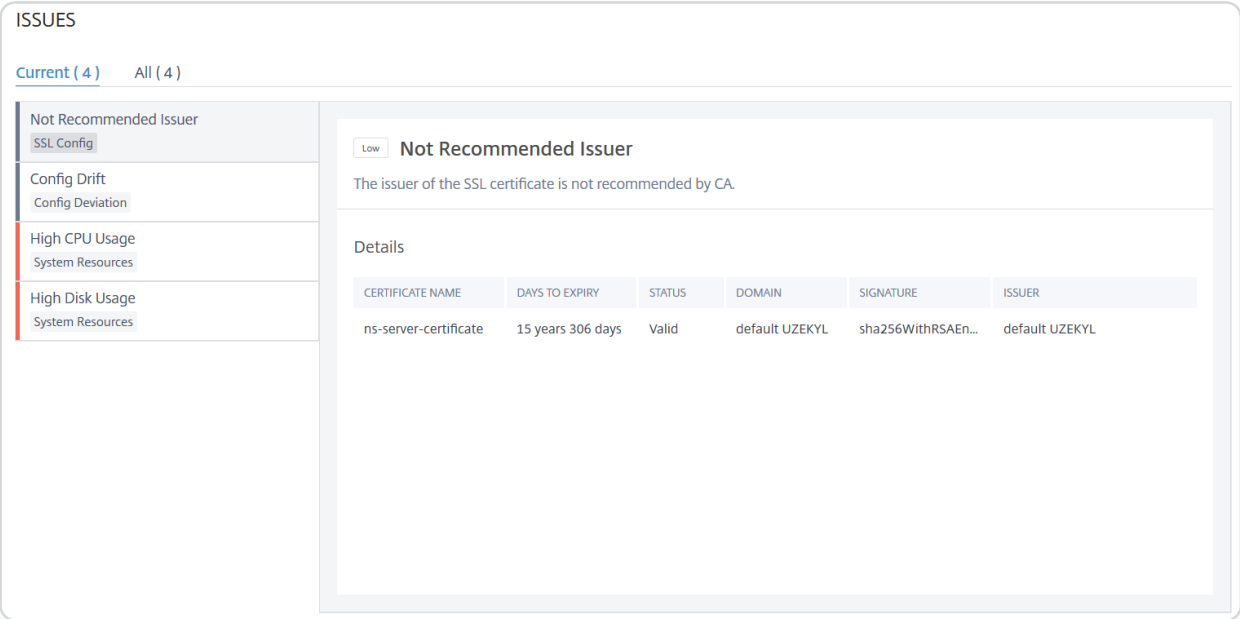
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage.	- High CPU Usage
		- High Memory Usage
		- High Disk Usage
		- SSL Card Failures
		- Power Failure
		- Disk Error
		- Flash Error
		- NIC Discards
SSL Config	Displays all issues related to the SSL configuration on the NetScaler instance.	- SSL Certs Expired
		- Not Recommended Issuer
		- Not Recommended Algorithm
		- Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in NetScaler instance.	- Config Drift
		- Running vs Template
Critical events	Displays all critical events related to NetScaler instances configured in HA pair and in Cluster.	- Cluster Prop Failure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
		- Cluster Sync Failure
		- Cluster versions Mismatch
		- HA Bad Secondary State
		- HA No Heat Beats
		- HA Sync Failure
		- HA Version Mismatch
Networking	Displays the operational issues that occur in the instances.	For more information, see Enhanced Infrastructure Analytics with new indicators.

Click each tab to analyze and troubleshoot the issue. For example, consider that an instance has the following errors for the selected time duration:



- The **Current** tab displays the issues that are currently affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View the capacity issues in an ADC instance

When an ADC instance has consumed most its available capacity, packet-drop may occur while processing the client traffic. This issue causes low performance in an ADC instance. By understanding such ADC capacity issues, you can proactively allocate additional licenses to steady the ADC performance.

In the **Circle Pack View**, you can view the ADC instance capacity issues if exists.

To view ADC capacity issues,

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Select the circle pack view.

NOTE

In **Infrastructure Analytics**, the circle-pack and tabular views display the events and issues that occurred in the last one hour.

The following illustration suggests the capacity issues exist in the selected instance:

The issues are categorized on the following capacity parameters:

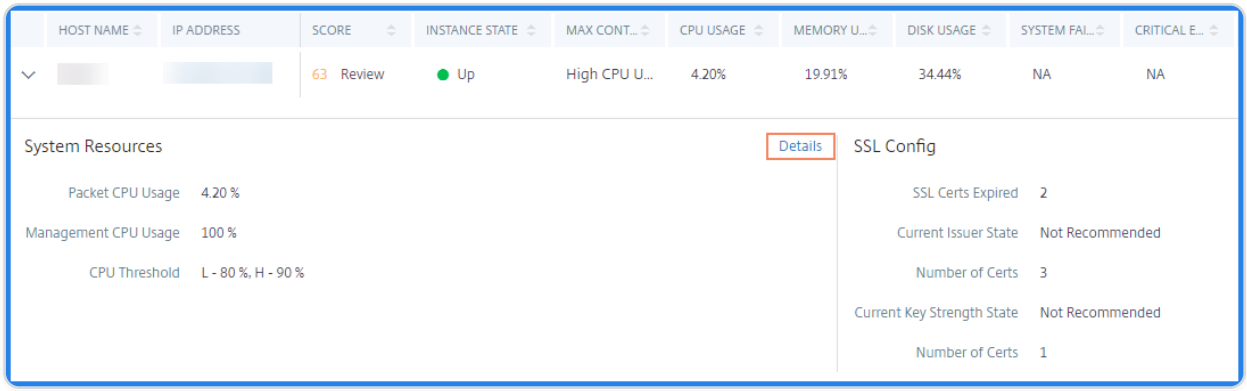
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Throughput Limit Reached** – The number of packets dropped in the instance after the throughput limit is reached.
- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** – The number of packets dropped in the instance after the PPS limit is reached.
- **SSL Throughput Rate Limit** – The number of times the SSL throughput limit reached.
- **SSL TPS Rate Limit** – The number of times the SSL TPS limit reached.

View recommended actions to solve capacity issues

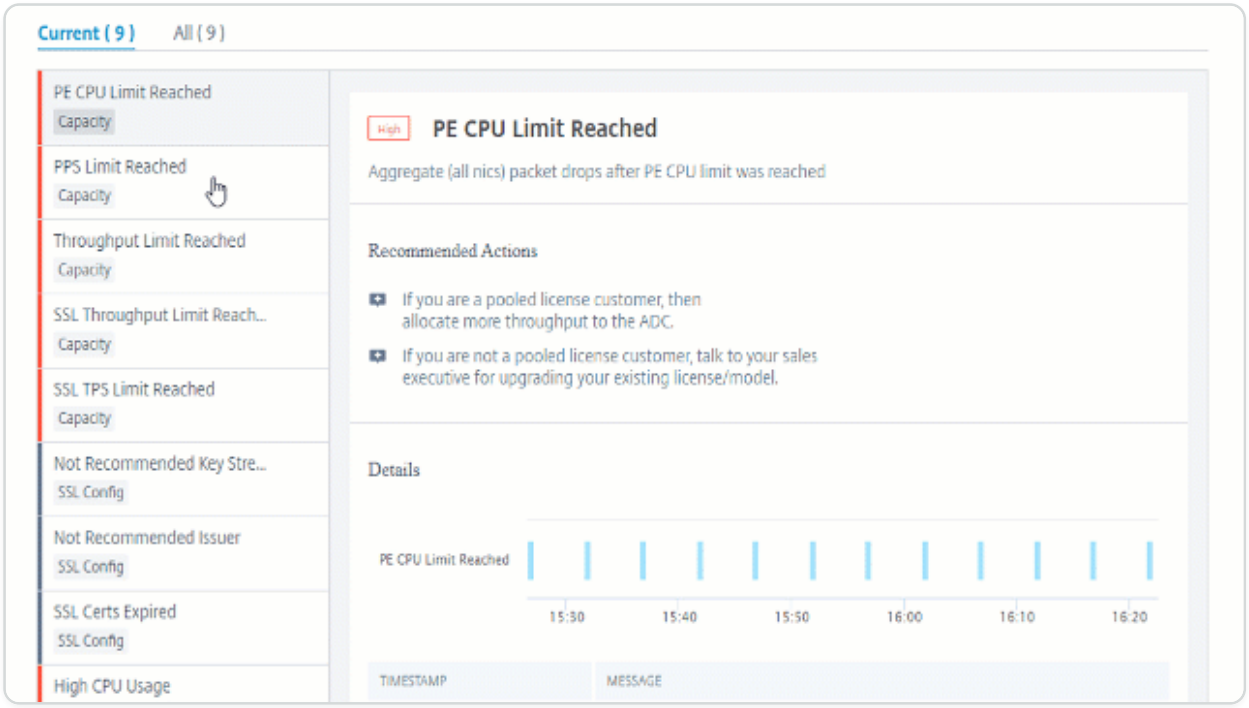
The ADM recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

1. In **Infrastructure > Infrastructure Analytics**, select the tabular view.
2. Select the instance that has capacity issues and click **Details**.



3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The ADM polls these events every five minutes from the ADC instance and displays the packet drops or rate-limit counter increments if exists.

The ADM calculates the instance score on the defined capacity threshold.

- **Low threshold** – 1 packet drop or rate-limit counter increment
- **High threshold** – 10000 packets drop or rate-limit counter increment

Therefore, when an ADC instance breaches the capacity threshold, the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the `ADCCapacityBreach` category. To view these events, navigate to **Accounts > System Events**.

Enhanced Infrastructure Analytics with new indicators

Using the NetScaler® ADM Infrastructure Analytics, you can:

- View a new set of operational issues that occur in NetScaler instances.
- View error messages and check recommendations to troubleshoot the issues.

As an administrator, you can quickly identify the root cause analysis of issues.

NOTE

Rule indicators are not supported for:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

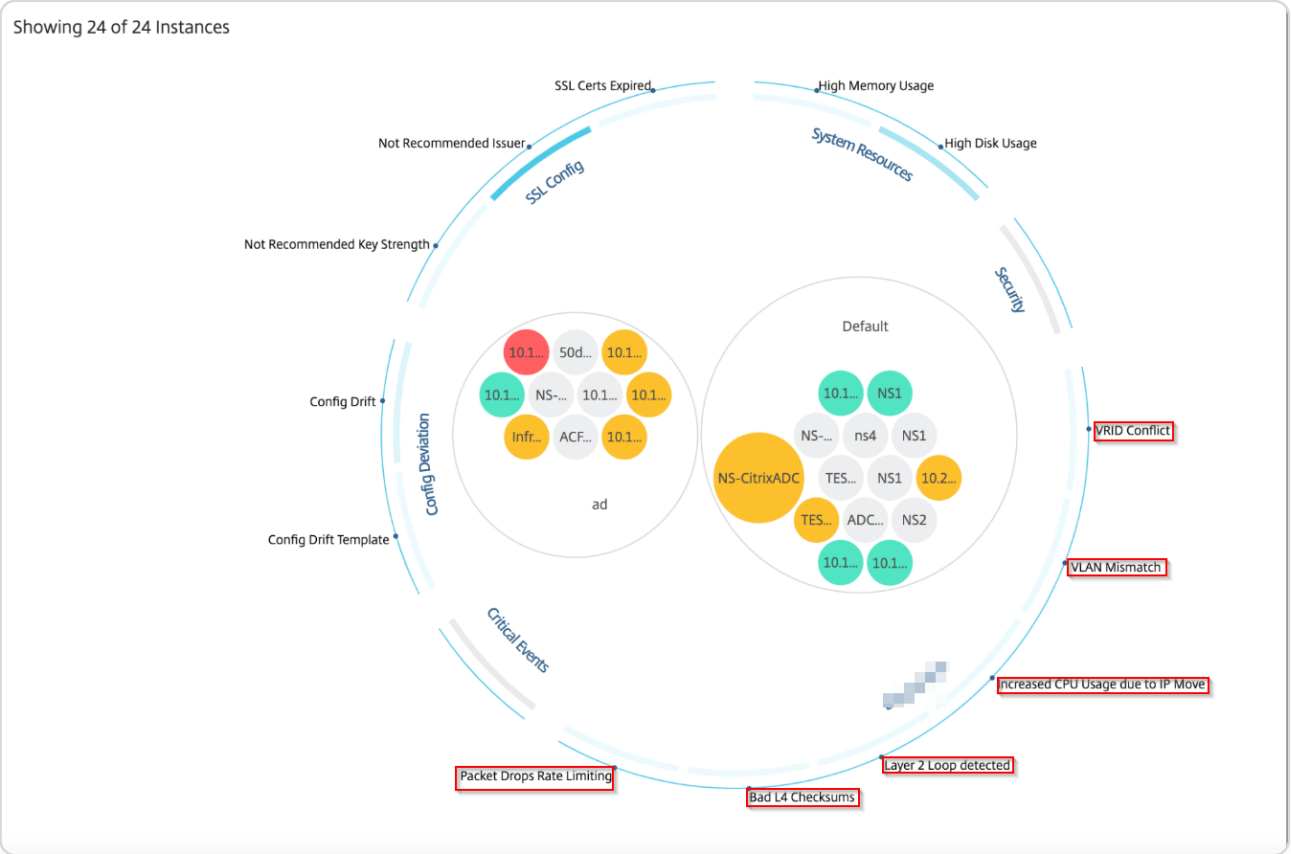
- NetScaler instances configured in a cluster mode.
- NetScaler instances configured with admin partitions.

In NetScaler ADM, navigate to **Infrastructure > Infrastructure Analytics** to view indicators for:

INDICATOR NAME IN INFRASTRUCTURE ANALYTICS	DESCRIPTION
Port allocation failure	Detects when NetScaler uses SNIP to communicate with a new server connection and total ports available on that SNIP are exhausted. The recommended action is to add another SNIP in the same subnet.
No default route configuration	Detects when the traffic gets dropped because of non-availability of routes.
IP conflict	Detects if a same IP address is configured or applied on two or more instances in a network.
VRID conflict	Detects when intermittent access problems occur for the specified VRID.
VLAN mismatch	Detects if any errors occur during VLAN configuration bound to IP subnets.
TCP small window attack	Detects when there is a possible small window attack in progress. This alert is just for informational, because ADC already mitigates this attack.
Rate control threshold	Detects when packets are dropped based on the configured rate control threshold.
Persistence Limit	Detects when maximum hits are imposed on the NetScaler memory.
GSLB site name mismatch	Detects when GSLB configuration synchronization failures occur because of site name mismatch.
Malformed IP header	Detects when sanity checks on IPv4 packets are failed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INDICATOR NAME IN INFRASTRUCTURE ANALYTICS	DESCRIPTION
Bad L4 checksums	Detects when checksum validation for TCP packets is failed.
Increased CPU usage due to IP move	Detects if a large number of macs need to be updated.
Excessive packet steering	Detects high levels of software packet steering due to the usage of asymmetric rss key type.
Layer 2 loop	Detects the presence of layer 2 loops in the network.
Tagged VLAN mismatch	Detects when tagged VLAN packets are received on an untagged interface.



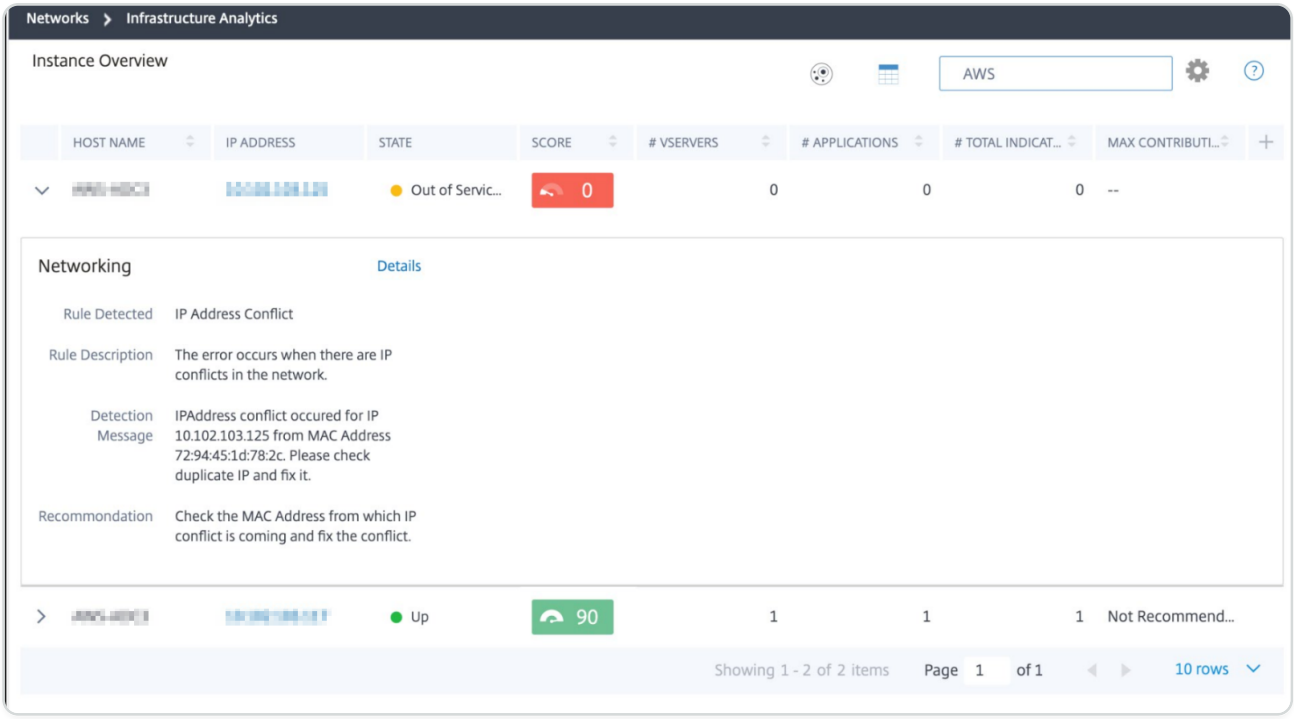
Tabular view

You can also view anomalies using the tabular view option in **Infrastructure Analytics**. Navigate to **Infrastructure > Infrastructure Analytics** and then click

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to display all managed instances. Click

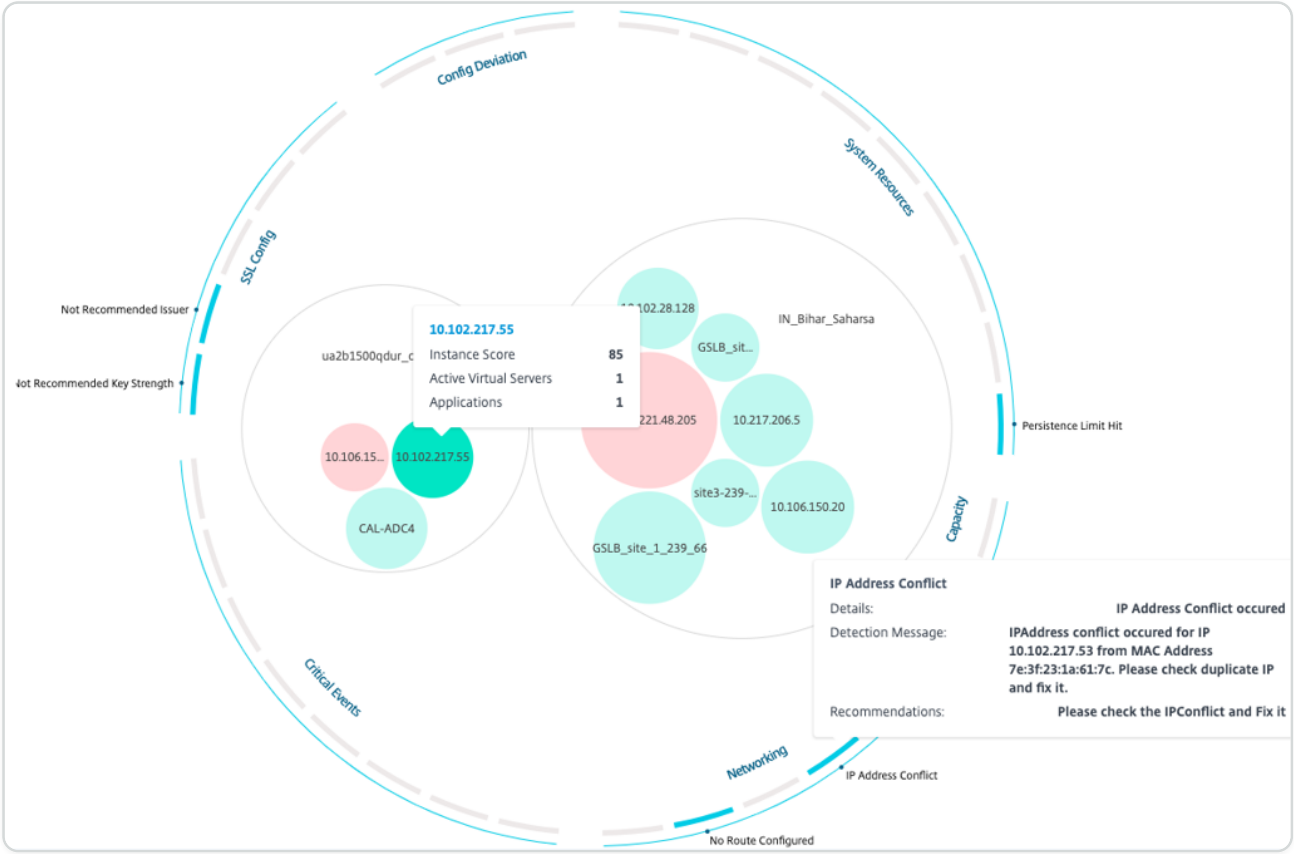
to expand for details.



View details of an anomaly

For example, if you want to view details for **IP address conflict** in the network, click the anomaly that is displayed for IP address conflict to view the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Details** - Indicates what anomaly is detected
- **Detection Message** - Indicates the MAC address for which the IP address has the conflict
- **Recommendations** - Indicates the action item to resolve this IP address conflict

Instance management

Instances are Citrix Application Delivery Controller™ (ADC) appliances that you can manage, monitor, and troubleshoot using NetScaler Application Delivery Management (ADM). You must add instances to NetScaler ADM to monitor them. Instances can be added when you set up NetScaler ADM or later. After you add instances to NetScaler ADM, they are continuously polled to collect information that can later be used to resolve issues or as reporting data.

Instances can be grouped as a static group or as a private IP-block. A static group of instances can be useful when you want to run specific tasks such as configuration jobs, and so on. A private IP-block groups your instances based on their geographical locations.

Add an instance

You can add instances either while setting up the NetScaler ADM server for the first time or later. To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To learn how to add an instance to NetScaler ADM, see Add Instances to NetScaler ADM.

When you add an instance to the NetScaler ADM server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance. To learn more, see How NetScaler ADM discovers instances.

After you've added an instance, you can delete it by navigating to **Infrastructure > Instances** and click **All Instances**. On the Instances page, select the instance you want to delete and click **Remove**.

How to use the instance dashboard

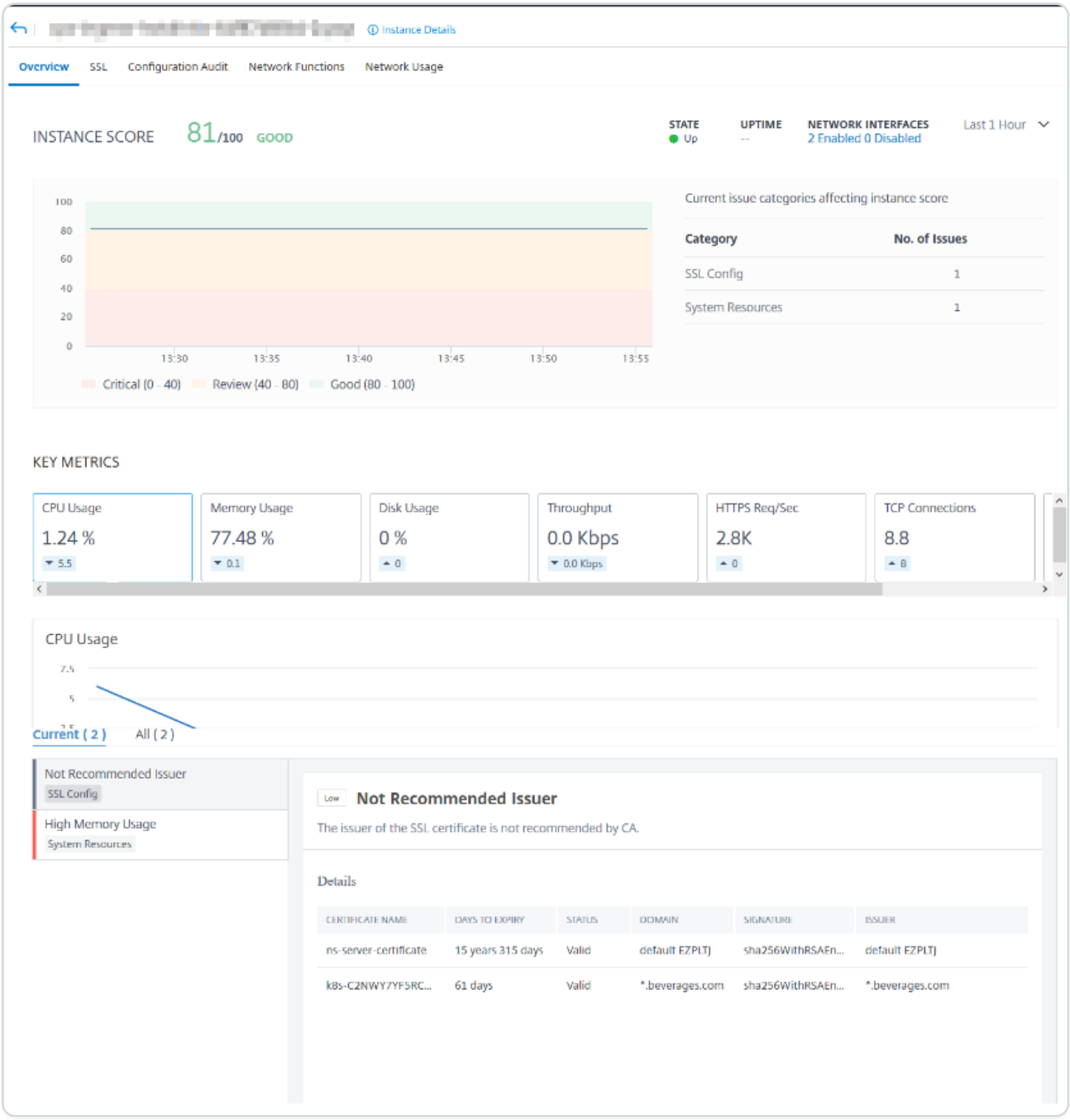
The per-instance dashboard in NetScaler® ADM displays data in a tabular and graphical format for the selected instance. Data collected from your instance during the polling process is displayed on the dashboard.

By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.

To view a specific instance's dashboard, navigate to **Infrastructure > Instances**. From the summary, choose the instance type and then, select the instance you want to view and click **Dashboard**.

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Overview**. The overview tab displays the CPU and memory usage of the chosen instance. You can also view events generated by the instance and the throughput data. Instance-specific information such as the IP address, its hardware and LOM versions, the profile details, serial number, contact person, and so on is also displayed here. By scrolling down further, the licensed features that are available on your chosen instance along with the modes configured on it.

  For more information, see Instance details.

- **SSL dashboard**. You can use the SSL tab on the per-instance dashboard to view or monitor the details of your chosen instance's SSL certificates, SSL virtual servers, and SSL protocols. You can click the "numbers" in the graphs to display further details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Configuration Audit**. You can use the configuration audit tab to view all the configuration changes that have occurred on your chosen instance. The **NetScaler config saved status** and **NetScaler config drift** charts on the dashboard display high-level details about configuration changes in saved against unsaved configurations.
- **Network Functions**. Using the network functions dashboard, you can monitor the state of the entities configured on your selected NetScaler instance. You can view graphs for your virtual servers that display data such as client connections, throughput, and server connections.
- **Network usage**. You can view network performance data for your selected instance on the network usage tab. You can display reports for an hour, a day, a week, or for a month. The timeline slider function can be used to customize the duration of the network reports being generated. By default, only eight reports are displayed, but you can click the “plus” icon at the bottom right-corner of the screen to add additional performance report.

Monitor globally distributed sites

As a network administrator, you might have to monitor and manage network instances deployed across geographical locations. However, it is not easy to gauge the requirements of the network when managing network instances in geographically distributed data centers.

Geomaps in NetScaler® Application Delivery Management (ADM) provides you with a graphical representation of your sites and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

The following section explains how you can monitor data centers in NetScaler ADM.

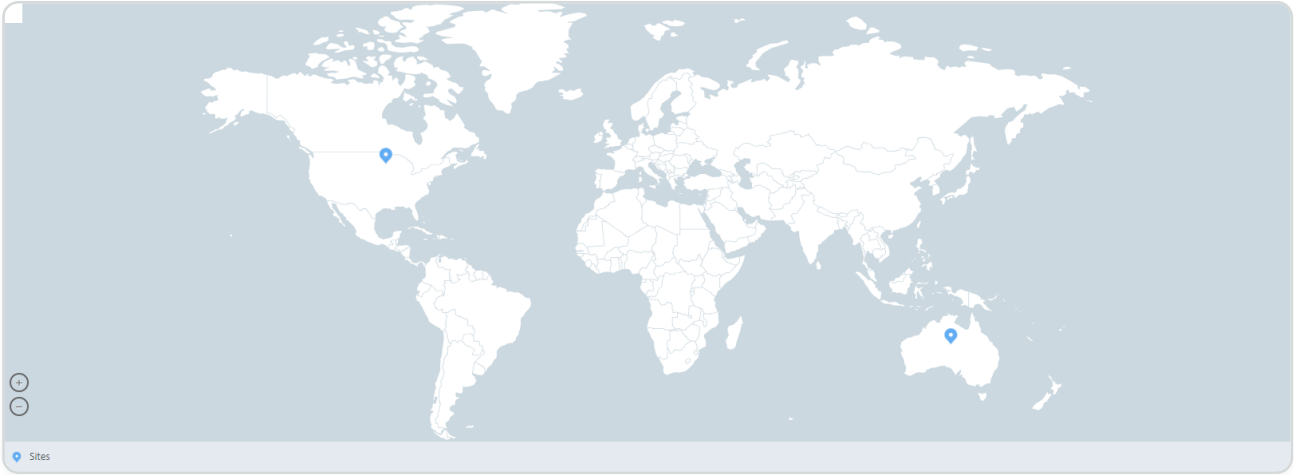
NetScaler ADM site is a logical grouping of Citrix Application Delivery Controller (ADC) instances in a specific geographical location. For example, while one site is assigned to Amazon Web Services (AWS) and another site might be assigned to Azure. Still another site is hosted on the premises of the tenant. NetScaler ADM manages and monitors all NetScaler instances connected to all sites. You can use NetScaler ADM to monitor and collect syslog, AppFlow, SNMP, and any such data originating from the managed instances.

Geomaps in NetScaler ADM provides you with a graphical representation of your sites. Geomaps also breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor all network issues. You can navigate to **Infrastructure > Instances** page for a visual representation of the sites created on the world map.

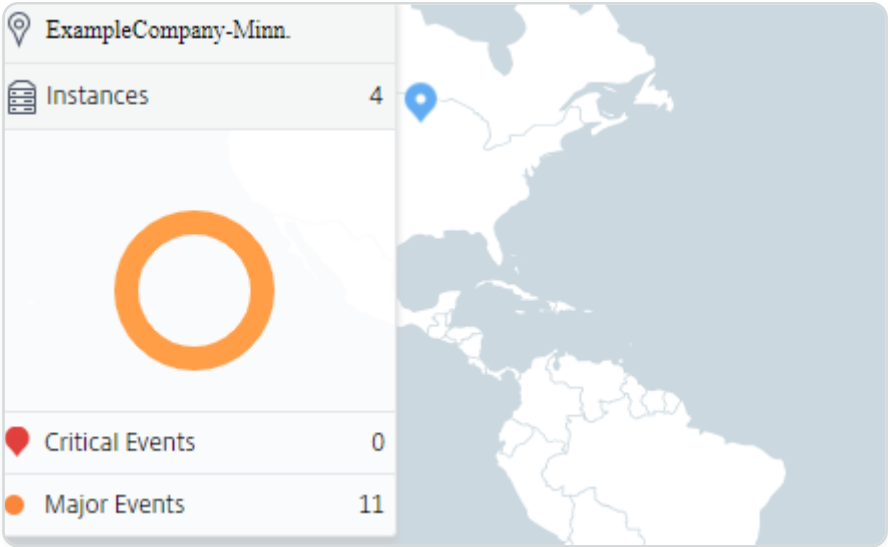
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use case

A leading mobile carrier company, ExampleCompany, was relying on private service providers for hosting their resources and applications. The company already had two sites - one at Minneapolis in the United States and another in Alice Springs in Australia. In this image, you can see that two markers represent the two existing sites.



The markers also display a number, which shows the number of applications in each site. You can click these markers for more information about each site.

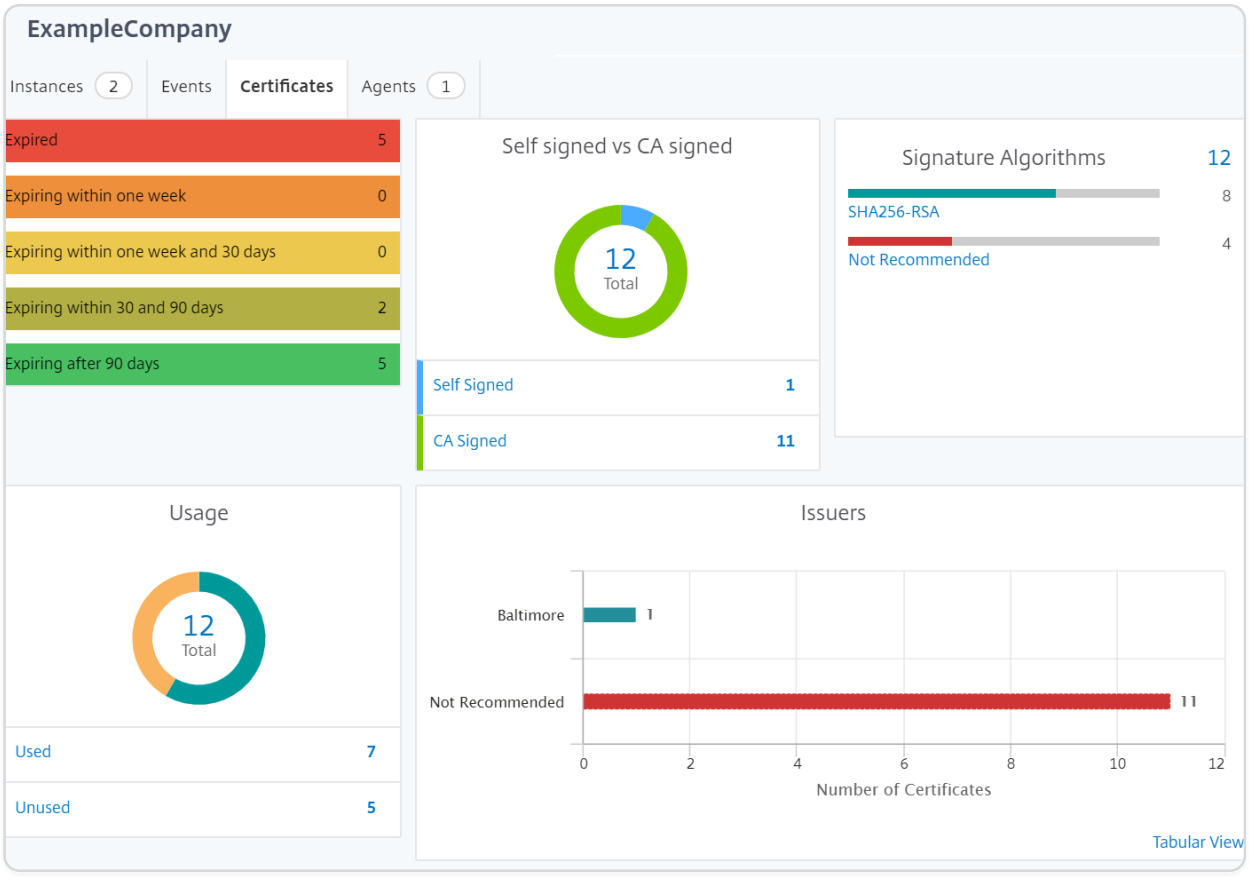


Click the tabs to view more information:

- **Instances** tab: View the following in this tab:
  - IP address of each network instance
  - Type of the instance
  - Number of critical events on them
  - Significant events and all events raised on a NetScaler instance.
- **Events** tab: View a list of critical and significant events raised on the instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Certificates** tab: View the following in this tab:
  - List of certificates of all the instances
  - Expiration status
  - Vital information and the top 10 instances by many certificates in use.
- **Agents** tab: View a list of agents to which the instances are bound.



Configuring Geomaps

ExampleCompany decided to create a third site in Bangalore, India. The company wanted to test the cloud by offloading some of their less-critical, internal IT applications to the Bangalore office. The company decided to use the AWS cloud computing services.

As an administrator, you must first create a site, and next add the NetScaler instances in NetScaler ADM. You must also add the instance to the site, add an agent, and bind the agent to the site. NetScaler ADM then recognizes the site that the NetScaler instance and the agent belong.

For more information on adding NetScaler instances, see Adding Instances.

To create sites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create sites before you add instances in NetScaler ADM. Providing location information allows you to locate the site precisely.

Navigate to **Infrastucture > Instances > Sites**, and then click **Add**.

1. In the **Create Site** page, specify the following information:

   a. **Site Type**: Select **Data Center**.

   > **NOTE**
   >
   > The site can function as the primary data center or as a branch. Choose accordingly.

   b. **Type**: Select AWS as the cloud provider from the list.

   > **NOTE**
   >
   > Check the **Use existing VPC as a site** box accordingly.

   c. **Site Name**: Type the name of the site.

   d. **City**: Type the city.

   e. **Zip Code**: Type the Zip Code.

   f. **Region**: Type the Region.

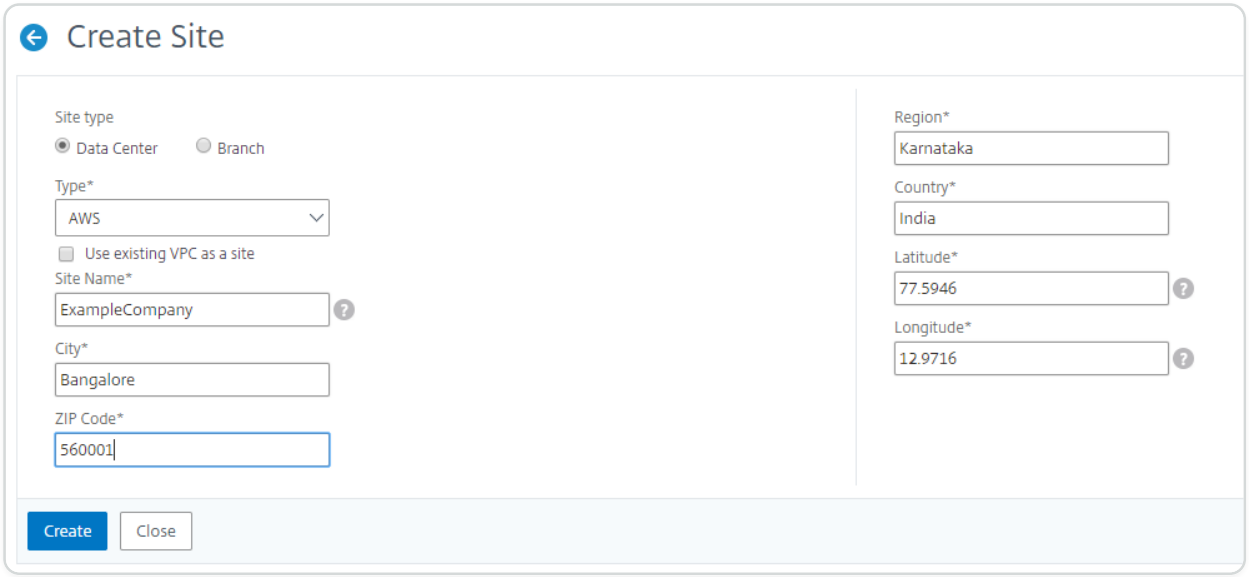
   g. **Country**: Type the Country

   h. **Latitude**: Type the latitude of the location.

   i. **Longitude**: Type the longitude of the location.

2. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



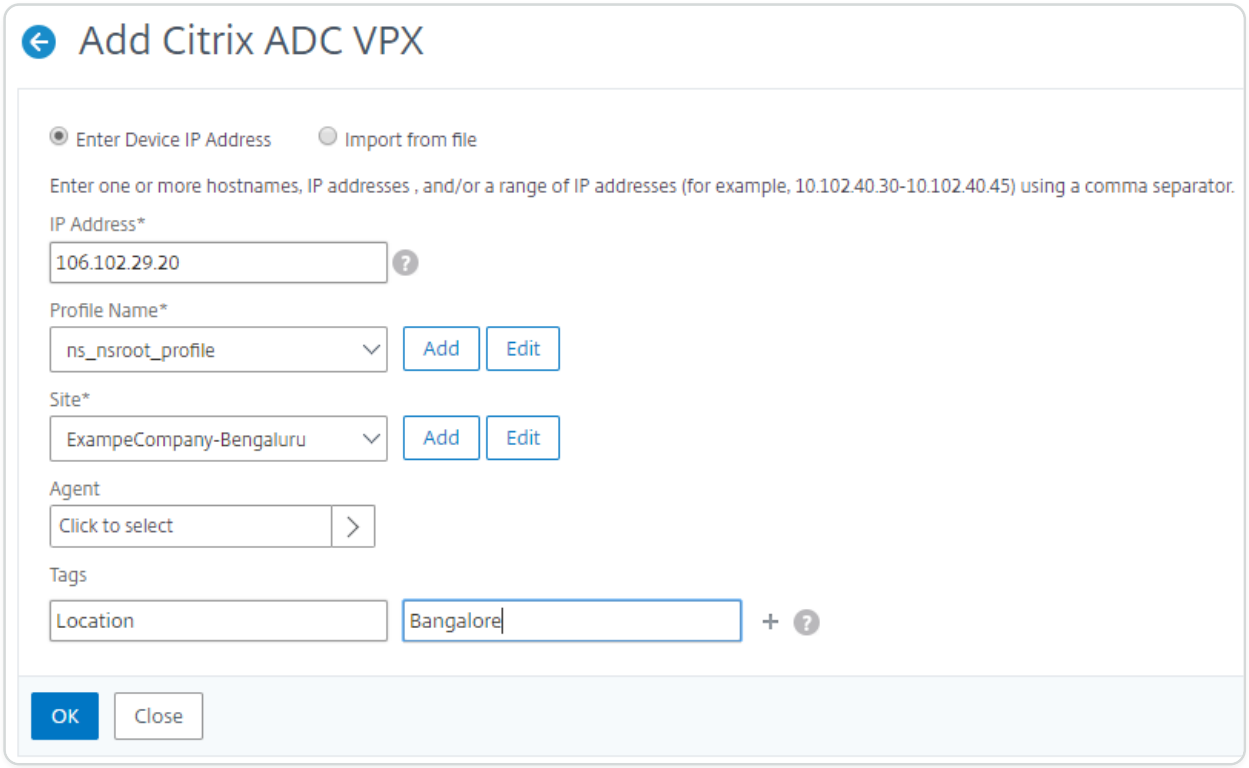
To add instances and select sites:

After creating sites, you must add instances in NetScaler ADM. You can select the previously created site, or you can also create a site and associate the instance.

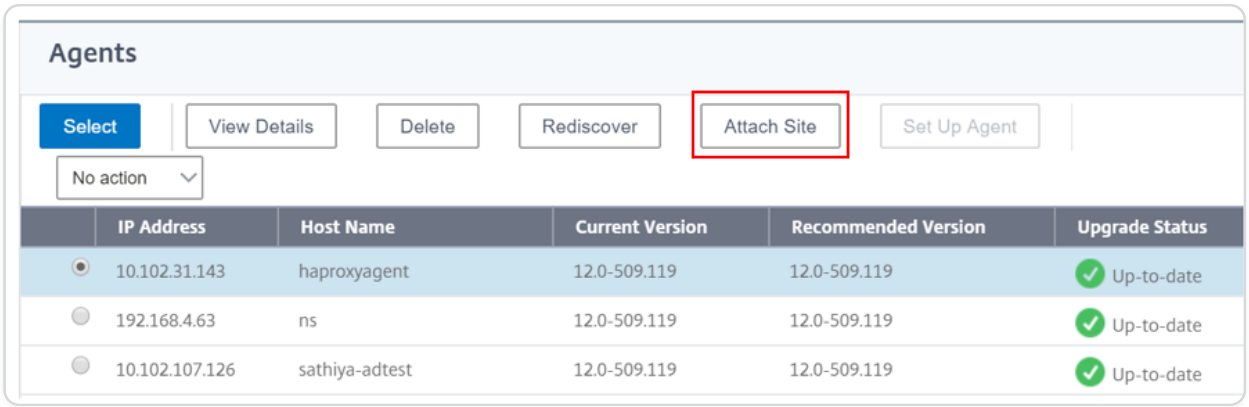
After creating sites, you must add instances in NetScaler ADM. You can select the previously created site, or you can also create a site and associate the instance.

1. In NetScaler ADM, navigate to **Infrastructure > Instances**.
2. Select the type of instance you want to create, and click **Add**.
3. On the **Add NetScaler VPX** page, type the IP address and select the profile from the list.
4. Select the site from the list. You can click the + sign next to **Site** field to create a site or click the edit icon to change the details of the default site.
5. Click the right arrow and select the agent from the list that displays.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. After choosing the agent, you must associate the agent with the site. This step allows the agent to be bound to the site. Select the agent and click **Attach Site**.



1. Select the site from the list and click **Save**.

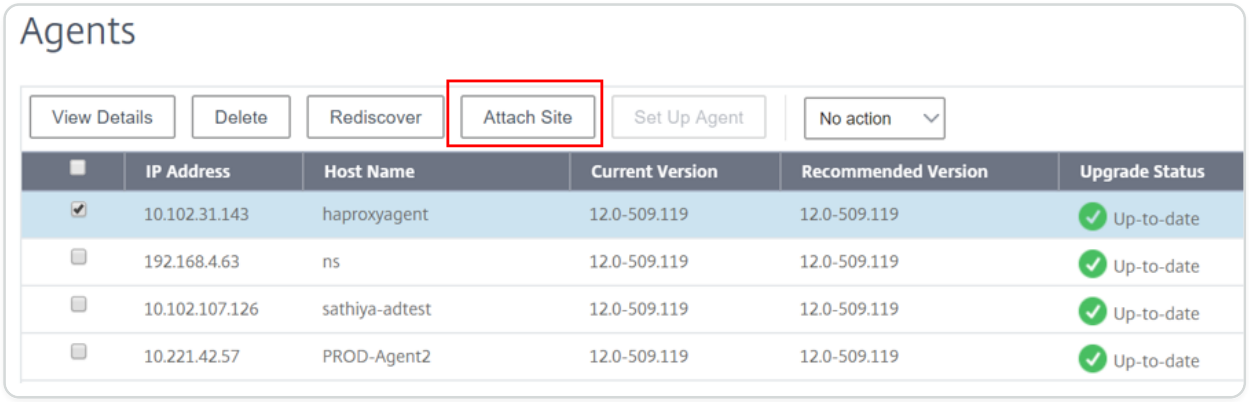
1. Click **OK**.

You can also attach an agent to a site by navigating to **Infrastructure > Instances > Agents**.

To associate a NetScaler agent with the site:

1. In NetScaler ADM, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent, and click **Attach Site**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. You can associate the site and click **Save**.

NetScaler ADM starts monitoring the NetScaler instances added in Bangalore site along with the instances at the other two sites as well.

How to create tags and assign to instances

NetScaler Application Delivery Management (ADM) now allows you to associate your Citrix Application Delivery Controller™ (ADC) instances with tags. A tag is a keyword or a one-word term that you can assign to an instance. The tags add some additional information about the instance. The tags can be thought of as metadata that helps describe an instance. Tags allow you to classify and search for instances based on these specific keywords. You can also assign multiple tags to a single instance.

The following use cases help you to understand how tagging of instances helps you to better monitor them.

- **Use case 1**: You can create a tag to identify all instances in the United Kingdom. Here, you can create a tag with the key as "Country" and the value as "UK." This tag helps you to search and monitor all those instances in the UK.
- **Use case 2**: You want to search for instances that are in the staging environment. Here, you can create a tag with the key as "Purpose" and the value as "Staging_NS." This tag helps you to segregate all instances that are being used in the staging environment from the instances that have client requests running through them.
- **Use case 3**: Consider a situation where you want to find out the list of NetScaler instances that are in "Swindon" area in the UK and owned by you, David T. You can create tags for all these requirements and assign that to all the instances that satisfy these conditions.

To assign tags to NetScaler VPX instance:

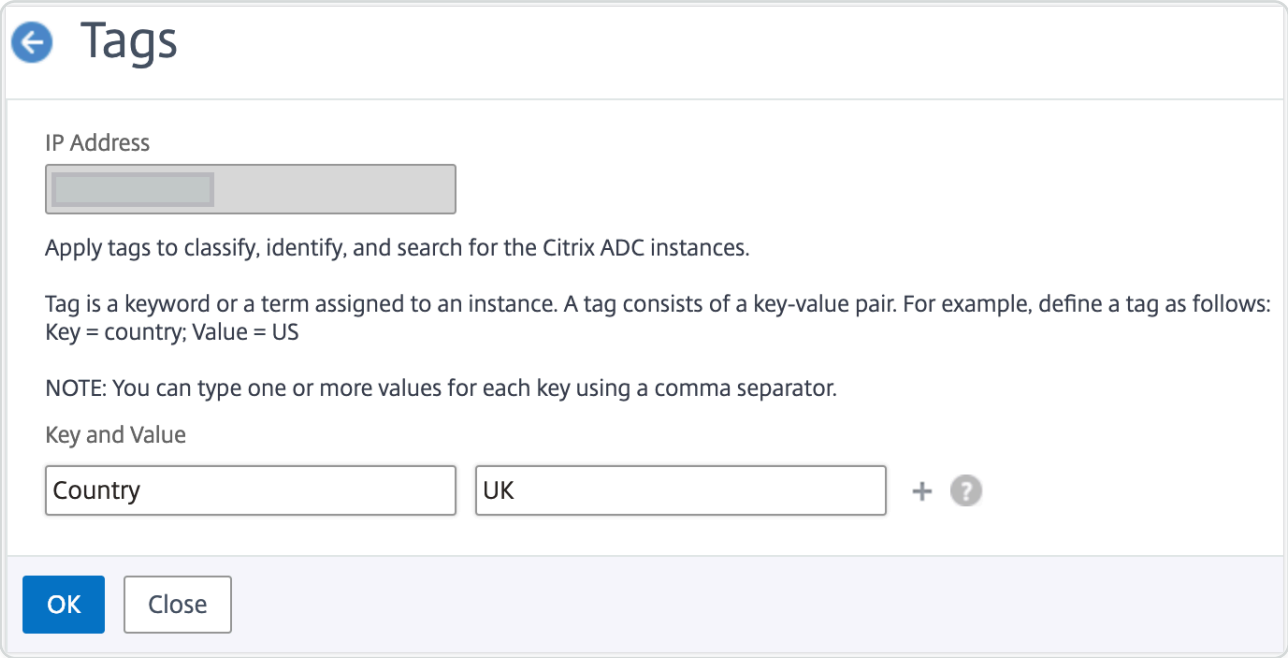
1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler**.

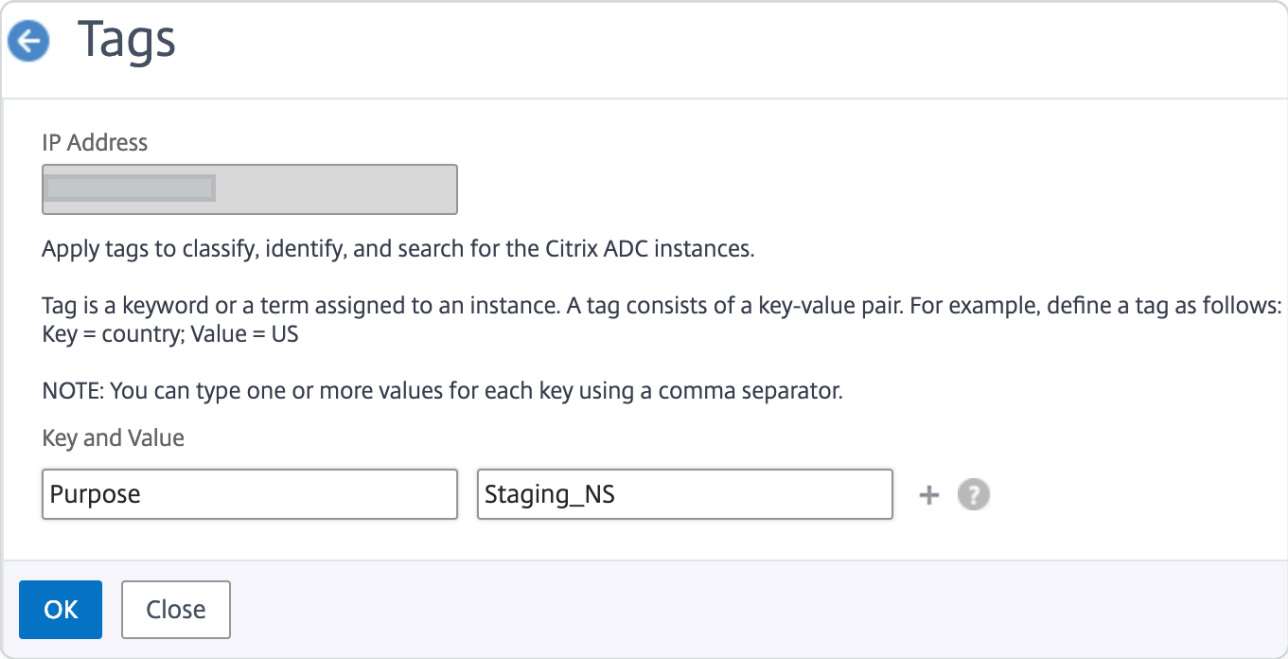
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the **NetScaler VPX** tab.
3. Select the required NetScaler VPX.
4. Click **Tags**.
5. Create tags and click **OK**.

The **Tags** window that appears allows you to create your own "key-value" pairs by assigning values to every keyword that you create.

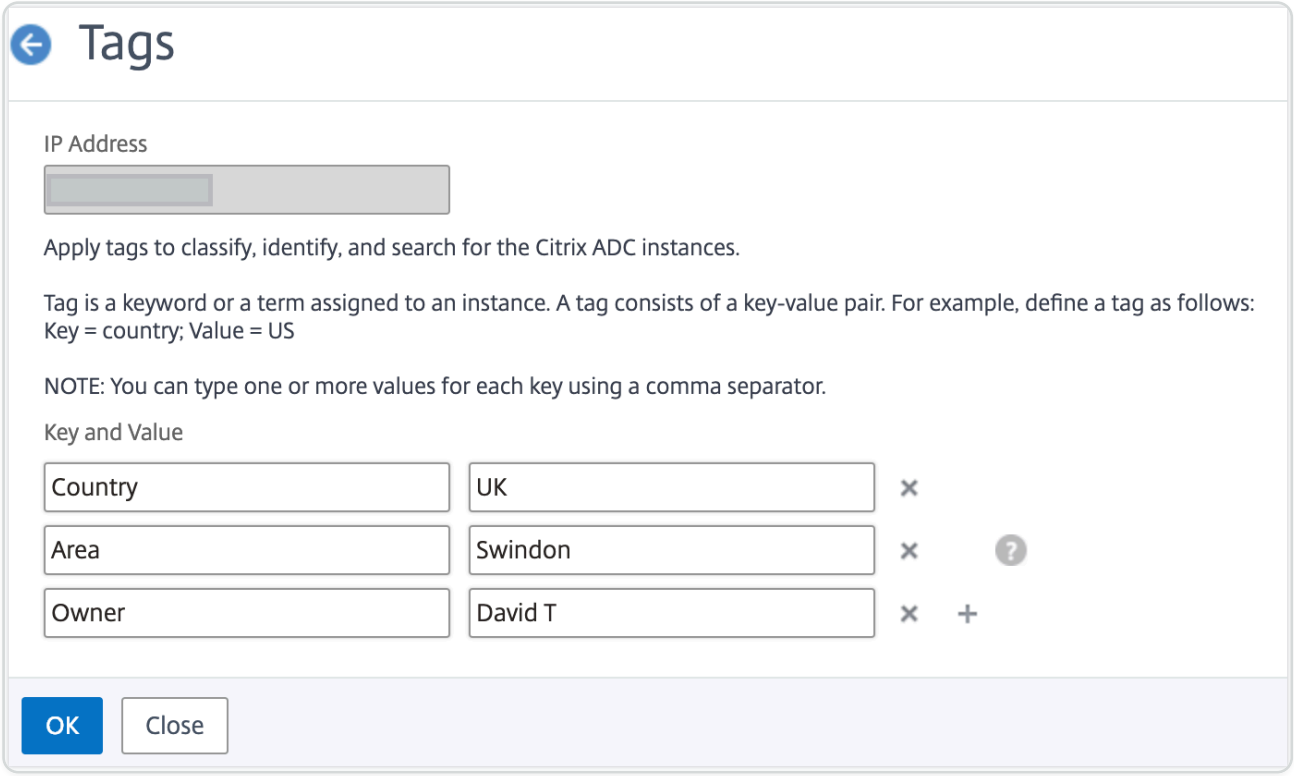
For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.





© 1997–2026 Citrix Systems, Inc. All rights reserved.

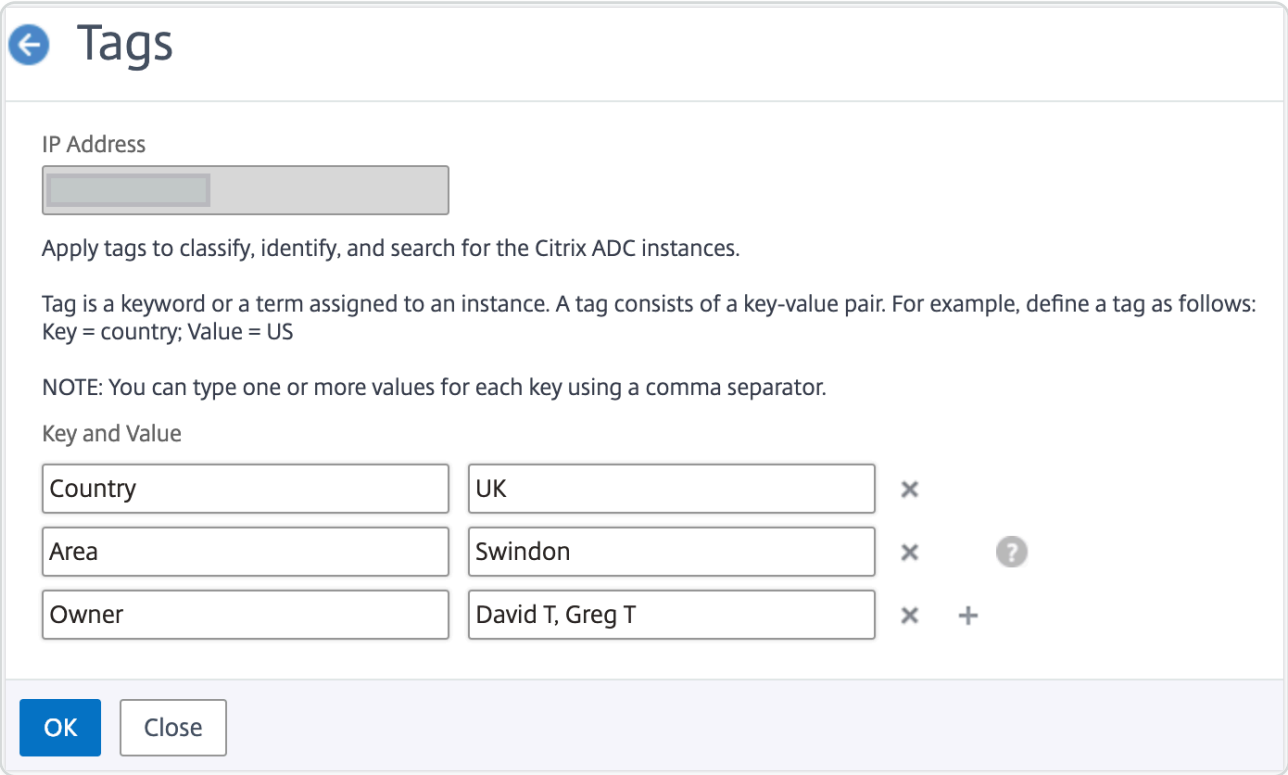
You can also add multiple tags by clicking "+." Adding multiple and meaningful tags allows you to efficiently search for the instances.



You can add multiple values to a keyword by separating them with commas.

For example, you are assigning admin role to another coworker, Greg T. You can add his name separated by a comma. Adding multiple names helps you to search by either of the names or by both names. NetScaler® ADM recognizes the comma separated values into two different values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

There might be a situation where NetScaler Application Delivery Management (ADM) is managing many NetScaler instances. As an admin, you might want the flexibility to search on the instance inventory based on certain parameters. NetScaler ADM now offers improved search capability to search a subset of NetScaler instances based on the parameters that you define in the search field. You can search for the instances based on two criteria - tags and properties.

- **Tags**. Tags are terms or keywords that you can assign to a NetScaler instance to add some additional description about the NetScaler instance. You can now associate your NetScaler instances with tags. These tags can be used to better identify and search on the NetScaler instances.
- **Properties**. Each NetScaler instance added in NetScaler ADM has a few default parameters or properties associated with that instance. For example, each instance has its own host name, IP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

address, version, host ID, hardware model ID and so on. You can search for instances by specifying values for any of these properties.

For example, consider a situation where you want to find out the list of NetScaler instances that are on version 12.0 and are in the UP state. Here, the version and the state of the instance are defined by the default properties.

Along with the 12.0 version and UP state of the instances, you can also search those instances owned by you. You can create an "Owner" tag and assign a value "David T" to that tag. For more information on how to create and assign tags, see How to create tags and assign to instances.

You can use a combination of tags and properties to create your own search criteria.

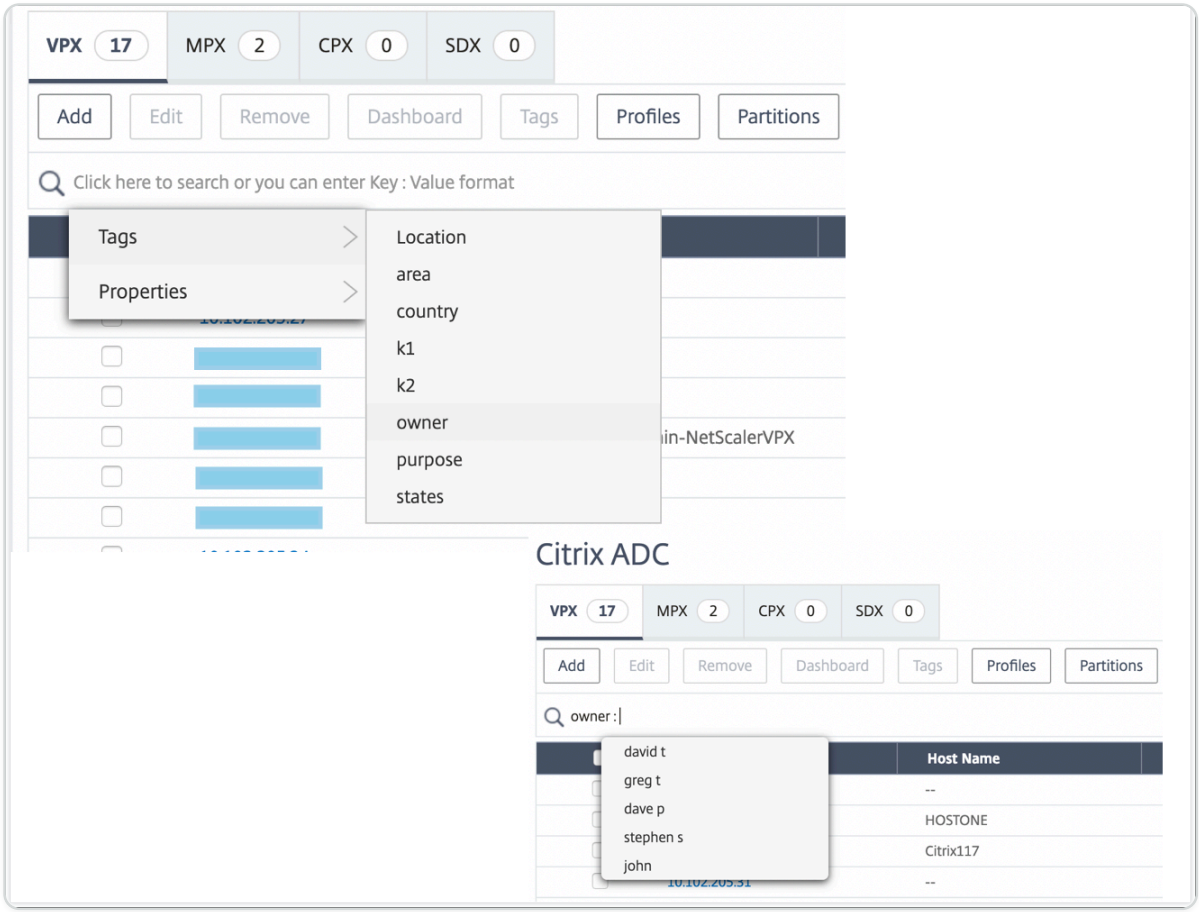
To search for NetScaler VPX instances

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. Click the search field. You can create a search expression by using Tags or Properties or by combining both.

   The following examples show how you can use the search expression efficiently to search for the instance.

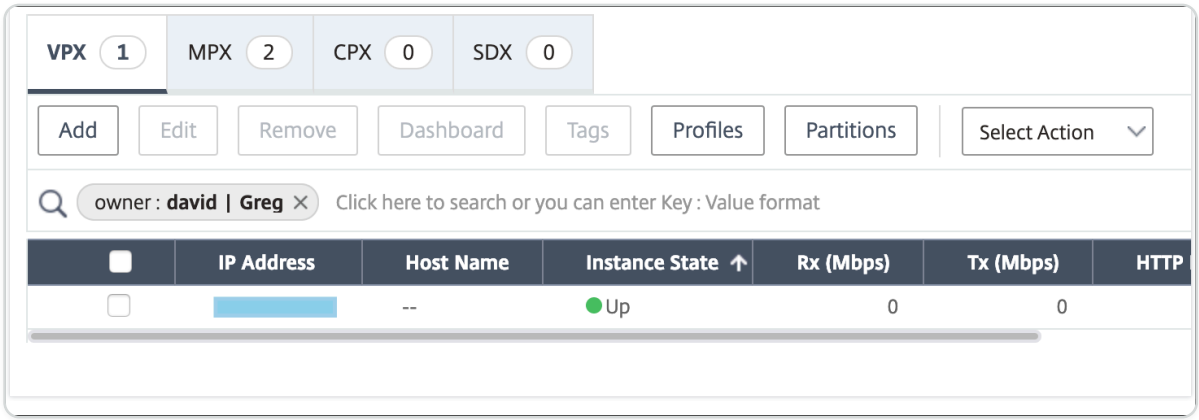
   a. Select **Tags** option and select **Owner**. Select "David T."

© 1997–2026 Citrix Systems, Inc. All rights reserved.



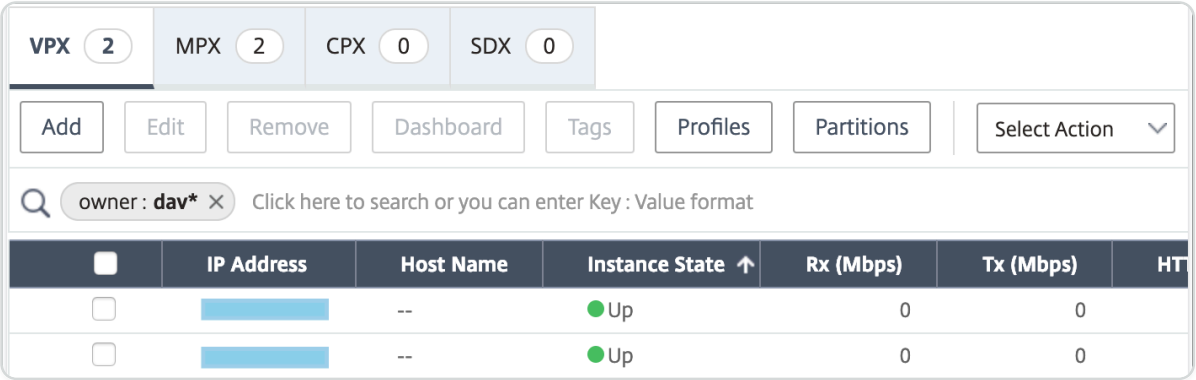
NetScaler® ADM supports regular expressions and wildcard characters in the search expressions.

b. You can use regular expressions to further expand the search criteria. For example, you want to search instances owned by either David or Stephen. In such a case, you can type the values by separating the values with a "\|" expression.



c. You can also use wildcard characters to replace or represent one or more characters. For example, you can type `Dav*` to search for all instances owned by David T and Dave P.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

For more information on regular expressions and wildcard characters and how to use them, click the "information" icon in the search bar.

Manage admin partitions of NetScaler instances

You can configure admin partitions on your Citrix Application Delivery Controller (ADC) instances so that different groups in your organization are assigned different partitions on the same NetScaler instance. A network administrator can be assigned to manage multiple partitions on multiple NetScaler instances.

NetScaler® Application Delivery Management (ADM) provides a seamless way of managing all partitions owned by an administrator from a single console. You can manage these partitions without disrupting other partition configurations.

To allow multiple users to manage different admin partitions, you have to create groups and then, assign users and partitions to those groups. Each user can view and manage only the partitions in the group to which the user belongs. Each admin partition is considered as an instance in NetScaler ADM. When you discover a NetScaler instance, the admin partitions configured on that NetScaler instance get added to the system automatically.

Consider that you have two NetScaler VPX instances with two partitions configured on each instance. For example, NetScaler instance 10.102.216.49 has Partition_1, Partition_2, and Partition_3, and NetScaler instance 10.102.29.120 has p1 and p2 as shown in the following image.

To view the partitions, navigate to **Infrastructure > Instances > NetScaler > VPX**, and then click **Partitions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can assign user-p1 the following partitions: 10.102.29.120-p1 and 10.102.216.49-Partition_1. And, you can assign user-p2 to manage partitions 10.102.29.80-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3.

Then , you have to create the two users, user-p1 and user-p2, and you have to assign the users to the groups that you created for them.

First, you have to create two groups with appropriate permissions (example: admin permissions) and include the required admin partition instances in each group. For example, create system group partition1-admin and add NetScaler admin partitions 10.102.29.120-p1 and 10.102.216.49-Partition_1 to this group. Also create system group partition2-admin and add NetScaler admin partitions 10.102.29.120-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3 and to this group.

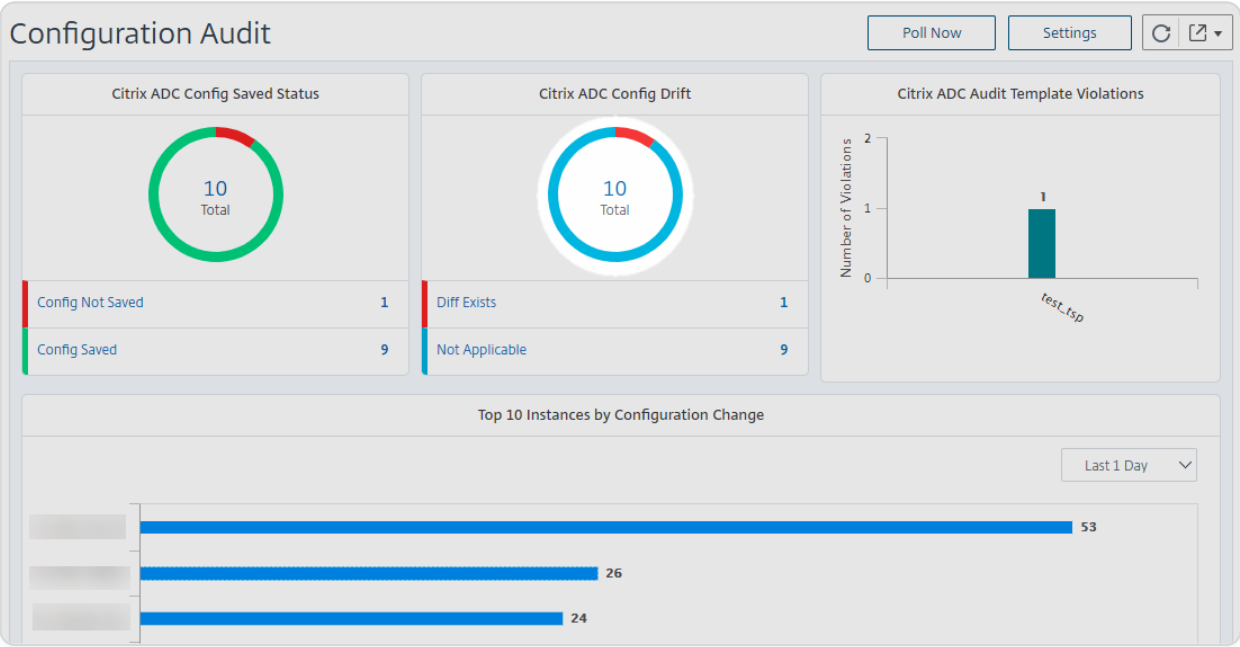
After you have created the admin partition, you can also use the revision history difference feature and the audit template for admin partition feature for auditing purposes

Revision history difference for admin partition allows you to view the difference between the five latest configuration files for a partitioned NetScaler instance. You can compare the configurations files against each other (example Configuration Revision - 1 with Configuration Revision -2) or against the current running/saved configuration with Configuration Revision. Along with the differences in configuration, the correction configurations are also shown. You can export all the corrective commands to your local folder and correct the configurations.

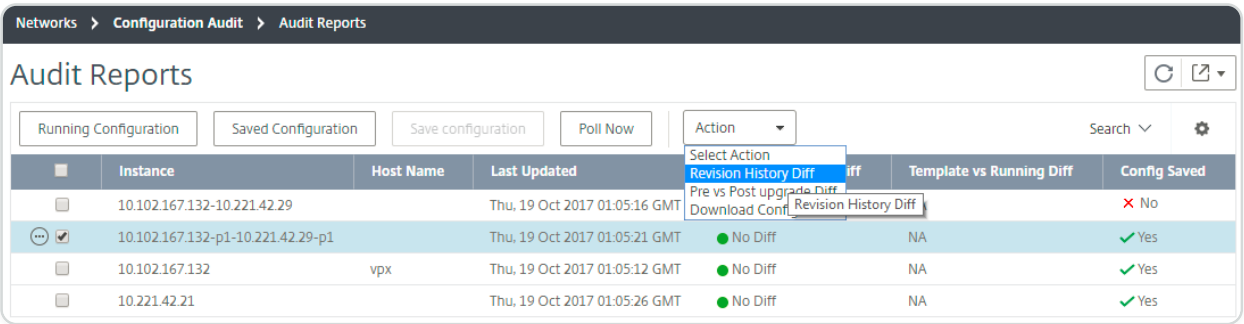
To view the revision history difference:

1. Navigate to **Infrastructure > Configuration Audit.** Click inside the donut chart that represents the instance config status. In the **Audit Reports** page that opens, click the partitioned NetScaler instance.

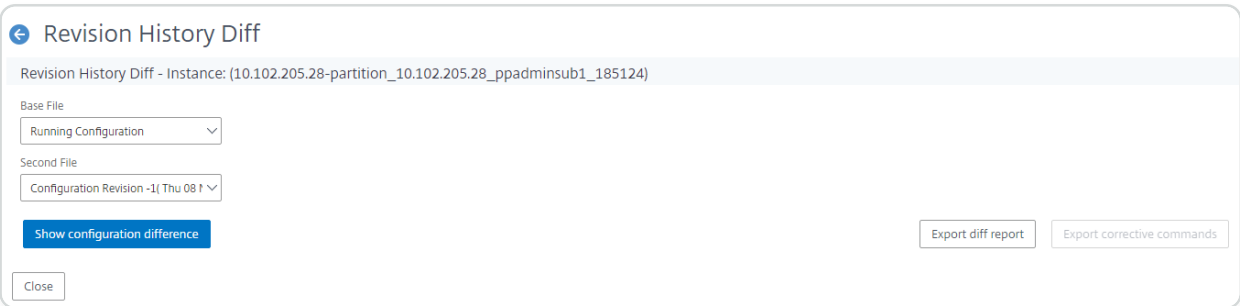
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. From the **Action** menu, click **Revision History Diff.**

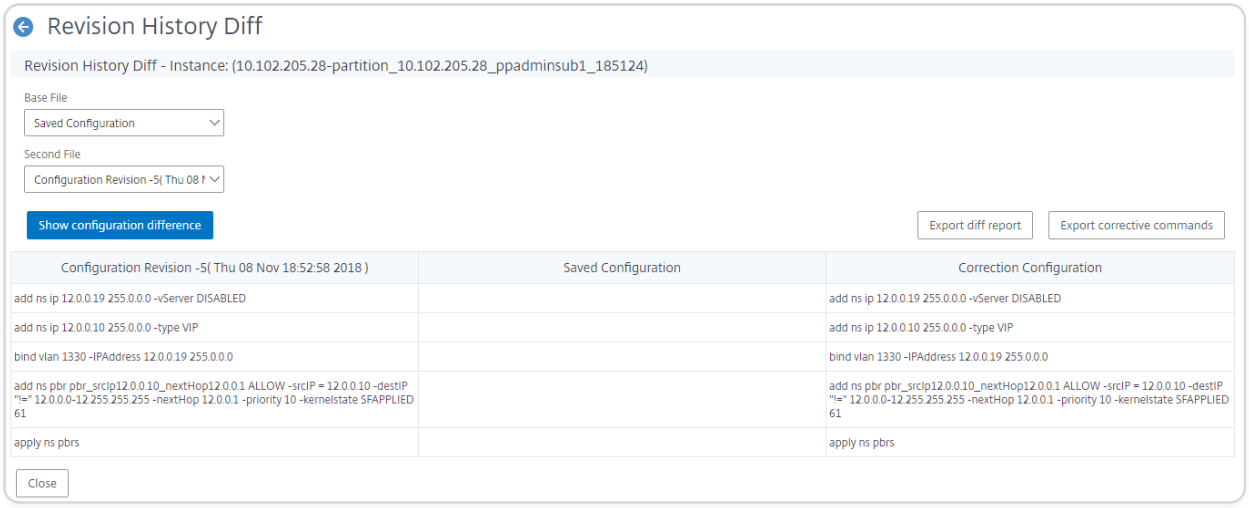


3. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision -1 and then, click **Show configuration difference**.



4. You can then view the difference between the five latest configuration files for the selected partitioned NetScaler instance as shown below. You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be run on the base file in order to get the configuration to the desired state (configuration file that is being used for comparison).

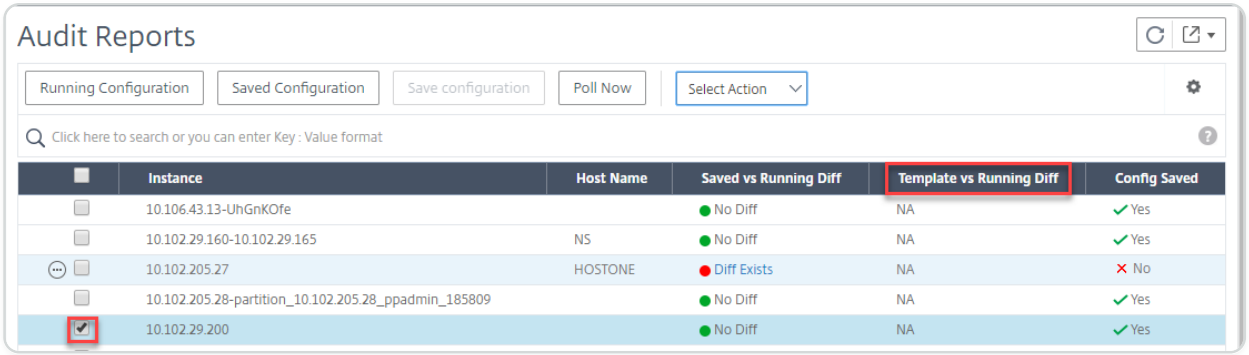
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Audit templates for partition allow you to create a custom configuration template and associate it with a partition instance. Any variation in the running configuration of the instance with the audit template is shown in the **Template vs Running diff** column of the **Audit Reports** page. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

To view the template vs running difference:

1. From the **Audit Reports** page, click the partitioned NetScaler instance.



2. If there is any difference between the audit template and the running difference, the difference is shown as a hyperlink. Click the hyperlink to view the differences if there is any. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

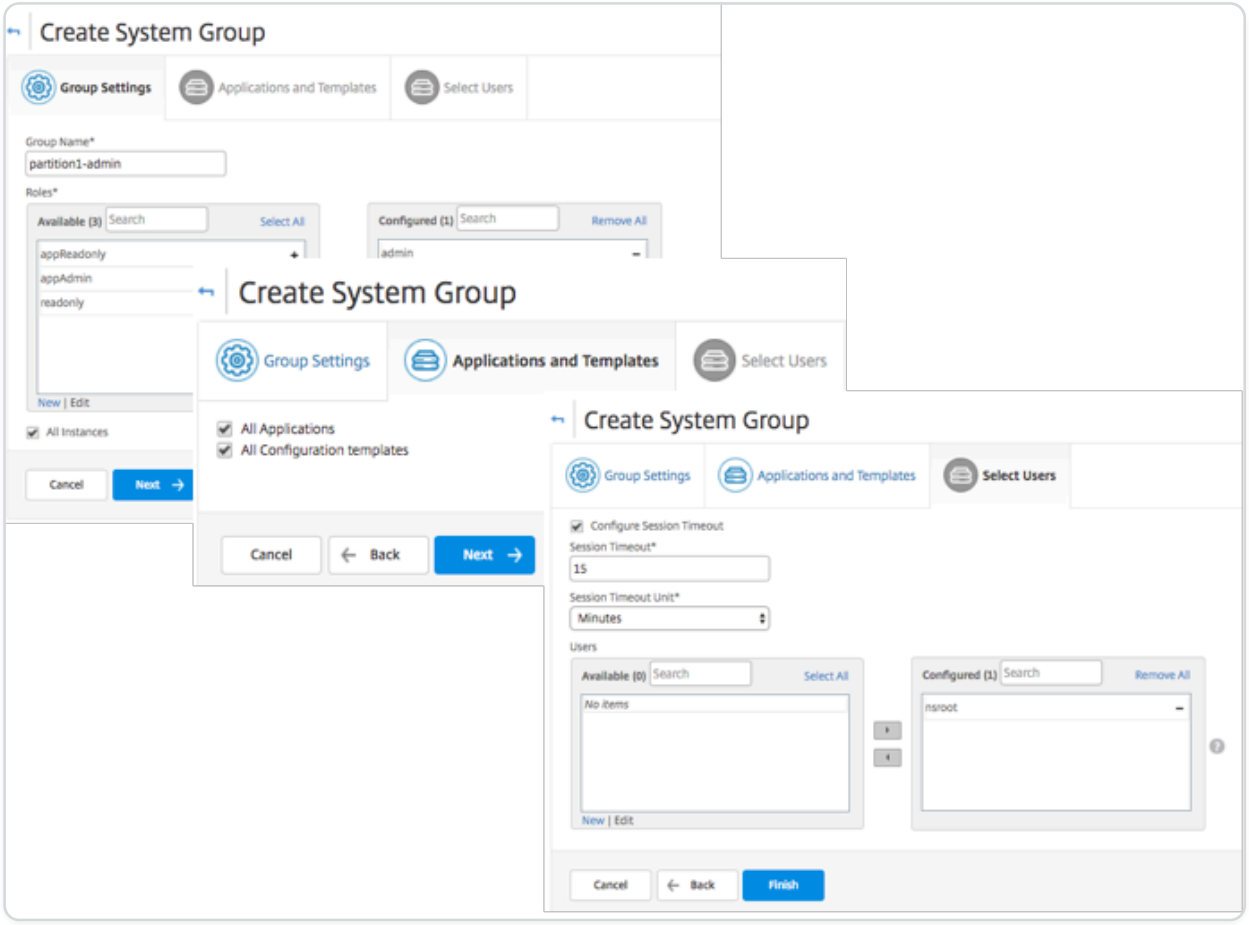
To create groups:

1. Navigate to **Settings > User Administration > Groups**, and then click **Add**.
2. In the **Create System User** page, specify the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Group Settings** tab: Enter the group name and role permissions. To allow access to specific instances, clear the **All Instances** check box, and then choose your instances on the **Select Instances** page.
- **Applications and Templates** tab: You can choose to use this group across all applications and configuration templates.
- **Select Users** tab: Select users that you'd like to add to this group. You can click the **New** link in the **Available** table to create new users. Optionally, configure the session timeout, where you can configure the time period for how long a user can remain active.

3. Click **Finish**.



To create users:

1. Navigate to **Settings > User Administration > Users**, and then click **Add**.
2. On the **Create System User** page, specify the user name and password. Optionally, you can enable external authentication and configure the session timeout.
3. Assign the user to a group by adding the group name from the **Available** list to the **Configured** list.
4. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Now log out and log on with user-p1 credentials. You can view and manage only the admin partitions assigned to you to manage and monitor.

Create a NetScaler high-availability pair

A NetScaler high-availability (HA) pair can provide an uninterrupted operation during downtime or network failures. You can create a HA pair of ADC instances using NetScaler ADM. For more information, see NetScaler high-availability.

Perform the following steps to create a HA pair of ADC instances in NetScaler® ADM:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select an ADC instance from the list with which you want to create a HA pair.

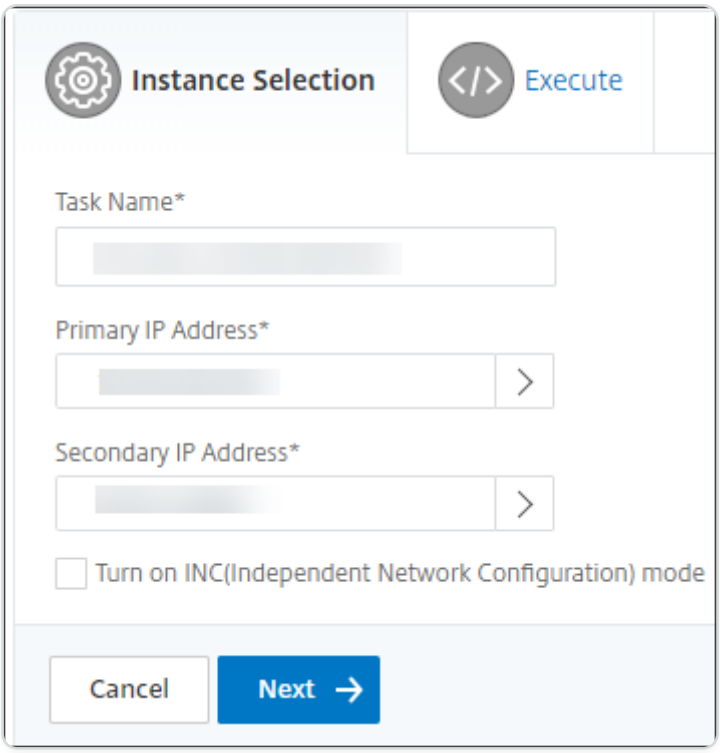
   The selected instance becomes a primary instance in the HA pair.
3. Click Select **Action > Create HA Pair**.
4. In **Instance Selection**, perform the following steps:

   a. In **Secondary IP Address**, click to select a secondary instance.

   b. Select an ADC instance that you want to configure as secondary in the HA pair.

   c. Optional, select **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.

   d. Click **Next**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In **Execute**, you can decide to create a HA pair now or later.

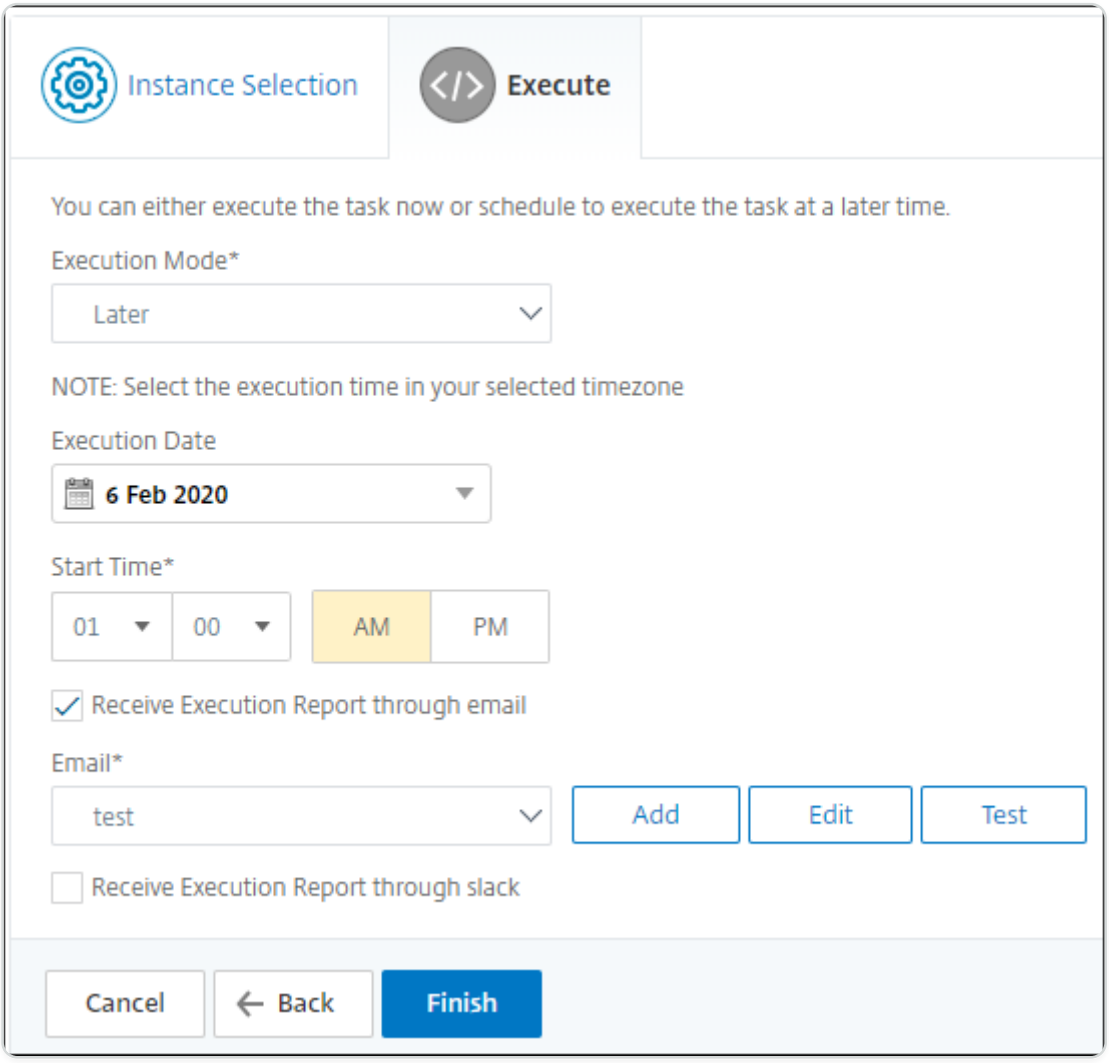
   a. In **Execution Mode**, select one of the following execution modes:

      - **Now** - Select this option to create a HA pair now.
      - **Later** - Select this option to create a HA pair on specific date and time.

   b. If you have selected **Later** in the **Execution Mode** list, select **Execution Date** and **Start Time** when you want to run this task.

      NOTE

      The execution time is displayed in the timezone set in NetScaler ADM.



You can receive an execution report of this task through the following:

- **Email** - Select the email distribution from the list.

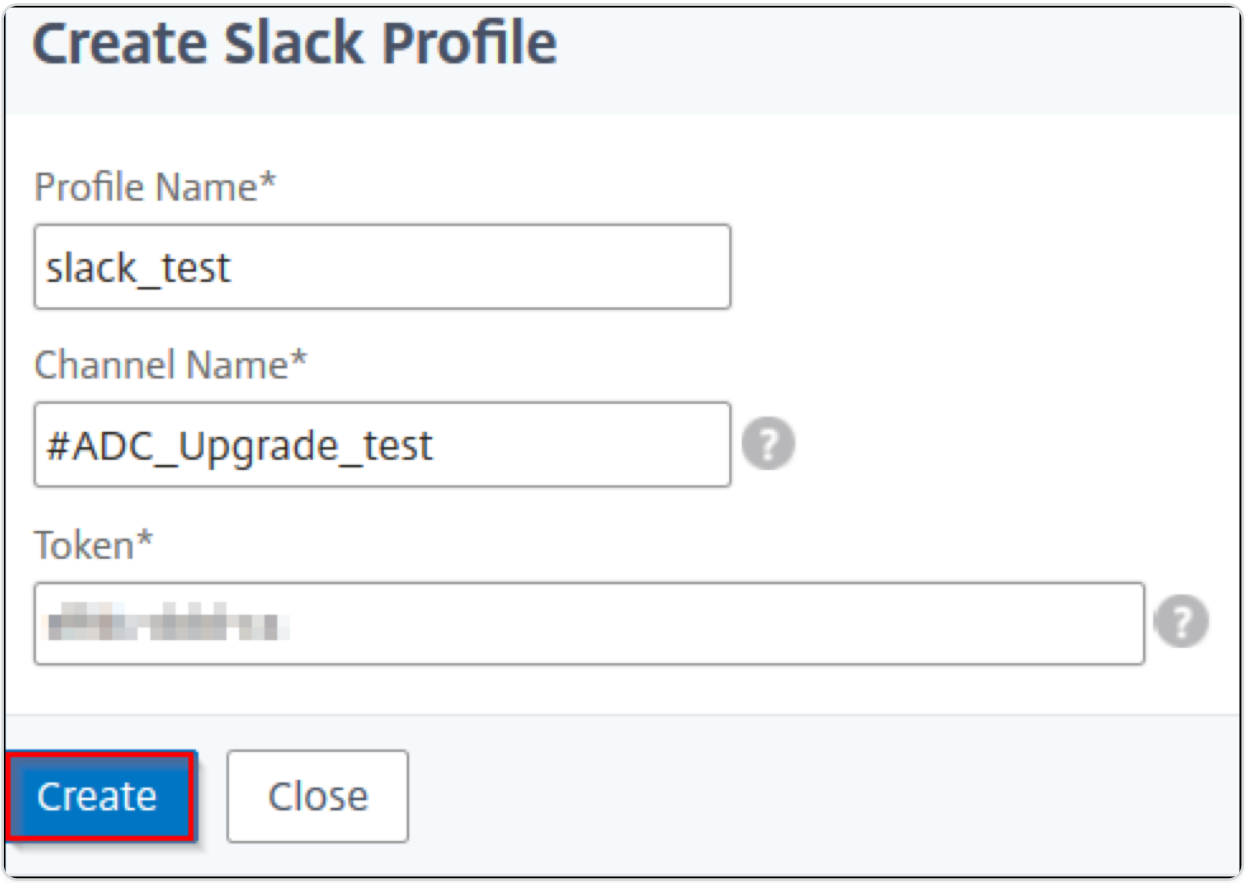
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add a distribution list, click **Add**. Specify the required parameters to add the distribution list and click **Create**.

- **Slack** - Select the Slack profile from the list.

  To add a Slack profile, click **Add**. Specify **Profile Name**, **Channel Name**, and **Token** and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Back up and restore NetScaler instances

You can back up the current state of a NetScaler instance and later use the backed-up files to restore it to the same state. Always back up an instance before you upgrade it or for precautionary reasons. A backup of a stable system enables you to restore it back to a stable point if it becomes unstable.

There are multiple ways to perform backups and restores on a NetScaler instance. You can manually backup and restore NetScaler configurations using the GUI and CLI. You can also use NetScaler ADM to perform automatic backups and manual restores.

NetScaler ADM backs up the current state of your managed NetScaler instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

NetScaler ADM creates a complete backup and restores the following NetScaler instance types:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Backup and restore an ADC instance.

NOTE

- Ensure that the NetScaler® ADM profile has the admin access to backup and restore ADC instances.
- From NetScaler ADM, you cannot perform the backup and restore operation on a NetScaler cluster.
- You cannot use the backup file taken from one instance to restore a different instance.

The backed-up files are stored as a compressed TAR file in the following directory:

```
/var/mps/tenants/root/device_backup/
```

To avoid issues due to non-availability of disk space, you can save a maximum of 50 backup files per ADC instance in this directory.

To back up and restore NetScaler instances, you must first configure the backup settings on NetScaler ADM. After configuring the settings, you can select a single NetScaler instance or multiple instances and create a backup of the configuration files in these instances. If necessary, you can also restore the NetScaler instances by using these backed-up files.

Configure instance backup settings

The **Instance Backup Settings** page allows you to configure settings on NetScaler ADM to back up a selected NetScaler instance or multiple instances:

1. In NetScaler ADM, navigate to **Settings** \> **Administration**.
2. In **Backup**, select **Configure System and Instance backup**.
3. Select **Instance** and specify the following:
   - **Enable Instance Backups**: By default, NetScaler ADM is enabled for taking backups of NetScaler instances. Clear this option if you do not want to create backup files for the instances.
   - **Password Protect File**: (optional) Select the password protect option to encrypt the backup file. Encrypting the backup file ensures that all the sensitive information inside the backup file is secure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

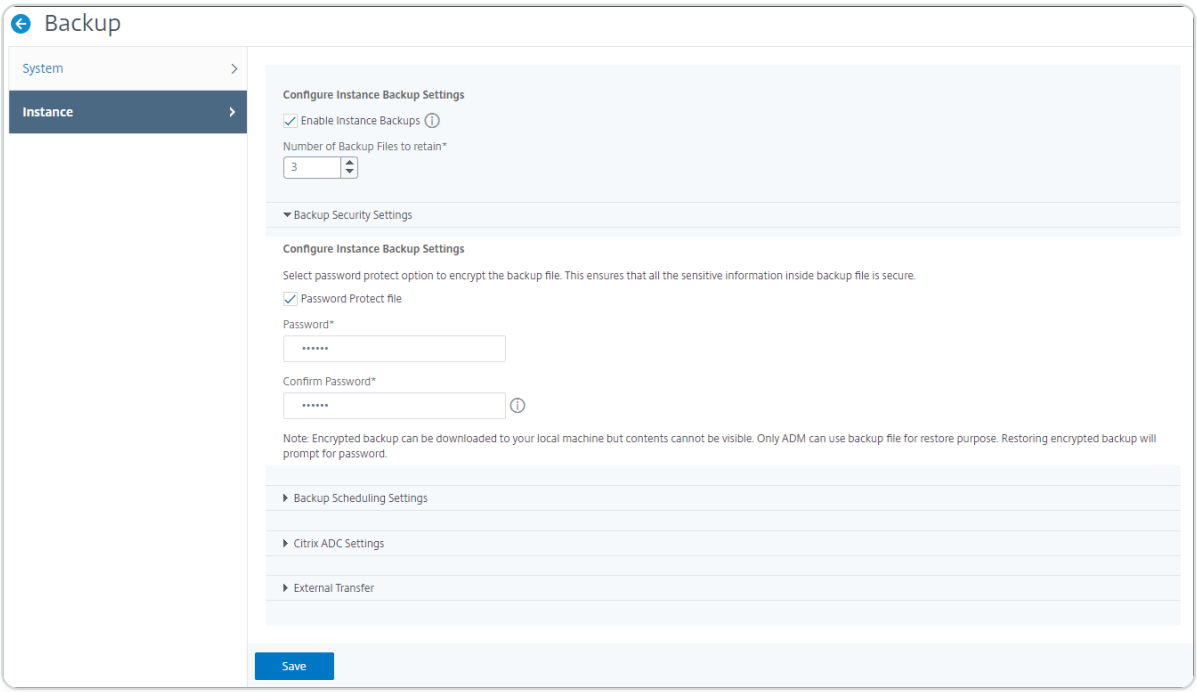
NOTE

You can download the encrypted backup file to your local machine, but you cannot open the file either with the NetScaler ADM GUI or with any text editor. You are prompted to provide the password when restoring the encrypted backup file. You can, however, open an unencrypted backup file on your system.

- **Number of Backup Files to retain**: Specify the number of backup files to retain in NetScaler ADM. You can retain up to 50 backup files per ADC instance. The default is three backup files.

NOTE

Each backup file accounts for some storage requirement. Citrix recommends that you store an optimal number of NetScaler backup files on NetScaler ADM as per your requirement.

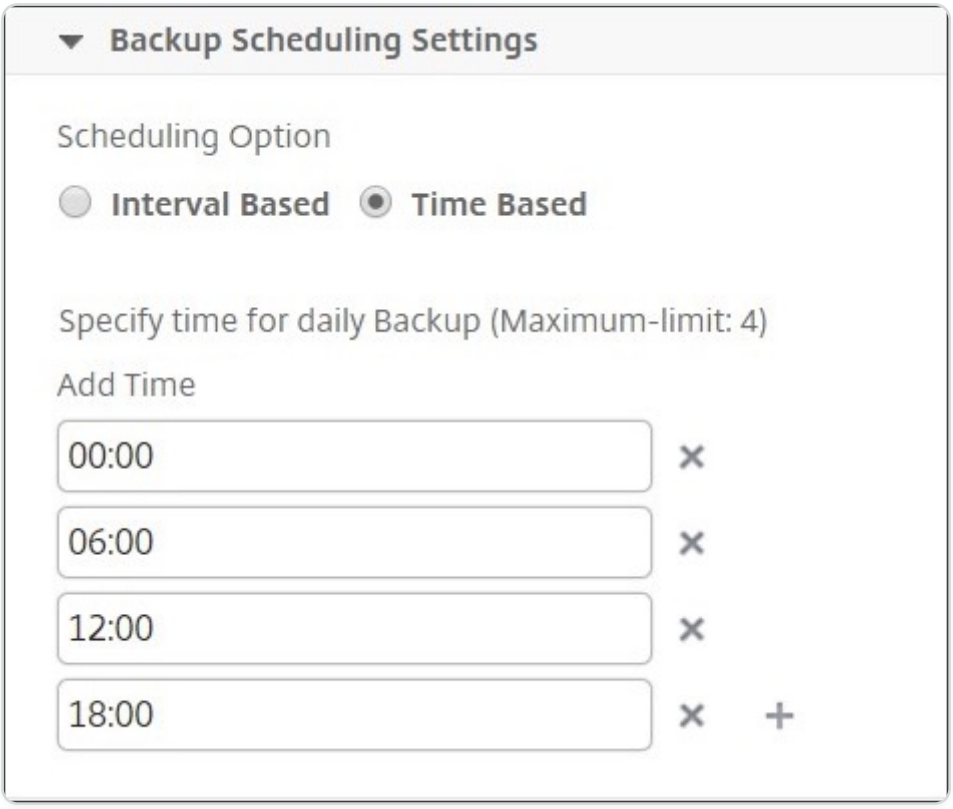


- **Backup scheduling settings**: (optional) There are two options available for creating backup files, though you can use only one option at a time:

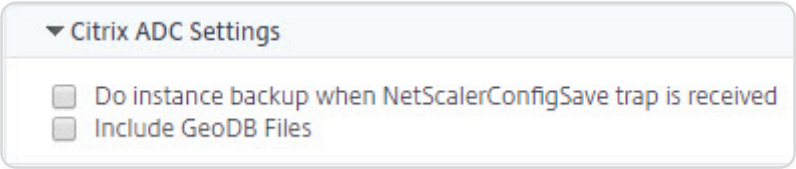
  a. The default backup scheduling option is "interval-based." A backup file is created in NetScaler ADM after the specified interval elapses. The default backup interval is 12 hours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. You can also change the type of scheduled backups to "time-based." In this option, specify the time in `hours:minutes` format to back up instances at the specified time. NetScaler ADM allows a maximum of four daily backups to happen on the instances.



- **NetScaler settings**: (optional) By default, NetScaler ADM does not create a backup file when it receives the “NetScalerConfigSave” trap. But, you can enable the option to create a backup file whenever a NetScaler instance sends a “NetScalerConfigSave” trap to NetScaler ADM. A NetScaler instance sends “NetScalerConfigSave” every time the configuration on the instance is saved.
- **Geodatabase files**: (optional) By default, NetScaler ADM does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.



- **External Transfer:**(optional) NetScaler ADM allows you to transfer the NetScaler instance backup files to an external location:

  a. Specify the IP address of the location.

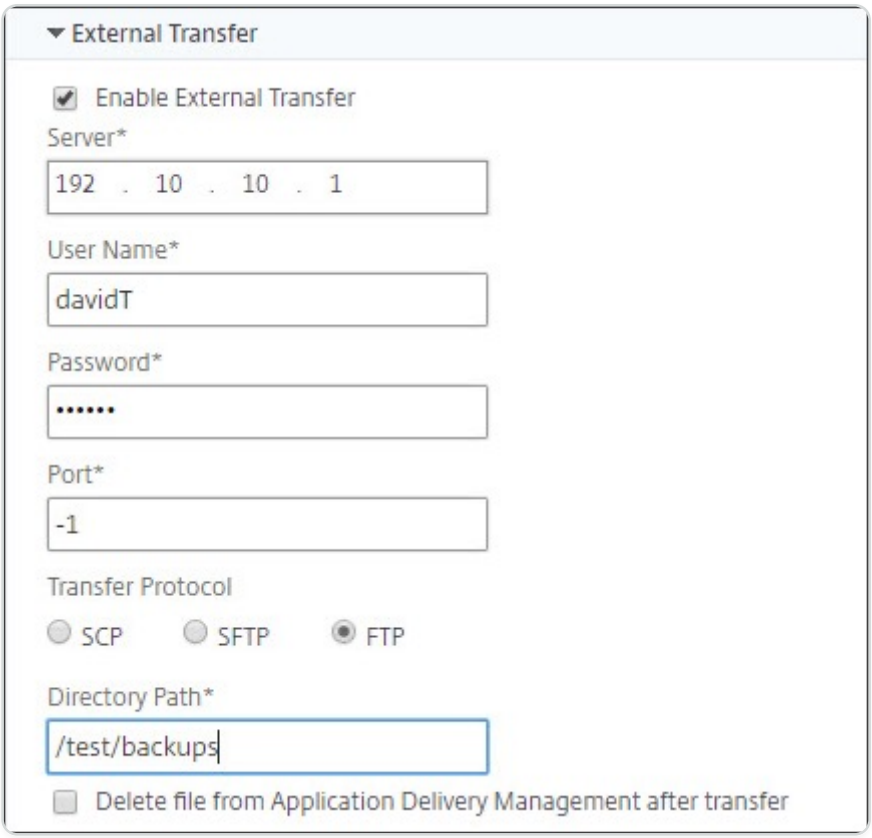
  b. Specify the user name and the password of the external server to which you want to transfer the backup files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Specify the transfer protocol and the port number.

d. You can specify the directory path where the file must be stored.

e. Optional, you can also delete the backup file from NetScaler ADM after transferring it to the external server.



NOTE

NetScaler ADM sends an SNMP trap or a Syslog notification to itself when there is a backup failure for any of the selected NetScaler instances.

Create a backup for a selected NetScaler instance by using NetScaler ADM

Perform this task if you want to back up a selected NetScaler instance or multiple instances:

1. In NetScaler ADM, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instances (for example, NetScaler VPX) to display on the screen.
2. Select the instance that you want to back up.
   - For MPX, VPX, and BLX instance, select **Backup/Restore** from the **Select Action** list.
   - For an SDX instance, click **Backup/Restore**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Backup Files** page, click **Back Up**.
4. You can specify whether to encrypt your backup file for more security. You can either enter your password or use the global password that you previously specified on the Instance Backup Settings page.
5. Click **Continue**.

Restore a NetScaler instance by using NetScaler ADM

Note:

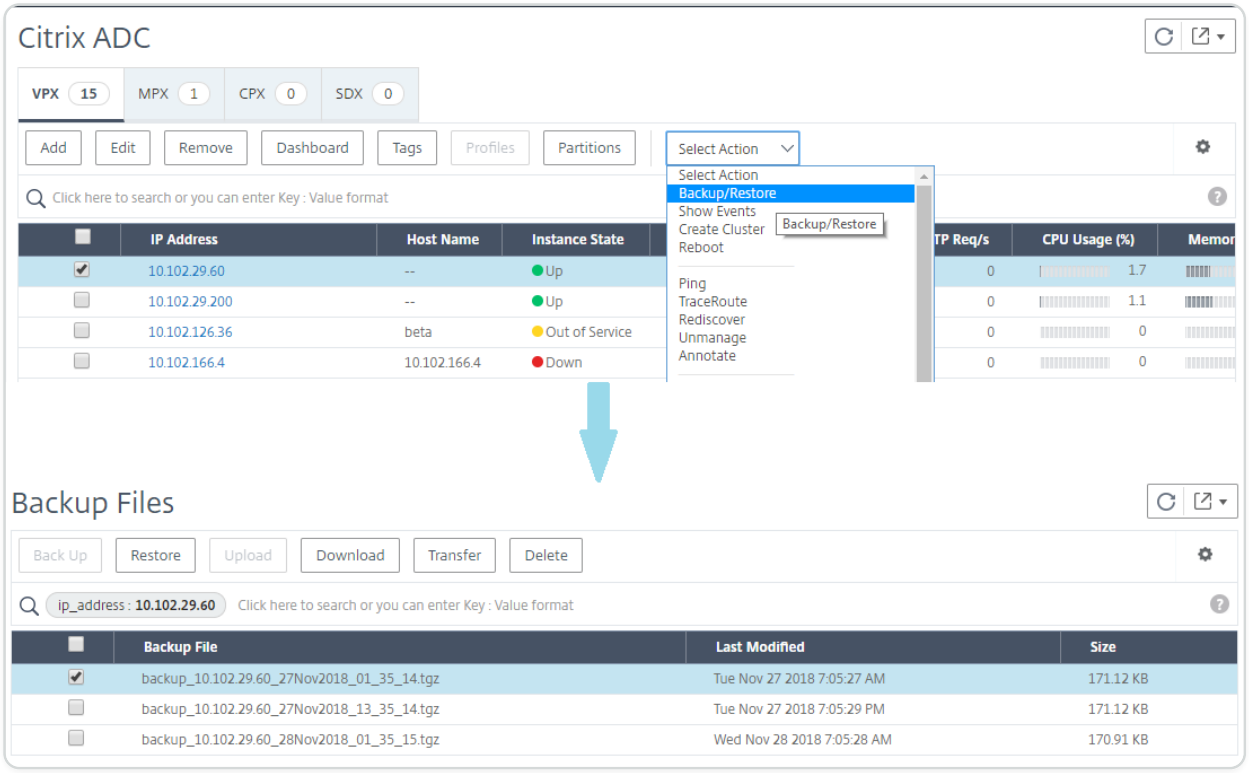
> If you have NetScaler instances in a HA pair, you need to note the following:

- Restore the same instance from which the backup file was created. For example, let us consider a scenario that a backup was taken from the primary instance of the HA pair. During the restore process, ensure that you are restoring the same instance, even if it is no longer the primary instance.
- When you initiate the restore process on the primary ADC instance, you cannot access the primary instance and the secondary instance gets changed to **STAYSECONDARY**. Once the restore process is completed on the primary instance, the secondary ADC instance changes from **STAYSECONDARY** to **ENABLED** mode and becomes part of the HA pair again. You can expect a possible downtime on the primary instance until the restore process gets completed.

Perform this task to restore a NetScaler instance by using the backup file that you created earlier:

1. Navigate to **Infrastructure > Instances**, select the instance that you want to restore, and then click **View Backup**.
2. On the **Backup Files** page, select the backup file containing the settings that you want to restore, and then click **Restore**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Restore a NetScaler SDX appliance using NetScaler ADM

In NetScaler ADM, the backup of the NetScaler SDX appliance includes the following:

- NetScaler instances hosted on the appliance
- SVM SSL certificates and keys
- Instance prune settings (in XML format)
- Instance backup settings (in XML format)
- SSL certificate poll settings (in XML format)
- SVM db file
- NetScaler config files of devices present on SDX
- NetScaler build images
- NetScaler XVA images, these images are stored in the following location: `/var/mps/sdx_images/`
- SDX Single Bundle Image (SVM+XS)
- Third Party instance images (if provisioned)

Restore your NetScaler SDX appliance to the configuration available in the backup file. During appliance restore, the entire current configuration is deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you are restoring the NetScaler SDX appliance by using a backup of a different NetScaler SDX appliance, ensure that you add the licenses and configure the new appliance's Management Service network settings to match the settings in the backup file before you start the restore process. That is, the new appliance must be licensed and meet the minimum license requirements of the backup file. For example, if the backup had five VPX instances with a total of 5 GB, then the new appliance must also be able to support these requirements. Or if the backup appliance had a platinum license, the new appliance must have the same or higher license. Network settings, such as IP address, netmask, gateway, XenServer IP address, and DNS server must be properly configured on the new appliance.

Before you restore the SDX appliance, ensure that the backed-up SDX appliance platform variant is the same as the appliance. You cannot restore from a different platform variant.

NOTE

Before you restore an SDX RMA appliance, ensure that the backed-up version is either the same or higher than the RMA version.

To restore the SDX appliance from the backed-up file:

1. In the NetScaler ADM GUI, navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Backup/Restore**.
3. Select the backup file of the same instance that you want to restore.
4. Click **Repackage Backup**.

   When the SDX appliance is backed up, the XVA files and images are stored separately to save the network bandwidth and the disk space. Therefore, you must repackage the backed-up file before you restore the SDX appliance.

   When you repackage the backup file, it includes all the backed-up files together to restore the SDX appliance. The repackaged backup file ensures the successful restoration of the SDX appliance.
5. Select the backup file that is repackaged and click **Restore**.

Force a failover to the secondary NetScaler instance

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the instance.

A forced failover fails in any of the following circumstances:

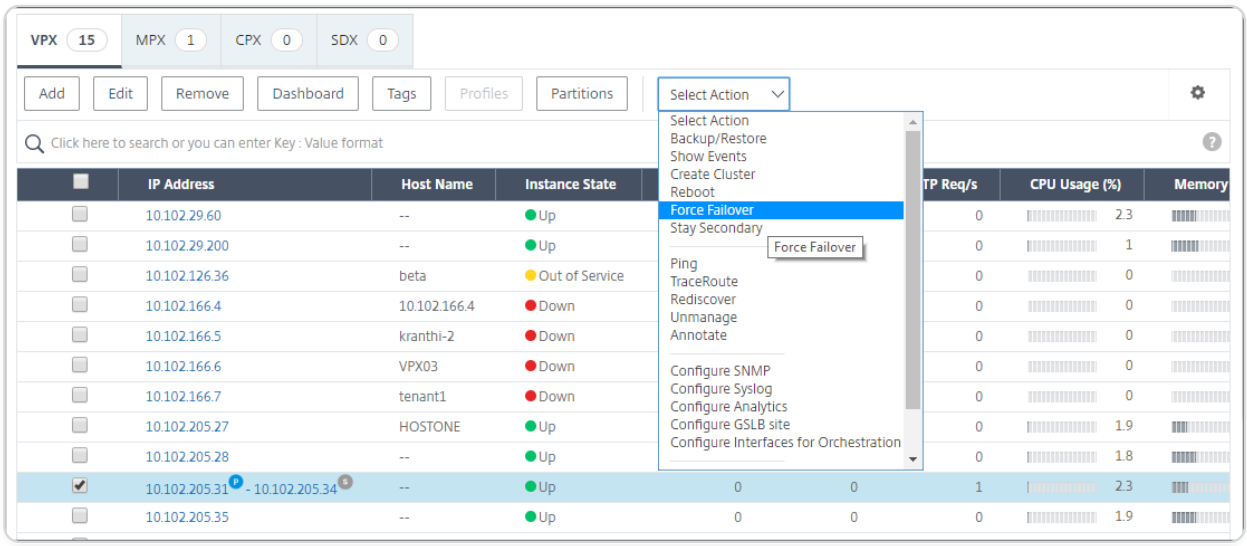
- You force failover on a standalone system.
- The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.
- The secondary instance is configured to remain secondary.

The NetScaler instance displays a warning message if it detects a potential issue when you run the force failover command. The message includes the information that triggered the warning, and requests confirmation before proceeding.

You can force a failover on a primary instance or on a secondary instance.

To force a failover to the secondary NetScaler instance using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Instances > NetScaler > VPX** tab, and then select an instance .
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Force Failover.**
4. Click **Yes** to confirm the force failover action.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Force a secondary NetScaler instance to stay secondary

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want the secondary node to take over. You want it to remain the secondary node even if it detects a failure in the primary node.

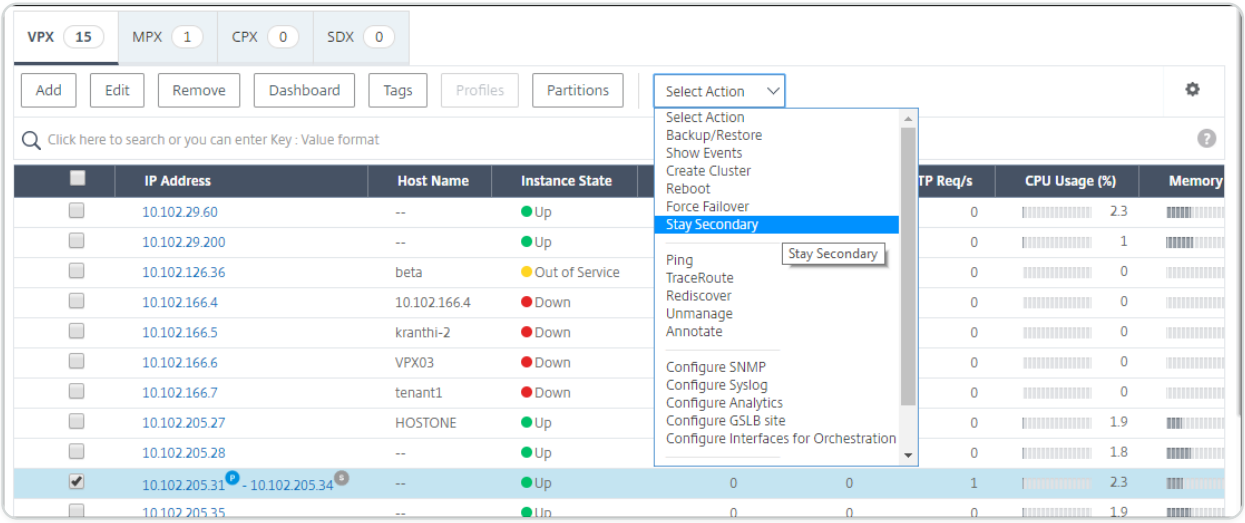
When you force the secondary node to stay secondary, it remains secondary even if the primary node goes down. Also, when you force the status of a node in an HA pair to stay secondary, it does not participate in HA state machine transitions. The status of the node is displayed as STAYSECONDARY.

NOTE

When you force a system to remain secondary, the forcing process is not propagated or synchronized. It affects only the node on which you run the command.

To configure a secondary NetScaler instance to stay secondary by using NetScaler ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Instances** > **NetScaler** > **VPX** tab, and then select an instance.
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the “Stay Secondary” action.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

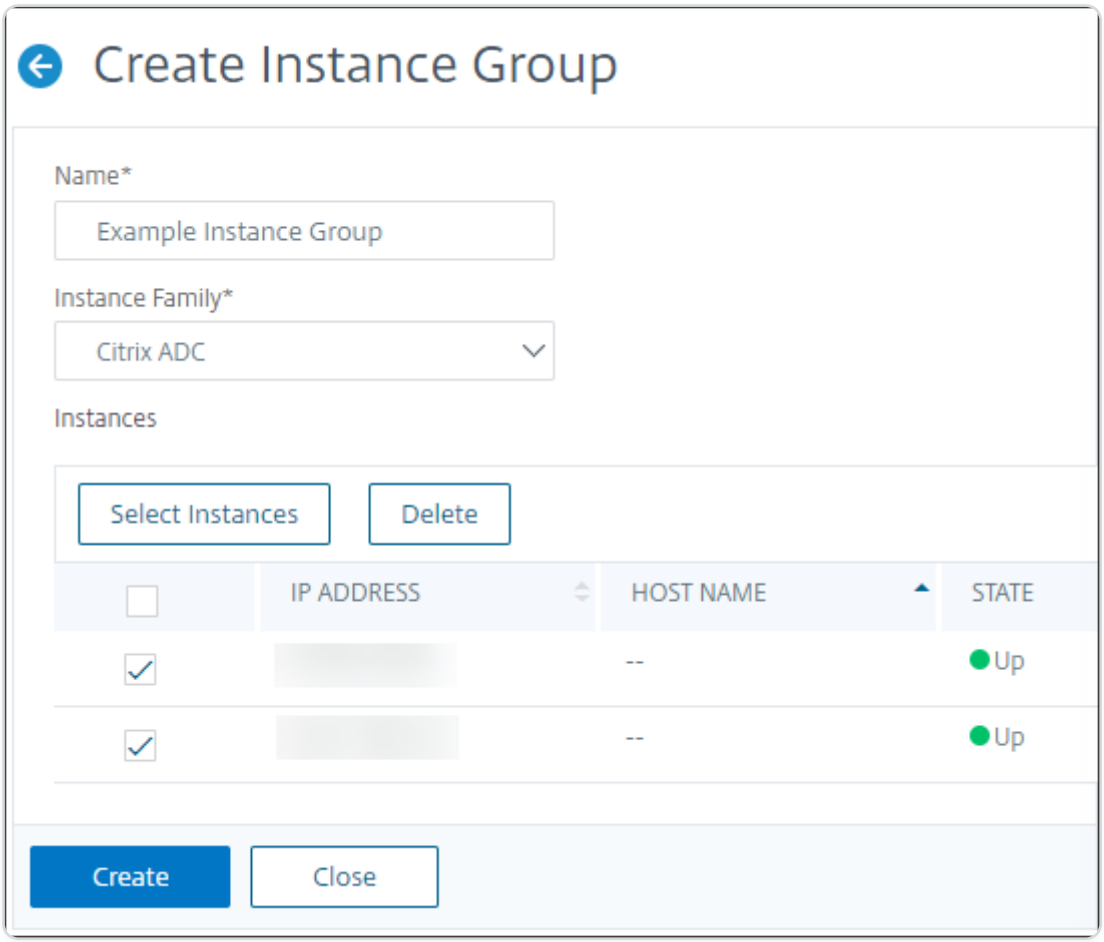
Create instance groups

To create an instance group, you must first add all your NetScaler instances to NetScaler ADM. After you have added the instances successfully, create instance groups based on their instance family. Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

To create an instance group using NetScaler® ADM

1. In NetScaler ADM, navigate to **Infrastructure > Instance Groups**, and then click **Add**.
2. Specify a name to your instance group and select **NetScaler** from the **Instance Family** list.
3. Click **Select Instances**. On the **Select Instances** page, select the instances that you want to group and click **Select**.

   The table lists the selected instances and their details. If you want to remove any instance from the group, select the instance from the table and click **Delete**.
4. Click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provision NetScaler VPX instances on SDX using ADM

You can provision one or more NetScaler VPX instances on the SDX appliance by using NetScaler ADM. The number of instances that you can deploy depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the ADM restricts you from provisioning more NetScaler instances.

Before you begin, ensure to add an SDX instance in ADM where you want to provision VPX instances.

To provision a VPX instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **SDX** tab, select an SDX instance where you want to provision a VPX instance.
3. In **Select Action**, select **Provision VPX**.

Step 1 - Add a VPX instance

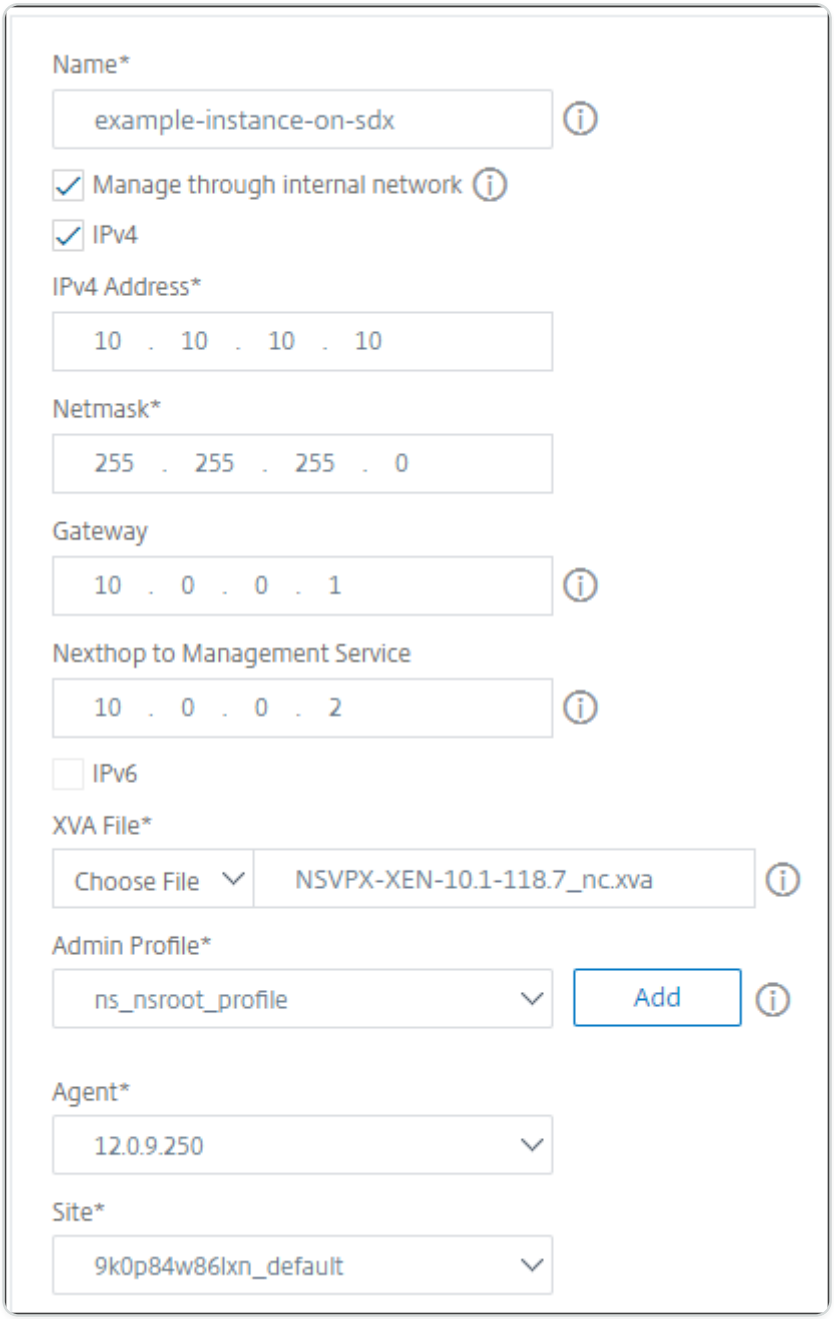
The ADM uses the following information to configure VPX instances in an SDX appliance:

- **Name** - Specify a name to an ADC instance.
- Establish a communication network between SDX and VPX. To do so, select the required options from the list:
  - **Manage through internal network** - This option establishes an internal network for a communication between the ADM and a VPX instance.
  - **IP address** - You can select an **IPv4** or **IPv6** address or both to manage the NetScaler VPX instance. A VPX instance can have only one management IP (also called NetScaler IP). You cannot remove the NetScaler IP address.

    For the selected option, assign a netmask, default gateway, and next hop to the ADM server for the IP address.
- **XVA File** - Select the XVA file from which you want to provision a VPX instance. Use one of the following options to select the XVA file.
  - **Local** - Select the XVA file from your local machine.
  - **Appliance** - Select the XVA file from an ADM file browser.
- **Admin Profile** - This profile provides access to provision VPX instances. With this profile, ADM retrieves the configuration data from an instance. If you have to add a profile, click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Agent** - Select the agent with which you want to associate the instances
- **Site** - Select the site where you want the instance to be added.



Step 2 - Allocate licenses

In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **Allocation mode** - You can choose **Fixed** or **Burstable** modes for the bandwidth pool.

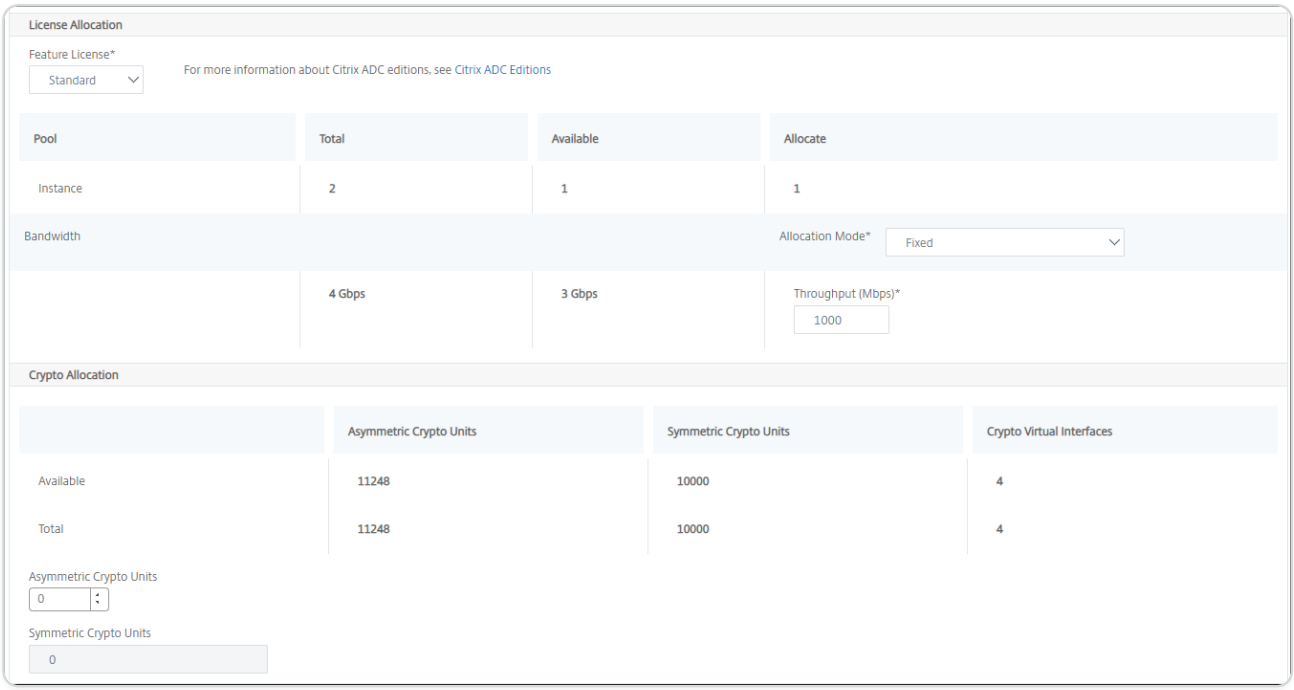
  If you choose **Burstable** mode, you can use extra bandwidth when the fixed bandwidth is reached.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Throughput** - Assign the total throughput (in Mbps) to an instance.

NOTE

Buy a separate license (SDX 2-Instance Add-On Pack for Secure Web Gateway) for Citrix Secure Web Gateway™ (SWG) instances on SDX appliances. This instance pack is different from the SDX platform license or SDX instance pack.



Step 3 - Allocate resources

In the **Resource Allocation** section, allocate resources to a VPX instance to maintain traffic.

- **Total Memory (MB)** - Assign total memory to an instance. The minimum value is `2048` MB.
- **Packets per second** - Specify the number of packets to transmit per second.
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  When you select a shared core to an instance, the other instances can use the shared core at the time of resource shortage.

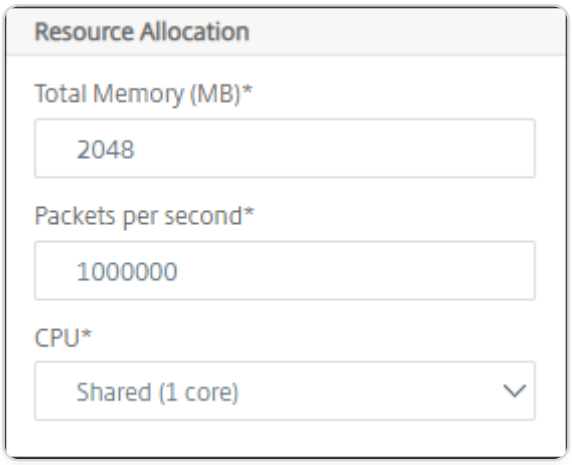
  Restart instances on which CPU cores are reassigned to avoid any performance degradation.

  If you are using the SDX 25000xx platform, you can assign a maximum of 16 cores to an instance. Also, if you are using the SDX 2500xxx platform, you can assign a maximum of 11 cores to an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

For an instance, the maximum throughput that you configure is 180 Gbps.



The following table lists the supported VPX, Single bungle image version, and the number of cores you can assign to an instance:

PLATFORM NAME	TOTAL CORES	TOTAL CORES AVAILABLE FOR VPX PROVISIONING	MAXIMUM CORES THAT CAN BE ASSIGNED TO A SINGLE INSTANCE
SDX 8015, SDX 8400, and SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542	12	10	5
SDX 17500, SDX 19500, and SDX 21500	12	10	5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PLATFORM NAME	TOTAL CORES	TOTAL CORES AVAILABLE FOR VPX PROVISIONING	MAXIMUM CORES THAT CAN BE ASSIGNED TO A SINGLE INSTANCE
SDX 17550, SDX 19550, SDX 20550, and SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 and SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100, and SDX 22120	16	14	7
SDX 24100 and SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G and SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS and SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S, and SDX 14100 40S	12	10	5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PLATFORM NAME	TOTAL CORES	TOTAL CORES AVAILABLE FOR VPX PROVISIONING	MAXIMUM CORES THAT CAN BE ASSIGNED TO A SINGLE INSTANCE
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (if version is 11.1-51.x or higher); 9 (if version is 11.1-50.x or lower; all versions of 11.0 and 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

NOTE

On the SDX 26xxx platform, a maximum of 26 CPU cores can be assigned to a VPX instance. If crypto units are assigned to the instance, the maximum number of cores depends on the number of crypto units and data interfaces.

For example, if you assign 24000 crypto units to an instance, you can assign 24 CPU cores and maximum two data interfaces to the instance. The SDX appliance considers data interfaces and crypto units as PCI devices. For 26000 crypto units, VPX instance provisioning fails because of no space to add data interfaces.

Step 4 - Add instance administration

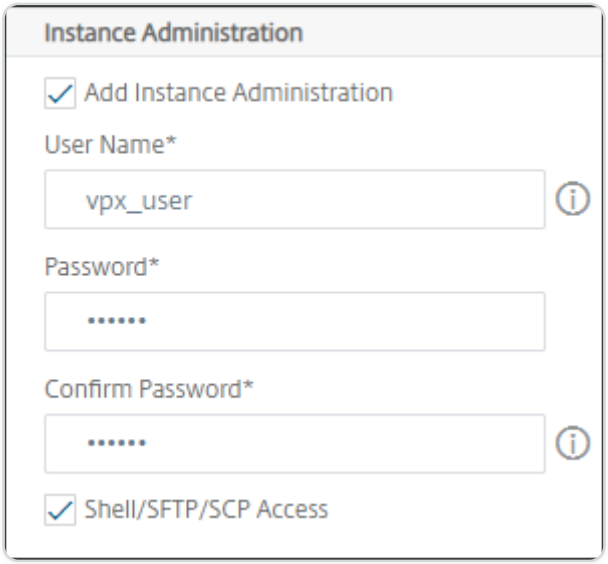
You can create an admin user for the VPX instance. To do so, select **Add Instance Administration** in the **Instance Administration** section.

Specify the following details:

- **User name**: The user name for the NetScaler instance administrator. This user has superuser access but does not have access to networking commands to configure VLANs and interfaces.
- **Password**: Specify the password for the user name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Shell/Sftp/Scp Access**: The access allowed to the NetScaler instance administrator. This option is selected by default.



Step 5 - Specify network settings

Select the required network settings to an instance:

- **Allow L2 Mode under network settings** - You can allow L2 mode on the NetScaler instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode.

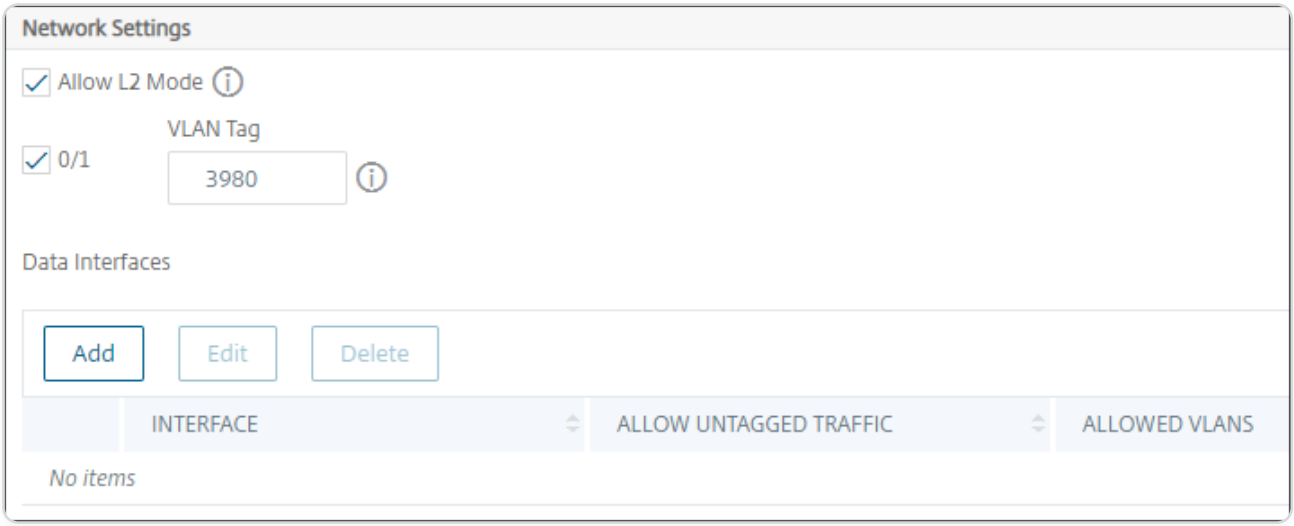
  NOTE

  If you disable L2 mode for an instance, you must log on to the instance and disable L2 mode from that instance. Otherwise, it might cause all the other NetScaler modes to be disabled after you restart the instance.

- **0/1** - In **VLAN tag**, specify a VLAN ID for the management interface.
- **0/2** - In **VLAN tag**, specify a VLAN ID for the management interface.

By default interface **0/1** and **0/2** are selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In **Data Interfaces**, click **Add** to add data interfaces and specify the following:

- **Interfaces** - Select the interface from the list.

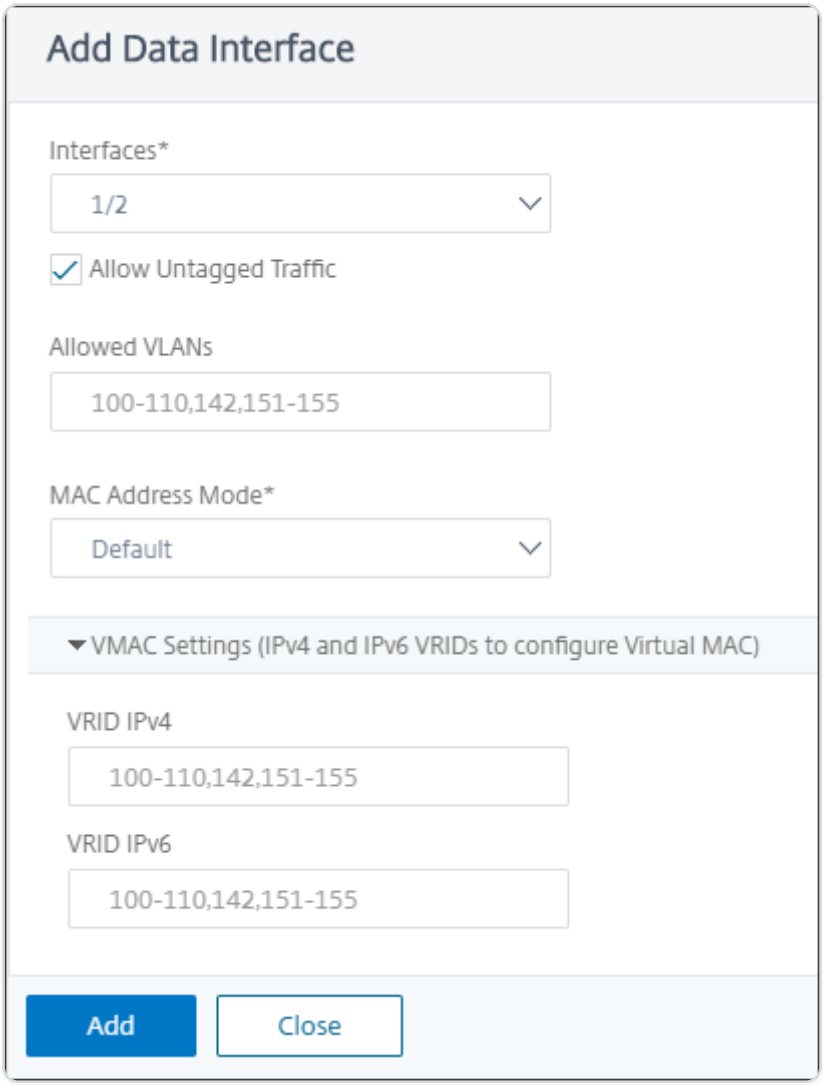
  NOTE

  The interface IDs of interfaces that you add to an instance do not necessarily correspond to the physical interface numbering on the SDX appliance.

  For example, the first interface that you associate with instance-1 is SDX interface 1/4, it appears as interface 1/1 when you view the interface settings in that instance. This interface indicates it is the first interface that you associated with instance-1.

- **Allowed VLANs** - Specify a list of VLAN IDs that can be associated with a NetScaler instance.
- **MAC Address Mode** - Assign a MAC address to an instance. Select from one of the following options:
  - **Default** - Citrix Workspace assigns a MAC address.
  - **Custom** - Choose this mode to specify a MAC address that overrides the generated MAC address.
  - **Generated** - Generate a MAC address by using the base MAC address set earlier.
- **VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)**
  - **VRID IPV4** - The IPv4 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.
  - VRID IPV6 - The IPv6 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Add**.

Step 6 - Specify Management VLAN settings

The Management Service and the management address (NSIP) of the VPX instance are in the same subnetwork, and communication is over a management interface.

If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

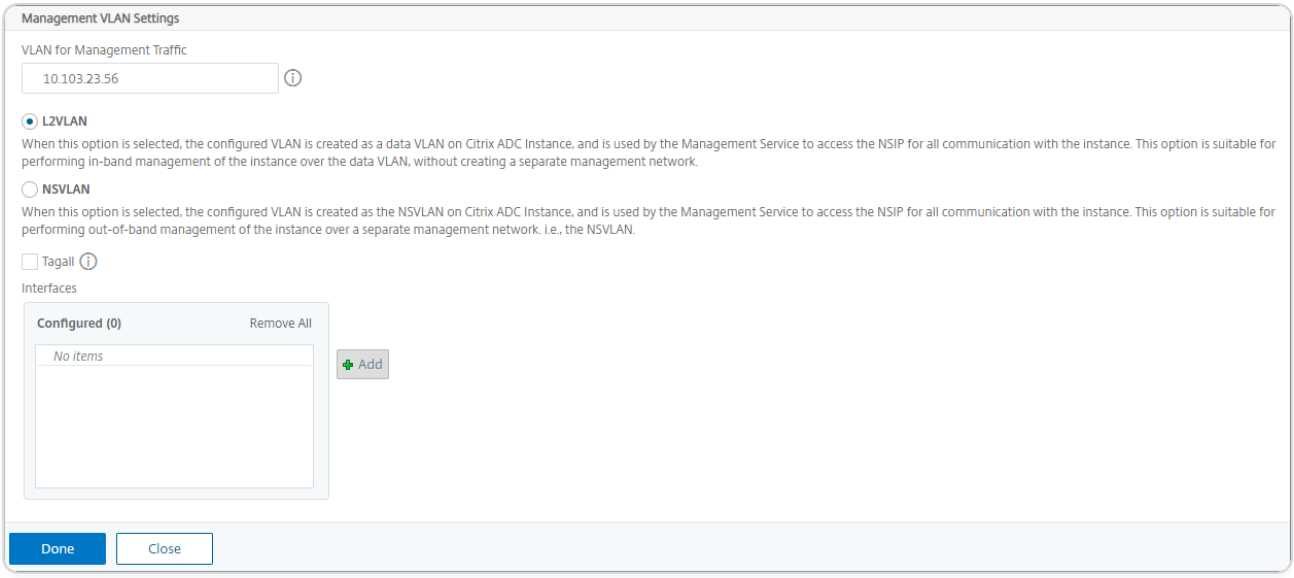
If your deployment requires the NSIP is accessible only through the selected interface while provisioning the VPX instance, select **NSVLAN**. And, the NSIP becomes inaccessible through other interfaces.

- HA heartbeats are sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from the VPX XVA build `9.3-53.4` and later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- You cannot change this setting after you provision the VPX instance.
- The `clear config full` command on the VPX instance deletes the VLAN configuration if **NSVLAN** is not selected.

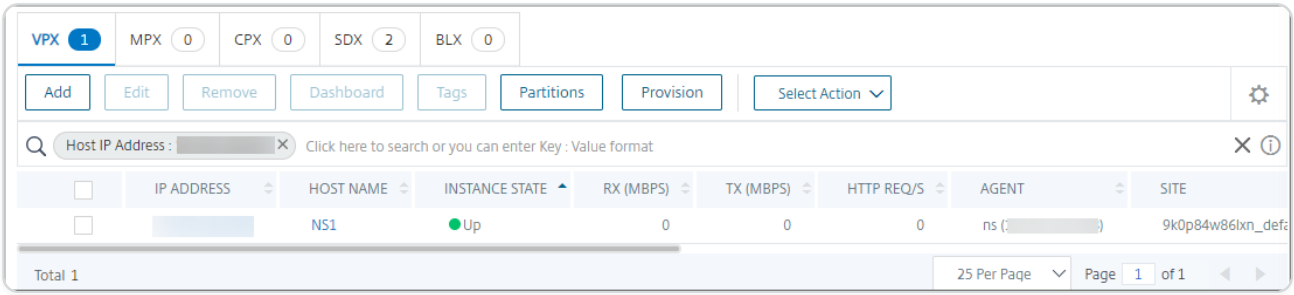


Click **Done** to provision a VPX instance.

View the provisioned VPX instance

To view the newly provisioned instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, search an instance by the **Host IP address** property and specify SDX instance IP to it.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provision NetScaler VPX instances on VMware ESX

You can use ADM to automate an NetScaler VPX instance deployment and management in VMware ESX. When you use NetScaler ADM to provision an NetScaler VPX instance on VMware ESX, the instance is readily available to manage in the ADM GUI.

The NetScaler® ADM uses ADC templates of the already deployed instances to provision a new instance in VMware ESX. It stores the required VMware ESX server details in a site. Also, it uses Cloud Access Profile to access the server.

Prerequisites

Before you provision an NetScaler VPX instance in VMware ESX, ensure to complete the following:

1. Install a supported VMware ESXi version (6.0, 6.5, and 6.7).
2. Install VMware Client on a management workstation that meets the minimum system requirements.
3. Downloading the NetScaler VPX setup files.
4. Convert NetScaler VPX files into templates in ESX.
5. Create a site in ADM.

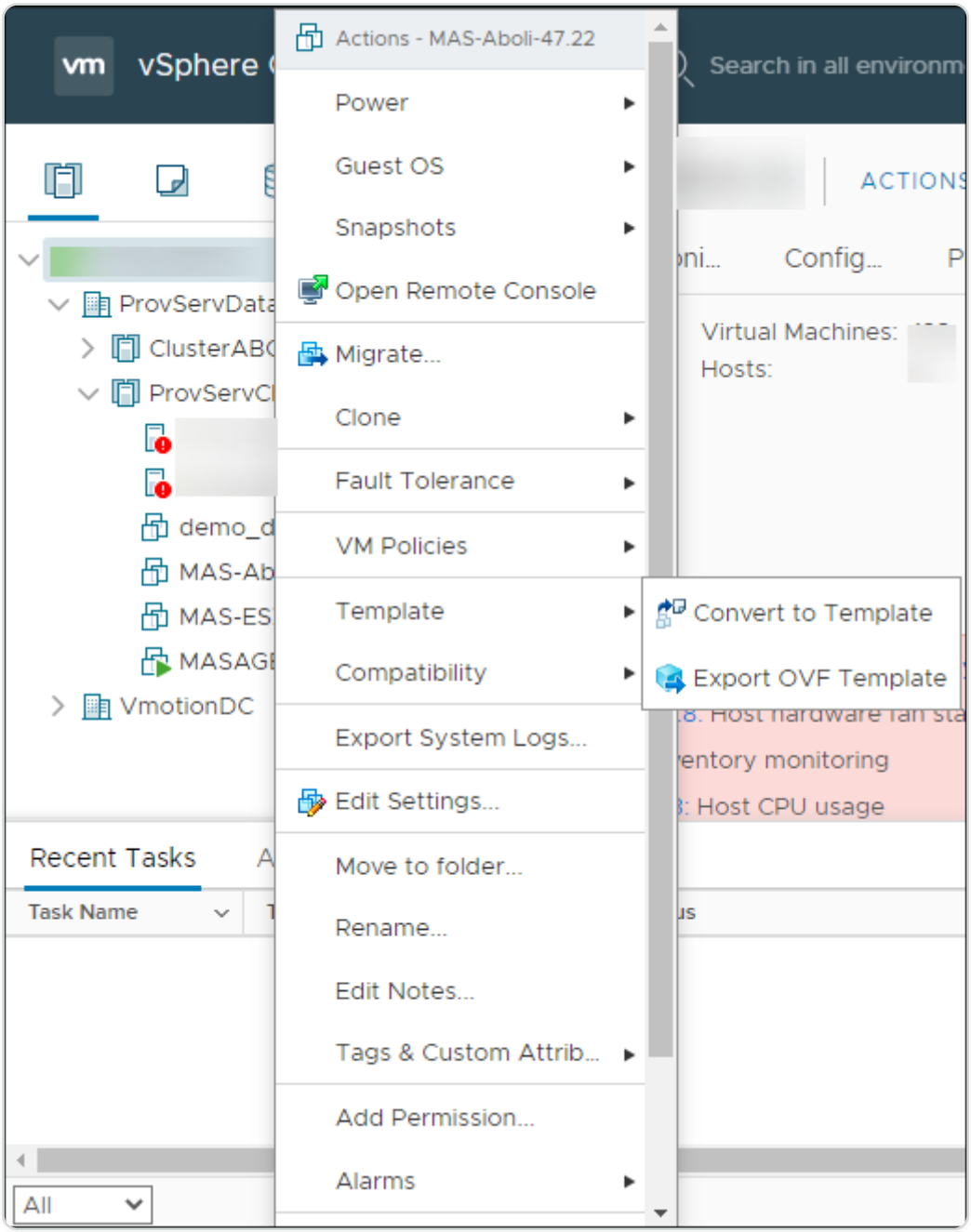
Convert NetScaler VPX files into templates

The NetScaler ADM uses the ADC template in ESX converted by an NetScaler VPX file. Perform the following steps to convert VPX files into templates.

1. Deploy a NetScaler VPX instance on VMware using the ADC setup files.

   For the first time, use ADC setup files to deploy the VPX instance. For more information, see Install NetScaler VPX instance on VMware.
2. Right-click the deployed VM and select **Template**.
3. Click **Convert to Template**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a site in ADM

Create a site in NetScaler ADM and add the VMware ESX details.

1. In NetScaler ADM, navigate to **Infrastructure > Instances > Sites**.
2. Click **Add**.
3. In the **Select Cloud** pane,
   a. Select **Data Center** as a **Site** type.
   b. Choose **VMware vCenter** from the **Type** list.
   c. Click **Next**.

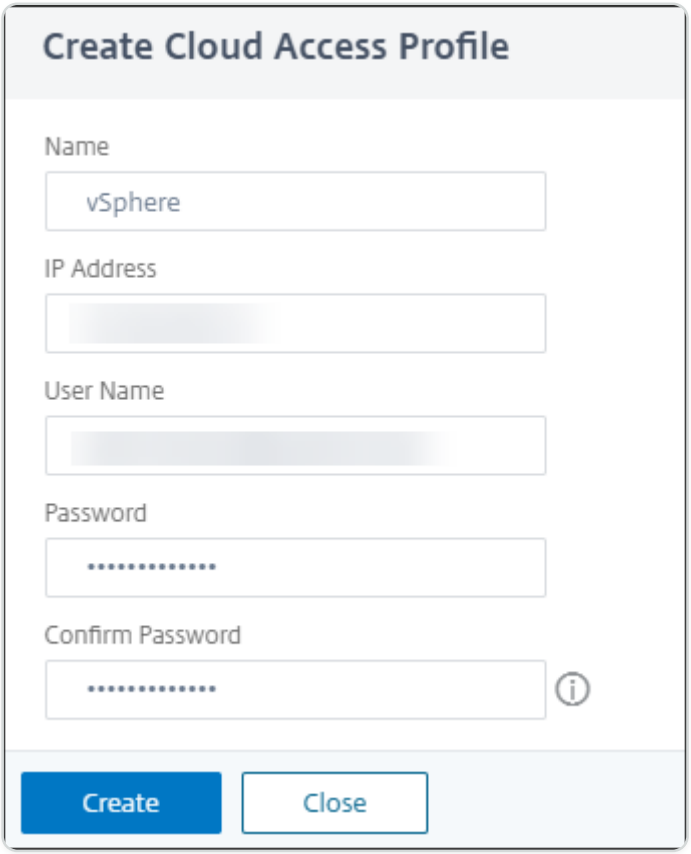
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the **Choose Region** pane,

   a. In the **Cloud Access Profile** pane, select the profile created for your VMware ESX. If there are no profiles, create a profile.

   b. To create a cloud access profile, click **Add** and specify the following:

      - **Name** – Specify a name to identify your cloud access profile in NetScaler ADM.
      - **IP address** – Specify the IP address of the VMware vCenter server where you want to provision VPX instances.
      - **Username** – Specify the user name to access the VMware vCenter server.
      - **Password** – Specify the password to access the VMware vCenter server and confirm the password.



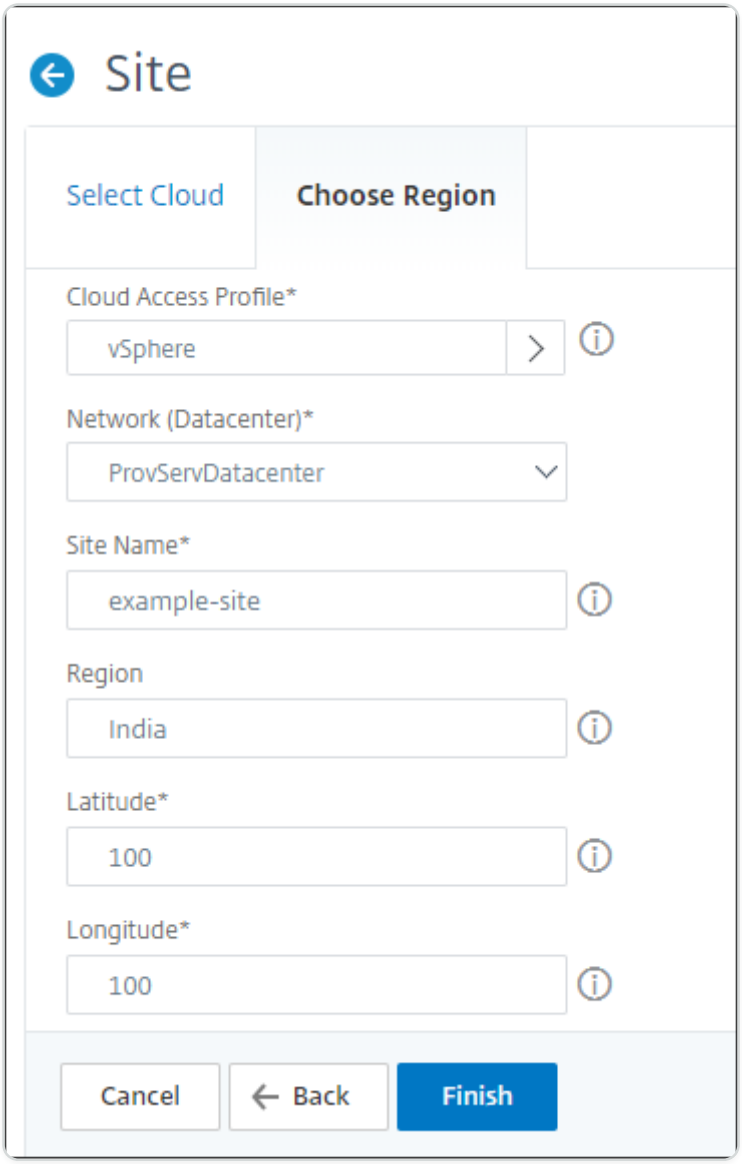
   c. In **Network (Datacenter)**, select the data center where you have the ADC templates.

   d. Specify the **Site Name**.

   e. Specify the **Region**, **Latitude**, and **Longitude** to identify the geo-location of your data center.

   f. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Provision an instance on VMware ESX

Use the site that you have associated with your VMware ESX to provision the NetScaler VPX instances.

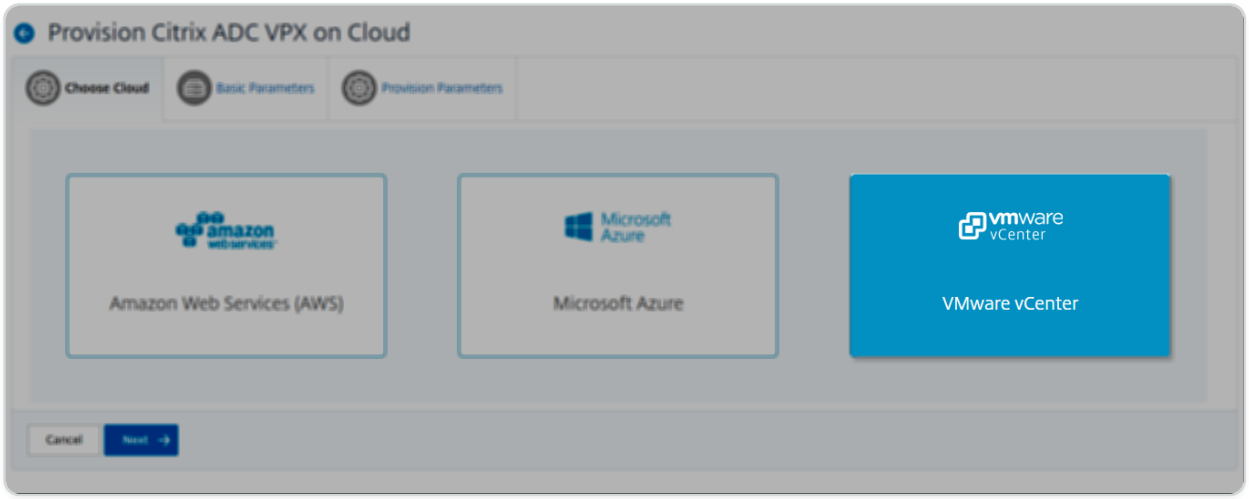
NOTE:

Currently, the NetScaler ADM supports only to provision standalone ADC instances.

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

   This option displays the **Provision NetScaler VPX on Cloud** page.
3. Select **VMware vCenter** and click **Next**.

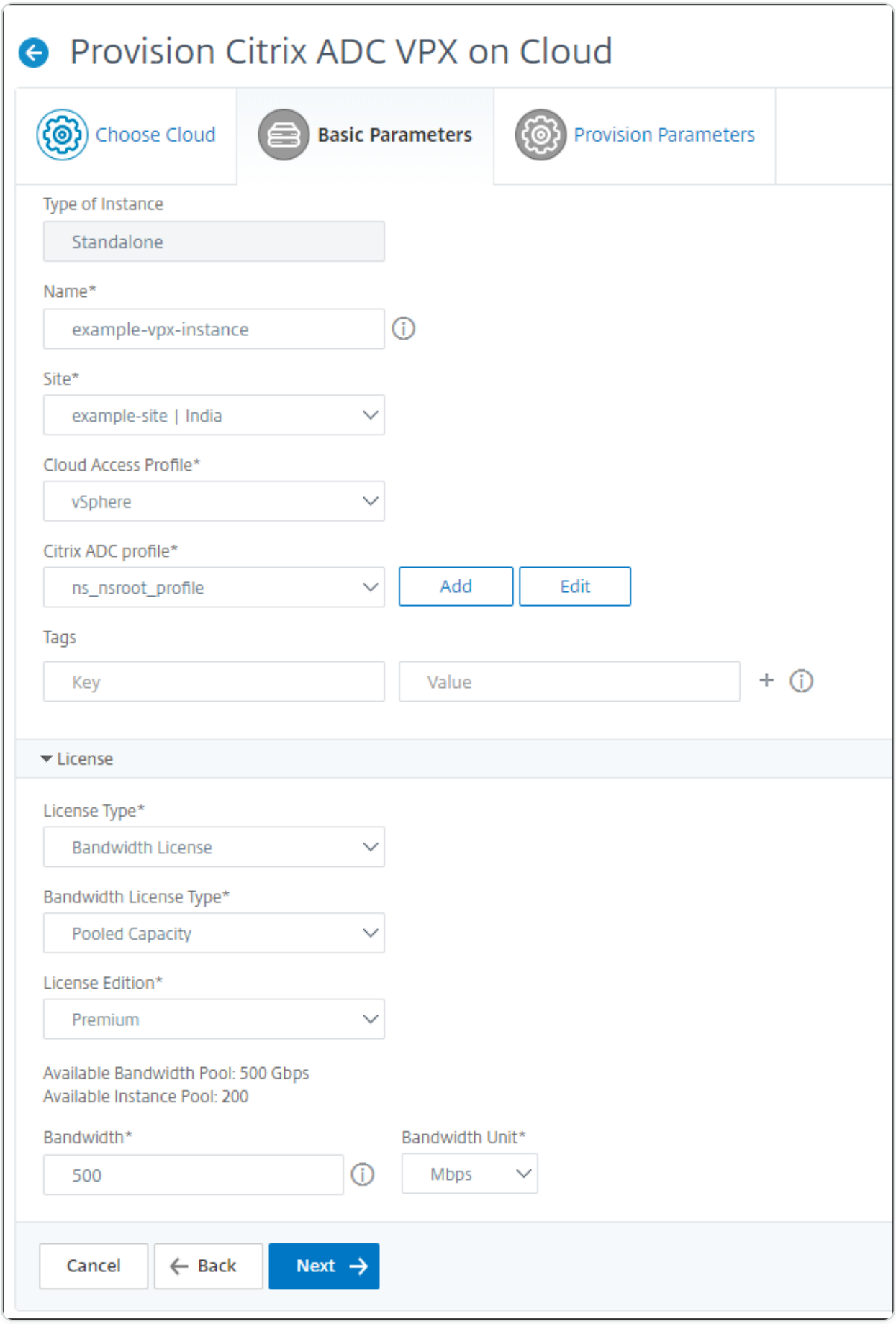
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In **Basic Parameters**, specify the following:

   - **Name** – Specify the name of an instance.
   - **Site** – Select the site that you have created earlier.
   - **Cloud Access Profile** – Select the cloud access profile created during site creation.
   - **NetScaler profile** – Select the ADC profile to provide authentication.
   - **License** – Use pooled capacity licensing to apply licenses to an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



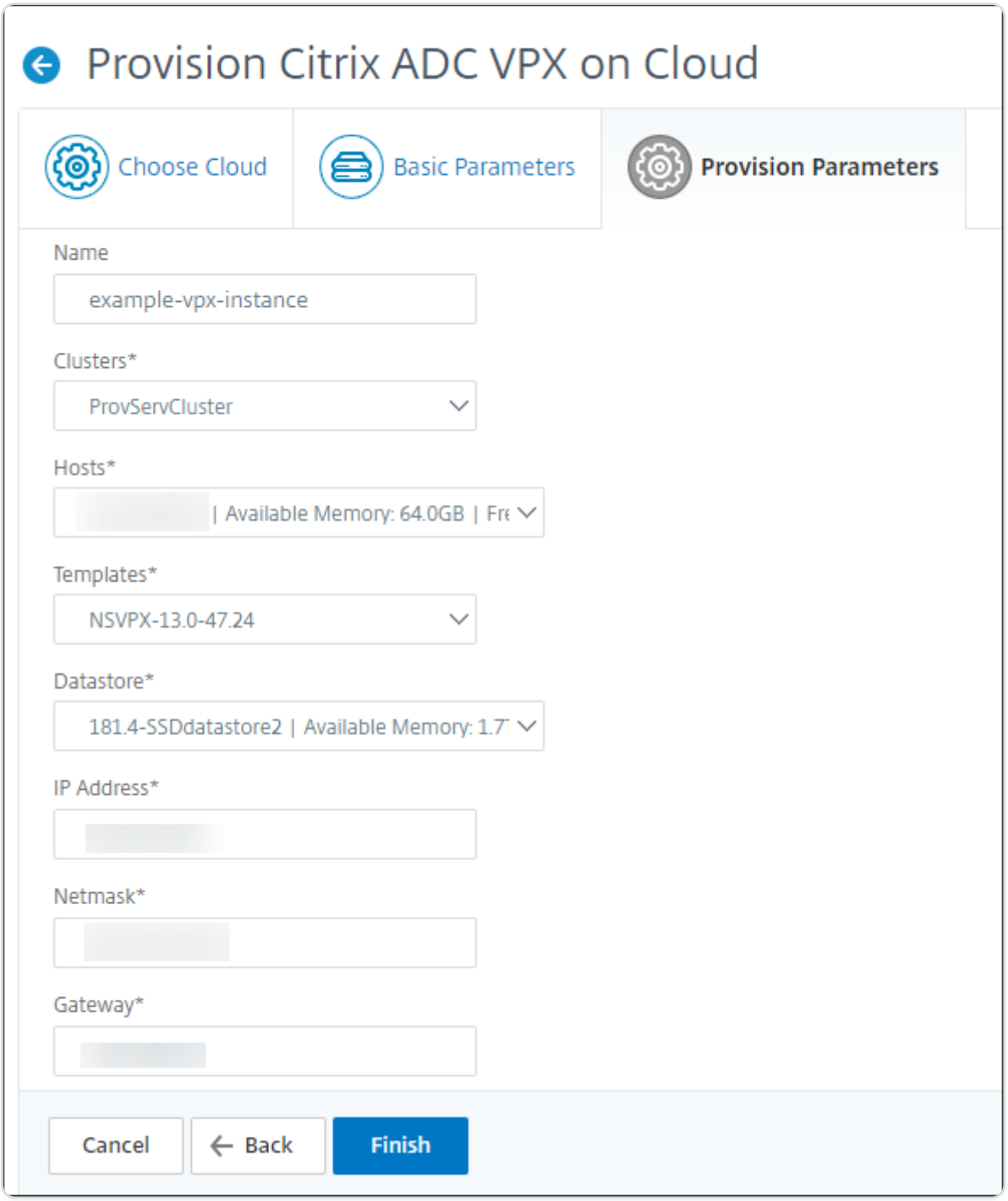
5. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. In **Provision Parameters**, specify the following details:

   - **Clusters** – Select the cluster where you want to provision an instance.
   - **Hosts** – Select the required host from the list.
   - **Templates** – Select the template from the list that you want to apply to an instance.
   - **Datastore** – Select the datastore from the list.
   - **IP address** – Specify an IP address to an instance.
   - **Net mask** – Specify a net mask to an instance.
   - **Gateway** – Specify a gateway to an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Click **Finish**.

Rediscover multiple NetScaler VPX instances

You can rediscover multiple NetScaler VPX instances in your NetScaler Application Delivery Management (ADM) setup. Also, you can rediscover multiple NetScaler VPX instances when you want to view the latest states and configurations of those instances. The NetScaler ADM server rediscovers all the NetScaler VPX instances and checks whether the Citrix Application Delivery Controller (ADC) instances are reachable.

To rediscover multiple NetScaler VPX instances:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In a web browser, type the IP address of the NetScaler ADM server (for example, `<http://192.168.100.1>`).
2. In the **User Name** and **Password** fields, enter the administrator credentials. The default administrator credentials are `nsroot` and `nsroot`.
3. Navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab and select the instances you want to rediscover.
4. In the **Select Action** menu, click **Rediscover**.
5. When the confirmation message for running the Rediscover utility appears, Click **Yes**.

   The screen reports the progress of rediscovery of each of the NetScaler VPX instances.

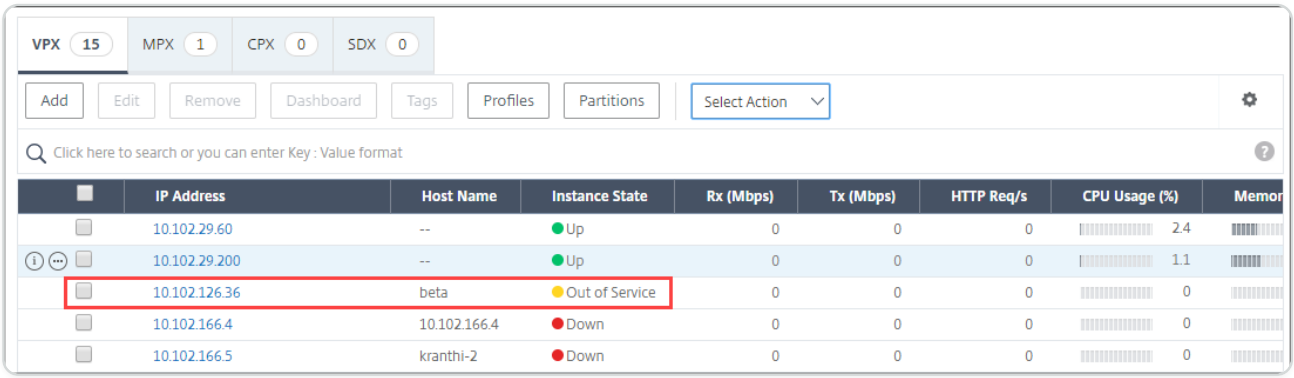
Unmanage an instance

If you want to stop the exchange of information between NetScaler® Application Delivery Management (ADM) and the instances in your network, you can unmanage the instances.

To unmanage an instance:

Navigate to **Infrastructure > Instances > NetScaler** \> **VPX** tab. In the list of instances, either right-click an instance and then select **Unmanage**, or select the instance and from the **Select Action** list, select **Unmanage**.

The status of the selected instance changes to **Out of Service** as shown in the following figure.



The instance is no longer managed by NetScaler ADM, and it no longer exchanges data with NetScaler ADM.

Trace the route to an instance

By tracing the route of a packet from the NetScaler® Application Delivery Management (ADM) to an instance, you can find information such as the number of hops necessary to reach the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

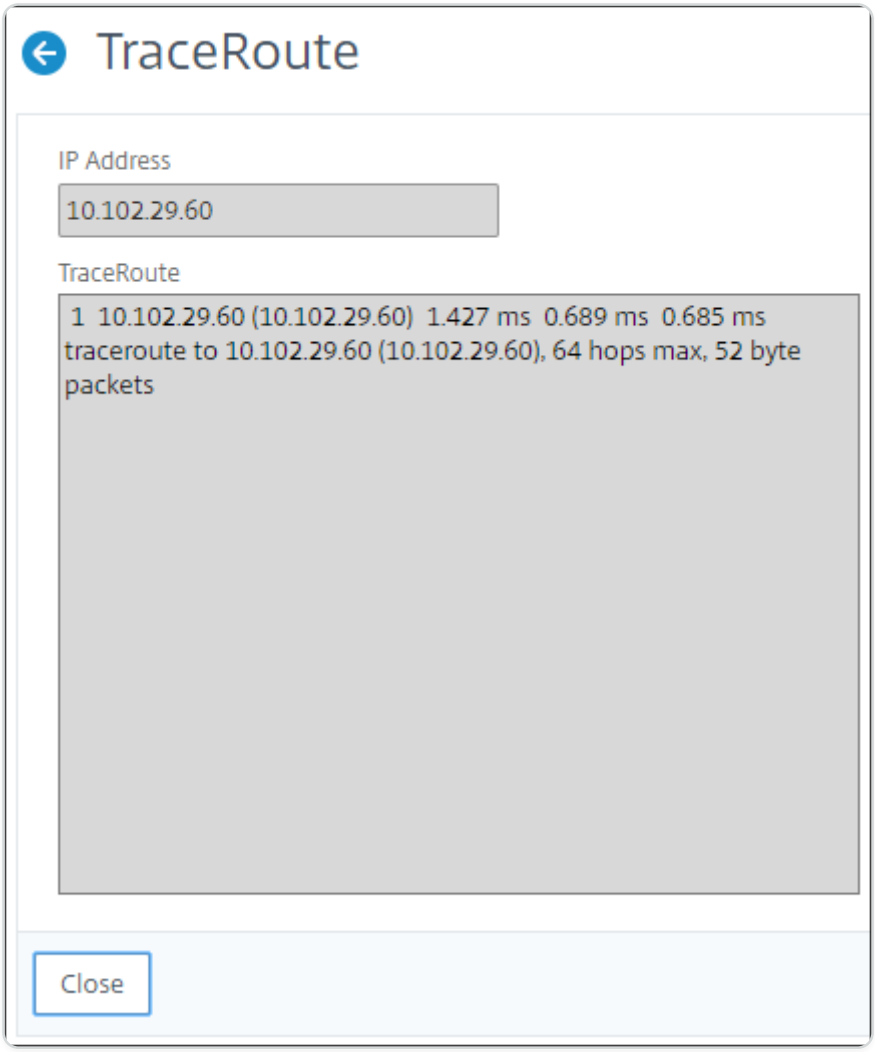
Traceroute traces the path of the packet from source to destination. It displays the list of network hops along with the host name and IP address of each entity in the route.

Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, traceroute shows where the problem exists.

To trace the route of an instance:

1. In NetScaler ADM, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. In the list of instances, either right-click an instance and then select **TraceRoute** or select the instance and from the **Select Action** menu, click **TraceRoute**.

The **TraceRoute** message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.



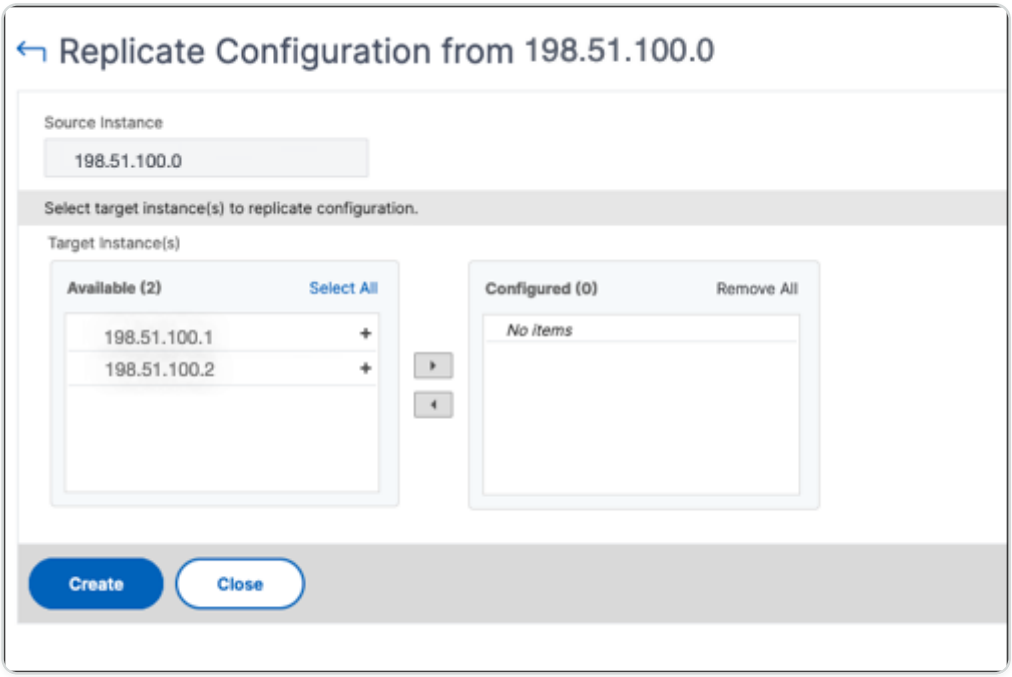
Replicate configurations from one NetScaler instance to another

You can use the Replicate Configuration feature of NetScaler® ADM to copy configurations from a NetScaler instance and replicate it on a single instance or many instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To replicate configurations from one instance to other NetScaler instances

1. Navigate to **Infrastructure > Instances > NetScaler**. Select the source instance whose configurations you want to replicate on other instances and from the **Select Action** list, click **Replicate Configuration**.
2. In **Replicate Configuration**, select the target instance on which you want to apply the configurations from the source instance. You can replicate the configurations from a single source instance to a single instance or many target instances.



3. Click **Create**.

The replicated configurations are added to the list of NetScaler instances. To view the status of the replicated instances, click the refresh icon.

NOTE:

During replication, all the network IPs from the source instance are replicated to the target instance. If the target instance is in a different network from the source instance, the IPs in the target instance might not be reachable. When IPs are not reachable, the status of the entities in the target instance is shown as Down.

To view the status of the entities configured on your managed NetScaler instance, navigate to **Infrastructure > Network Functions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL certificate management

Any organization or individual website that requires handling confidential or sensitive information must have an SSL certificate. SSL certificate on a web server helps guarantee the authenticity of the web server to the connecting client. It not only authenticates a website's identity but also helps in generating the session key, which is used later for encryption of the entire session.

A Secure Socket Layer (SSL) certificate, which is a part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the Citrix Application Delivery Controller™ (ADC) appliance, is used to complete asymmetric key (or public key) encryption and decryption.

NetScaler® Application Delivery Management (ADM) provides you a unified console to automate the installation, updating, deletion, linking, and download of SSL certificates. It helps in retaining the reputation of the website and customer trust. NetScaler ADM now streamlines every aspect of certificate management for you. Through a unified console, you can configure automated policies to ensure the recommended issuer, key strength, protocol, and algorithms as per organization IT policies. By doing so, you can keep close watch on certificates that are unused or about to expire.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as Verisign
- By generating a new SSL certificate and key on the NetScaler appliance

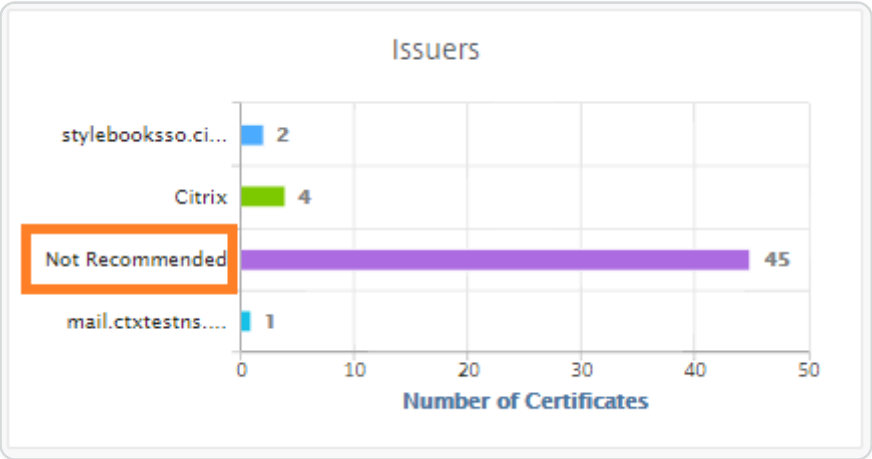
Enterprise SSL policy settings

Every enterprise has its own SSL policy and defines the requirements that all SSL Certificates must adhere to. Security has always been among the top priorities across all enterprise users and hence SSL settings play an important role.

For example, an ABC Company mandates that all certificates must have minimum key strengths of 2,048 bits and above. The certificates must be authorized by trusted CA or issuers. Administrators must check all such SSL parameters to ensure that the certificates abide by the company policy. It is a tedious job to verify each certificate manually. To overcome this scenario, the NetScaler ADM helps you to configure enterprise SSL policy settings, and shows any non-compliance certificate with the "Not Recommended" tag.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view the summary of the non-compliance (Not Recommended) certificates on the SSL Dashboard.



NOTE

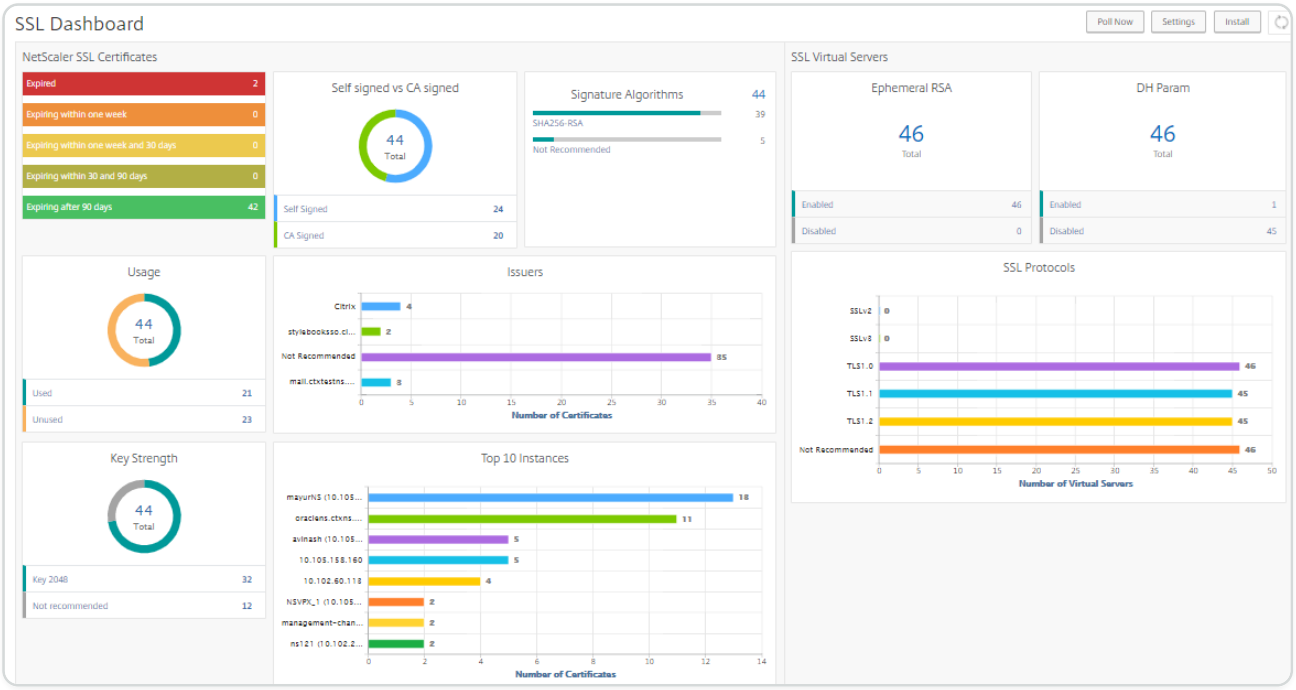
The “Not Recommended” certificates are categorized based on different parameters, and you can view them in relevant components.

How the NetScaler ADM certificate works

SSL Dashboard provides you a visual presentation of all the SSL certificates that are installed on different NetScaler instances. SSL dashboard includes the following information for each certificate installed on NetScaler instances. It is categorized based on the following:

- **Self-signed vs CA signed.** The self-signed vs CA signed section helps you to segregate the certificates into Self-signed certificates and, CA signed certificates.
- **Signature Algorithms.** This section segregates the SSL certificates based on signature algorithms being used for encryption.
- **Usage.** This section segregates your SSL certificates based on used and unused certificates. Unused certificates demand special attention as they might have been missed to be bound to the virtual servers.
- **Issuers.** This section segregates the SSL certificates based on the issuer of the certificates.
- **Key Strength.** This section segregates the SSL certificates based on the key strength of a private key.
- **Top 10 Instances.** This section provides the details of the top 10 NetScaler instances based on the number of SSL certificates installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SSL certificate management use cases

The following use cases describe how you can use the SSL certificate to manage and monitor the certificates across multiple NetScaler instances.

Install SSL certificates

Imagine, you have a fleet of NetScaler instances across, on which you have to deploy the required SSL certificates. NetScaler ADM provides you a unified console to deploy the SSL certificates across multiple NetScaler instances in one attempt.

For example, you might want to install some SSL certificates on one or more NetScaler instances. With this approach, you can minimize the manual intervention of installing the SSL certificate on each NetScaler instance. You can do a bulk installation of SSL certificates across one or more NetScaler instances.

To obtain a summary of the SSL certificates, log on to **NetScaler ADM**, and then navigate to **Infrastructure > SSL Dashboard**.

Notification settings for certificate expiry

In this use case, you might have many certificates across multiple NetScaler instances, and it becomes an overhead to track the expiry of each certificate. It is a tedious job for you to track each certificate manually and update it before it expires. To avoid such scenarios, you can configure NetScaler ADM to send the notifications or alerts to the configured email, pager, Slack, or

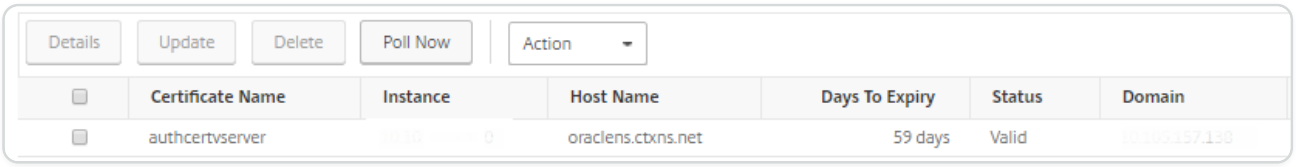
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ServiceNow profiles. This way you can stay abreast of the certificates expiry dates and renew the certificates well before the expiry dates.

For example, you might forget to track the certificate that is nearing expiry. And the certificate expires causing service outage, which might affect numerous applications to the users. With ADM certificate expiry notification settings, you can avoid such unforeseen scenarios.

You can view the summary and track the certificates that are nearing expiry on the **SSL Dashboard**.

To view the report of certificates expiring in any duration, you can click the tile to get the details of all such certificates expiring in that window.



Renewal of certificates

You can now renew the certificates from NetScaler ADM. You can either renew the existing certificates or create the certificates based on the following:

Update the existing certificate

In this use case, you have to update an existing certificate once you receive a renewed certificate from the certificate authority (CA). You can now update the existing certificates from NetScaler ADM without logging into NetScaler instances.

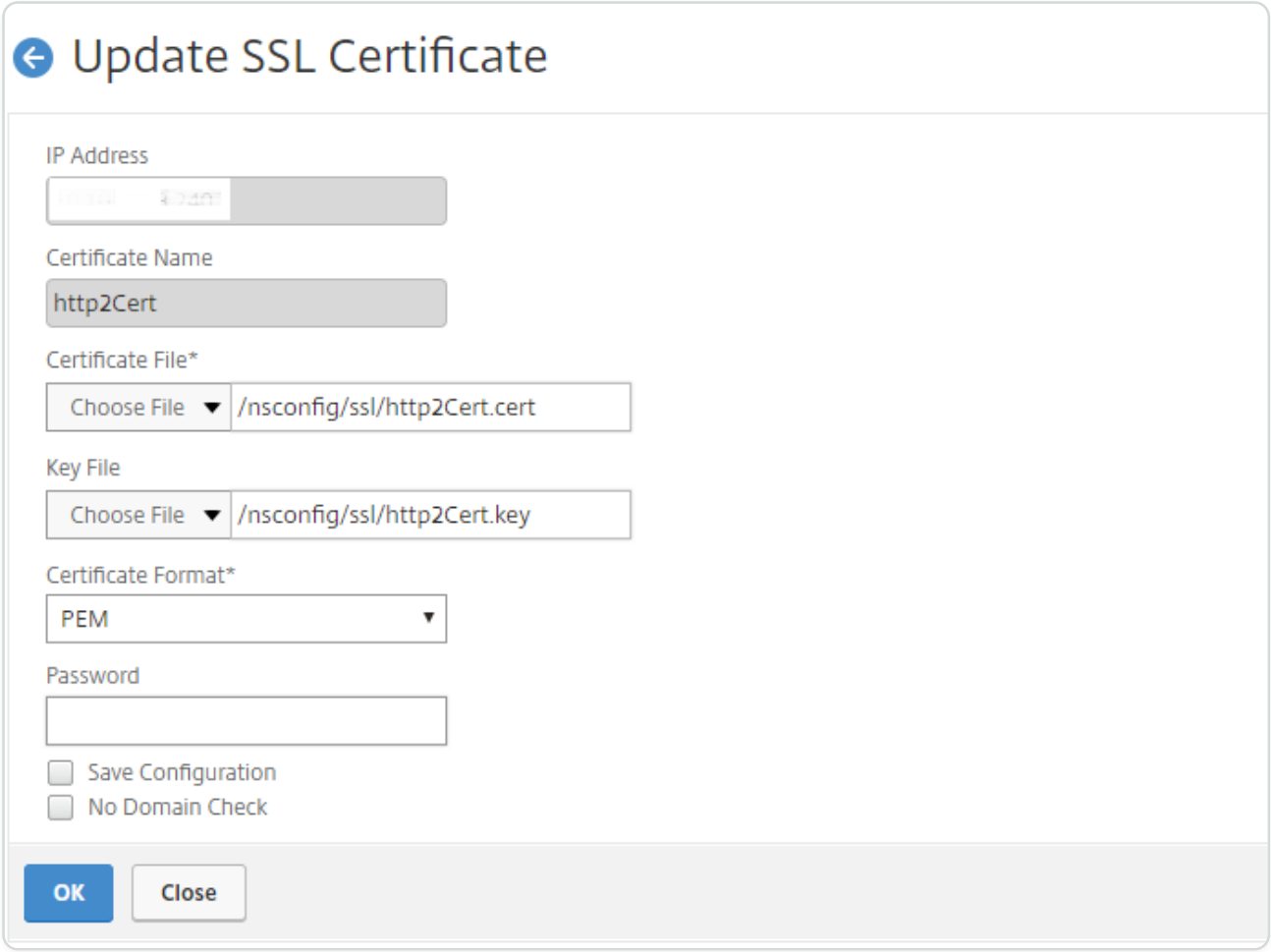
For example, there might be some changes or modifications to the existing certificates. The CA issues renewed certificates. Instead of going to the NetScaler appliance, you can now update the SSL certificate from NetScaler ADM.

To update any certificate, log on to NetScaler ADM, then navigate to **Infrastructure > SSL Dashboard**.

Select the certificate you want to update, and click **Update**.

You have an option to update the relevant fields of the selected certificate from NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



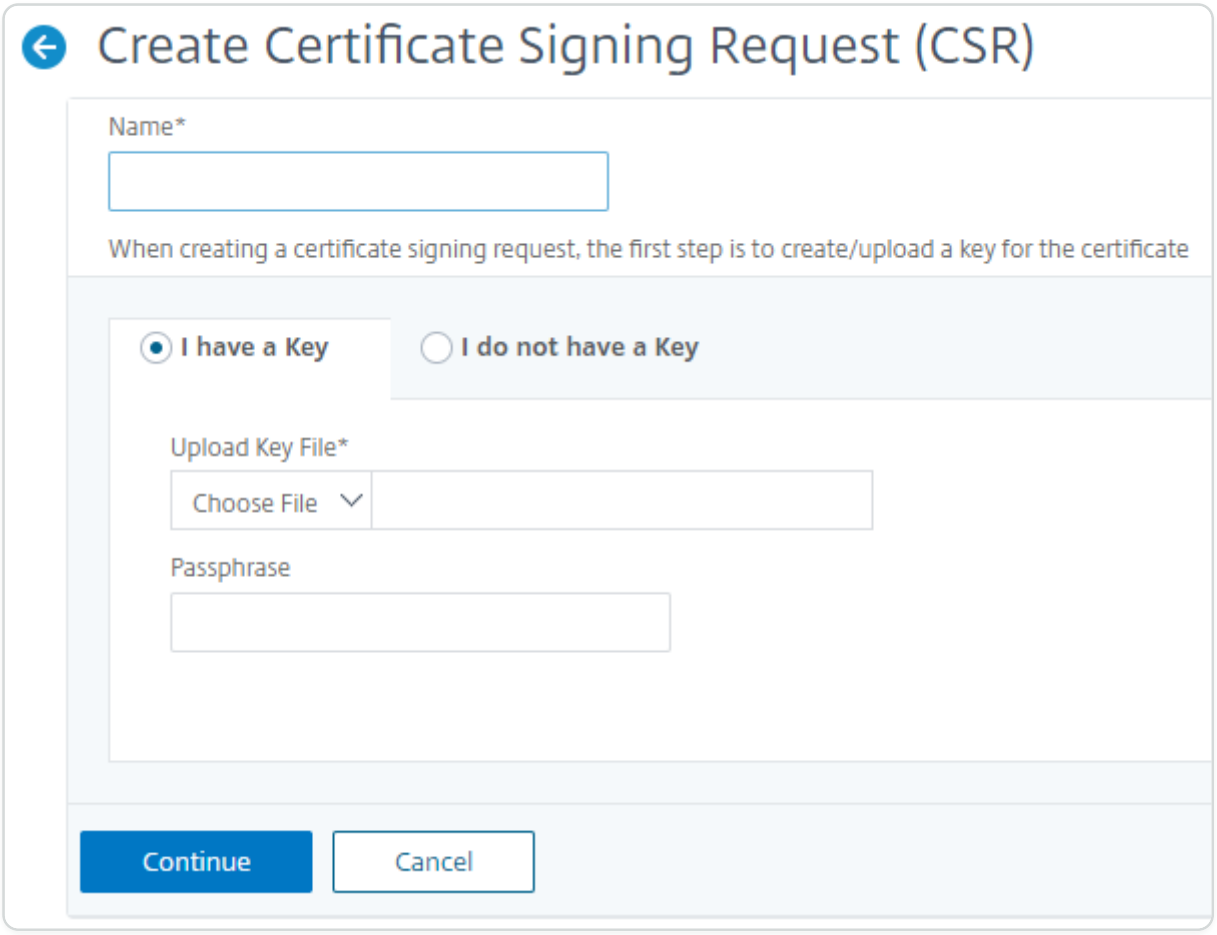
Create certificate signing request

Imagine a use case where one of the SSL certificates does not comply with the organization policies. You want to get a new certificate from the certification authority. You can now generate a certificate signing request (CSR) from NetScaler ADM. A CSR and a public key can be sent to a CA to obtain the SSL certificate.

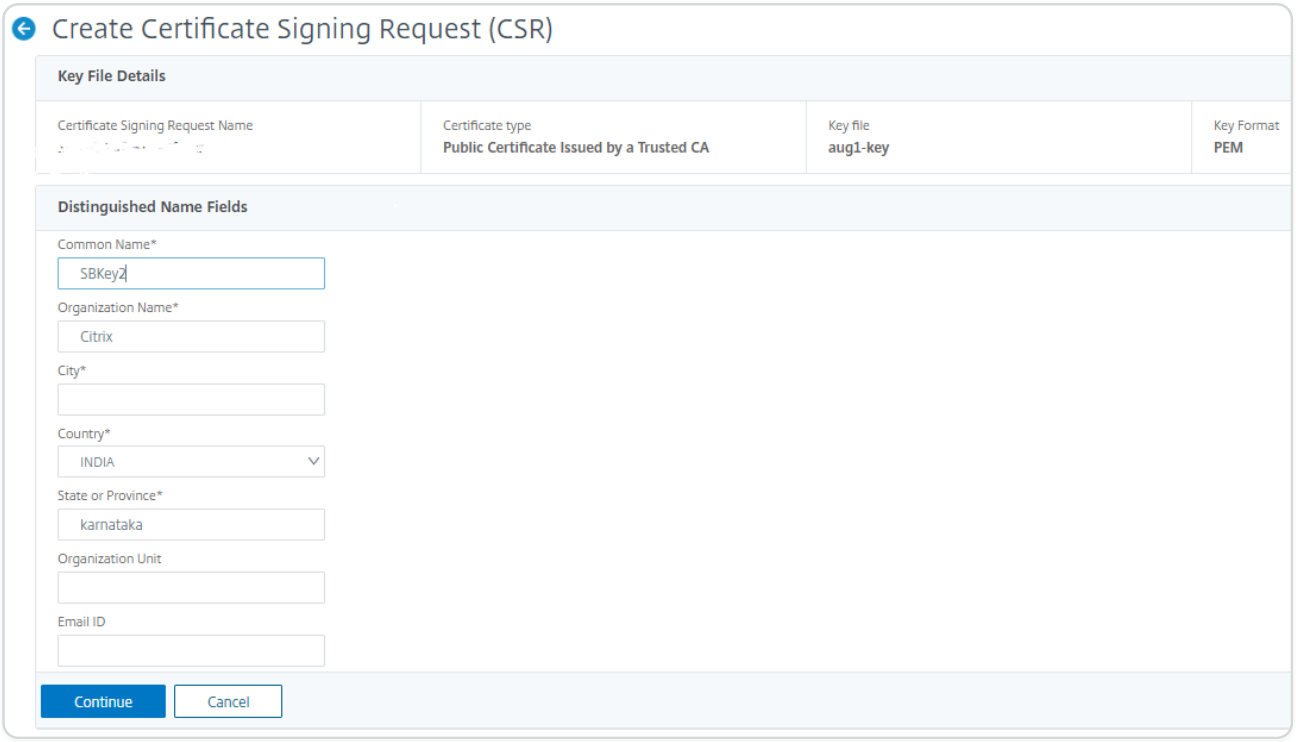
To determine and create CSR, select the desired certificate and click **Create CSR**.

You need to have a public or private key value pair. To upload a key, click **Choose File** and select from the list. To create a key, select **I do not have a Key option** and specify the relevant parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



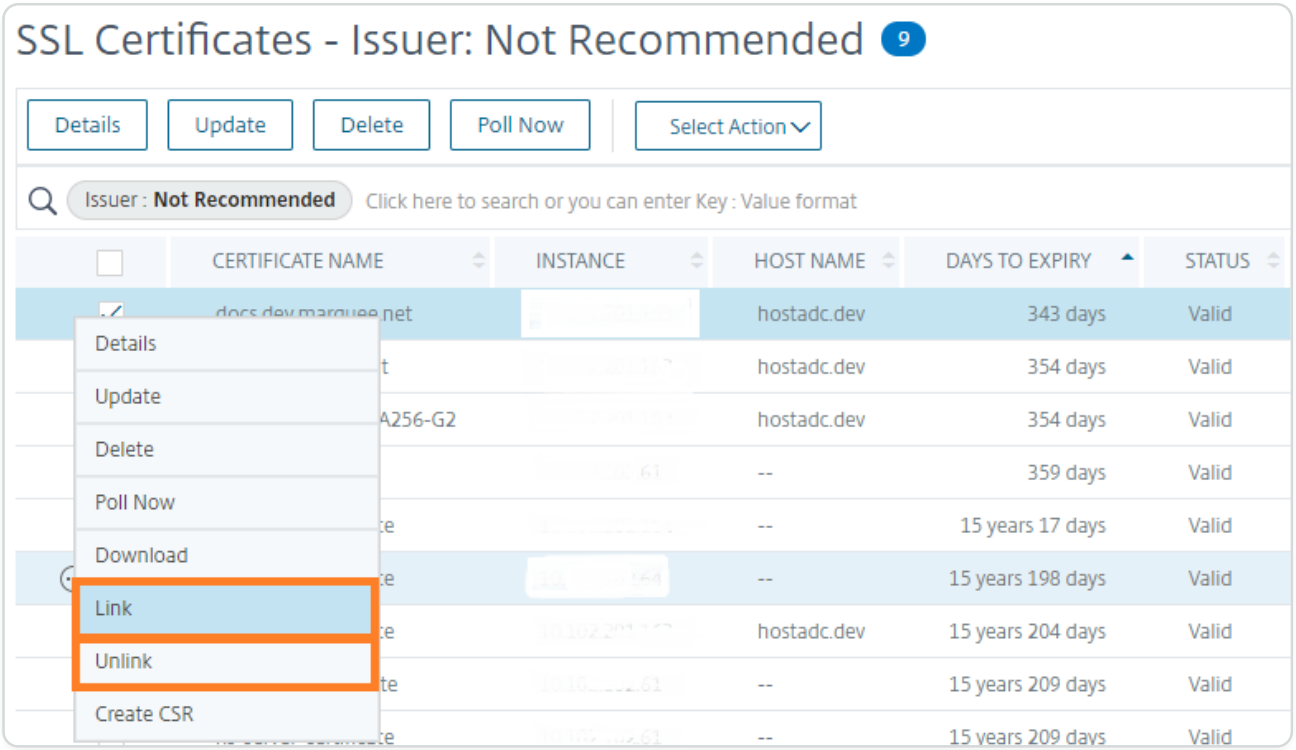
To give more details of the selected key like Common Name, Org Name, City, Country, State, Org Unit, and Email ID to create the CSR.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Link and unlink SSL certificates

You can bind multiple SSL certificates to each other to create a certificate bundle. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate.

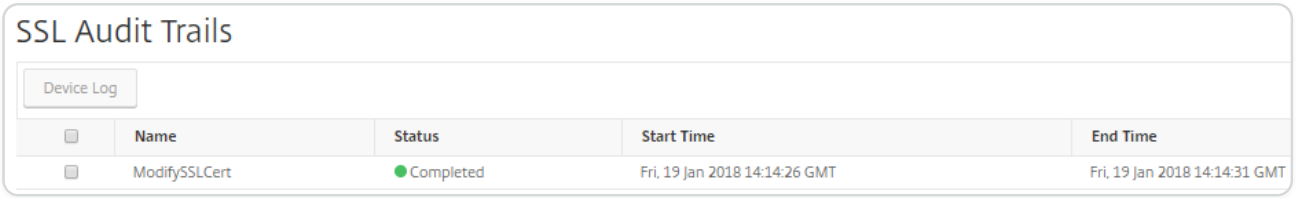


Audit logs

Audit Logs is a collection of text log files generated by the NetScaler ADM. It shows a history of SSL certificates that are added, modified, and changed by using NetScaler ADM to the specific NetScaler appliance. The Audit Logs also shows the IP Address of the NetScaler appliance, Status, Start Time, and End Time of the particular operation.

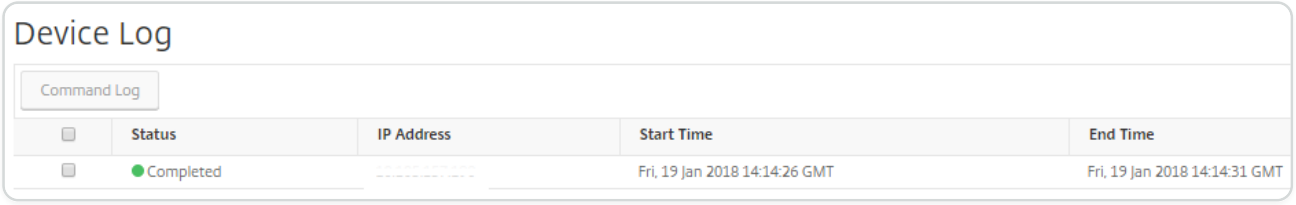
In this example, you might want to verify the change that has taken place over a period to the particular certificate. And you have an option to view the history of changes to the certificate over the Device Log and Command Log.

To determine the information of SSL certificates, on the **SSL Dashboard**, click **Audit Log**. The application summary includes the SSL certificates status with Start Time and End Time.

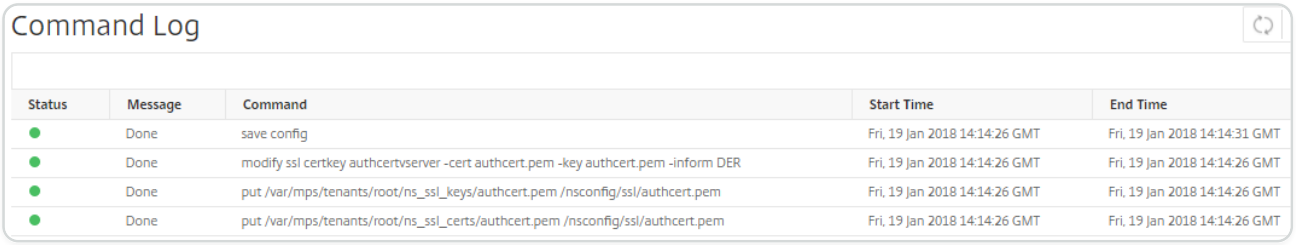


© 1997–2026 Citrix Systems, Inc. All rights reserved.

To determine the information of the NetScaler appliance of a particular SSL certificate, choose the relevant certificate check box of your choice. Click **Device Log**.



To view the information of command type, and message, click **Command Log**.



Use the SSL Dashboard

You can use the SSL certificate dashboard in NetScaler® Application Delivery Management (ADM) to view graphs that help you track certificate issuers, key strengths, and signature algorithms. The SSL certificate dashboard also displays graphs that indicate the following:

- Number of days after which certificates expire
- Number of used and unused certificates
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

To monitor SSL certificates

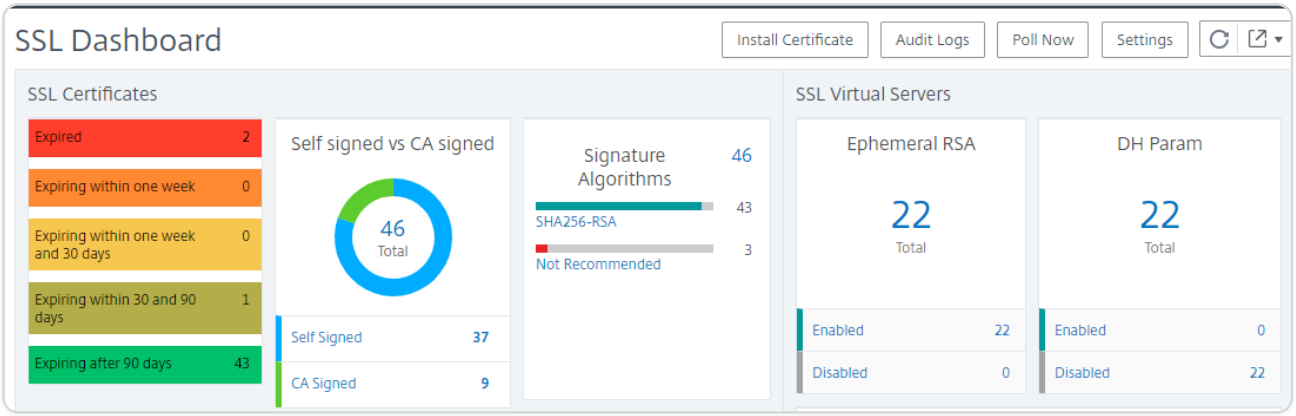
You might use the SSL dashboard on NetScaler ADM to monitor your certificates if your company has SSL Policy where you have defined certain SSL certificate requirements such as all certificates must have minimum key strengths of 2048 bits and a trusted CA authority must authorize it.

In another example, you might have uploaded a new certificate but forgotten to bind it to a virtual server. The SSL dashboard highlights the SSL certificates being used or not used. In the **Usage** section, you can see the number of certificates that have been installed, and the number of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

certificates being used. You can further click the graph, to see the certificates name, the instance on which it's being used, its validity, its signature algorithm, and so on.

To monitor SSL certificates in NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.



NetScaler ADM allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to NetScaler ADM. To do so,

1. Navigate to **Infrasturcture > SSL Dashboard**.
2. Click **Poll Now**.

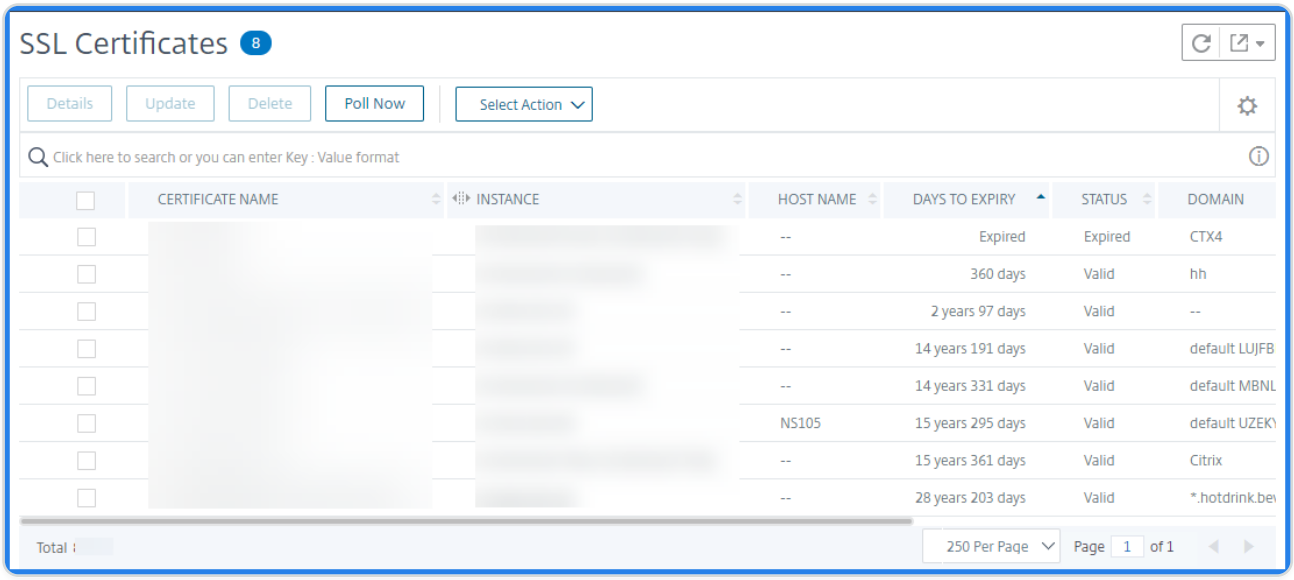
   On the **Poll Now** page, you can either poll all managed ADC instances or select specific instances.
3. Click **Start Polling**.

In **SSL Dashboard**, you can monitor the ADC SSL certificates, SSL virtual servers, and SSL protocols.

You can click the metrics on the dashboard to view details related to SSL certificates, SSL Virtual Servers, or SSL protocols.

For example, when you click the number under **Self signed vs CA signed** on the dashboard, the ADM GUI displays all the SSL certificates on the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler ADM SSL Dashboard also shows the distribution of SSL protocols that are running on your virtual servers. As an administrator, you can specify the protocols that you want to monitor through the SSL policy, for more information, see Configuring SSL Policies. The protocols supported are SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. The SSL protocols used on virtual servers appear in a bar chart format. Clicking a specific protocol displays a list of virtual servers using that protocol.

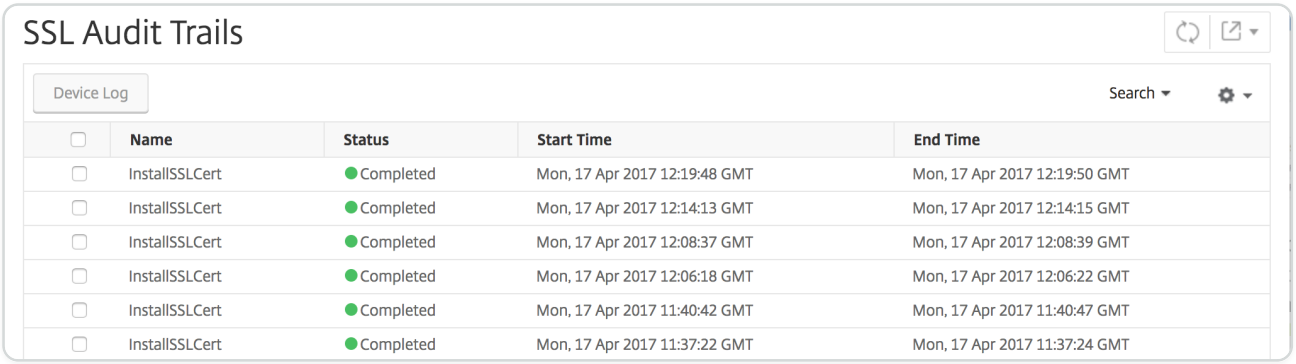
A donut chart appears after Diffie-Hellman (DH) or Ephemeral RSA keys are enabled or disabled on the SSL dashboard. These keys enable secure communication with export clients even if the server certificate does not support export clients, as in the case of a 1024-bit certificate. Clicking the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.

To view audit trails for SSL certificates

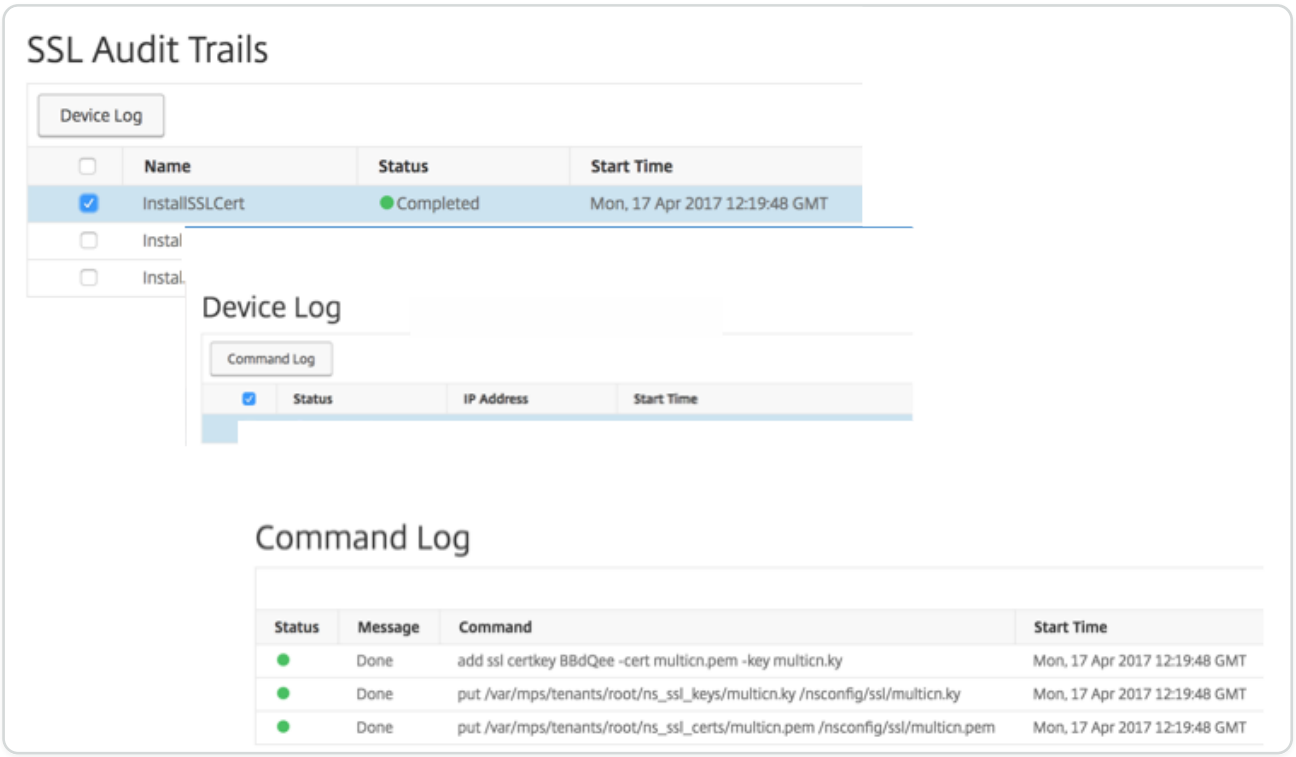
You can now view log details of SSL certificates on NetScaler ADM. The log details display operations performed using SSL certificates on NetScaler ADM such as: installing SSL certificates, linking and unlinking SSL certificates, updating SSL certificates, and deleting SSL certificates. Audit trail information is useful while monitoring SSL certificate changes done on an application with multiple owners.

To view an audit log for a particular operation performed on NetScaler ADM using SSL certificates, navigate to **Infrastructure > SSL Dashboard** \> and click **Audit Logs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For a particular operation performed using SSL certificate you can view its status, start time, and end time. Furthermore, you can view the instance on which the operation was performed and the commands run on that instance.



To exclude default NetScaler certificates on the SSL Dashboard

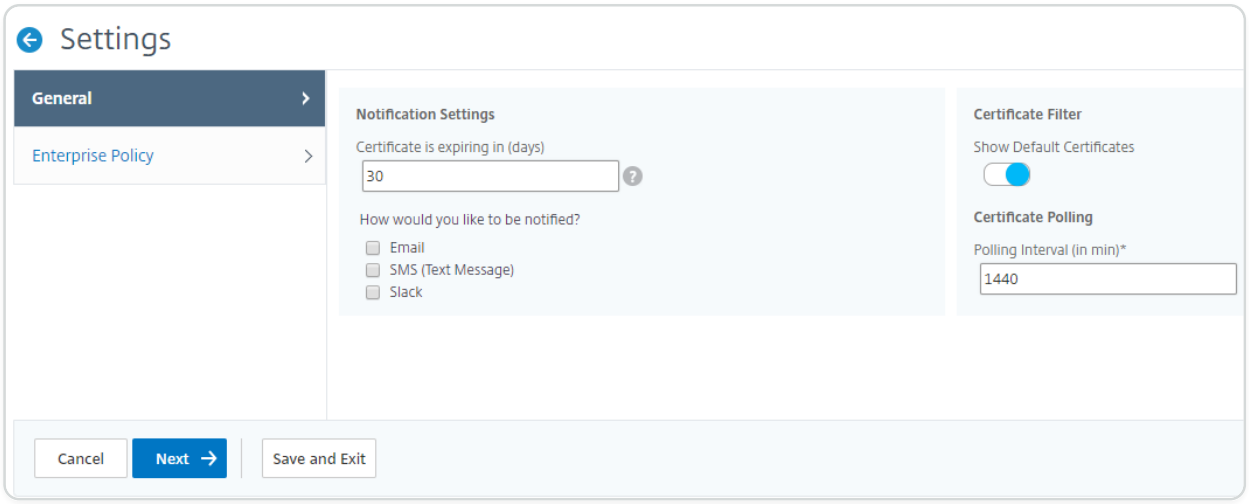
NetScaler ADM allows you to show or hide default NetScaler certificates showing up on the SSL Dashboard charts based on your preferences. By default, all certificates are displayed on the SSL dashboard including default certificates.

To show or hide default certificates on the SSL dashboard:

1. Navigate to **Infrastructure > SSL Dashboard** in the NetScaler ADM GUI.
2. On **SSL Dashboard** page, click **Settings**.
3. On the **Settings** page, select **General**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Type the number of days when the certificate expires to receive notification about certificate expiry.
5. Select the method of notification and create the respective profiles.
6. In the **Certificate Filter** section, clear the **Show Default Certificates** check box and click **Save and Exit**.



View, upload, and download SSL files

To view SSL files on NetScaler ADM, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler ADM**.

In this page, you can view, upload, and download the following files on NetScaler ADM:

- SSL certificates
- SSL keys
- SSL CSRs

To view and download SSL files on a NetScaler instance, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler**.

You can access the SSL files only after the NetScaler instances have been backed up, either manually or through a scheduled backup process.

IMPORTANT:

To enable the SSL files download from ADC instances, enable the **Instance SSL certificates** feature. For more information, see Enable or disable ADM features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set up notifications for SSL certificate expiry

As a security administrator, you can set up notifications to inform you when certificates are about to expire and to include information about which Citrix Application Delivery Controller™ (ADC) instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

For example, you can set an email notification to be sent an email distribution list 30 days before your certificate is due to expire.

To set up notifications from NetScaler® ADM:

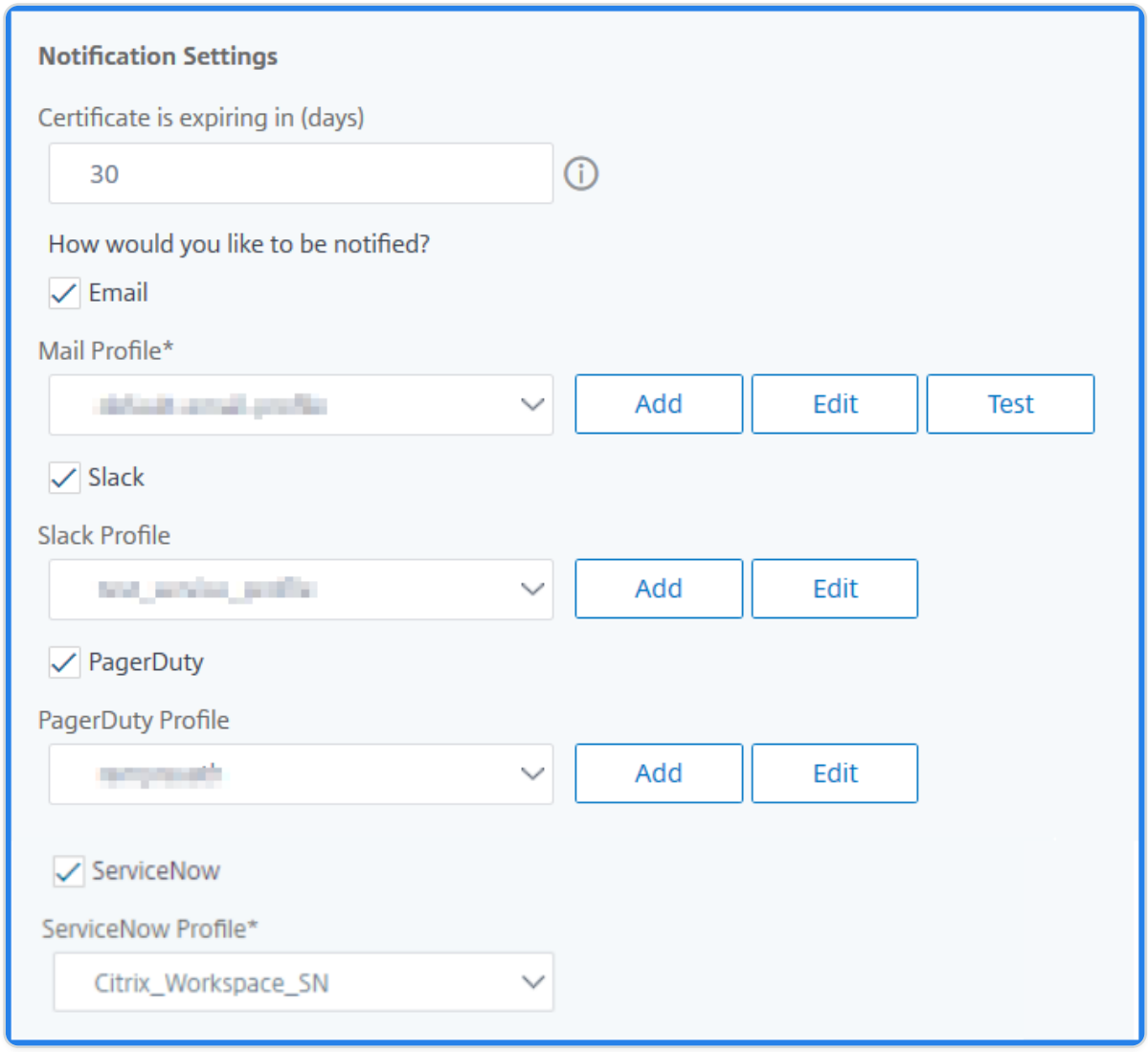
1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. On the **SSL Dashboard** page, click **Settings**.
3. On the **SSL Settings** page, click the **Edit** icon .
4. In the **Notification Settings** section, specify when you want to send the notification in terms of number of days prior to the expiration date.
5. Choose the type of notification you want to send. Select the notification type and the distribution list from the drop-down menu. The notification types are as follows:

   - **Email** – Specify a mail server and profile details. An email is triggered when your certificates are about to expire.
   - **SMS** – Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your certificates are about to expire.
   - **Slack** - Specify Slack profile details.
   - **PagerDuty alerts** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
   - **ServiceNow** - A notification is sent to the default ServiceNow profile when your certificates are about to expire.

   IMPORTANT

   Ensure Citrix Cloud ITSM Adapter is configured for ServiceNow and integrated with NetScaler ADM. For more information, see Integrate NetScaler ADM with ServiceNow instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Save and Exit**.

NetScaler ADM now sends SSL certificate expiry trap to external trap destination server when your SSL certificates are due for expiry. NetScaler ADM sends a trap when the following two conditions are satisfied:

- You have configured the number of days for the certificate expire in SSL dashboard settings page.
- You have added the trap destination.

You can set trap destinations by navigating to **Settings > SNMP > Trap Destinations**. Type the IP address of the destination SNMP server where the traps are sent. Enter the port number and type "public" (without quotes) as the community string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update an installed certificate

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from NetScaler Application Delivery Management (ADM) without needing to log on to individual Citrix Application Delivery Controller™ (ADC) instances.

To update an SSL certificate, key, or both from NetScaler® ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. On the **SSL Certificates** page, select a certificate and click **Update**. Alternatively, click the SSL certificate to view its details, and then click **Update** in the upper-right corner of the **SSL Certificate** page.
4. On the **Update SSL Certificate** page, make the required modifications to the certificate, key, or both and click **OK**.

Install SSL certificates on a NetScaler instance

Before installing SSL certificates on Citrix Application Delivery Controller™ (ADC) instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed with secure signature algorithms.

To install an SSL certificate from another NetScaler Instance:

You can also import a certificate from a chosen NetScaler instance and apply it to other targeted NetScaler instances from the NetScaler Application Delivery Management (ADM) GUI.

1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the SSL dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:

   a. Certificate Source Select the option to **Import from Instance**.

      - Choose the **Instance** that you want to import the certificate from.
      - Choose the **Certificate** from the list of all SSL certificate files on the instance.

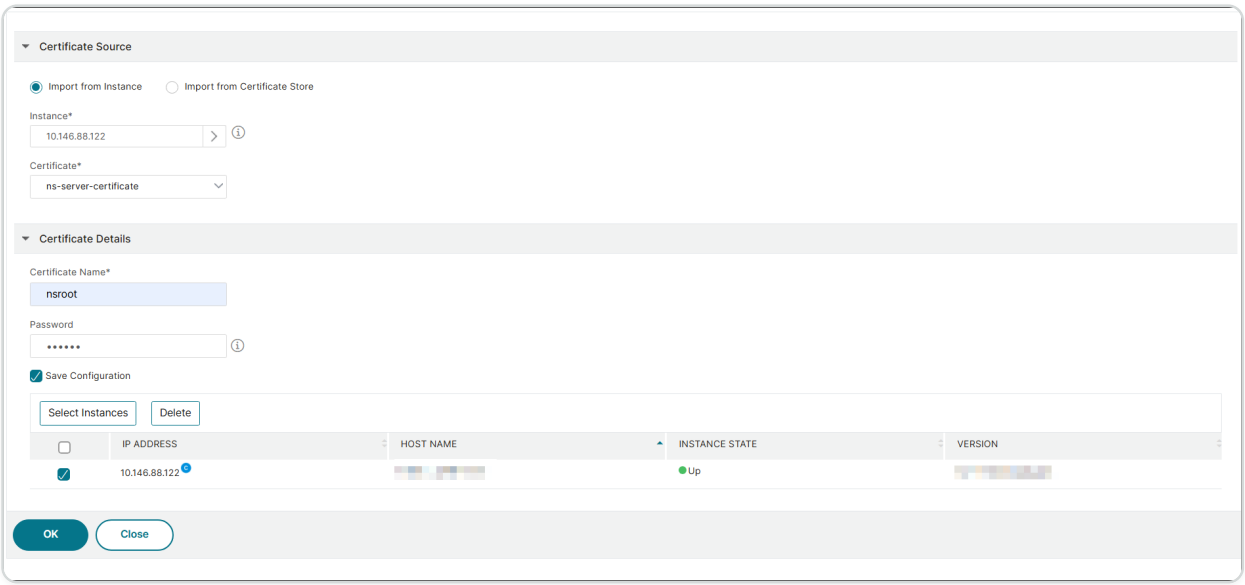
   b. Certificate Details

      - **Certificate Name**. Specify a name for the certificate key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Password**. Password to encrypt the private key. You can use this option to upload encrypted private keys.

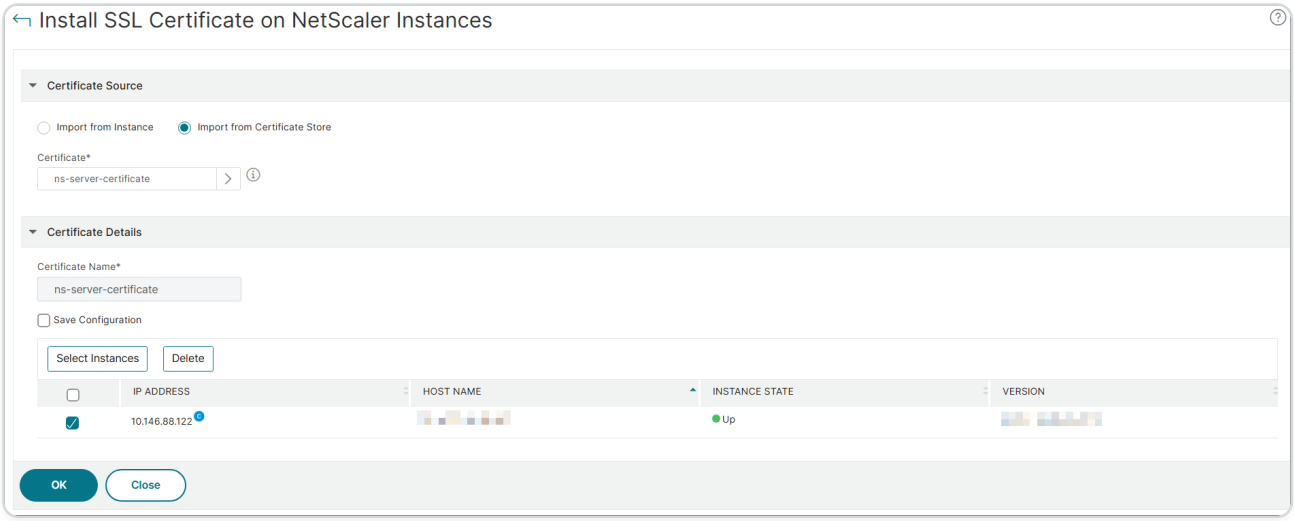
4. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.
5. Click **OK**.



To install an SSL certificate from NetScaler® ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instance** page, select **Upload Certificates File** and specify the following parameters:
   - **Certificate File** - Upload an SSL certificate file by selecting either **Local** (your local machine) or **Appliance** (the certificate file must be present on the NetScaler ADM virtual instance).
   - **Key File** - Upload the key file.
   - **Certificate Name** – Specify a name for the certificate key.
   - **Password** - Password to encrypt the private key. You can use this option to upload encrypted private keys.
   - **Select Instances** - Select the NetScaler ADM instances on which you want to install your certificates.
4. To save the configuration for future use, select the **Save Configuration** check box.
5. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate will be used. It contains information that will be included in the certificate such as the name of your organization, common name (domain name), locality, and country.

To create a CSR using NetScaler® ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select **Create CSR** from the **Select Action** list.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:
   - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the NetScaler ADM virtual instance).
   - **Create a key** - Select the I do not have a Key option, and then specify the following parameters:

Encryption Algorithm	Type of key. For example, RSA.
Key File Name	Name for your file in which the RSA key is stored.
Key Size	Key size in bits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Public Exponent Value	Choose either **3** or **F4** from the drop-down list provided. This value is part of the cipher algorithm that is required to create your RSA key.
Key Format	Be default PEM is selected. PEM is the recommended key format for your SSL certificate.
PEM Encoding Algorithm	In the drop-down list, select the algorithm (**DES** or **DES3**) that you want to use to encrypt the generated RSA key. If you select this algorithm, you'll need to provide a PEM Passphrase.
PEM Passphrase	If you've chosen the PEM Encoding Algorithm, enter a passphrase.
Confirm PEM Passphrase	Confirm your PEM passphrase.

5. Click **Continue**.
6. On the following page, provide more details.

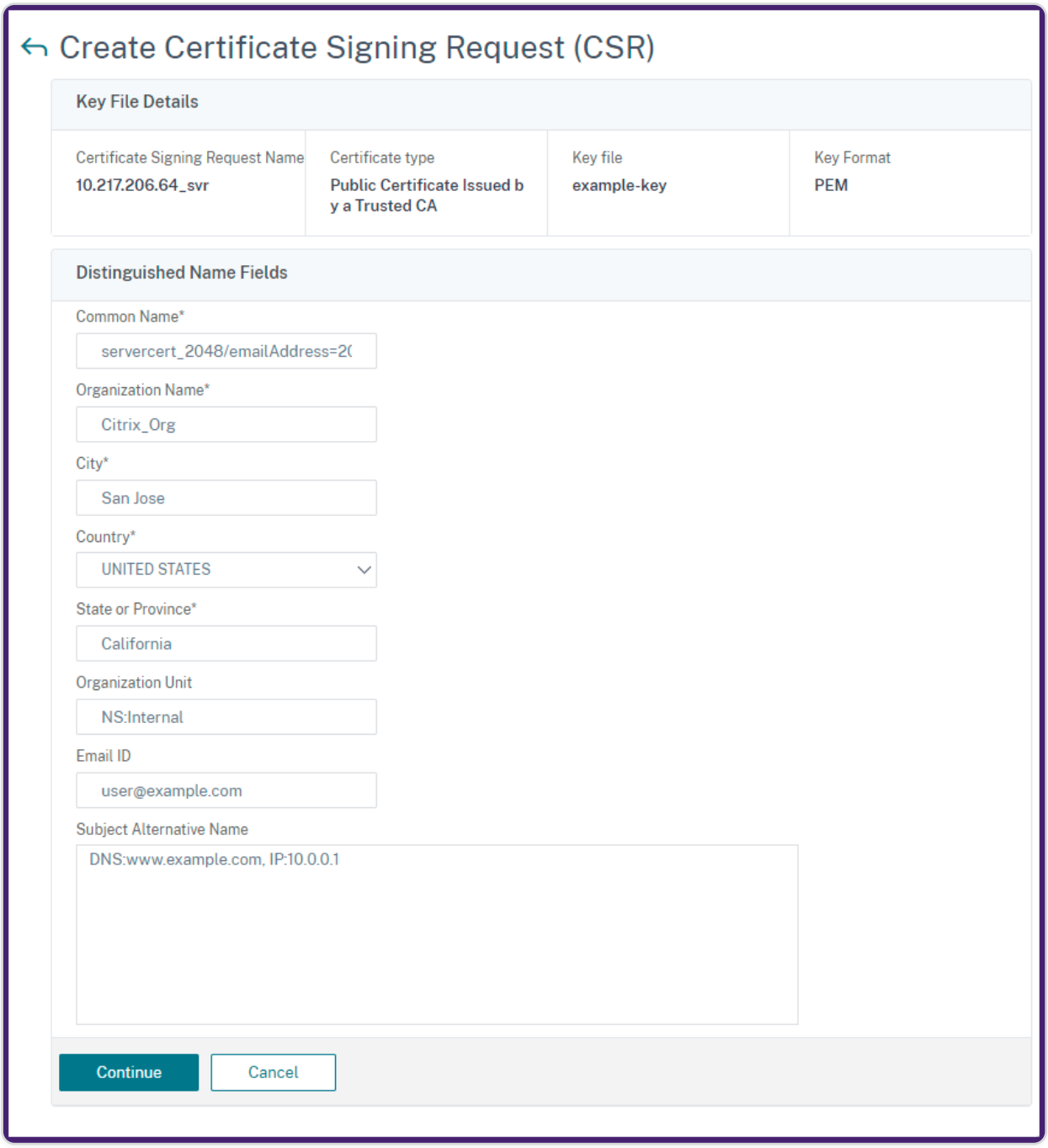
   Most fields have default values extracted from the subject of the selected certificate. The subject contains details such as the common name, organization name, state, and country.

   In the **Subject Alternative Name** field, you can specify multiple values, such as domain names and IP addresses with a single certificate. The Subject Alternative names help you secure multiple domains with a single certificate.

   Specify the domain names and IP addresses in the following format:

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this example, it secures `10.0.0.1` and `www.example.com`.

Review the fields and click **Continue**.

NOTE

Most CAs accept certificate submissions by email. The CA returns a valid certificate to the email address from which you submit the CSR.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Link and unlink SSL certificates

You create a certificate bundle by linking multiple certificates together. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate. For example, if you want to link certificate A to certificate B, the “issuer” of certificate A must match the “domain” of certificate B.

To link one SSL certificate to another certificate using NetScaler® ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select **Link** from the **Action** drop-down list.
4. From the list of matched certificates, select the certificate to which you want to link, and then click **OK**.

NOTE

If a matching certificate is not found, the following message is displayed: No certificate found to link.

To unlink an SSL certificate using NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select **Unlink** from the **Action** drop-down list.
4. Click **OK**.

NOTE

If the selected certificate is not linked to another certificate, the following message is displayed: Certificate does not have any CA link.

Configure an enterprise policy

You can configure an enterprise policy and add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificate keys in NetScaler Application Delivery

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Management (ADM). If any of the certificates installed on your Citrix Application Delivery Controller™ (ADC) instance have not been added to the enterprise policy, the SSL certificate dashboard displays the issuer of those certificates as **Not Recommended**.

Also, if the certificate key strength does not match the recommended key strength in the enterprise policy, the SSL certificate dashboard displays the strengths of those keys as **Not Recommended**.

To configure an enterprise policy on NetScaler® ADM:

1. In NetScaler ADM, navigate to **Infrastructure** \> **SSL Dashboard**, and then click **Settings**.
2. On the SSL Settings page, click the **Edit** icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys.
3. Click **Save** to save your enterprise policy.

> **NOTE**
>
> The SSL dashboard displays only the **Signature Algorithms** that are selected through the **Settings** option and others are displayed as **Not Recommended**.

Poll SSL certificates from NetScaler instances

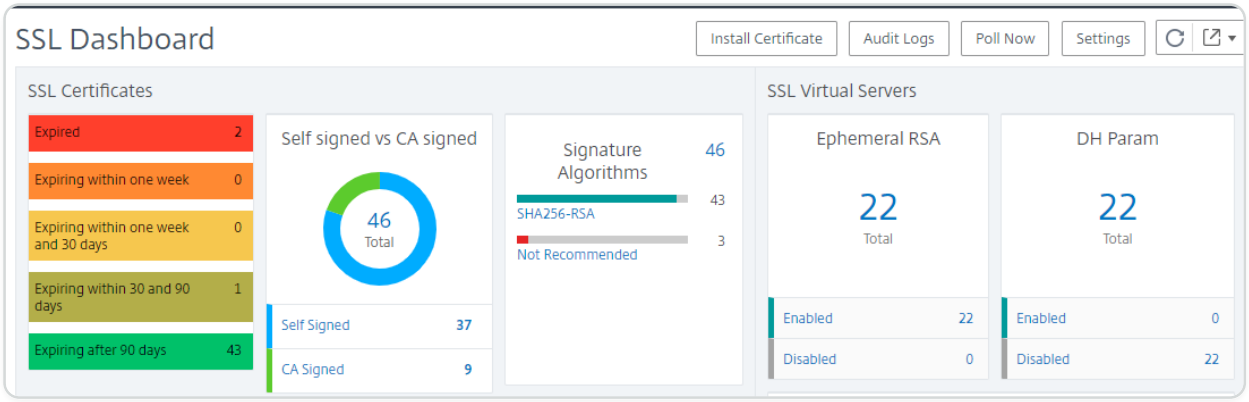
NetScaler Application Delivery Management (ADM) automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix Application Delivery Controller (ADC) instances. Polling all the NetScaler instances SSL certificates places a heavy load on the network.

Instead of polling all the NetScaler instances SSL certificates, you can manually poll only the SSL certificates of a selected instance or instances.

To poll SSL certificates on NetScaler instances:

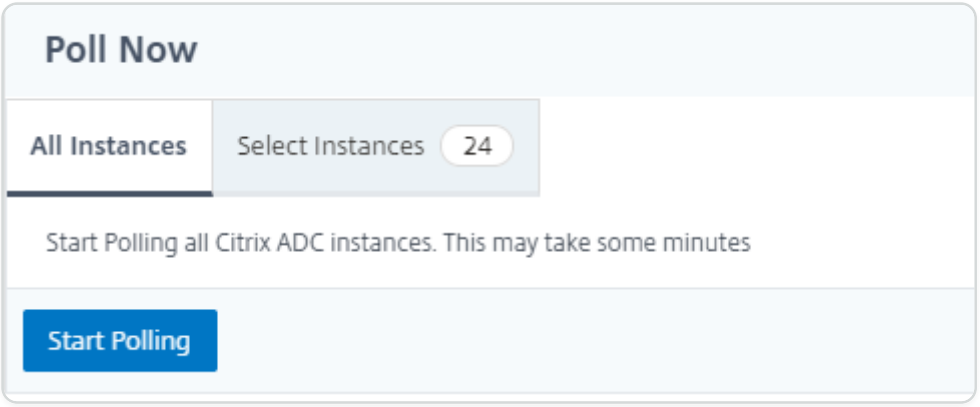
1. In NetScaler® ADM, navigate to **Infrastructure > SSL Dashboard**.
2. On **SSL Dashboard** page, in the top right-hand corner, click **Poll Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

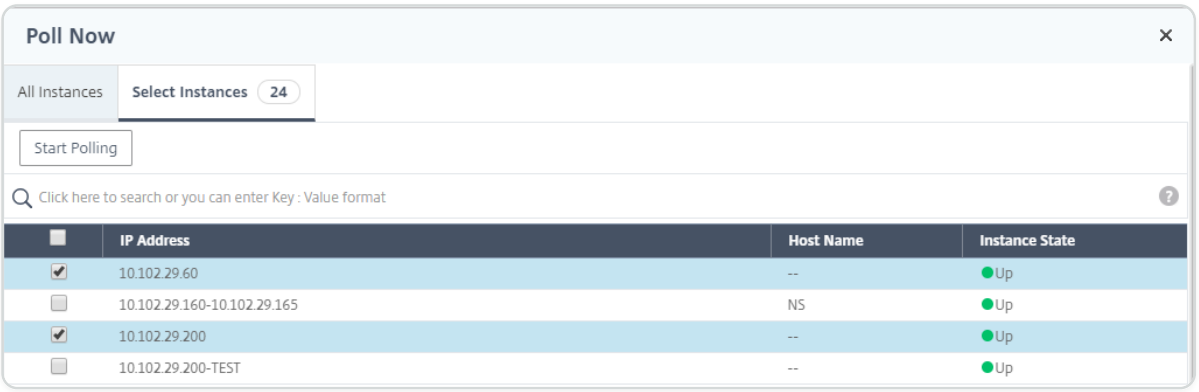


3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or to poll the selected instances.

   a. To poll the SSL certificates of all the NetScaler instances, select the **All Instances** tab and click **Start Polling**.



   b. To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.



Events

When the IP address of a Citrix Application Delivery Controller™ (ADC) instance is added to NetScaler Application Delivery Management (ADM), NetScaler ADM sends a NITRO call and implicitly adds itself as a trap destination for the instance to receive its traps or events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Events represent occurrences of events or errors on a managed NetScaler instance. For example, when there is a system failure or change in configuration an event is generated and recorded on the NetScaler ADM server. Events received in NetScaler ADM are displayed on the Events Summary page (**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**).

NetScaler® ADM also checks the events generated on instances to form alarms of different severity levels. These alarms are then displayed as messages, some of which might require immediate attention. For example, system failure can be categorized as a “Critical” event severity and would need to be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor the events, which can be many, generated across your NetScaler infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, NetScaler instances, category, failure objects, configuration commands, and messages.

You can also ensure multiple notifications are triggered for an event for a specific time interval, until the event is cleared. As an extra measure, you can customize your email with a specific subject line and user message, and upload an attachment.

Use events dashboard

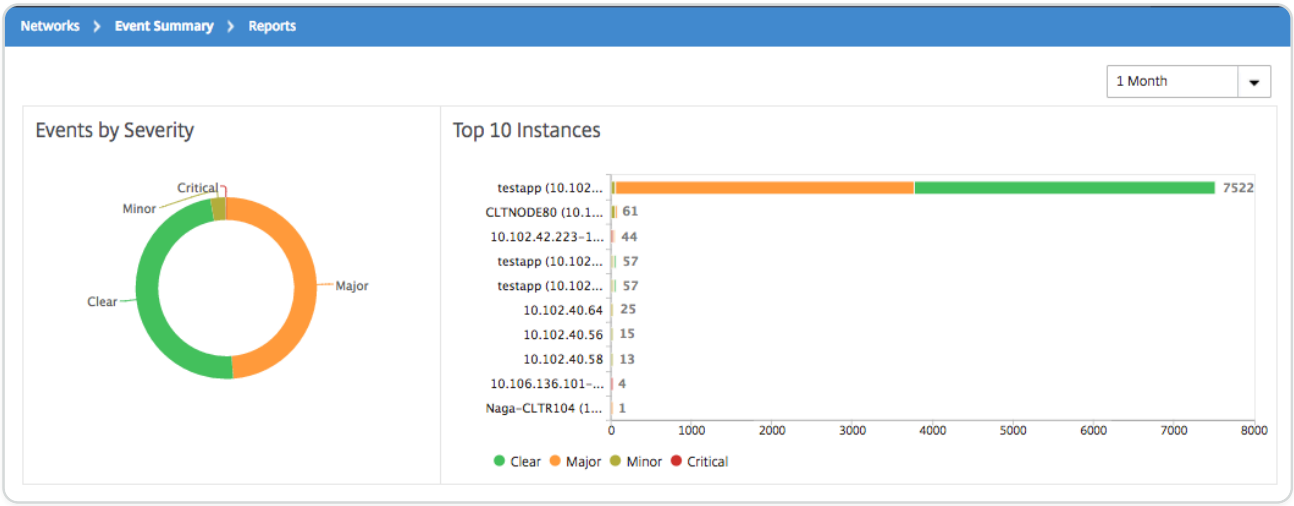
As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your Citrix Application Delivery Controller (ADC) instances, along with events and their severity on specific instances. You can use the NetScaler Application Delivery Management (ADM)’s events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

To view the details on the events dashboard:

Navigate to **Infrastructure > Events > Reports**.

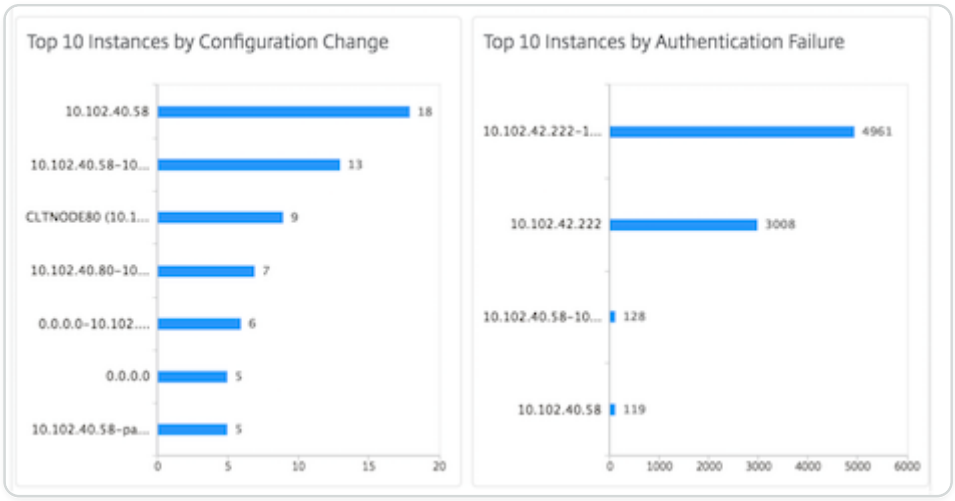
The Top 10 Devices graph on the dashboard displays a report of the top 10 instances by the number of events generated on them. You can click an instance on the graph to view further details of the event’s severity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



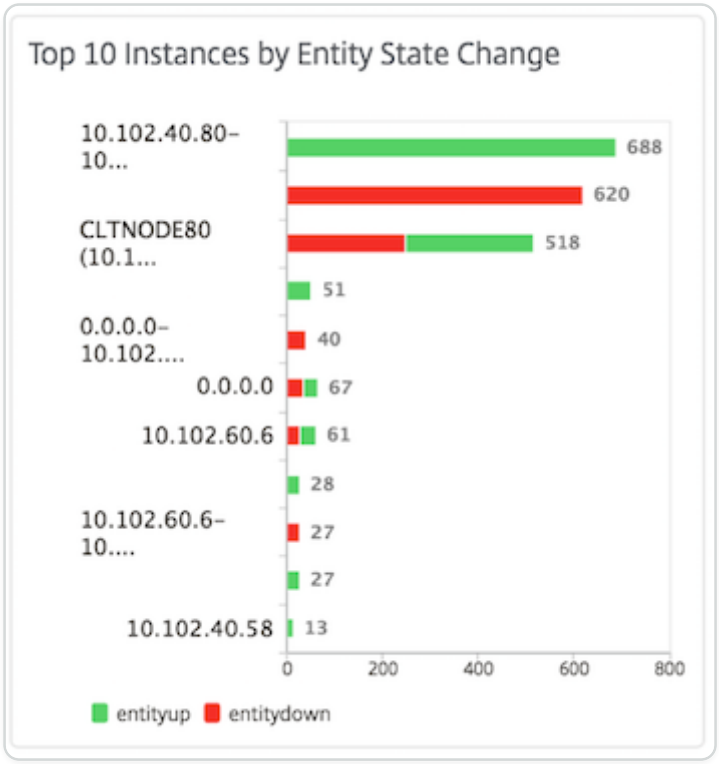
You can view more details by navigating to the NetScaler instance type (**Infrastructure > Events > Reports** \> **NetScaler/ NetScaler SDX**) to view the following:

- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure

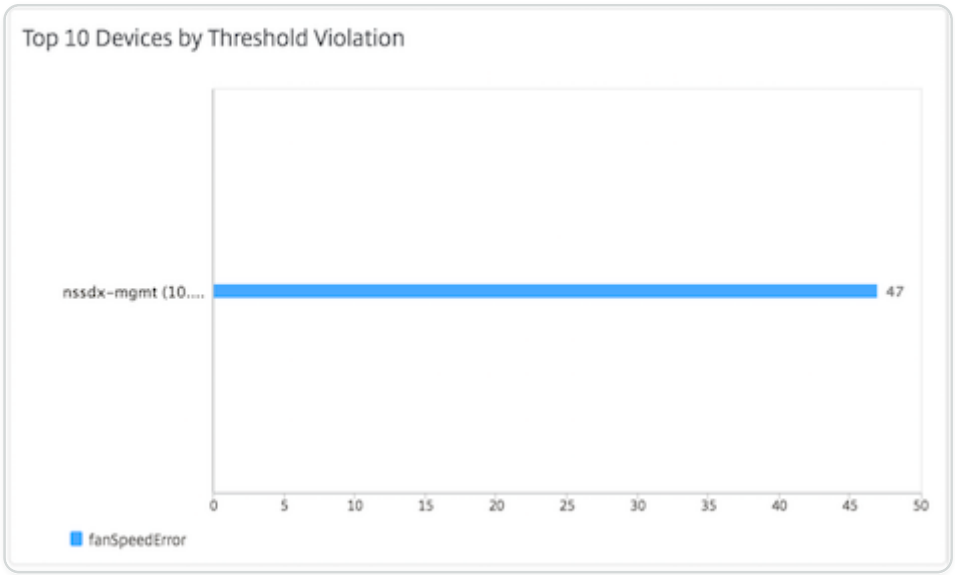


- Top 10 devices by entity state changes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Top 10 devices by threshold violation



Set event age for events

You can set the event age option to specify the time interval (in seconds). NetScaler® ADM monitors the appliances until the set duration and generates an event only if the event age exceeds the set duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note:

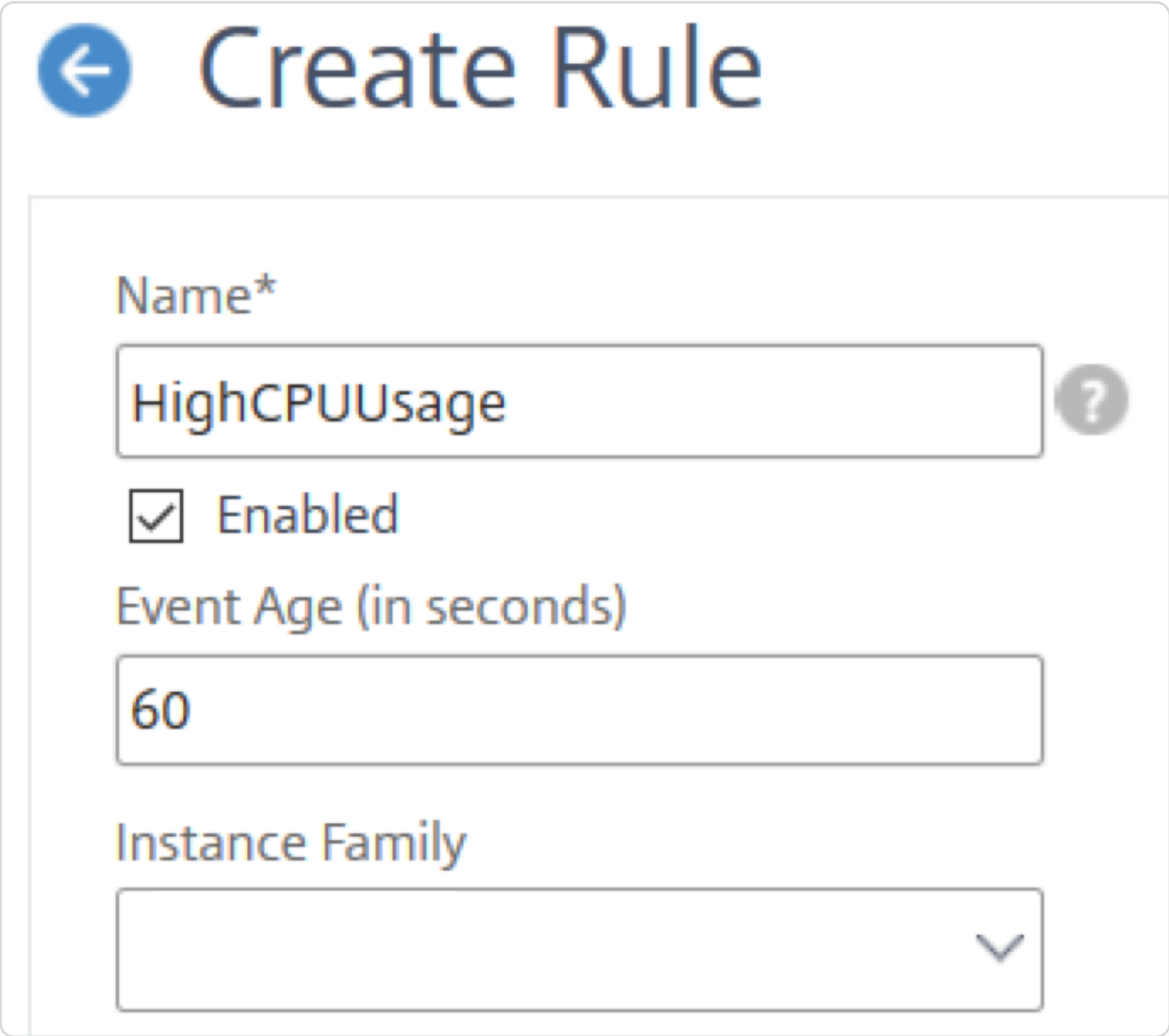
> The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event is occurred.

For example, consider that you want to manage various ADC appliances and get notified by email when any of your virtual servers goes down for 60 seconds or longer. You can create an event rule with the necessary filters and set the rule's event age to 60 seconds. Then, whenever a virtual server remains down for 60 or more seconds, you receive an email notification with details such as entity name, status change, and time.

To set event age in NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > Events > Rules**, and click **Add**.
2. On the **Create Rule** page, set the rule parameters.
3. Specify the event age in seconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Ensure to set all the co-related traps in the **Category** section and also set the respective severity in the **Severity** section when you set event age. In the preceding example, select the `entityup`, `entitydown`, and `entityofs` traps.

Schedule an event filter

After creating a filter for your rule, if you do not want the NetScaler® Application Delivery Management (ADM) server to send a notification every time the event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals such as daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

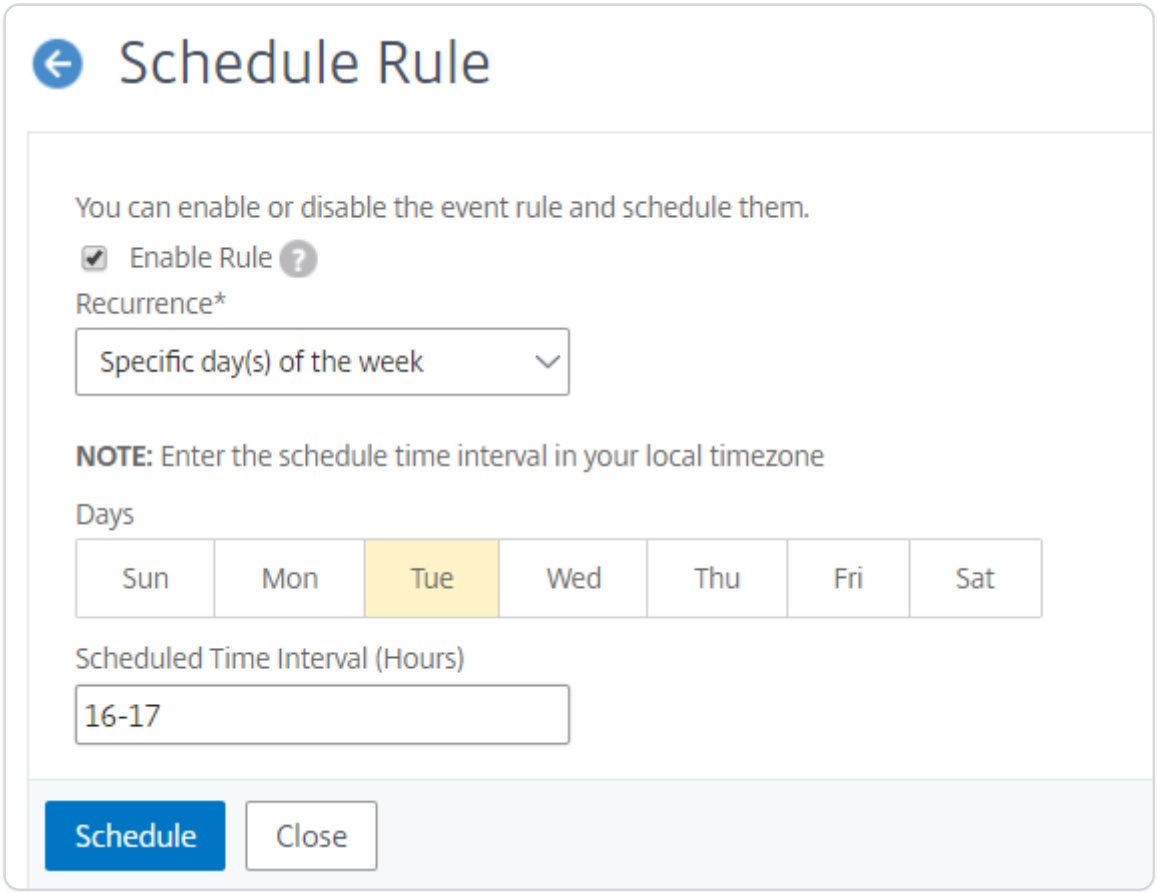
If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends a large number of email notifications when NetScaler ADM receives these traps. If

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using NetScaler ADM:

1. In the NetScaler ADM, navigate to **Infrastructure > Events > Rules**.
2. Select the rule you want to schedule a filter for, and click **View Schedule**.
3. On the **Scheduled Rule** page, click **Schedule** and specify the following parameters:
   - **Enable Rule** – Select this check box to enable the scheduled event rule.
   - **Recurrence** - Interval at which to schedule the rule. Select either a specific day of the week or a specific date in a month.
   - **Days**: Select the day of the week to run the rule. You can select multiple days.
   - **Dates**: Type in the dates. You can type multiple dates as comma-separated values.
   - **Scheduled Time Interval (Hours)** – Hours, at which to schedule the rule (use the 24-hour format).
4. Click **Schedule**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set repeated email notifications for events

To ensure that all critical events are addressed and no important email notifications are missed, you can opt to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

NOTE

Events can only be cleared automatically if there is an equivalent "clear" trap set and sent from your Citrix Application Delivery Controller™ (ADC) instance.

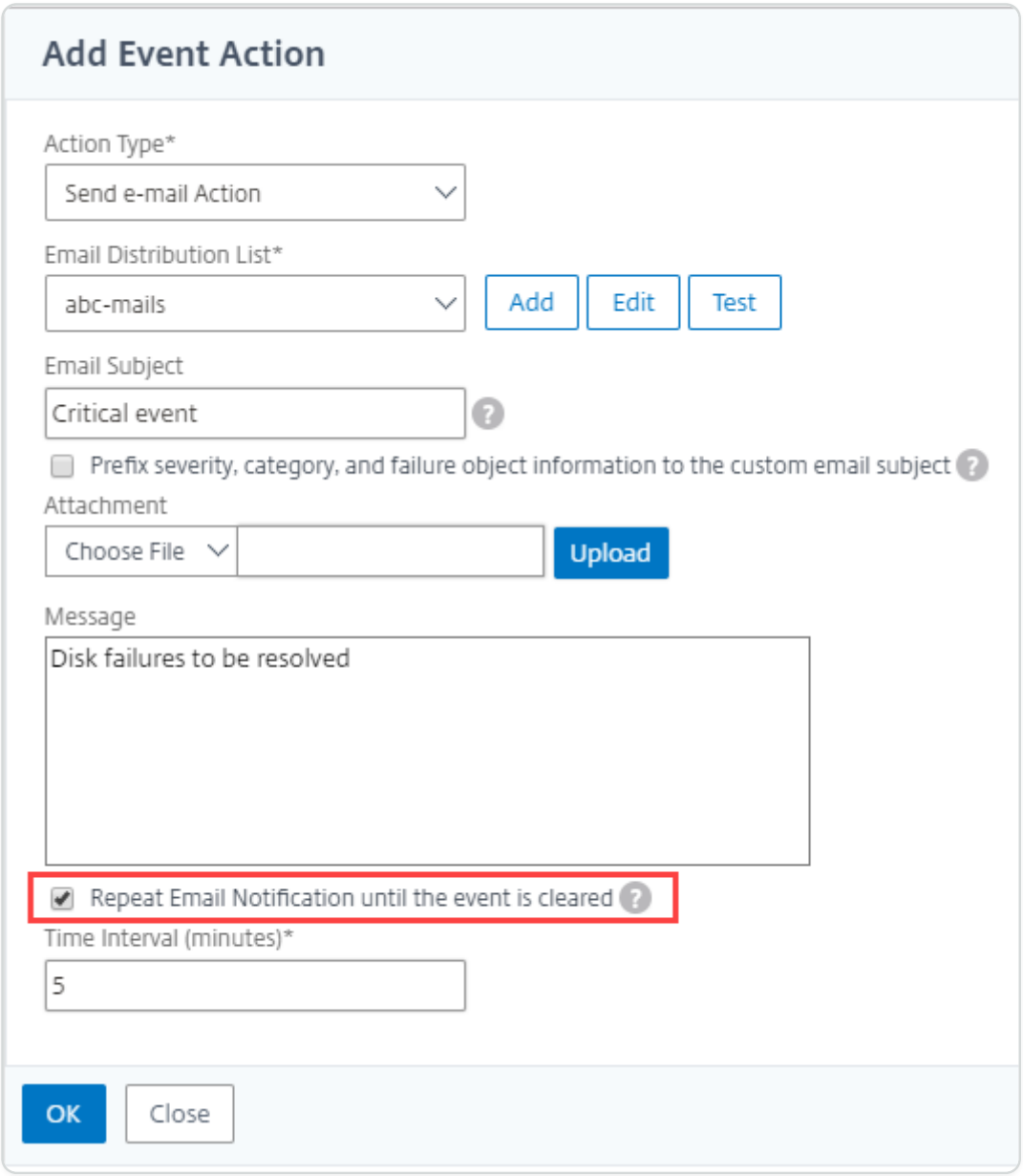
To clear an event manually, you can do the following:

- Navigate to **Infrastructure > Events > Event Summary**, choose a **Category** and select an event in the category and click **Clear**.
- Or, navigate to **Infrastructure > Events > Event Messages**. Choose an instance type and then, select an event from the grid below and click **Clear**.

To set repeated email notifications from NetScaler® ADM:

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters.
3. Under **Event Rule** Actions, click **Add Action**. Then, select **Send e-mail Action** from the **Action Type** drop-down list and select an **Email Distribution List**.
4. You can also add a customized subject line and user message, and upload an attachment to your email when an incoming event matches the configured rule.
5. Select the **Repeat Email Notification until the event is cleared** check box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Suppress events

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.

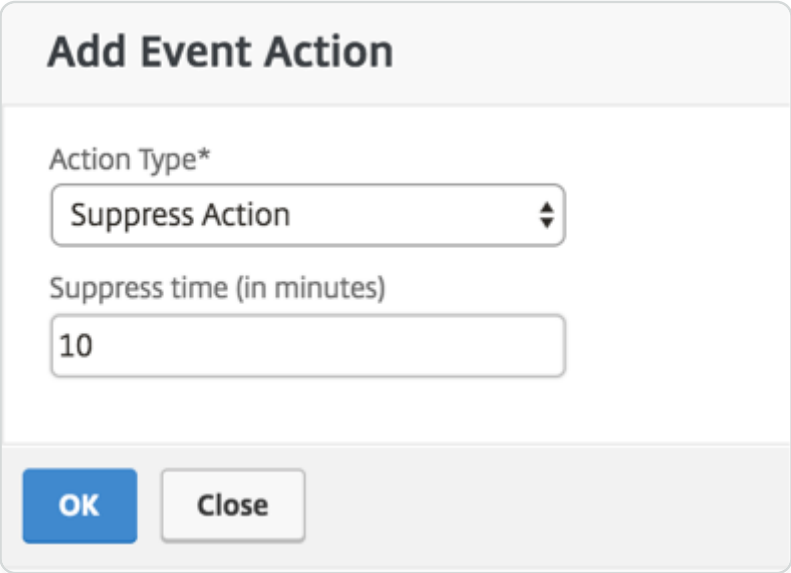
Note:

> You can also configure the suppress time as 0 minutes and it means infinite time. If you do not specify any time duration, then NetScaler® ADM considers the suppress time as zero and it never expires.

To suppress events by using NetScaler ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Events > Rules**. Click **Add**.
2. Specify all the parameters required to create a rule.
3. Under **Event Rule Actions**, click **Add Action** to assign notification actions for the event.
4. On the **Add Event Action** page, select **Suppress Action** from the **Action Type** drop-down list and specify the time period, in minutes, for which an event must be suppressed.
5. Click **OK**.



Create event rules

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of events generated across your infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, Citrix Application Delivery Controller (NetScaler) instances, category, failure objects, configuration commands, and messages.

You can assign the following actions to the events:

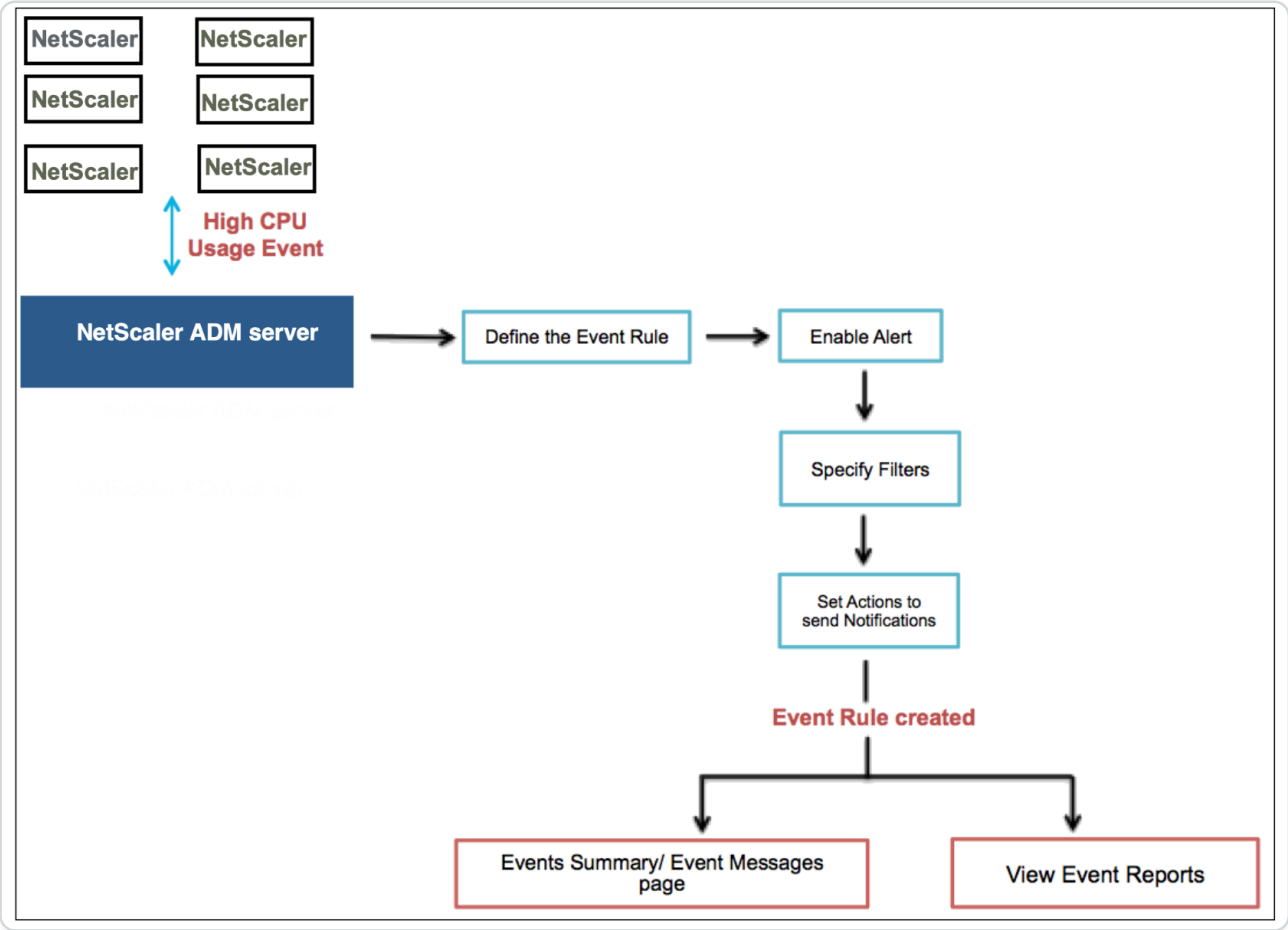
- **Send e-mail Action**: Send an email for the events that match the filter criteria.
- **Send Trap Action**: Send or forward SNMP traps to an external trap destination
- **Run Command Action**: Run a command when an incoming event meets the configured rule.
- **Execute Job Action**: Run a job is for events that match the filter criteria that you've specified.
- **Suppress Action**: Suppresses drop an event for a specific time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Send Slack Notifications**: Send notifications on the configured Slack channel for the events that match the filter criteria.
- **Send PagerDuty Notifications**: Send event notifications based on the PagerDuty configurations for the events that match the filter criteria.
- **Send ServiceNow Notifications**: Auto-generate ServiceNow incidents for an event that match the filter criteria.

For more information, see Add event rule actions

You can also have notifications resent at a specified interval until an event is cleared. And you can customize the email with a specific subject line, user message, and attachment.



For example, as an administrator you might want to monitor “high CPU usage” events for specific NetScaler instances if those events can lead to an outage of your NetScaler instances. You can:

- Create a rule to monitor the instances and specify an action that sends you an email notification when an event in the “high CPU usage” category occurs.
- Schedule the rule to run at a specific time, such as between 11 AM to 11 PM, so that you are not notified every time there is an event generated.

Configuring an event rule involves the following tasks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Define the rule
2. Choose the severity of the event that the rule detects
3. Specify the category of the event
4. Specify NetScaler instances to which the rule applies
5. Select failure objects
6. Specify advanced filters
7. Specify actions to be taken when the rule detects an event

Step 1 - Define an event rule

Navigate to **Infrastructure > Events > Rules**, and click **Add**. If you want to enable your rule, select the **Enable Rule** check box.

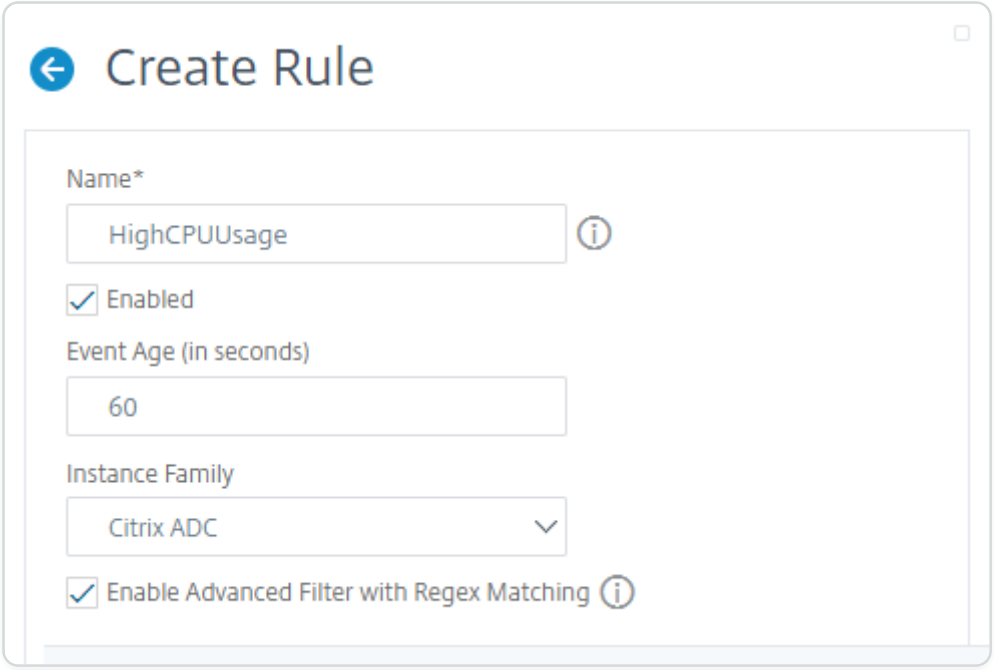
You can set the **Event Age** option to specify the time interval (in seconds) after which NetScaler® ADM refreshes an event rule.

Note:

> The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event is occurred.

Based on the example above, you may want to be notified by email every time your NetScaler instance has a “high CPU usage” event for 60 seconds or longer. You can set the event age as 60 seconds, so that every time your NetScaler instance has a “high CPU usage” event for 60 seconds or more, you receive an email notification with details of the event.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



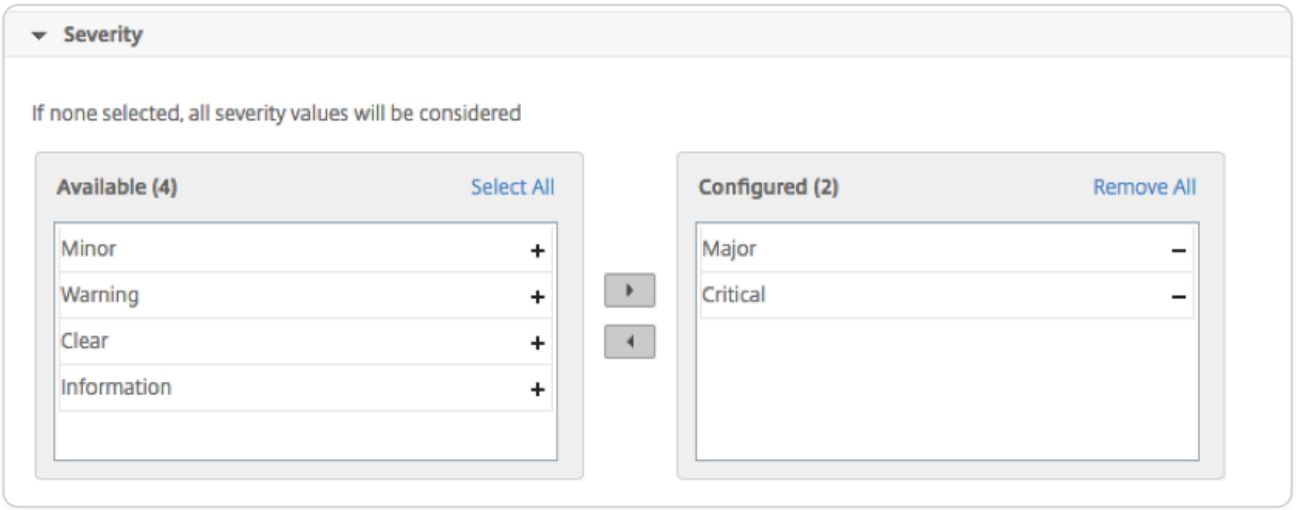
You can also filter event rules by **Instance Family** to track the NetScaler instance from which NetScaler ADM receives an event.

If you want to include a regular expression other than asterisk (*) pattern matching, select **Enable Advanced Filter with Regex Matching**.

Step 2 - Choose the severity of the event

You can create event rules that use the default severity settings. Severity specifies the current severity of the events you which you want to add the event rule.

You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

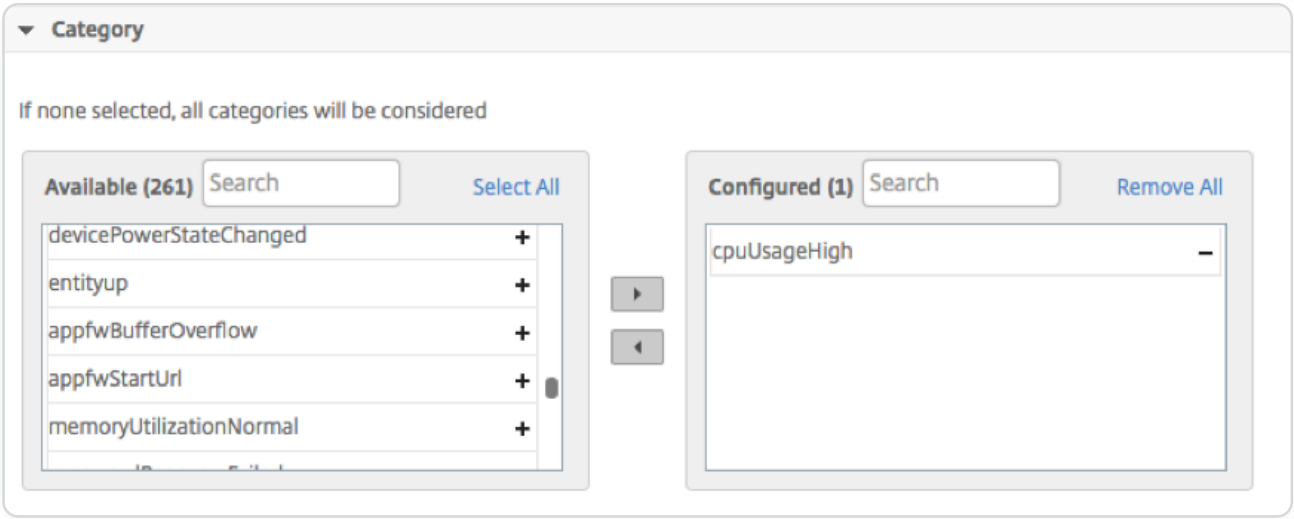
NOTE

You can configure severity for both generic and Advanced-specific events. To modify event severity for NetScaler instances managed on NetScaler ADM, navigate to **Infrastructure > Events > Event Settings**. Choose the **Category** for which you want to configure event severity and click **Configure Severity**. Assign a new severity level and click **OK**.

Step 3 - Specify the event category

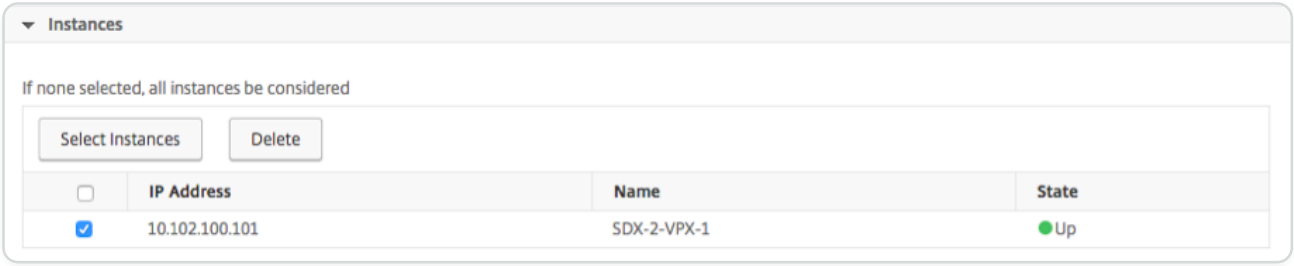
You can specify the category or categories of the events generated by your NetScaler instances. All categories are created on NetScaler instances. These categories are then mapped with NetScaler ADM that can be used to define event rules. Select the category you want to consider and move it from the **Available** table to the **Configured** table.

In the example above, you must choose “cpuUsageHigh” as the event category from the table displayed.



Step 4 - Specify NetScaler instances

Select the IP addresses of the NetScaler instances for which you want to define the event rule. In the **Instances** section, click **Select Instances**. In the **Select Instances** page, choose your instances, and click **Select**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5 - Select failure objects

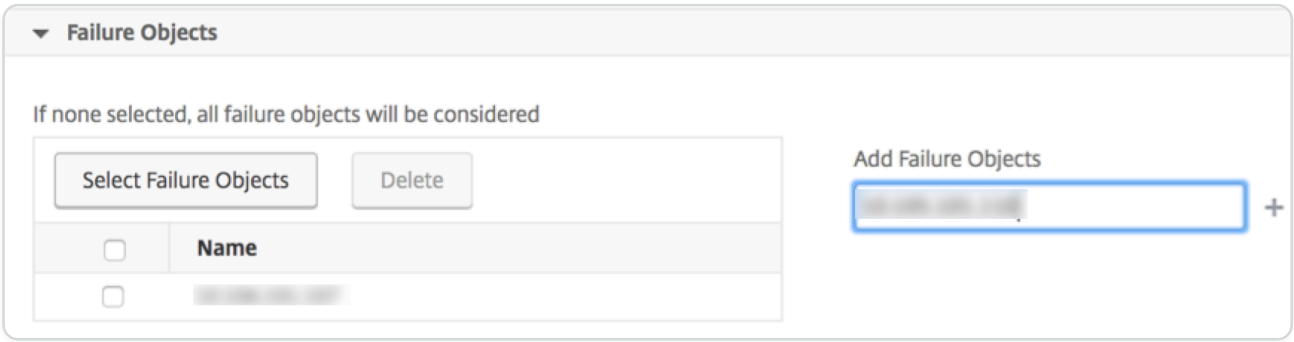
You can either select a failure object from the list provided or add a failure object for which an event has been generated. You can also specify a regular expression to add failure objects. Depending on the specified regular expression, the failure objects are automatically added to the list. Failure objects are entity instances or counters for which an event has been generated.

IMPORTANT

To list failure objects using regular expression, select **Enable Advanced Filter with Regex Matching** in Step 1.

The failure object affects the way that an event is processed and ensures it reflects the exact problem as notified. With this filter, you can track issues on the failure objects quickly and identify the cause for an issue. For example, if a user has login issues, then the failure object here is the user name or password, such as `nsroot`.

This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events, and so on.



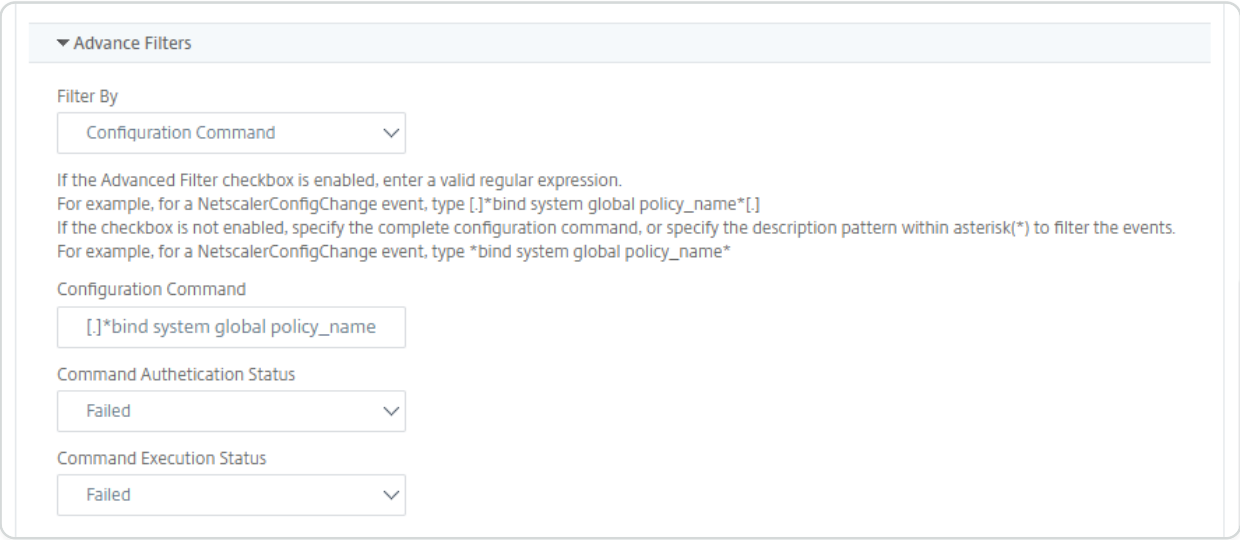
Step 6 - Specify advanced filters

You can further filter an event rule by:

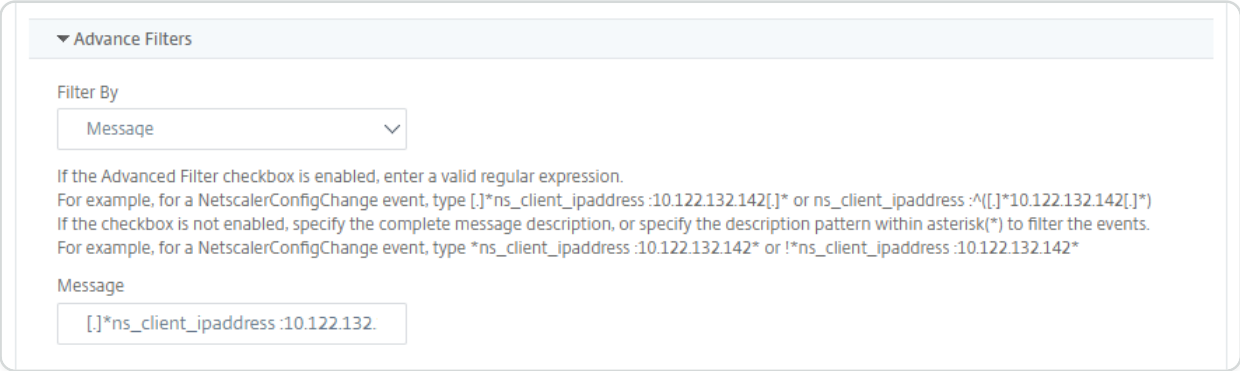
- **Configuration Commands** - You can specify the complete configuration command, or specify a regular expression to filter events.

  You can further filter the event rule by the command's authentication status and/ or its execution status. For example, for a `NetscalerConfigChange event`, type `[.]*bind system global policy_name[.]*`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Messages** - You can specify the complete message description, or specify a regular expression to filter the events.For example, for a `NetscalerConfigChange` event, type `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress : \^([.]*10.122.132.142[.]*)`.



Step 7 - Add event rule actions

You can add event rule actions to assign notification actions for an event. These notifications are sent or performed when an event meets the defined filter criteria that you've set above. You can add the following event actions:

- Send email Action
- Send Trap Action
- Run Command Action
- Run Job Action
- Suppress Action
- Send Slack Notifications
- Send PagerDuty Notifications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Send ServiceNow Notifications

To set email Event Rule Action

When you choose the Send email Action event action type, an email is triggered when the events meet the defined filter criteria. You must either create an email distribution list by providing mail server or mail profile details or you can select an email distribution list that you've previously created.

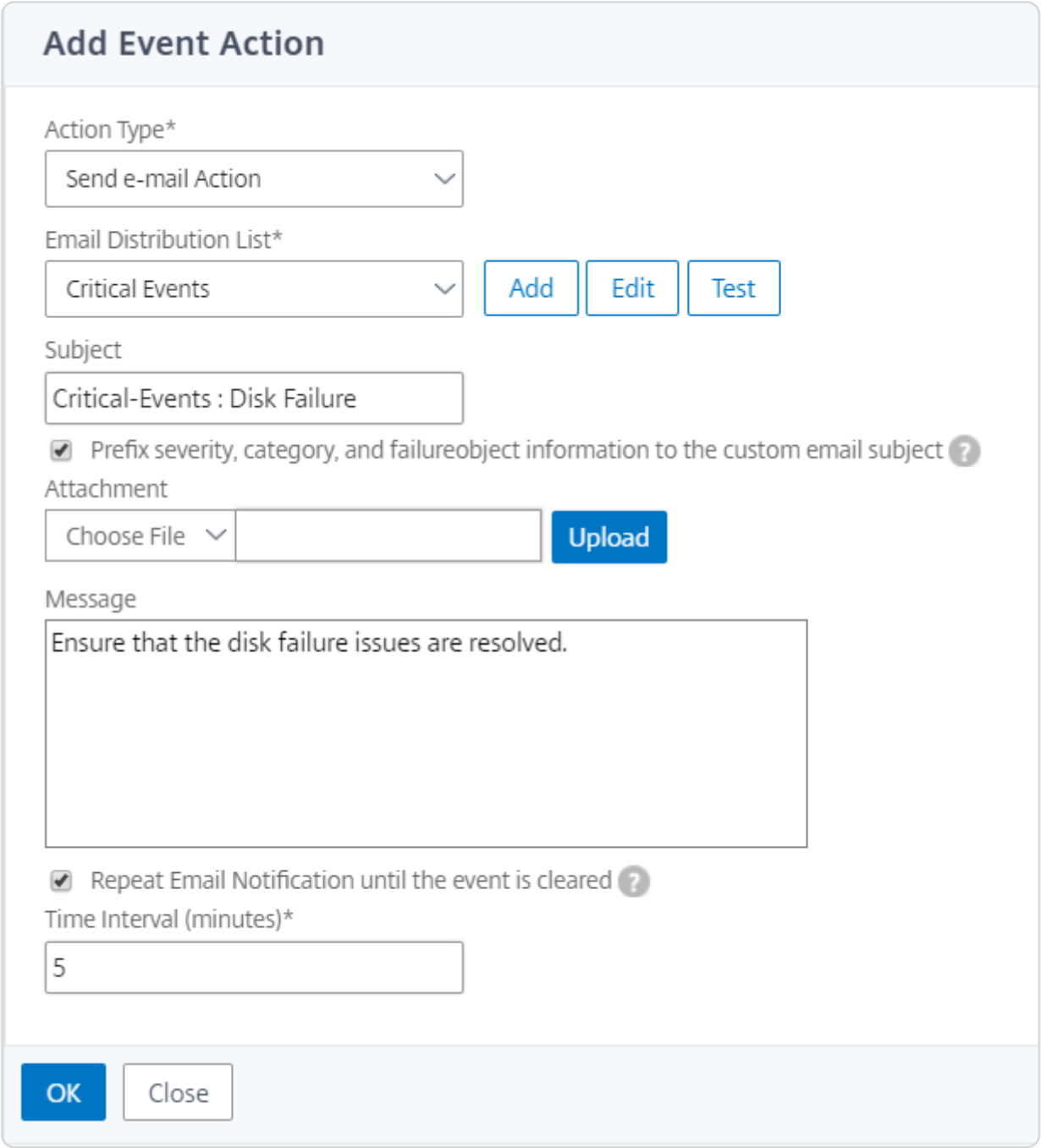
Due to a high number of virtual servers being configured in NetScaler ADM, you might receive a high number of emails every day. The emails have a default subject line that provides information about the severity of the event, the category of the event and the failure object. But the subject line does not carry any information about the name of the virtual server where these events originate from. You now have an option to include some additional information like the name of the affected entity, name of the failure object.

You can also add a customized subject line and a user message, and upload an attachment to your email when an incoming event matches the configured rule.

While sending emails for event notifications, you might want to send a test email to test the configured settings. The "Test" button now allows you to send a test email after configuring an email server, associated distributed lists, and other settings. This feature ensures that settings are working fine.

You can also ensure that all critical events are addressed and no important email notifications are missed, by selecting the **Repeat Email Notification until the event is cleared** check box to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To set Trap Event Rule Action

When you choose the **Send Trap Action** event action type, SNMP traps are sent or forwarded to an external trap destination. By defining a trap distribution list (or a trap destination and trap profile details), trap messages are sent to specific trap listeners when events meet the defined filter criteria.

To set the Run Command Action

When you choose the **Run Command Action** event action, you can create a command or a script that can be run on NetScaler ADM for events matching a particular filter criterion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also set the following parameters for the **Run Command Action** script:

Parameter	Description
$source	This parameter corresponds to the source IP address of the received event.
$category	This parameter corresponds to the type of traps defined under category of the filter
$entity	This parameter corresponds to the entity instances or counters for which an event has been generated. It can include the counter names for all threshold-related events, entity names for all entity-related events, and certificate names for all certificate-related events.
$severity	This parameter corresponds to the severity of the event.
$failureobj	The failure object affects the way that an event is processed and ensures that the failure object reflects the exact problem as notified. This can be used to track down problems quickly and to identify the reason for failure, instead of simply reporting raw events.

NOTE

During command execution, these parameters are replaced with actual values.

For example, consider that you want to set a run command action when a load balancing virtual server status is **Down**. As an administrator, you might want to consider providing a quick workaround by adding another virtual server. In NetScaler ADM, you can:

- Write a script (.sh) file.

  The following is a sample script (.sh) file:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
#!/bin/sh

source=$1

failureobj=$2

payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
json" -X POST -d $payload $url
```

- Save the .sh file in any persistent location on NetScaler agent. For example, `/var`.
- Provide the .sh file location in NetScaler ADM to run when the rule criteria are met.

To set the **Run Command** action for creating a new virtual server:

1. Define the rule
2. Select the severity of the event
3. Select the event category **entitydown**
4. Select the instance that has the virtual server configured
5. Select or create a failure object for the virtual server
6. Under **Event Rule Actions**, click **Add Action** and select **Run Command Action** from the **Action Type** list.
7. Under **Command Execution List**, click **Add**.

   The Create Command Distribution List page is displayed.

   a. In **Profile Name**, specify a name of your choice
   b. In **Run Command**, specify the NetScaler agent location, where the script must be run. For example: `/sh/var/demo.sh $source $failureobj`.
   c. Select **Append Output** and **Append Errors**

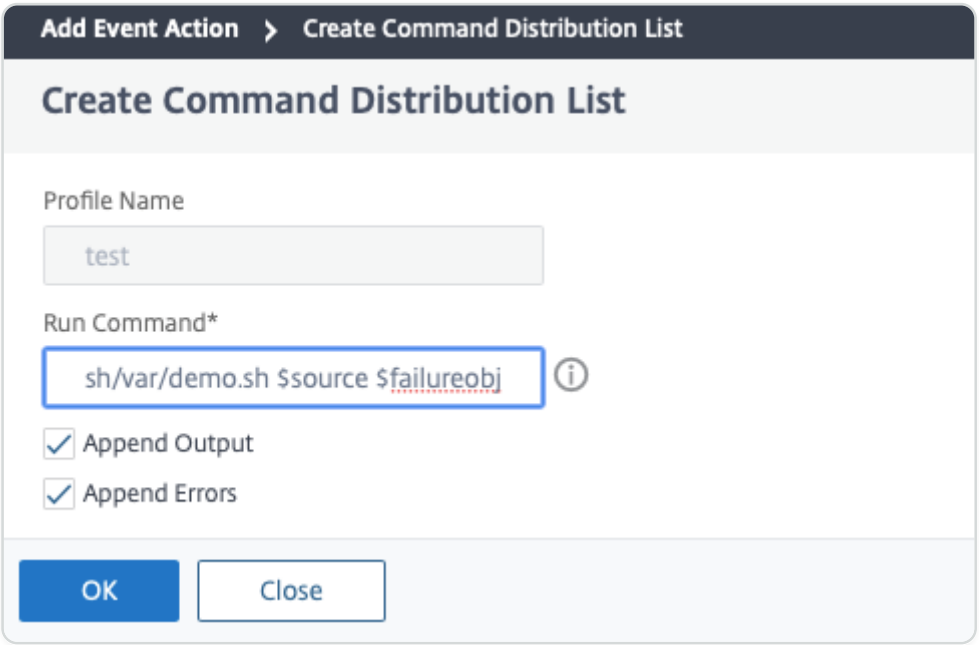
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler ADM server log files. If you do not enable these options, NetScaler ADM discards all outputs and errors generated while running the command script.

d. Click **Create**.

8. In the **Add Event Action** page, click **OK**.



NOTE

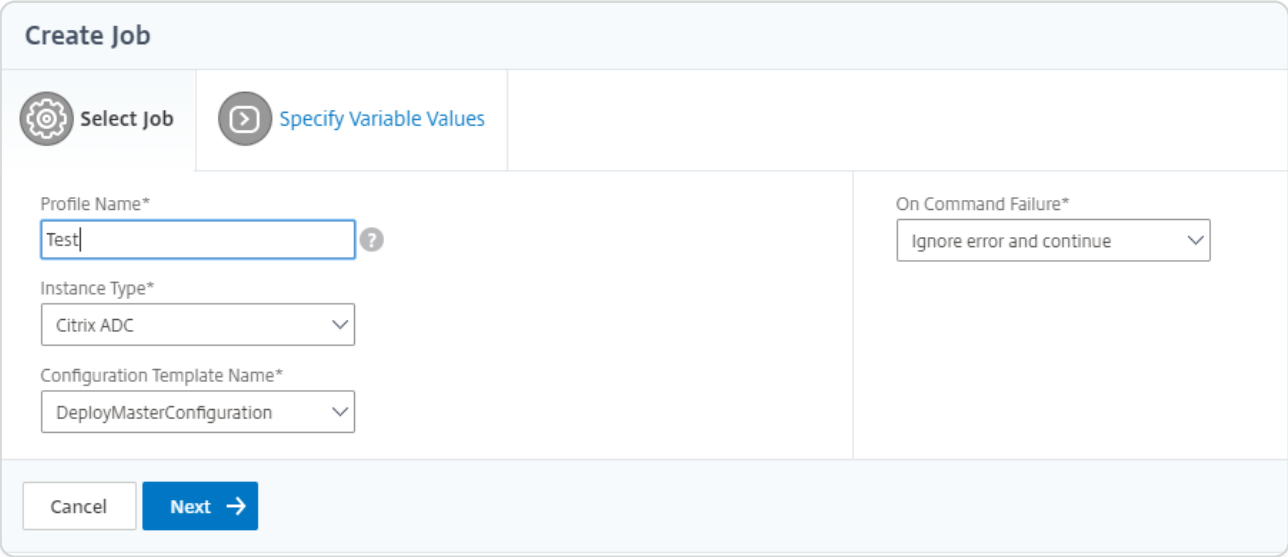
You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler ADM server log files. If you do not enable these options, NetScaler ADM discards all outputs and errors generated while running the command script.

To set the `Execute` Job Action

By creating a profile with configuration jobs, a job is run as a built-in job or a custom job for NetScaler and NetScaler SDX instances, for events and alarms that match the filter criteria you've specified.

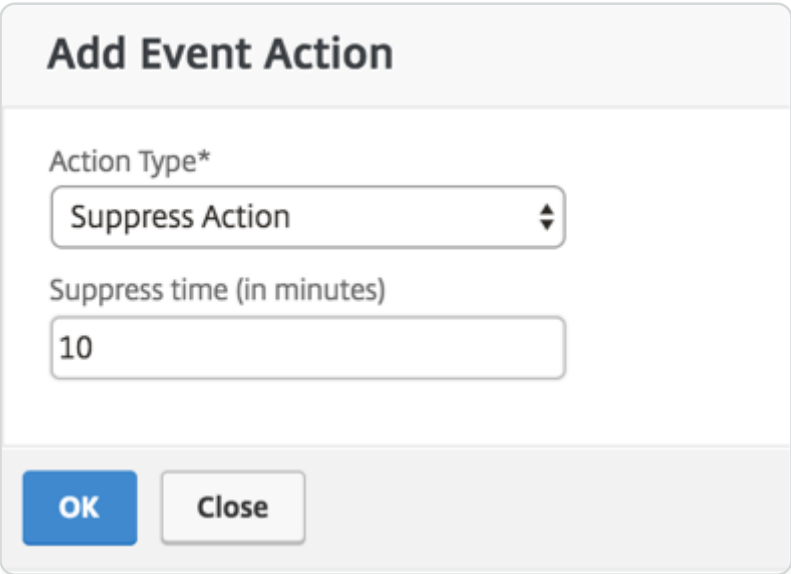
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Under **Event Rule Actions**, click **Add Action** and select **Execute Job Action** from the **Action Type** drop-down list.
2. Create a profile with a job that you want to run when the events meet the defined filter criteria.
3. While creating a job, specify a profile name, the instance type, the configuration template, and what action you'd like to perform if the commands on the job fail.
4. Based on the instance type selected and the configuration template chosen, specify your variables values and click **Finish** to create the job.



To set the Suppress Action

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set Slack notifications from NetScaler ADM

Configure the required Slack channel by providing the profile name and the webhook URL in NetScaler ADM GUI. The event notifications are then sent to this channel. You can configure multiple Slack channels to receive these notifications

1. In NetScaler ADM, navigate to **Infrasturcture > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters such as severity and category. Select instances and also failure objects that must be monitored.
3. Under **Event Rule Actions**, click **Add Action**. Then, select **Send Slack Notifications** from the **Action Type** list and select **Slack Profile List.**
4. You can also add a Slack profile list by clicking **Add** next to the **Slack Profile List** field.
5. Type the following parameters to create a profile list:
   a. **Profile Name**. Type a name for the profile list to be configured on NetScaler ADM
   b. **Channel Name**. Type the name of the Slack channel to which the event notifications are to be sent.
   c. **Webhook URL**. Type the Webhook URL of the channel that you have entered earlier. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name and all event notifications are sent to this URL to be posted on the designated Slack channel. An example of a webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`
6. Click **Create** and click **OK** in the **Add Event Action** window.

NOTE:

You can also add the Slack profiles by navigating to **System** \> **Notifications** \> **Slack Profiles**. Click **Add** and create the profile as described in the earlier section.

You can view the status of the Slack profiles that you have created.

Your event rule is now created with appropriate filters and well defined event rule actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set PagerDuty notifications from NetScaler ADM

You can add a PagerDuty profile as an option in NetScaler ADM to monitor the incident notifications based on your PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on registered number.

Before you add a PagerDuty profile in NetScaler ADM, ensure you have completed the required configurations in PagerDuty. For more information, see PagerDuty documentation.

You can select your PagerDuty profile as one of the options to get notifications for the following features:

- **Events** – List of events that are generated for NetScaler instances.
- **Licenses** – List of licenses that are currently active, about to expire, and so on.
- **SSL Certificates** – List of SSL certificates that are added to NetScaler instances.

To add a PagerDuty profile in ADM:

1. Log on to NetScaler ADM using administrator credentials.
2. Navigate to **Settings > Notifications > PagerDuty Profiles**.
3. Click **Add** to create a new profile.
4. In the Create PagerDuty Profile page:

   a. Provide a profile name of your choice.

   b. Enter the **Integration Key**.

      You can get the Integration Key from your PagerDuty portal.

   c. Click **Create**.

   Use case:

   Consider a scenario that you:

   - want to send notifications to your PagerDuty profile.
   - have configured phone call as an option in PagerDuty to receive notifications.
   - want to get phone call alerts for NetScaler events.

   To configure:

   a. Navigate to **Events** > **Rules**

   b. On the **Create Rule** page, configure all other parameters to create a rule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Under **Create Rule Actions**, click **Add Action**.

   The **Add Event Action** page is displayed.

   i. Under **Action Type**, select **Send PagerDuty Notifications**.

   ii. Select your PagerDuty profile and click **OK**.

After the configuration is complete, whenever a new event is generated for NetScaler instance, you will receive a phone call. From the phone call, you can decide to:

- Acknowledge the event
- Mark it as resolved
- Escalate to another team member

To auto-generate ServiceNow incidents from NetScaler ADM

You can auto-generate ServiceNow incidents for NetScaler ADM events by selecting the ServiceNow profile on the NetScaler ADM GUI. You must choose the ServiceNow profile in NetScaler ADM to configure an event rule.

Before you configure an event rule to auto-generate ServiceNow incidents, integrate NetScaler ADM with a ServiceNow instance. For more information, see Configure ITSM adapter for ServiceNow.

To configure an event rule, navigate to **Events** > **Rules**.

1. On the **Create Rule** page, configure all other parameters to create a rule.
2. Under **Create Rule Actions**, click **Add Action**.

   The **Add Event Action** page is displayed.

   a. In **Action Type**, select **Send ServiceNow Notifications**.

   b. In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.

   c. Click **OK**.

Modify the reported severity of events that occur on NetScaler instances

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

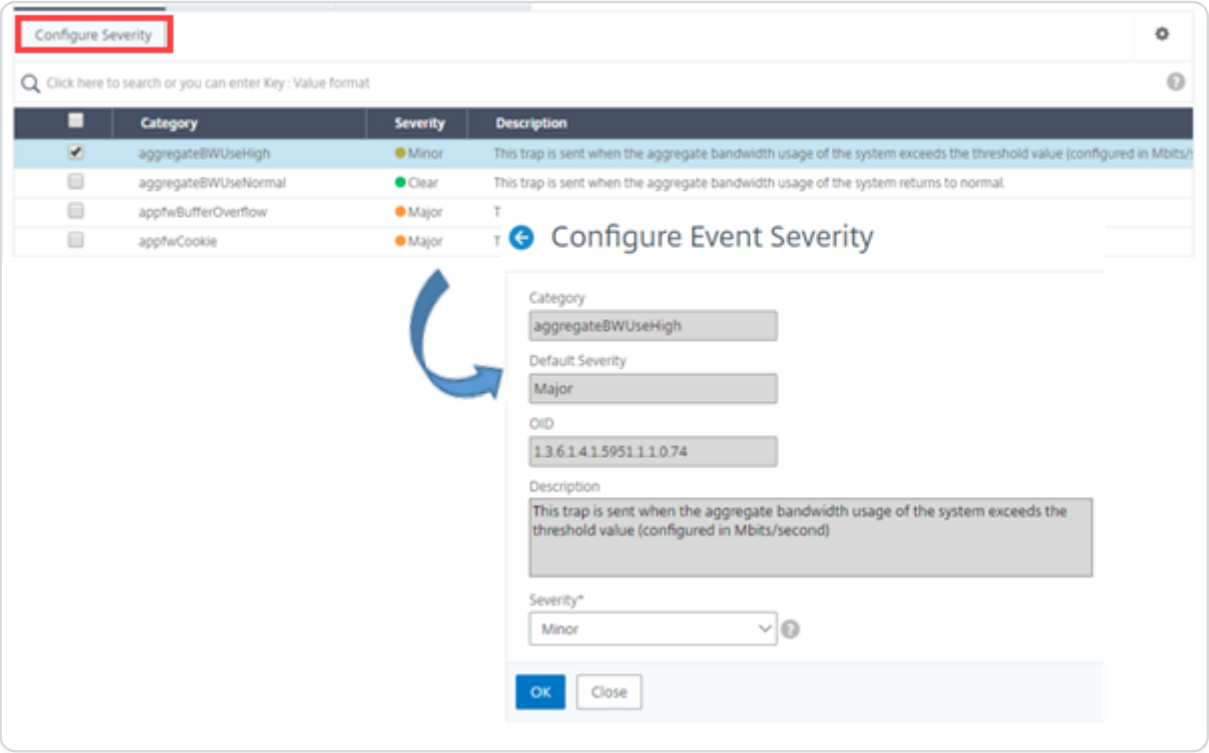
© 1997–2026 Citrix Systems, Inc. All rights reserved.

severity. You can create event rules that use the default severity settings, and you can change the severity settings. You can configure severity for both generic and enterprise-specific events.

You can define the following levels of severity: Critical, Major, Minor, Warning, and Clear.

To modify event severity:

1. Navigate to **Infrastructure > Events > Event Settings**.
2. Click the tab for the Citrix Application Delivery Controller™ (ADC) instance type that you want to modify. Then, select the category from the list and click **Configure Severity**.
3. In **Configure Event Severity**, select the severity level from the drop-down list.
4. Click **OK**.



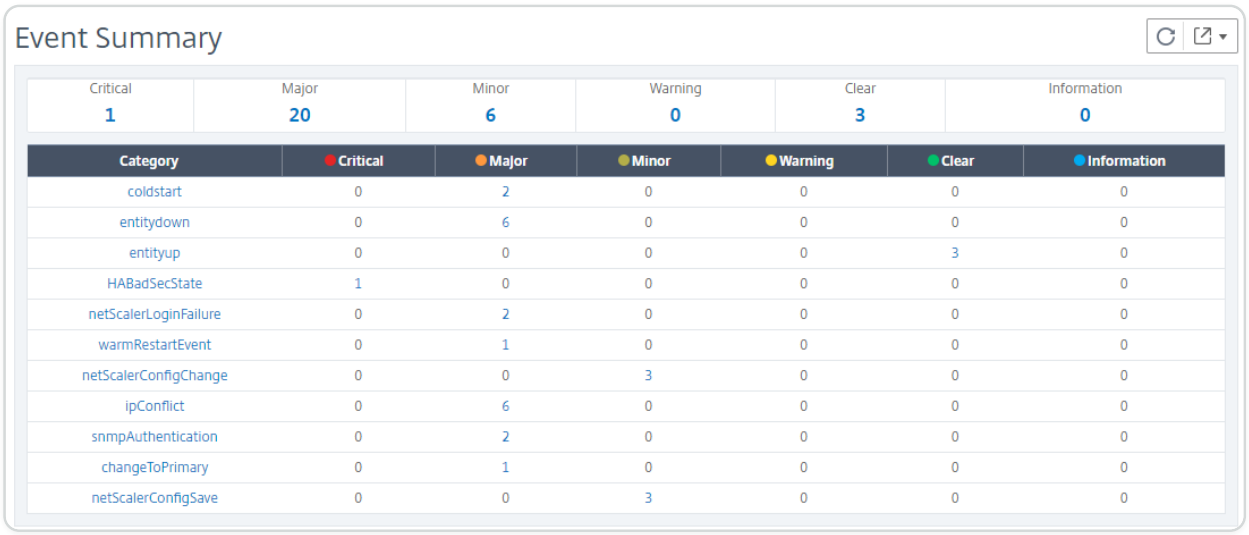
View events summary

You can now view an Events Summary page to monitor the events and traps received on your NetScaler® Application Delivery Management (ADM) server. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by NetScaler ADM**. The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a Citrix Application Delivery Controller™ (ADC) instance goes down and stops sending information to the NetScaler ADM server. During the event, a notification is sent to an administrator, explaining

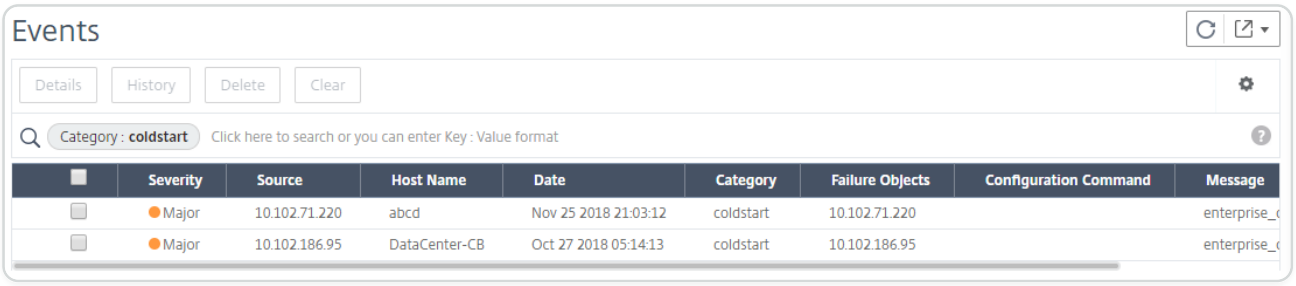
© 1997–2026 Citrix Systems, Inc. All rights reserved.

the reason why the instance is down, the time for which it had been down, and so on. The event is then recorded on the Events Summary page, on which you can view a summary and access the details of the event.



- **Number of traps received for each category**. The number of traps received, categorized by severity. By default, each trap sent from NetScaler instances to NetScaler ADM has an assigned severity, but as the network administrator, you can specify its severity in the NetScaler ADM GUI.

If you click a category type or a trap, you are taken to the **Events** page, on which filters such as the Category and Severity are preselected. This page displays more information about the event, such as the NetScaler instance's IP address and host name, date on which the trap was received, category, failure objects, configuration command run, and the message notification.



Display event severities and SNMP trap details

When you create an event and its settings in NetScaler Application Delivery Management (ADM), you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all Citrix Application Delivery Controller™ (ADC) instances added to your NetScaler ADM server in minute detail on the Infrastructure Dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the Infrastructure dashboard, you can now mask irrelevant values so that you can more easily view and monitor information such as event by severities, health, up time, models, and version of NetScaler instances in minute detail.

For example, events with a **Critical** severity level might occur rarely. However, when these critical events do occur on your network, you might want to further investigate, troubleshoot, and monitor where and when the event occurred. If you select all severity levels except Critical, the graph displays only the occurrences of critical events. Also, by clicking the graph, you are taken to the **Severity based events** page, where you can see all the details regarding when a critical event occurred for the duration that you've selected: the instance source, the date, category, and message notification sent when the critical event occurred.

Similarly, you can view the health of a NetScaler VPX instance on the Dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of service. By clicking on the graph, you are taken to that instance's page, where the *out of service* filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and so on. You can also select the instance and see the particular Citrix instance's dashboard for more details.

To select specific events by severity in NetScaler® ADM:

1. Log on to NetScaler ADM, using your administrator credentials.
2. Navigate to **Infrastructure > Dashboard**.

   Or,

   Navigate to **Infrastructure > Events > Reports**.
3. From the menu in the upper-right corner of the page, select the duration for which you want to see events by severity.

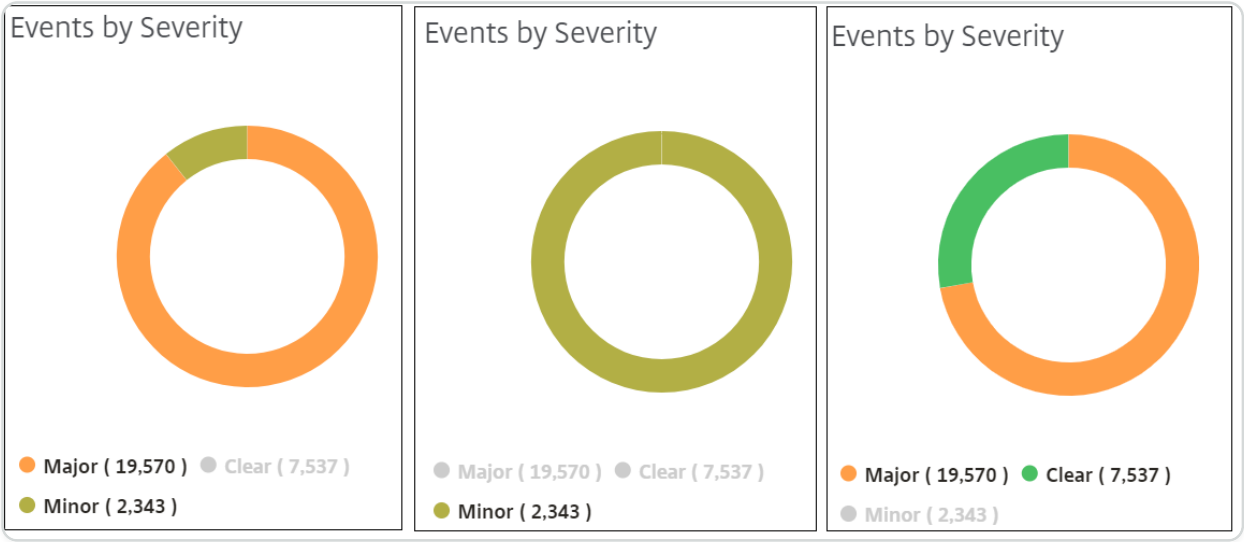
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.
5. You can click each section on the donut chart to display the corresponding **Severity based events** page, which shows the following details for the selected severity for the selected duration:
   - Instance Source
   - Data of the event
   - Category of events generated by the NetScaler instance
   - Message notification sent

NOTE

Below the donut chart you can see a list of severities that are represented in the chart. By default, a donut chart displays all events of all severity types, and therefore all severity types in the list are highlighted. You can toggle the severity types to more easily view and monitor your chosen severity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To view NetScaler SNMP trap details on NetScaler ADM:

You can now view the details of each SNMP trap received from its managed NetScaler instances on the NetScaler ADM server on the **Event Settings** page. Navigate to **Infrastructure > Events > Event Settings**. For a specific trap received from your instance, you can view the following details in tabular format:

- **Category** - Specifies the category of the instance to which the event belongs.
- **Severity** - The severity of the event is indicated by colors and its severity type.
- **Description** - Specifies the messages associated with the event.

For example, an event with the trap category **monRespTimeoutBelowThresh**, the description of the trap is displayed as “This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set.”

View and export NetScaler syslog messages

From your ADM software, you can monitor the syslog events generated on your Citrix Application Delivery Controller (ADC) instances. For that, you must configure ADM as the syslog server for your NetScaler instances. After you've configured ADM, all syslog messages are redirected from the ADC instances to ADM.

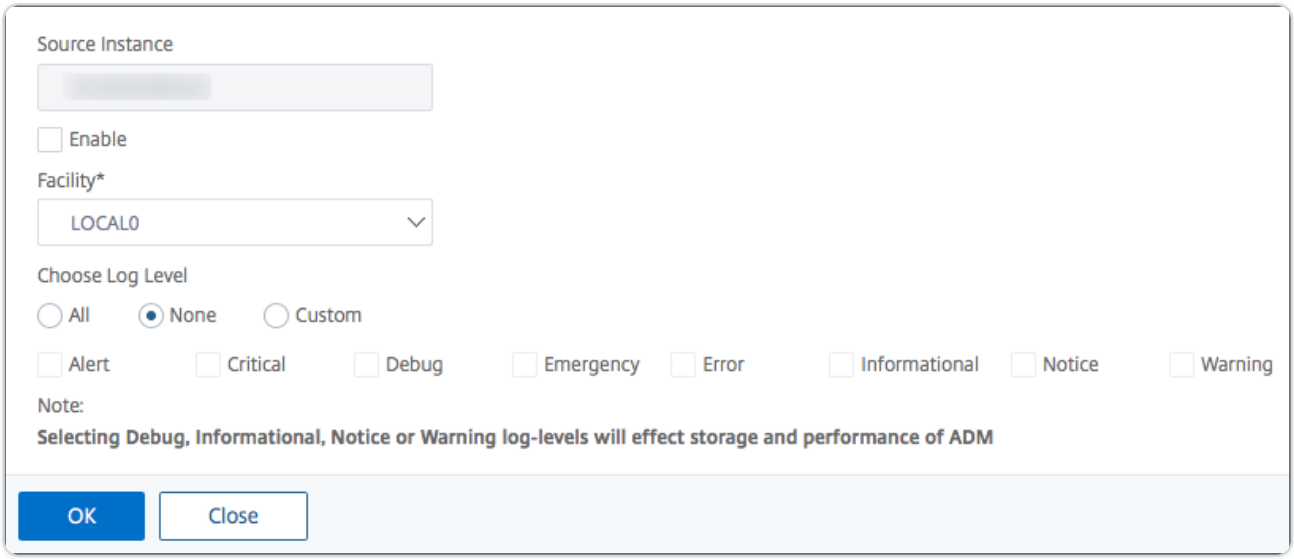
Configure ADM as a syslog server

Follow these steps to configure ADM as the syslog server:

1. From the ADM GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.



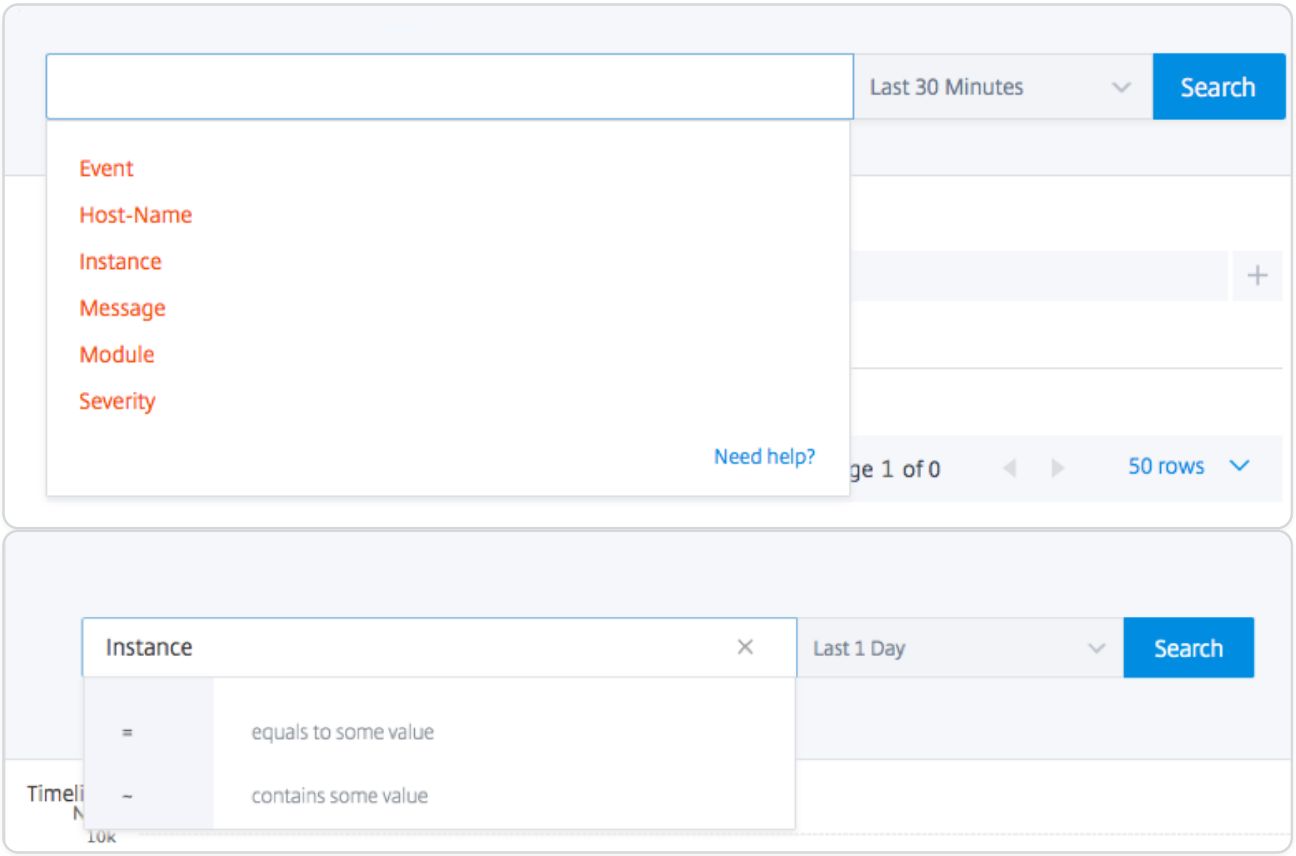
These steps configure all the syslog commands in the NetScaler instance, and NetScaler ADM starts receiving the syslog messages.

View and search syslog messages

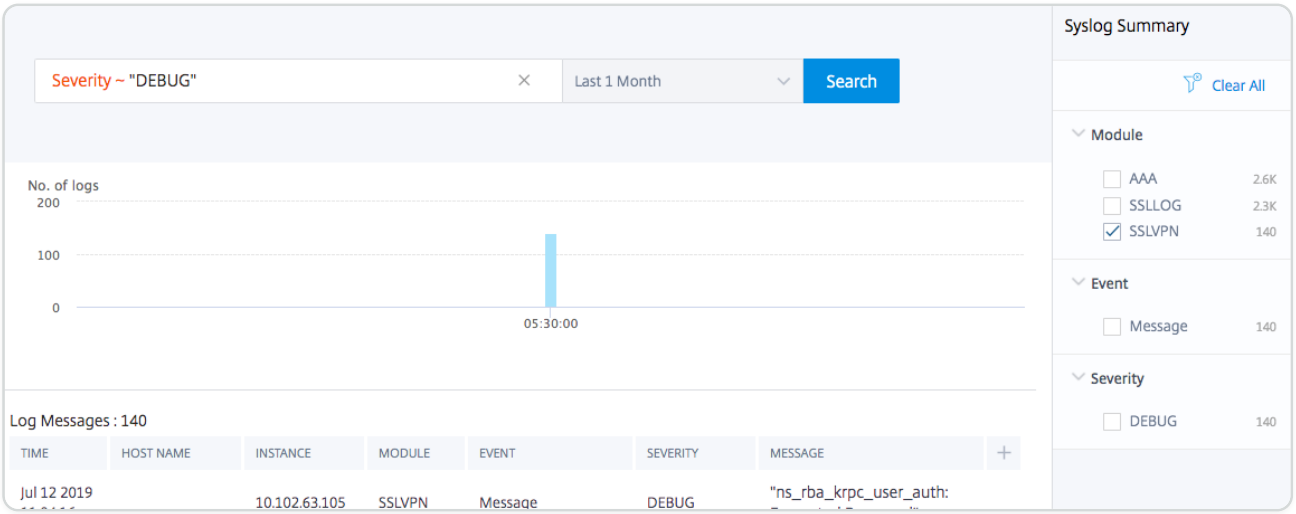
You can view all your syslog messages generated on your managed NetScaler instances. The syslog messages are stored in the database centrally and are available under **Infrastructure > Events > Syslog Messages** for auditing purposes. You can combine this logging information and derive reports for analytics from the collected data.

Further, you can use filters to narrow down the search results of syslog messages and find exactly what you are looking for and in real time. Click **Need Help?** to open the built-in search help.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Next, add the search term. For some categories, a prepopulated list of search terms is displayed. By default, the search time is 1 day. You can change the time and date range by clicking the down arrow. You can further narrow down your search by selecting options from the **Syslog Summary** pane.



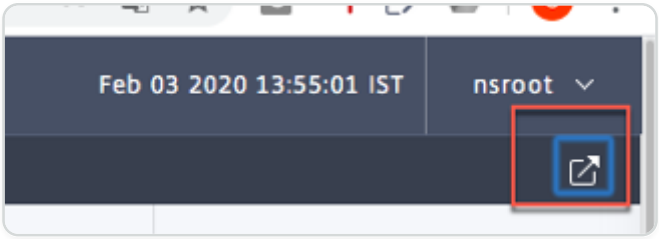
Export and schedule syslog messages

You can view syslog messages without logging into ADM, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

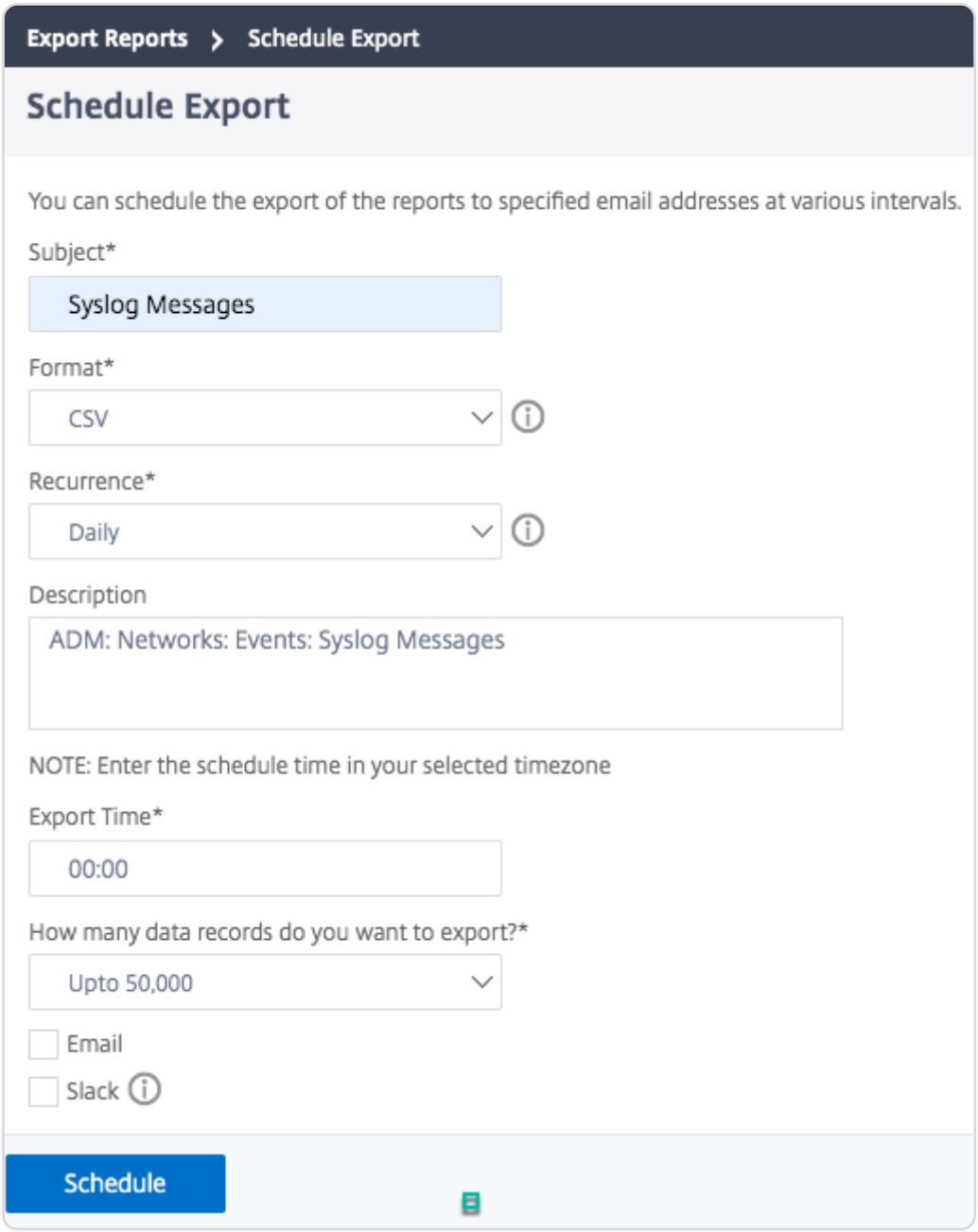
ADC instances in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses or Slack account at various intervals.

To export and schedule the log messages, click the arrow icon on the upper right corner.



- To export the log messages, click **Export Reports > Export Now**, select the required format, and then click **Export**.
- To schedule the export of syslog messages, click **Export Reports > Schedule Report**, and set the required parameters. You can receive the report through email or Slack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Suppress syslog messages

When configured as a syslog server, NetScaler Application Delivery Management (ADM) receives all syslog messages sent to it by the configured Citrix Application Delivery Controller™ (ADC) instances. There might be a large number of messages that you might not want to see. For example, you might not be interested in seeing all informational level messages. You can now discard some of the syslog messages that you are not interested in. You can suppress some of the syslog messages coming into NetScaler ADM by setting up some filters. NetScaler ADM drops all messages that matches with the criteria. These dropped messages do not appear on the NetScaler ADM GUI and these messages are also not stored in the customer's NetScaler ADM database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can suppress some of the logged syslog messages coming into NetScaler ADM by setting up some filters. The two filters that can be used for suppressing syslog messages are severity and facility. You can also suppress messages coming from a particular NetScaler instance or multiple instances. You can also provide a text pattern for NetScaler ADM to search and suppress messages. NetScaler ADM drops all messages that matches with the criteria. These dropped messages do not appear on the NetScaler ADM GUI and these messages are also not stored in the customer database. Therefore, a good amount of space is saved on the storage server.

Some use cases for suppressing syslog messages are as follows:

- If you want to ignore all information level messages, suppress level 6 (informational)
- If you only want to record firewall error conditions, suppress all levels other than level 3 (errors)

Suppressing syslog messages by creating filters

1. In NetScaler ADM, navigate to **Infrastructure > Events > Syslog Messages** \> **Suppress Filter**.
2. On **Create Suppress Filter** page, update the following information:

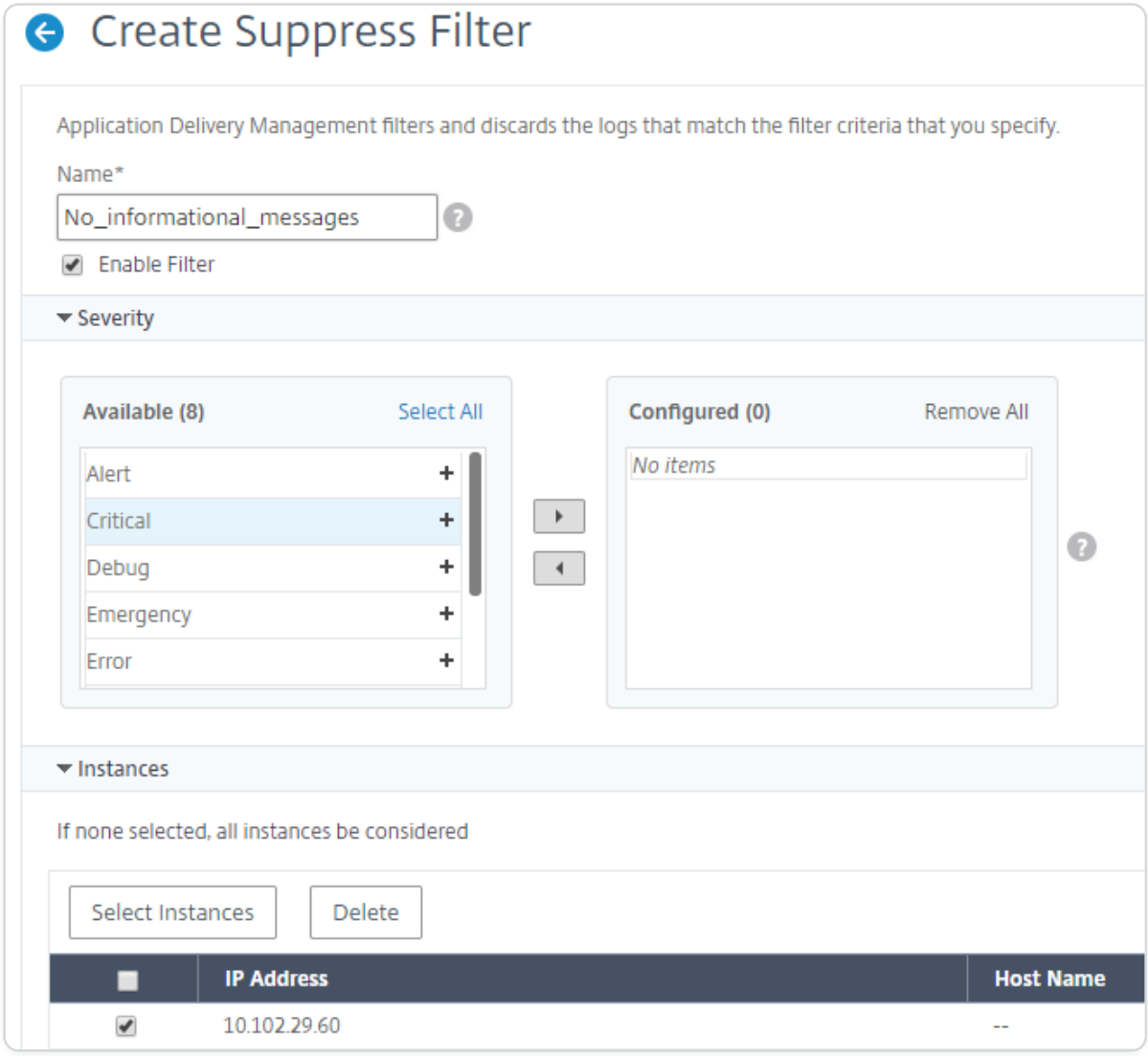
   a. **Name** - type a name for the filter.

   > **NOTE**
   >
   > If different users have different access to multiple NetScaler instances, different filters must be created for different instances as users can see only those filters in which they have access to all the instances.

   b. **Severity** - Select and add the log levels for which you must suppress the messages. For example, if you do not want to view any informational messages coming in, you can select Informational to suppress those messages.

   c. **Instances** - Select the NetScaler instances on which the syslog messages have been configured.

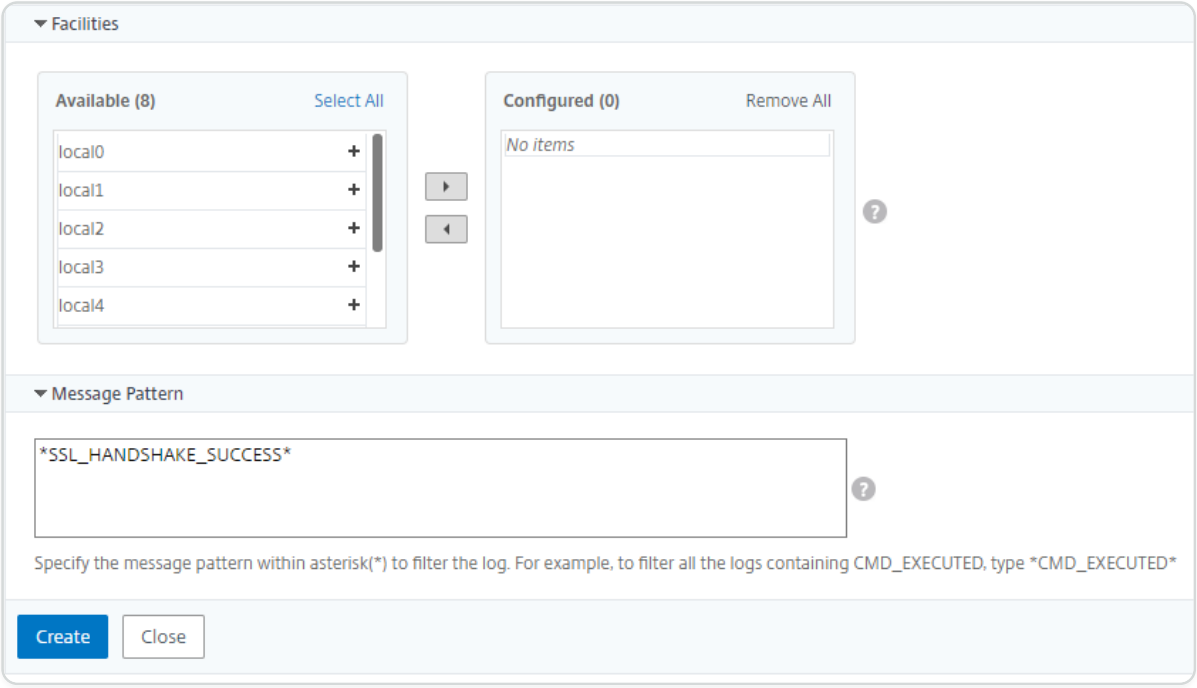
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Disabling the filter

To allow the messages to be viewed on NetScaler® ADM, you must disable the filter.

1. Navigate to **Infrastructure > Events > Syslog Messages** \> **Suppress Filter**, and on **Suppress Filter** page, select the filter and click **Edit**.
2. On **Configure Suppress Filter** page, clear **Enable Filter** check box to disable the filter.

Configure prune settings for instance events

Citrix Application Delivery Controller (ADC) instances managed by your NetScaler Application Delivery Management (ADM) server send event messages data continuously to be stored on NetScaler ADM. You can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

NOTE

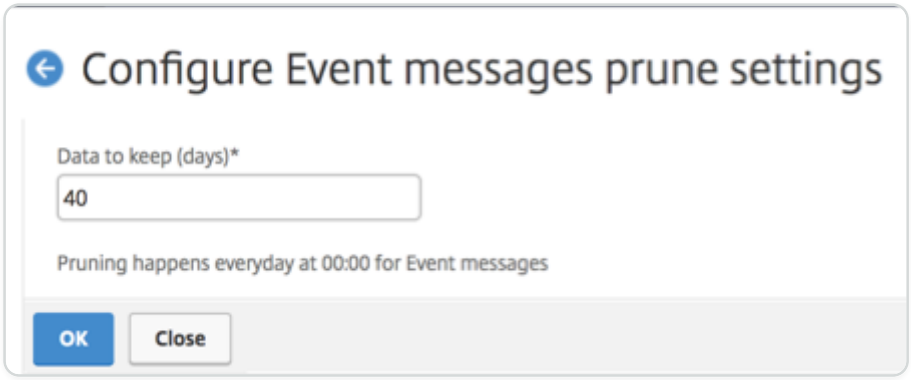
The value you can specify cannot exceed 40 days or be less than 1 day.

To configure prune settings for instance events:

1. Navigate to **System** \> **System Administration**.
2. Under **Prune Settings**, click **Instance Events Prune Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Enter the time interval, in days, for which you want to retain data on the NetScaler® ADM server and click **OK**.



Network functions

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix Application Delivery Controller™ (ADC) instances. You can view statistics such as transaction details, connection details, and throughput of a load balancing virtual server. You can also enable or disable the entities when you plan a maintenance.

The Network Functions dashboard provides you with the following graphs:

- Top 5 virtual servers with highest client connections
- Top 5 virtual servers with highest server connections
- Top 5 virtual servers with maximum throughput (MB/sec)
- Bottom 5 virtual servers with lowest throughput (MB/sec)
- Top 5 instances with most virtual servers
- State of the virtual servers
- Health of the load balancing virtual servers
- Protocols

Generate reports for load balancing entities

NetScaler Application Delivery Management (ADM) allows you to view the reports of Citrix Application Delivery Controller (ADC) instance entities at all levels. There are two types of reports that you can download in NetScaler ADM \> Network Functions - consolidated reports and individual reports.

Consolidated reports: You can download and view a consolidated or a summarized report for all entities that are managed on NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This report allows you to have a high-level view of the mapping between the NetScaler instances, partitions, and the corresponding load balancing entities (virtual servers, service groups, and services) that are present in the network.

The following image shows an example of a summarized report.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	beta		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				

The consolidated report is in a CSV format. The entries in each column are described as follows:

- **NetScaler IP Address**: IP address of the NetScaler instance is displayed in the report
- **NetScaler® HostName**: Host name is displayed in the report.
- **Partition**: IP address of the administrative partition is displayed
- **Virtual Server**: \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **Services**: \<name_of_the_service\>#service-IP_address:port_number
- **Service Groups**: \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

NOTE

- If there is no host name available, the corresponding IP address is displayed.
- Blank columns indicate that the respective entities are not configured for that NetScaler instance.

Individual reports: You can also download and view independent reports of all instances and entities. For example, you can download a report for only load balancing virtual servers or load balancing services or load balancing service groups.

NetScaler ADM allows you to download the report instantly. You can also schedule the report to be generated at a fixed time once a day, once a week, or once a month.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generate a combined load balancing report

1. In NetScaler ADM, navigate to **Infrasturcture > Network Funtions > Load Balancing.**
2. On **Load Balancing** page, click

   .
3. On the **Export** page that opens, you have two options to view the report:

   a. Select **Export Now** tab and click **OK**.

      The consolidated report downloads to your system.

   b. Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

      i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

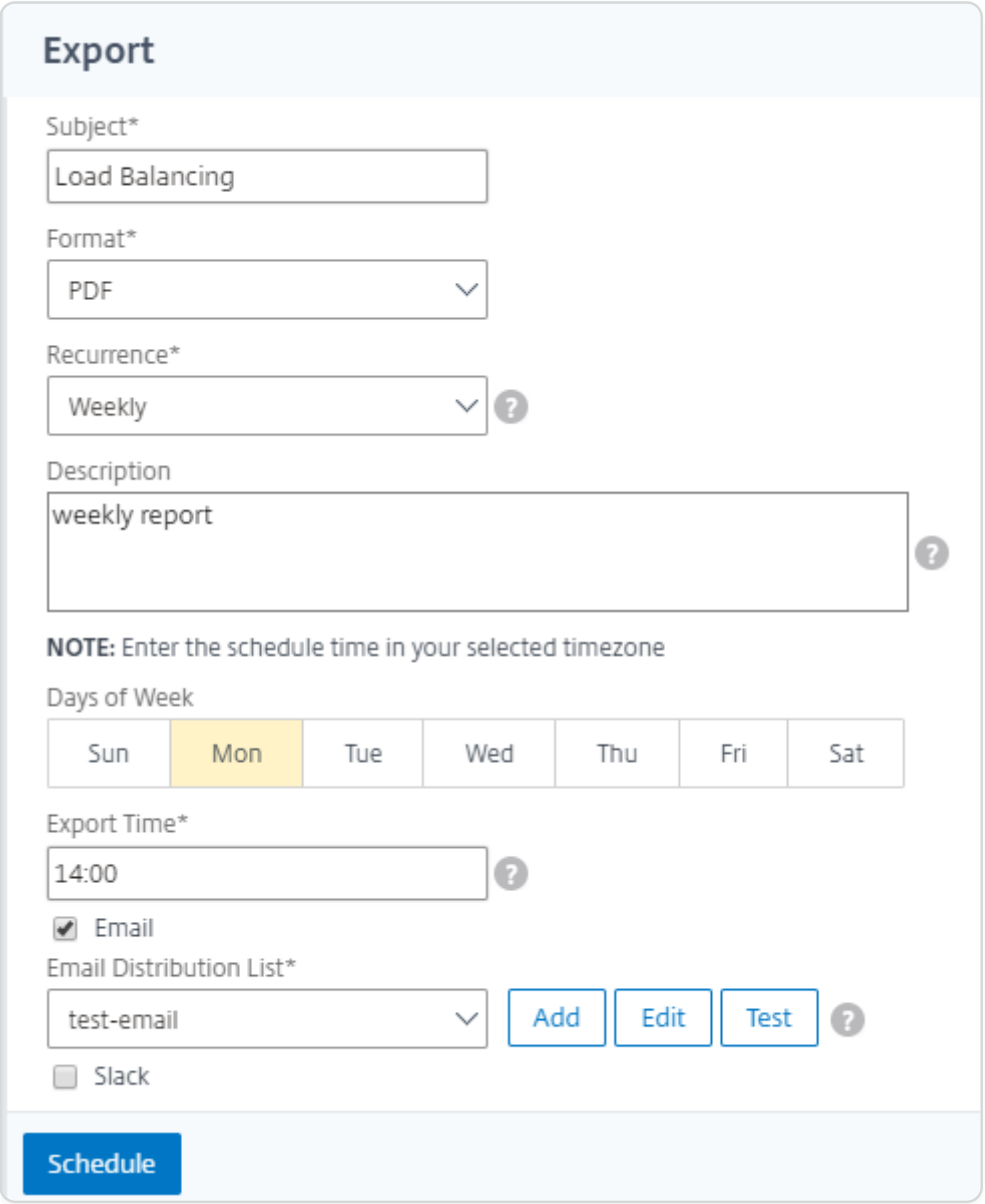
      ii. **Recurrence time** - Enter the time as Hour:Minute in 24-hour format.

      iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** to create an email profile.

NOTE

If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

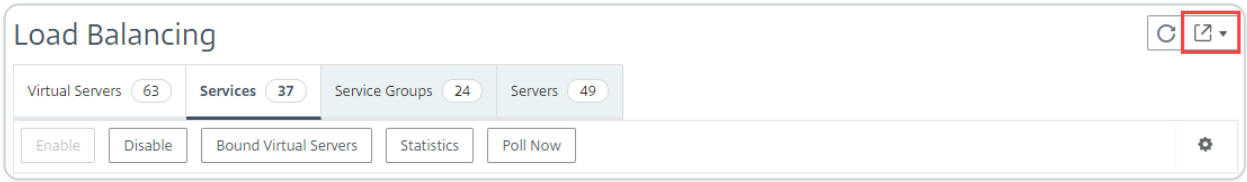
If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Generate an individual load balancing entity report

You can generate and export an individual report for a particular type of entity associated with the instances. For example, consider a scenario where you want to see a list of all load balancing services in the network.

1. In NetScaler ADM, navigate to **Infrasturcture > Network Funtions > Load Balancing > Services.**
2. On **Services** page, click the **Export** button at the top right-hand corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Select **Export Now** tab if you want to generate and view the report at this instant.

b. Select **Schedule Export** to schedule generating and exporting of the report at regular intervals.

NOTE

You can only download the reports or export the reports as mail attachments. You cannot view the reports on the NetScaler ADM GUI.

Export or schedule export of network functions reports

You can generate a comprehensive report for selected network functions such as Load Balancing, Content Switching, Cache Redirection, Global Server Load Balancing (GSLB), Authentication, and NetScaler Gateway in NetScaler Application Delivery Management (ADM). This report allows you to have a high-level view of the mapping between the NetScaler instances, partitions, and the corresponding bound entities (virtual servers, service groups, and services) that are present in the network. You can export these reports in .csv file format.

The report displays the following virtual server data:

- NetScaler® IP address
- Host name
- Partition data
- Virtual Server name
- Type of virtual server
- Virtual server
- Target LB virtual server

NOTE

For Content Switching and Cache Redirection virtual servers, the Target LB virtual server column lists all the LB servers, that is, both default servers and policy-based servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Service name
- Service group name

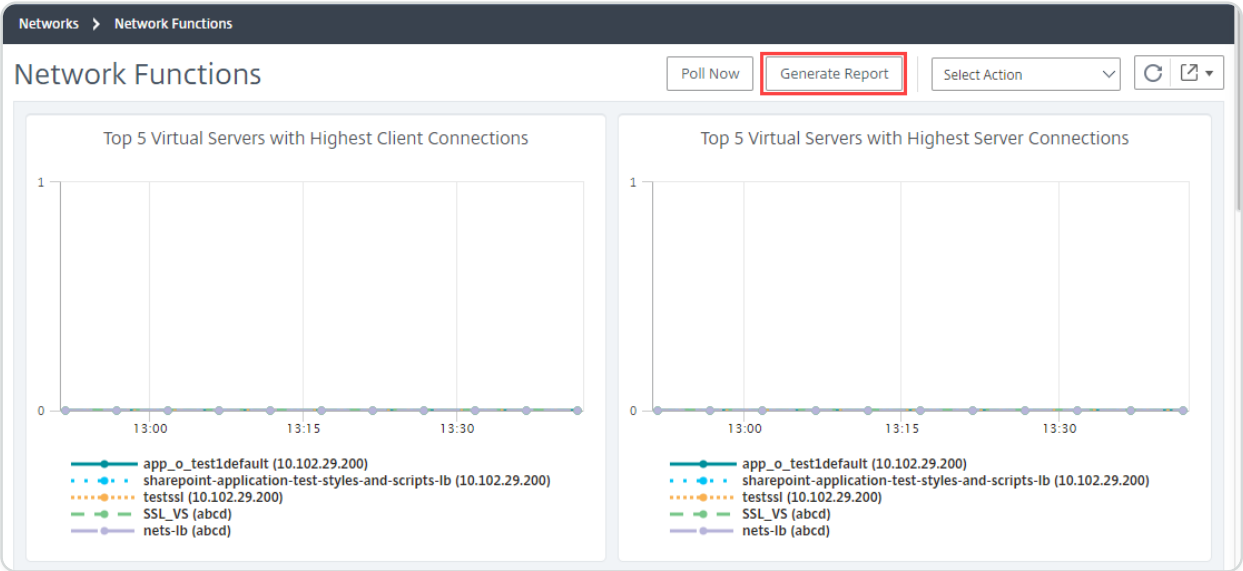
You can schedule to export these reports to specified email addresses at different intervals.

NOTE

- For GSLB virtual servers, the network functions report displays only GSLB virtual servers and associated services.
- For Content Switching and Cache Redirection virtual servers, the report displays only the bindings to the associated LB servers.
- SSL virtual servers are not listed in this report because a separate list of SSL virtual servers is not maintained on NetScaler ADM.
- When a new report is generated, the older reports are automatically purged from your account.
- You cannot generate a network functions report for HAProxy.

To export and schedule network functions reports:

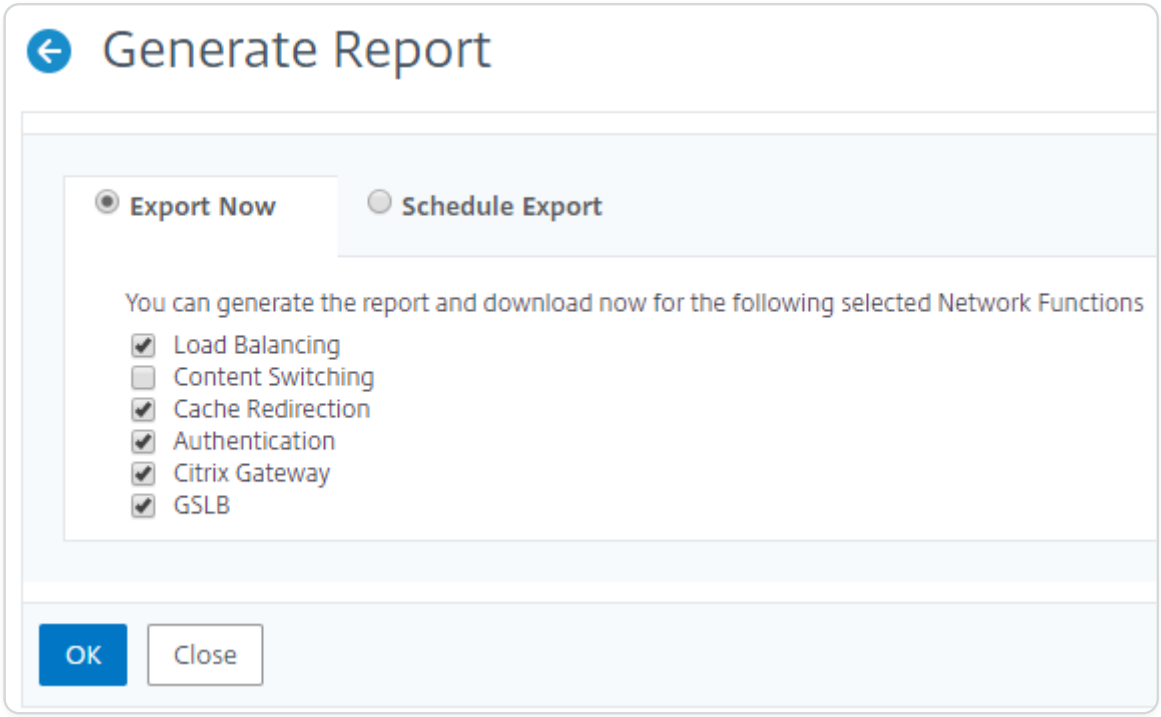
1. Navigate to **Infrastructure > Network Functions**.
2. On the **Network Functions** page, in the right pane, click **Generate Report** at the top right corner of the page.



3. On the **Generate Report** page, you have the following 2 options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Select **Export Now** tab and click **OK**. The report downloads to your system.



The following image shows an example of a network functions report.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.106	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

b. Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

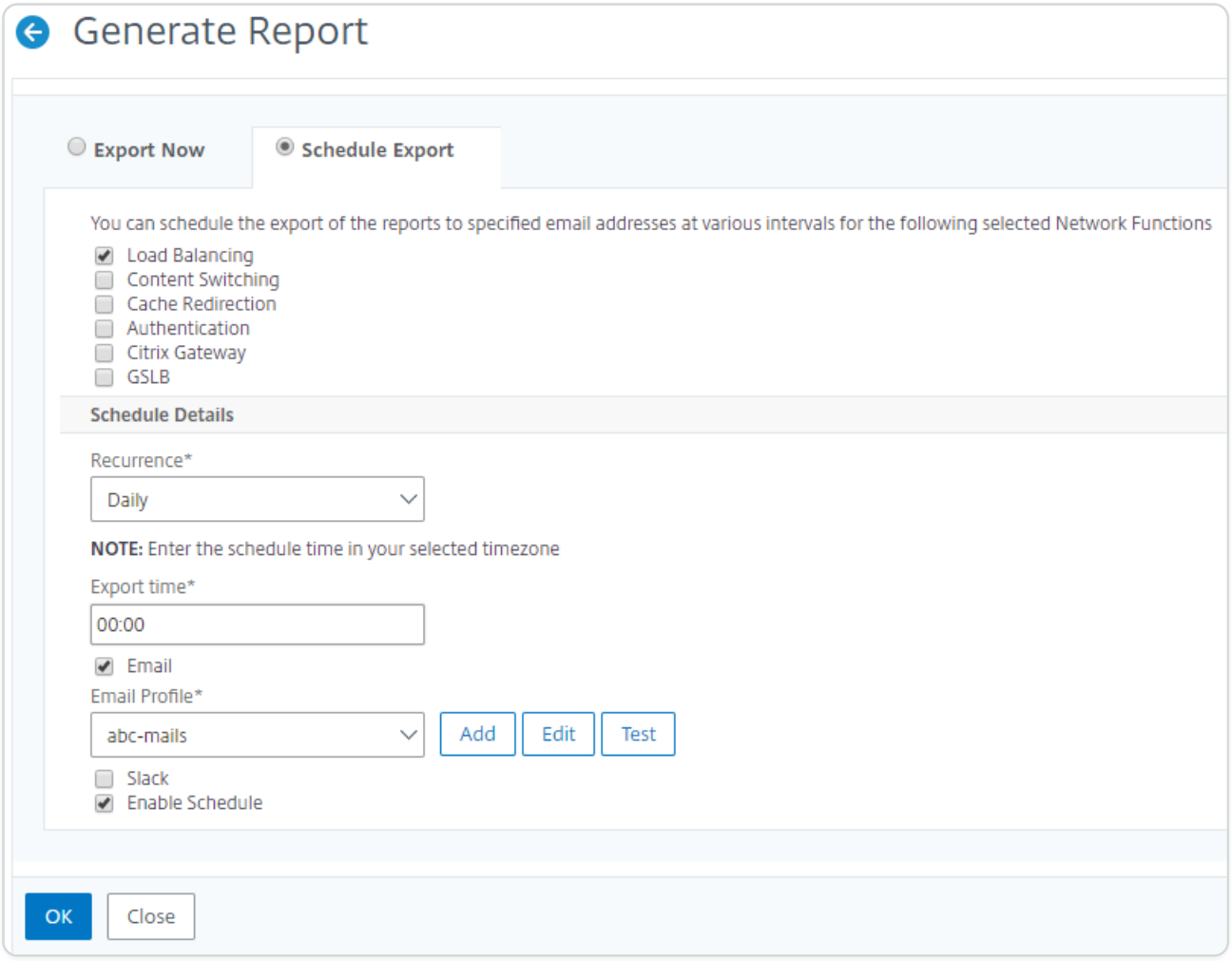
   i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

   ii. **Recurrence time**- Enter the time as Hour: Minute in 24-hour format.

   iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** to create an email profile.

Click **Enable Schedule** to schedule your report and then, click **OK**. By clicking the **Enable Schedule** check box, you can generate the selected reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Network reporting

You can optimize resource usage by monitoring your network reporting on NetScaler Application Delivery Management (NetScaler ADM). You may have a distributed deployment with many applications deployed at multiple locations. To ensure optimal performance of your applications, you have also deployed multiple Citrix Application Delivery Controller (NetScaler) instances to load balance, content switch, or compress the traffic. Network performance can impact the application performance. To continue to maintain the performance of your applications, you must regularly monitor your network performance and make sure all resources are used optimally.

NetScaler ADM now allows you to generate reports not only for instances at a global level but also for entities such as the virtual servers and network interfaces. The instance family comprises NetScaler instances. The virtual servers for which you can generate reports are as follows:

- Load balancing servers, services, and service groups
- Content switching servers
- Cache redirection servers

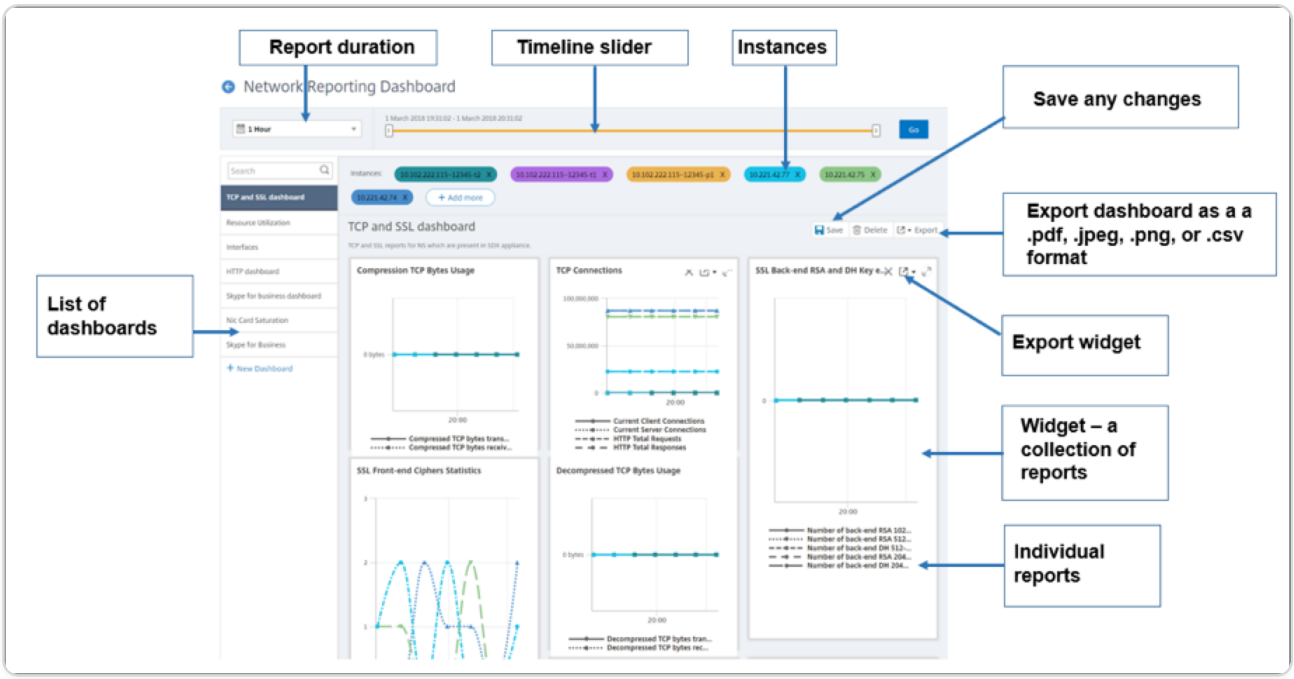
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Global service load balancing (GSLB)
- Authentication
- NetScaler Gateway

The network reporting dashboard in NetScaler® ADM is a highly customizable. You can now create multiple dashboards for various instances, virtual servers, and other entities.

Network reporting dashboard

The following image calls out the various features in the dashboard:



- The left side panel lists all the custom dashboards that are created in NetScaler ADM. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each dashboard with multiple widgets to display various reports. A widget represents a report on the dashboard, that is a collection of more related reports. For example, a compression TCP Bytes Usage report contains reports for compressed TCP bytes transferred and received per second.
- You can display reports for one hour, one day, one week, or for one month. In addition, you can now use the timeline slider option to customize the duration of reports being generated on the NetScaler ADM.
- You can remove a report by clicking "X". You can also export the report as a .pdf, .jpeg, .png, or .csv format to your system. You can also schedule a time and recurrence of when the report

© 1997–2026 Citrix Systems, Inc. All rights reserved.

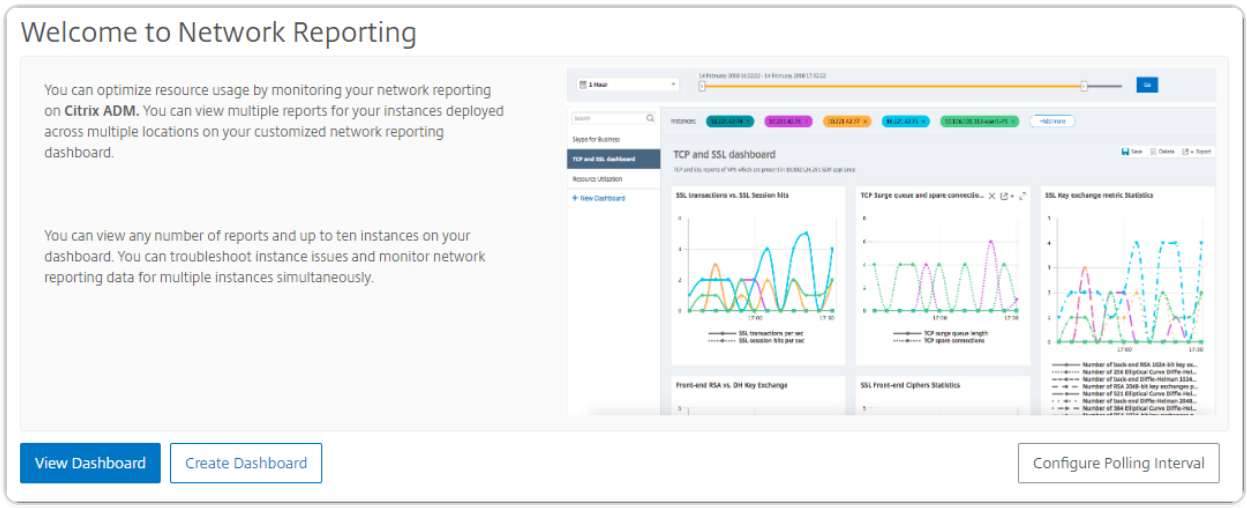
must be generated. You can also configure an email distribution list to which the reports must be sent.

- The Instances section at the top of the dashboard lists the IP addresses of all the instances for which the report is generated.
- You can either remove instances by clicking "X" or add more instances to the reports. But, currently NetScaler ADM allows you to view reports for 10 instances.
- You can also export the entire dashboard as a .pdf, .jpeg, .png, or .csv format to your system. Any changes made to the dashboard must be saved. Click Save to save the changes.

The following section explains in detail the tasks to create a dashboard, generate reports, and to export reports.

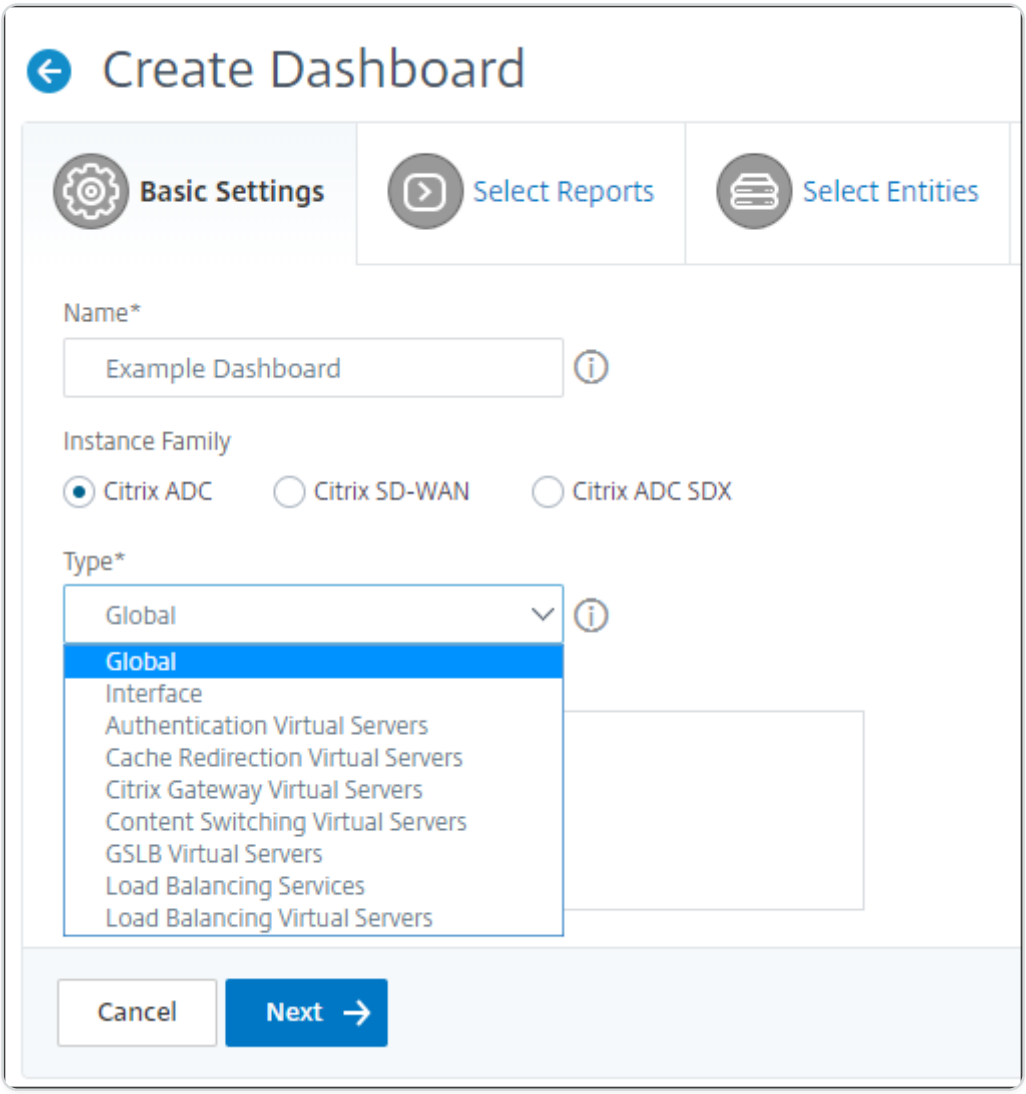
To view or to create a dashboard:

1. In NetScaler ADM, navigate to **Infrastructure > Network Reporting**.



2. To view the existing dashboards, click **View Dashboard**. The Network Reporting **Dashboard** page opens where you can view all your dashboards and report widgets.
3. To create a dashboard, click **New Dashboard**. The Create Dashboard page opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In the Basic Settings tab, enter the following details:

   a. **Name**. Type the name of the dashboard.

   b. **Instance Family**. Select the type of instance - NetScaler or NetScaler SDX.

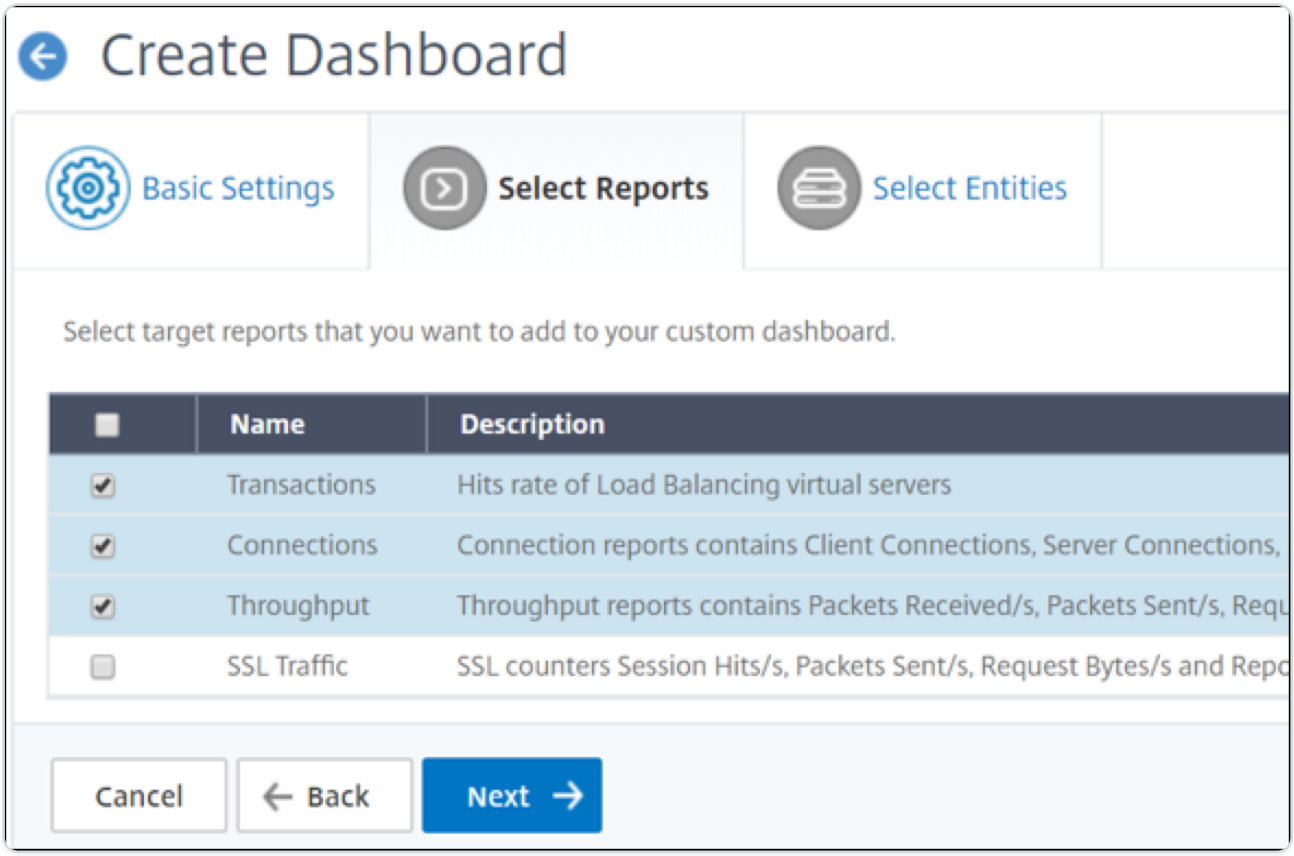
   c. **Type**. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.

   d. **Description**. Type a meaningful description for the dashboard.

5. Click **Next**. All the supported reports for the instance and the specific entity appear.

6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. In the **Select Entities** tab, click **Add**.

   A window appears with the entities list depending on the selected entity type in the **Basic Settings** tab. In this example, **Choose LB Virtual Servers** window appears.

2. Select the entities that you want to monitor.

3. Click **Create**.

The dashboard is created and displays all the reports that you have selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Currently, any changes that you make to legends or filters cannot be saved.

Exporting network reports

While you can export widget reports in .pdf, .png, .jpeg, or .csv formats, you can export the entire dashboards in only .pdf, .jpeg, or .png formats.

NOTE

You cannot export reports in NetScaler ADM if you have read-only permissions. You need an edit permission to be able to create a file in NetScaler ADM and to be able to export the file.

To export dashboard reports:

1. Navigate to **Infrastructure > Network Reporting**
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example, click **Dashboard 1**.
4. Click the export button at the top right corner of the page.
5. Under the **Export Now** tab, select the required format, and then click **Export**.

   On the **Export** page, you can do one of the following:

6. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
7. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or slack message.

   You can schedule an export of the **Network Reporting** dashboard page on a recurrent basis. For example, you can set an option to generate a dashboard report every week for the previous one hour at a particular time. The report is generated every week then and shows the status of the dashboard. The report overrides the time and date stamp, if set by the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- if you select Weekly recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select Monthly recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

While scheduling network reports, you can customize the heading of the report by entering a text string in the **Subject** field. The report created at the scheduled time has this string as its name.

For example, for network reports originating from a particular virtual server, you can type in the subject as "authentication-reports-10.106.118.120," where 10.106.118.120 is the IP address of the monitored virtual server.

NOTE

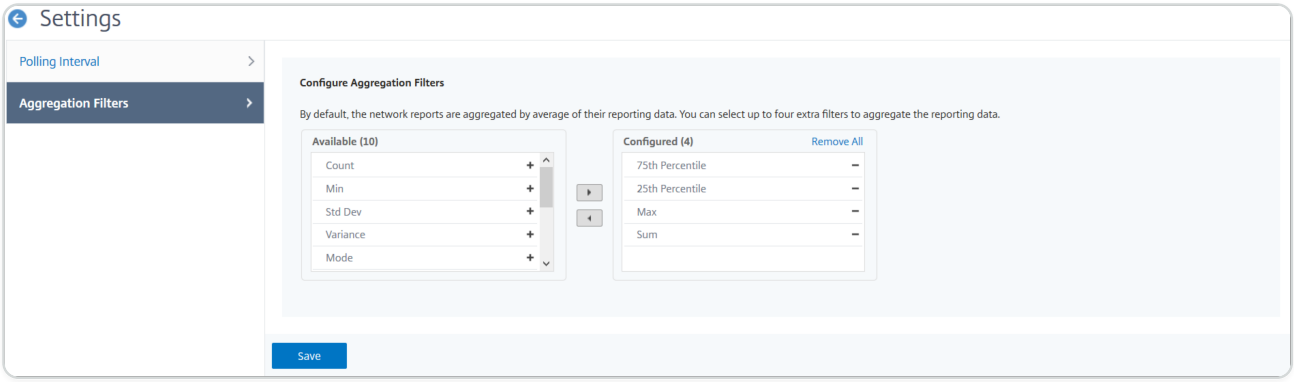
Currently, this option is available only when you schedule the export of reports. You cannot add a heading to the report when you export them instantly.

View network reporting data by applying aggregations

You can apply aggregations to the network performance data and view application performance on the dashboard. You can also export the results based on your requirement. Using these aggregations applied to the data, you can analyze and ensure if all resources are used optimally. Navigate to **Network > Network Reporting** and select the time duration 1 day or later to get the **View By** option.

In the existing average data, you can apply aggregations by selecting the option from the **View By** list. When you apply aggregation, the data is updated for each metric in the dashboard. Click **Settings** and select **Aggregation Filters**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following are the aggregations that you can add:

- Count
- Max
- Min
- Sum
- Std Dev
- Variance
- Mode
- Median
- 25th Percentile
- 75th Percentile
- 95th Percentile
- 99th Percentile
- First
- Last

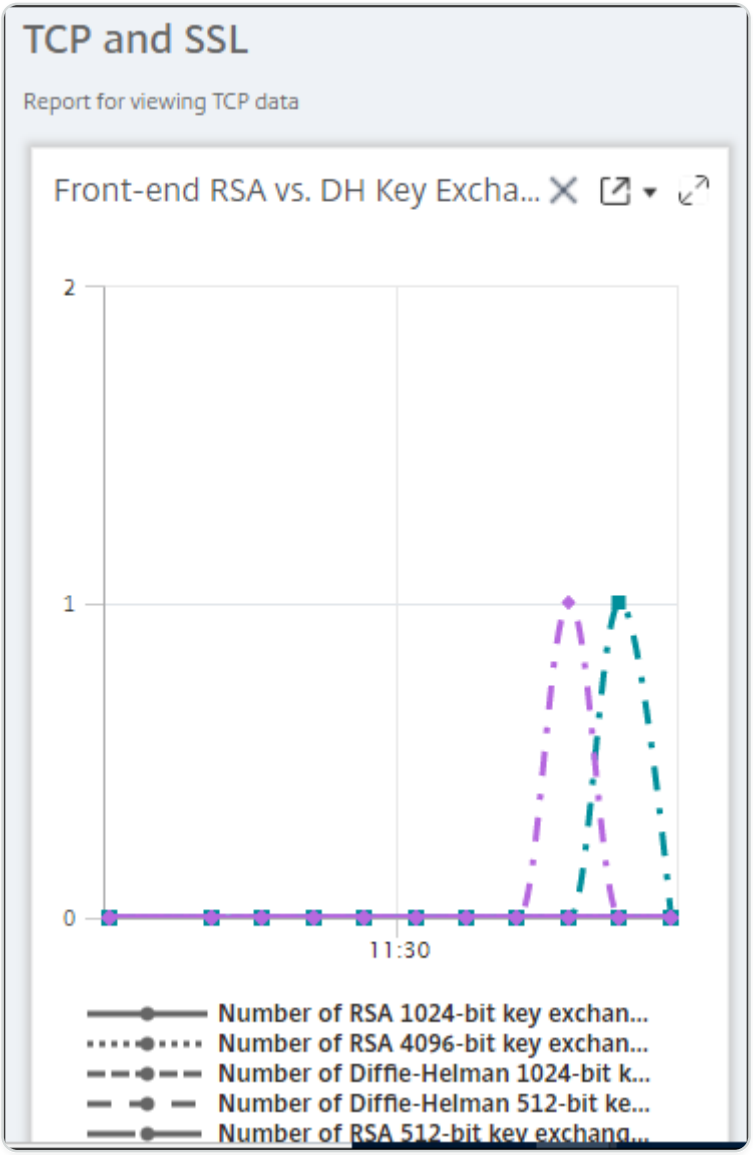
You can add up to 4 aggregation options to the dashboard. After you add the aggregation options, NetScaler ADM takes approximately 1 hour to generate reports for the selected aggregation options.

To export widget reports:

1. Navigate to **Infrastructure > Network Reporting**.
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example also click **Skype for Business**.
4. Select a widget. For example, select **Load Balancing Virtual Server Transactions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click the export button at the top right corner of the page
6. Under the **Export Now** tab, select the required format, and then click **Export**.



How to manage Thresholds for Network Reports on NetScaler ADM

To monitor the state of a NetScaler instance, you can set thresholds on counters and receive notifications when a threshold is exceeded. On NetScaler ADM, you can configure thresholds and view, edit, and delete them.

For example, you can receive an email notification when the Connections counter for a content switching virtual server reaches a specified value. You can define a threshold for a specific instance type. You can also choose the reports you want to generate for specific counter metrics from your chosen instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the value of a counter exceeds or falls below (as specified by the rule) the threshold value, an event of the specified severity is generated to signify a performance-related issue. When the counter value returns to a value that you consider normal, the event is cleared. These events can be viewed by navigating to **Infrastructure > Events > Reports**. On the Reports page, you can click the **Events by Severity** donut to view events by their severity.

You can also associate an action with a threshold such as sending an email or SMS message when the threshold is breached.

To create a threshold:

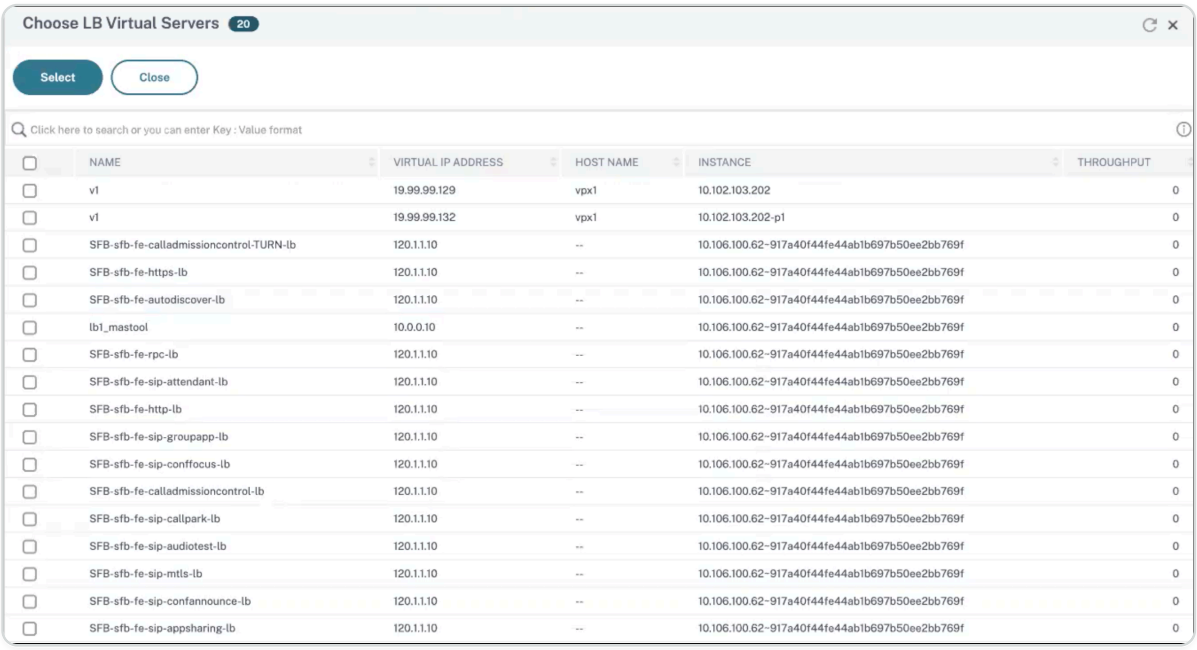
1. In NetScaler ADM, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Threshold** page, specify the following details:
   - **Name**. Name of the threshold.
   - **Instance Type**. Choose NetScaler.
   - **Report Name**. Name of the performance report that provides information about this threshold.
3. You can also set rules to specify when an event is to be generated or cleared. You can specify the following details under the **Configure Rule** section:
   - **Metric**. Select the metric for which you want to set a threshold.
   - **Comparator**. Select a comparator to check whether the monitored value is greater than or equal to or less than or equal to the threshold value.
   - **Threshold Value**. Type the value for which the event severity is calculated. For example, you might want to generate an event with critical event severity if the monitored value for Current Client Connections reaches 80 percent. In this case, type 80 as the threshold value. You can view “critical severity” events by navigating to **Infrastructure > Events > Reports**. On the Reports page, you can click the **Events by Severity** donut to view events by their severity.
   - **Clear Value**. Type the value that indicates when to clear the value. For example, you might want to clear the Current Client Connections threshold when the monitored value reaches 50 percent. In this case, type 50 as the clear value.
   - **Event Severity**. Select the security level that you want to set for the threshold value.
4. You can choose instances and entities to be set with the threshold value. In the **Instances** section, choose one of the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **All Instances**. The threshold is set for all the instances.
- **Specific Instances**. The threshold is set for specific instances. Use the right arrow to move instances from the **Available** list to the **Configured** list. The threshold is set for the instances in the **Configured** list.
- **Specific Entities**. The threshold is set for specific entities.

  Click **Add** to select the entities.

  A window appears with the entities list depending on the selected report type in the **Report Name** field. In this example, the **Choose LB Virtual Servers** window appears.



NAME	VIRTUAL IP ADDRESS	HOST NAME	INSTANCE	THROUGHPUT
v1	19.99.99.129	vpx1	10.102.103.202	0
v1	19.99.99.132	vpx1	10.102.103.202-p1	0
SFB-sfb-fe-calladmissioncontrol-TURN-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-https-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-autodiscover-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
lb1_mastool	10.0.0.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-rpc-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-attendant-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-http-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-groupapp-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-conffocus-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-calladmissioncontrol-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-callpark-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-audiotest-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-mtls-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-confannounce-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0
SFB-sfb-fe-sip-appsharing-lb	120.1.1.10	--	10.106.100.62~917a40f44fe44ab1b697b50ee2bb769f	0

  Select the entities for which you want to set a threshold. Click **Select**. The selected entities appear in the **Instances** section.

  NOTE

  The **Specific Entities** option appear only if you select vserver based reports in **Report Name**. For example, if you select **LB Service Statistics**

5. You can also add an **Event Message**. Type a message that you want to appear when the threshold is reached. NetScaler ADM appends the monitored value and the threshold value to this message.
6. Select **Enable** to enable the threshold to generate alarms.
7. Optionally, you can configure **Actions** such as email or Slack notifications or both email and Slack notifications.

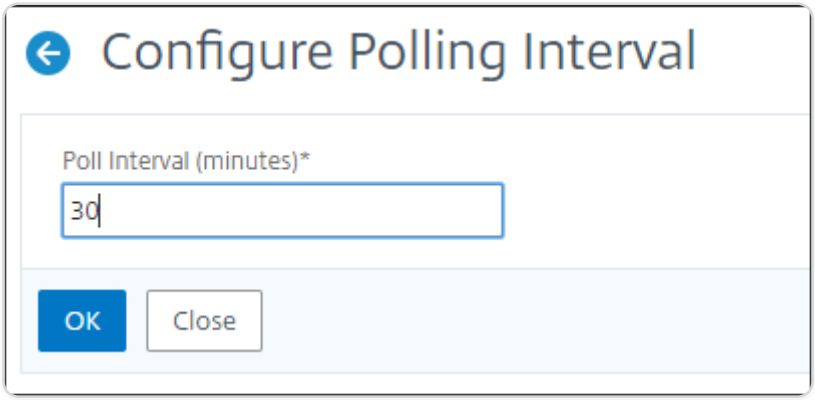
© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Create**.

Set Performance Polling Interval for Network Reports

By default, every 5 minutes, NITRO calls collect performance data for network reporting. ADM retrieves instance statistics such as counter information and aggregates them based on per minute, per hour, per day, or per week. You can view this aggregated data in predefined reports.

To set the performance polling interval, navigate to **Infrasturcture > Network Reporting** and click **Configure Polling Interval**. Your polling interval cannot be less than 5 minutes or more than 60 minutes.



Configuring Network Reporting Prune Settings

You can configure the purge interval of network reporting data in NetScaler ADM. This setting limits the amount of network reporting data being stored in the NetScaler ADM server's database. By default, pruning happens every 24 hours (at 01.00 hours) for the network reporting historical data.

NOTE

The value that you can specify cannot exceed 30 days or be less than 1 day.

Configuration jobs

NetScaler Application Delivery Management (NetScaler ADM) configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple Citrix Application Delivery Controller™ (ADC) instances in the network.

NetScaler® ADM allows you to create configuration jobs that help you to perform all these activities with ease on several devices as a single task. Configuration jobs and templates simplify the most

© 1997–2026 Citrix Systems, Inc. All rights reserved.

repetitive administrative tasks to a single task on NetScaler ADM. A configuration job contains a set of configuration commands that you can run on one or multiple managed devices.

Configuration Jobs can either use SSH commands to do configuration commands or use SCP to do file copy from either locally or to another appliance, for example, we can schedule a HA-failover or HA-upgrade.

You can create a configuration job by using one of the following four options in NetScaler ADM. Use one of these to create a reusable source of commands and instructions to the system to run a configuration job.

1. Configuration Template
2. Instance
3. File
4. Record and Play

Configuration Template

You can create configuration templates while creating a job and saving a set of configuration commands as a template. When you save these templates on the Create Jobs page, they are automatically displayed on the Create Template page.

Note The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

You can use one of the following templates:

Configuration Editor: You can use the configuration editor to type in CLI commands, save the configuration as a template, and use it to configure jobs.

Inbuilt Template: You can choose from a list of configuration templates. These templates provide the syntaxes of the CLI commands and allow you to specify values for the variables. The inbuilt templates are listed, with their descriptions in the table below. You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can also, choose to run the job immediately or schedule the job to be run at a later stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance

You can perform a single-bundle upgrade of your NetScaler SDX instances running NetScaler release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in NetScaler ADM. You can also upgrade a NetScaler instance by extracting the running configuration or a saved configuration and running the commands on another NetScaler instance of the same type. This allows you to replicate the configuration of one instance on the other.

File

You can upload a configuration file from your local machine and create jobs.

Advantages of using a file

- You can use any text file to create a reusable source of configuration commands.
- Any kind of formatting is not required.
- The file can be saved on your local machine.

You can either create and save a new file or import an existing file, and run the commands.

Record and Play

Using Create job you can either enter your own CLI commands, or you can use the record and play button to get commands from a NetScaler session. When you run the job, changes in the ns.conf on the selected instance are recorded and copied to NetScaler ADM.

Related Articles

- How to Use SCP (put) Command in Configuration Jobs
- How to Use Variables in Configuration Jobs
- How to Create Configuration Jobs from Corrective Commands
- How to Use Configuration Templates to Create Audit Templates
- How to Use Record-and-Play to Create Configuration Jobs
- How to Use the Master Configuration Template on NetScaler ADM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a configuration job

A job is a set of configuration commands that you can create and run on one or more multiple managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler Application Delivery Management (ADM) GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of NetScaler® ADM to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on NetScaler ADM:

1. Navigate to the **Infrastructure > Configuration Jobs**.
2. Click **Create Job**.
3. On the **Create Job** page, under the **Select Configuration** tab, specify the Job Name and select the **Instance Type** from the list.
4. In the **Configuration Source** list, select the configuration job template that you want to create. Add the commands for the selected template.

   - You can either enter the commands or import the existing commands from the saved configuration templates.
   - You can also add multiple templates of different types in the Configuration editor while creating a job in the Configuration Jobs.
   - From the **Configuration Source** list, select the different templates and then drag the templates into the configuration editor. The template types can be **Configuration Template**, **In built Template**, **Master Configuration**, **Record and Play**, **Instance** and **File**.

   NOTE

   If you add the `Deploy Master Configuration Job` template for the first time, add a template of different type, then the whole job template becomes a `Master Configuration` type.

   You can also rearrange and reorder the commands in the configuration editor. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the command line number in the text box. You can also rearrange and reorder the command line while editing the configuration job.

You can define variables that enable you to assign different values for these parameters or run a job across multiple instances. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view. Click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

You can customize rollback commands for every command on the configuration editor. To specify your customized commands, Enable the custom rollback option.

IMPORTANT

For custom rollback to take effect, complete the **Create Job** wizard. And in the **Execute** tab, select the **Rollback Successful Commands** option from the **On Command Failure** list.

5. In the **Select Instances** tab, select the instances on which you want to run the configuration audit.

   a. In a NetScaler high-availability pair, you can run a configuration job local to a primary or a secondary node. Select on which node you want to run the job.

      - **Execute on primary nodes** - Select this option to run the job only on primary nodes.
      - **Execute on secondary nodes** - Select this option to run the job only on secondary nodes.

      You can also choose both primary and secondary node to run the same configuration job. If you do not select either primary or secondary node, automatically the configuration job runs on the primary node.

6. In the **Specify Variable Values** tab, you have two options:

   a. Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler ADM server.

   b. Enter common values for the variables that you have defined for all instances

   c. Click **Next**.

To send an email and Slack notification for a job:

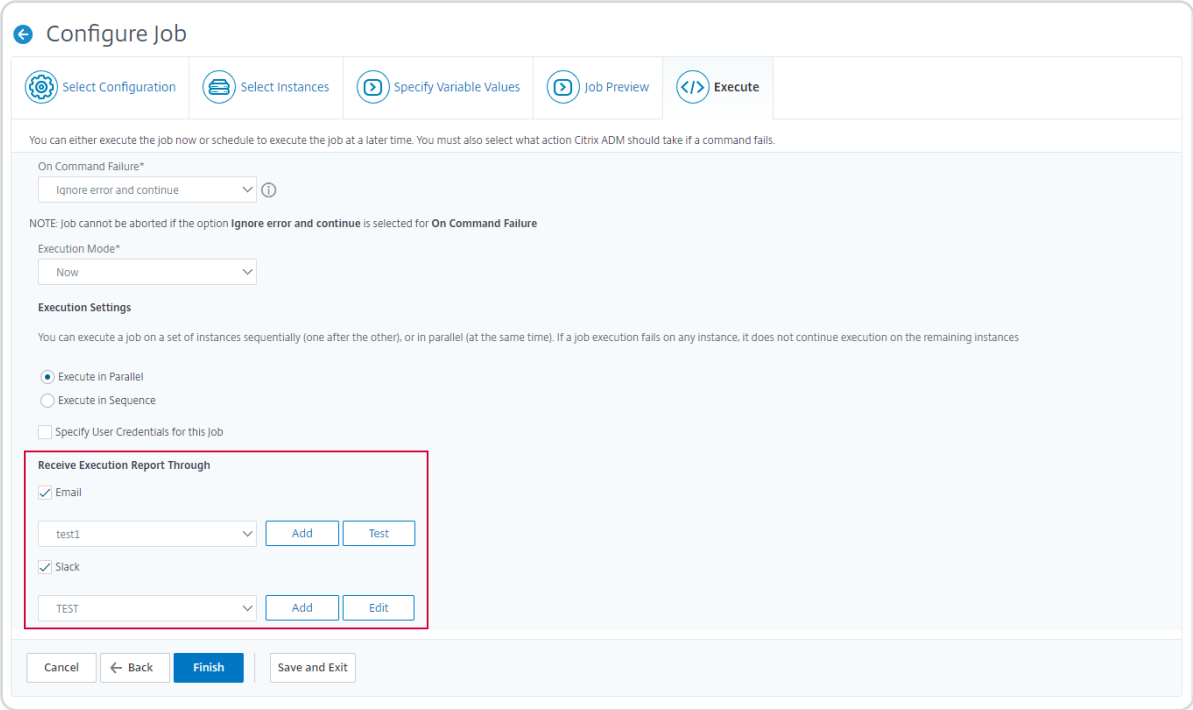
© 1997–2026 Citrix Systems, Inc. All rights reserved.

An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

1. Navigate to **Infrastructure > Configuration Jobs**.
2. Select the job that you want to enable email and Slack notification and click **Edit**.
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

     If you want to add an email distribution list, click **Add** and specify the email server details.
   - Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

     If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.



4. Click **Finish**.

To send an email and Slack notification for a job:

An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

1. Navigate to **Infrastructure > Configuration Jobs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

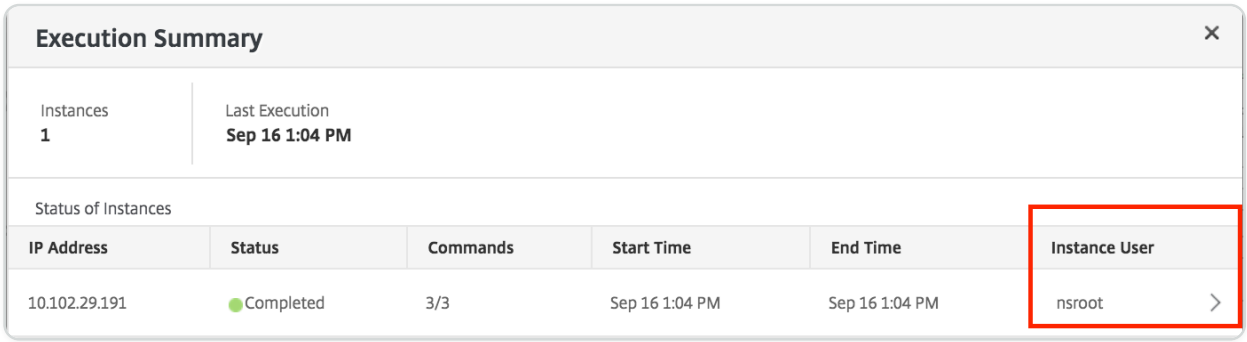
2. Select the job that you want to enable email and Slack notification and click **Edit**.
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

     If you want to add an email distribution list, click **Add** and specify the email server details.
   - Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

     If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.
4. Click **Finish**.

To view execution summary details:

1. Navigate to **Infrastructure > Configuration Jobs**.
2. Select the job that you want to view the execution summary and click **Details**.
3. Click **Execution Summary** to see:
   - The status of the instance on that run the job
   - The commands run on the job
   - The start and end time of the job, and
   - The instance user's name



Use record-and-play to create configuration jobs

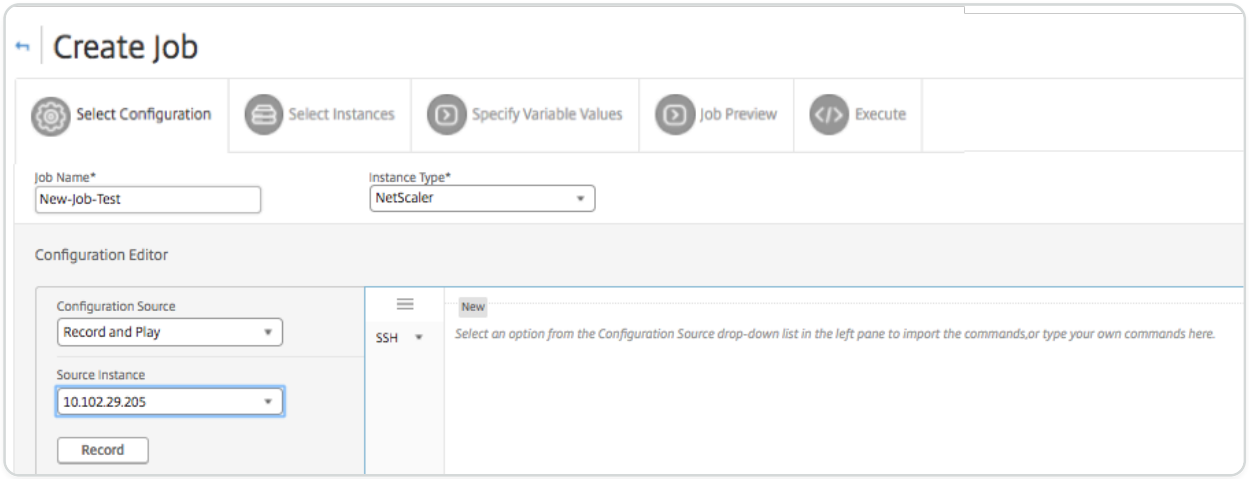
If you are accustomed to using the NetScaler GUI to configure a NetScaler instance, at times, you might find it difficult to recall the exact CLI commands to create a configuration task and run it on multiple NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

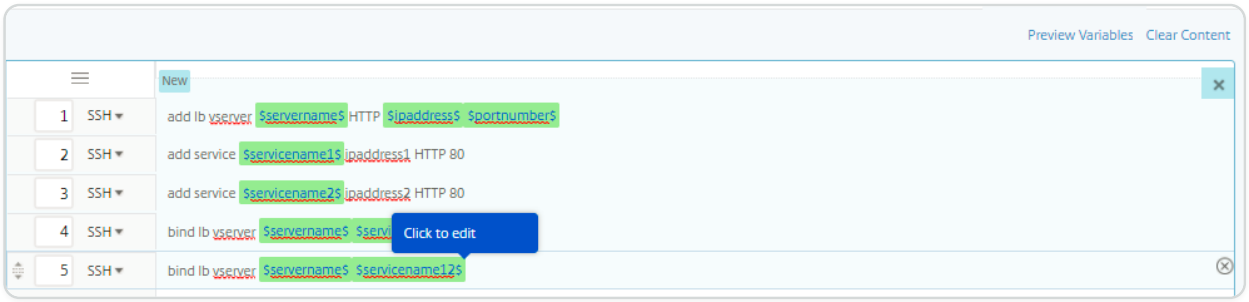
NetScaler ADM enables you to record the configuration tasks performed using the GUI of a NetScaler instance and convert it into CLI commands. You can then create a configuration task from these CLI commands and run this task on multiple instances.

To record the GUI configuration and convert it into a configuration task

1. Navigate to **Infrastructure > 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 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.

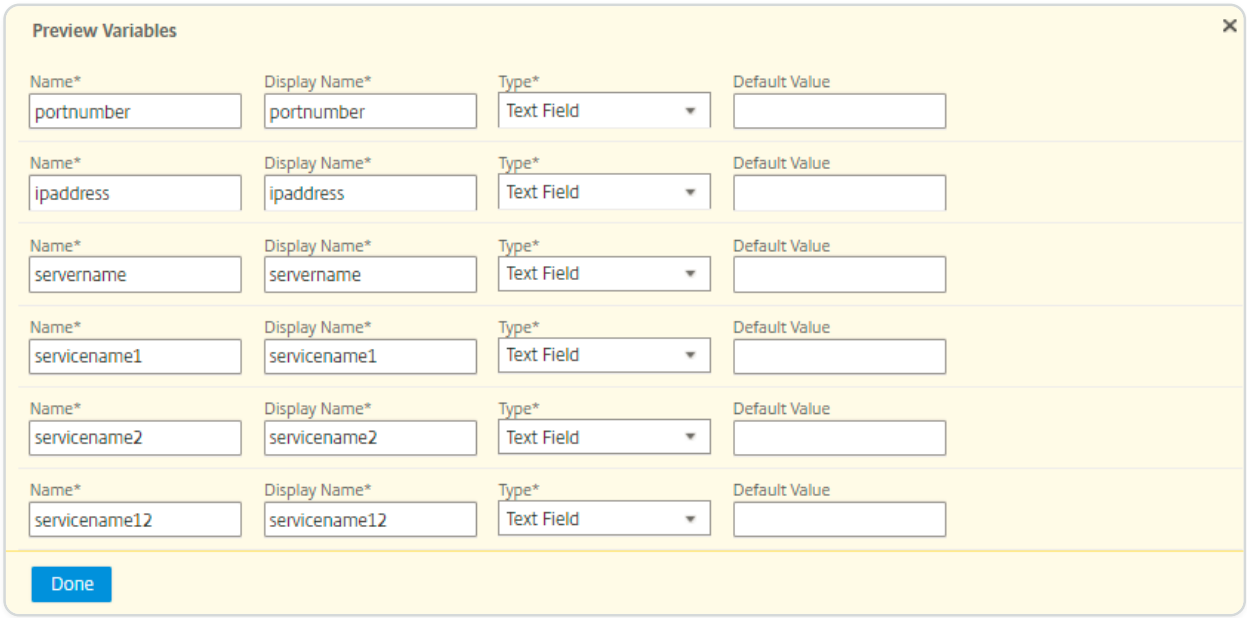
5. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
6. Do one of the following to view all the variables in a single consolidated view:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- While creating a configuration job, navigate to **Infrastructure > 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.

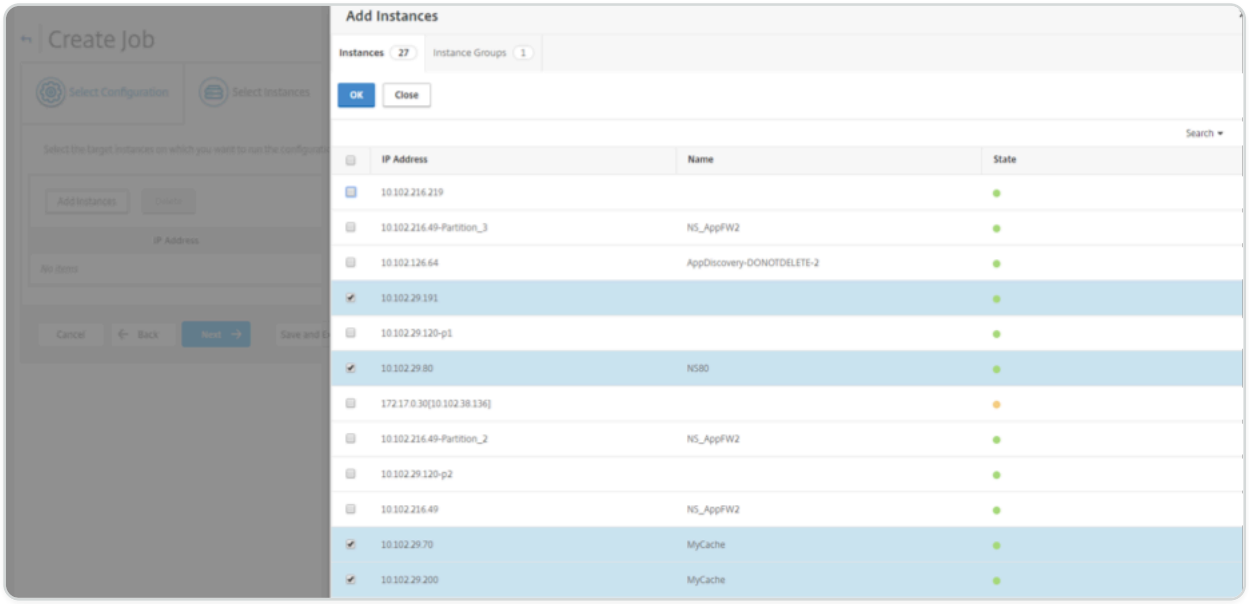
7. You can then click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

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 **Add Instances** and select the instances on which you want to run the configuration job. Click **OK**, and then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler® 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 run 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).

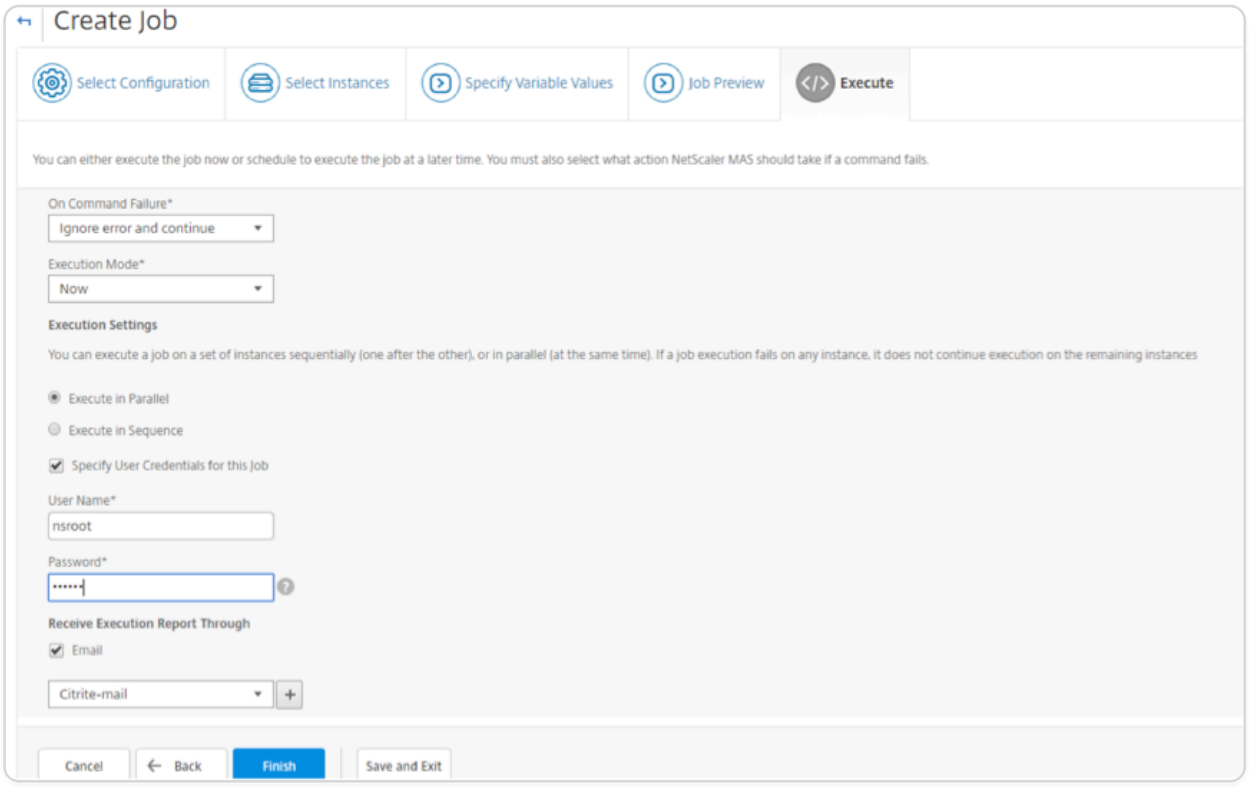
    To view the already run configuration jobs while editing a configuration job, navigate to **Network \> Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to 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).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 **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

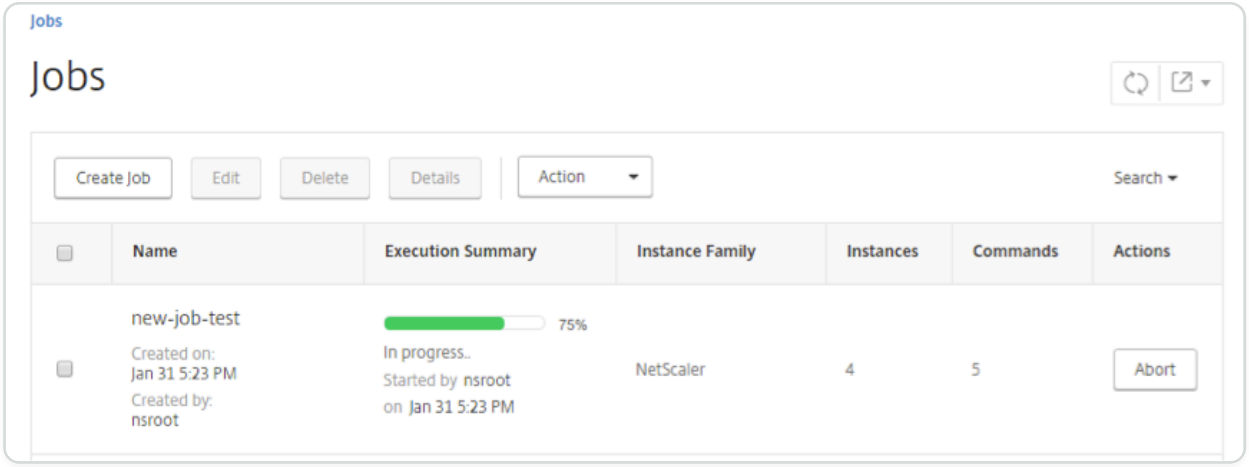
© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. On the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler ADM must take if the command fails.

    You can also choose to allow authorized users to run 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

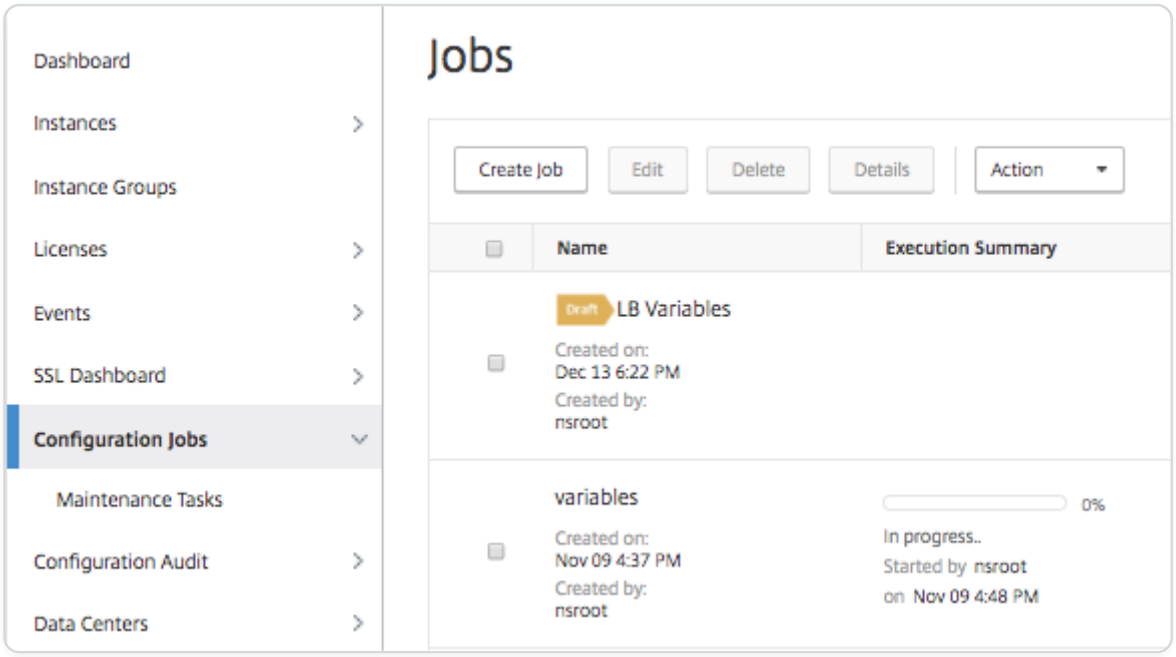
Use configuration jobs to replicate configuration from one instance to multiple instances

You can use the Configuration Jobs feature of NetScaler 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:

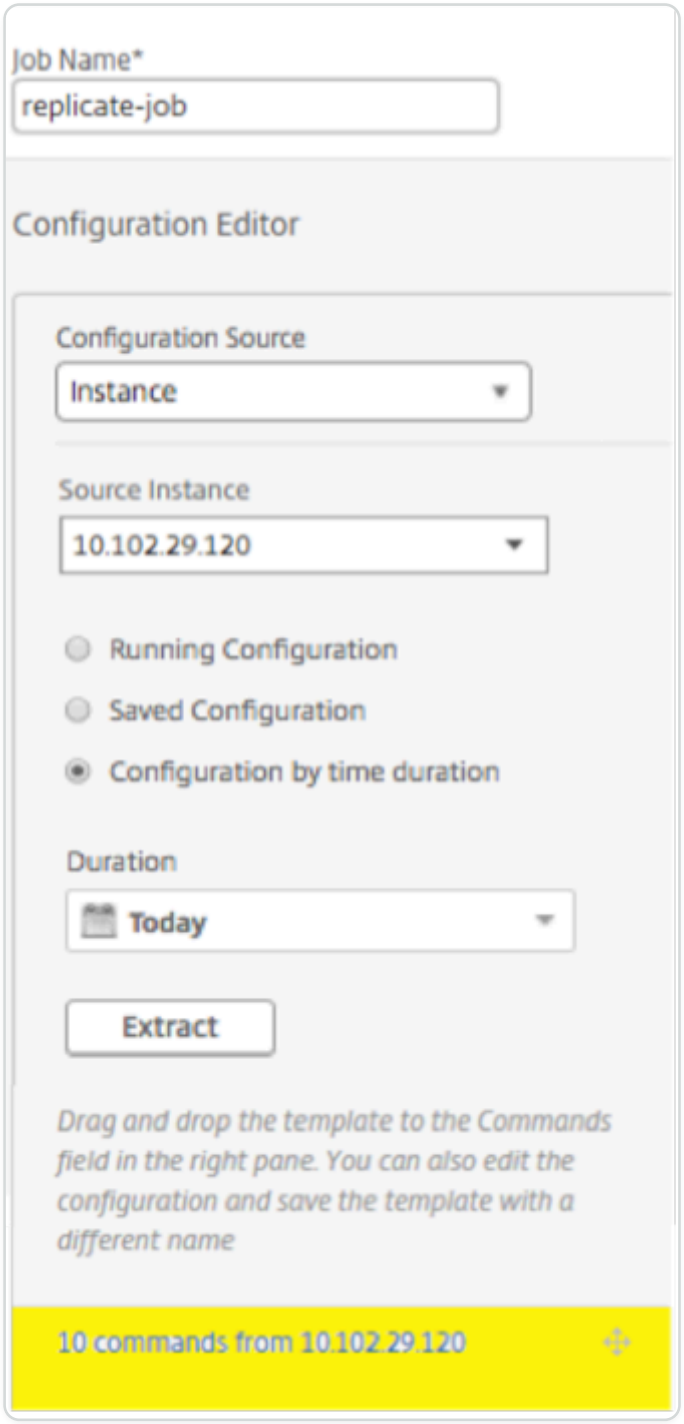
1. Navigate to **Infrastructure > Configuration Jobs**, and then click **Create Job**.



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 run on that instance in the time duration you selected is displayed on the screen as highlighted in the following image.

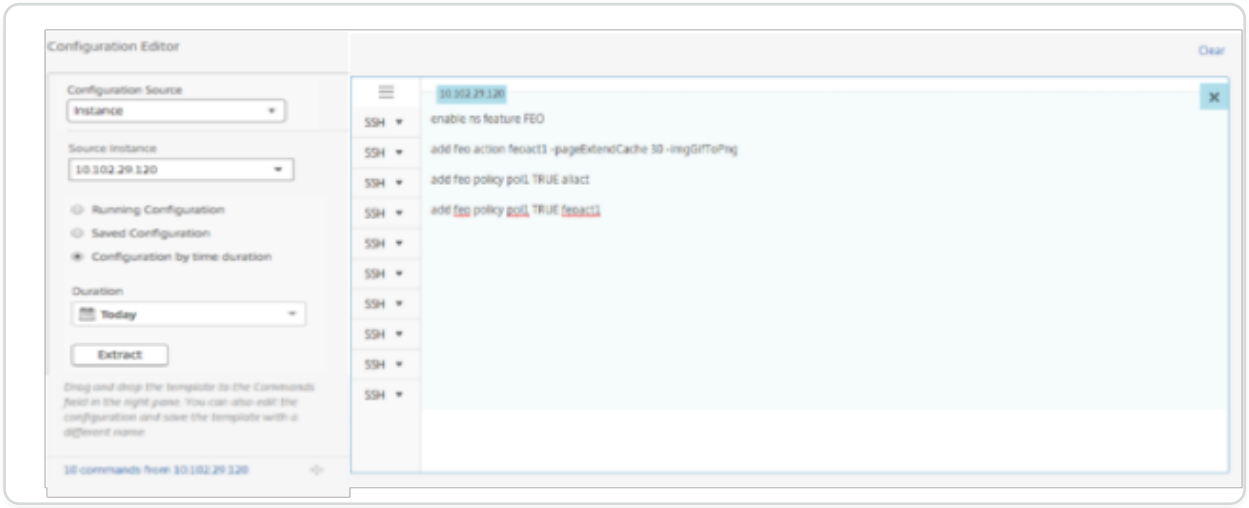
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Drag the commands to the **Commands** field in the right pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler® 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 run the job on the selected NetScaler instances.

Use variables in configuration jobs

A configuration job is a set of configuration commands that you can run on one or more managed instances. When you run the same configuration on multiple instances, you might want to use

© 1997–2026 Citrix Systems, Inc. All rights reserved.

different values for the parameters used in your configuration. You can define variables that enable you to assign different values for these parameters or run 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
```

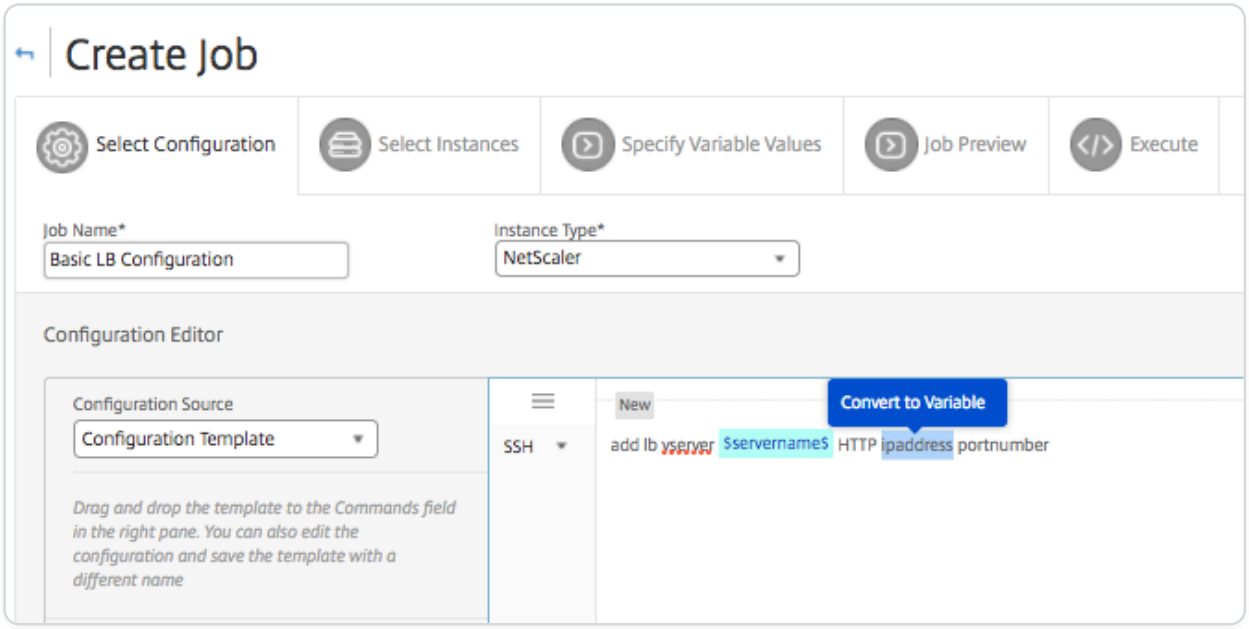
```
bind lb vserver <servername> <servicename1>
```

```
bind lb vserver <servername> <servicename2>
```

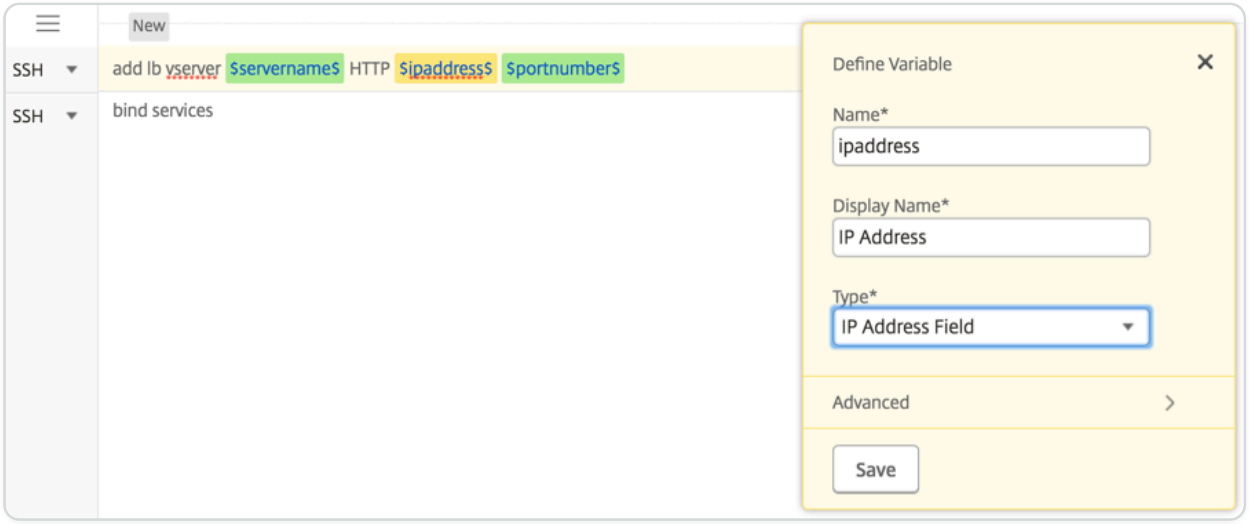
To create a configuration job by defining variables in NetScaler® ADM:

1. Navigate to **Infrastructure > 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 following image.

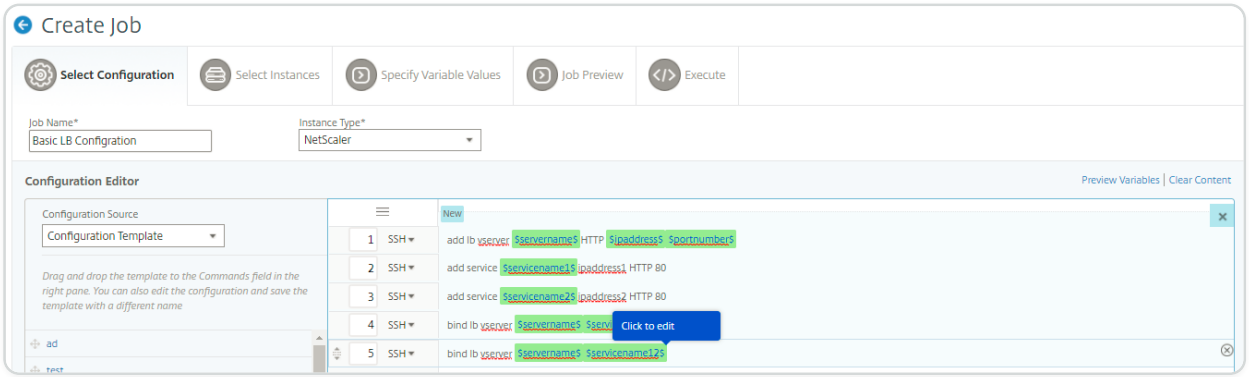
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Once you see dollar signs enclose the variable's value, click 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**.

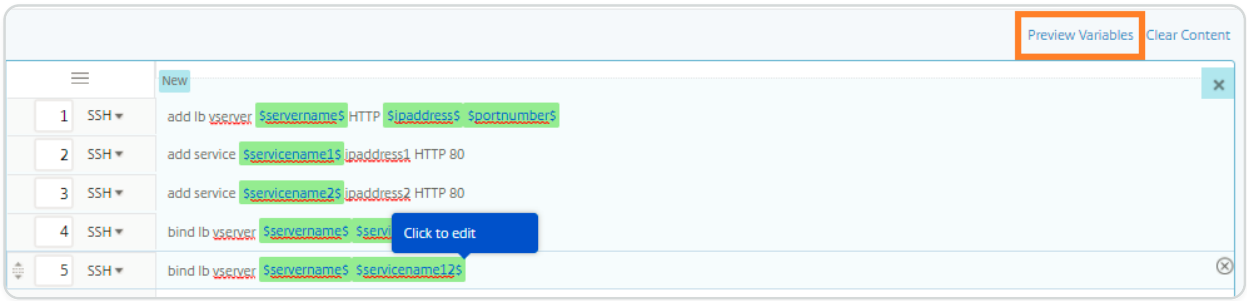


Type in the rest of your commands and define all the variables.

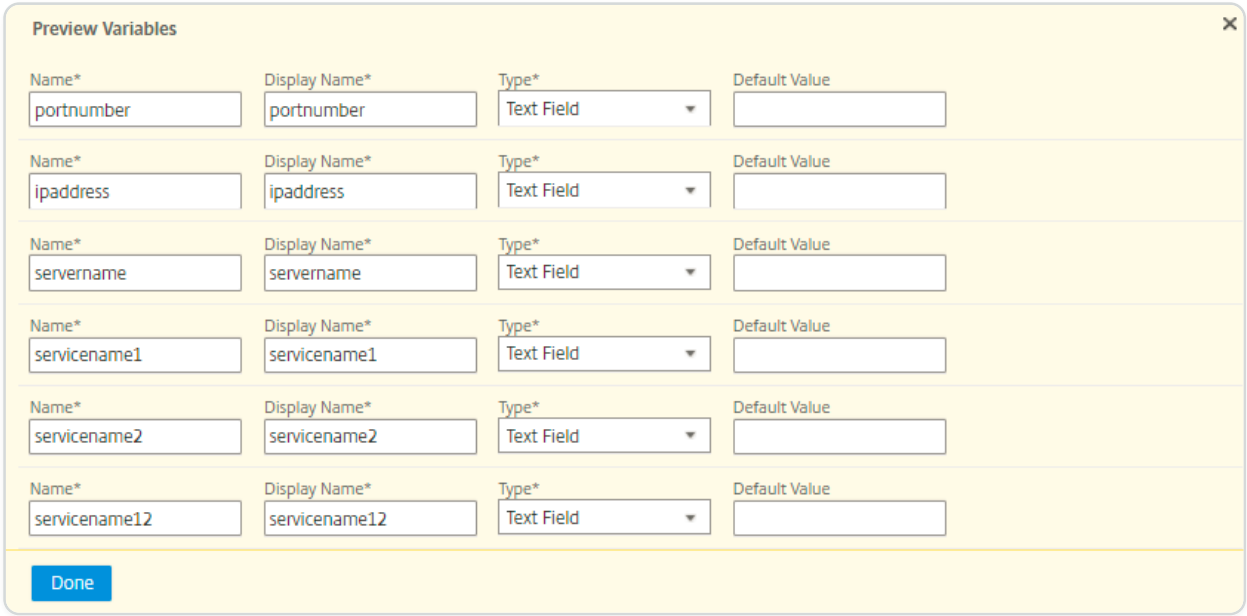


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **Infrastructure > 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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler 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.

    NetScaler ADM gives first priority to instance level values. If there are no values provided to the variables for individual instances, NetScaler ADM uses the value provided at the group level. If there are no values provided at group level, NetScaler ADM uses the variable value provided at the global level. If you provide an input for a variable across all three levels, NetScaler ADM uses the instance level value as the default value.
14. Click **Upload** to upload the input key file to NetScaler ADM. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

When you upload a CSV file from a Mac, the 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 NetScaler 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.

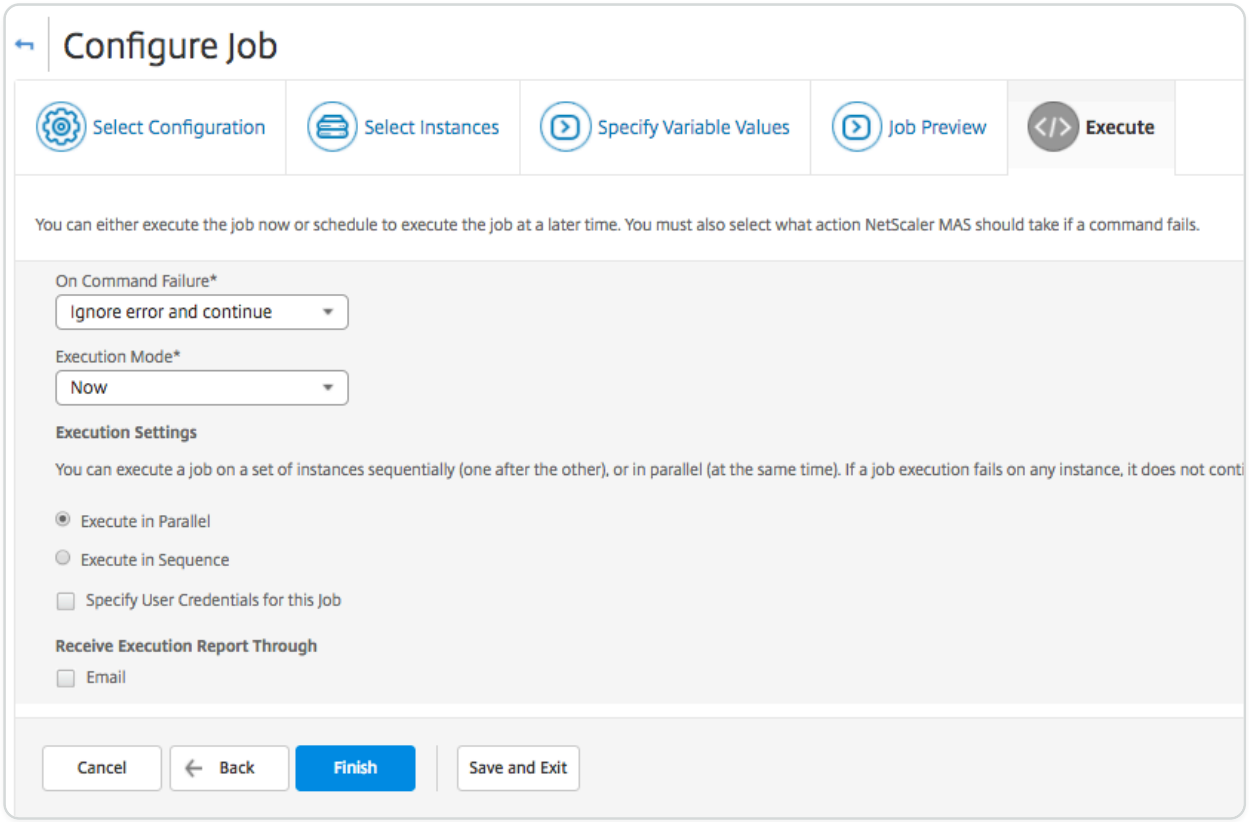
    To view the run configuration jobs while creating a configuration job, navigate to **Network \> Configuration Jobs**, and click **Create Job**. In the **Create Job** page. On the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. 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 run 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).

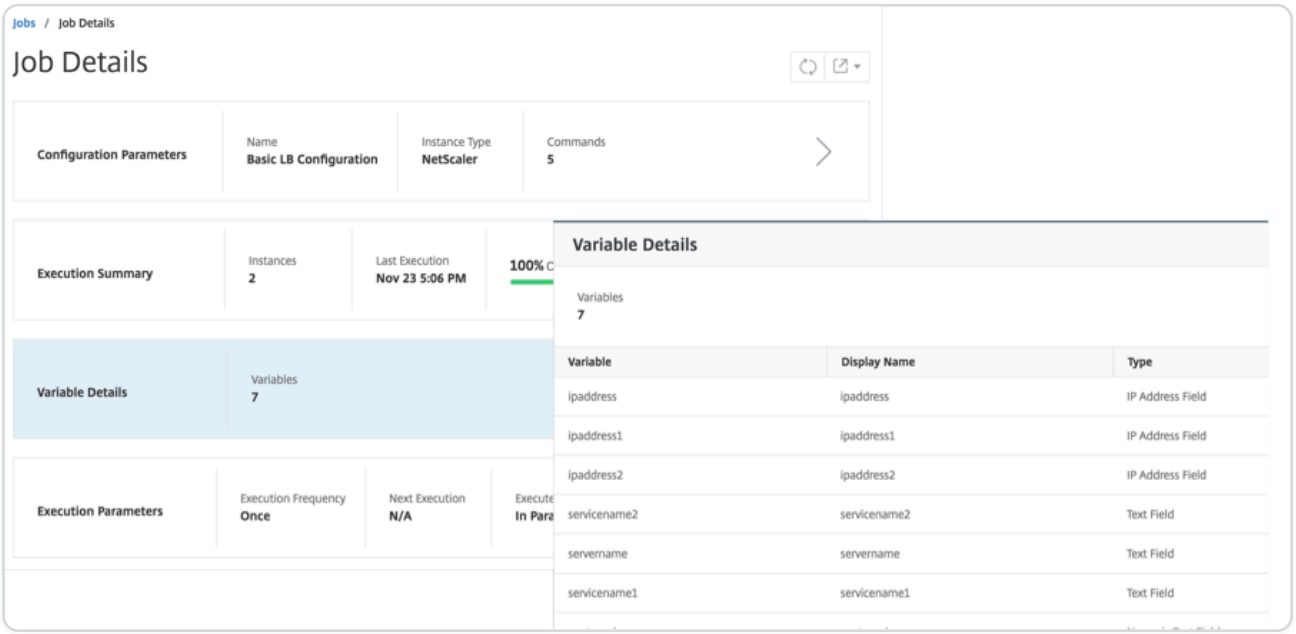
16. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

17. In the **Execute** tab, you can choose to run your job now or schedule it to be run at a later time. You can also choose what action NetScaler ADM must 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After configuring your jobs and running it, you can see the job details by navigating to **Infrastructure > Configuration Jobs** and select the job you just configured. Click **Details** and then, click **Variable Details** to see the list of variables added to your job.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The values that you have provided for the variables in **STEP 5** are retained by NetScaler 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

You can use the audit template feature in NetScaler Application Delivery Management (ADM) to monitor configuration changes across managed NetScaler 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 NetScaler commands for auditing instance configurations.
2. Select the NetScaler 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 NetScaler 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 NetScaler instances and runs it against the instances. NetScaler 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 NetScaler ADM corrective commands feature to create a configuration job with the modified and corrected configuration commands for specific NetScaler instances.

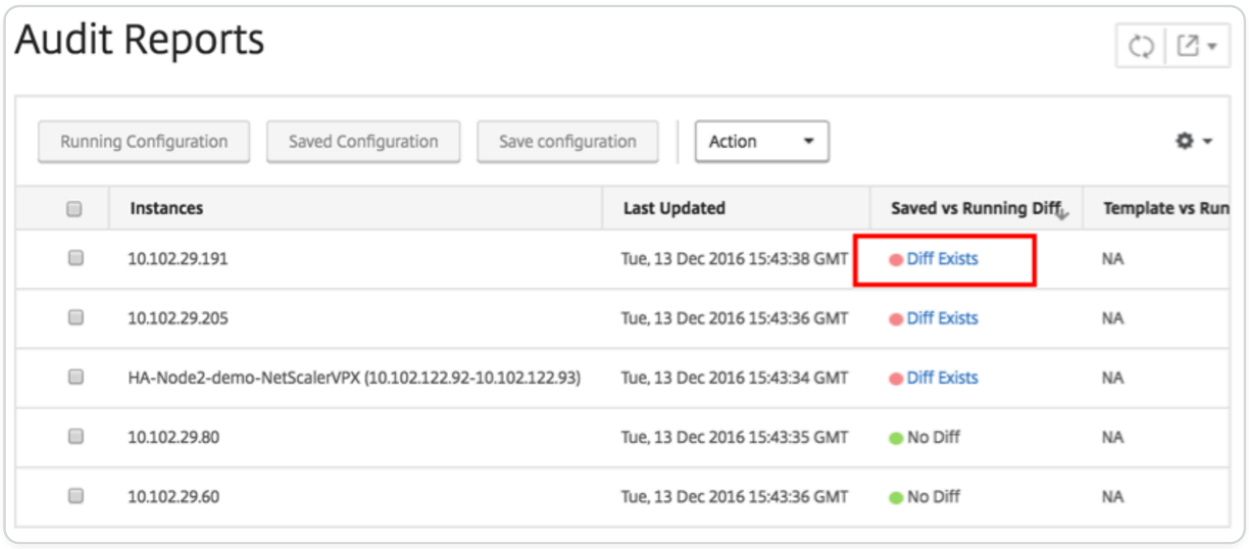
If any difference exists between the audit template configuration and the running configuration, a **Diff Exists** status message appears on the **Audit Report** page. Clicking the **Diff Exits** link takes you to the **Configuration Diff** page, where you can view the corrective command. You can also

© 1997–2026 Citrix Systems, Inc. All rights reserved.

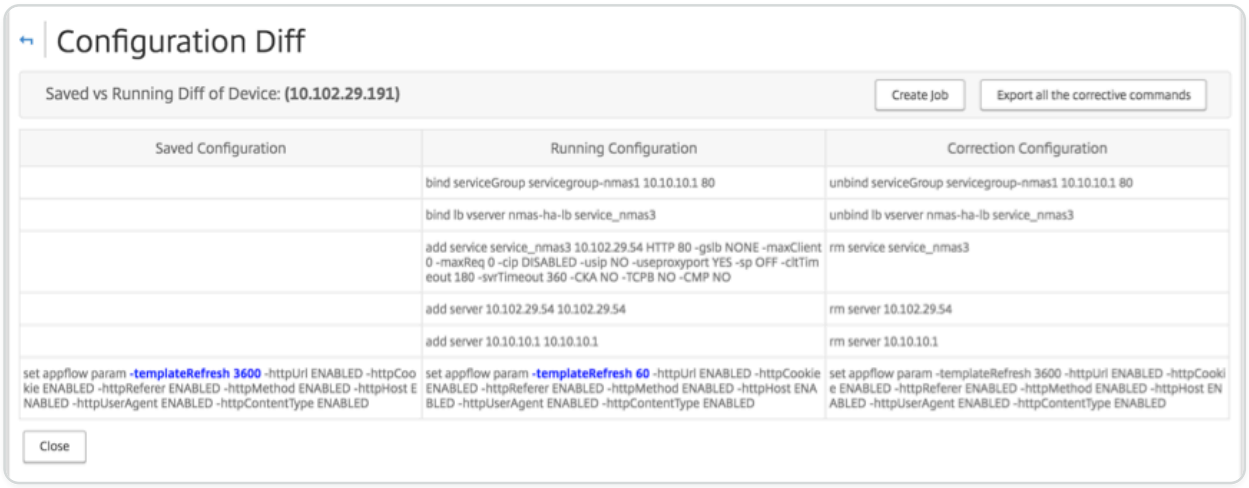
use these corrective commands to create a configuration job and run that on the specific NetScaler instances to get them back to the desired configuration.

To create a configuration job from corrective commands on NetScaler® ADM

1. Navigate to **Infrastructure > 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 pre-populated. For instructions on how to create a configuration job, see How to Create a Configuration Job on NetScaler ADM.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Replicate running and saved configuration from one NetScaler instance to another

May 24, 2018

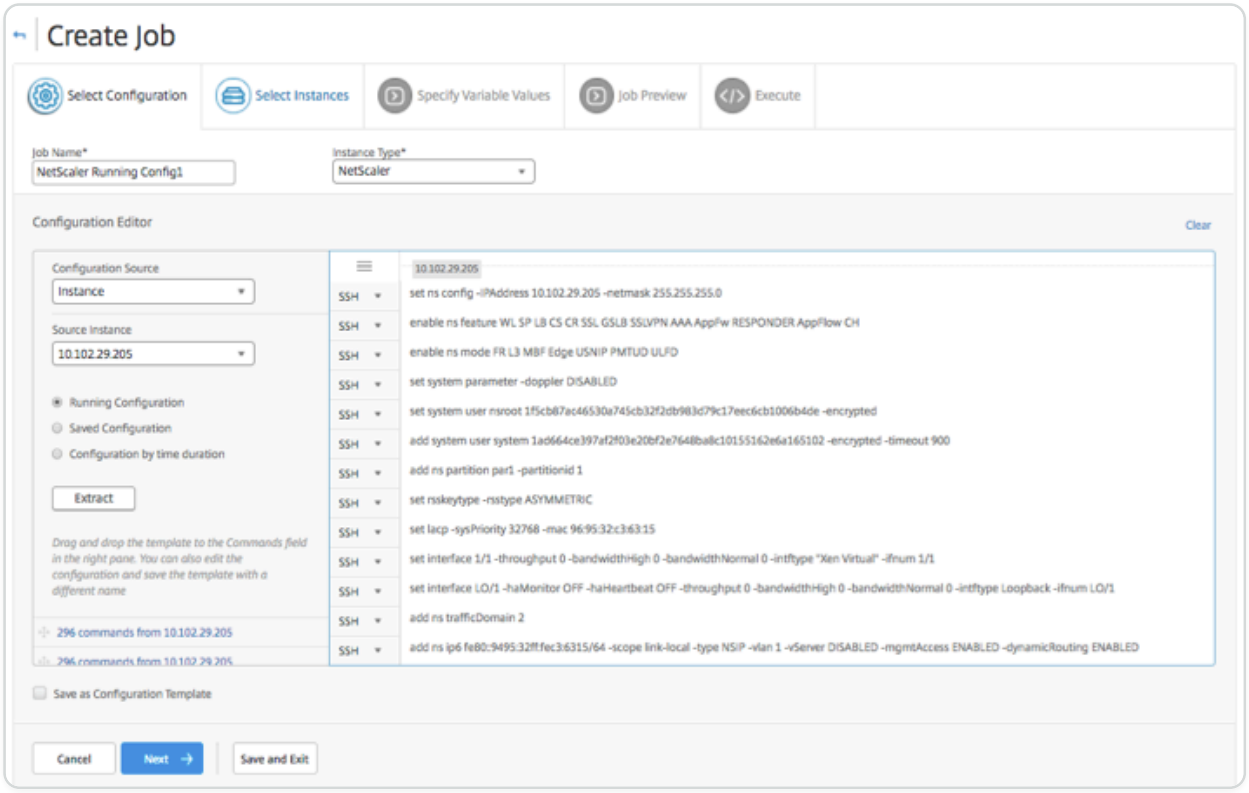
You can now replicate a NetScaler instance's configuration on other instances. When you configure a job in NetScaler ADM, select an instance as the Configuration Source and choose the selected instance's running or saved configuration.

For example, when you select **Running Configuration** and click **Extract**, NetScaler ADM sends a request to the selected NetScaler instance to locate the running configuration, and displays it as a template. You can drag the template into the **Commands** field in the right-hand pane. You can modify the commands, parameters, and instances.

To replicate running and saved configuration commands of one instance to another instance on NetScaler® ADM:

1. Navigate to **Infrastructure > 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 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 run on that instance is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Drag 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 might include adding partitions, setting up load balancing, binding the load balancing server to services, and so on. You might 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 NetScaler 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 run your job now or schedule it to be run later. You can also choose what action NetScaler ADM must 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 run configuration jobs

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 run on a different instance, or when the job encounters an error and stops further execution.

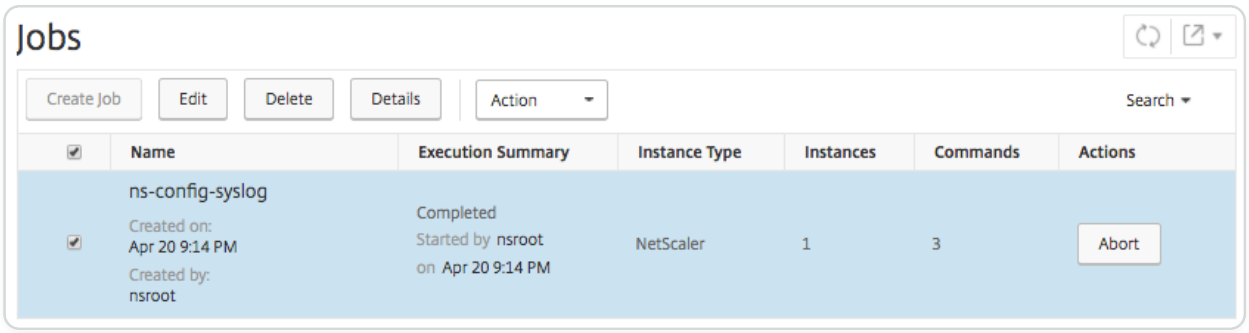
NetScaler® Application Delivery Management (ADM) provides a function to run the completed jobs again. With this function, jobs that are run completely can be run again without changing the job name.

NOTE

You can re-execute only those jobs that are run when the mode of execution is "Now."

To edit completed jobs:

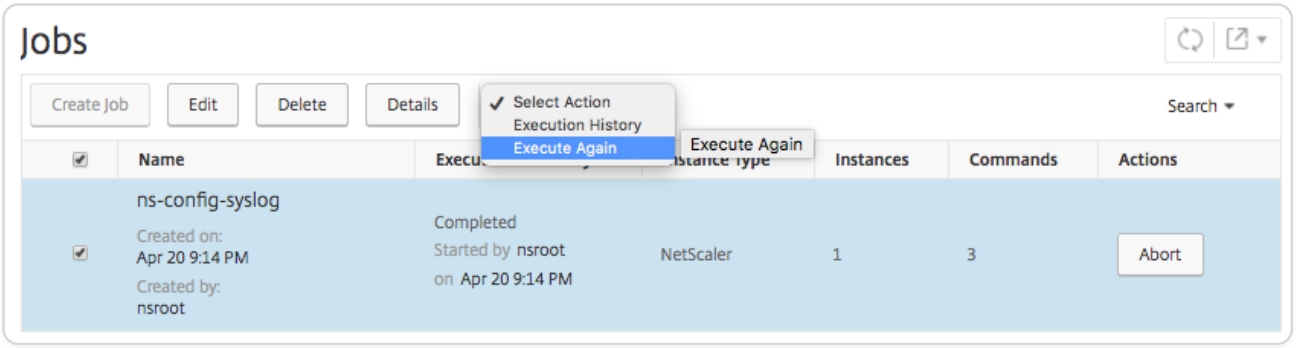
1. From the NetScaler ADM home page, navigate to **Infrasturcture > Configuration Jobs**.
2. In **Jobs** page, select a job that shows the Execution Summary as Completed, and click **Edit**. You can also edit a scheduled configuration job.
3. In **Configure Job** page, you can see that the Job Name and 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.



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 the same instances. Sometimes, the job might encounter a transient error from the server side, and you might have to run the job again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use SCP (put) command in configuration jobs

You can use the Configuration Jobs feature of NetScaler® 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 NetScaler 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" command. 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 NetScaler ADM and then to a directory on the NetScaler instance or instances.

NOTE

The file is uploaded to NetScaler ADM and it is later copied (put) to the selected NetScaler instances. The uploaded file is stored in NetScaler ADM and is deleted only when the job is deleted. This is necessary for jobs scheduled to run later.

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 run the job. Also, when you use a file at multiple places in a job and if you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **Infrastructure > 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.

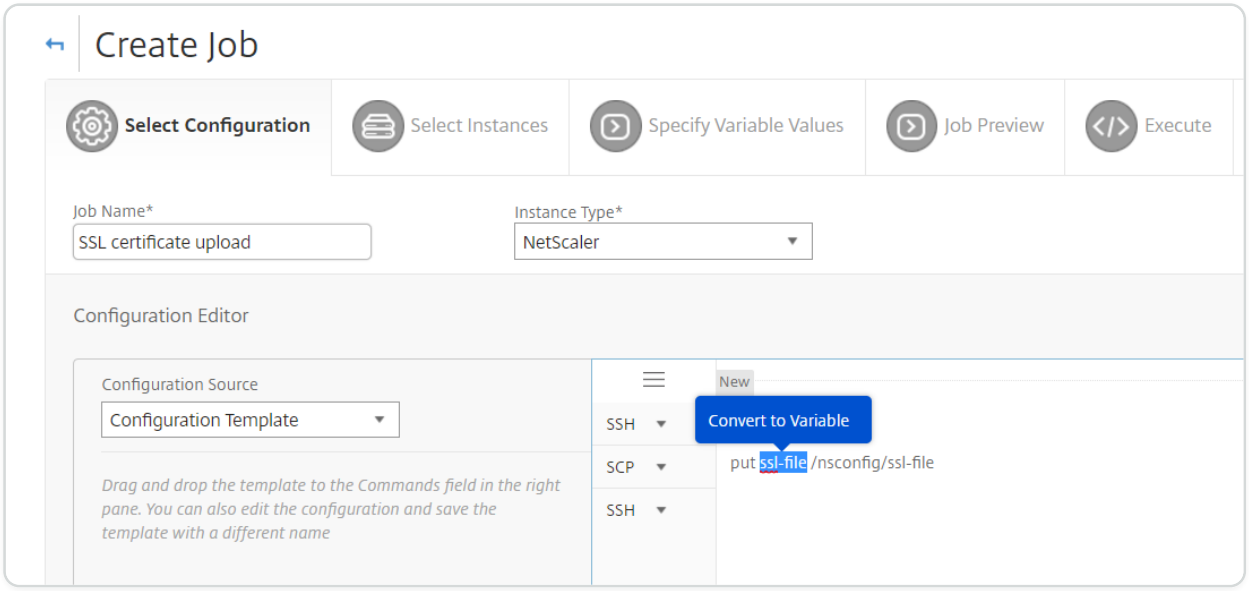
   For example, if you want to create a configuration job that copies an SSL certificate file saved on your local system to multiple NetScaler instances, you can add a "put" command that uses a variable instead of the name of a particular file, and define the variable type as "file".

   `put ssl-file /nsconfig/ssl-file`

   In this example,

   - `ssl-file` - This is the name of the file that must 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.

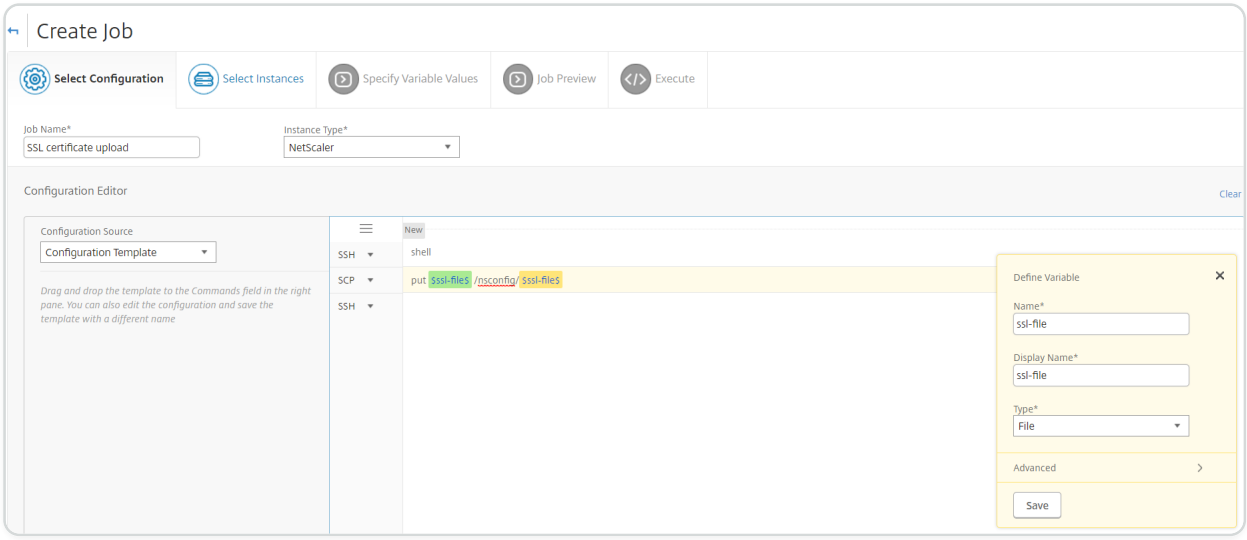
4. In the command that you entered, select the file name that you want to convert to a variable, and then click **Convert to Variable**, as shown in the following figure.



5. Verify that the file name is 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.

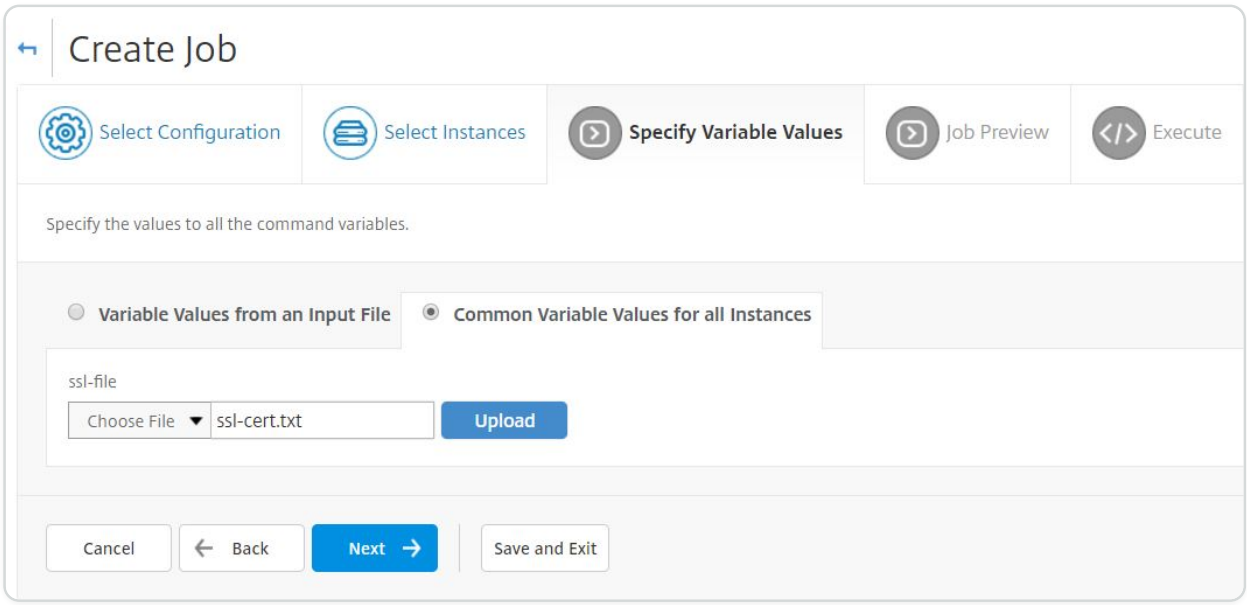
© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. From the **Type** drop-down list, select **File**. Click **Save**. Declaring the variable as a "File" type allows you to upload files to NetScaler 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 NetScaler ADM, and click **Next**.

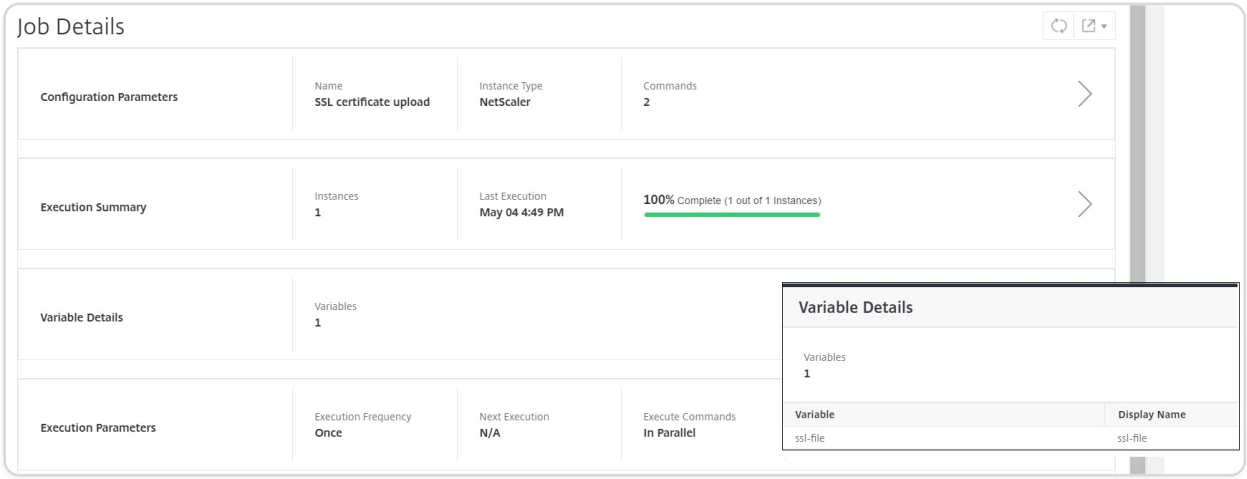


10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

11. On the **Execute** tab, you can run the job now or schedule it to be run later. You can also choose what action NetScaler ADM must 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. You can see the job details by navigating to **Infrastructure > Configuration Jobs**, and selecting the job that you configured. Click **Details**, and then click **Variable Details** to list the variables added to your job.



Use configuration templates

Configuration templates enable you to save and reuse a set of configuration commands so that you can apply consistent configurations across your NetScaler instances. The following topics help you create and manage configuration templates:

- Use the master configuration template
- Schedule jobs created by using built in templates
- Use configuration templates to create audit templates
- Reschedule jobs configured by using built in templates
- Reuse configuration audit templates in configuration jobs
- Import and export configuration templates

Use the master configuration template

Using a main configuration template is a flexible option for creating and deploying a master configuration on multiple NetScaler 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 configuratio**n. 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 job, you can customize it further for each specific ADC instance by adding more 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 run a configuration job using the DeployMasterConfiguration template on NetScaler CPX instances, instances configured in a cluster, or on partitioned ADC instances.

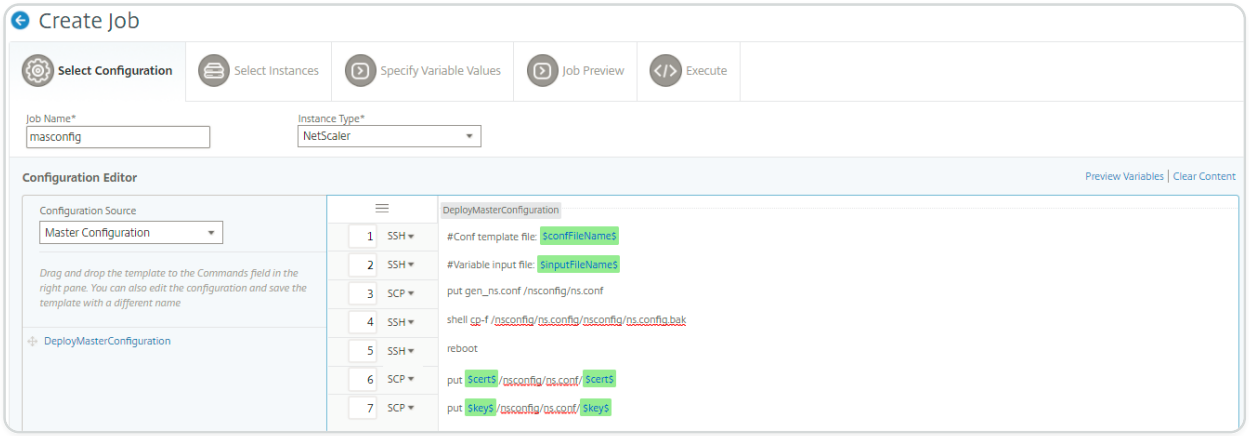
To create a configuration job using the Master Config configuration template on NetScaler® ADM:

1. In NetScaler ADM, navigate to **Infrastructure > 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 the DeployMasterConfiguration template's commands to the right pane. You can add, modify, or delete commands in the right pane as well. Click **Next**.

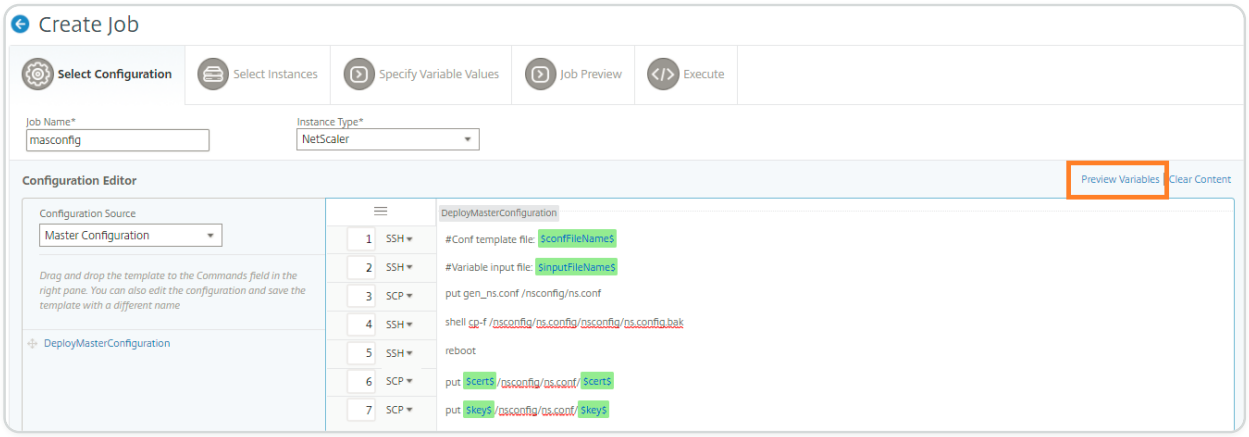
   NOTE

   You can add ***put*** commands to add input files to your template. In our example, we must upload certificate and key files in addition to the configuration template file and variable input files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

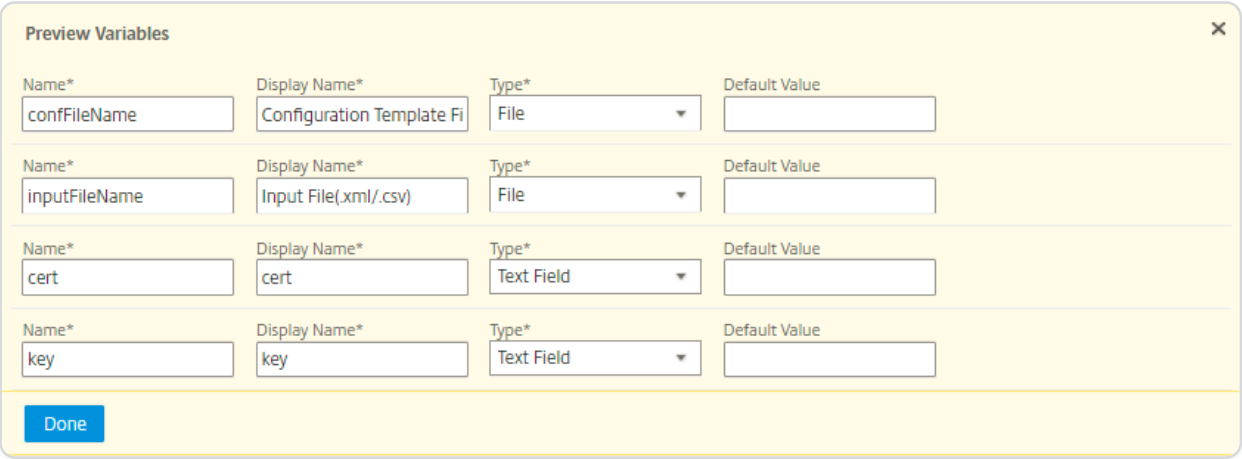


4. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
5. Do one of the following to view all the variables in a single consolidated view:
   - While creating a configuration job, navigate to **Infrastructure > Configuration 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 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.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

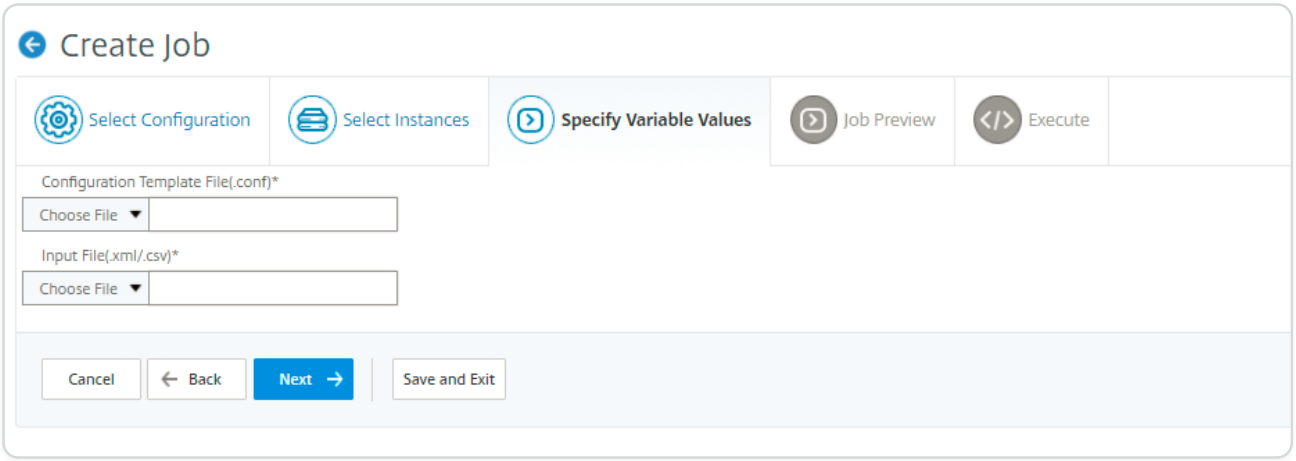
```
-  devicegroup. This tag contains all the instance group specific
parameters and values.


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 attibute.


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.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-->


<global>


</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>


<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>
```

10. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



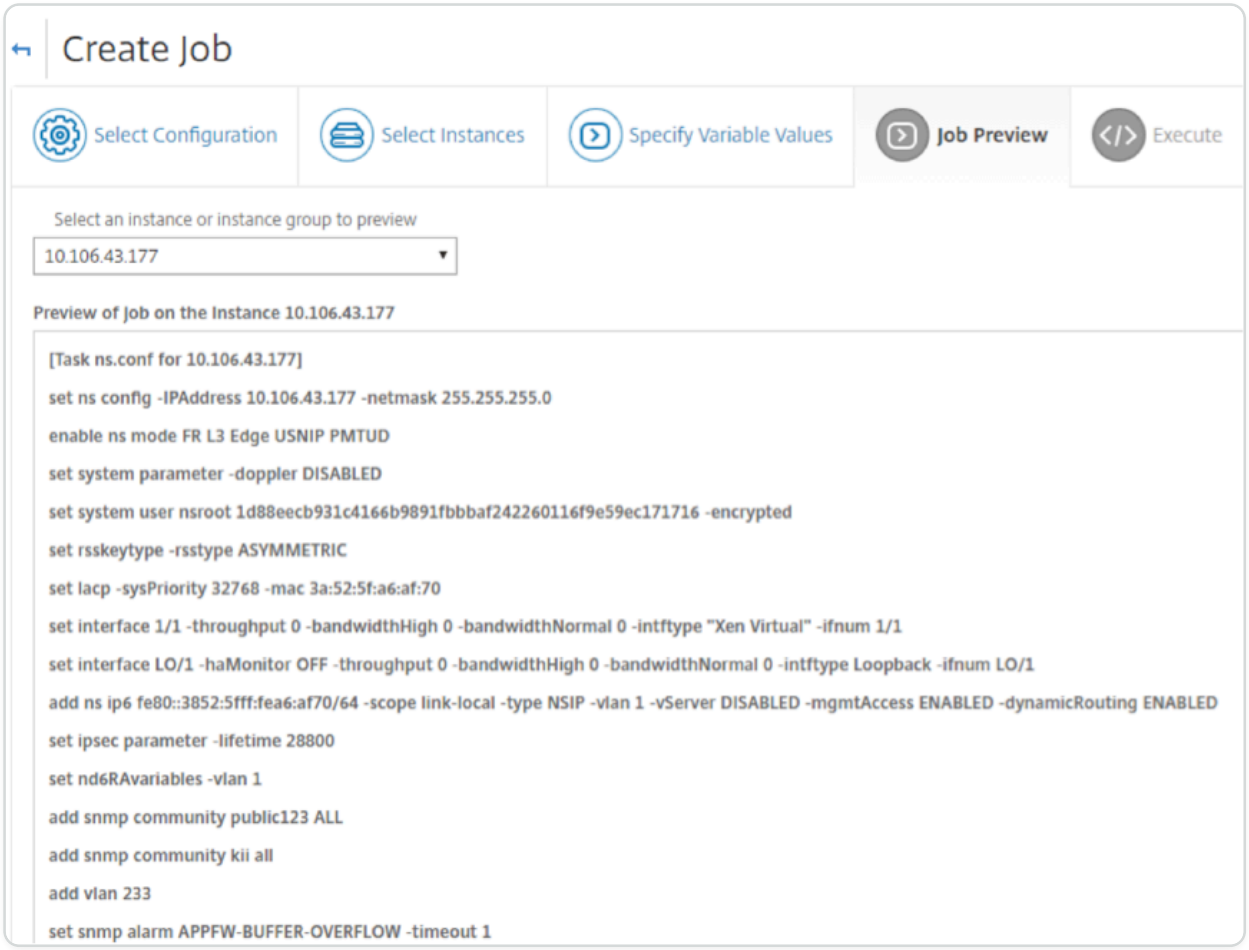
The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

To view the run 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 run 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**.

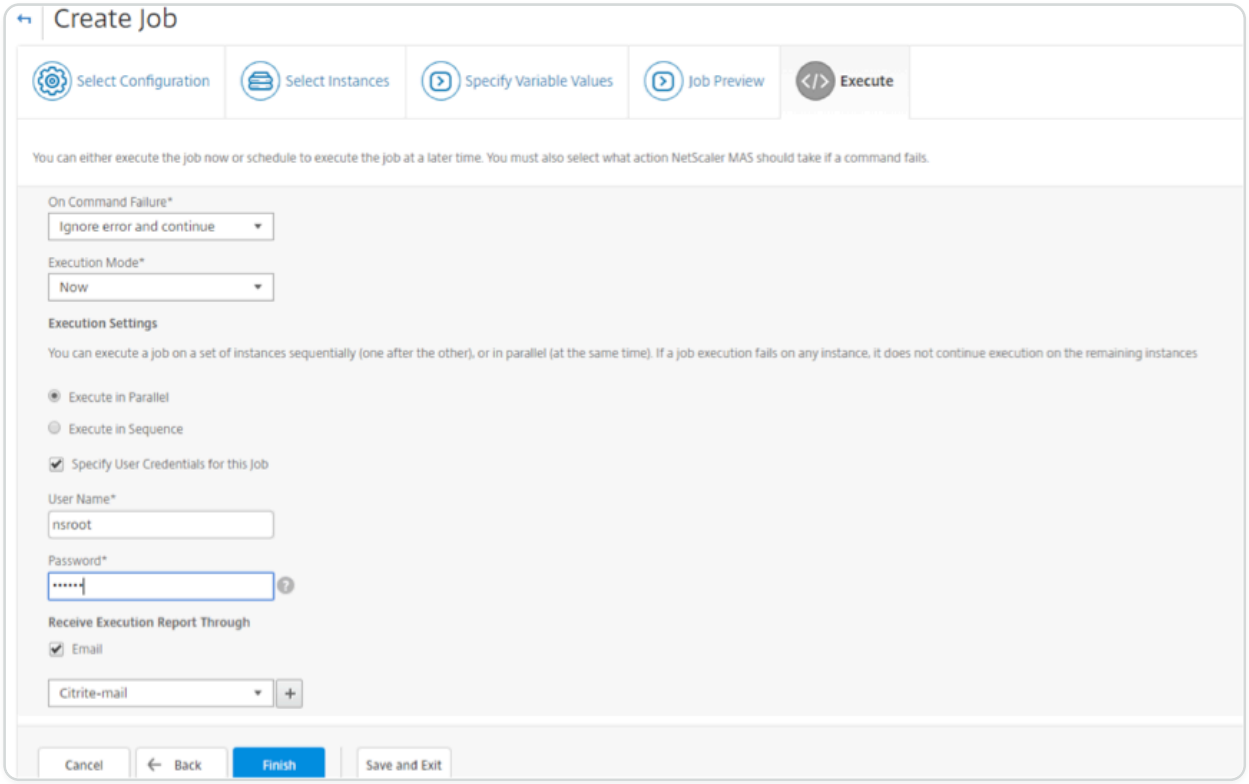
© 1997–2026 Citrix Systems, Inc. All rights reserved.



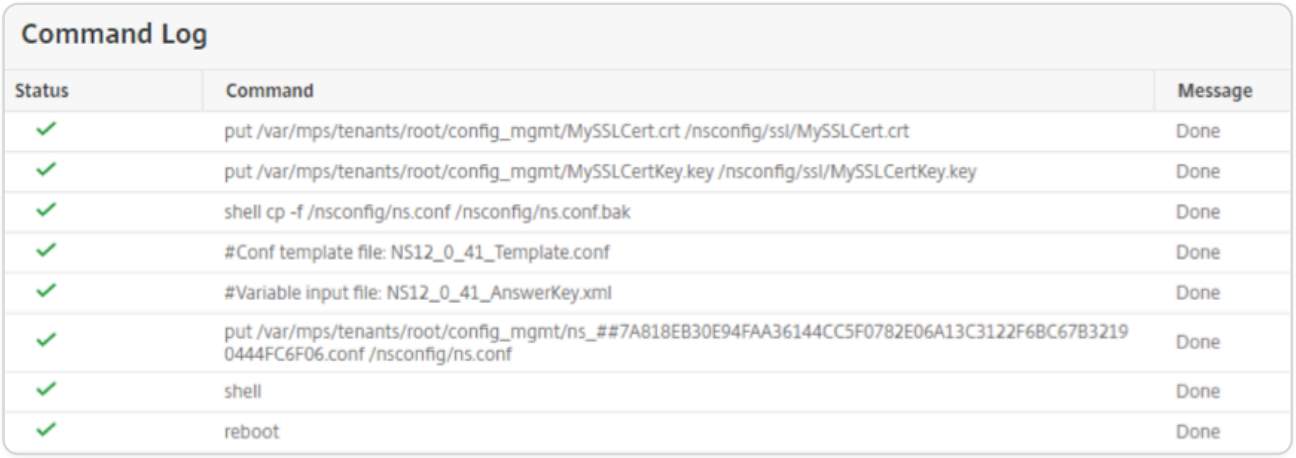
2. On the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler ADM must take if the command fails.

   You can also choose to allow authorized users to run 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After running your job, you can see the job details by navigating to **Infrastructure > Configuration Jobs** and select the job you configured. Click **Details** and then, click **Execution Summary** to see the details of your job. Click the instance to see the **Command Logs** to see the commands run on the job.



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B3219 0444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

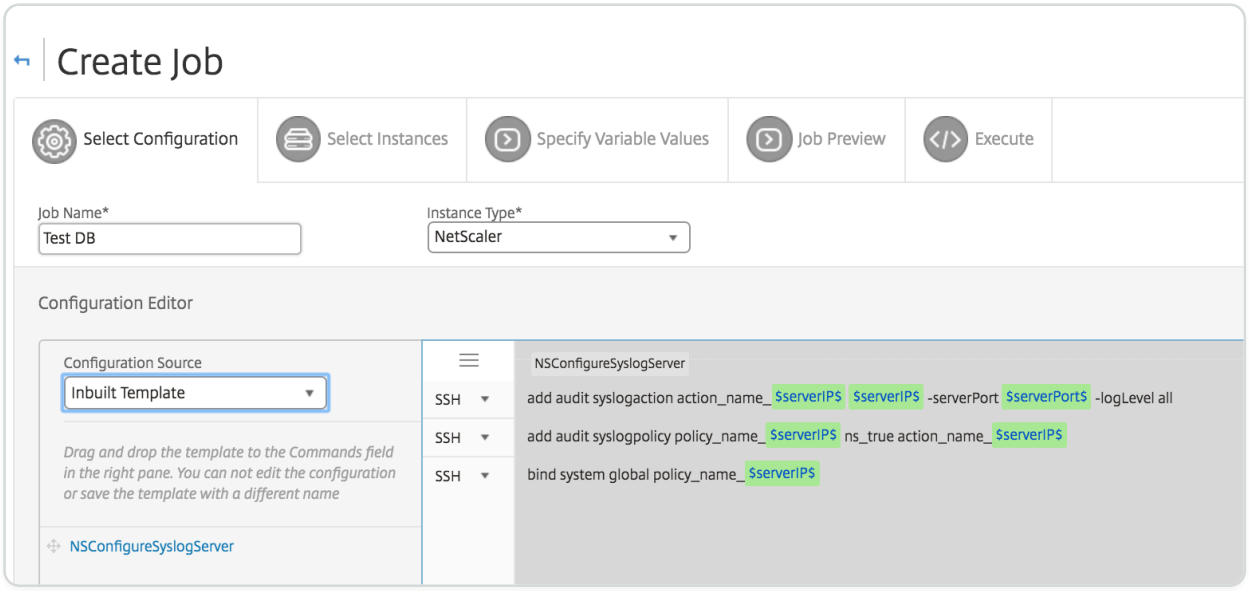
Schedule jobs created by using built in templates

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 run the job immediately, or schedule the job to be run at a later stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To schedule a job by using built-in templates in NetScaler® Application Delivery Management (ADM)

1. In NetScaler ADM, navigate to **Infrastructure > 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 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 NetScaler 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:

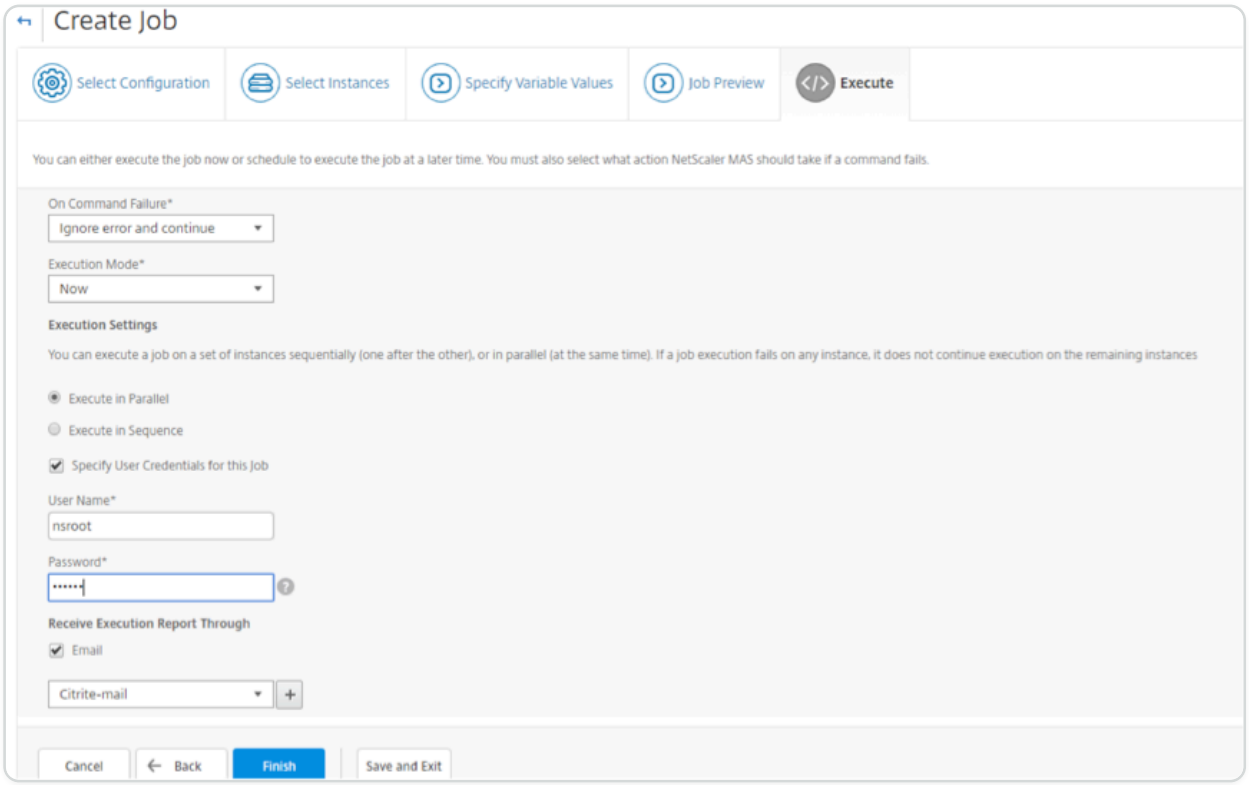
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **On Command Failure** - If a command fails, you can either choose to ignore the errors and continue to run the job or stop further execution of the job. Choose the action that you want to run from the drop-down list.
- **Execution Mode** - You can either run the job now or schedule to run 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 run 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 run 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**.



Use configuration templates to create audit templates

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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler instances. NetScaler 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 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
```

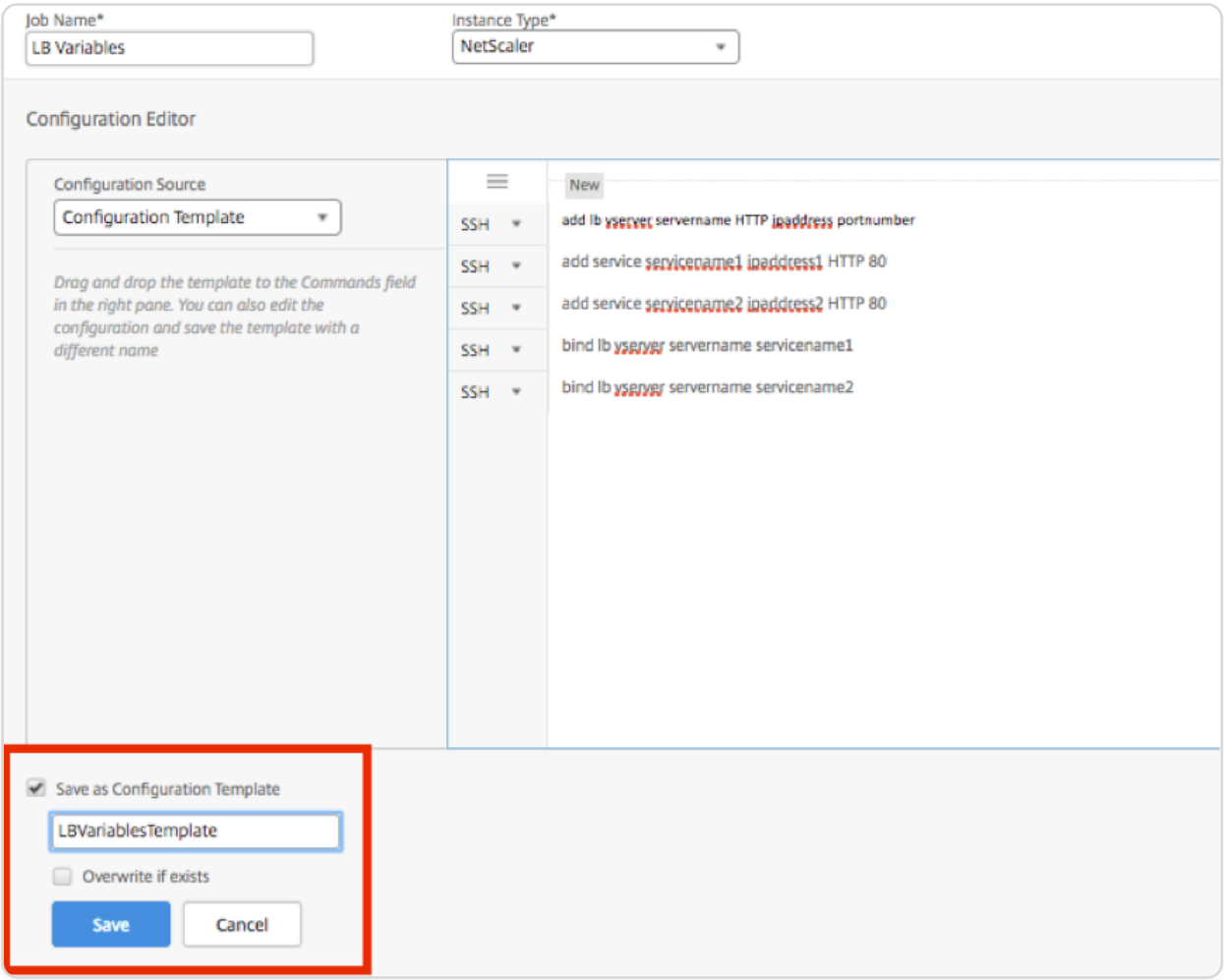
```
bind lb vserver <servername servicename1>
```

```
bind lb vserver <servername servicename2>
```

To save a configuration template in NetScaler® ADM:

1. Navigate to **Infrastructure > 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** check box and specify a name for your template. You can choose to overwrite other templates that exist with the same name.
5. Click **Save**.

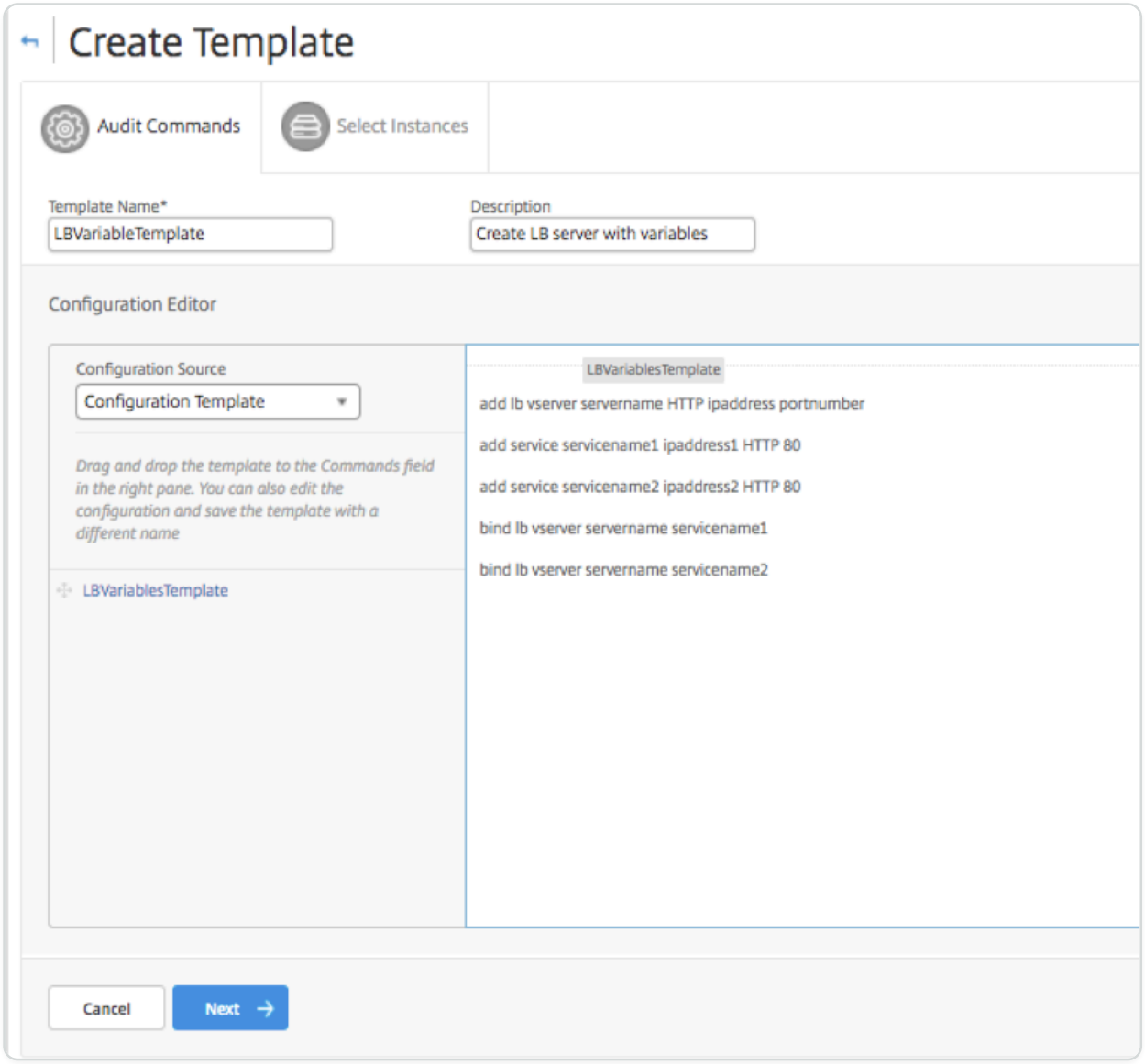
© 1997–2026 Citrix Systems, Inc. All rights reserved.



To use a configuration template to create an audit template in NetScaler ADM:

1. Navigate to **Infrastructure > 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 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances.

Reschedule jobs configured by using built in templates

You can reschedule a job that you scheduled by using built-in templates in NetScaler® Application Delivery Management (ADM). For example, you can change the action that NetScaler 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 NetScaler ADM

1. In NetScaler ADM, navigate to **Infrastructure > Configuration Jobs**.
2. Select the job you want to edit, add or remove instances, specify variable values, and then change execution actions and settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 feature is useful when you have to run the same set of commands on the same instances. Sometimes, the job might encounter a transient error from the server side, and you might have to run the job again.

Reuse configuration audit templates in configuration jobs

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 NetScaler 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.

NetScaler® 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:

```
add lb vserver servername HTTP ipaddress portnumber



add service servicename1 ipaddress1 HTTP 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add service servicename2 ipaddress2 HTTP 80



bind lb vserver servername servicename1



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.

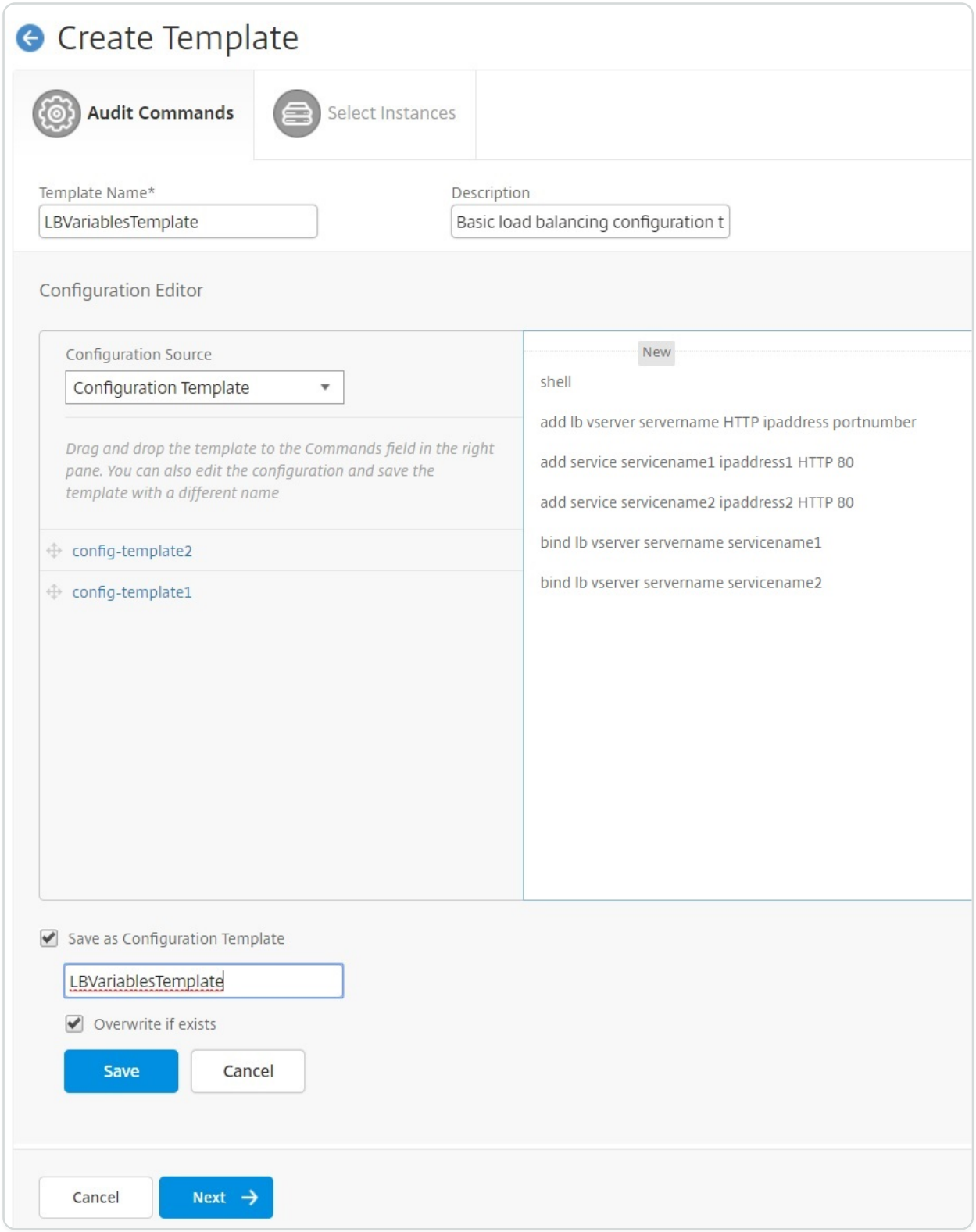
To create an audit template:

1. In NetScaler ADM, navigate to **Infrasturcture > 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** check box 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.

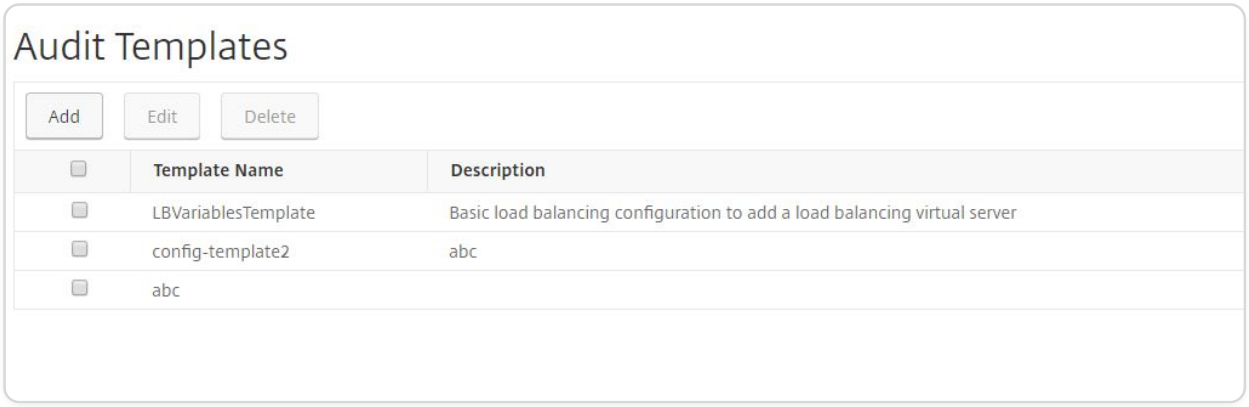
5. Click **Save** and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Next**.
7. In **Select Instances** tab, select the **NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. When you want to run these configuration commands, navigate to **Infrastructure > 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 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 NetScaler instances every time you run 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.
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 NetScaler 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Drag 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.

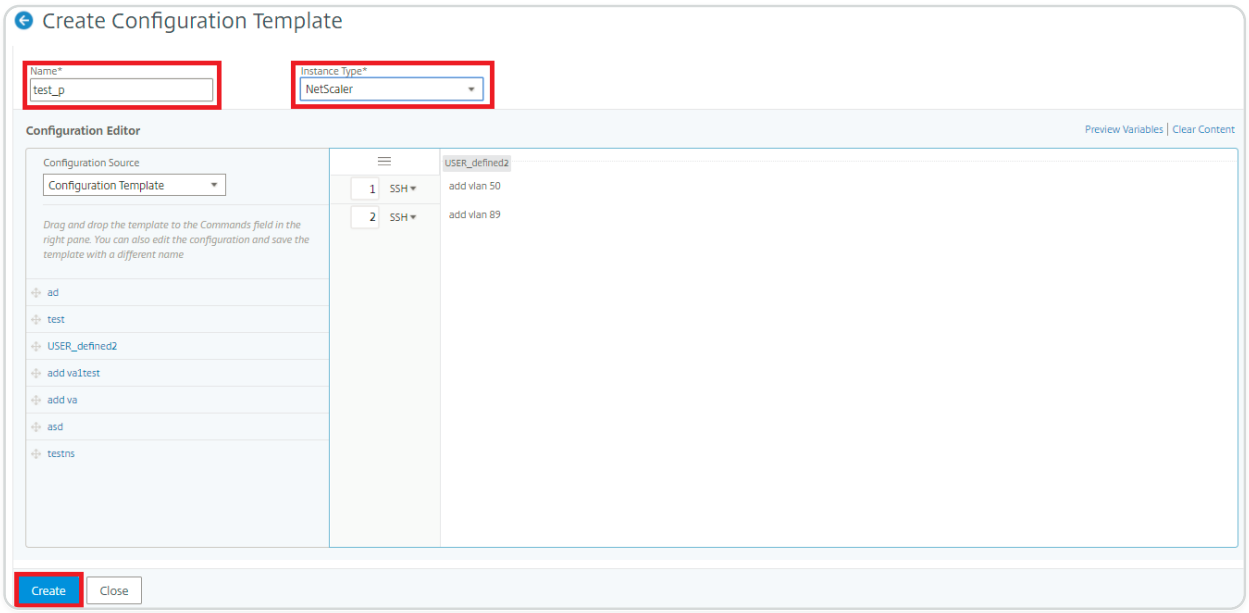
Import and export configuration templates

You can export the configuration templates from any NetScaler® Application Delivery Management (ADM). You can also import the file to the same or another NetScaler 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 NetScaler ADM. This file might be new or the one that you have exported from the same or other NetScaler ADM.

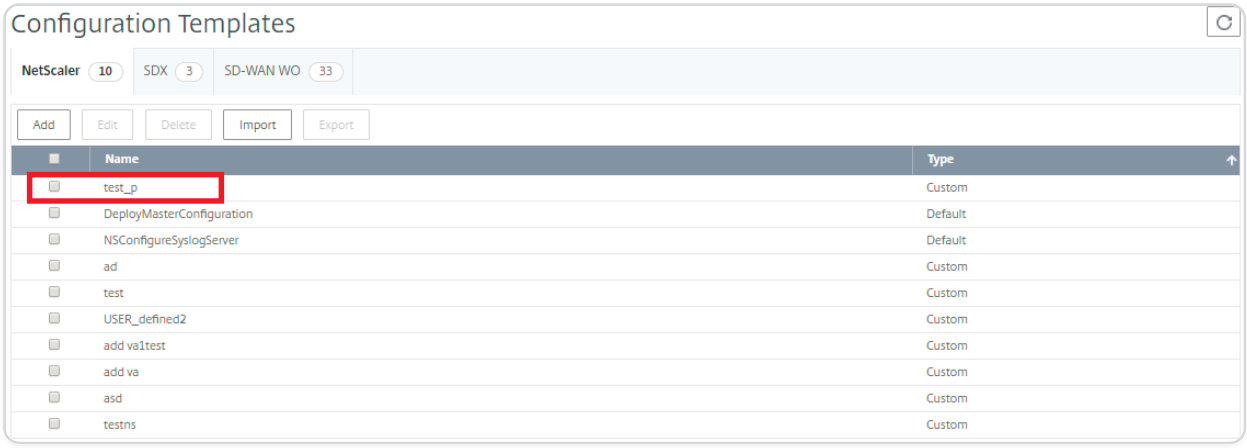
To export the configuration templates:

1. Navigate to **Infrastructure > Configuration Jobs > Configuration Templates**.
2. Click 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 the existing configuration templates to the configuration editor. Click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Navigate to **Infrastructure > Configuration Jobs > Configuration Templates** to view the templates created in the list of Configuration Templates.

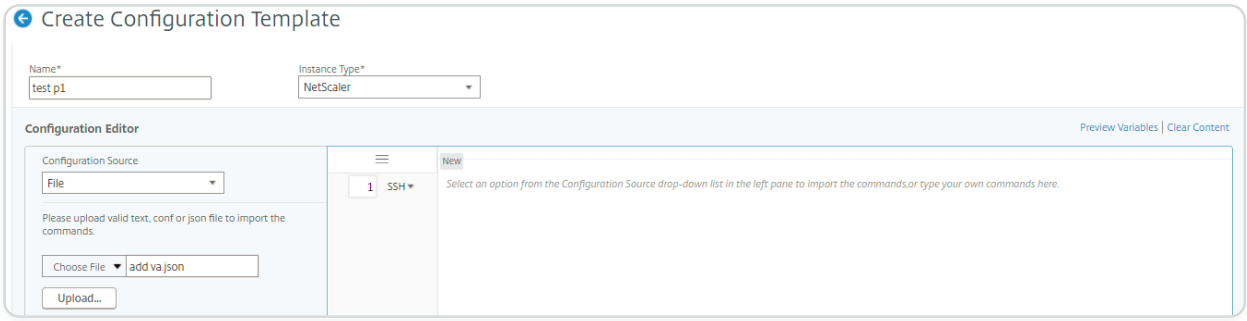


5. Select the newly created configuration template and click the **Export** button.

The corresponding configuration template gets downloaded on your local system in **.json** format.

To import the configuration templates:

1. Navigate to **Infrastructure > 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- 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.

Configuration audit

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

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. NetScaler Application Delivery Management (NetScaler ADM) compares these instances with the audit template and reports if there is a mismatch in the configuration. Whenever there is a configuration mismatch, NetScaler 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 must be run
- Setting the frequency at which NetScaler® ADM must 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 NetScaler ADM to specified email addresses that you can configure. By this option, your user can receive the report as a mail

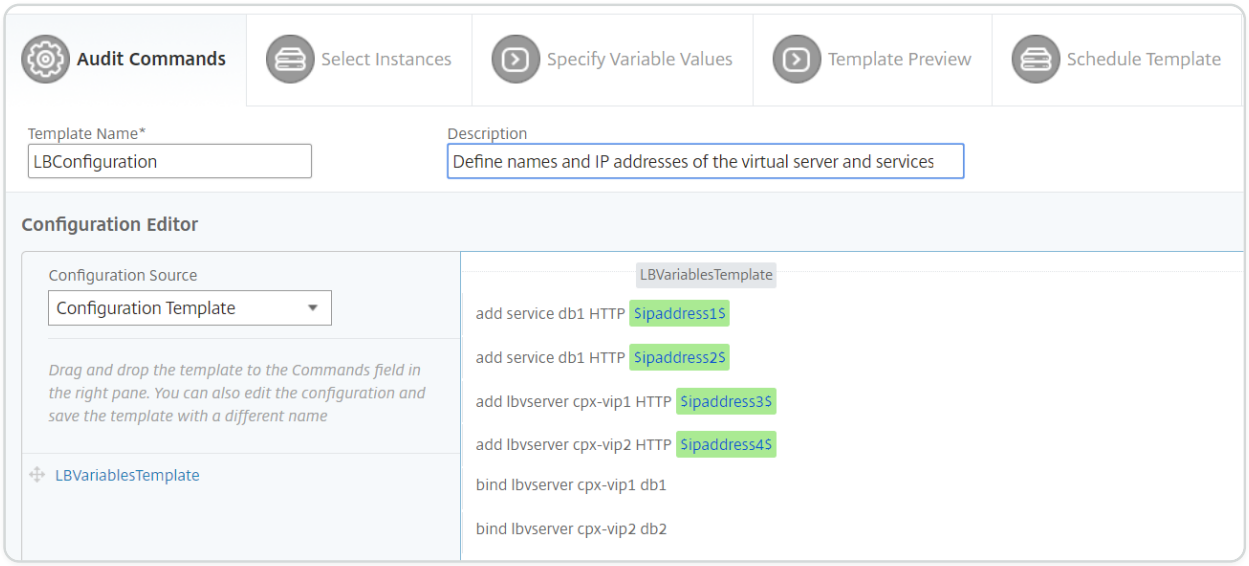
© 1997–2026 Citrix Systems, Inc. All rights reserved.

attachment and there is no need for the user to log on to NetScaler ADM to export the reports manually.

Note The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

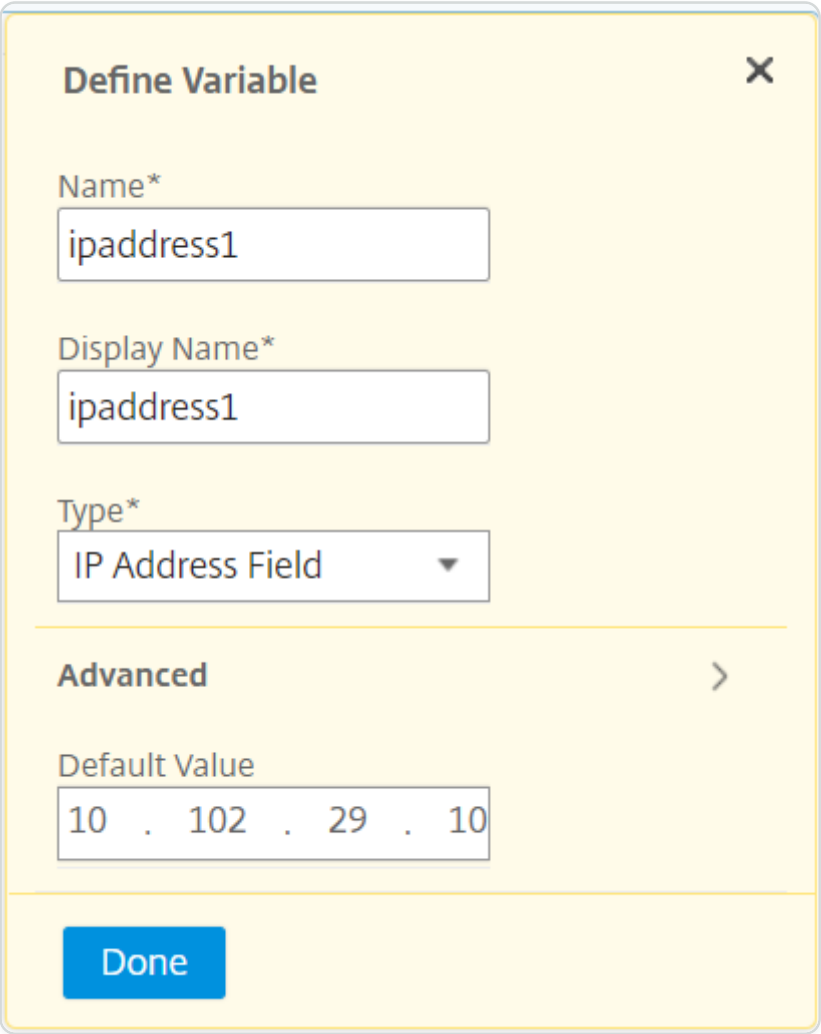
To create audit templates:

1. Navigate to **Infrastructure > 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.

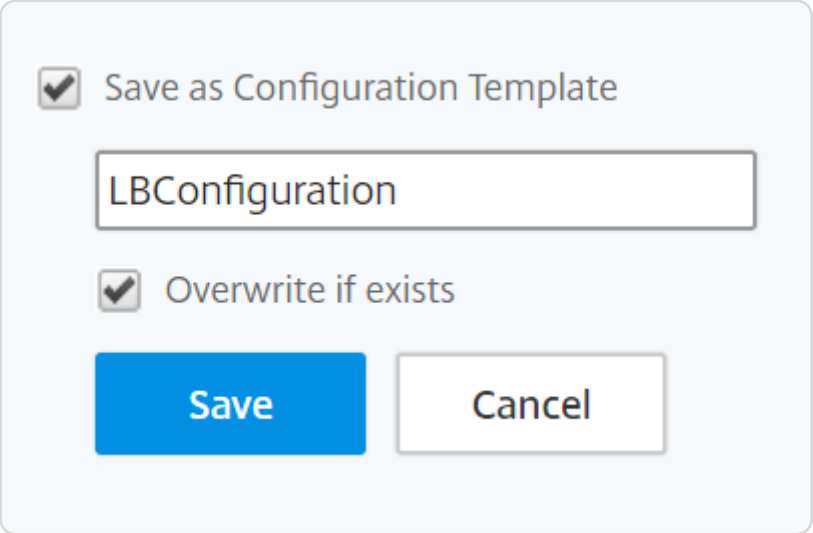


In the **Define Variable** window, set the properties for this variable - name, display name, and the type of the variable. Click the **Advanced** option if you want to further specify a default value for your variable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

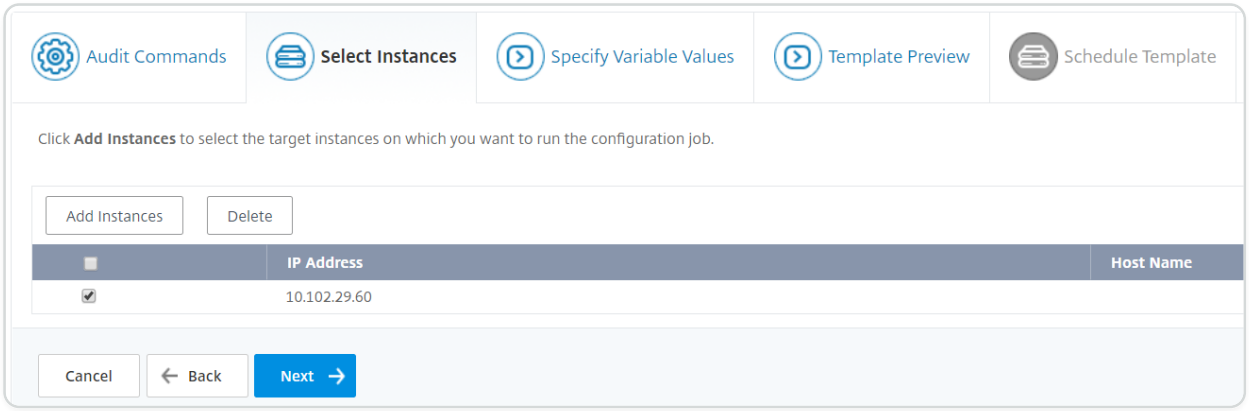


You can also save the commands as a configuration template.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

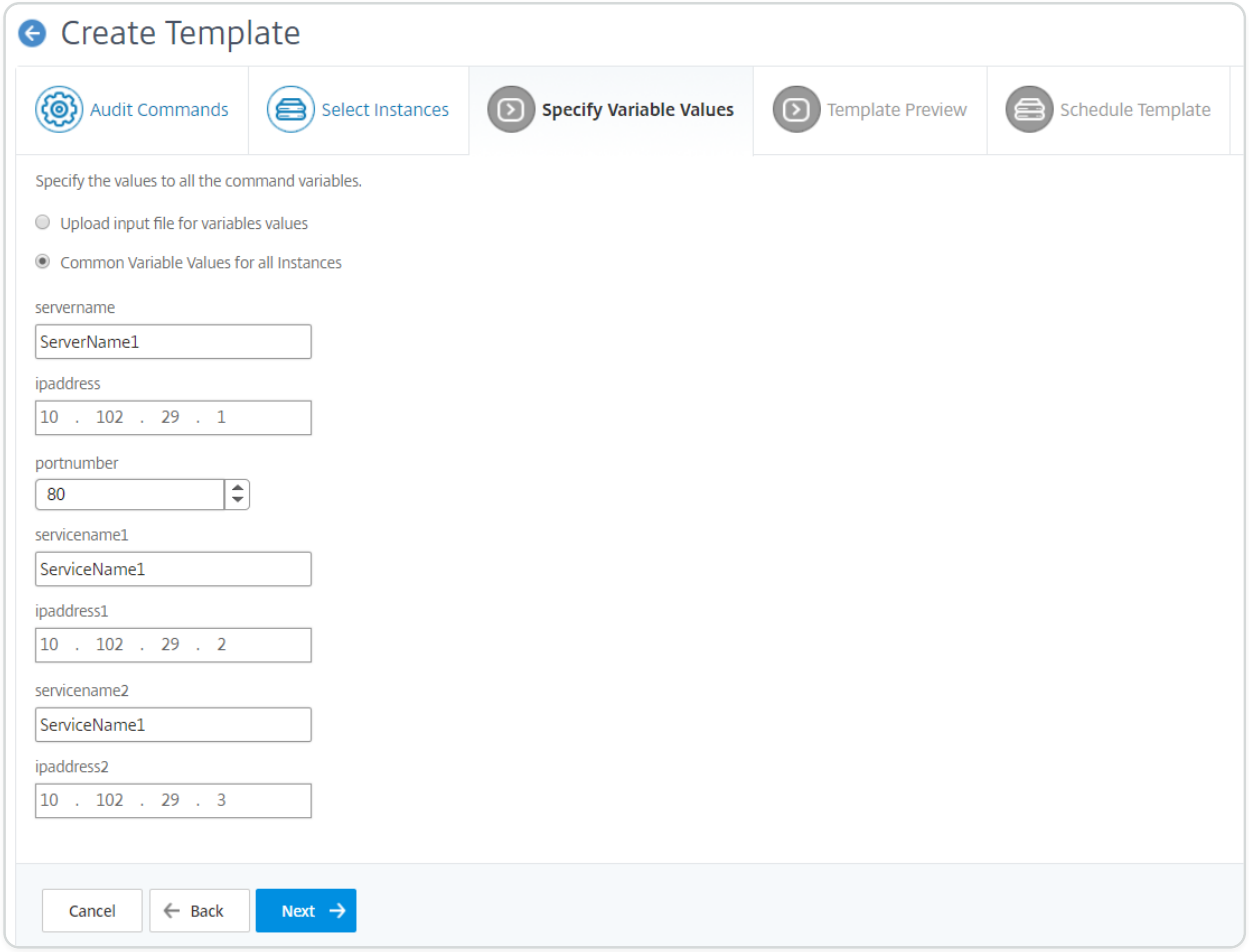


7. In the **Specify Variable Values** tab, you have two options:

   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 NetScaler ADM server

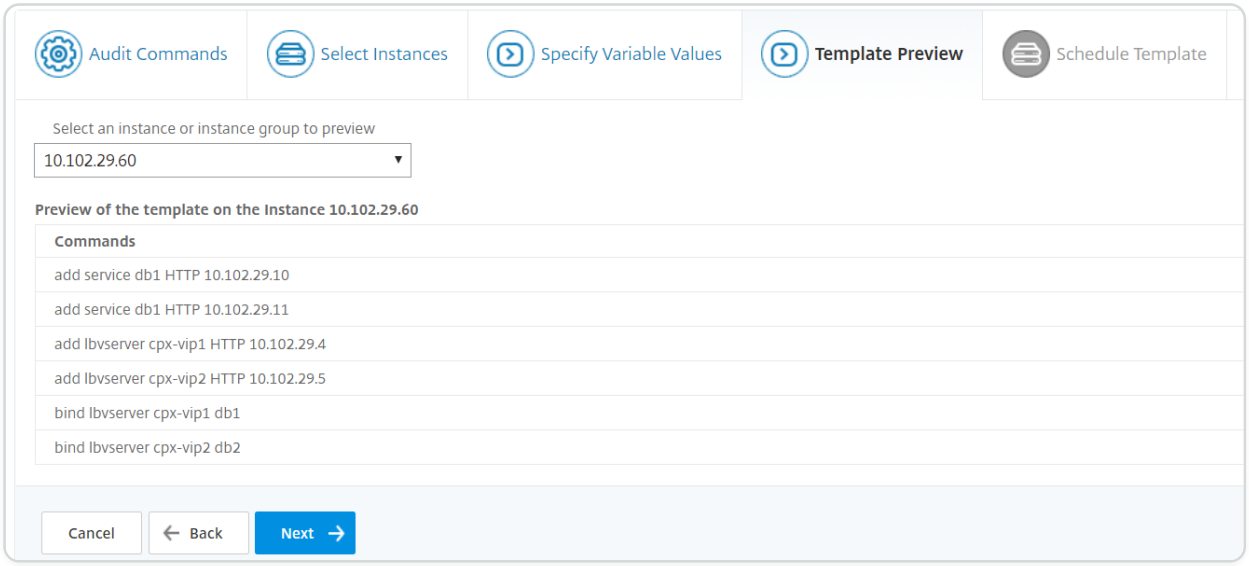
   b. Enter common values for the variables that you have defined for all instances

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler ADM.

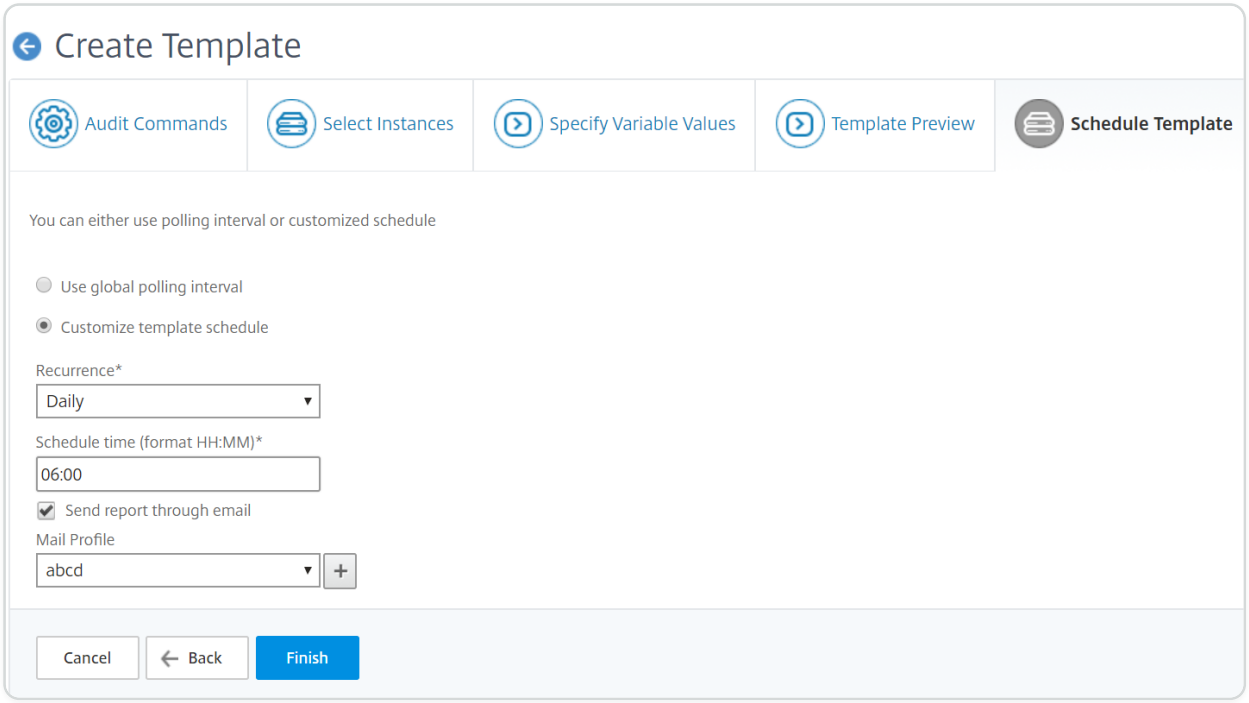
      NOTE

      To configure global polling interval in NetScaler ADM, navigate to **Infrastructure > Configuration Audit > Audit Templates,** and click **Global Polling Interval**. In the **Poll Interval** field, enter the minutes at which NetScaler ADM must 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 must be sent as a mail attachment.

11. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

NetScaler® Application Delivery Management (NetScaler 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 NetScaler ADM.

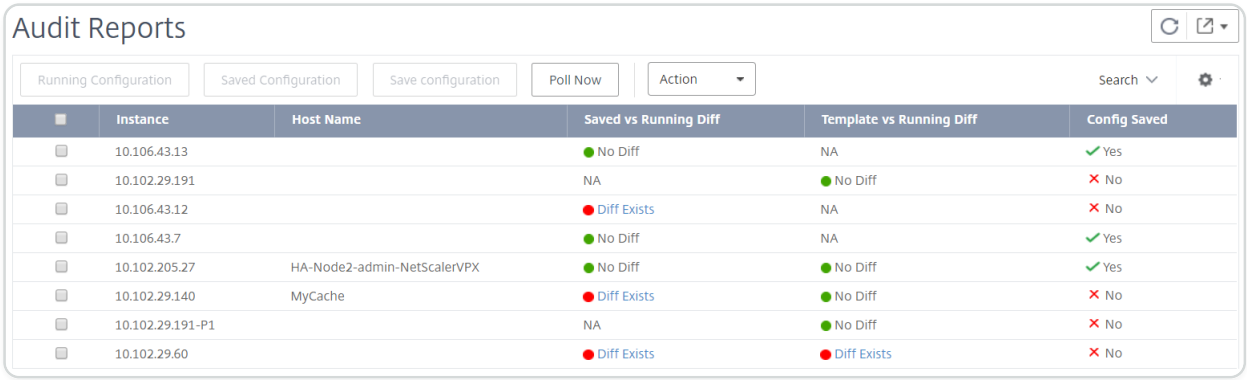
NetScaler ADM also provides an option to schedule automatic export of diff report as a mail attachment. For more information on how to schedule export of reports, see Creating Audit Templates.

To export configuration audit reports:

1. In NetScaler ADM, navigate to **Infrastructure > Configuration Audit**.
2. On the **Configuration Audit** page, click inside the **NetScaler Config Drift** chart.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

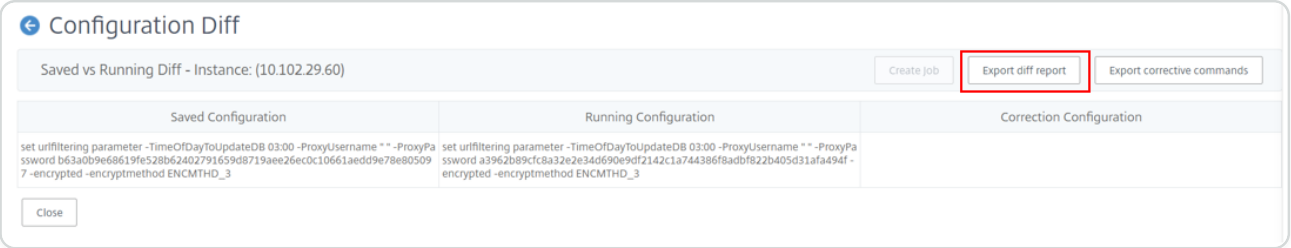


In the image you can see that for some instances a diff is present only in **Saved Vs Running Diff** and for some instances, a diff is present only in **Template vs Running Diff**. For some instances, differences exist in both **Saved Vs Running Diff** and **Template vs Running Diff.**

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.

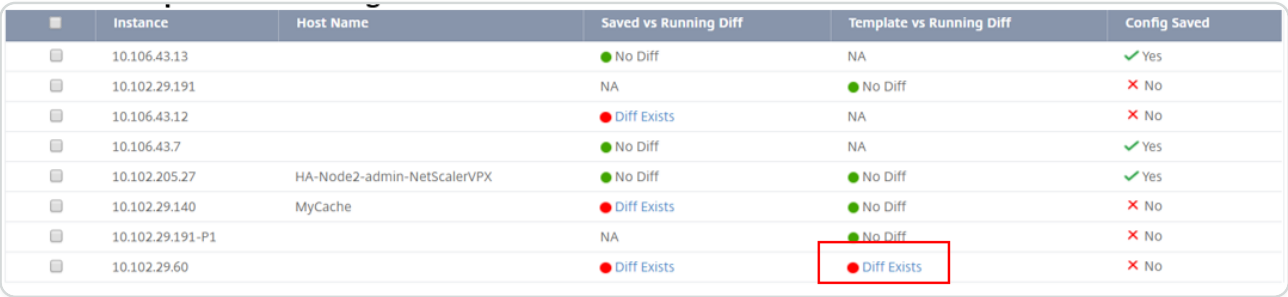


Click **Export diff report** to download a .csv file of the diff report. You can also click Export corrective commands to export the commands to a .txt file. You can then run the commands on the associated NetScaler ADM instance from configuration jobs to correct the configuration in that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.**



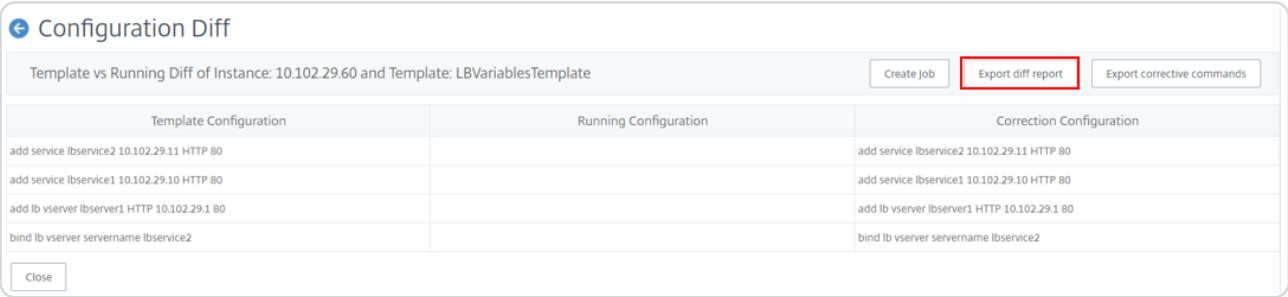
Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

Now you can see that two templates show diff and the NetScaler ADM instance has a different configuration from what the template is looking for.

Templates of Instance: 10.102.29.60

Templates	Diff Exists	Last Updated
LBVariablesTemplate	Diff Exists	Oct 10 2017 05:30:02
LBConfigurationAudit	Diff Exists	Oct 27 2017 12:14:30

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.



Configuration Diff

Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate

Create Job | Export diff report | Export corrective commands

Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

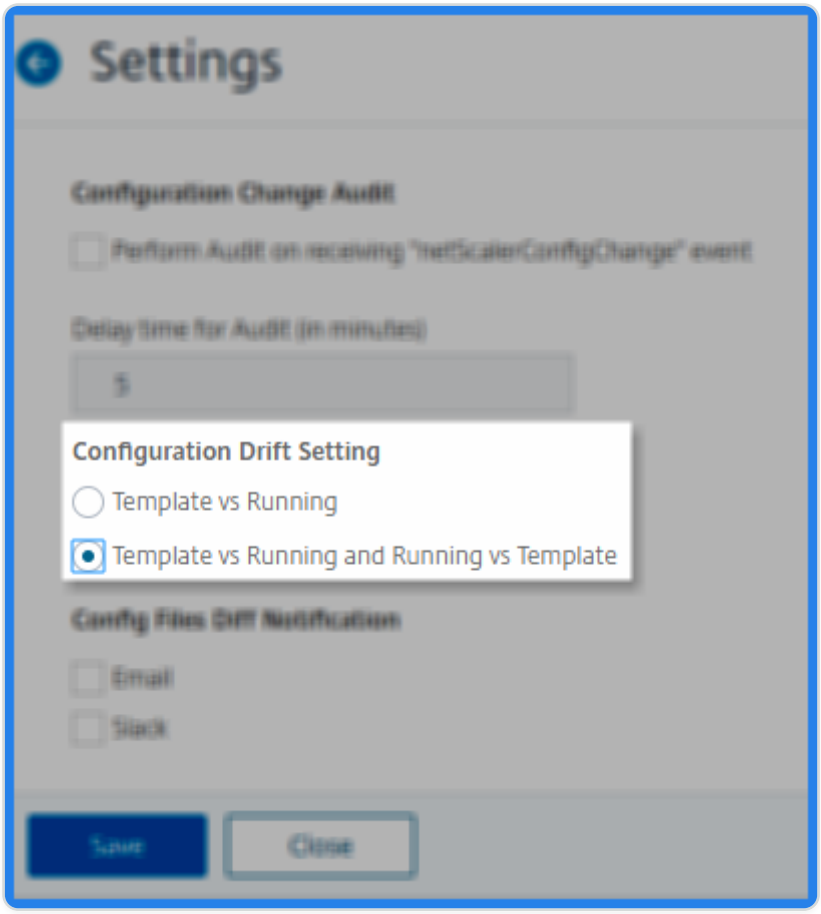
Close

You can also use Template vs Running and Running vs template drift setting, to compare the configuration from both ways:

- Compares the audit template configuration with the running configuration on the instance.
- Compares the running configuration on the instance with the audit template.

By default, the Template vs. running drift setting is selected. To modify the drift setting, from the ADM GUI, select **Settings** in the **Configuration Audit** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

View the file status audit reports

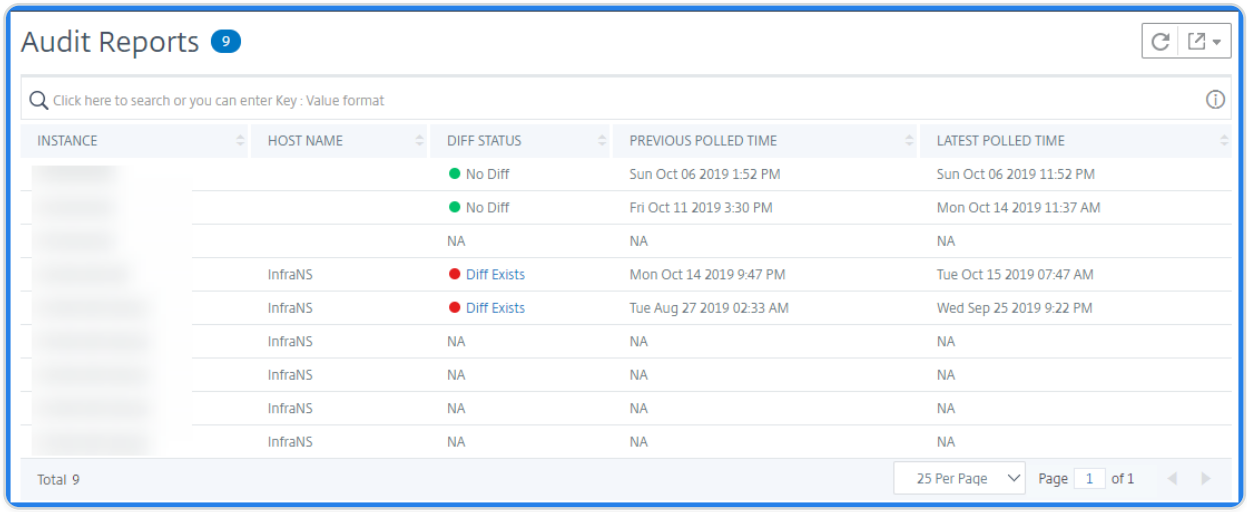
Using the **NetScaler File Status** chart, you can monitor whether any files are added, modified or removed in the `nsconfig` folder. For example: if the license file is updated on an ADC instance, you can check when this file was last updated and take actions appropriately.

To export the file status audit reports for the NetScaler instances:

1. In NetScaler ADM, navigate to **Infrastructure > Configuration Audit**.
2. On the **Configuration Audit** page, click inside the **NetScaler File Status** chart.

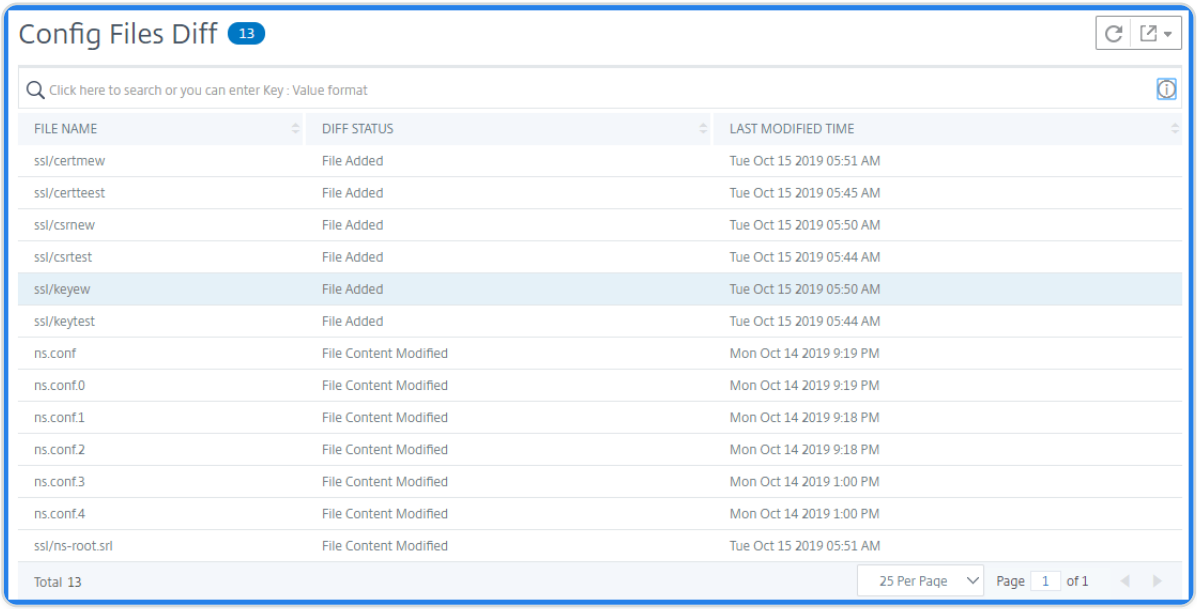
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Audit Reports** page lists instances with the Diff status.



The **Diff Status** is calculated for the interval between the **Previous Polled Time** to the **Latest Polled Time**. The **Diff Status** can be one of the following:

- **Diff exists** - This status indicates the files have changed in the `nsconfig` folder of an instance since the **Previous Polled Time**. To view what has changed on the file, click **Diff Exists**.



- **No Diff** - This status indicates the files in the `nsconfig` folder hasn't changed since the previous polled time.
- **NA** - This status indicates monitoring the file status is not applicable. This status appears when the NetScaler ADM doesn't poll the instance. For example, when an instance is added newly or instance state is inactive the polling of the instance doesn't occur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

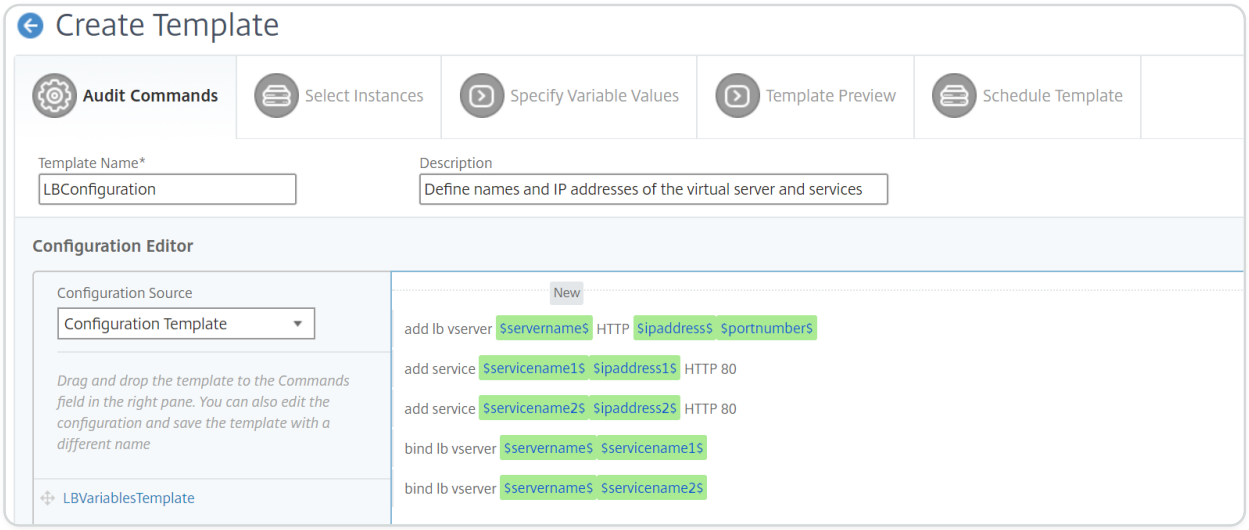
Audit configuration changes across instances

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 run on certain instances. The NetScaler Application Delivery Management (NetScaler 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 has to run. You can also set the frequency at which NetScaler® ADM must 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 NetScaler 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 NetScaler ADM to check the reports manually.

To create audit templates:

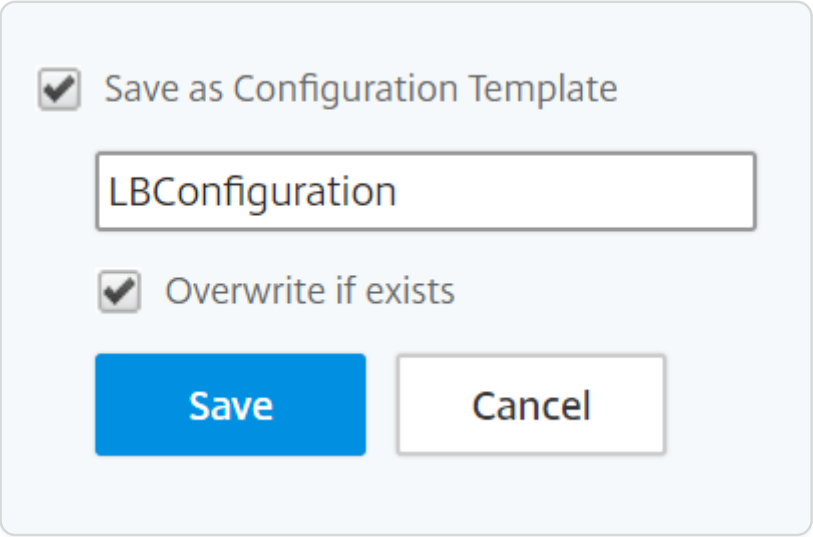
1. Navigate to **Infrasturcture > Configuration Audit > Audit Templates**, and click **Add**.
2. On the **Create Template** page, and in the **Audit Commands** tab, specify the template name and its description.
3. In the **Configuration Editor**, type in your commands and save the commands as a configuration template. You can also drag 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

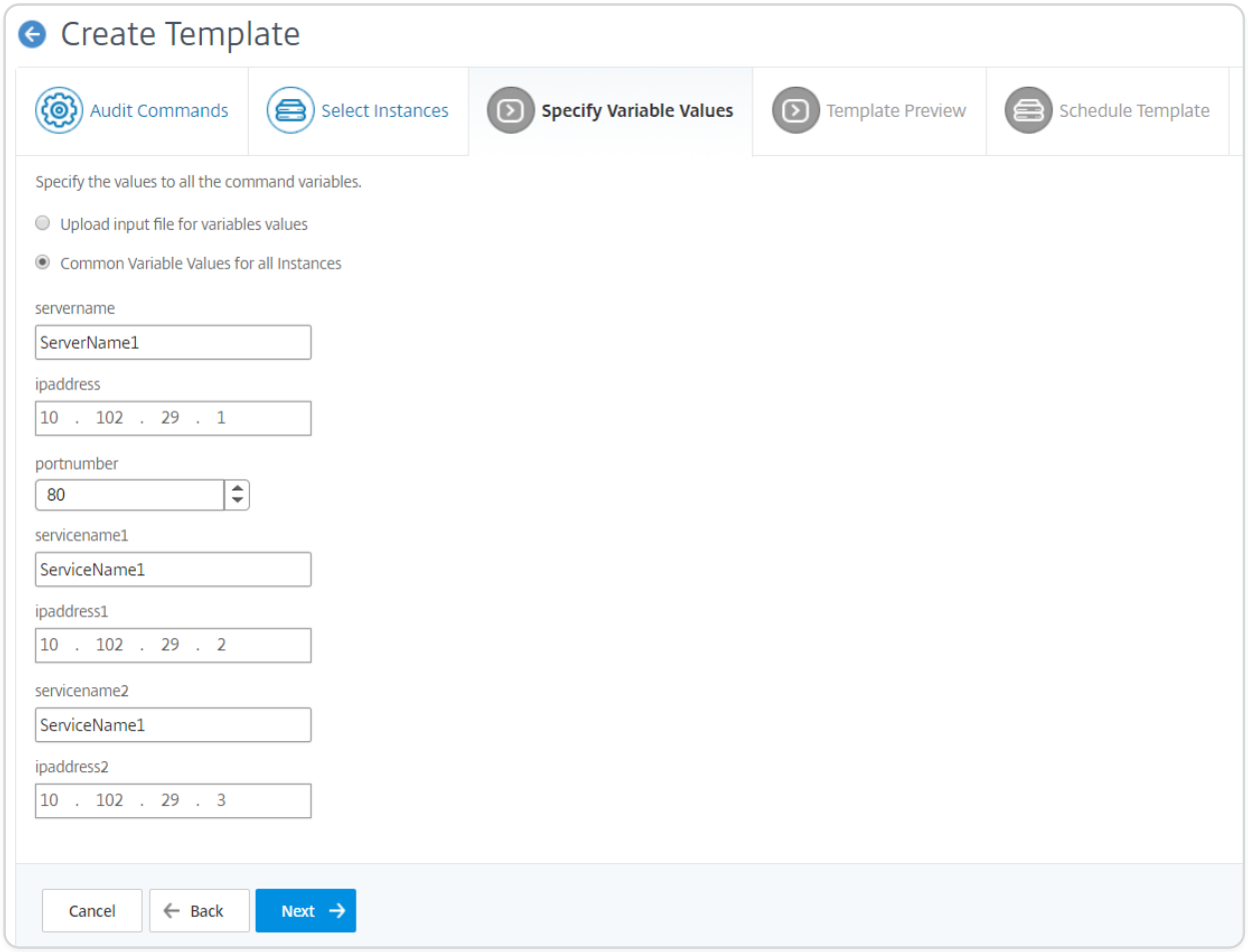
Click the **Advanced** option if you want to further specify a default value for your variable.

You can also save the commands as a configuration template.



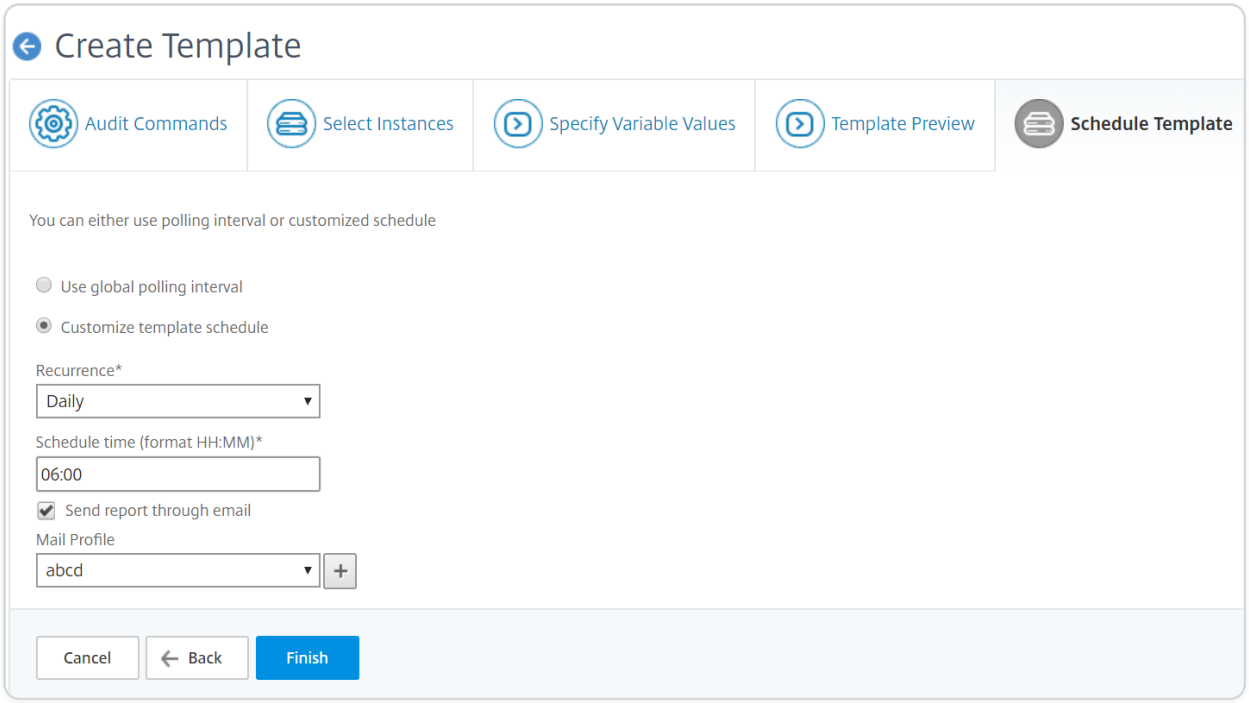
5. Click **Save** and then, click **Next**.
6. In the **Select Instances** tab, select the instances you want to run the configuration audit on.
7. In the **Specify Variable Values** tab, you have two options:
   a. Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler ADM server
   b. Enter common values for the variables that you have defined for all instances
8. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler 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 has to be sent as a mail attachment.
11. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



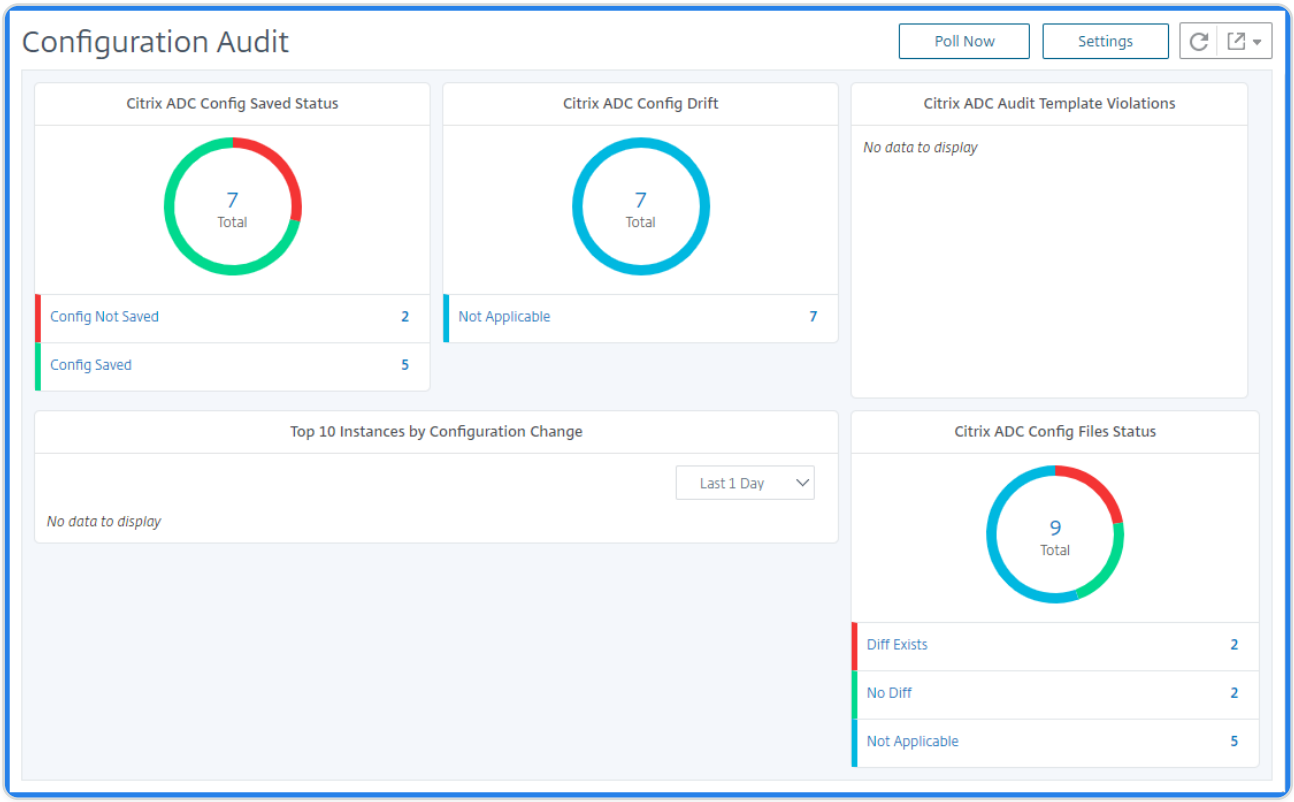
The audit template appears in the Audit Templates list and is run at the scheduled time against the configurations in the specified instances.

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
- The number of saved and unsaved configurations
- The file added, removed, or modified in the `nsconfig` folder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

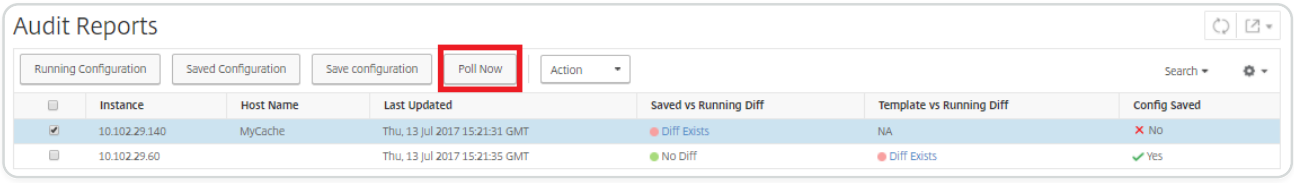


NetScaler ADM also allows you to poll configuration audits manually and adds all the configuration audits of the instances immediately to the NetScaler ADM. To do so, navigate to **Infrastructure > Configuration Audit**, click **Poll Now,** the pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network, or poll the selected instances.

You can also force an audit on an instance. To do so, click any of the following charts:

- **NetScaler Config Saved Status**
- **NetScaler Config Drift**

On the **Audit Reports** page, select the instance and, in the **Action** list, select **Poll Now**.



The **NetScaler Config File Status** chart provides you the status of the NetScaler files present in the `nsconfig` folder. The NetScaler ADM records and compares changes in files within the `nsconfig` folder and displays the differences. See, View the file status audit reports.

Set configuration audit notifications

1. Navigate to **Infrastructure > Configuration Audit**.
2. On the **Configuration Audit** page, click **Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

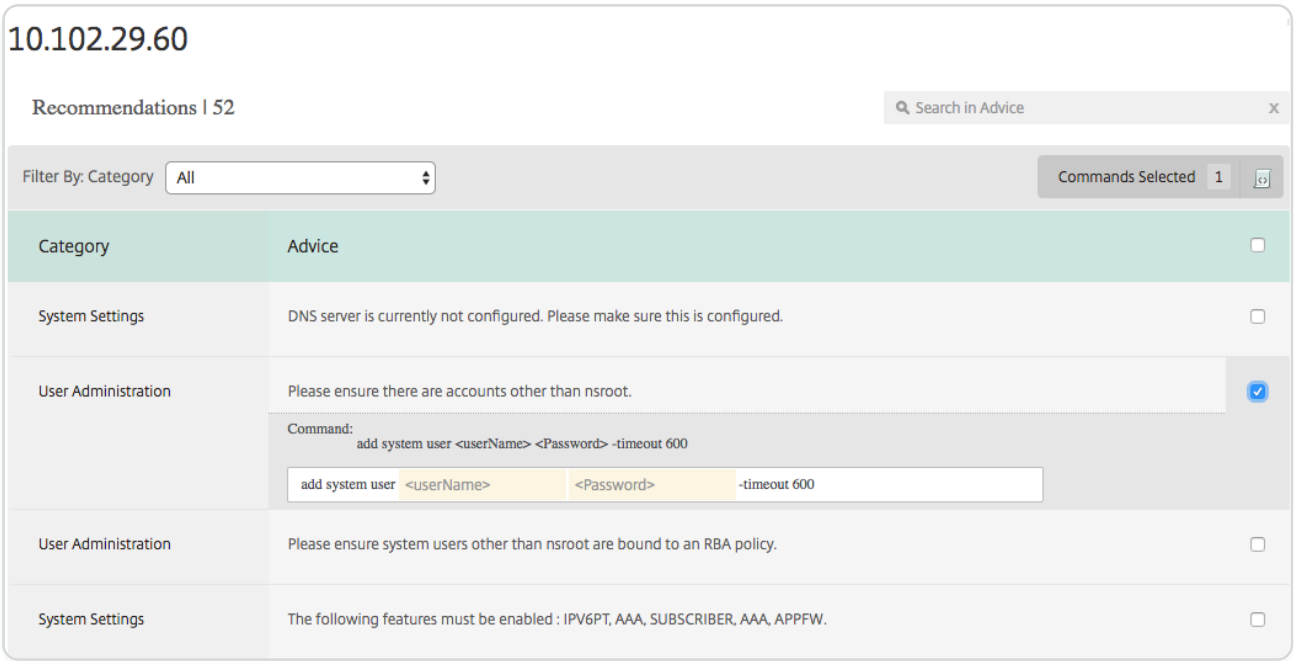
You set up your Citrix Application Delivery Controller™ (ADC) instances with optimal configurations so that you can achieve optimal performance on your applications. However, some configurations might not be standard configurations, which might affect your applications' performance.

To help you optimize your application performance, NetScaler Application Delivery Management (NetScaler ADM) analyzes the NetScaler instance configuration and provides you with recommendations. You can apply the recommended configurations from NetScaler ADM.

To analyze the NetScaler instance:

1. Navigate to **Infrastructure > 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 NetScaler instance that you want to analyze.

NetScaler® ADM analyzes the configuration on your instance and provides a list of configuration recommendations as shown in the following image. Click the check box next to a configuration advice to view the corrective commands.

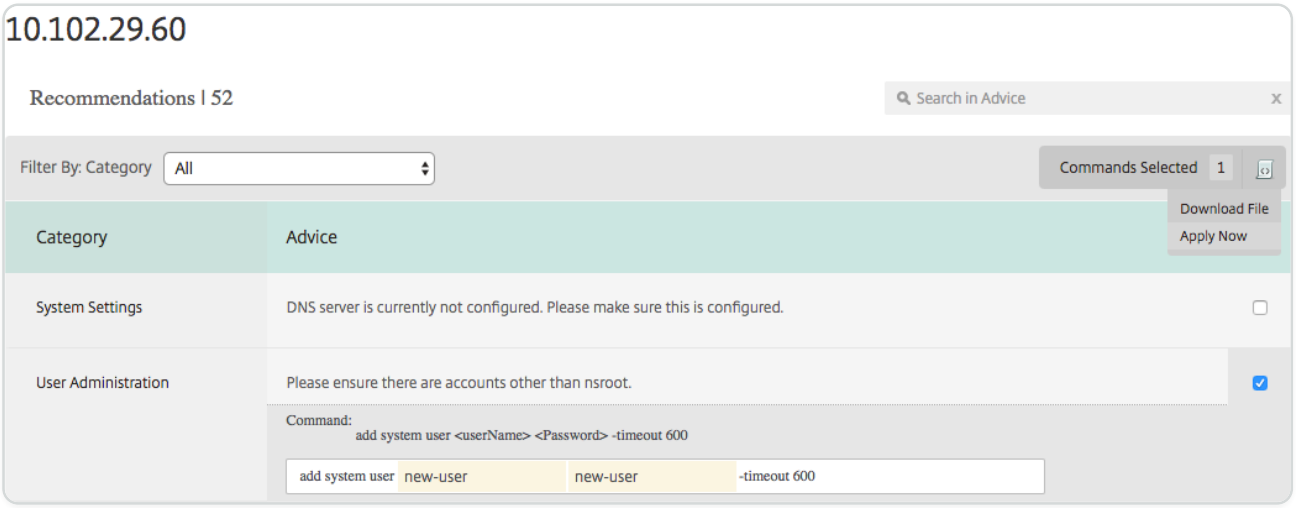


© 1997–2026 Citrix Systems, Inc. All rights reserved.

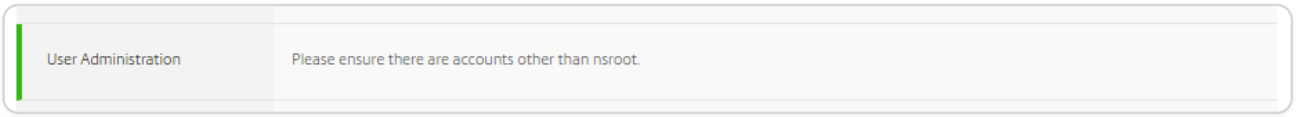
If you want to update your configuration, specify the values for the variables in the corrective commands and click **Apply Now** as shown in the following image.

NOTE

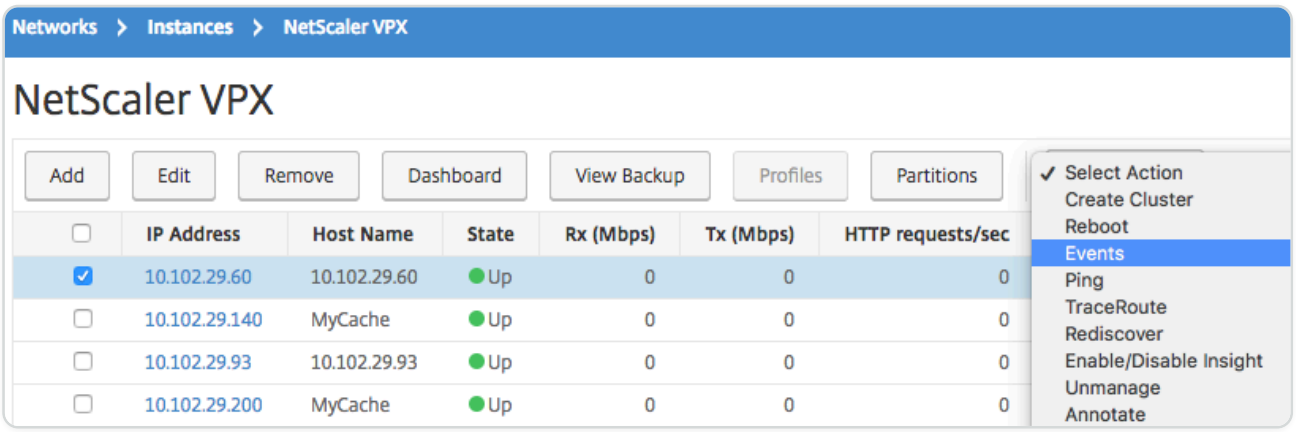
The commands listed here are only recommendations. A user with read and write access might be able to edit any command using this feature. Ensure that you grant a limited privileged access to users whom you think must not edit the commands.



When the command is successfully run on the network instance, the check box next to the advice disappears.

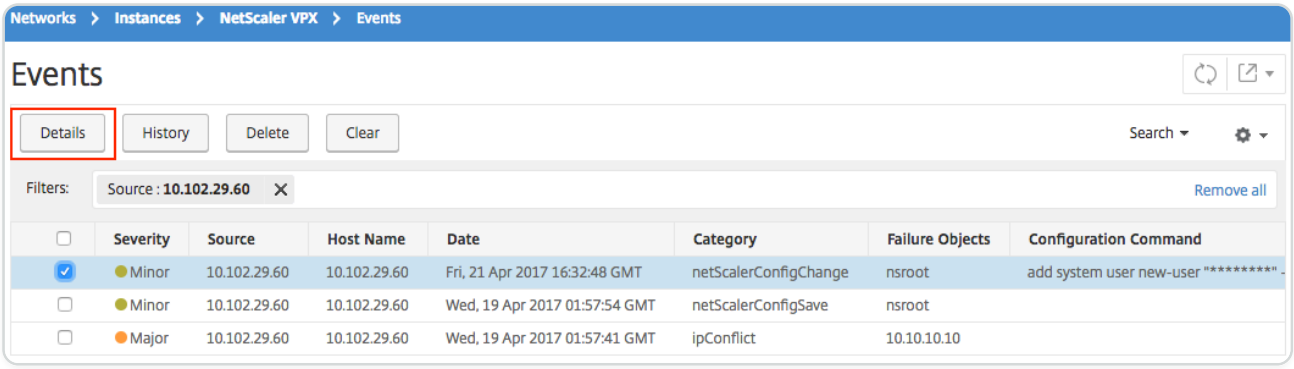


If you want to view the details of the commands run on your network instance, navigate to **Infrastructure > Instances >** `<Instance\_Type\>`, select the IP address of the instance, and then click **Events** from the **Actions** drop-down list.



On the **Events** page, you can view the details of the configuration change.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



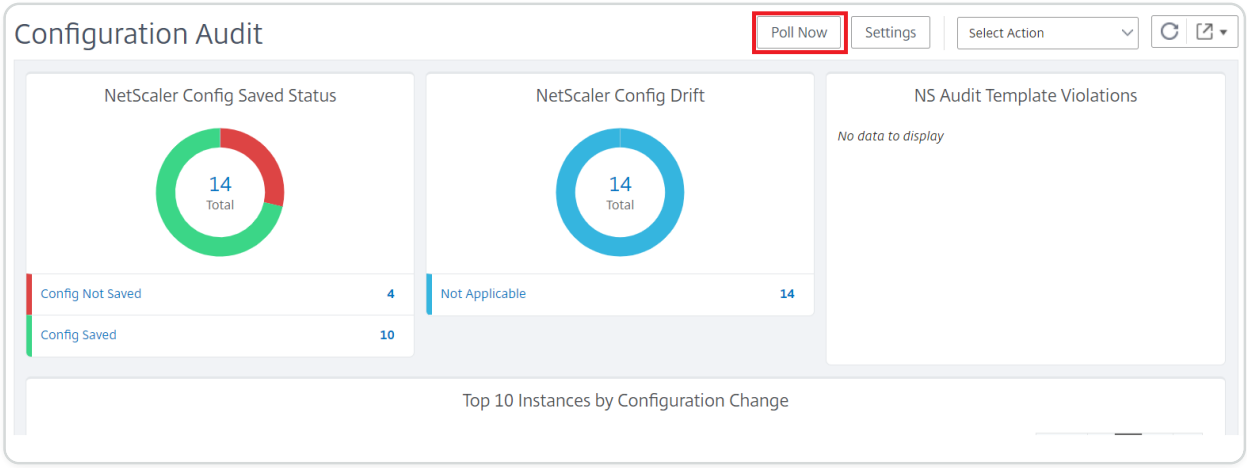
Poll configuration audit of NetScaler instances

NetScaler Application Delivery Management (NetScaler 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 NetScaler instances configuration places a heavy load on the network.

Instead of polling the entire NetScaler instances configuration audit, you can manually poll only the configuration audits of a selected instance or instances.

To poll configuration audits of NetScaler instances:

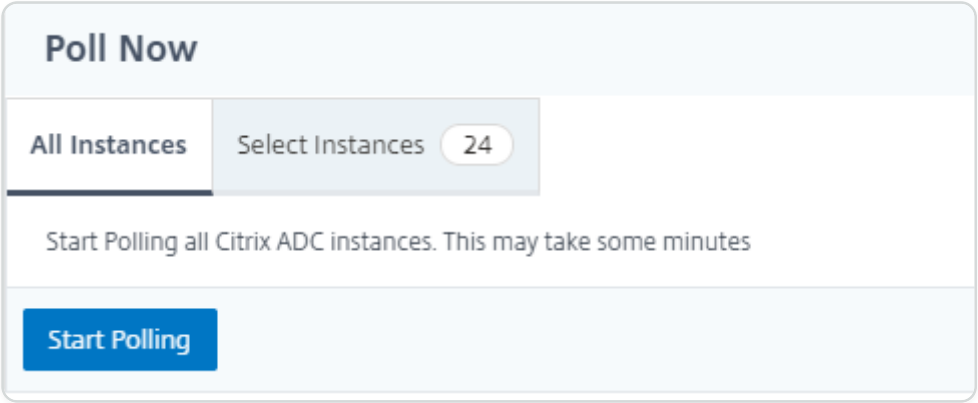
1. In NetScaler® ADM, navigate to **Infrastructure > Configuration Audit**.
2. On **Configuration Audit** page, in the top right-hand corner, click **Poll Now**.



3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or poll selected instances.

   a. To poll all NetScaler instances, select the **All Instances** tab and click **Start Polling**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.

Generate configuration audit diff for ConfigChange SNMP Traps

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 NetScaler Application Delivery Management (NetScaler ADM). You can enable NetScaler 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 run that on the specific NetScaler 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 NetScaler ADM.

To run configuration audit templates on receiving ConfigChange SNMP trap:

NetScaler® ADM allows you to enable the option to run the configuration audit template in NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler ADM, navigate to **Infrastructure > 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. NetScaler 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. NetScaler ADM runs the configuration audit template on the NetScaler instance after this time delay when it receives the ConfigChange SNMP trap by that instance.

Upgrade jobs

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

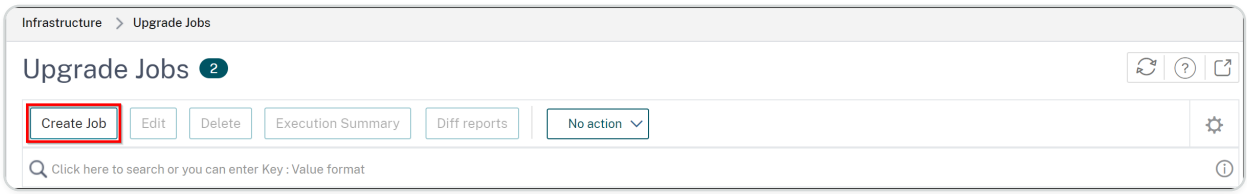
LAS based licenses may not be available to customers where prohibited by law or regulations. If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

You can create the following maintenance tasks using NetScaler ADM. You can then schedule the maintenance tasks at a specific date and time.

- Upgrade NetScaler instances
- Upgrade NetScaler SDX instances
- Upgrade NetScaler BLX instances
- Upgrade NetScaler instances in the Autoscale Group
- Configure HA pair of NetScaler instances
- Convert HA pair of instances to Cluster

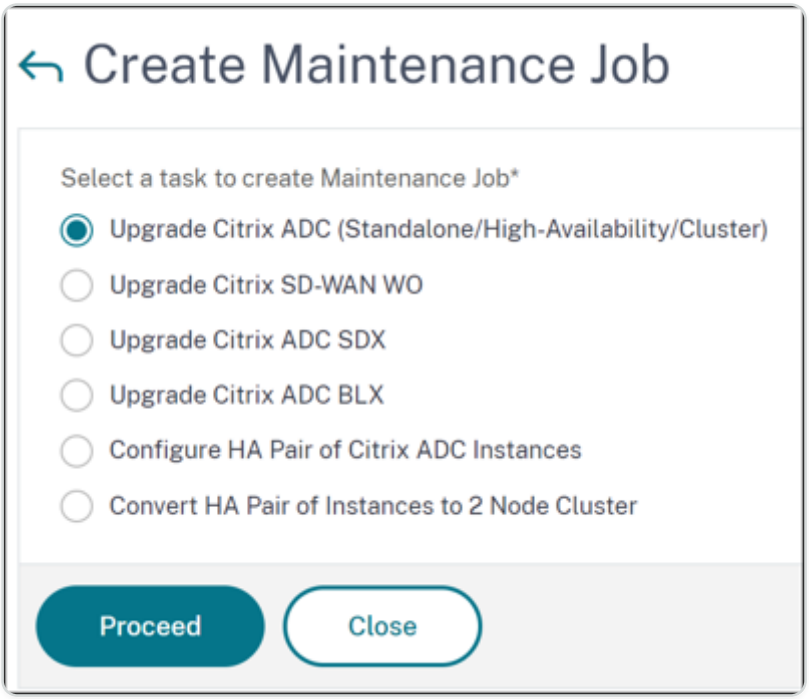
Schedule upgrading of NetScaler instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.

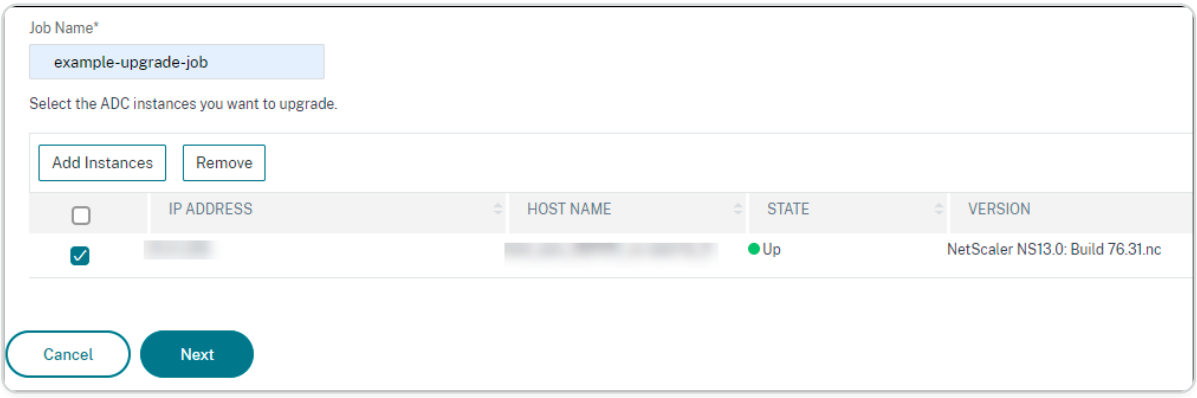


2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/Cluster)** and click **Proceed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add ADC instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.



5. Click **Next** to select the image. Select one of the following options from the **Software Image** list:
   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from NetScaler ADM file browser. The NetScaler ADM GUI displays the instance files that are present at `/var/mps/mps_images`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.
- **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.

6. Click **Next** to start the pre-upgrade validation on the selected instances.

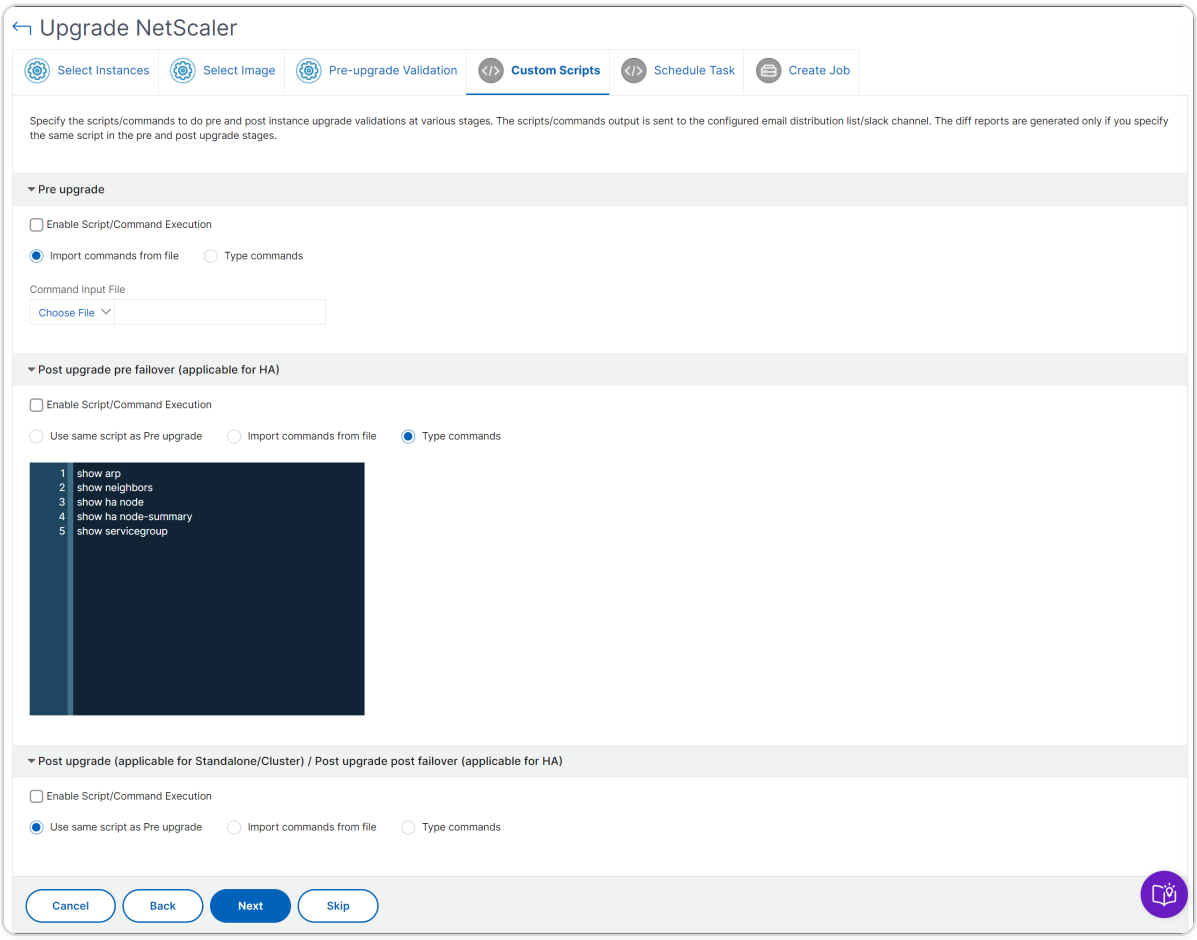
   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   IMPORTANT

   If you specify cluster IP address, NetScaler ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. Click **Next**. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an ADC HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

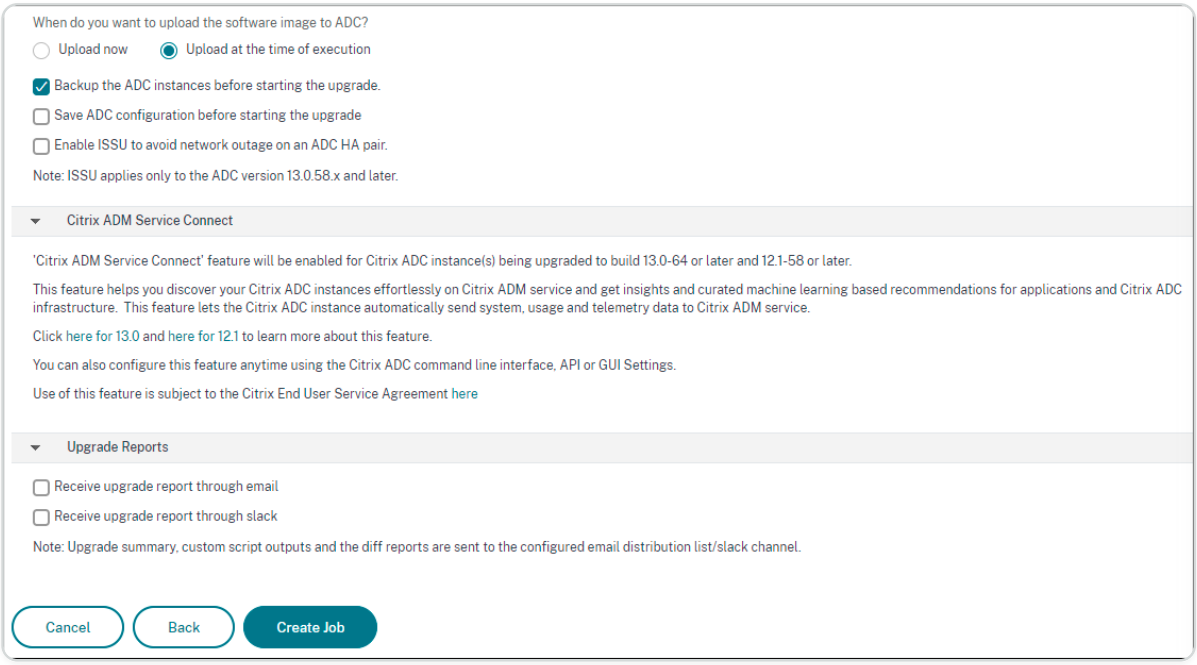
9. Click **Next**. In **Create Job**, specify the following details:

   a. Specify when you want to upload the image to an instance:

      - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
      - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
      - **Backup the ADC instances before starting the upgrade.** - Creates a backup of the selected ADC instances.
      - **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
      - **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler ADM Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler ADM Service Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using NetScaler ADM service connect.
- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

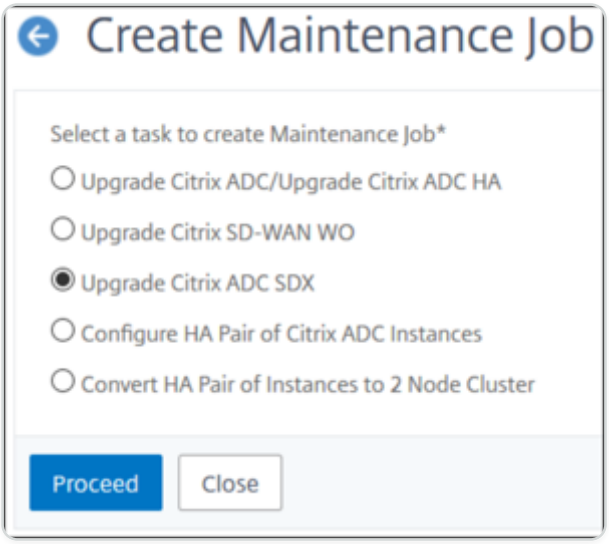


10. Click **Create Job**.

Schedule upgrading of NetScaler SDX instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade NetScaler SDX** and click **Proceed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

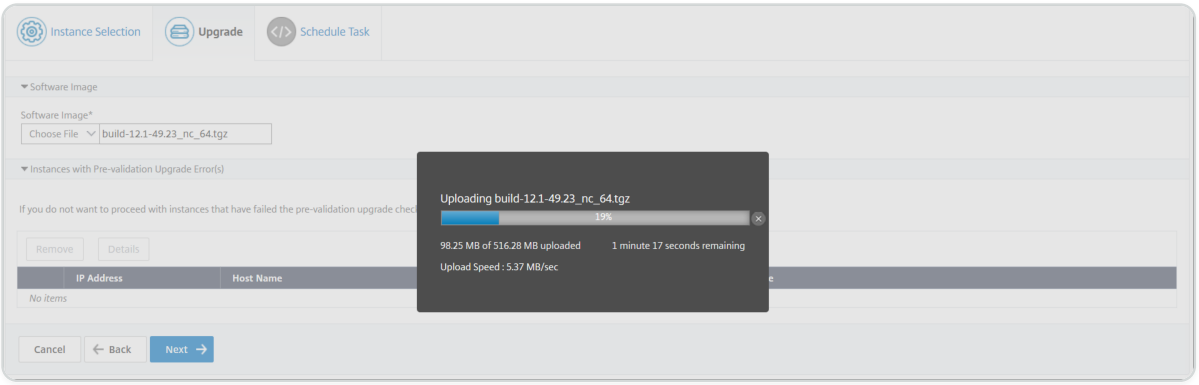


3. On the **Upgrade NetScaler SDX** page, in the **Instance Selection** tab:

   a. Add a **Task Name**.

   b. From the **Software Image** list, select either **Local** (your local machine) or **Appliance** (the build file must be present on NetScaler ADM virtual appliance).

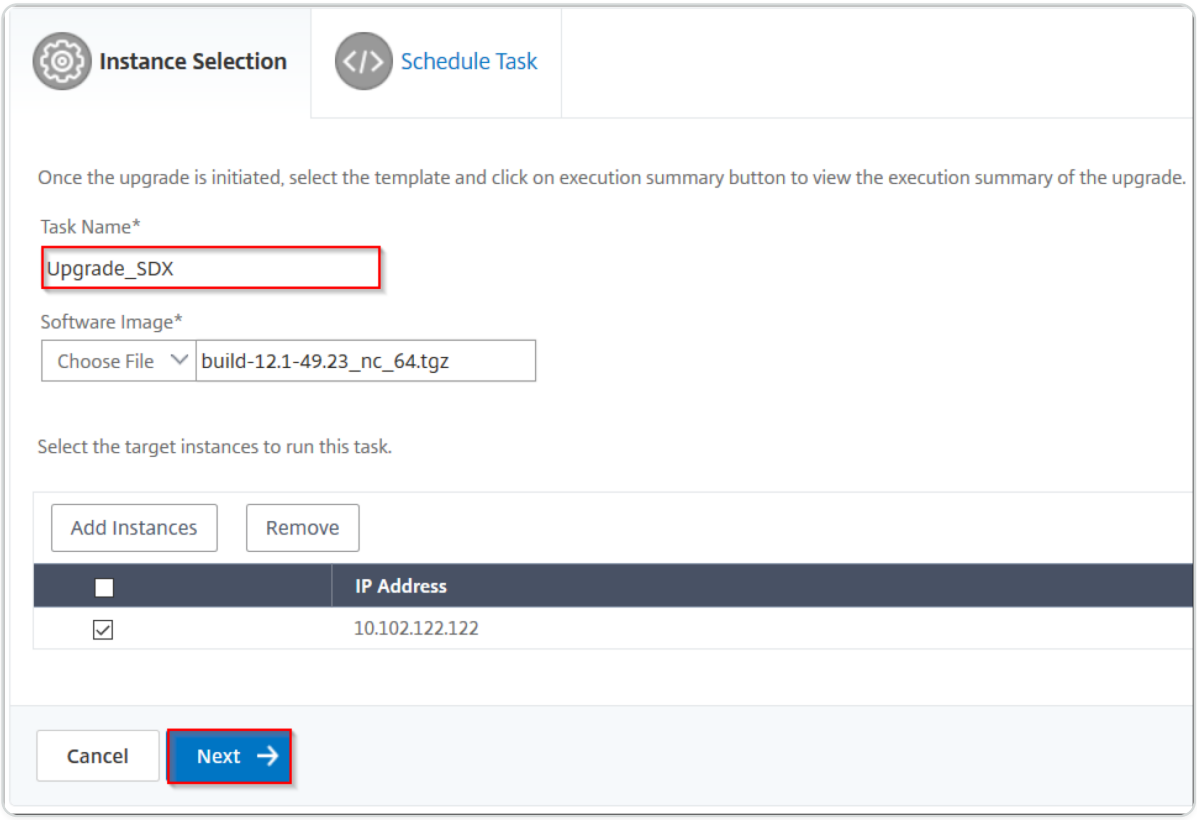
      The upload process begins.



   c. Add the NetScaler SDX instances on which you want to run the upgrade process.

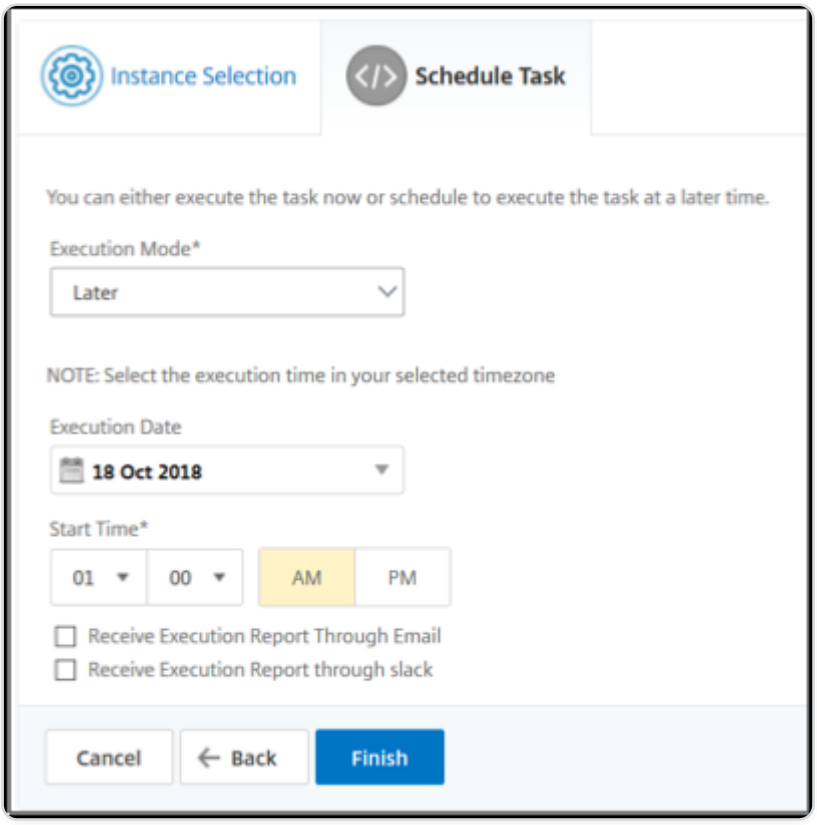
   d. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler SDX instance now, and click **Finish**.
5. To upgrade a NetScaler SDX instance later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the NetScaler instance, and click **Finish**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

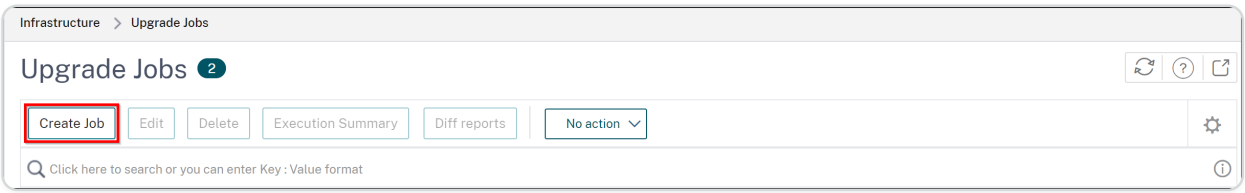


6. You can also enable email and slack notifications to receive the execution report of the upgrading NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

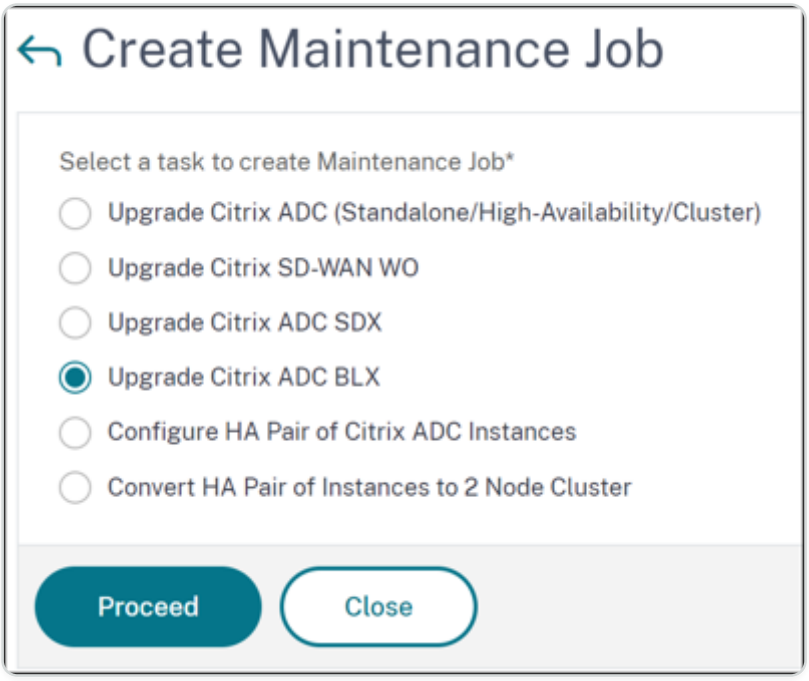
Schedule upgrading of NetScaler BLX instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.

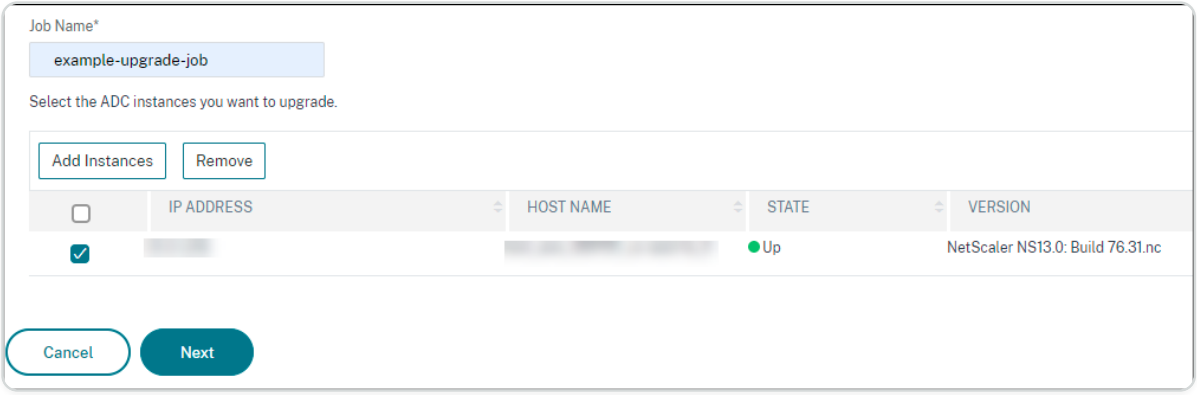


2. In **Create Maintenance Jobs**, select **Upgrade NetScaler BLX** and click **Proceed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



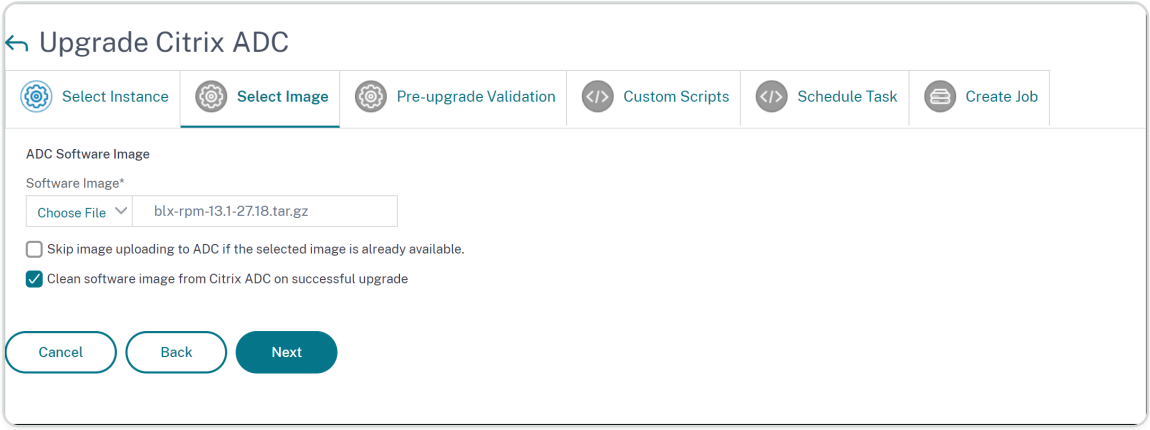
3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add the BLX instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.



5. Click **Next** to select the image. elect one of the following options from the **Software Image** list:
   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from NetScaler ADM file browser. The NetScaler ADM GUI displays the instance files that are present at `/var/mps/mps_images`.
     - **Skip image uploading to ADC if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.



6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

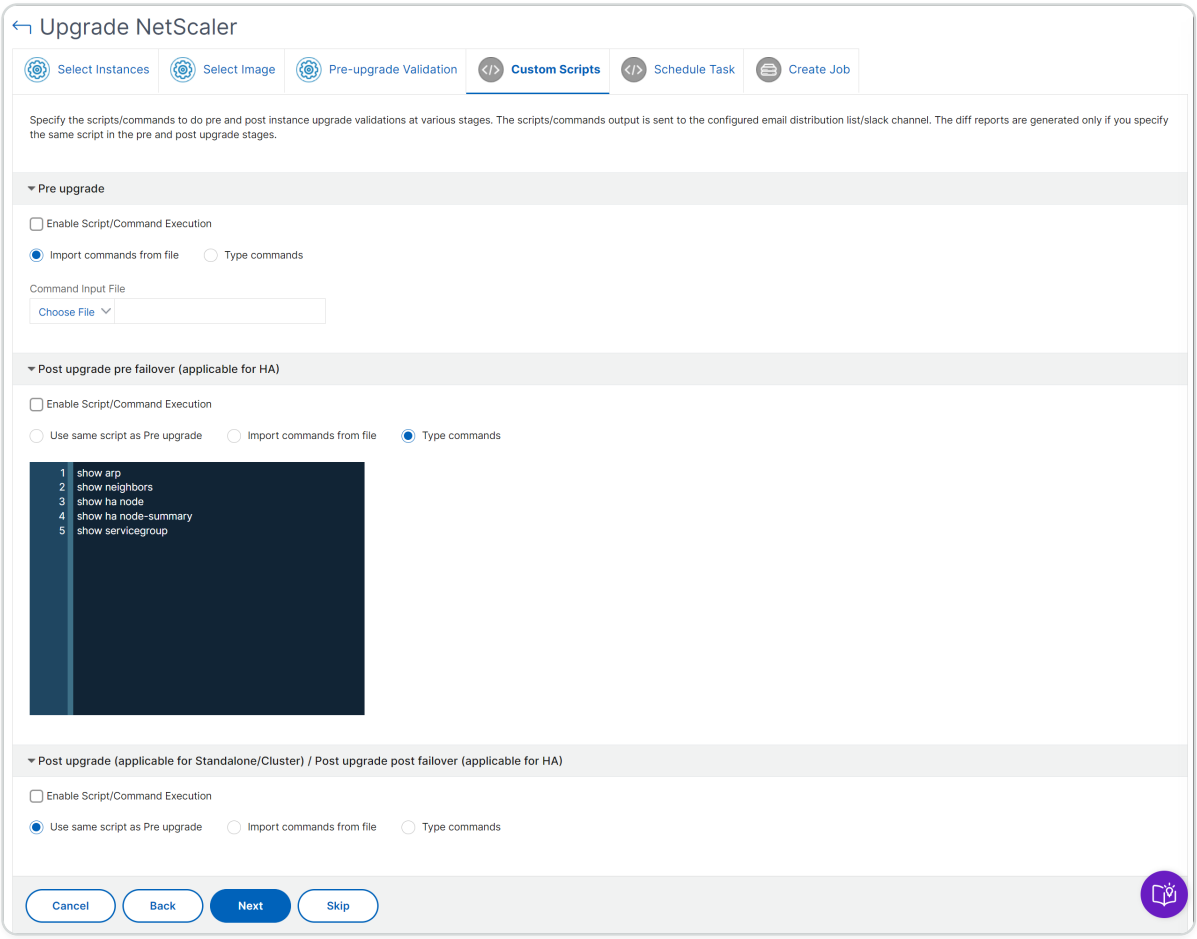
   IMPORTANT

   If you specify cluster IP address, NetScaler ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

8. Click **Next**. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

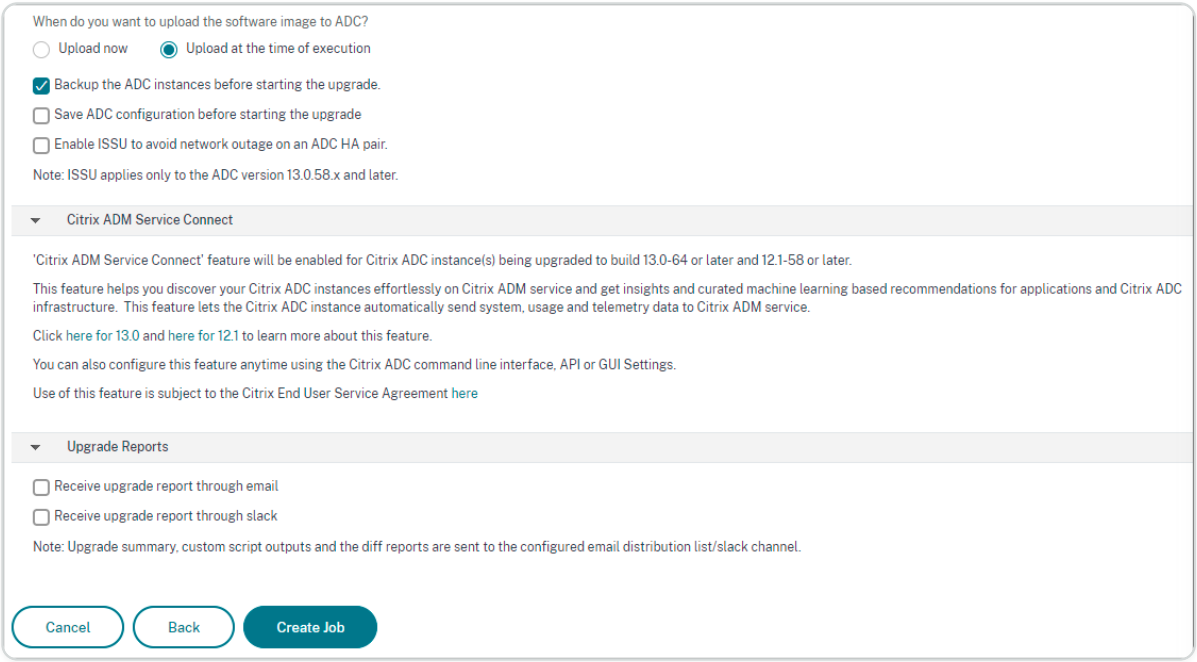
9. Click **Next**. In **Create Job**, specify the following details:

   a. Specify when you want to upload the image to an instance:

      - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
      - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
      - **Backup the ADC instances before starting the upgrade** - Creates a backup of the selected ADC instances.
      - **Saves ADC Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
      - **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

   - **NetScaler ADM Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler ADM Service Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using NetScaler ADM service connect.
   - **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
   - **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Click **Create Job**.

Schedule upgrading Autoscale™ group

Perform the following steps to upgrade all the instances in the cloud services that are part of the Autoscale group:

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade Autoscale Group** and click **Proceed**.
3. In the **Upgrade Settings** tab:
   a. Select the **Autoscale Group** that you want to upgrade.
   b. In **Image**, select the NetScaler version. This image is the existing version of NetScaler instances in the Autoscale group.
   c. In **NetScaler Image**, browse the NetScaler version file to which you want to upgrade.

      If you check **Graceful Upgrade**, the upgrade task waits until the specified drain connection period to expire.
   d. Click **Next**.
4. In the **Schedule Task** tab:
   a. Select one of the following from the Execution Mode list:
      - **Now:**To start the NetScaler instances upgrade immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Later:** To start the NetScaler instances upgrade at later time.

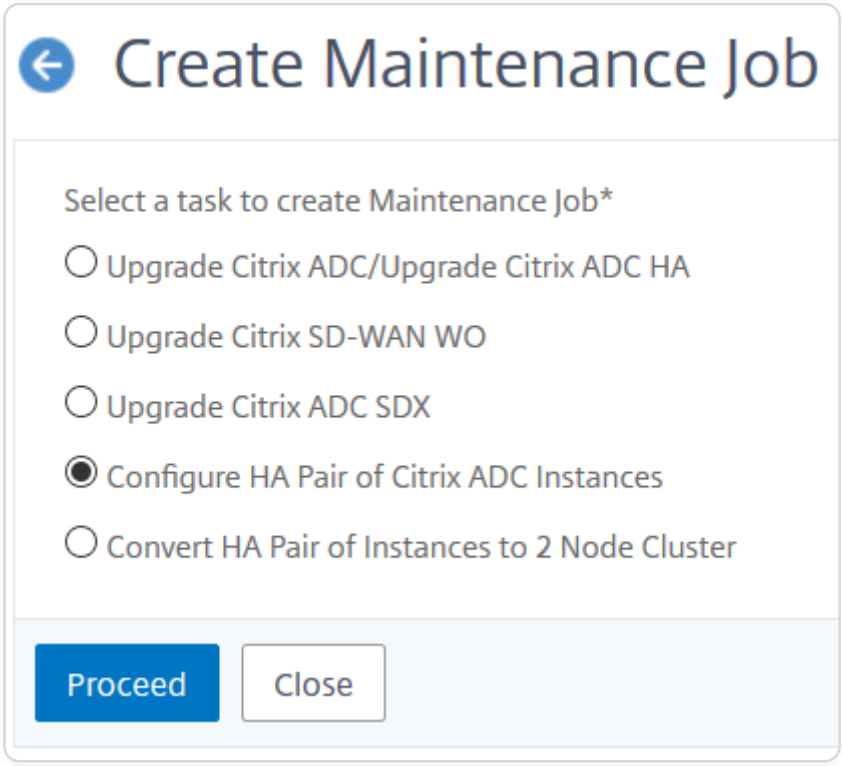
b. If you select the **Later** option, select the Execution Date and Start Time when you want to start the upgrade task.

You can also enable email and slack notifications to receive the execution report of the upgrading Autoscale group. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

5. Click **Finish**.

Schedule configuring HA pair of NetScaler instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Configure HA Pair of NetScaler Instances** and click **Proceed**.



3. On the **NetScaler HA Pair** page, in the **Instance Selection** tab:

   a. Add a **Task Name**.

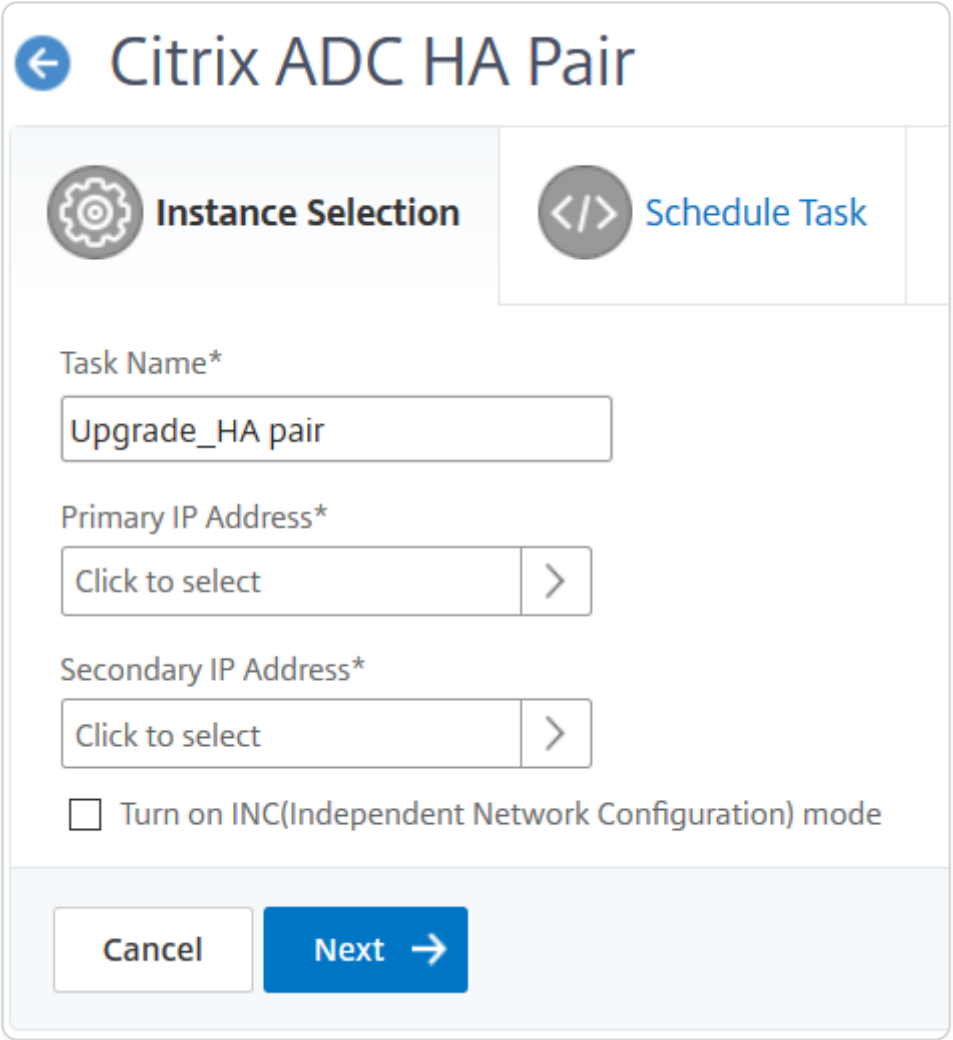
   b. Enter the Primary IP Address.

   c. Enter the Secondary IP Address.

   d. Click **Next**.

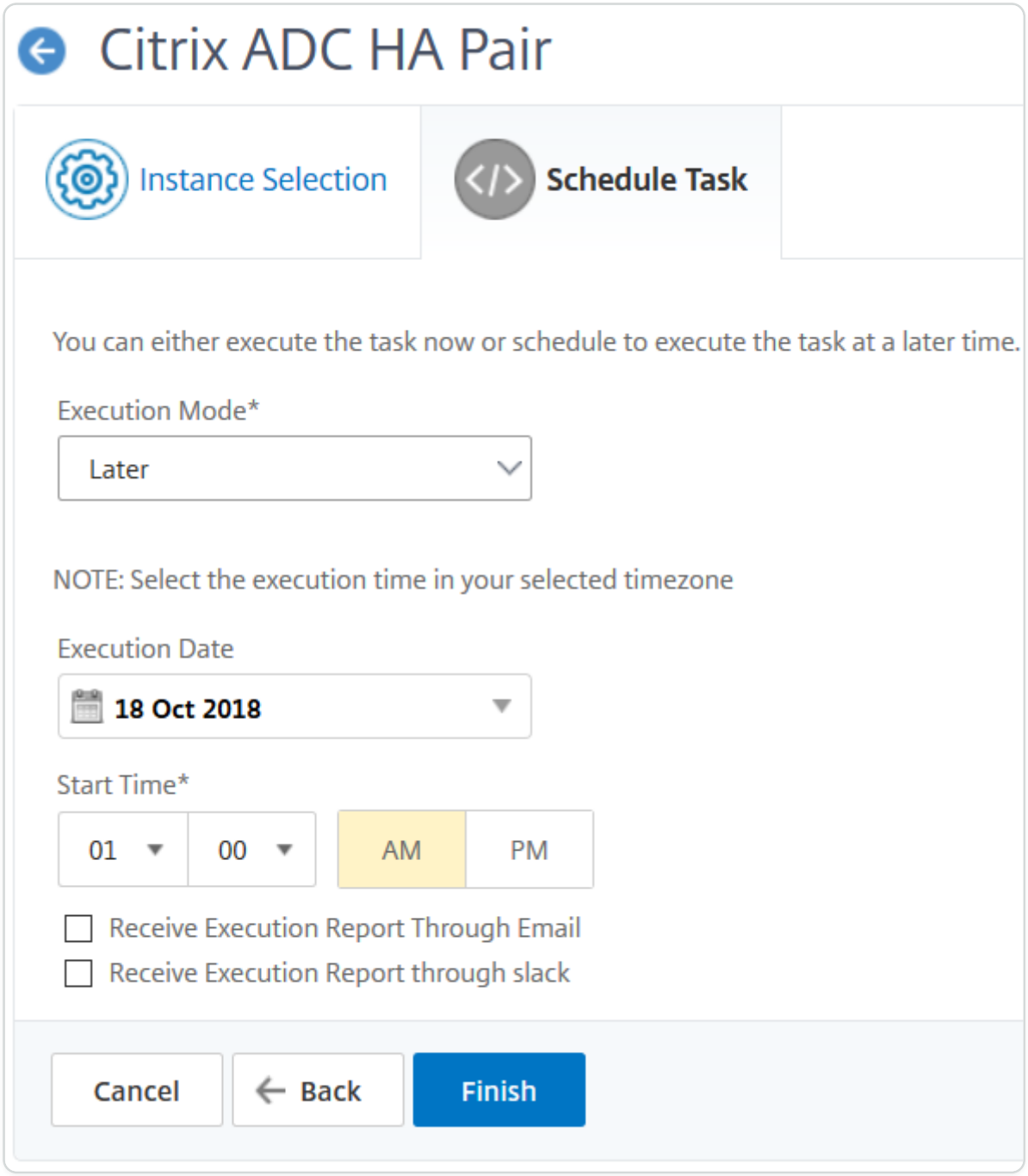
   e. Click to enable **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.
5. To upgrade a NetScaler HA pair later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the NetScaler instance, and click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



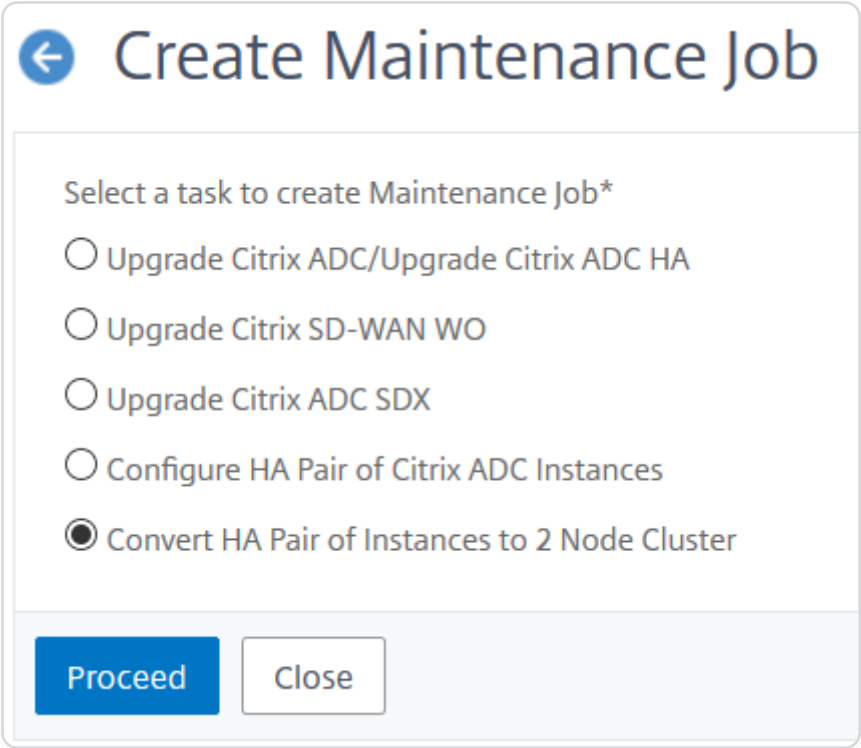
6. You can also enable email and slack notifications to receive the execution report of creating the ADC HA pair. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Schedule converting HA pair of instances to cluster

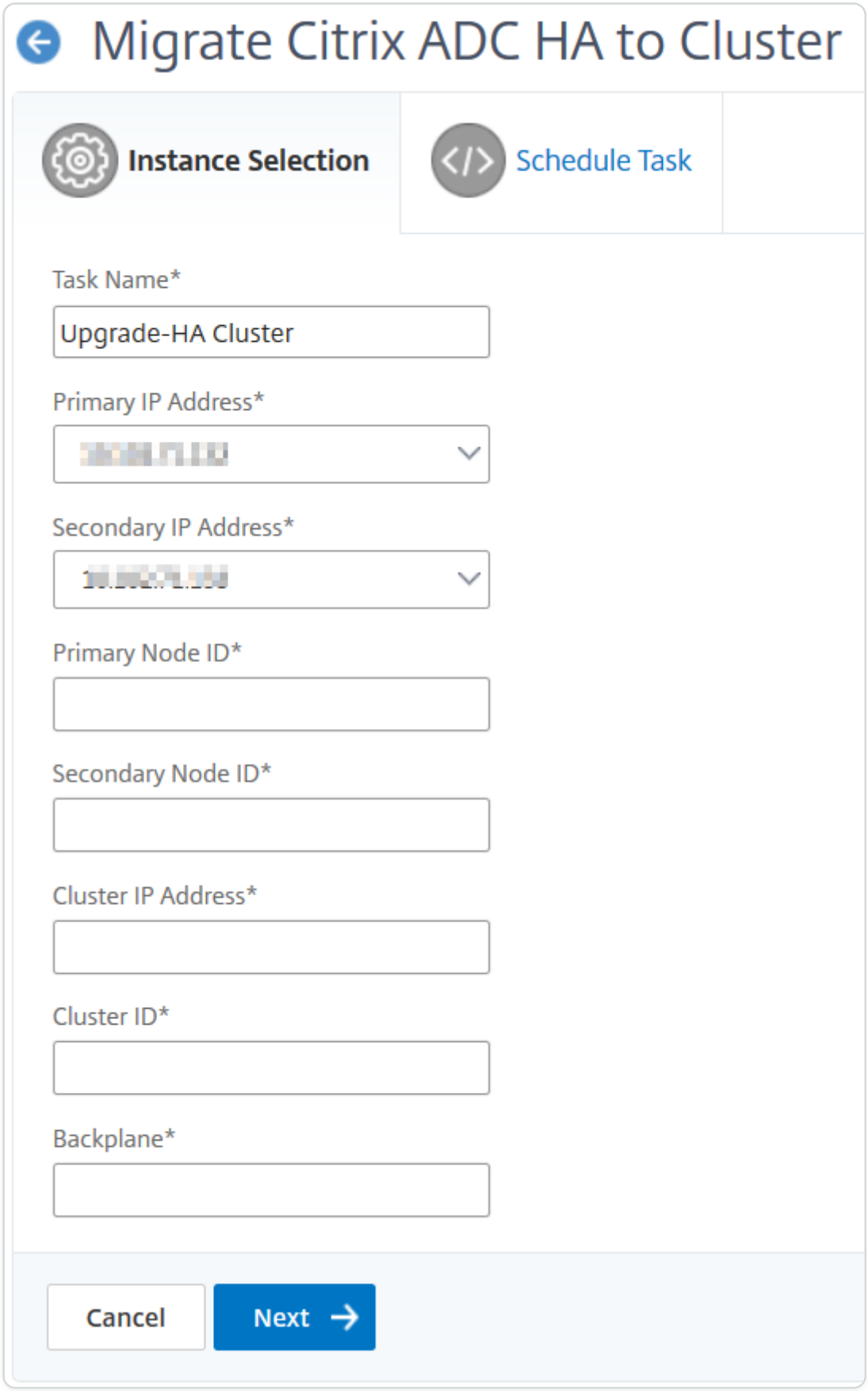
1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. On the **Migrate NetScaler HA to Cluster** page, in the **Instance Selection** tab, add a **Task Name**. Specify the Primary IP address, Secondary IP address, Primary Node ID, Secondary Node ID, Cluster IP Address, Cluster ID, and Backplane, and then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. To upgrade later, select **Later** from the **Execution Mode** list. You can then choose the **Execution Date** and the **Start Time** for upgrading the NetScaler HA pair instance, and click **Finish**.
6. You can also enable email and slack notifications to receive the execution report of upgrading a NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Instance Advisory

Instance advisory provides recommendations that help you keep your NetScaler instances secure and up to date. The following topics help you review and act on these advisories:

- Upgrade Advisory
- Security Advisory

Upgrade Advisory (Preview)

As a network administrator, you might manage many ADC instances running on different ADC builds in NetScaler ADM. Monitoring the lifecycle of each ADC instance can be a cumbersome task. You must visit NetScaler product Matrix, identify the ADC instances that are reaching or have reached the End of Life (EOL) or End of Maintenance (EOM). Then, plan their upgrade.

NetScaler ADM on-premises Upgrade Advisory performs a version scan on the ADCs and provides a view of the EOM/EOL builds across your ADC instances.

IMPORTANT

For detailed insights, and the workflow to upgrade the ADC instances, **try NetScaler® ADM Service**.

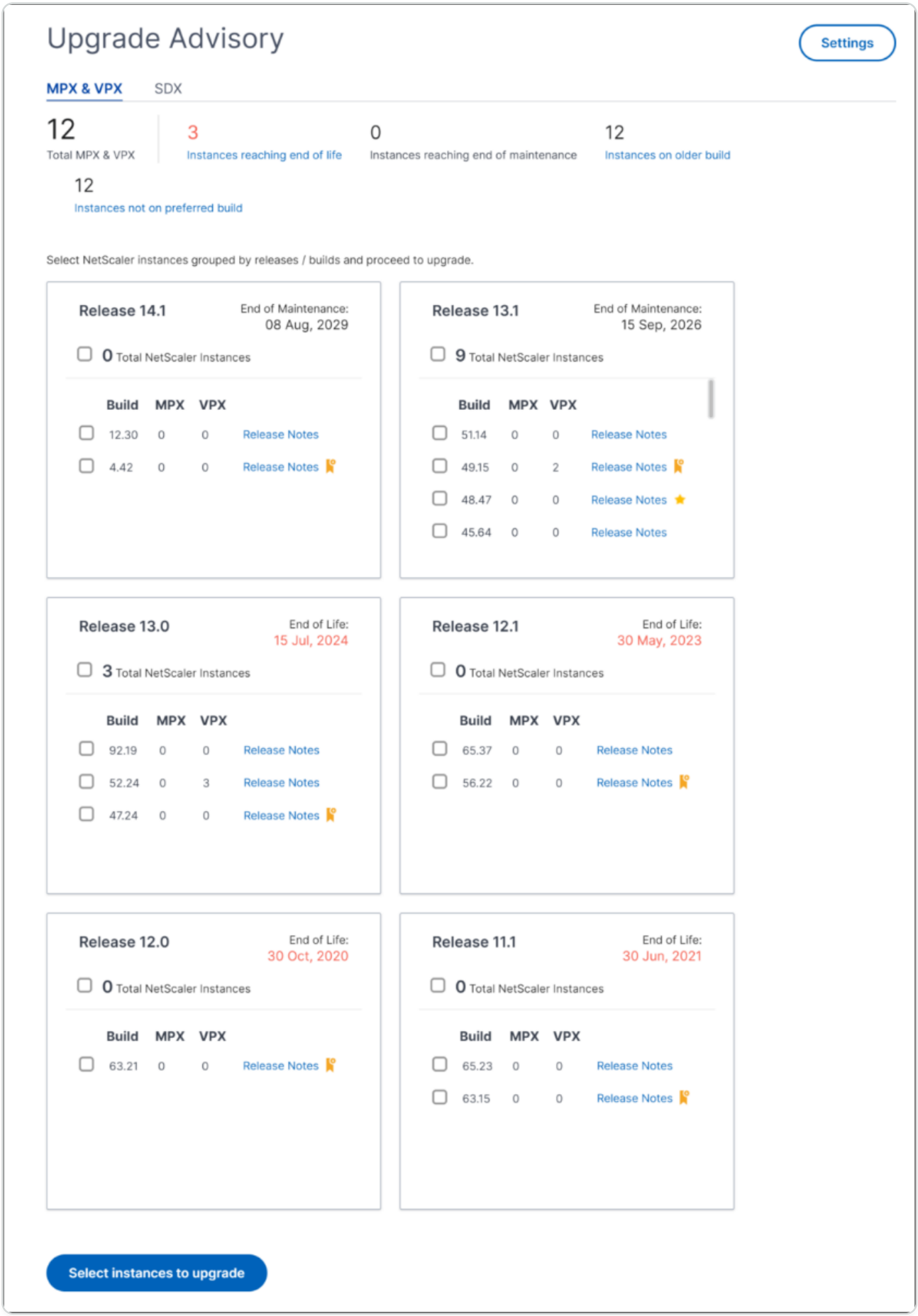
View upgrade advisory

Navigate to **Infrastructure > Instance Advisory > Upgrade Advisory** and view the following information:

- Total count of ADC instances.
- Instances reaching the end of life.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Instances reaching the end of maintenance.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Upgrade Advisory** page groups the ADC instances by their releases.

NetScaler ADM on-premises upgrade advisory also allows you to select one of the ADC instances, and onboard the ADC instance to ADM Service. Click **Try ADM Service** and onboard the ADC instance to ADM Service. ADM Service Upgrade Advisory provides you the workflow to upgrade by selected ADC instance.

For more information on the ADM Service Upgrade Advisory, view the gif animation on the **Upgrade advisory** page.

Security Advisory (Preview)

NOTE:

Starting from 13.1-53.22 build, Security Advisory is automatically enabled. For more information, see Security Advisory

A safe, secure, and resilient infrastructure is the lifeline of any organization. Organizations must track new Common Vulnerabilities and Exposures (CVEs), and assess the impact of CVEs on their infrastructure. They must also understand and plan the mitigation and remediation to resolve the vulnerabilities.

NetScaler® ADM on-premises Security Advisory only highlights the NetScaler CVEs and the ADC instances that are at risk.

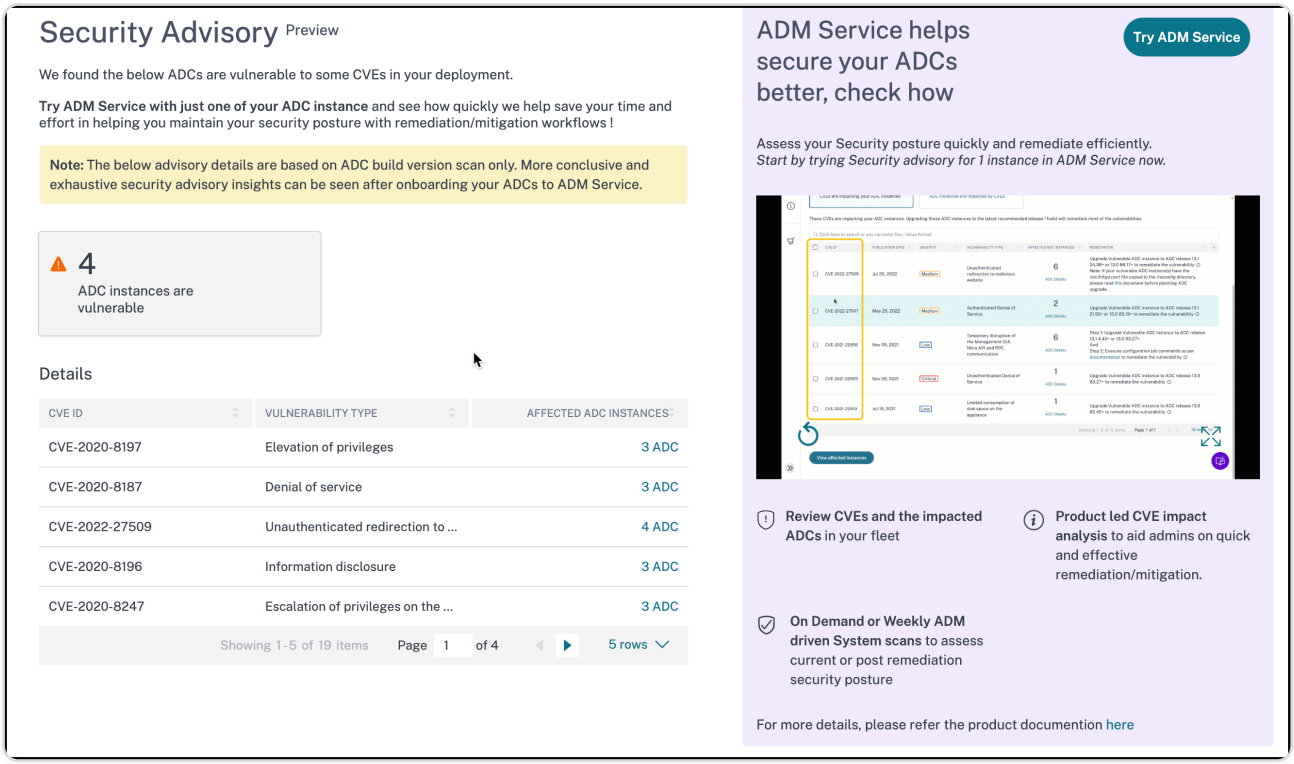
IMPORTANT

For a detailed analysis on the CVE impact, conclusive information on custom scans/system scans, remediation and mitigation workflows, **try NetScaler ADM Service**.

View security advisory

To access **Security Advisory**, navigate to **Infrastructure > Instance Advisory > Security Advisory**. You can see the vulnerability status of all the ADC instances that you manage through NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler ADM on-premises Security Advisory performs only ADC Version scan to check for CVEs and following information is displayed.

- **CVE ID**: The ID of the CVE impacting the instances.
- **Vulnerability type**: The type of vulnerability for this CVE.
- **Affected ADC instances**: The instance count that the CVE ID is impacting.

NetScaler ADM on-premises Security Advisory also allows you to select one of the ADC instances, and onboard the ADC instance to ADM Service. Click **Try ADM Service** and onboard the ADC instance to ADM Service. ADM Service Security Advisory allows you to check the vulnerability type of a particular CVE and get information on mitigation and remediation to resolve the vulnerability.

For more information on the ADM Service Security Advisory, view the gif animation on the **Security Advisory** page.

Supported CVEs through Security Advisory

In your NetScaler Console on-prem, the full version of Security Advisory is supported if you have enabled Security Advisory through the auto-enabled channel. For more information, see Security Advisory.

Latest supported CVEs

The following table provides the latest supported CVE details that you can identify and remediate in Security Advisory:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE DATE	CVE ID	IDENTIFICATION	REMEDIATION	RESOURCE LINK
11 Nov 2025	CVE-2025-12101	Requires version scan.	Upgrade to the recommended build mentioned in the security bulletin.	Security Bulletin

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect on the impact of CVEs in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

Supported CVEs

The following are the existing CVEs supported in Security Advisory:

RELEASE DATE	CVE ID	RESOURCE LINK
Nov 11, 2025	CVE-2025-12101	Security Bulletin
Aug 26, 2025	CVE-2025-8424	Security Bulletin
Aug 26, 2025	CVE-2025-7776	Security Bulletin
Aug 26, 2025	CVE-2025-7775	Security Bulletin
Jun 25, 2025	CVE-2025-6543	Security Bulletin
Jun 17, 2025	CVE-2025-5349	Security Bulletin

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE DATE	CVE ID	RESOURCE LINK
Jun 17, 2025	CVE-2025-5777	Security Bulletin
Nov 12, 2024	CVE-2024-8534	Security Bulletin
Nov 12, 2024	CVE-2024-8535	Security Bulletin
Jul 09, 2024	CVE-2024-5491	Security Bulletin
Jul 09, 2024	CVE-2024-5492	Security Bulletin
Jan 16, 2024	CVE-2023-6549	Security bulletin
Jan 16, 2024	CVE-2023-6548	Security bulletin
Oct 10, 2023	CVE-2023-4967	Security bulletin
Oct 10, 2023	CVE-2023-4966	Security bulletin
Jul 18, 2023	CVE-2023-3519	Security bulletin
Jul 18, 2023	CVE-2023-3467	Security bulletin
Jul 18, 2023	CVE-2023-3466	Security bulletin
May 09, 2023	CVE-2023-24488	Security bulletin
May 09, 2023	CVE-2023-24487	Security bulletin
Dec 13, 2022	CVE-2022-27518	Security bulletin
Nov 08, 2022	CVE-2022-27516	Security bulletin
Nov 08, 2022	CVE-2022-27513	Security bulletin
Nov 08, 2022	CVE-2022-27510	Security bulletin
Jul 26, 2022	CVE-2022-27509	Security bulletin
May 25, 2022	CVE-2022-27508	Security bulletin
May 25, 2022	CVE-2022-27507	Security bulletin

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE DATE	CVE ID	RESOURCE LINK
Nov 09, 2021	CVE-2021-22956	Security bulletin
Nov 09, 2021	CVE-2021-22955	Security bulletin
Jul 19, 2021	CVE-2021-22927	Security bulletin
Jul 19, 2021	CVE-2021-22920	Security bulletin
Jul 19, 2021	CVE-2021-22919	Security bulletin
Jun 08, 2021	CVE-2020-8300	Security bulletin
Jun 08, 2021	CVE-2020-8299	Security bulletin
Sep 17, 2020	CVE-2020-8247	Security bulletin
Sep 17, 2020	CVE-2020-8246	Security bulletin
Sep 17, 2020	CVE-2020-8245	Security bulletin
Jul 07, 2020	CVE-2020-8197	Security bulletin
Jul 07, 2020	CVE-2020-8199	Security bulletin
Jul 07, 2020	CVE-2020-8195	Security bulletin
Jul 07, 2020	CVE-2020-8196	Security bulletin
Jul 07, 2020	CVE-2020-8193	Security bulletin
Jul 07, 2020	CVE-2020-8187	Security bulletin
Jul 07, 2020	CVE-2020-8191	Security bulletin
Jul 07, 2020	CVE-2020-8190	Security bulletin
Jul 07, 2020	CVE-2019-18177	Security bulletin
Jul 07, 2020	CVE-2020-8194	Security bulletin
Jul 07, 2020	CVE-2020-8198	Security bulletin

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RELEASE DATE	CVE ID	RESOURCE LINK
Dec 17, 2019	CVE-2019-19781	Security bulletin

Orchestration

In Software Defined Networking (SDN), a software application controller manages a network and its activities instead of hardware that supports the network. That is, SDN allows the network administrators to virtualize a physical network connectivity into a logical network connectivity and manage network services using a software based centralized management tool. SDN allows network engineers and administrators to respond to rapidly changing business requirements.

While the better known advantages of SDN are traffic programmability, greater agility, the ability to create policy driven network supervision, and implementing network automation, some of the specific advantages of SDN are listed below:

- Centralized network provisioning
- Increased network security at granular level
- Reduced operating costs
- Increased levels of cloud abstraction
- Guaranteed content delivery
- Reduced network downtime

NetScaler® Application Delivery Management (ADM) supports SDN in enterprises network by integrating with SDN controllers of different vendors. NetScaler ADM supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

NetScaler ADM integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter administrators to programmatically deploy NetScaler services faster.

VMware NSX Manager exposes logical firewalls, switches, routers, ports, and other networking elements to allow virtual networking among diverse hypervisors, cloud management systems, and associated network hardware. It also supports external networking, and security services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Cloud Orchestration feature of NetScaler ADM enables the integration of NetScaler products with VMware NSX, and provides the following capabilities:

- Ability to allocate a pre-provisioned VPX on-demand to a certain Edge gateway as part of service insertion.
- Ability to configure advanced features of NetScaler such as SSL and CS along with basic load balancing through application templates on the instances that are running inside NSX environment.
- Ability to de-allocate a VPX from a certain Edge gateway as part of service deletion and reallocate the same VPX for another Edge gateway.
- Ability to rapidly deploy NetScaler functions from the vCenter console as part of the deployment workflow of all the infrastructure required for an application.

Benefits:

- Automated, on-demand allocation of new ADC services as part of an application deployment workflow
- Simplified configuration of application specific, advanced ADC functionality through application templates
- Multitenant separation-of-duties and a self-service consumption model while providing cloud administrators a single point of control
- Easier integration with NetScaler ADM API's, which help to support unanticipated future uses.

For more information on how to configure VMware NSX Manager on NetScaler ADM, see Integrating NetScaler Appliances with VMware NSX Manager.

Cisco ACI Hybrid Mode

Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to NetScaler ADM, which acts as a Device Manager in the APIC.

The NetScaler Hybrid Mode solution is supported by a hybrid mode device package and NetScaler ADM. You need to upload the hybrid mode device package in the APIC. For more information, see NetScaler Automation Using NetScaler ADM in Cisco ACI's Hybrid Mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenStack: Integrating NetScaler instances

The Cloud Orchestration feature of NetScaler Application Delivery Management (ADM) enables integration of NetScaler products with OpenStack platform. By using this feature with OpenStack platform, the OpenStack users are able to avail the load balancing feature (LBaaS) of the NetScaler. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in NetScaler instance.

The following sections provide a brief description of the features in NetScaler® ADM and OpenStack integration workflow.

NetScaler Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plug-in includes a NetScaler driver that enables OpenStack to communicate with the NetScaler ADM. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the NetScaler ADM, which creates the load balancer configuration on the desired NetScaler instances. OpenStack also uses the driver to call NetScaler ADM at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the NetScalers. NetScaler driver software for OpenStack platform is bundled along with the NetScaler ADM. To download and install the drivers, you have to first install NetScaler ADM and launch the application.

Registering NetScaler ADM and OpenStack with each other

You have to first register OpenStack information on the NetScaler ADM. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack NetScaler driver user credentials. You can later specify the same login credentials in the NetScaler_driver section of the Neutron configuration file (neutron.conf) so that NetScaler driver in OpenStack can connect to NetScaler ADM during LB configurations.

After OpenStack and NetScaler ADM are registered with each other, both can talk to each other. Also, OpenStack users can use their existing credentials in OpenStack to log on to the NetScaler ADM user interface to check how their LB configurations are performing in NetScalers.

Tenants in OpenStack

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Placement policies

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Alternatively, the NetScaler ADM also provides an option to assign a NetScaler instance based on OpenStack tenants.

Service packages

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
- Multiple tenants can be associated with the same service package.
- In a service package that is set for auto-provisioning, virtual NetScaler instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

Features Supported on LBaaS V1 and LBaaS V2

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
  - Load Balancing
- LBaaS V2
  - Load Balancing
  - SSL Offload with certificates managed by **Barbican**, the Key Manager in OpenStack
  - Certificate Bundles (includes intermediary Certification Authorities)
  - SNI support

This document provides information about:

- Use Case Scenario
- NetScaler ADM Integration with OpenStack Workflow
- Prerequisites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pre-configuration Tasks in NetScaler ADM and OpenStack
- Configuration Steps for LBaaS V1 using Horizon
- Configuration Steps for LBaaS V2 using Command Line
- Manual Provisioning of NetScaler VPX Instance on OpenStack
- Integrating NetScaler ADM with OpenStack Heat Services
- Monitoring OpenStack Applications in NetScaler ADM

Use Case Scenario

The following use-case scenario explains the workflow of integrating NetScaler ADM with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider's cloud infrastructure. Tom's organization, Example-SportsOnline.com, requires two servers S1 and S1, and Tom also requires a dedicated NetScaler device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and NetScaler ADM, and prepare them to compatible with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.

Steve has to register OpenStack details with NetScaler ADM, and configure the NetScaler LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, NetScaler ADM displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the NetScaler LBaaS features and configure Tom to get a dedicated NetScaler allotted for his load balancer configurations in NetScaler ADM.

For this, Steve can either provision a NetScaler VPX instance on the computing layer (Nova) of OpenStack using NetScaler ADM user interface or enable MAS to auto-provision a NetScaler VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, NetScaler ADM manages the VPX instance. For achieving this, Steve creates a service package in NetScaler ADM, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the 'dedicated' isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many NetScaler VPX instances to the service package, and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

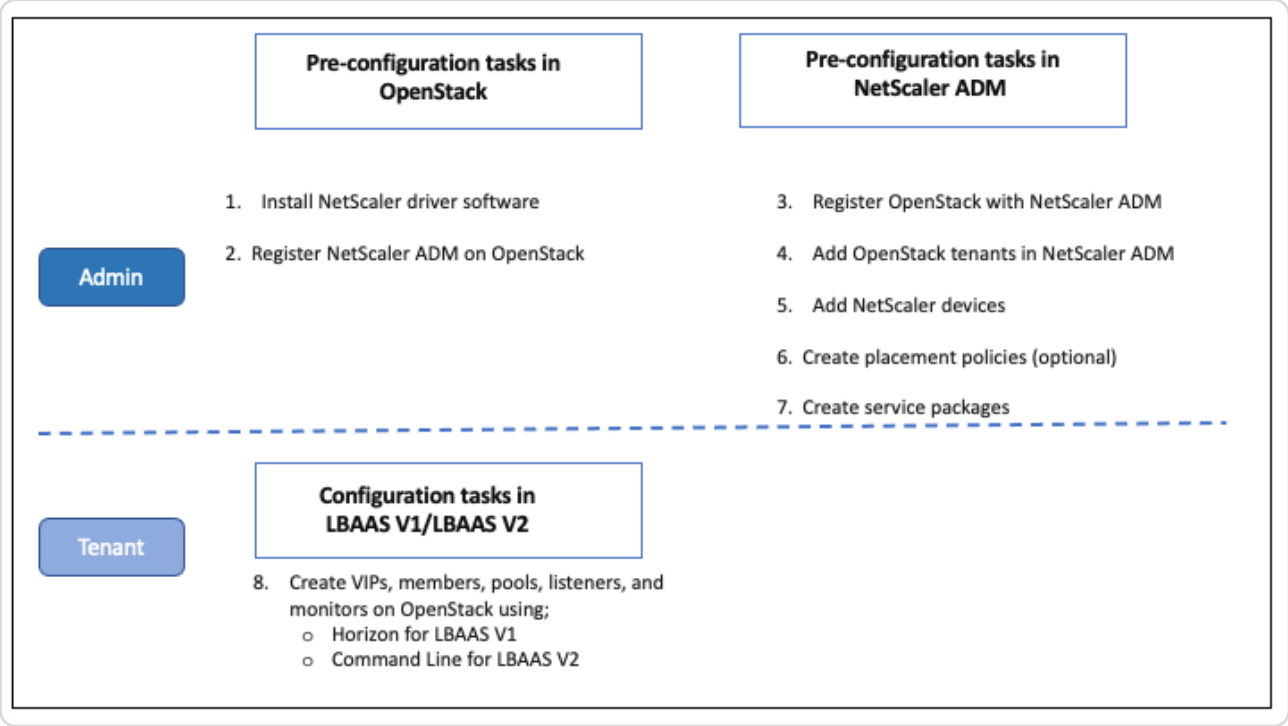
associates Example-SportsOnline, along with other tenants, who require a dedicated NetScaler with the service package. As a result, when Tom performs his first load balancer configuration, NetScaler ADM allots one of the NetScaler VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that NetScaler.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and virtual servers on the NetScaler instance. Tom can also create health monitors to monitor the servers, and send application traffic to only those servers which are UP at any point of time and reachable from NetScaler.

The load balancing configuration created in OpenStack is now implemented on the NetScaler instance. Once fully configured, the NetScaler VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

NetScaler ADM Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.



OpenStack: Integrating NetScaler instances

The Cloud Orchestration feature of NetScaler Application Delivery Management (ADM) enables integration of NetScaler products with OpenStack platform. By using this feature with OpenStack

© 1997–2026 Citrix Systems, Inc. All rights reserved.

platform, the OpenStack users are able to avail the load balancing feature (LBaaS) of the NetScaler. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in NetScaler instance.

The following sections provide a brief description of the features in NetScaler® ADM and OpenStack integration workflow.

NetScaler Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plug-in includes a NetScaler driver that enables OpenStack to communicate with the NetScaler ADM. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the NetScaler ADM, which creates the load balancer configuration on the desired NetScaler instances. OpenStack also uses the driver to call NetScaler ADM at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the NetScalers. NetScaler driver software for OpenStack platform is bundled along with the NetScaler ADM. To download and install the drivers, you have to first install NetScaler ADM and launch the application.

Registering NetScaler ADM and OpenStack with each other

You have to first register OpenStack information on the NetScaler ADM. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack NetScaler driver user credentials. You can later specify the same login credentials in the NetScaler_driver section of the Neutron configuration file (neutron.conf) so that NetScaler driver in OpenStack can connect to NetScaler ADM during LB configurations.

After OpenStack and NetScaler ADM are registered with each other, both can talk to each other. Also, OpenStack users can use their existing credentials in OpenStack to log on to the NetScaler ADM user interface to check how their LB configurations are performing in NetScalers.

Tenants in OpenStack

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

Placement policies

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Alternatively, the NetScaler ADM also provides an option to assign a NetScaler instance based on OpenStack tenants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service packages

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
- Multiple tenants can be associated with the same service package.
- In a service package that is set for auto-provisioning, virtual NetScaler instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

Features Supported on LBaaS V1 and LBaaS V2

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
  - Load Balancing
- LBaaS V2
  - Load Balancing
  - SSL Offload with certificates managed by **Barbican**, the Key Manager in OpenStack
  - Certificate Bundles (includes intermediary Certification Authorities)
  - SNI support

This document provides information about:

- Use Case Scenario
- NetScaler ADM Integration with OpenStack Workflow
- Prerequisites
- Pre-configuration Tasks in NetScaler ADM and OpenStack
- Configuration Steps for LBaaS V1 using Horizon
- Configuration Steps for LBaaS V2 using Command Line
- Manual Provisioning of NetScaler VPX Instance on OpenStack

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Integrating NetScaler ADM with OpenStack Heat Services
- Monitoring OpenStack Applications in NetScaler ADM

Use Case Scenario

The following use-case scenario explains the workflow of integrating NetScaler ADM with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider's cloud infrastructure. Tom's organization, Example-SportsOnline.com, requires two servers S1 and S1, and Tom also requires a dedicated NetScaler device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and NetScaler ADM, and prepare them to compatible with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.

Steve has to register OpenStack details with NetScaler ADM, and configure the NetScaler LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, NetScaler ADM displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the NetScaler LBaaS features and configure Tom to get a dedicated NetScaler allotted for his load balancer configurations in NetScaler ADM.

For this, Steve can either provision a NetScaler VPX instance on the computing layer (Nova) of OpenStack using NetScaler ADM user interface or enable MAS to auto-provision a NetScaler VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, NetScaler ADM manages the VPX instance. For achieving this, Steve creates a service package in NetScaler ADM, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the 'dedicated' isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many NetScaler VPX instances to the service package, and associates Example-SportsOnline, along with other tenants, who require a dedicated NetScaler with the service package. As a result, when Tom performs his first load balancer configuration, NetScaler ADM allots one of the NetScaler VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that NetScaler.

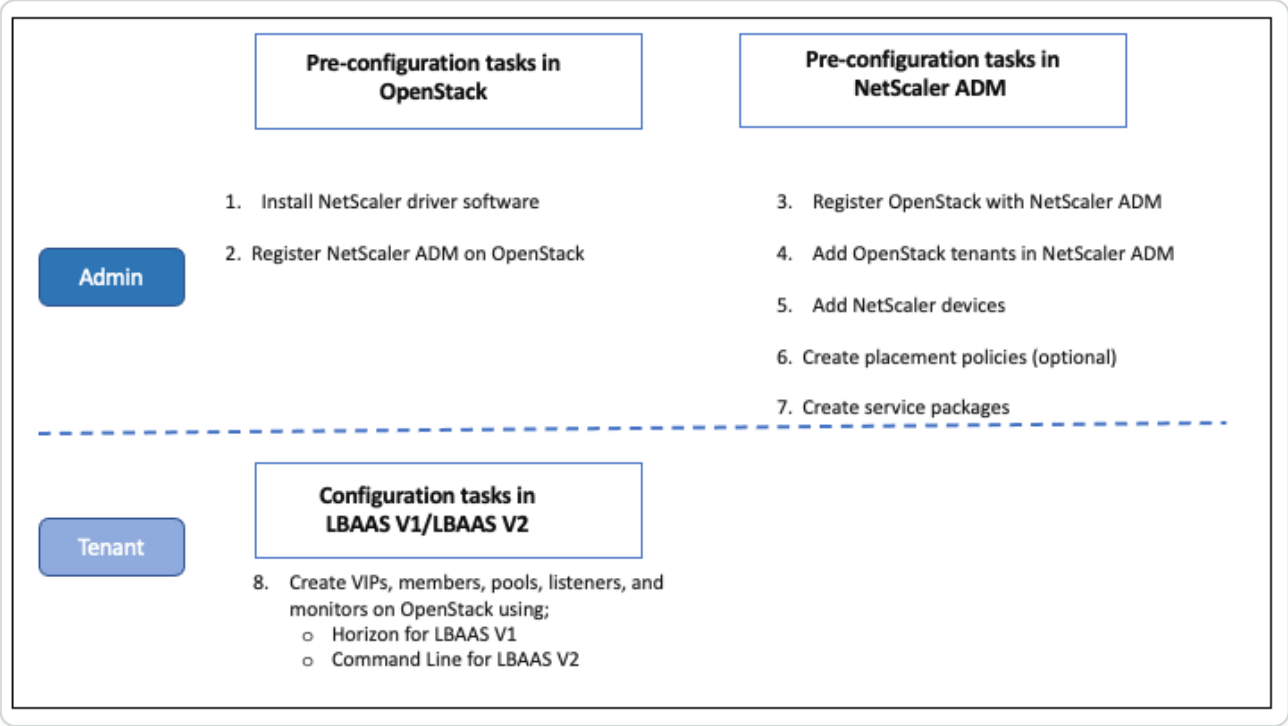
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and virtual servers on the NetScaler instance. Tom can also create health monitors to monitor the servers, and send application traffic to only those servers which are UP at any point of time and reachable from NetScaler.

The load balancing configuration created in OpenStack is now implemented on the NetScaler instance. Once fully configured, the NetScaler VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

NetScaler ADM Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.



Prerequisites

Before you integrate the NetScaler virtual instance with OpenStack platform, ensure that the following requirements are met:

NetScaler® ADM and OpenStack Software Requirements

- NetScaler ADM 13.1 is installed on a supported hypervisor workstation that meets the minimum hardware requirements system.
- OpenStack components are installed and running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADM 13.1 supports the following OpenStack versions - **Newton**, **Ocata**, **Pike**, and **Queens**.

NetScaler ADM Hardware Requirements

Ensure the following virtual computing resources are on your OpenStack server to install NetScaler virtual instances:

COMPONENT	REQUIREMENT
RAM	8 GB
Virtual CPU	8
Storage Space	500 GB
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps

NOTE

The memory and hard disk requirements specified are for deploying NetScaler ADM on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depend on the number of virtual machines running on it.

Pre-configuration tasks in NetScaler® ADM and OpenStack

This section assists you to perform the pre-configuration tasks before you configure NetScaler Application Delivery Management (ADM) and OpenStack.

Installing NetScaler ADM

Install NetScaler ADM on a supported hypervisor. For more information on how to download and install NetScaler ADM, see Deploying NetScaler ADM.

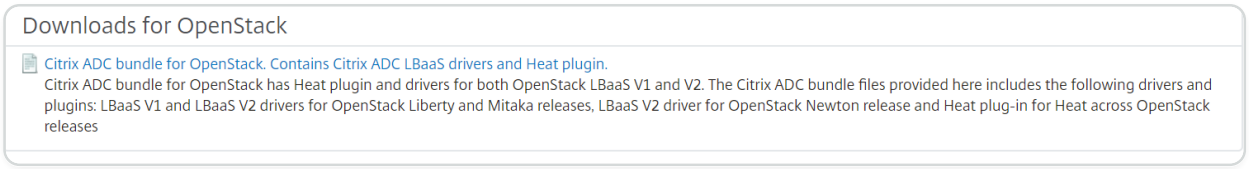
Installing the NetScaler driver software and registering NetScaler ADM on OpenStack

Download the NetScaler bundle for OpenStack from the NetScaler ADM Downloads page.

To install NetScaler driver on OpenStack platform using NetScaler ADM GUI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler ADM, click **Downloads**. The **Downloads** page in NetScaler ADM provides you links to download **NetScaler bundle for OpenStack** software required for **Newton**, **Ocata**, and **Pike** OpenStack versions.
2. Download the latest NetScaler 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 NetScaler driver tar file: `tar -xvzf <name_of_tar_file>`
4. If you have an OpenStack \<Release Name\> setup, at the prompt, type the following command:

   `cd <Release Name>`

   Example:

   `cd Newton`

5. Run the following command to install the driver and specify the NetScaler ADM IP address, the NetScaler driver password that you configured when you registered OpenStack with NetScaler ADM, and the protocol:

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   Example for single node OpenStack setup:

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas`

   Example for multinode OpenStack setup:

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler ADM is registered successfully on OpenStack, you can log on to NetScaler ADM using your OpenStack user credentials also.
After NetScaler ADM is registered successfully on OpenStack, restart the OpenStack Neutron services.

Registering OpenStack with NetScaler ADM

To register OpenStack with NetScaler ADM using NetScaler ADM GUI:

1. In NetScaler 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 NetScaler ADM. You have two options here - Default and Customized.

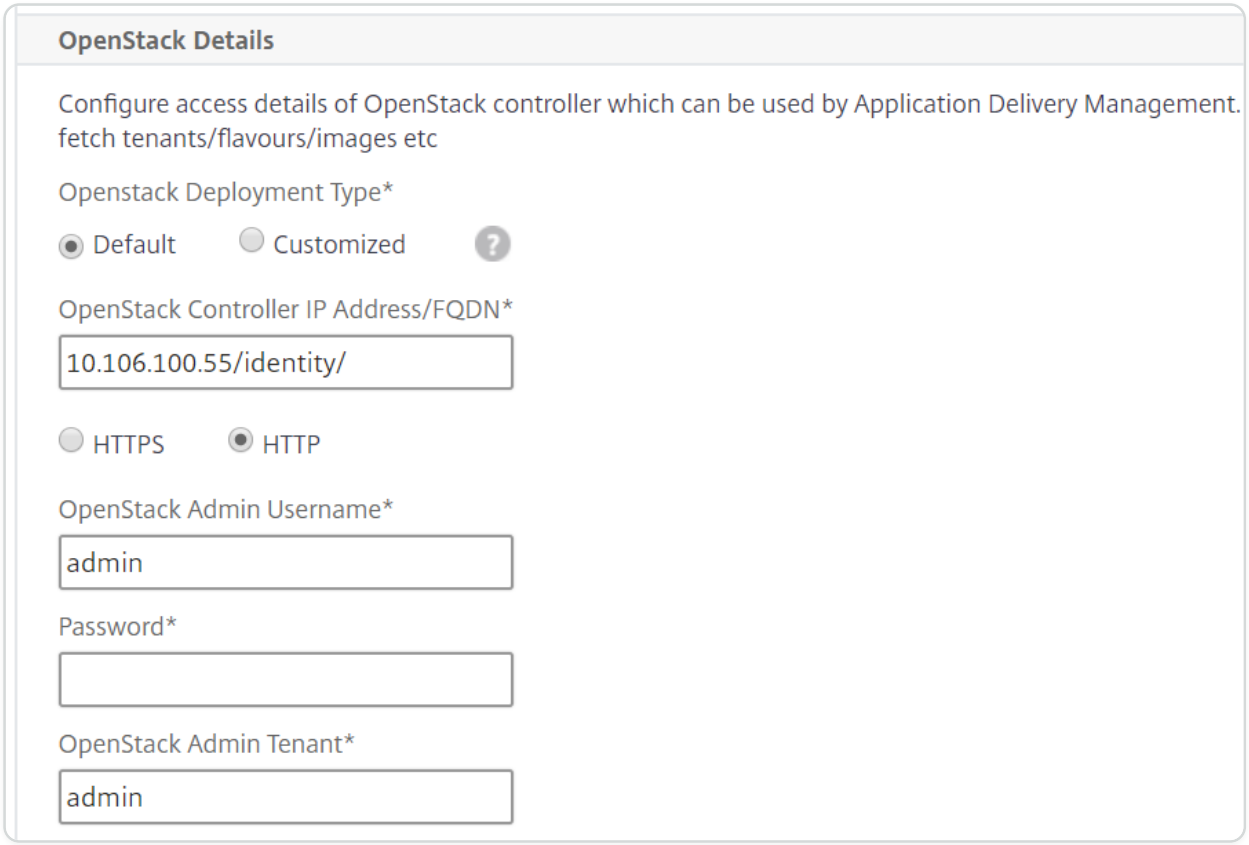
   For Newton and **Ocata** releases of OpenStack, you can use either default or customized deployment type. But for Pike release, you must use customized deployment type to register OpenStack with NetScaler ADM.

- **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 user name - administrative user name 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



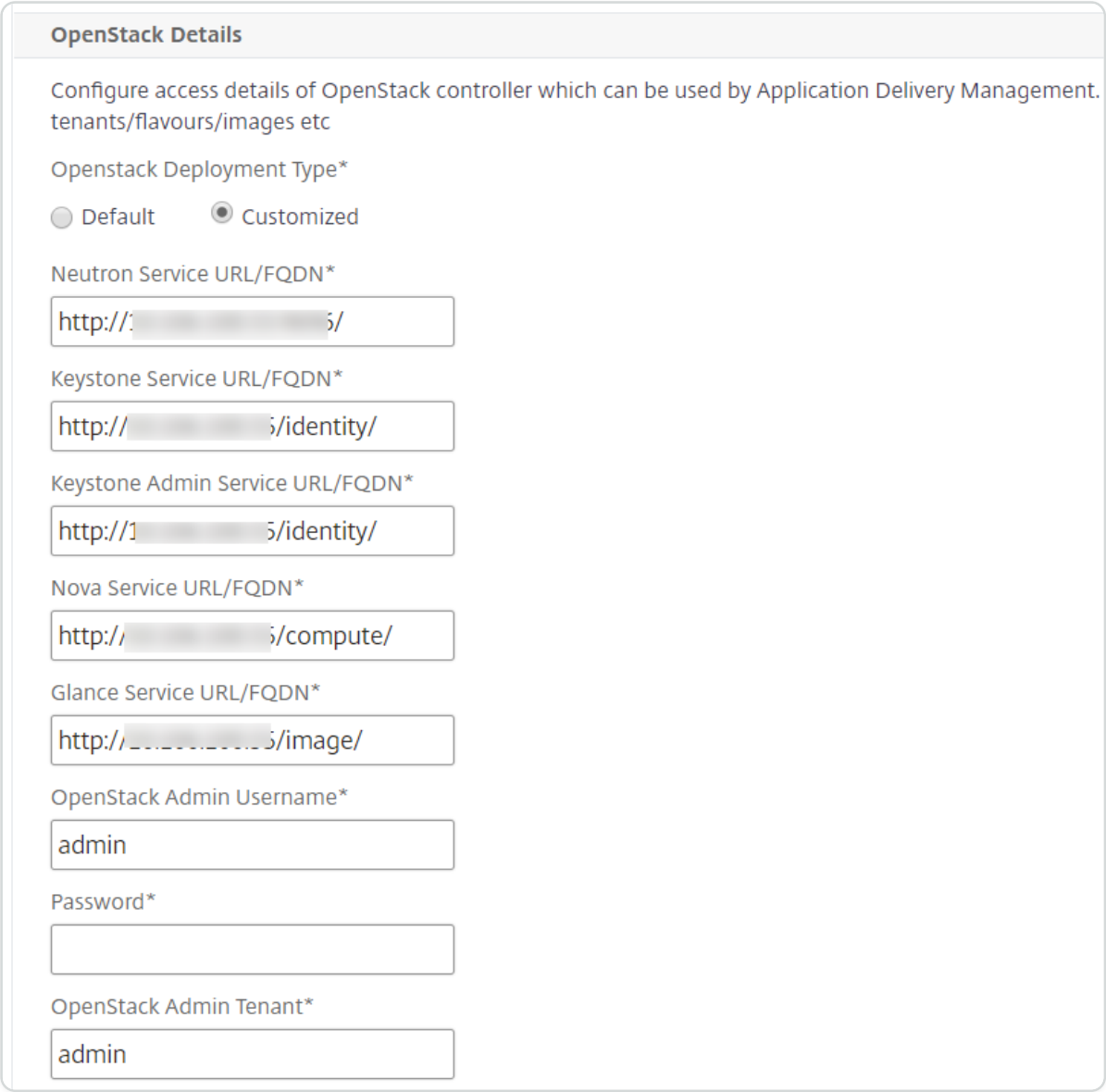
- **Customized Deployment Type**

  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 NetScaler ADM is different from registering OpenStack Pike release.

  Newton and Ocata Release of OpenStack:

  a. Specify the port numbers for the various OpenStack services if you are registering Newton release of OpenStack.
  b. Specify the OpenStack Admin user name, password, and OpenStack Admin Tenant user name as you had specified earlier in the **Default** settings.

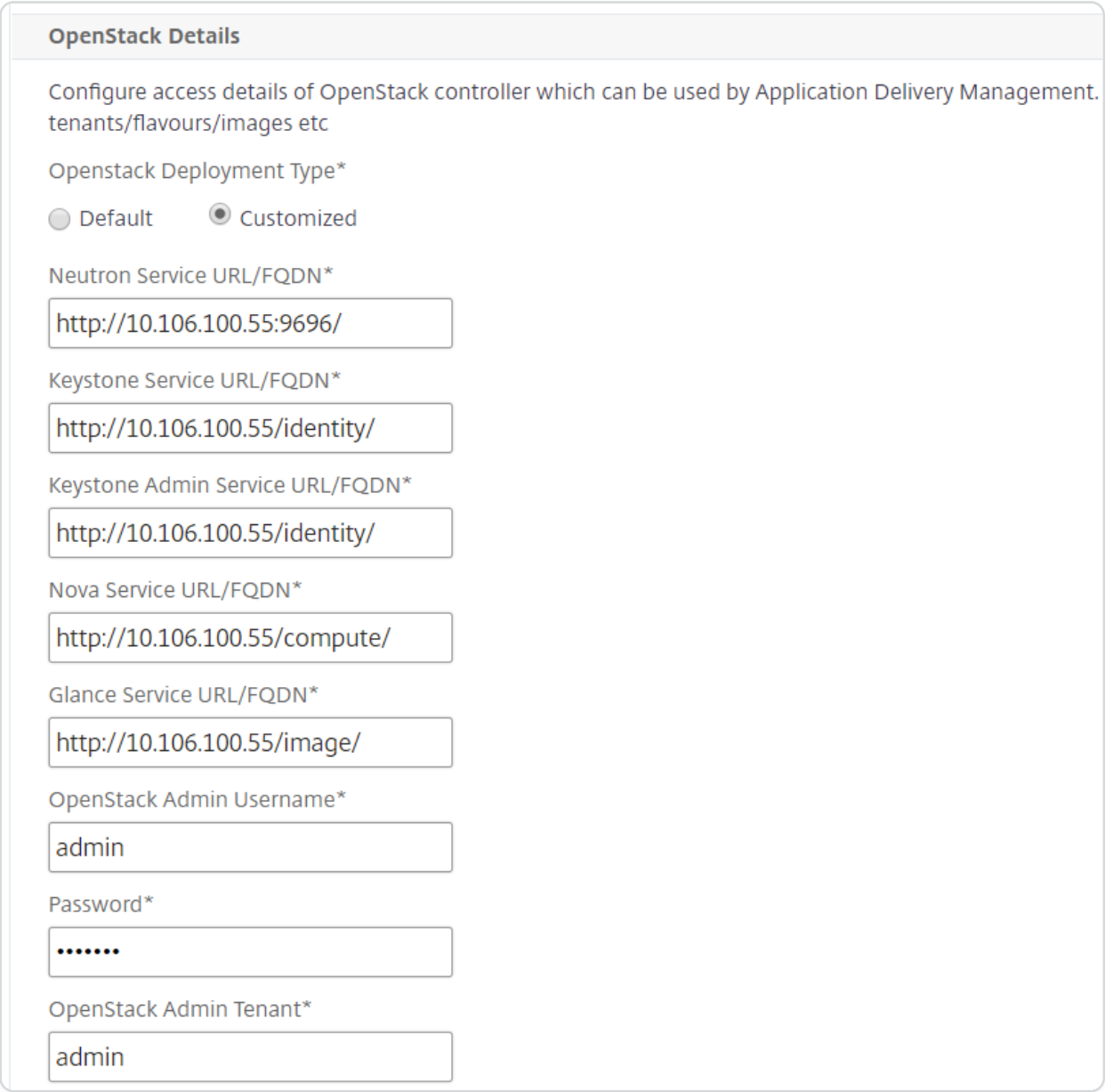
© 1997–2026 Citrix Systems, Inc. All rights reserved.



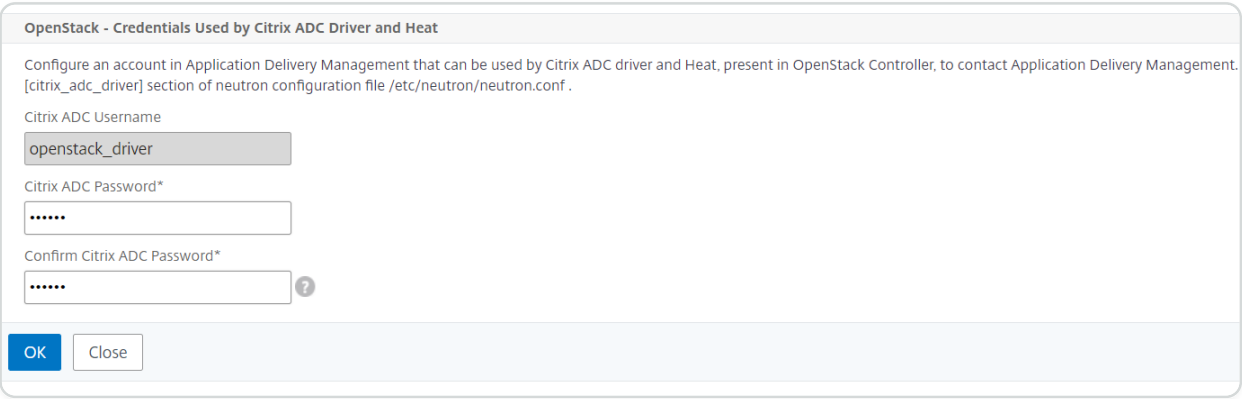
Pike Release of OpenStack:

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 user name, password, and OpenStack Admin Tenant user name as in Default settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. In **OpenStack Neutron LBaaS - Credentials Used by NetScaler Driver** section, set the NetScaler Driver Password for the OpenStack NetScaler driver user account. NetScaler ADM authenticates the calls from the OpenStack NetScaler driver by using these credentials. You must specify the same password when you run the NetScaler driver installation script in the OpenStack controller.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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/>`.

Adding OpenStack tenants

1. In NetScaler 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 NetScaler Devices
- Auto-provision the NetScaler VPX devices on OpenStack

Provisioning NetScaler 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 NetScaler Devices
- Auto-provision the NetScaler VPX devices on OpenStack

Pre-provisioning NetScaler devices

Install the NetScaler device on any of the hypervisor platforms such as Citrix Hypervisor, KVM, or ESX, and add the instance to NetScaler ADM. NetScaler ADM then manages this device that load balances the traffic in the servers.

To add an existing NetScaler VPX instance in NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure** \> **Instances** \> **NetScaler VPX**, and then click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Add NetScaler VPX** page, specify the IP address of the NetScaler VPX instance and select an instance profile from the **Profile Name** list. The instance profile contains the credentials used to logon to the NetScaler VPX. You can also create a new instance profile by clicking the + icon. Click **OK**.

Autoprovisioning NetScaler devices

Download the required NetScaler instance image from the NetScaler download page, and upload it on Glance, the OpenStack Imaging service. Having an image available on Glance allows you to configure a NetScaler instance on-demand when assigning the instance to the tenant.

To auto-provision the NetScaler VPX devices on OpenStack:

1. In NetScaler 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 NetScaler VPX is connected.

   b. Profile Name - select the profile from the drop-down list. The NetScaler ADM uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.

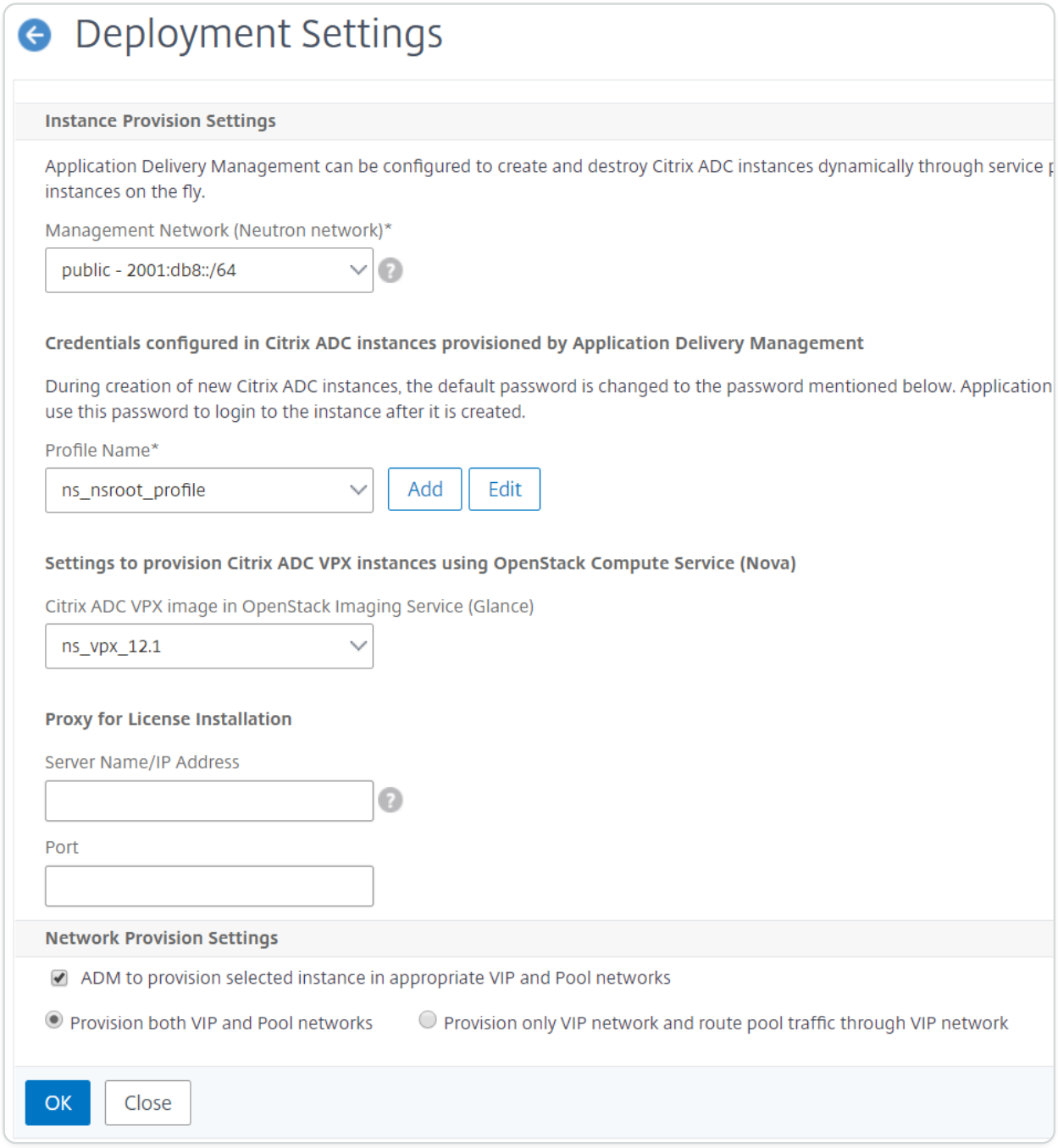
   c. Licenses - provide the NetScaler ADM license access codes used to license new auto-provisioned NetScaler instances. NetScaler ADM provisions NetScaler instances on OpenStack compute in management network, then triggers license installation on them using the specified license code. The NetScaler instance then downloads the license files from Citrix website using the license access code specified here.

   d. NetScaler VPX Image in Glance - select the NetScaler VPX image available in the OpenStack Glance that is used to create a NetScaler VPX instance.

   e. Proxy Settings - provide details of NetScaler proxy server for installing licenses. This may be required when NetScaler does not have direct access to the Internet through the management network.

4. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Creating a service package in NetScaler ADM

To create service packages for a tenant in NetScaler ADM:

1. In NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. NetScaler Instance Allocation - the type of instance allocation defined in the service package based which NetScaler instance resources are allocated to a tenant. Select **Dedicated**. For more information on policies, see Service Package Isolation Policies.

c. NetScaler Instance Provisioning - select **Existing Instance** to allocate an existing NetScaler instance to a tenant. If you want to create NetScaler instances during the configuration itself, select **Create Instance OnDemand**.

d. NetScaler Instance Type - select **NetScaler VPX**.

> **NOTE**
>
> Select NetScaler VPX to allocate pre-provisioned NetScaler instances hosted on SDX platform.

3. Click **Continue** to associate a tenant with a service package.

> **NOTE**
>
> Enable **Provision pair of NetScaler instances for high availability**, if you are deploying the NetScaler instances in high availability mode.

4. In **Assign Instances** section, click **Add**, and then select the NetScaler 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 NetScaler ADM assigns NetScaler instances based on tenants. If the tenant is not part of any service package, the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create placement policies for a tenant in NetScaler ADM:

1. In NetScaler 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 NetScaler instances to back-end servers through client network

By default, in the OpenStack orchestration workflow, NetScaler 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 NetScaler 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.

NetScaler ADM then configures the NetScaler 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 NetScaler VPX devices deployed on NetScaler SDX platform

Add the NetScaler SDX platform in NetScaler ADM, so that NetScaler ADM provisions the instances on this platform on-demand.

To auto-provison NetScaler instances deployed on NetScaler SDX platform:

1. In NetScaler ADM GUI, navigate to **Infrastructure > Instances** \> **NetScaler SDX**, and click **Add** to add a NetScaler SDX platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler SDX is connected.
   a. In **Profile Name**, select the profile from the drop-down list. The NetScaler ADM uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.
   b. Click **OK**.
4. To provision the NetScaler 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 **NetScaler Instance Allocation** field, select **Dedicated**.
   d. In **NetScaler Instance Provisioning** field, select **Create Instance OnDemand**, and in **Auto Provision Platform** field, select **NetScaler SDX**.
   e. By default, only NetScaler VPX instances are provisioned on NetScaler SDX platform.
   f. Click **Continue**.
   g. In **Auto Provision Settings** section, set the **Resources** properties.
      i. **Throughput** field. Enter 1000 Mbps.
      ii. **NetScaler Version** field. From the list, select the right version of the NetScaler VPX image present on the NetScaler SDX platform.
   h. In **NetScaler 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 run the configuration tasks. For more information on how to run configuration commands, see Configuring LBaaS V2 using Command Line.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure LBaaS V1 using Horizon

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 NetScaler, and NetScaler 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

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 run 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.

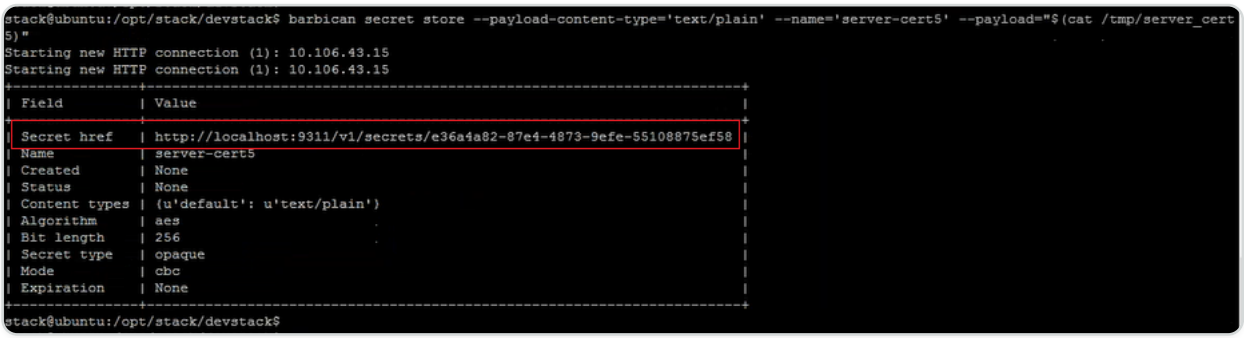
1. Upload certificate to **Barbican** service using the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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"
```



```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-cert5' --payload="$(cat /tmp/server_cert
5)"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
+---------------+-----------------------------------------------------------------------+
| Field         | Value                                                                 |
+---------------+-----------------------------------------------------------------------+
| Secret href   | http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 |
| Name          | server-cert5                                                          |
| Created       | None                                                                  |
| Status        | None                                                                  |
| Content types | {u'default': u'text/plain'}                                           |
| Algorithm     | aes                                                                   |
| Bit length    | 256                                                                   |
| Secret type   | opaque                                                                |
| Mode          | cbc                                                                   |
| Expiration    | None                                                                  |
+---------------+-----------------------------------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

2. Upload key to **Barbican** service using the following command:

```
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"
```

```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-key5' --payload="$(cat /tmp/server_key5)
"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
+---------------+-----------------------------------------------------------------------+
| Field         | Value                                                                 |
+---------------+-----------------------------------------------------------------------+
| Secret href   | http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0 |
| Name          | server-key5                                                           |
| Created       | None                                                                  |
| Status        | None                                                                  |
| Content types | {u'default': u'text/plain'}                                           |
| Algorithm     | aes                                                                   |
| Bit length    | 256                                                                   |
| Secret type   | opaque                                                                |
| Mode          | cbc                                                                   |
| Expiration    | None                                                                  |
+---------------+-----------------------------------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you run 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.

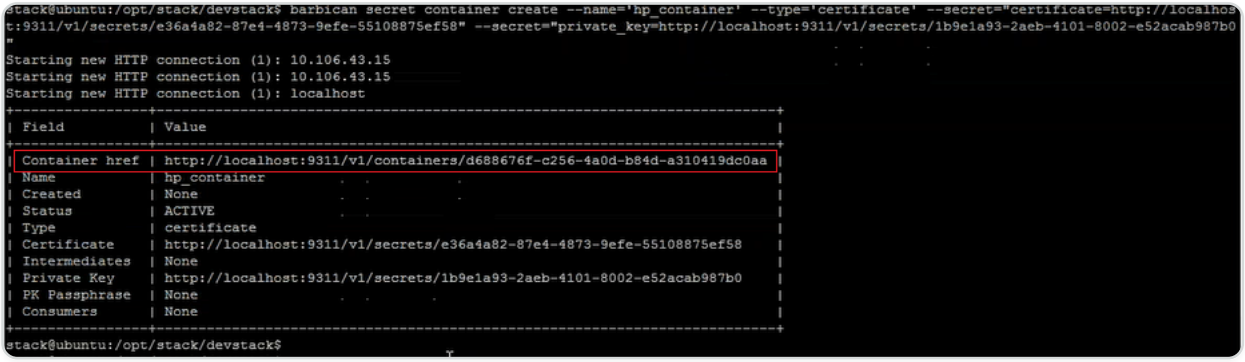
3. Create a container in **Barbican** service to store the certificate and the key using the following command:

   In the command, replace <certificate_url> with the url that you obtained from the Secret href field when you uploaded the certificate. Similarly, replace <key_url> with the url that you obtained from the Secret href field when you uploaded the key.

```
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="`certificate=http://localhost:9311/v1/
secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --
secret="private_key=http://localhost:9311/v1/secrets/
1b9e1a93-2aeb-4101-8002-e52acab987b0`"
```



   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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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/`"

```
stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

The status changes from PENDING_CREATE to ACTIVE after the load balancer is successfully created.

```
+--------------------------------------+------------+--------------+---------------------+------------+
| id                                   | name       | vip_address  | provisioning_status | provider   |
+--------------------------------------+------------+--------------+---------------------+------------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25    | ACTIVE              | netscaler  |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19    | ACTIVE              | netscaler  |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24    | ACTIVE              | netscaler  |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27    | ACTIVE              | netscaler  |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18    | ACTIVE              | netscaler  |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23    | ACTIVE              | netscaler  |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20    | ERROR               | netscaler  |
+--------------------------------------+------------+--------------+---------------------+------------+
```

6. Create a listener using the following command:

```
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, run the following command without providing locations to the container:

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name
<listener-name> --protocol <protocol_type> --protocol-port <port_number>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --prot
ocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
Created a new listener:
+-------------------------+-------------------------------------------------------------------------------+
| Field                   | Value                                                                         |
+-------------------------+-------------------------------------------------------------------------------+
| admin_state_up          | True                                                                          |
| connection_limit        | -1                                                                            |
| default_pool_id         |                                                                               |
| default_tls_container_id | http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| description             |                                                                               |
| id                      | 734a0361-153d-4983-bc2c-55a3ec2ff6fb                                         |
| loadbalancers           | {"id": "746d730b-3b63-418f-a816-d8dd5472963c"}                                |
| name                    | hp-lb-test-list                                                               |
| protocol                | TERMINATED_HTTPS                                                              |
| protocol_port           | 443                                                                           |
| sni_container_ids       |                                                                               |
| tenant_id               | 0f30b93cd0cd4482b92d033e1628aa8f                                              |
+-------------------------+-------------------------------------------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

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
demolistener --protocol http --name demopool
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-pool-create --lb-algorithm ROUND_ROBIN --listener hp-lb-test-list --protocol HTTP --name hp-lb-test
-pool
Created a new pool:
+---------------------+--------------------------------------------+
| Field               | Value                                      |
+---------------------+--------------------------------------------+
| admin_state_up      | True                                       |
| description         |                                            |
| healthmonitor_id    |                                            |
| id                  | 714c44d0-5cf7-4ef8-b84d-f6d3a258c770       |
| lb_algorithm        | ROUND_ROBIN                                |
| listeners           | {"id": "734a0361-153d-4983-bc2c-55a3ec2ff6fb"} |
| members             |                                            |
| name                | hp-lb-test-pool                            |
| protocol            | HTTP                                       |
| session_persistence |                                            |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f           |
+---------------------+--------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 15.0.0.15                            |
| admin_state_up | True                                 |
| id             | ced7a563-5ecc-474f-8d2a-cb69923215b0 |
| protocol_port  | 80                                   |
| subnet_id      | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
| tenant_id      | 0f30b93cd0cd4482b92d033e1628aa8f     |
| weight         | 1                                    |
+----------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

Monitoring OpenStack Applications in NetScaler® ADM

Your tenants can log on to NetScaler Application Delivery Management (ADM) using their OpenStack credentials to monitor VIPs and pools created from OpenStack from any browser. The URL must be in the following format:

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

Where, `mas-ip-address`, is the NetScaler ADM IP address that is registered with the OpenStack.

NOTE

- OpenStack VIPs correspond to virtual servers in NetScaler ADM.
- OpenStack Pools correspond to service groups in NetScaler ADM.
- OpenStack Pool members correspond to service group members in NetScaler ADM.

Configure layer 7 content switching

NetScaler Application Delivery Management (ADM) orchestrates with OpenStack to configure the Layer 7 (L7) switching or content-based switching functionalities on NetScaler 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 NetScaler instance as the provider, NetScaler ADM allots a NetScaler instance, and deploys content switching and responder configurations corresponding to the L7 configurations. The NetScaler 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 running only those policies that are applicable to the content. Layer 7 load balancing also facilitates increased efficiency of the application infrastructure. The ability to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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` is 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` is 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 are essentially serve specific types of content. For example, one server can serve only images, another might run server-side scripting languages, such as PHP and ASP, and another can 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:

- Host name: The host name 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 host name, 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 webpages.

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 NetScaler Entities

OpenStack	NetScaler Entity	Description

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 policy with action REDIRECT_TO_POOL	Content switching policy > Content switching action	NetScaler 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.
L7 policy with action REDIRECT_TO_URL	Responder policy > Responder action	NetScaler 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.
L7 policy with action REJECT	Responder policy > Drop the request	NetScaler ADM creates a responder policy that is bound to the content switching virtual server and associated with a responder action that drops the request.

If the action of an L7 policy that evaluates to "true" redirects traffic to a pool that is in "create_pending" state, NetScaler ADM implements the specified pool along with a load balancing virtual server. NetScaler 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 second L7 policy redirects to the same pool, NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ran 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 re-ordered 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 NetScaler 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` processes at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in NetScaler, 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" or "redirect_to_url" policy is first evaluated, and then the "redirect_to_pool policy is evaluated. In a NetScaler 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 must not have identical expressions. The derived expressions are 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 polices so that all the responder policies to reject the request are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

arranged at the top of the evaluation list, followed by the responder policies for web direct, followed by the content switching policies.

In NetScaler 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` processes at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in NetScaler, 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" or "redirect_to_url" policy is first evaluated and then the "redirect_to_pool policy is evaluated. In NetScaler, 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 have similar expressions. Similar derived expressions are 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 polices 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

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action&lt;action-name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-url &lt;redirect-
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.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
value &lt;value-string> &lt;L7 policy name>



neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
&lt;value-string> &lt;L7 policy name>
```

The above two rules can be connected with an AND operator to derive the expression for the responder policy.

Create L7 Policy to Redirect Requests to a Pool

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-pool &lt;redirect-
pool>
```

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler VPX instance on OpenStack

In a few enterprise networks, NetScaler VPX instances cannot connect to NetScaler license Server to automatically download the licenses, for security reasons. In such a scenario, you need to manually deploy NetScaler VPX instances on OpenStack platform. Using the license access code received by you from Citrix, download the appropriate NetScaler VPX license and save it on your local system.

To Manually Provision NetScaler VPX Instance on OpenStack:

1. Install the NetScaler Driver Software and Register NetScaler Application Delivery Management (ADM) on OpenStack
   a. In NetScaler 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 NetScaler® 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 NetScaler VPX is connected.
   b. **Profile Name** - select the profile from the drop-down list. The NetScaler ADM uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.
   c. NetScaler VPX Image in Glance - select the NetScaler VPX image available in the OpenStack Glance that is used to create a NetScaler VPX instance. The drop-down list will display only those images that are present on OpenStack Glance.
3. In NetScaler ADM, navigate to **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Service Packages**, and then click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the **Service Package** page specify the following parameters:

   a. **Name** - name for the service package. For example, enter SVC-PKG-GOLD.

   b. **NetScaler Instance Allocation** - select **Dedicated** or **Partitioned** as the type of instance allocation defined in the service package.

   c. **NetScaler Instance Provisioning** - select **Create Instance OnDemand** to create NetScaler instances during the configuration itself.

   d. **Auto Provision Platform** - select **OpenStack Compute**. By default, NetScaler VPX will be selected as the instance type.

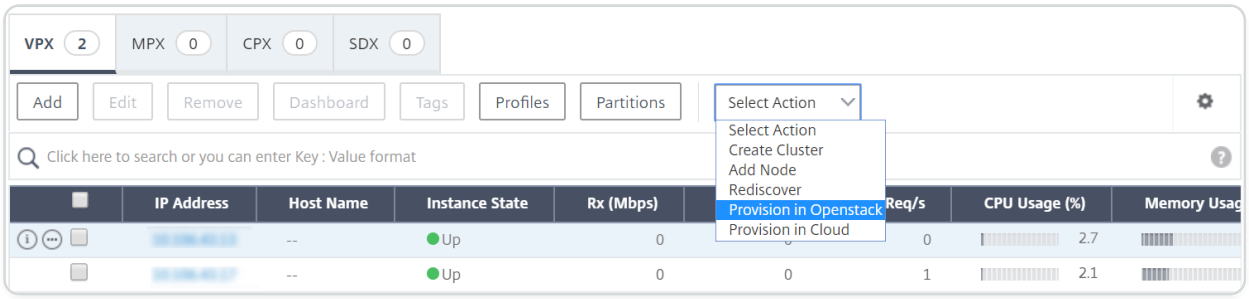
   e. **Assign OpenStack Tenants/Placement Policies** - section, under OpenStack Tenants, click **Add**, and select the tenant.

   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 **Infrastructure > Instances > NetScaler VPX**.

7. In **NetScaler 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**.

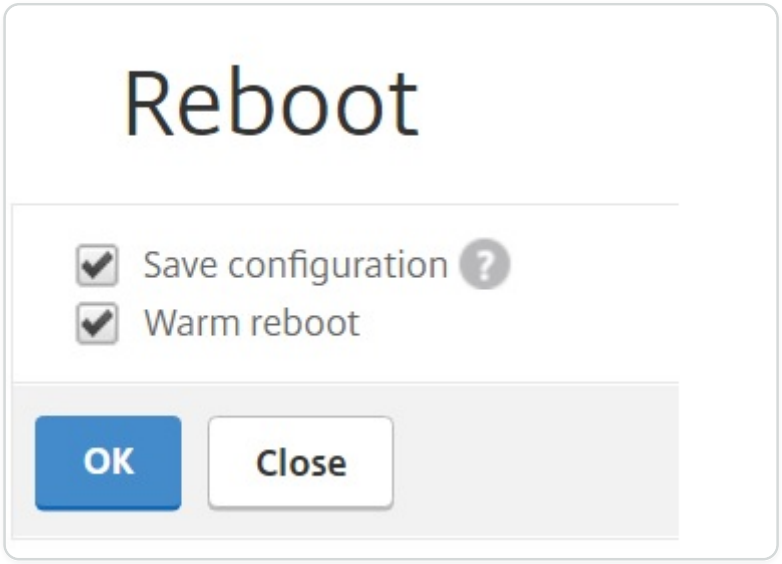
8. Navigate to **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Requests** tab. Select the request and click **Tasks** to view the tasks. When the status of the task changes to **Finished**, it means that the NetScaler VPX is provisioned in NetScaler ADM.

9. Navigate to **Infrastructure > Instances** \> **NetScaler VPX** to check that the NetScaler VPX instance appears in NetScaler VPX page.

10. Click the NetScaler VPX instance. When the NetScaler 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 NetScaler Licensing Overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Restart the NetScaler VPX instance.



12. After a few minutes, you can log on to OpenStack and in **System** \> **Instances**, you can see that the NetScaler VPX instance is deployed on OpenStack.
13. LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and run the configuration tasks. For more information on how to run configuration commands, see Configuring LBaaS V2 using Command Line.

Provisioning of NetScaler VPX instance on OpenStack using StyleBook

In the OpenStack orchestration workflow, NetScaler Application Delivery Management (ADM) now uses the `os-cs-lb-mon` StyleBook to deploy LBaaS configurations on NetScaler 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 an OpenStack workflow provides the following benefits:

- Better visualization by viewing all the configuration objects.
- Reliability through rollback.
- Support for various NetScaler instance types (NetScaler HA, partitions, VPX, CPX, MPX, and others.)
- Customization by using your own StyleBooks to deploy configuration for OpenStack tenants.

As NetScaler ADM admin, navigate to **Applications** > **Configurations** to view the configuration pack deployed on the NetScaler instance. You can perform the following tasks:

- Scroll to view the `os-cs-lb-mon` configuration pack deployed for the load balancer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 NetScaler objects or entities deployed on the instances.

Points to note before provisioning instances using StyleBooks

From NetScaler ADM 12.1 build 49.23 onwards, the architecture of an OpenStack orchestration workflow has been updated. The workflow now uses NetScaler ADM StyleBooks to configure NetScaler instances. If you are upgrading to NetScaler 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 fail until the migration script is run.

NOTE

- Once you run the migration script, you cannot downgrade to the previous build of NetScaler ADM.
- Ensure that you have upgraded the NetScaler drivers for OpenStack LBaaS V2 to the latest version. Use the NetScaler bundle files provided along with the latest NetScaler ADM 13.0 build.

LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and run the configuration tasks. For more information on how to run configuration commands, see Configuring LBaaS V2 using Command Line.

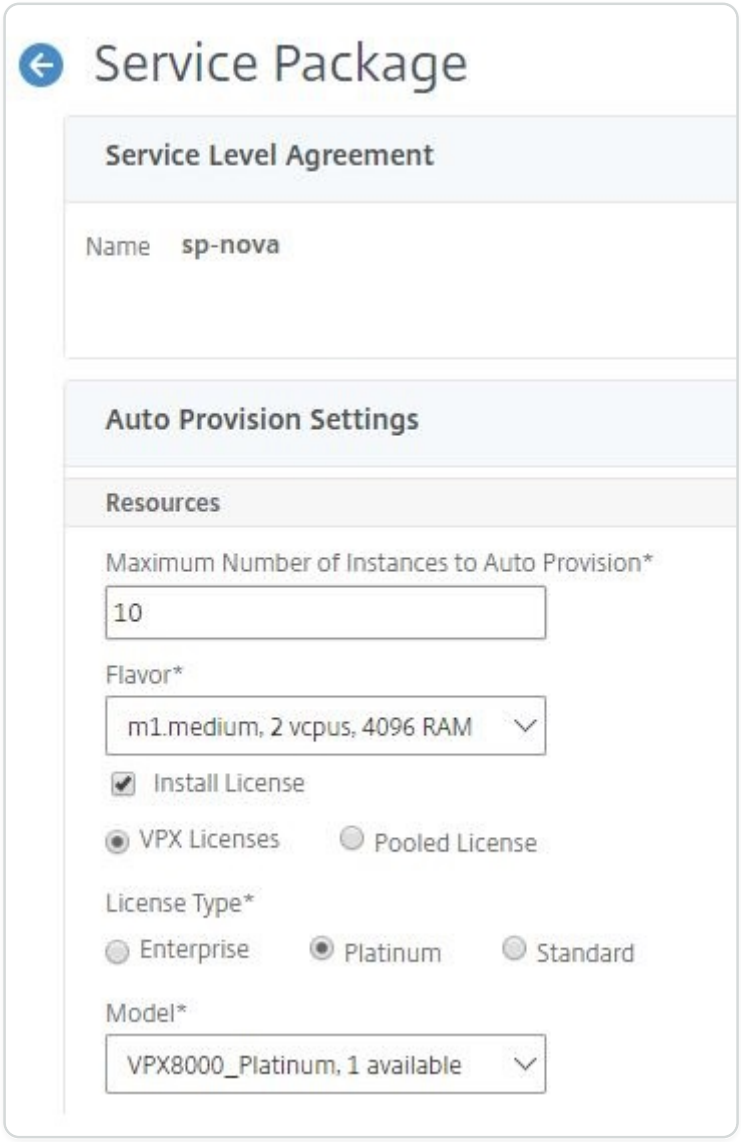
© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPX check-in and check-out license and pooled license support for OpenStack environment

In OpenStack orchestration workflow, NetScaler Application Delivery Management (ADM) creates NetScaler VPX instances on demand when you select service package with **OpenStack Compute**. Now, the service package page in the Orchestration feature in NetScaler ADM is enhanced to provide the license that is required to be installed on the NetScaler VPX instances that are created on demand. The licenses provided can be either VPX check-in and check-out license or pooled license.

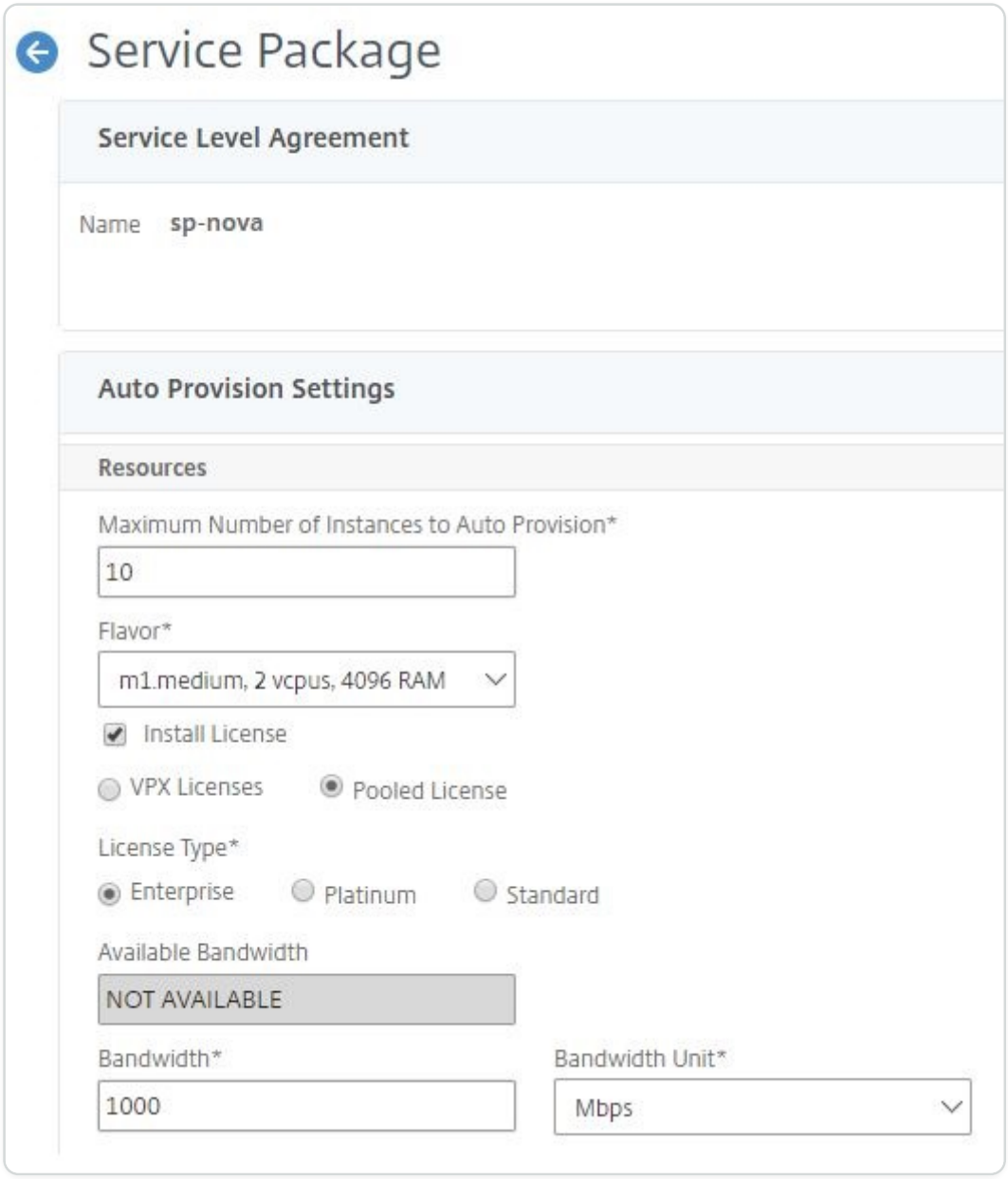
To use this feature, you must first upload the licenses in NetScaler® ADM and then create service packages that use OpenStack compute.

- If it is a check-in and check-out license, then you can choose the license to be installed from the various licenses available.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 NetScaler ADM as a provider, NetScaler ADM creates the NetScaler 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 NetScaler ADM. This allows for optimal use of licenses available in NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

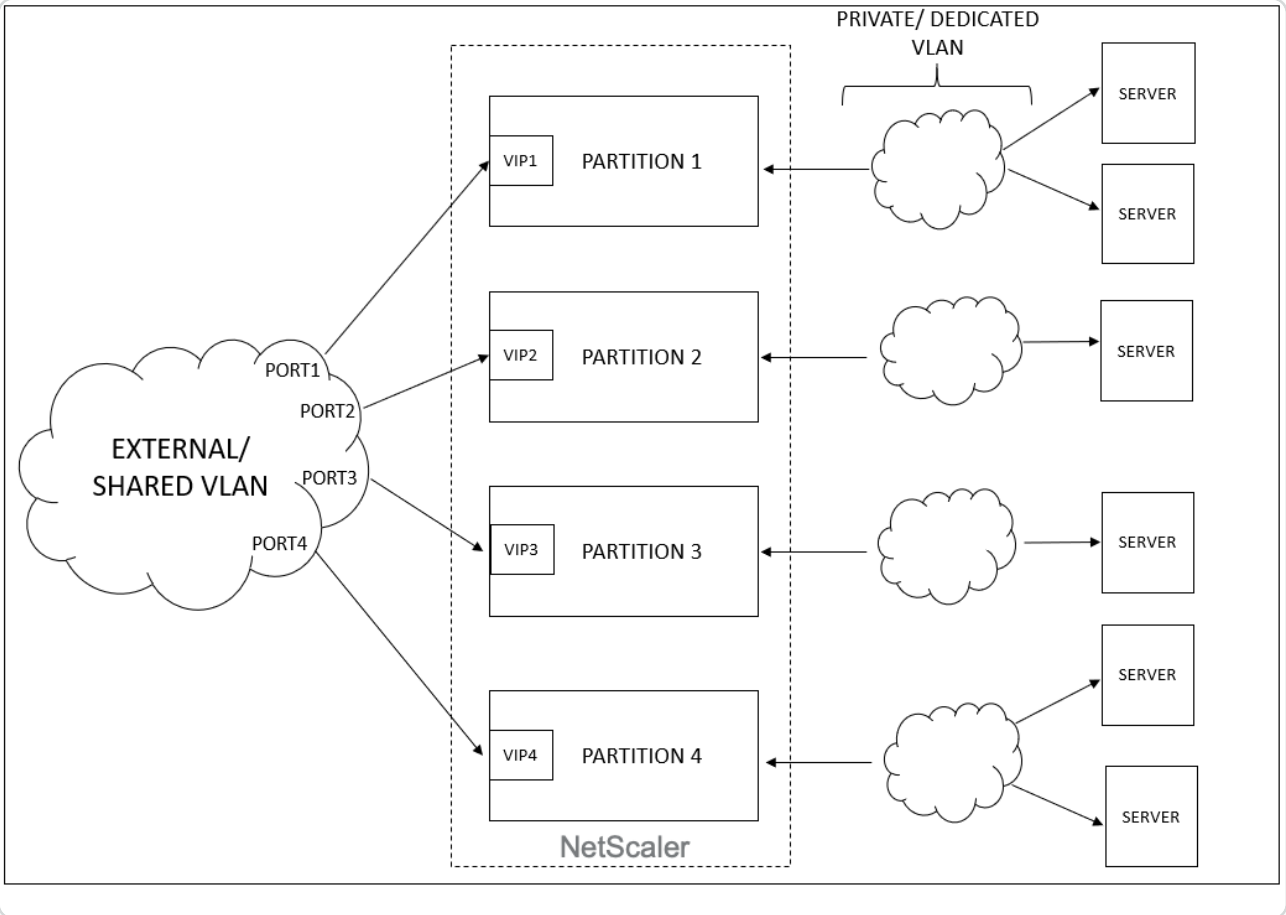
When NetScaler ADM is deployed in high availability mode, consider that the licenses are uploaded to the current active or the primary NetScaler ADM, MAS-HA-1. When you deploy the first request and NetScaler ADM creates the NetScaler VPX instances, the instance checks out the required licenses from MAS-HA-1. At later point in time, assume the secondary NetScaler ADM, MAS-HA-2, which does not have the licenses is active now. The NetScaler 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 NetScaler 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 NetScaler ADM high availability deployment, see High Availability.

Shared VLAN support for admin partitions

For tenants connecting from private networks, the NetScaler® 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



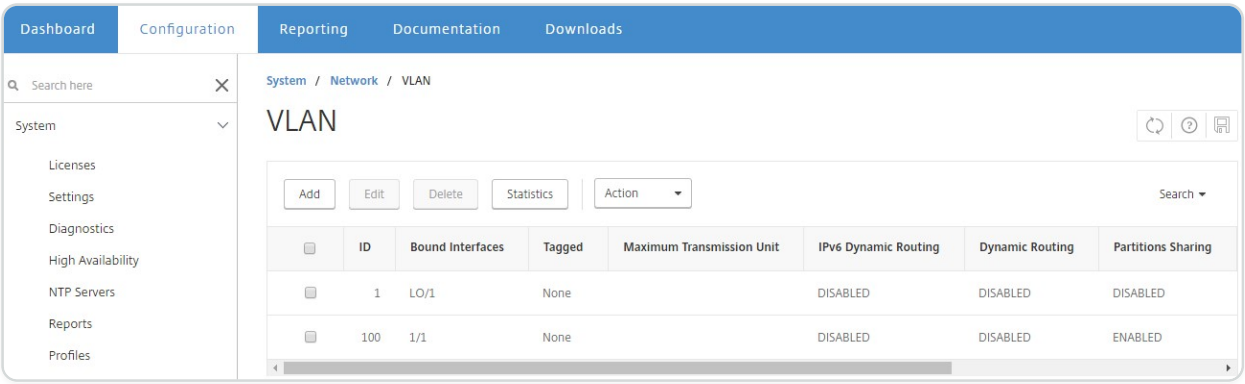
When an tenant configures a VIP or a listener, an admin partition is created in the NetScaler device for that tenant. All load balancer configuration is pushed to that admin partition that is created. If the tenant is using a shared network or an external network to create a load balancer, then the VLAN 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 NetScaler 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 NetScaler ADM supports virtual destination MAC address. When tenants share a VLAN, the NetScaler ADM assigns different MAC addresses to the partition on the NetScaler device. This allows a VLAN to be shared across partitions or across all tenants and all traffic domains.

Configuring Shared VLAN from NetScaler Instance

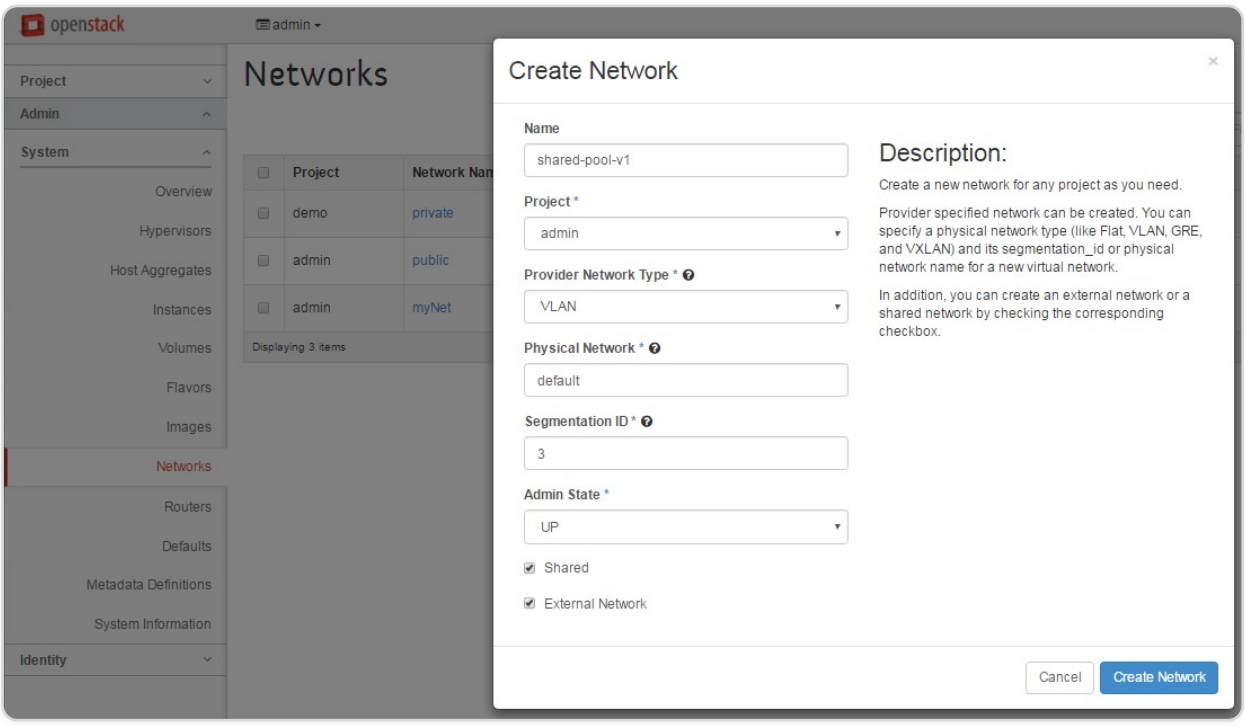
1. In a NetScaler instance, navigate to **Configuration** \> **System** \> **Network** \> **VLANs**, select a VLAN profile, and click **Edit** to set the partition sharing parameter.
2. On the **Configure VLAN** page, select the **Partitions Sharing** check box.
3. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 form 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**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Trial licensing workflow

During auto-provisioning of the NetScaler VPX instance using OpenStack orchestration, the NetScaler Application Delivery Management (ADM) uses OpenStack Compute to launch a NetScaler VPX instance. The newly provisioned NetScaler VPX instance contacts the Citrix licensing portal during the set up, and uses the license access code to automatically download and install the license files.

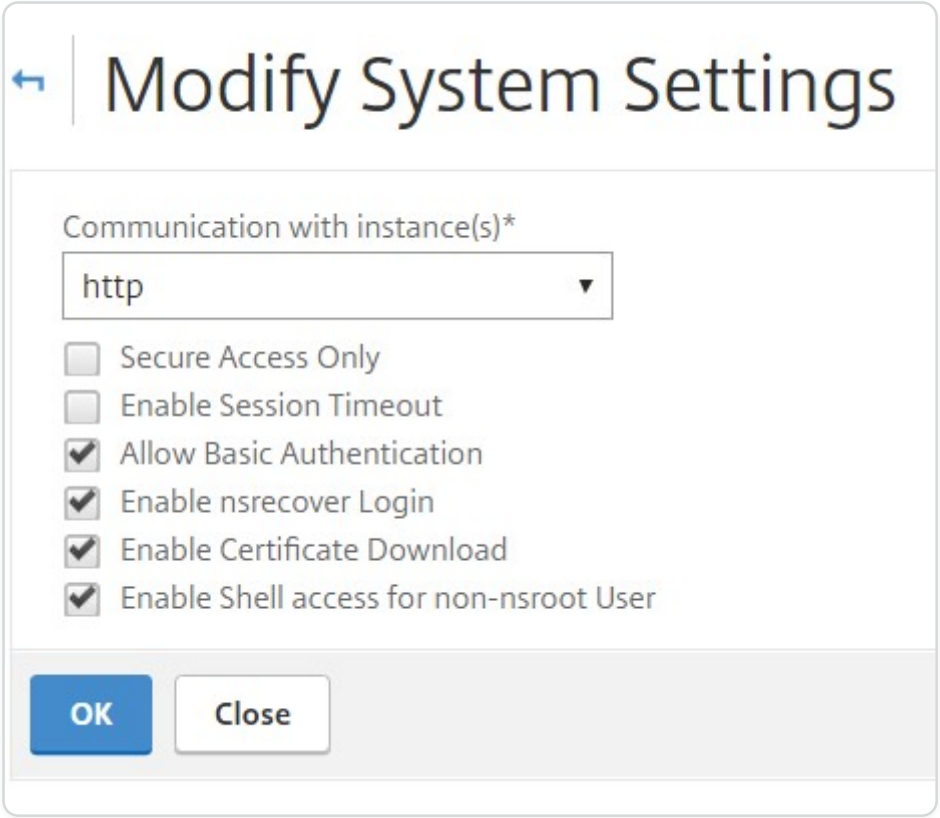
Trial Licenses

Technical support staff use trial licenses when they install NetScaler ADM and NetScaler VPX devices in field. A trial or evaluation license for NetScaler VPX is valid for 90 days. If there is a need to evaluate more than one NetScaler or extend the testing after 90 days, a new evaluation license needs to be requested. Instead of automatic installation of trial license files, NetScaler ADM provides you an alternate solution. You can manually download the license files and install them on NetScaler VPX to complete the installation of the instance.

If the NetScaler VPX is unable to connect to the internet, configure the NetScaler ADM to act as a proxy server for the Citrix Licensing Portal and install the license files.

NetScaler VPX instances that have a trial license can communicate with NetScaler ADM on HTTP only. To configure HTTP communication in NetScaler 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Integrate with OpenStack Heat services

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 REST 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 NetScaler features during the orchestration process. The NetScaler 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 NetScaler Heat plug-in allows you to configure advanced application delivery controller (ADC) functionalities on any NetScaler instance.

NetScaler StyleBooks

NetScaler Application Delivery Management (ADM) StyleBooks can be used to create and configure NetScaler functionalities. Just like Heat templates, the StyleBooks are also written in

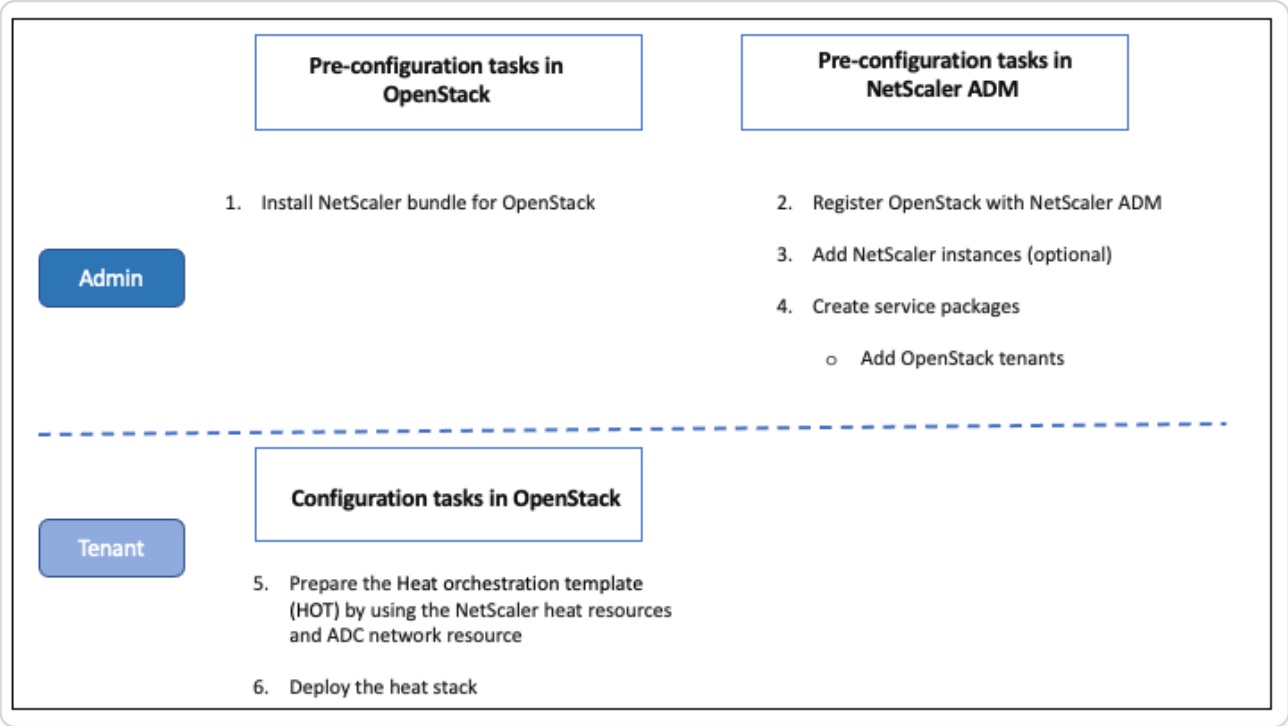
© 1997–2026 Citrix Systems, Inc. All rights reserved.

YAML. A separate StyleBooks can be created for each functionality, and a single StyleBooks can be used to deploy configurations on multiple NetScaler instances.

During NetScaler integration with OpenStack, NetScaler ADM publishes all NetScaler ADM StyleBooks as a resource in the Heat service. This includes both the StyleBooks that are shipped with NetScaler 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 NetScalers using these StyleBooks resources.

Workflow to Configure NetScaler Instances using Heat

The following flowchart illustrates the workflow for deploying the Heat stack:



Perform the following tasks as a cloud administrator:

To configure Heat services in OpenStack:

1. Download NetScaler bundles for OpenStack

   Install the NetScaler bundles in OpenStack. In NetScaler ADM, navigate to **Downloads** and download the NetScaler 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. When the communication is HTTP, the parameters are updated as follows:

NMAS_BASE_URI=< `http://10.146.103.45:80` >

NMAS_USERNAME=<openstack_driver_username>

NMAS_PASSWORD=<openstack_driver_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," NetScaler 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, NetScaler ADM sends this path in the verify parameter of request, otherwise NetScaler ADM sends verify=True.

NOTE

For deploying NetScaler 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 NetScaler Heat services in OpenStack, all the defined NetScaler ADM StyleBooks are imported into Heat as resources. Also, the NetScaler network resource and the certificate resource are imported into OpenStack as NetScaler Heat resources.

4. Register NetScaler® ADM with OpenStack.

a. In NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Select **Default** if the OpenStack services are running on default ports. Enter the following parameters:

   i. OpenStack Controller IP Address

   ii. Admin user name

   iii. Password

   iv. OpenStack Admin Tenant

   v. NetScaler 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 NetScaler 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 NetScaler ADM to import StyleBooks as Heat resources in OpenStack.

> **NOTE**
>
> For more information about creating service packages and other pre-configuration tasks in NetScaler ADM and OpenStack, see Integrating NetScaler ADM with OpenStack Platform.

6. Observe that all the relevant StyleBooks in NetScaler ADM are imported into OpenStack Heat as resources. Also, observe that the NetScaler network resource and NetScaler certificate resource are imported into OpenStack Heat as resources.

> **NOTE**
>
> Currently, you can use only the StyleBooks that are shipped with NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuration is pushed to NetScaler ADM, and the required NetScaler 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 NetScaler ADM to observe the lists of tasks. Also, navigate to **Applications** \> **Configuration** in NetScaler ADM to observe that the NetScaler instances are successfully configured in the form of StyleBooks configuration packs.

An Example of a NetScaler ADM StyleBooks:

The following image shows an example of how a NetScaler ADM StyleBooks is constructed and briefly explains the components. For more information about NetScaler ADM StyleBooks and how to use the shipped StyleBooks, see StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```yaml
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"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
     -
    name: name
    type: string
    required: true
    -
    name: ip
    type: ipaddress
    required: true
   -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
        name: $parameters.name
        servicetype: HTTP
        ipv46: $parameters.ip
        port: 80
        lbmethod: $parameters.lb-alg
```

header

StyleBooks imported

parameters

components

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 NetScaler network resources that are imported as Heat resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
    - allowed_values: [HTTP, SSL, TCP, UDP, ANY]
    default: HTTP
    description: This is lb-service-type
    label: Service-type
    type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for_each:
            ipvar%: {get_param: server_ips}
          template:
            ip: ipvar%
            port: {get_param: server_port}
    type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator
```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

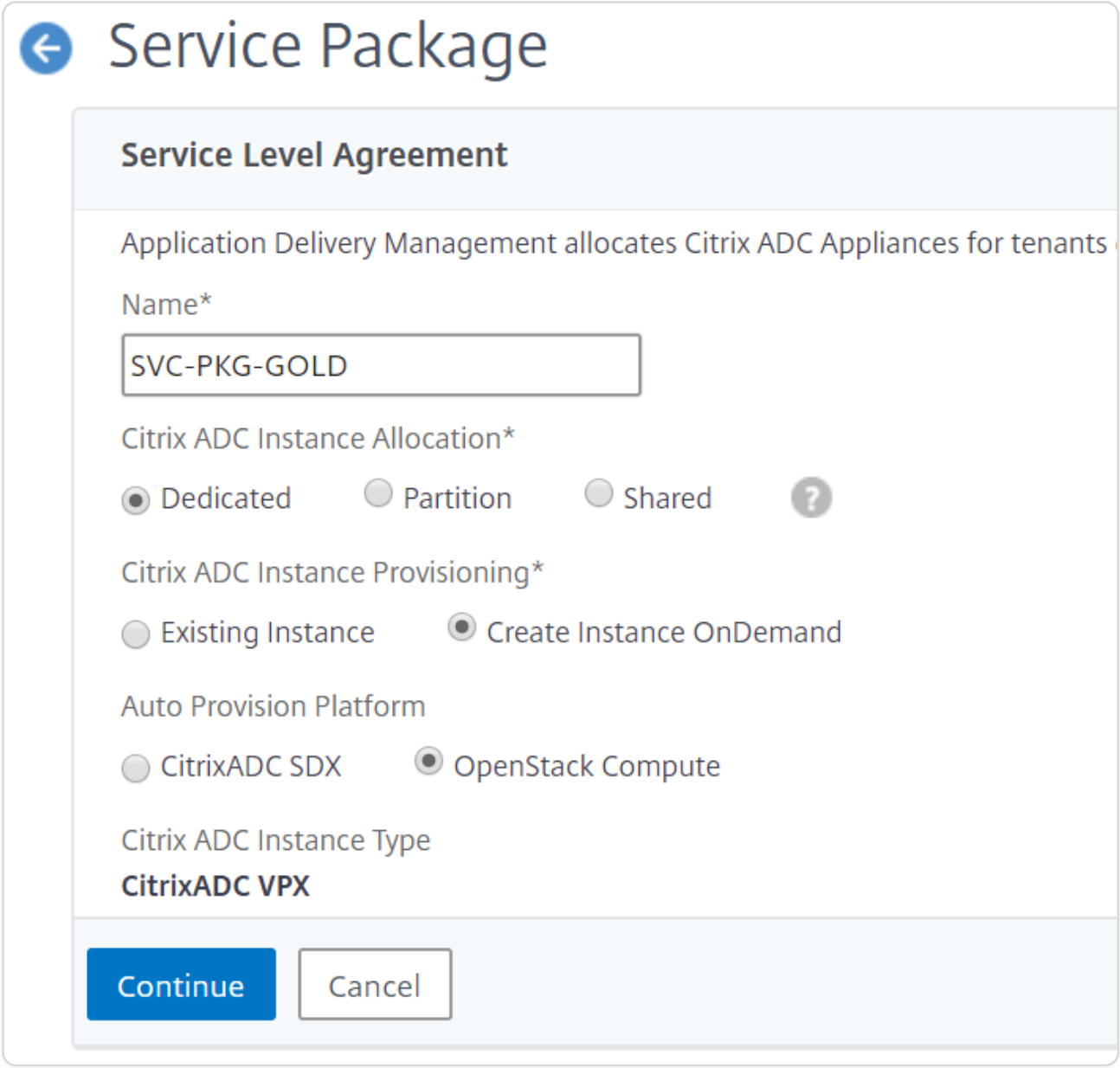
For more information about Heat services and how to create templates, see OpenStack Heat documentation.

Service package isolation policies

Dedicated Isolation Policy

Every tenant associated with the NetScaler Application Delivery Management (ADM) service package of a dedicated policy is assigned a NetScaler instance from among the instances that are part of this service package. This assigned NetScaler instance is not shared with other tenants.

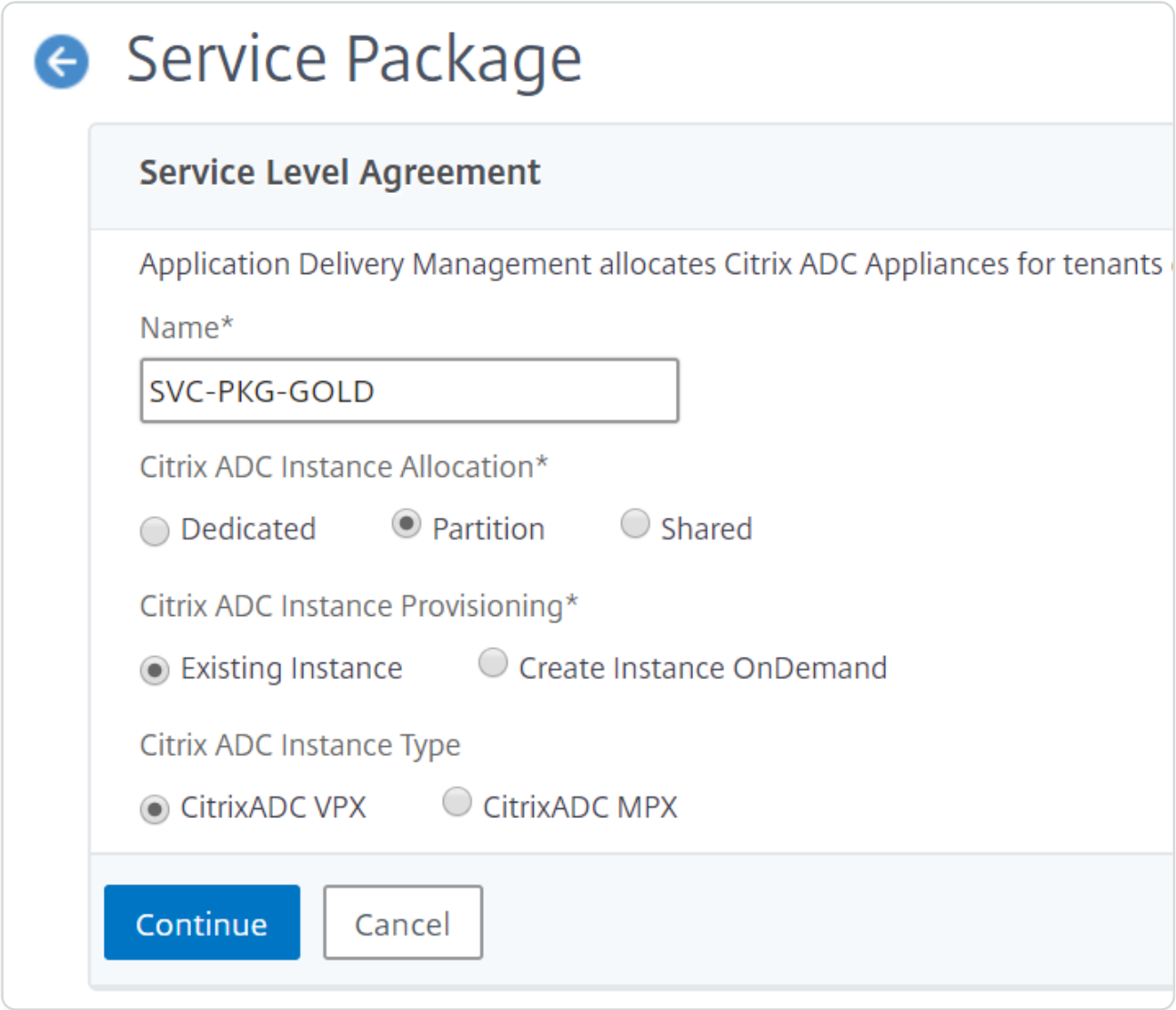
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Partition Isolation Policy

Every tenant associated with the service package of partition policy is assigned a dedicated logical admin partition of a NetScaler instance that is part of the service package.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



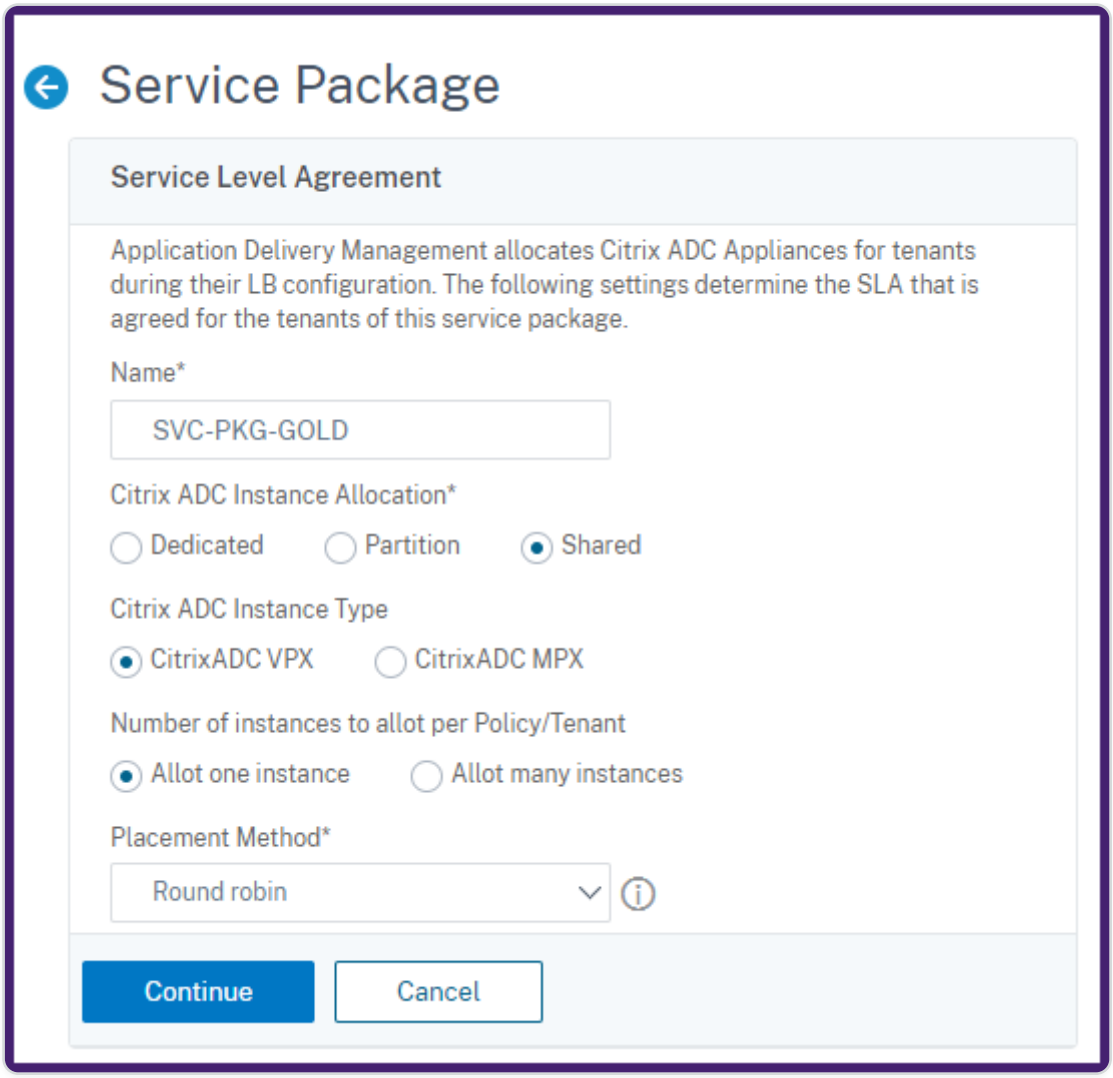
Shared Isolation Policy

Tenants associated with the service package share the NetScaler instances that are part of the service package. All configurations of a tenant are assigned to one NetScaler instance. In this mode, configurations from multiple tenants can be hosted on the same NetScaler instance. You can select **NetScaler VPX** or **NetScaler MPX** as device type. You can choose to allot only one NetScaler instance or many instances to the service package. That is, multiple tenants can share one or multiple virtual instances of the NetScaler device.

NOTE

Add NetScaler SDX instances in the service packages as NetScaler VPX instances only, as a NetScaler SDX has a NetScaler VPX provisioned on it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

NetScaler Application Delivery Management (ADM) assigns NetScaler 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, NetScaler® ADM allows you to precisely define placement policies

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler instance that is used in each load balancer configuration created by users. Flexible placement policies in NetScaler ADM provide an added option to the existing method of assigning NetScaler instances based on tenants.

NOTE

You can assign instances to tenants manually or use placement policies to assign instances based on the expressions created. You cannot use both these methods simultaneously on a single service package.

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 NetScaler 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 NetScaler 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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"
```

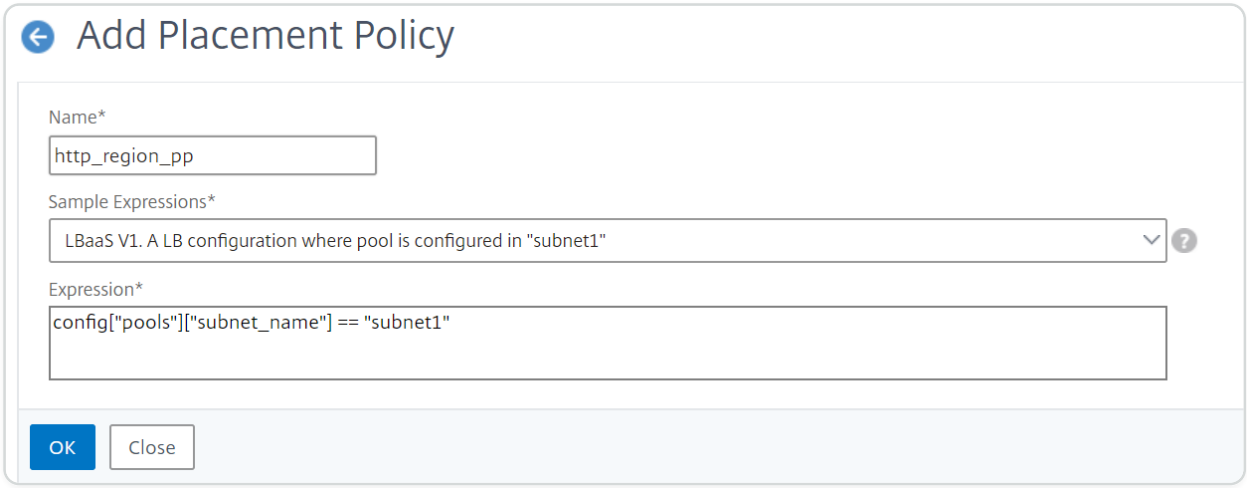
Adding Placement Policy

1. From the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 **NetScaler VPX** or **NetScaler 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.

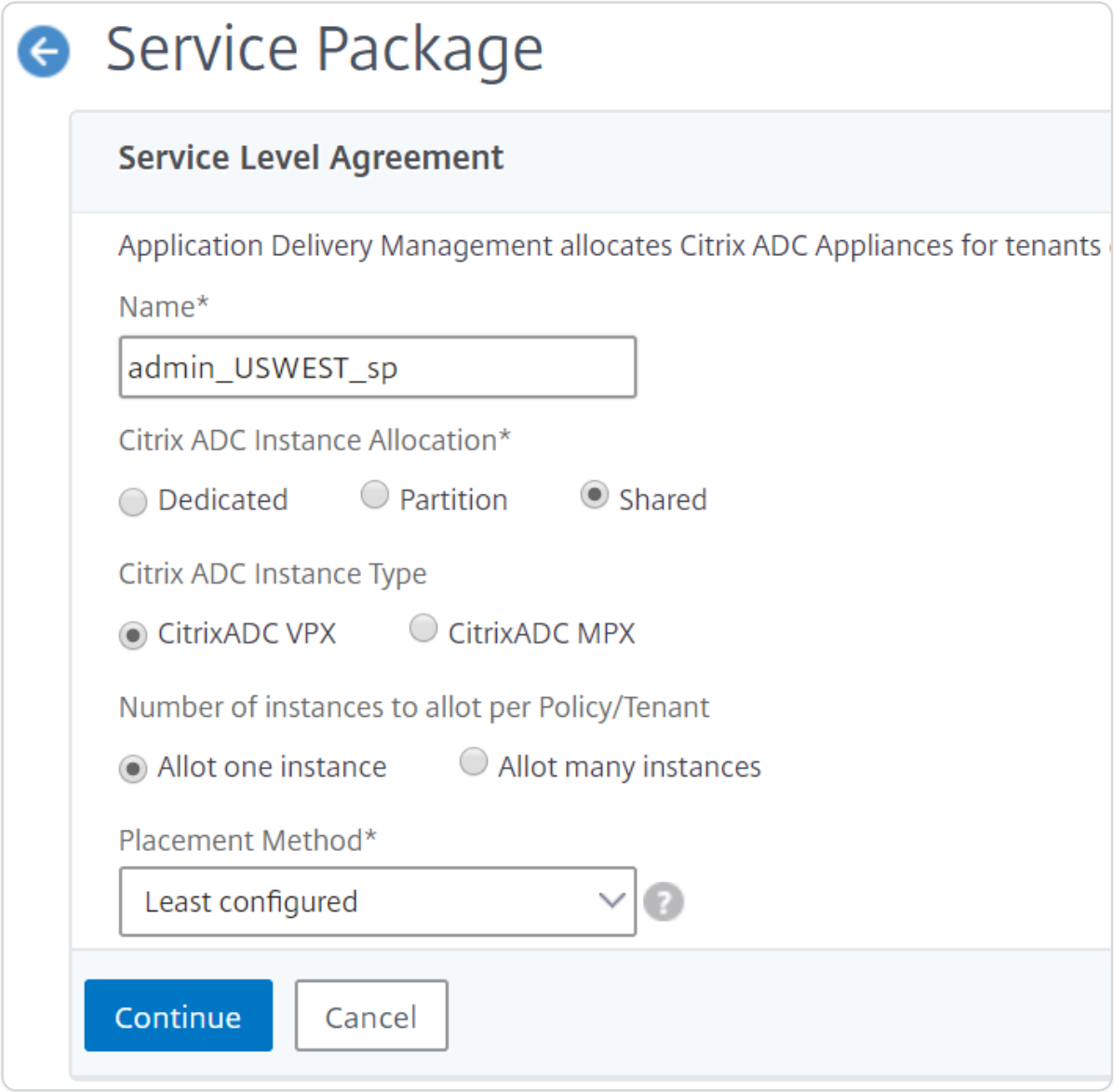
      NOTE

      NetScaler SDX has to be added in the service packages as NetScaler VPX instances only, as a NetScaler SDX has a NetScaler VPX provisioned on it.

   d. Placement Method - select **Least Configured**

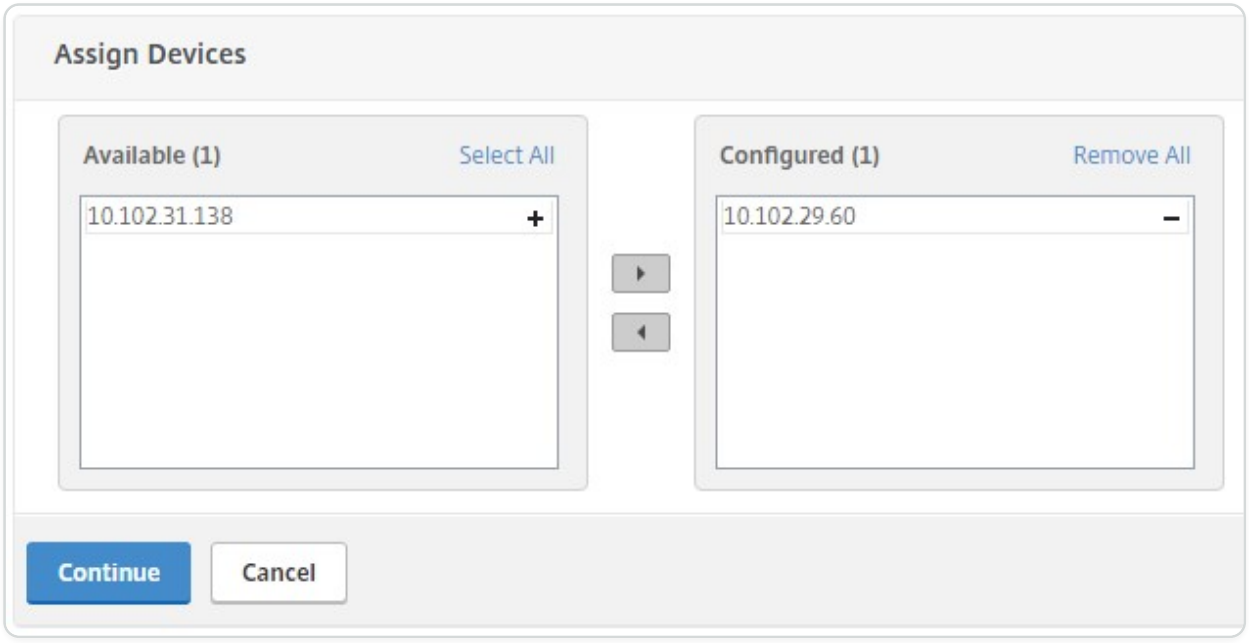
      When Least Configured is selected, the NetScaler instance that has the least number of pool members configured at that point in time is chosen as the device for the tenant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

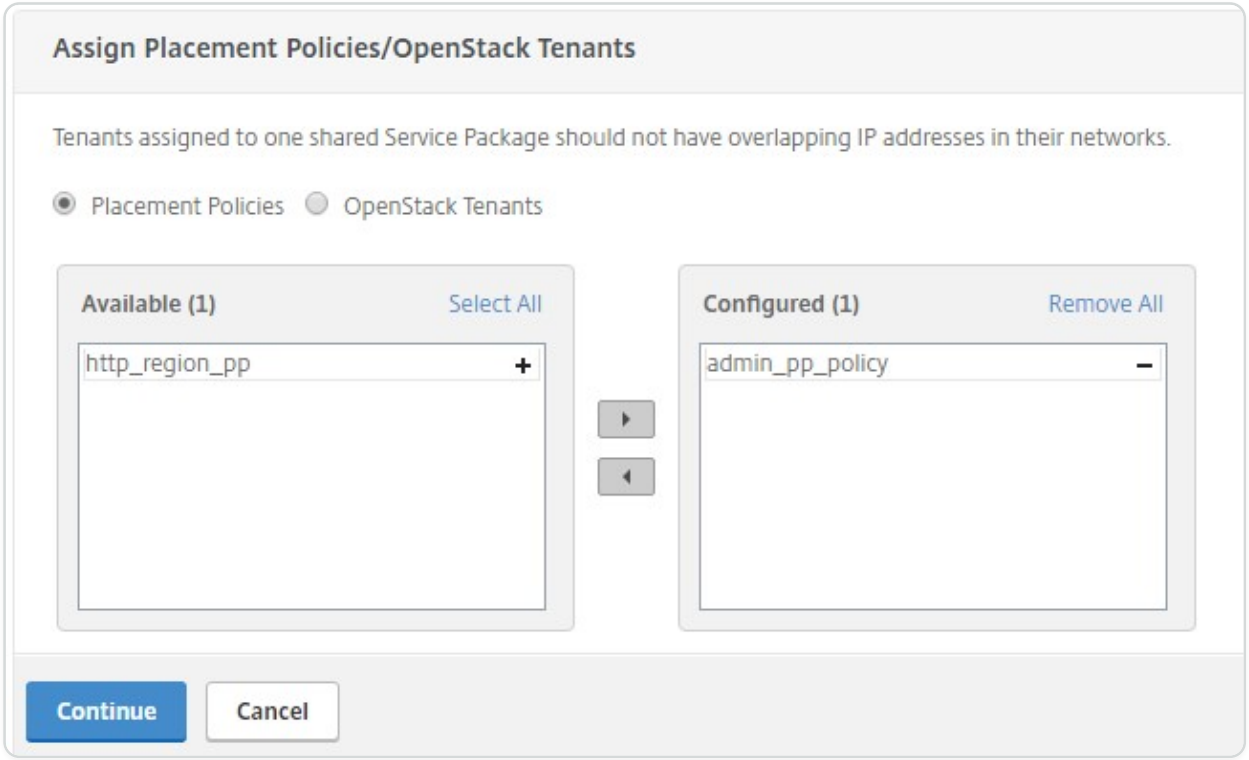


6. Click **Continue**.
7. In **Assign Devices** section, add the available NetScaler devices to the configured devices list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 NetScaler ADM assigns NetScaler instances based on tenants. If the tenant is not part of any service package, the NetScaler ADM displays an error message that says:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

"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 NetScaler instances

NetScaler Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

This article provides you with a list of tasks that you have to perform on both VMware NSX Manager and on NetScaler® ADM.

NOTE

Ensure that VMware NSX for vSphere 6.2 and above is installed and configured, and the edge gateways, DLR, and virtual machines that have to be load balanced are already created.

Prerequisites

- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
- Install NetScaler ADM on any of the supported hypervisors.

  For tasks to install NetScaler ADM build 13.1, on any of the supported hypervisors, see Deploying NetScaler ADM.

VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you require on your VMware ESXi server to install a NetScaler ADM virtual appliance.

Component	Requirement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RAM	8 GB
Virtual CPU	8
Storage space	500 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

NOTE

The memory and hard disk requirements specified above are for deploying NetScaler ADM on VMware ESXi server, considering that there are no other virtual machines running on the host. The hardware requirements for VMware ESXi server depends on the number of virtual machines running on it.

Configuring VMware NSX

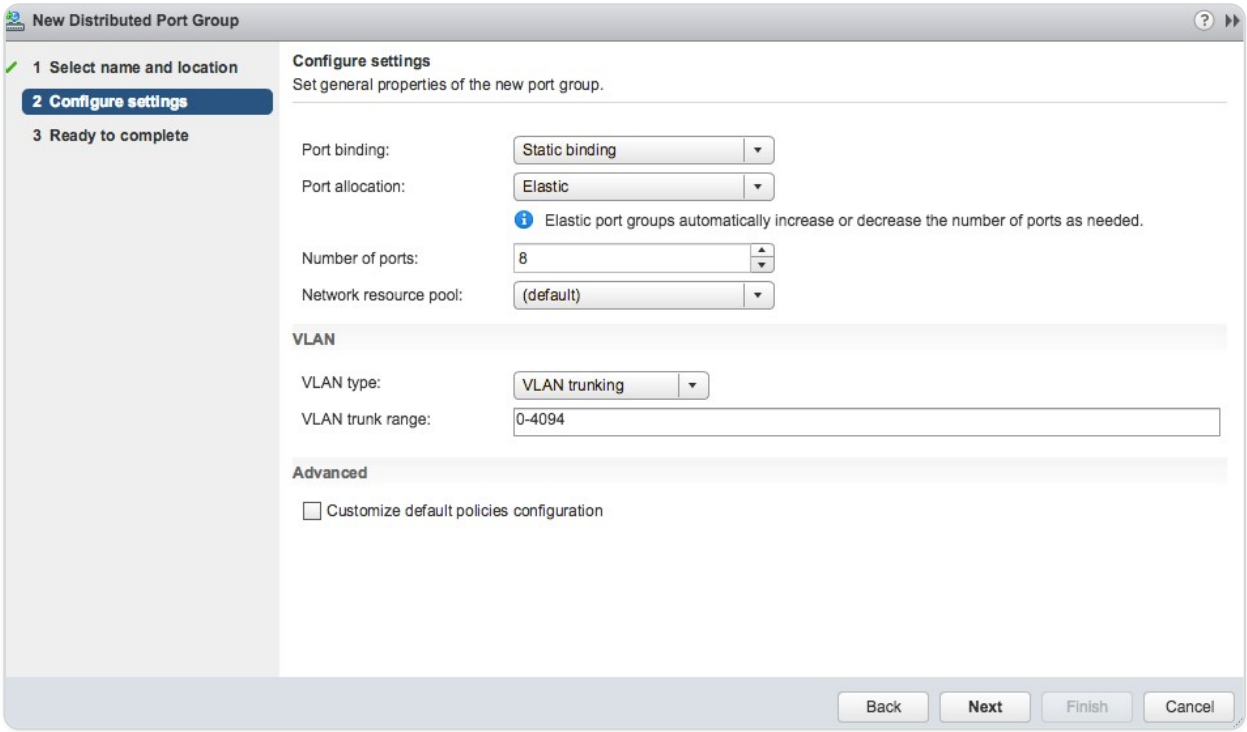
- Create a pool of NetScaler VPX instances of different capacities, which are added to the different service packages.

For example:

- Create five NetScaler VPX instances of VPX1000 (1 Gbps). These instances are added to the Gold service package.
- Create five NetScaler VPX instances of VPX10 (10 Mbps). These instances are added to the Bronze service package.

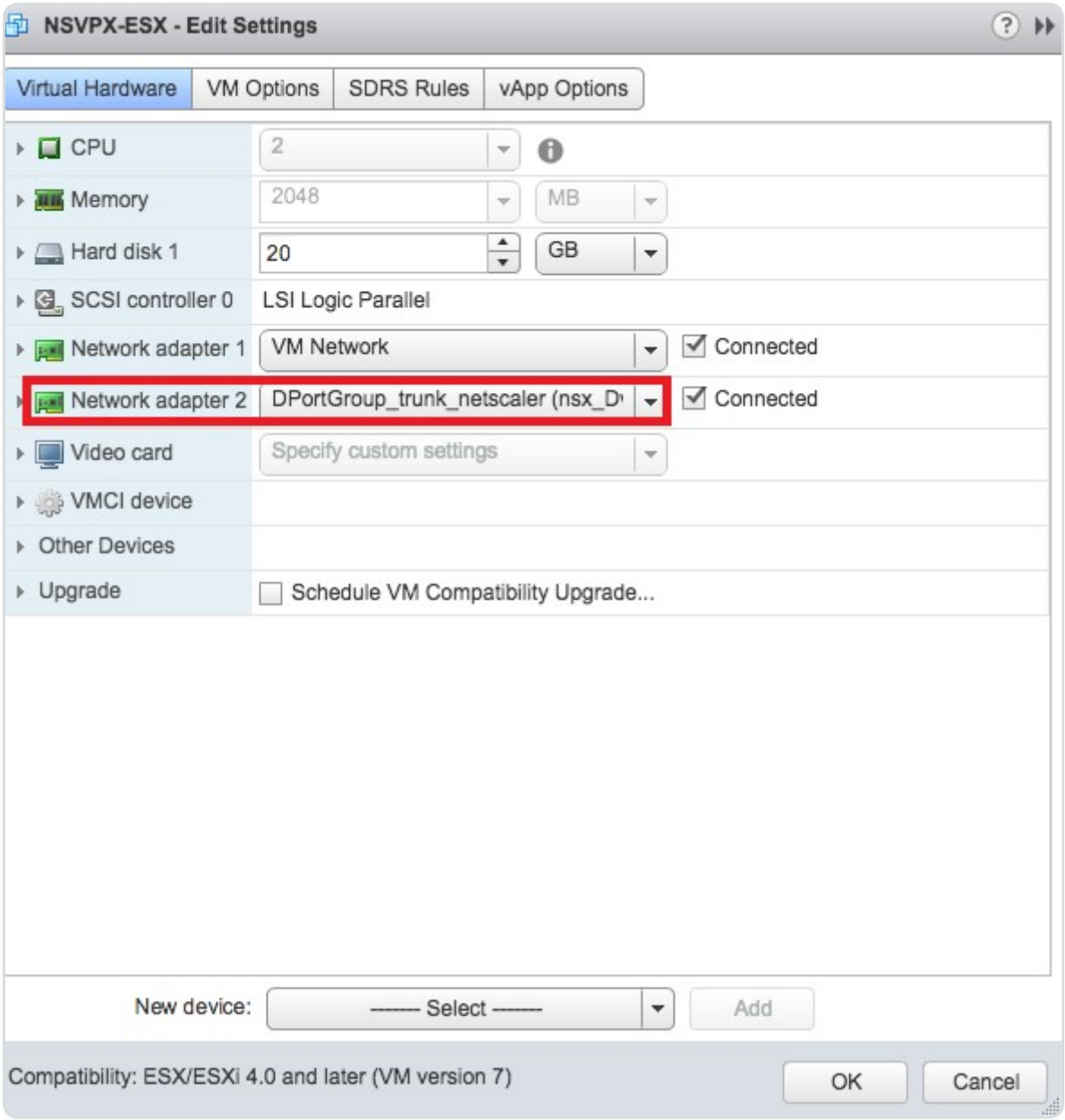
1. In vSphere client, navigate to **Networking**, and create a port group of type VLAN trunking with range, for example, 101-105 (you can even provide the full range, but create port group of type VLAN for only the required VLANs).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Create a new interface for each NetScaler VPX instance, and attach it to the VLAN range trunk port group that was created above.

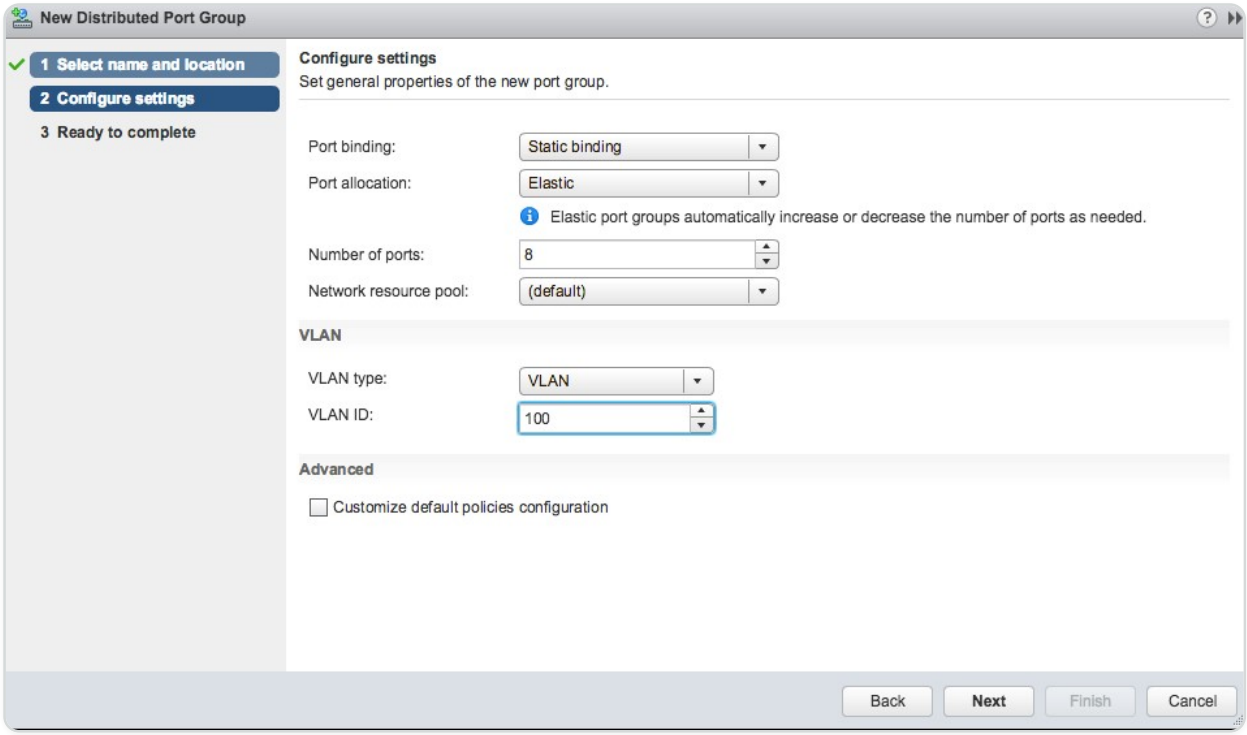
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

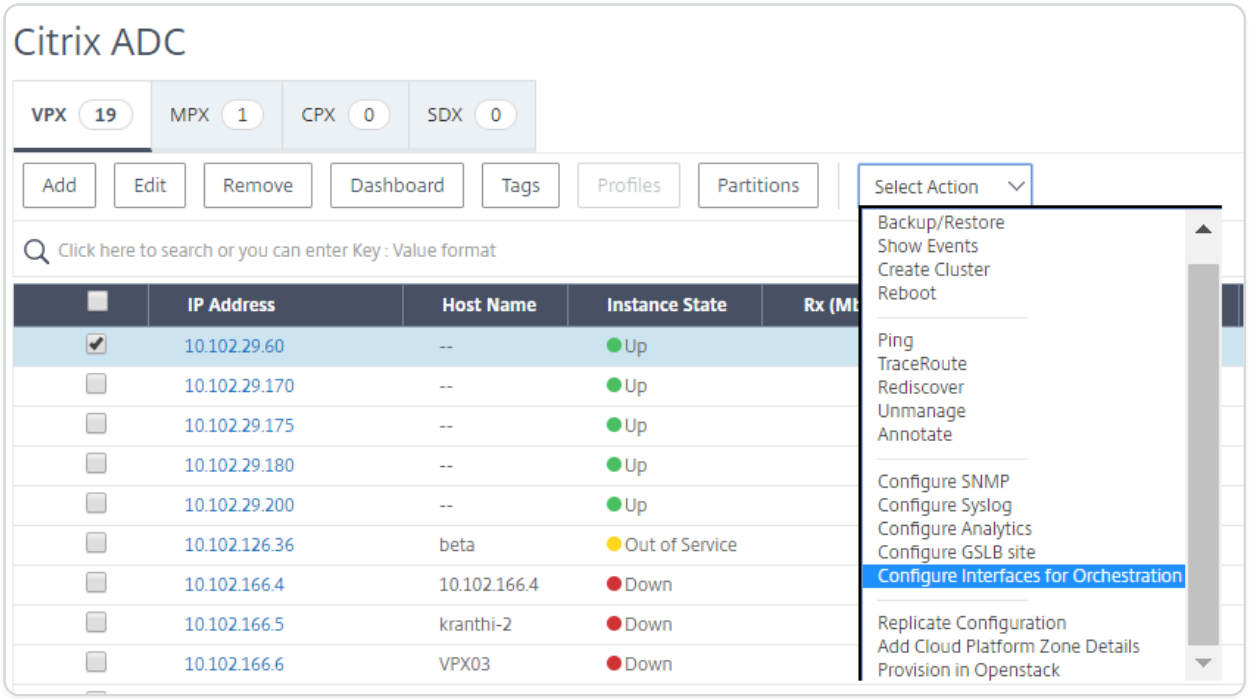


Adding NetScaler VPX Instance in NetScaler ADM

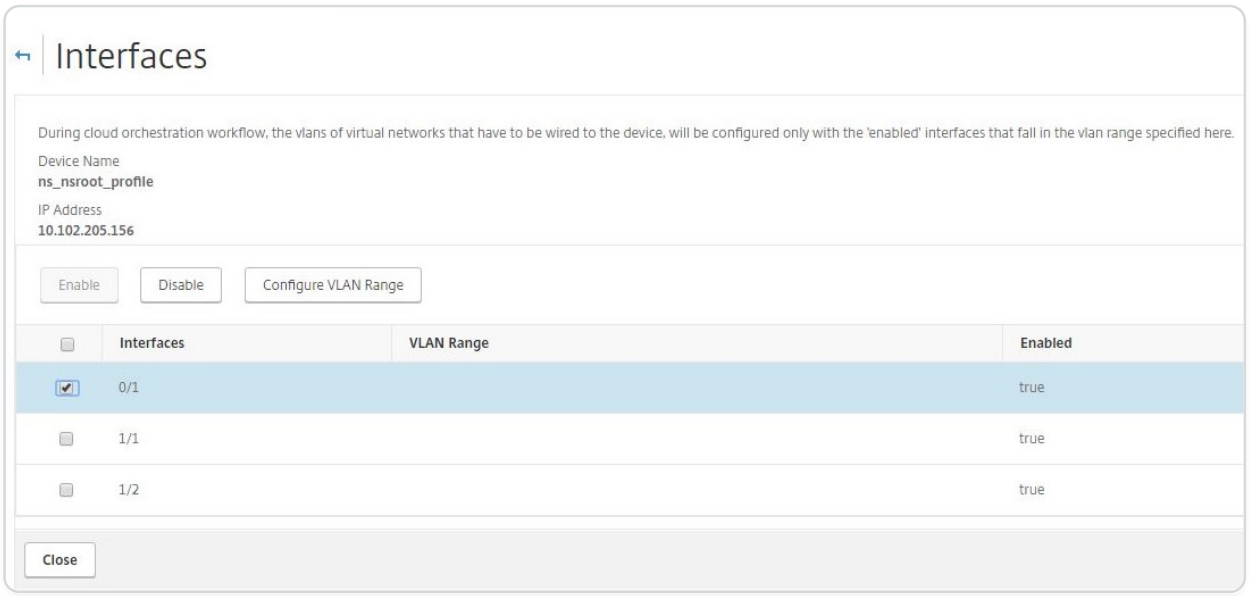
Add NetScaler VPX instances in NetScaler ADM and specify the VLAN range of the trunked group for each device.

1. In NetScaler ADM, navigate to **Infrastructure** \> **Instances** \> **NetScaler VPX**, and click **Add**.
2. On the **Add NetScaler VPX** page, specify either the host names of the instances, the IP address of each instance, or a range of IP addresses, and then select an instance profile from the P**rofile Name** list. You can also create a new instance profile by clicking the + icon.
3. Click **OK**.
4. Select the newly added NetScaler VPX instance from the list on the **NetScaler VPX** page, and click the down arrow button in **Action** field. Select **Configure Interfaces for Orchestration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

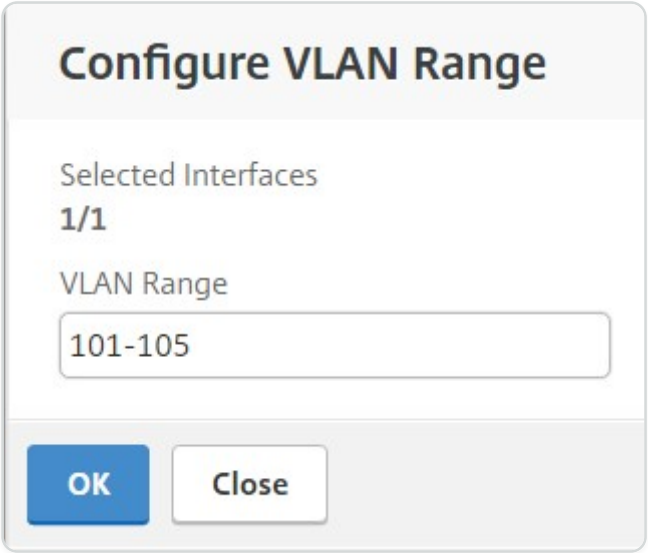


5. On the **Interfaces** page, select the management interface, and click **Disable** to disable VLAN from binding to the management interface.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

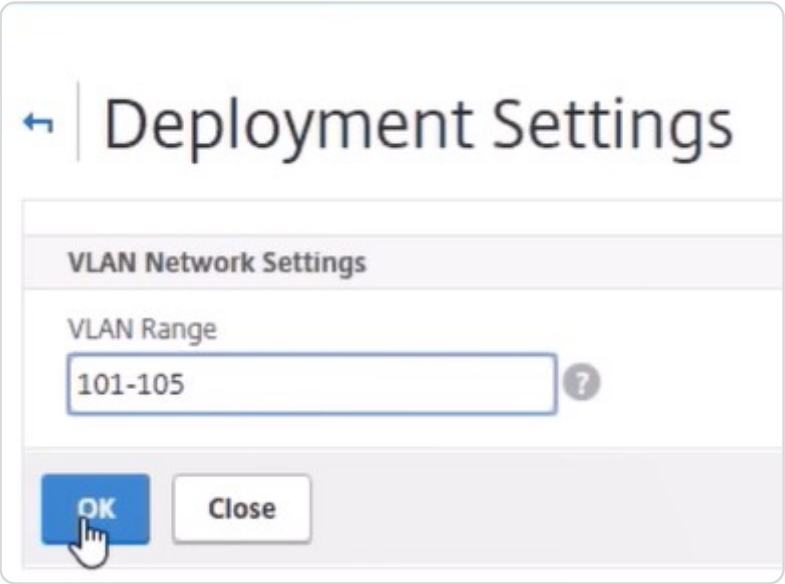


Registering VMware NSX Manager with NetScaler ADM

Register VMware NSX manager with NetScaler ADM to create a communication channel between them.

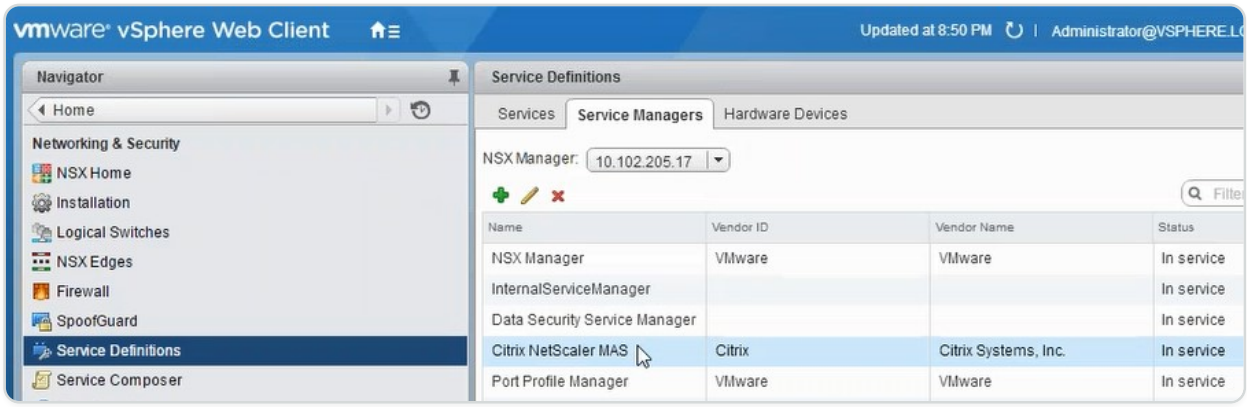
1. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** from the drop-down list, and click **Configure NSX Manager Settings**.
2. On **Configure NSX Manager Settings** page, set the following parameters:
   a. NSX Manager IP Address - IP address of NSX Manager.
   b. NSX Manager user name - Administrative user name of NSX Manager.
   c. Password - Password of the administrative user of NSX Manager.
3. In **NetScaler ADM account used by NSX Manager** section, set the NetScaler Driver user name and Password for the NSX Manager. NetScaler ADM authenticates load balancer configuration requests from the NSX Manager by using these logon credentials.
4. Click **OK**.
5. Navigate to **Orchestration** \> **System** \> **Deployment Settings**. Provide the VLAN range which was configured in trunked port group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** \> **Service Managers**.

   You can view Citrix NetScaler ADM as one of the service managers. This indicates that the registration is successful and a communication channel is established between the NSX manager and NetScaler ADM.



Creating a Service Package in NetScaler ADM

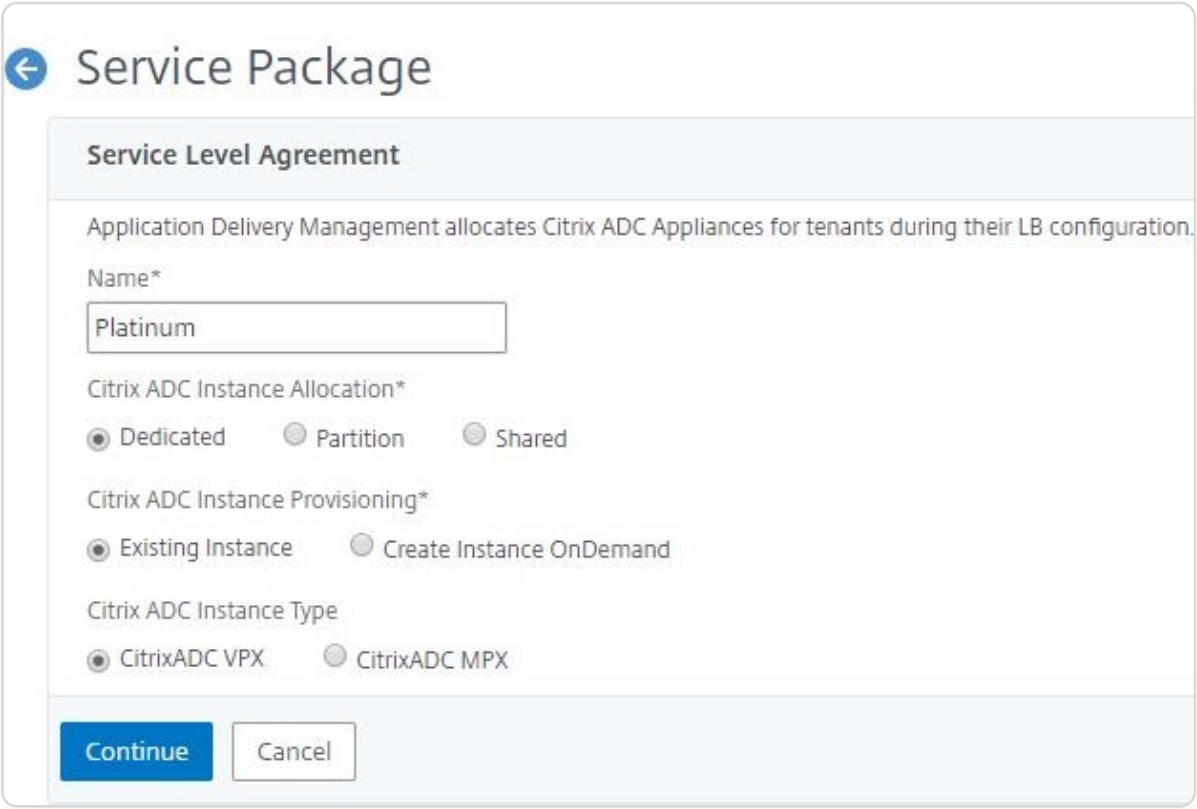
1. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a. Name – type the name of a service package
   b. Isolation Policy – by default, the isolation policy is set to Dedicated
   c. Device Type – by default, the device type is set to NetScaler VPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

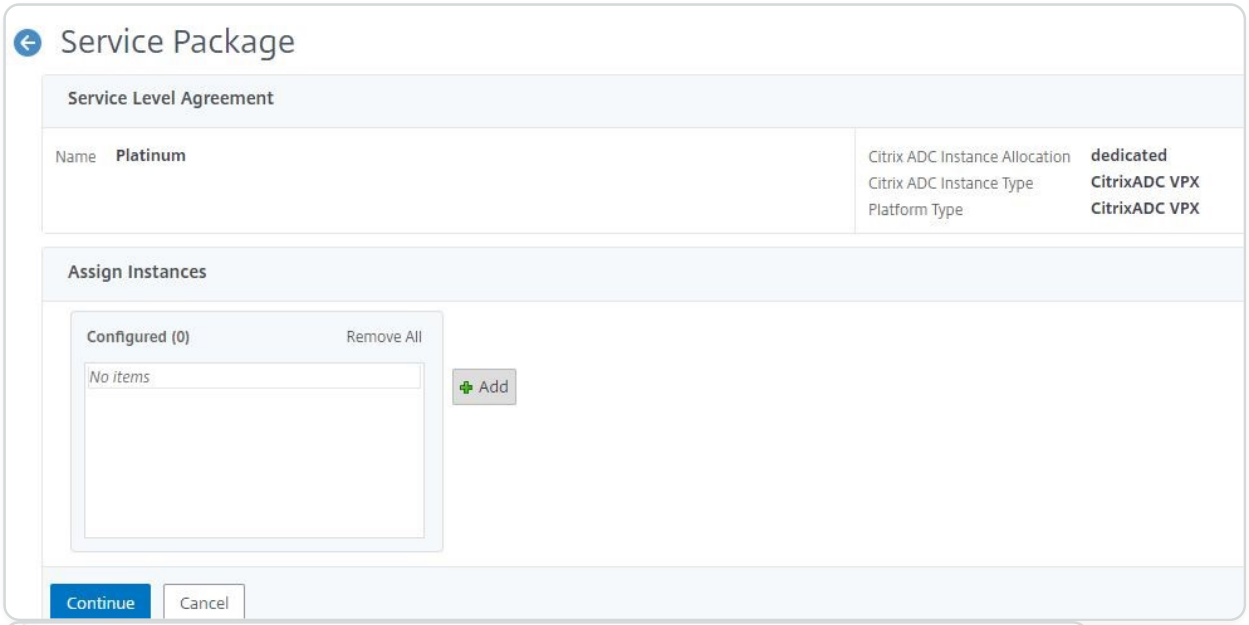
These values are set by default in this version, and you cannot modify them.

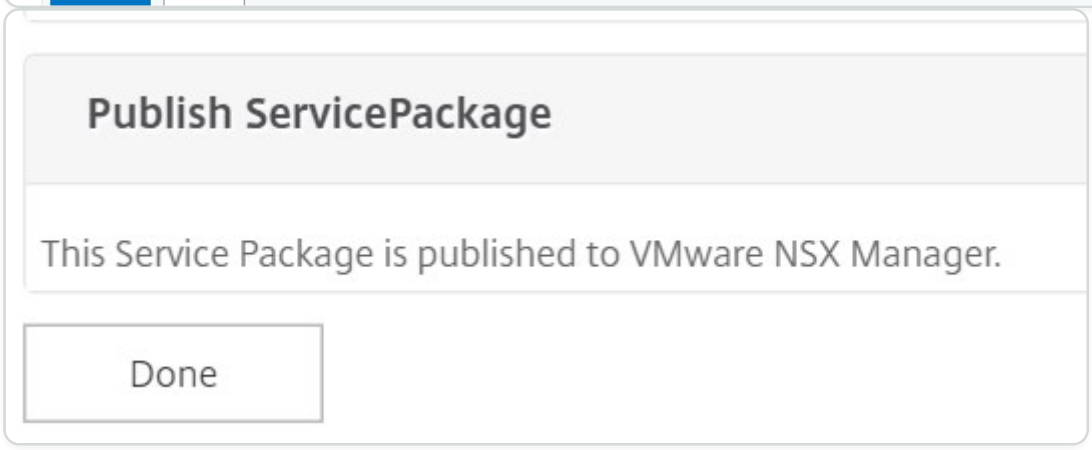
d. Click **Continue**.



3. In **Assign Devices** section, select the pre-provisioned VPX for this package, and click **Continue**.
4. In **Publish Service Package** section, click **Continue** to publish the service package to VMware NSX, and then click **Done**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





This procedure configures a service package in the NSX Manager. A service can have multiple devices added to it and multiple edges can use the same service package to offload the NetScaler VPX instance to NetScaler ADM.

5. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** \> **Services**.

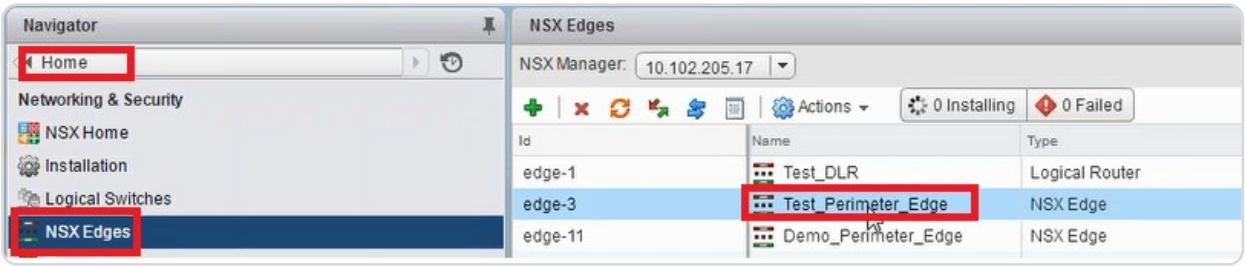
   You can see that the NetScaler ADM service package is registered.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

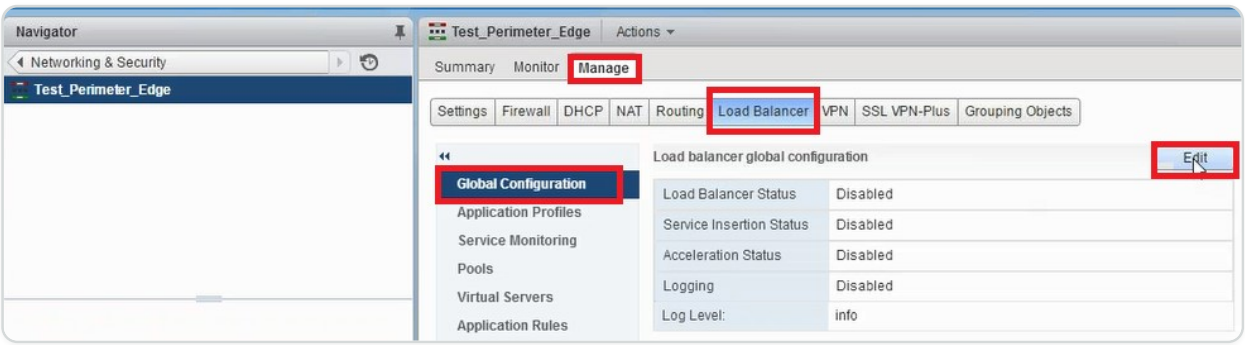
Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the previously created NSX Edge gateway (offload the load balancing function from NSX LB to NetScaler).

1. In NSX Manager, navigate to **Home** \> **NSX Edges**, and select the edge gateway that you have configured.

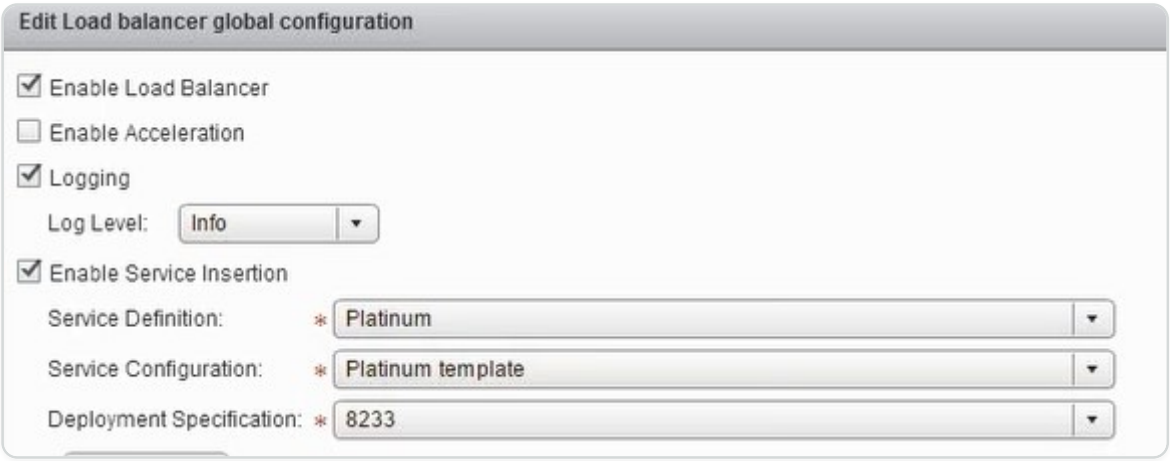


2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.



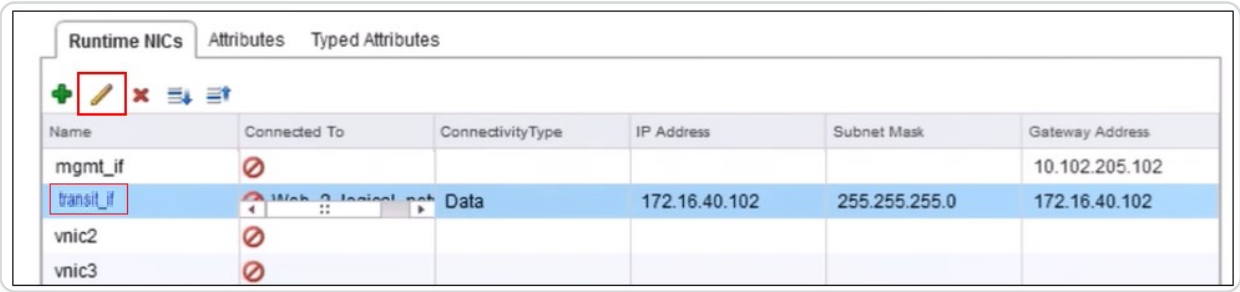
3. Select **Enable Load Balancer**, **Logging**, **Enable Service Insertion** to enable them.

   a. In **Service Definition,** select the service package that was created in NetScaler ADM and published to NSX Manager.

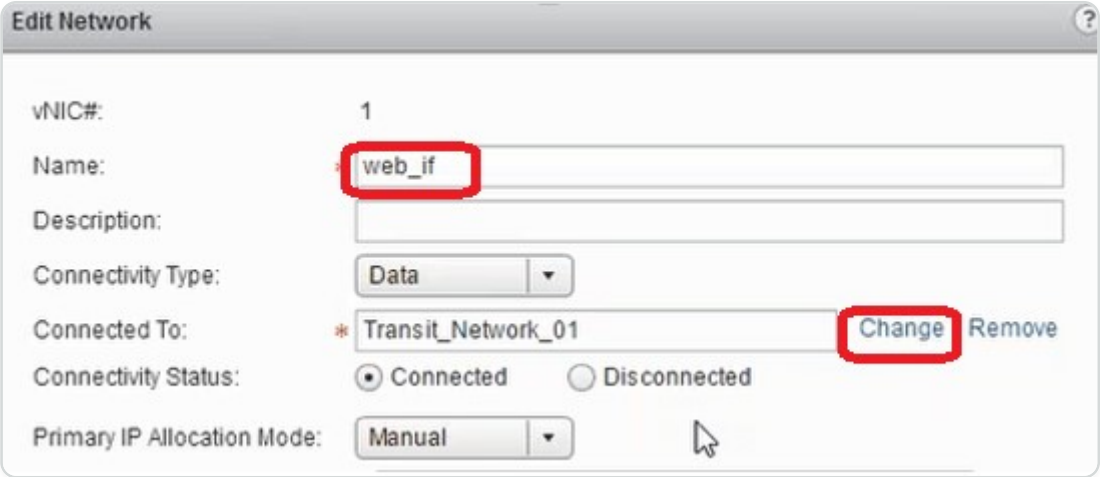


4. Select the existing runtime NICs and click the Edit icon to edit runtime NICs that have to be connected when NetScaler VPX is allocated.

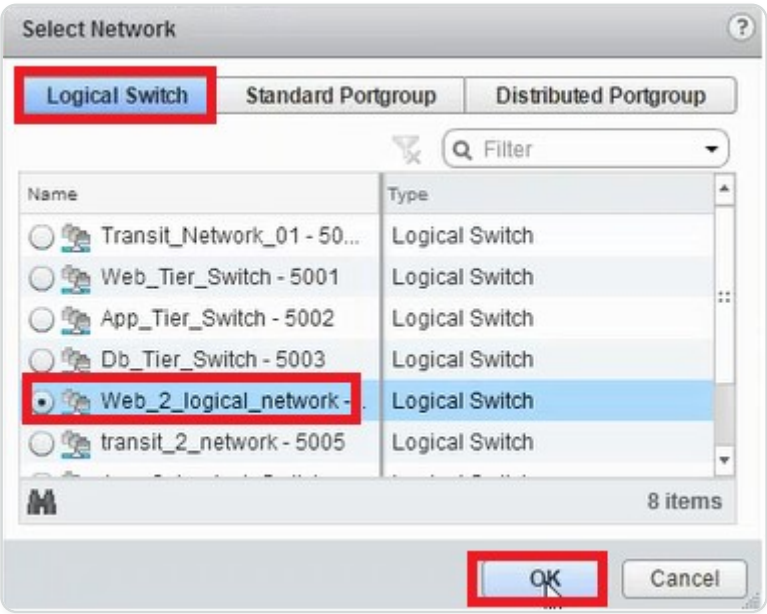
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Edit the name of the NIC, specify Connectivity Type as **Data**, and click **Change**.

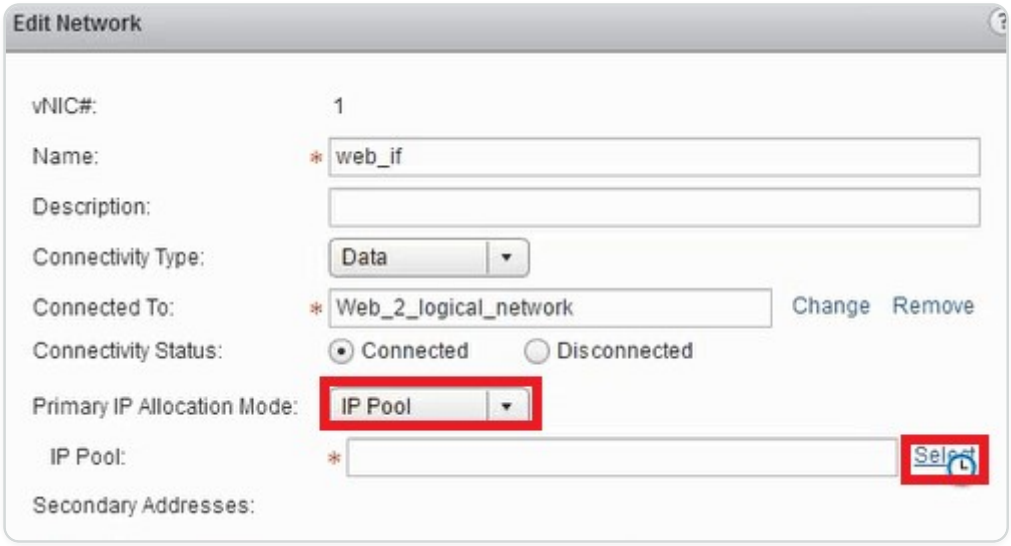


6. Select the appropriate web logical switch.

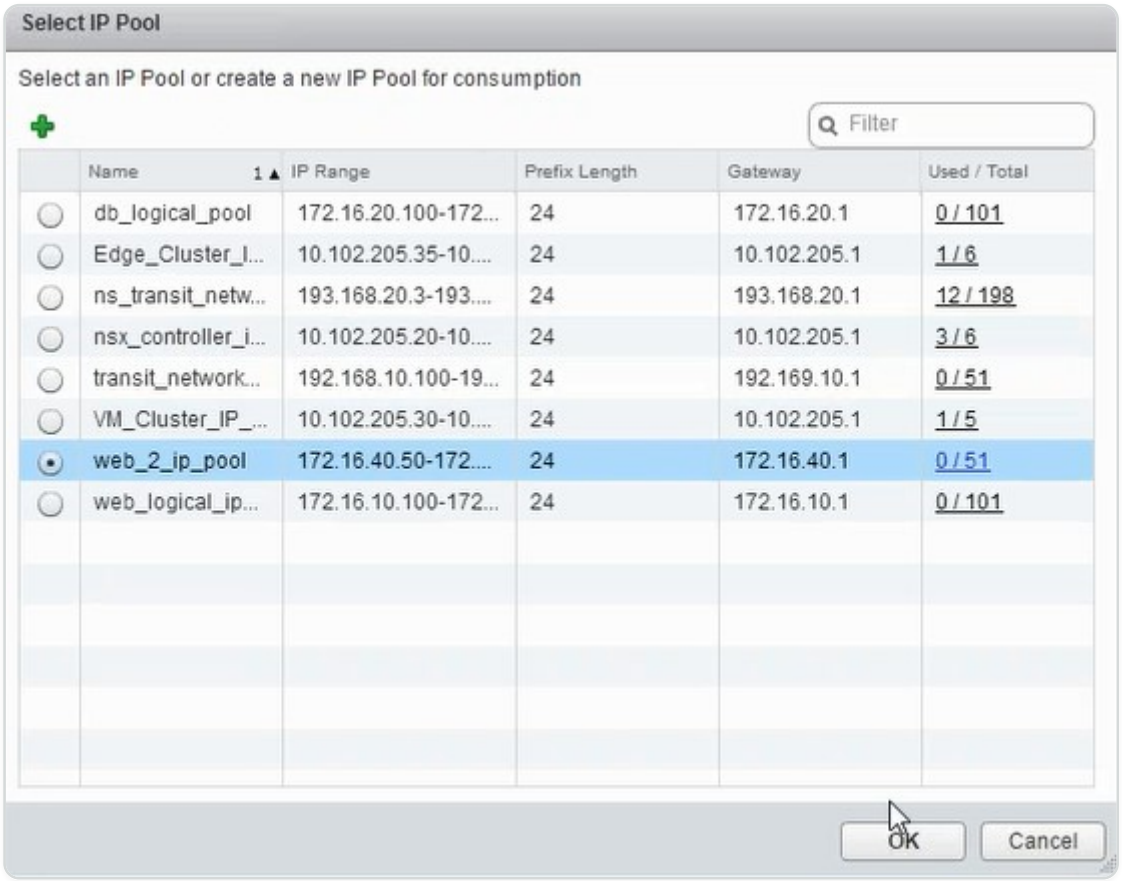


7. In **Primary IP Allocation Mode**, select IP Pool from the drop-down list, and click the down-arrow button on IP Pool field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. In the **Select IP Pool** window, select the appropriate IP pool, and click **OK**.



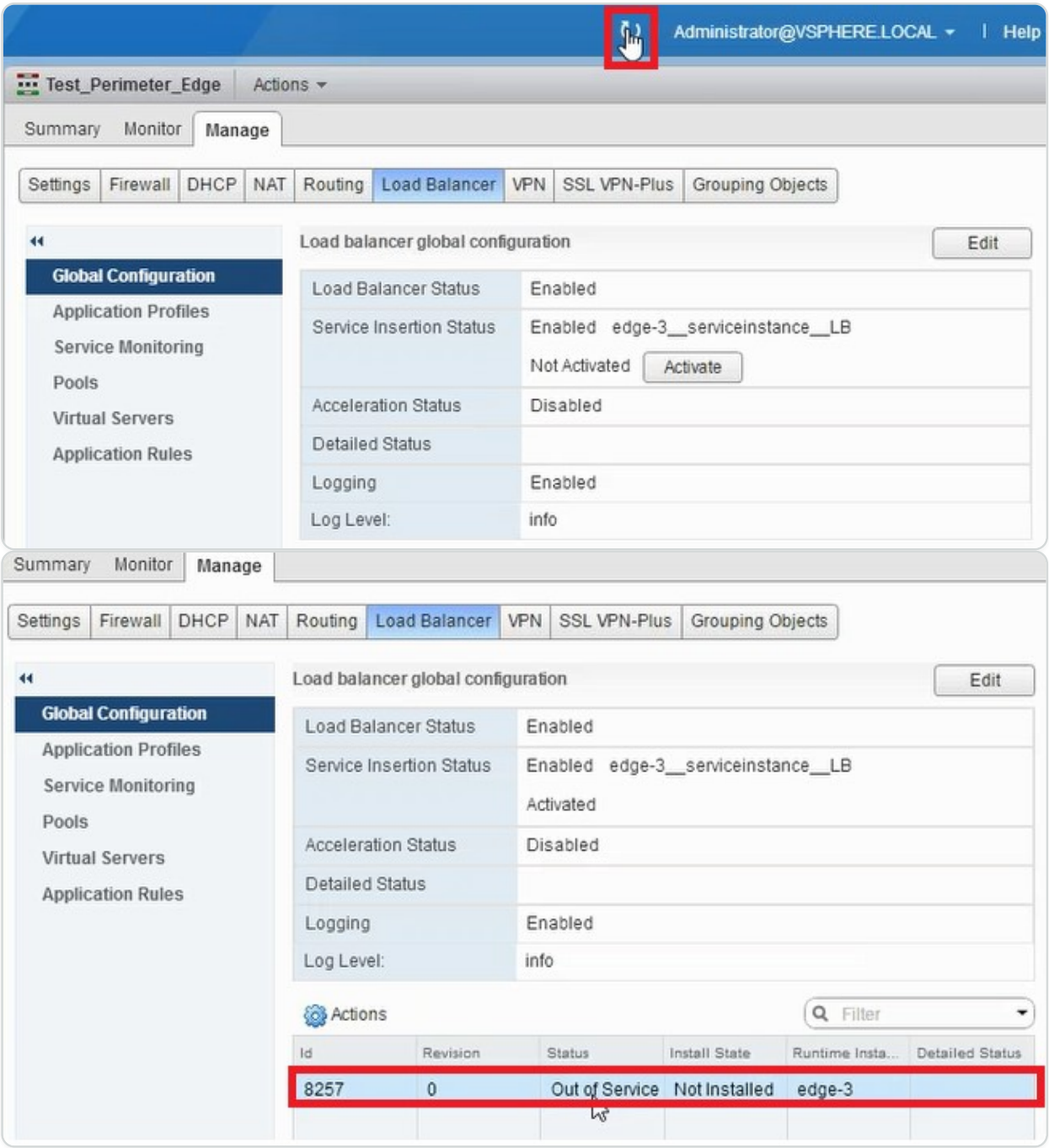
The IP address is acquired and is set as the source net IP address in the NetScaler VPX appliance. A L2 gateway is created in the NSX Manager to map the VXLAN to VLAN.

NOTE

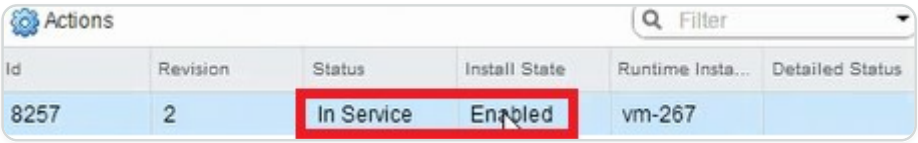
All data interfaces are connected as run-time NICs, and they are part of interfaces for DLR.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



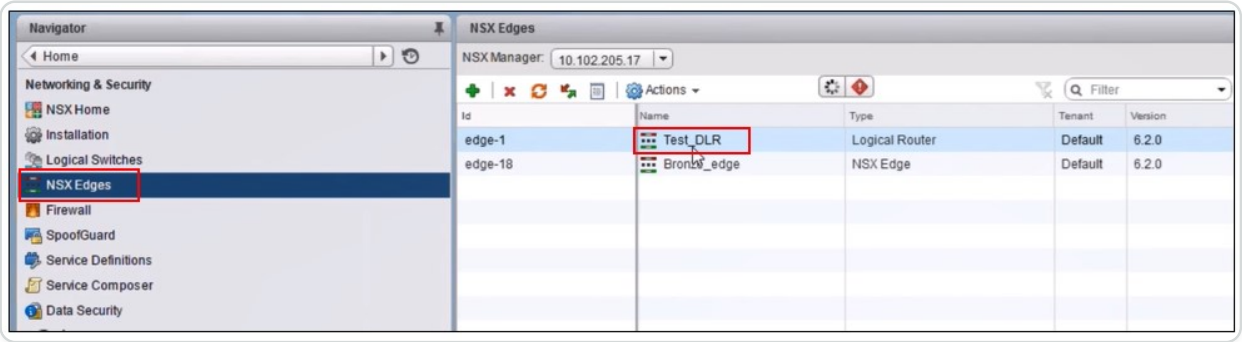
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

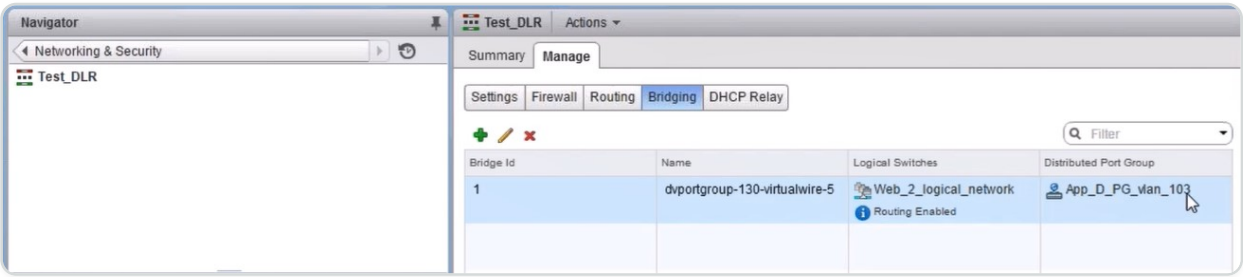
In NetScaler ADM, navigate to **Orchestration** \> **Requests** to see progress details of completion of LB service insertion.

Viewing L2 Gateway on NSX Manager

1. Log on to the NSX Manager on vSphere Web Client, navigate to **NSX Edges**, and select the DLR created.



2. In the DLR page, navigate to **Manage** \> **Bridging**. You can see the L2 gateway displayed in the list.



NOTE

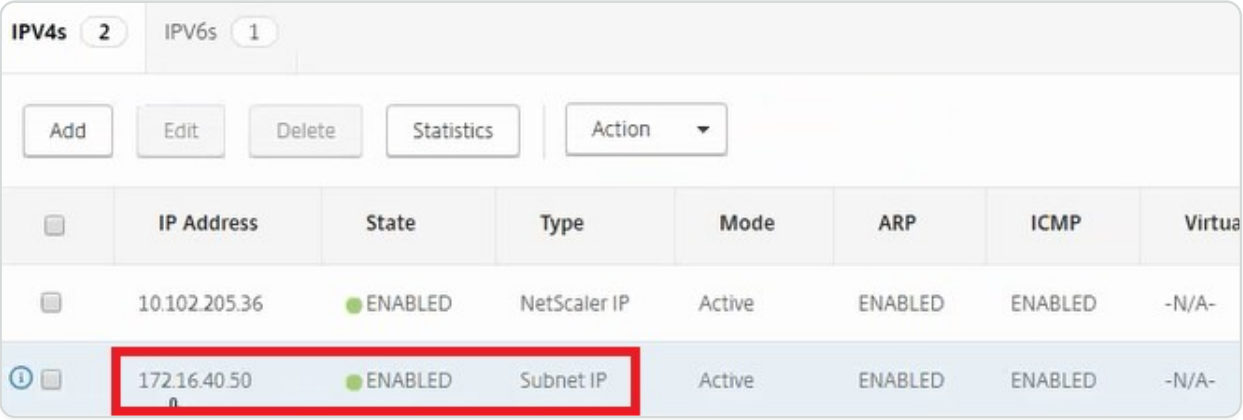
An L2 gateway gets created for each data interface.

Viewing Allotted NetScaler

1. Log on to the NetScaler VPX instance using the IP address displayed in NetScaler ADM. Then, navigate to **Configuration** \> **System** \> **Networking**. In the right pane, you can see that the two IP address are added. Click the IP address hyperlink to see the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The subnet IP address is same as the IP address of the web interface added in the NSX.



2. Navigate to **Configuration** \> **System** \> **Licenses** to view the licenses that are applied to this instance.

Configuring NetScaler VPX Instance Using StyleBook

1. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **Configure NSX Manager** \> **Edge Gateways**.

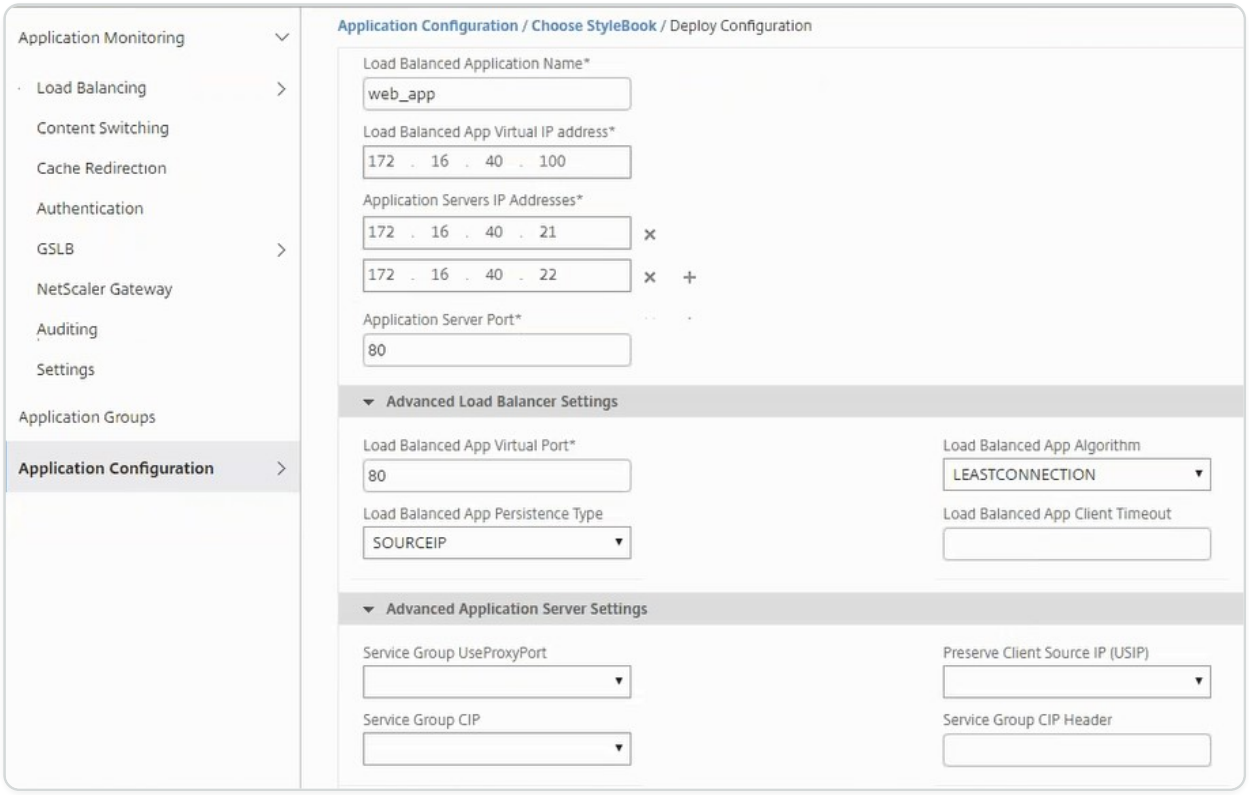
   Make a note of the NetScaler instance IP that is allotted to the respective Edge Gateway on which Load Balancing configuration through StyleBooks has to be applied.

2. Create a new StyleBook. Navigate to **Applications** \> **Configuration**, import the StyleBook, and select the StyleBook from the list.

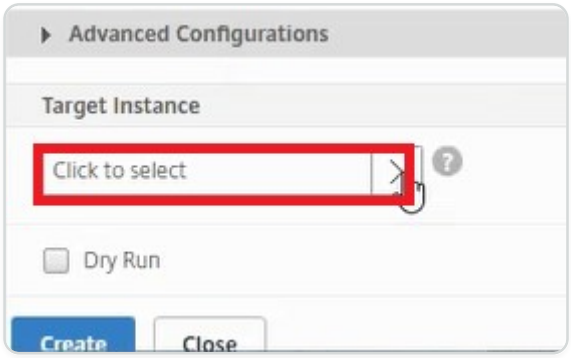
   To create a new StyleBook, see Create Your Own StyleBook.

3. Specify values for all the required parameters.

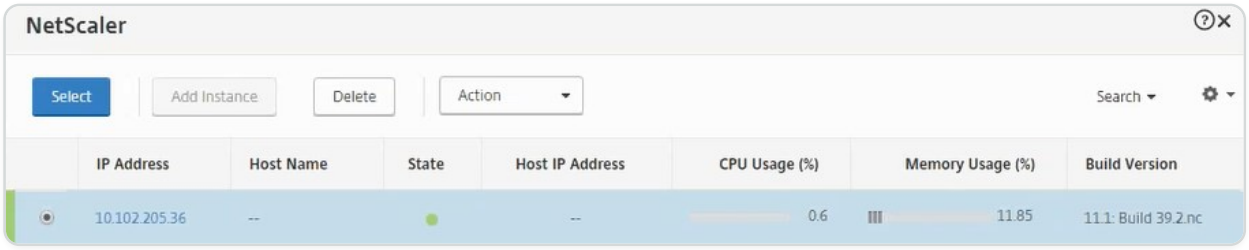
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Specify the NetScaler VPX instance on which you want to run these configuration settings.

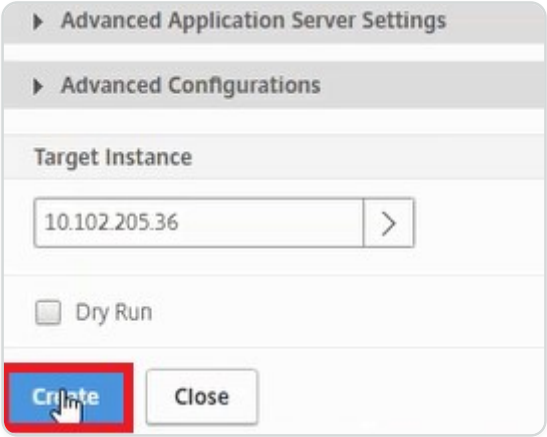


5. Select the IP instance noted earlier, and click **Select**.



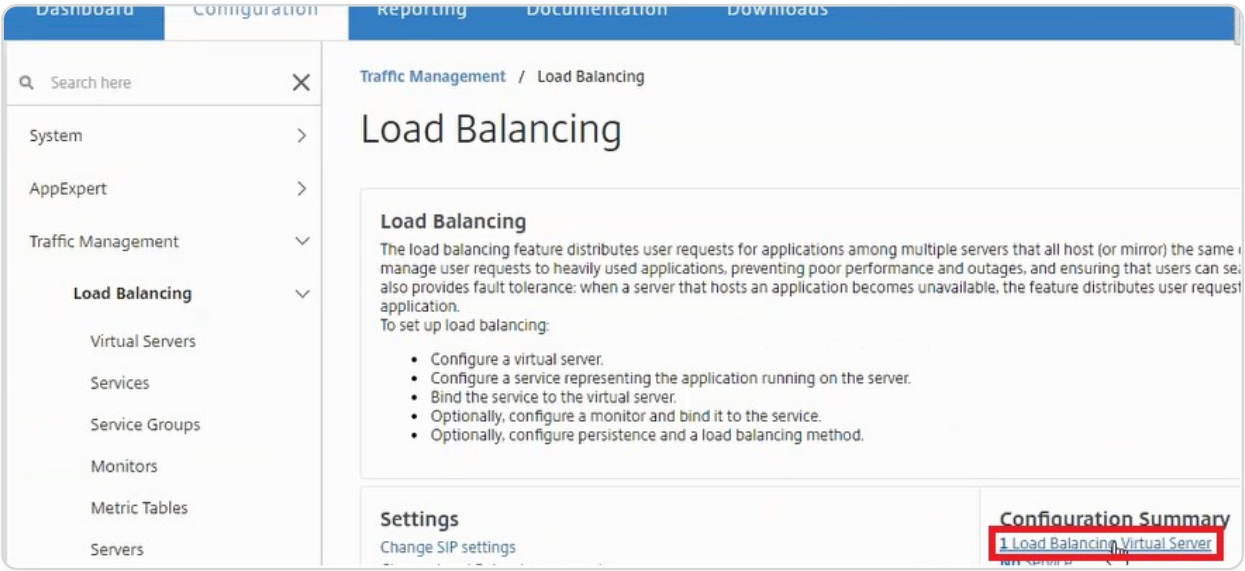
6. Click **Create** to apply the configuration on the selected device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

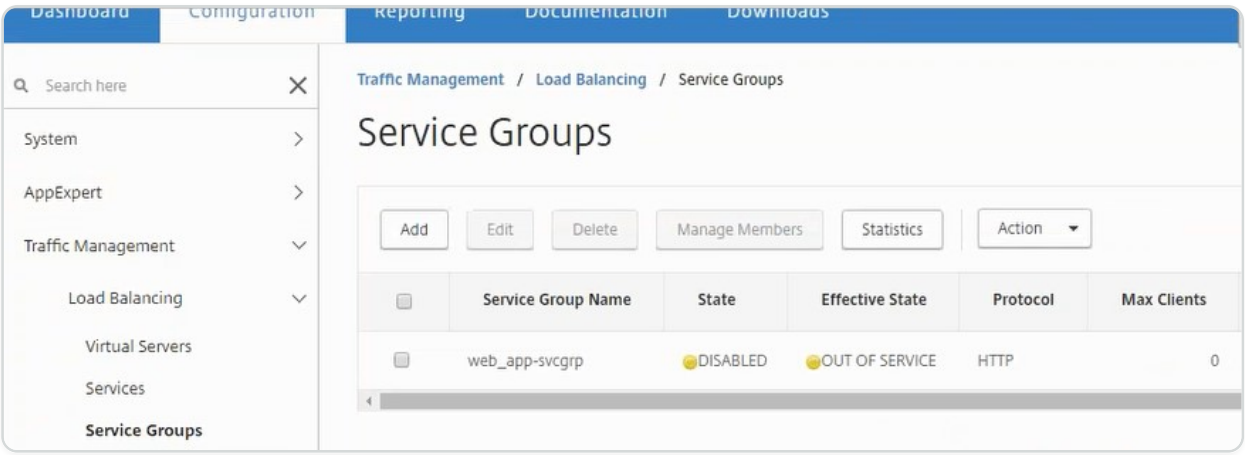


Viewing Load Balancer Configuration

1. Log on to the NetScaler VPX instance, navigate to **Configuration** \> **Traffic Management** \> **Load Balancing** to view the load balancing virtual server that is created.

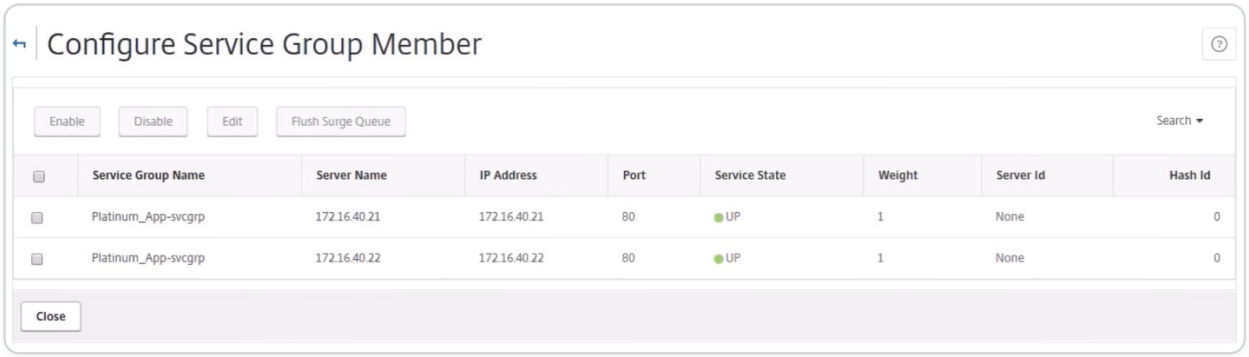


You can also view the service groups that are created.



2. Select the service group, and click **Manage Members**. The **Configure Service Group Member** page displays the members associated with the service group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



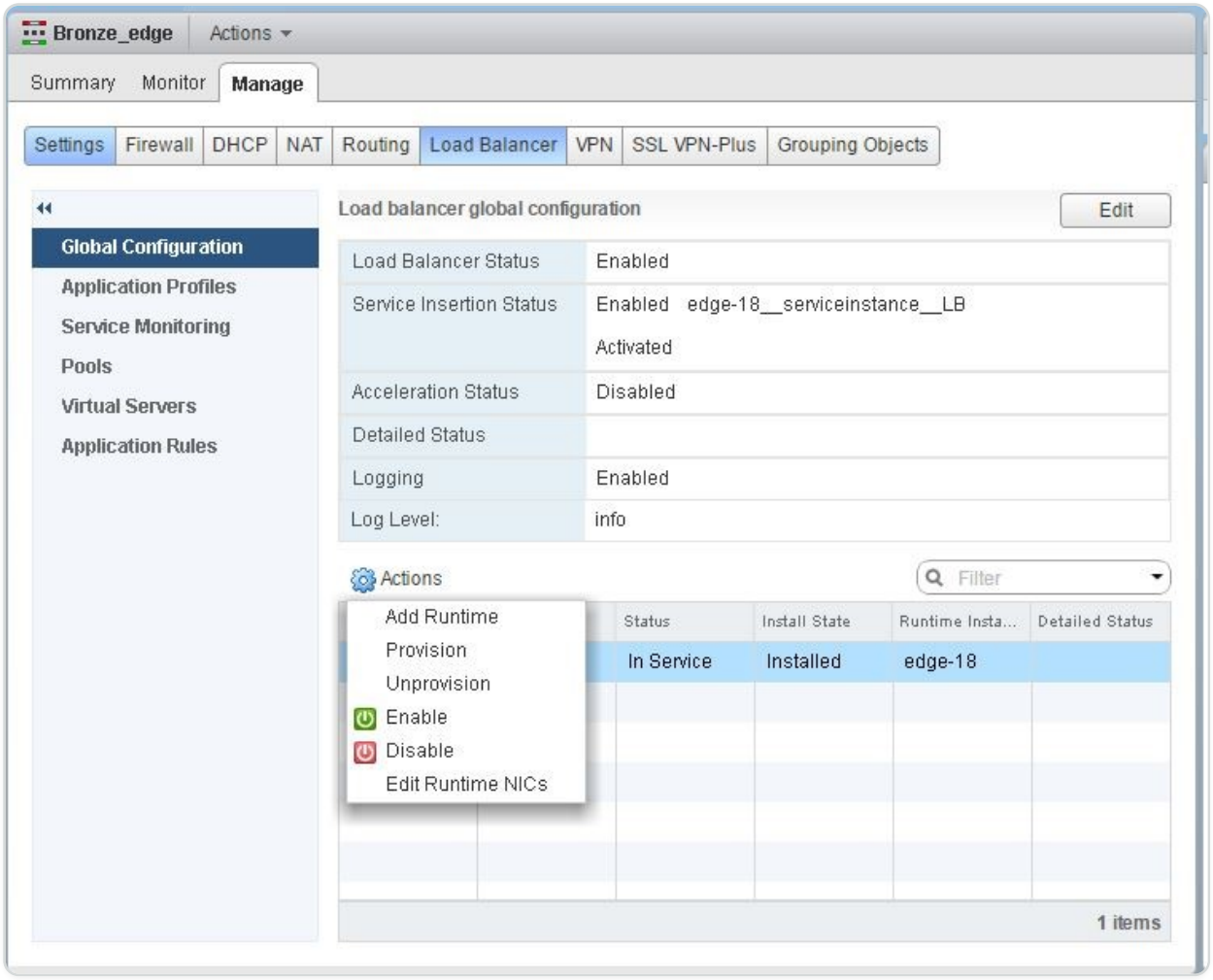
Deleting Load Balancer Service

1. In NetScaler ADM, navigate to **Applications** \> **Configuration**, and click **X** icon to delete the application configuration.
2. Log on to the NSX Manager on vSphere Web Client and navigate to the edge gateway to which the NetScaler VPX instance is connected.
3. Navigate to the **Manage** \> **Load Balancer** \> **Global Configuration**, right-click on the runtime entry, and click **Unprovision**.

NOTE

Edge Gateways in NetScaler ADM corresponds to runtime entries in NSX manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler VPX instance is rendered out of service.

4. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **Configure NSX Manager** \> **Edge Gateways**. Verify that the respective mapping of Edge Gateway to the deleted instance is not present.

NSX Manager: auto provisioning of NetScaler instances

Overview

NetScaler Application Delivery Management (ADM) integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

During load-balancing service insertion and deletion on VMware NSX Manager, NetScaler ADM dynamically provisions and destroys the NetScaler instances. This dynamic provisioning requires the NetScaler VPX license assignments to be automated in NetScaler ADM. When the NetScaler licenses are uploaded to the NetScaler ADM, NetScaler ADM performs the role of license server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

NOTE

This integration is supported only for **VMware NSX for vSphere 6.1 or earlier**.

- NetScaler ADM, version 13.0 setup in high availability and installed on ESX.
- NetScaler VPX, version 13.0
- NetScaler VPX licenses for NetScaler VPX instances, version 13.0
- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.

High-Availability Deployment of NetScaler ADM and NetScaler Instances

To provision the NetScaler ADM HA setup, install the NetScaler ADM image file that you have downloaded from the NetScaler site. For more information on how to provision NetScaler ADM HA setup, see Deploying NetScaler ADM in High Availability.

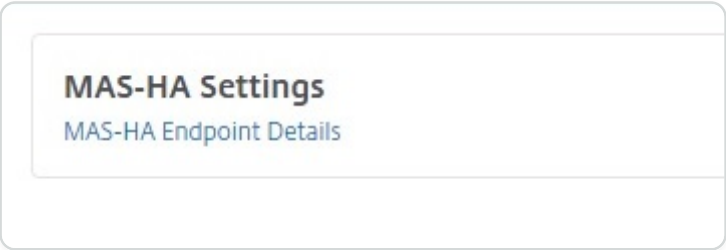
Setting up NetScaler® ADM HA Endpoint Details

To integrate VMware NSX manager with NetScaler ADM that is deployed in a HA mode, you must first enter the virtual IP address of the load balancing NetScaler instance. You must also upload the certificate file that is present on the NetScaler load balancing virtual server to the NetScaler ADM file system.

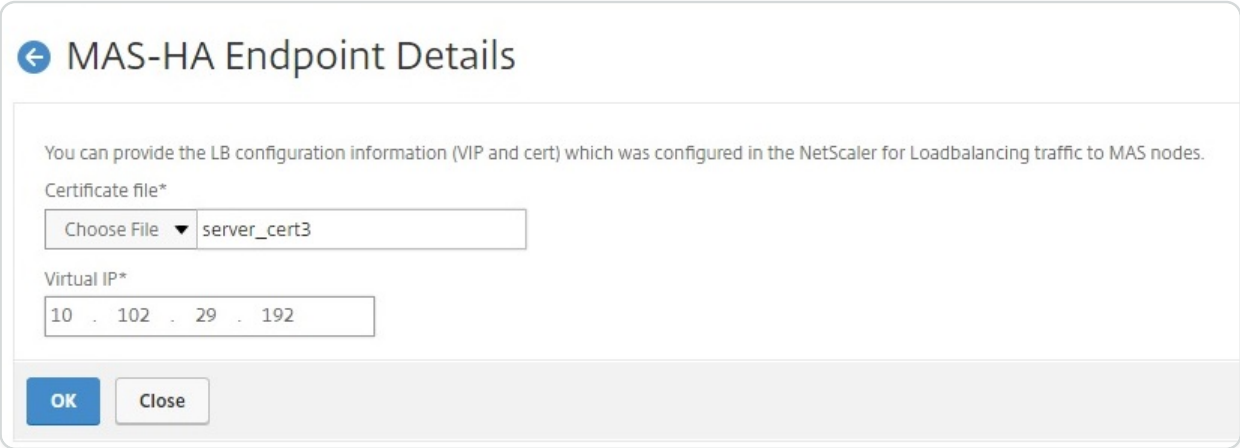
To provide load balancing configuration information in NetScaler ADM:

1. In NetScaler ADM HA node, navigate to **System** \> **Deployment**.
2. Click **HA Settings** in the top-right corner, and in **MAS-HA Settings** page, click **MAS-HA Endpoint Details**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. On **MAS-HA Endpoint Details** page, upload the same certificate that is already present on the load balancing NetScaler instance.
4. Enter the virtual IP address of the load balancing NetScaler instance and click **OK**.



Registering VMware NSX Manager with NetScaler ADM

When you set up two NetScaler ADM servers in high availability, the two server nodes are in active-passive mode. Log on to the primary NetScaler ADM server node to register VMware NSX manager with NetScaler ADM in HA, to create a communication channel between them.

To register VMware NSX manager with NetScaler ADM in HA:

1. In the primary NetScaler ADM server node, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager**.
2. Click **Configure NSX Manager Settings**.
3. On **Configure NSX Manager Settings** page, set the following parameters:
   a. NSX Manager IP Address - IP address of NSX Manager.
   b. NSX Manager user name - Administrative user name of NSX Manager.
   c. Password - Password of the administrative user of NSX Manager.
4. In NetScaler ADM account used by NSX Manager section, set the NetScaler Driver Password for the NSX Manager.
5. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

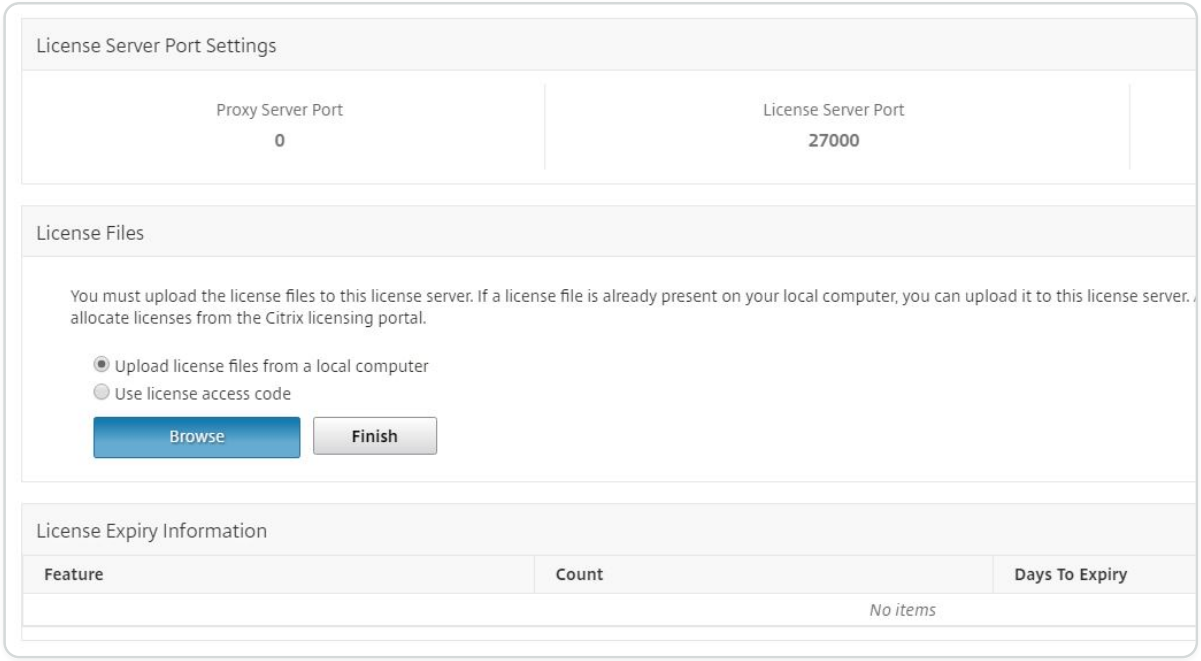
Uploading Licenses in NetScaler ADM

Upload the NetScaler VPX licenses to NetScaler ADM, so that NetScaler ADM can automatically allocate licenses to the instances during orchestration with NSX.

To install license files on NetScaler ADM:

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing**.
2. In **License Files** section, select one of the following options:
   a. **Upload license files from a local computer** - If a license file is already present on your local computer, you can upload it to the NetScaler ADM. To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   b. **Use License Access Code** - Citrix emails the License Access Code for the licenses that you purchase. To add license files, enter the license access code in the text box and then click **Get Licenses**.

> **NOTE**
>
> At any time, you can add more licenses to the NetScaler ADM from the License Settings.



Uploading NetScaler VPX Images in NetScaler ADM

Add the NetScaler images to NetScaler ADM, so that the NetScaler ADM uses these images as defined in the service package.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To upload NetScaler VPX Images in NetScaler ADM:

1. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **ESX NSVPX Images**.
2. Click **Upload**, and select the NetScaler VPX zip package from the local storage folder.

Creating Service Packages in NetScaler ADM

Create service packages in NetScaler ADM to define the set of SLAs, which states how the NetScaler resources are allocated.

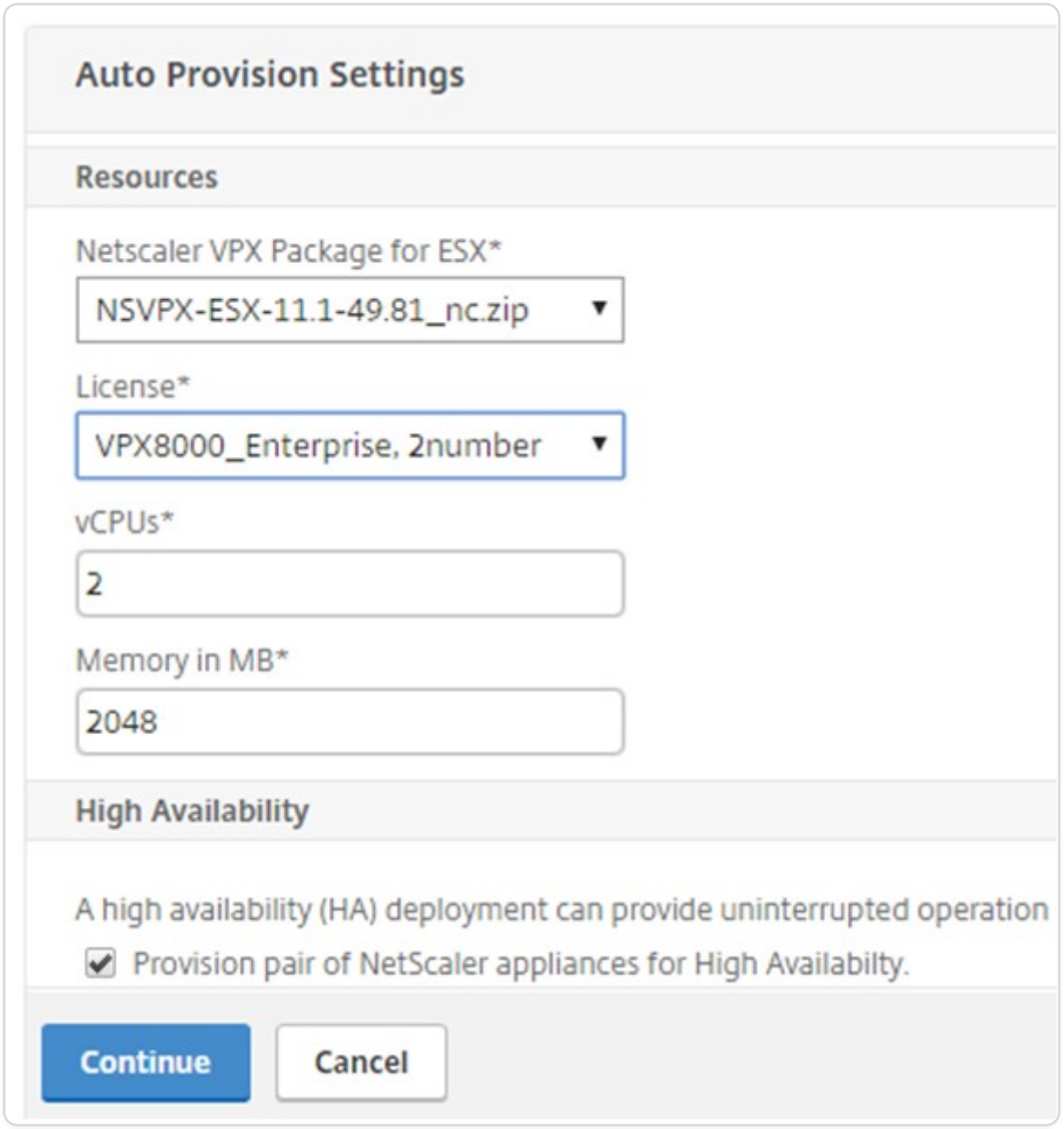
To create service packages in NetScaler ADM:

1. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a. Name - name of a service package
   b. Isolation Policy - select **Dedicated**
   c. NetScaler Instance Provisioning - select **Create Instance OnDemand**
   d. Auto Provision Platform - select **CitrixNetScaler SDX**
   e. Click **Continue**
3. In the **Auto Provision Settings** section, select the recently uploaded NetScaler VPX zip package for deploying it on NSX platform, select the corresponding license, and click **Continue**.

   NOTE

   In **High Availability** section, check the box to provision NetScaler instances for HA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

The name of license displayed in the list box shown in the figure above, VPX8000_Advanced, 2 number is an example and is explained as below:

- VPX - the license is to deploy NetScaler VPX instances
- 8000 - consumable bandwidth is 8GB
- Advanced - NetScaler provides three types of licenses - Standard, Advanced, and Premium
- 2 number - two NetScaler VPX instances can be deployed by using this license

The name of license displayed in the **License** list box depends on the license that you have purchased from Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Continue**.
5. The service package is published to NSX Manager. In NSX Manager, navigate to **Service Definitions** \> **Service Managers**. You can view NetScaler ADM as one of the service managers. This indicates that the registration is successful and bi-directional communication is established between the NSX manager and NetScaler ADM.

> **NOTE**
>
> For NetScaler ADM in high availability deployment, the licenses are uploaded only in the NetScaler ADM license server node. The NetScaler ADM nodes are in an active-passive mode.

Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the existing NSX Edge Gateway, that is, offload the load balancing function from NSX load balancer to NetScaler.

To insert load balancing service on NSX Edge Gateway:

1. In NSX Manager, navigate to **Home** \> **Networking and Security** \> **NSX Edges**, and double-click to select the edge gateway that you have configured.
2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.
3. Select **Enable Load Balancer** and **Enable Service Insertion** to enable them.
4. In **Service Definition**, select the service package that was published to NSX Manager.
5. Configure one virtual NIC for management interface, and one or more virtual NICs for data interfaces. Select the networks for management and data accordingly.

> **NOTE**
>
> Select IP Pool option in Primary IP Allocation mode. NetScaler ADM does not support manual or DHCP allocation of IP addresses.

6. Click the refresh icon to see the creation of the run time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Because you are deploying two NetScaler VPX instances in HA deployment, two run times are created in the NSX manager.

You might have to refresh the screen to view the run times displayed on the screen.

7. Select the run time, click **Actions**, and select **Install** from the pop-up menu. For HA, repeat this for the other run time also.
8. When both the virtual machines start, the value of Status changes to "In Service" and that of Install State changes to "Enabled."

NOTE

You might have to refresh the screen to view the change in status.

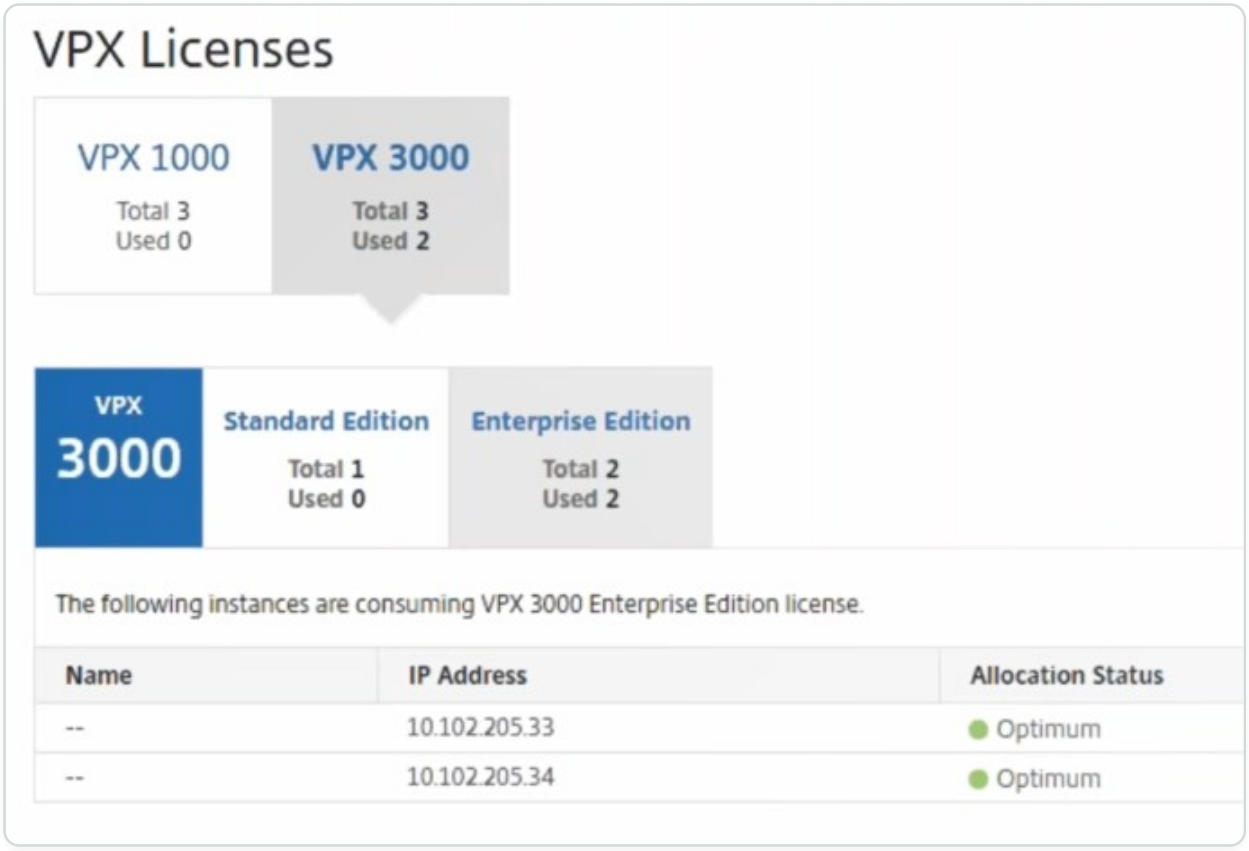
9. In NetScaler ADM, navigate to **Orchestration** \> **Requests** to see progress details of completion of service insertion. You can see that a request to create and update the run time has come in to NetScaler ADM. When the run time has been updated, select the request and click the **Tasks** button to view that NetScaler ADM has been added in NSX Manager.

   For HA, there will be two requests to create and update two run times in NetScaler ADM. When both run times have been updated, select both requests and click the **Tasks** button to view that two NetScaler ADM HA nodes have been added in NSX Manager.
10. In NetScaler ADM, navigate to **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Edge Gateways**. In the right-hand side panel, you can view that the NetScaler VPX has been added to the NSX Edge Gateway.

    For HA, you can see that two NetScaler VPX instances in HA mode have been added to the NSX Edge Gateway.
11. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**. Select the NetScaler VPX license and the edition that you have installed.

    The NetScaler VPX instances that are in HA mode consume two licenses and the status is displayed on your screen as below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When the service insertion is complete, you can use StyleBooks to configure the NetScaler instances in one of the following two methods:

- Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI
- Configuring Load Balancing Services on NetScaler VPX in NetScaler ADM GUI

Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI

Perform the following task to enable configuration of load balancing services on the NSX Edge gateway device using built-in StyleBooks.

In NSX Manager, navigate to **Home** \> **Networking and Security** \> **NSX Edges**, and double-click to select the edge gateway that you have configured.

Creating pools and pool members

Create a pool of servers and members of different capacities.

1. Click **Manage**, and on the **Load Balancer** tab, select **Pools**, and click "**+**" icon to add a new pool, and set the following parameters:

   a. Name - Name of the new pool

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Algorithm - Select an algorithm from the drop-down list base on which the pool will be selected.

c. Monitors - Make sure the service monitor is set to default_http_monitor

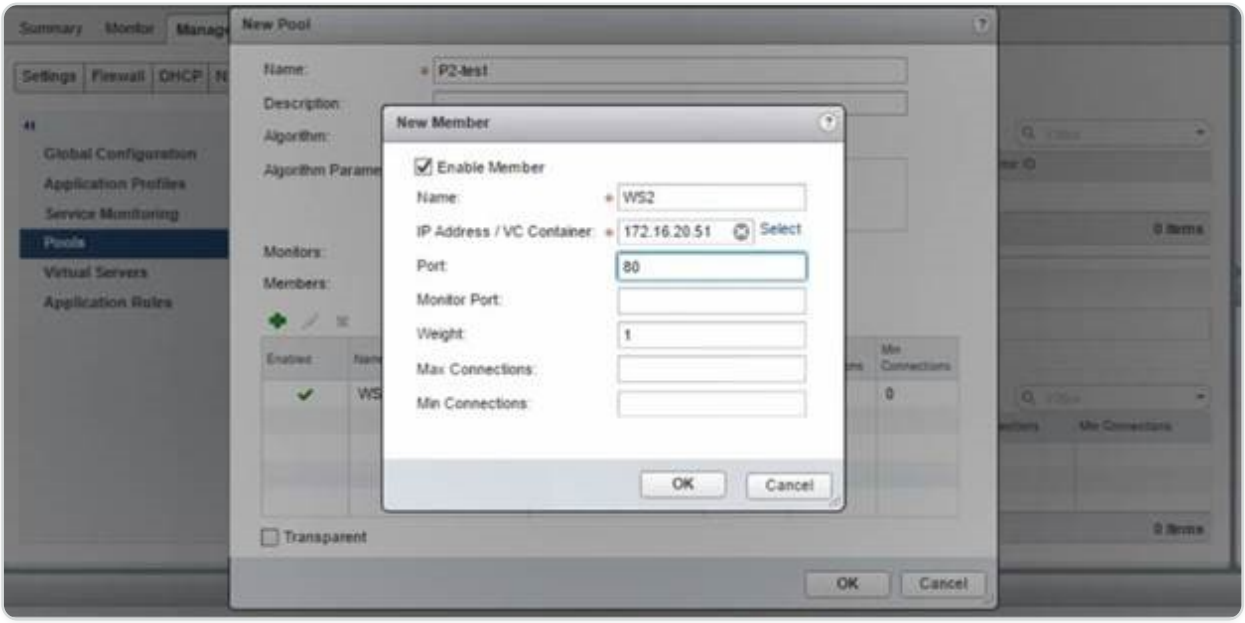
d. Members - Click "+" to add members to the pool and enter the required parameters in the New Member window.

   i. Name - Name of the member

   ii. IP Address/ VC Container - Click Select to select the object from the available list or enter the IP address of the object.

2. Click **OK**.

   Add as many members as required.



Creating virtual servers

Create a set of virtual servers and assign a pool to each virtual server.

1. Click **Manage**, and on the Load Balancer tab, select **Virtual Servers**, and click "**+**" icon to add a virtual server, and set the following parameters:

   a. Application profile - By default, the service profile that you created in NetScaler ADM is displayed.

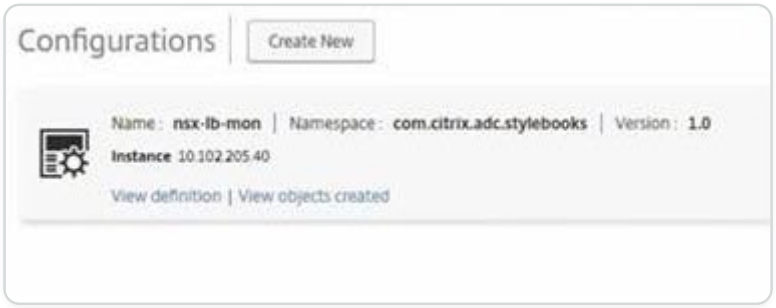
   b. Name - Name of the virtual server.

   c. IP Address - Click Select to select an existing pool of IP addresses or create a new pool of IP addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Default pool - Select the default pool from the drop-down list.

2. Click **OK**.
3. In NetScaler ADM, navigate to **Orchestration** \> **Requests** to see progress details of completion of service creation on one or more selected NetScaler instances.
4. In NetScaler ADM, navigate to **Applications** \> **Configuration**, and check that the `nsx-lb-mon` config pack has been created.



Configuring Load Balancing Services on NetScaler VPX in NetScaler ADM GUI

Deploy load balancer configurations on the NetScaler instance using NetScaler ADM StyleBooks. For HA, the configuration is deployed on both NetScaler instances that are in HA.

To create configuration packs through StyleBooks:

1. In NetScaler ADM, navigate to **Applications** \> **Configuration** \> **Create New**, and select the **HTTP/SSL LoadBalancing (with Monitors) StyleBook** from the list. The StyleBook opens as a user interface page on which you enter the values for all the parameters defined in this StyleBook.
2. Specify values for all the required parameters.
3. Select the target NetScaler VPX instance that is provisioned in the NSX environment, and click **Create** to apply the configuration on the selected device. For HA deployment, select the instances that are in HA mode.

Verifying Creation of Virtual Servers and Service Groups in NetScaler VPX Instances

You can view that the service groups and virtual servers are created by login on to the NetScaler VPX instance.

To view the service groups and virtual servers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to the NetScaler VPX instance. For HA deployment, you must log on to both NetScaler instances that are in HA.
2. Navigate to **Configuration** \> **System** \> **Networking**. In the right pane, you can view the IP addresses that are added. Click the IP address hyperlink to see the details. You can see that the subnet IP address is same as the IP address of the web interface that was added in NSX.
3. Next, navigate to **Traffic Management** \> **Load Balancing** \> **Virtual Servers** and view the virtual server details.
4. Next, navigate to **Service Groups** and view the service group details.
5. Finally, navigate to **Configuration** \> **System** \> **Licenses** to view the licenses that are applied to this instance.

Deleting Load Balancing Services

When the load balancing services are no longer required on the NetScaler VPX instances deployed on the NSX manager, you can delete the service insertions that were performed earlier.

To delete configuration and service insertion:

1. In NetScaler ADM, Navigate to **Applications** \> **Configuration**, select the application configuration created, and then delete the configuration by clicking the "X" icon.
2. In NSX Manager, navigate to the edge gateway to which the NetScaler VPX instance is connected. Navigate to **Manage** \> **Load Balancer** \> G**lobal Configuration**, right-click on the runtime entry, and then click **Unprovision**. The virtual machine is rendered out of service.
3. In NetScaler ADM, navigate to **Orchestration** \> **Cloud Orchestration** \> **Edge Gateways**. Ensure there is no respective mapping of Edge gateway to deleted instance.

NetScaler automation using NetScaler ADM in Cisco ACI hybrid mode

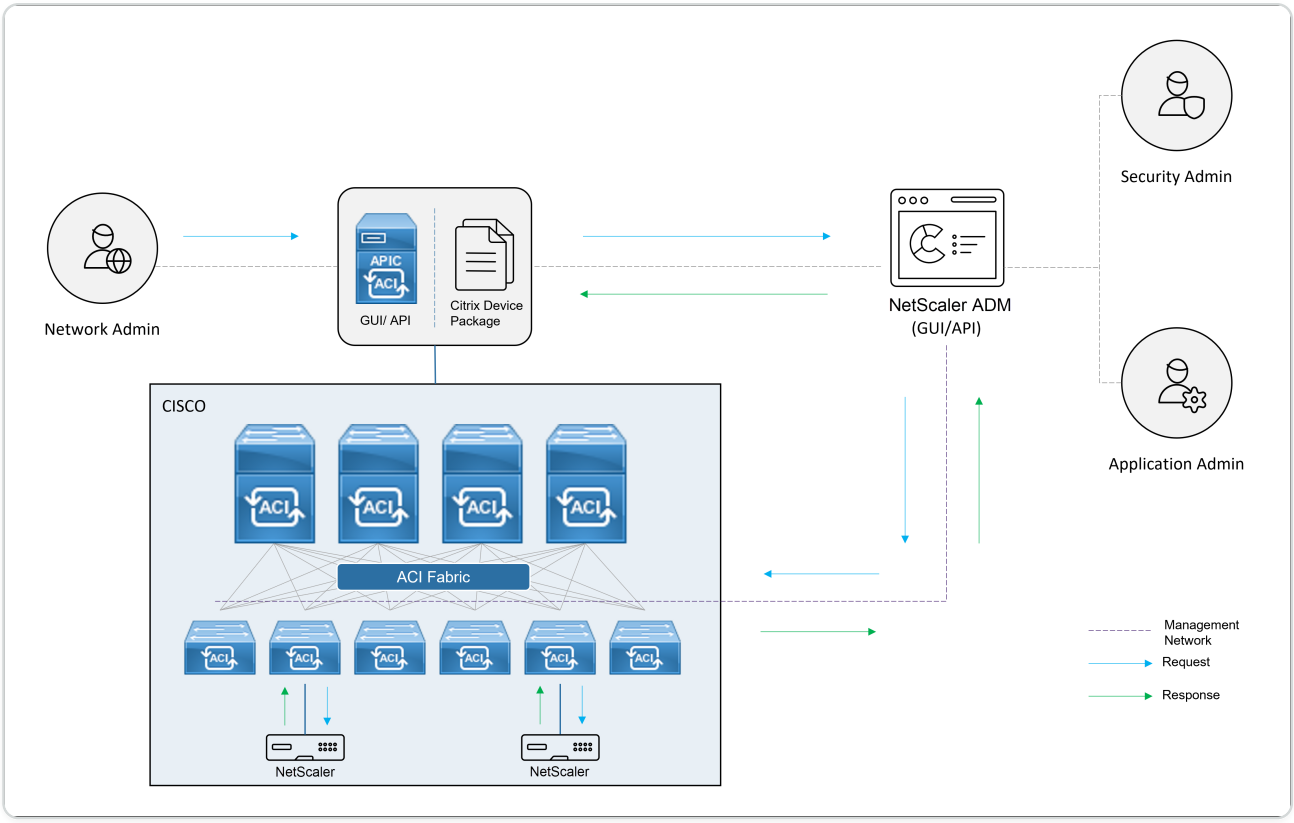
Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to NetScaler Application Delivery Management (ADM), which acts as a Device Manager in the APIC.

The NetScaler Hybrid Mode solution is supported by a hybrid mode device package and NetScaler ADM. You need to upload the hybrid mode device package in the APIC. This package provides all network L2-L3 configurable entities from NetScaler. Application parity is mapped by StyleBook from NetScaler ADM to the APIC. In other words, StyleBook acts as reference between L2-L3 and L4-L7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configurations for a given application. You must provide a StyleBook name while configuring the network entities from the APIC for NetScaler.

The following illustration provides an overview of NetScaler in a hybrid mode solution:



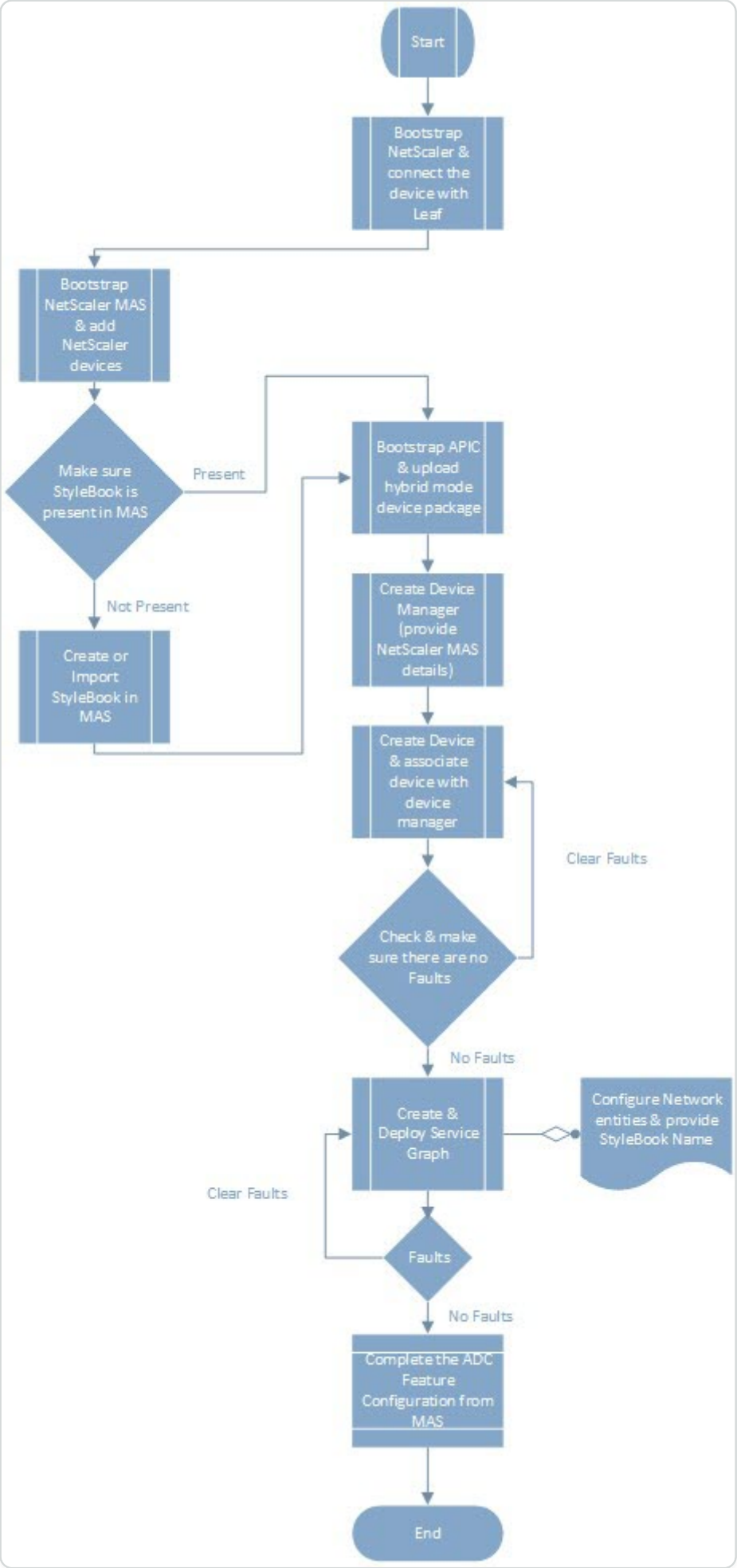
In Hybrid Mode, the NetScaler configuration is performed in the following two phases:

1. Network stitching is done from the Cisco APIC
2. Configuration is done from the NetScaler® ADM

For any given application, a network administrator has to provide network specific details, such as IP addresses, port, VLAN (automated) and so on, as part of the service graph creation and deployment in the Cisco APIC. These configuration details are then pushed to NetScaler ADM through the device package, and NetScaler ADM internally processes them and configures the NetScaler. An application administrator creates the application's ADC related configuration by using StyleBook in NetScaler ADM, and these configurations are then pushed from NetScaler ADM to the NetScaler. The Cisco APIC and NetScaler ADM communicate with the ADC through the management network.

The following diagram shows a NetScaler workflow in the hybrid solution:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

Ensure that:

- You have conceptual knowledge of Cisco ACI components and NetScalers.
  - 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>`.
  - For more information about the NetScalers, see the NetScaler 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 NetScaler 11.1 or later.
- You have configured NetScalers in Cisco ACI so that they can be managed by using the Cisco APIC.
- You have deployed NetScaler Application Delivery Management (ADM) in your environment. For more information, see NetScaler ADM 13.1.
- Management connectivity from APIC to NetScaler® 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: NetScaler IP addresses, ports, interfaces, and so on.

NOTE

In this release, the hybrid mode solution supports NetScaler in a single-context, that is, admin partitions are not supported.

Configure NetScaler in hybrid mode using Cisco APIC and NetScaler ADM

Perform the following tasks to configure a NetScaler in Hybrid Mode by using Cisco APIC and NetScaler Application Delivery Management (ADM):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Add NetScaler instances in your fabric to NetScaler ADM. For instructions, see Adding an Instance to NetScaler ADM.
2. Use NetScaler ADM to create a StyleBook for the application. For instructions, see Creating a StyleBook for the Application Using NetScaler ADM.
3. Import the NetScaler hybrid mode device package into Cisco APIC. For instructions, see Importing the NetScaler Hybrid Mode Device Package into Cisco APIC
4. Add NetScaler ADM as a device manager in the Cisco APIC. For instructions, see Adding NetScaler ADM as a Device Manager in Cisco APIC
5. Use Cisco APIC to add a NetScaler device in Cisco ACI. For instructions, see Adding the NetScaler 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 NetScaler ADM. For instructions, see Configure L4-L7 parameter using StyleBook from NetScaler 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 NetScaler ADM

A StyleBook is a configuration template that you can use to create and manage NetScaler configurations for any application. You can create a StyleBook for configuring a specific NetScaler 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 NetScaler Application Delivery Management (ADM).

To create your own StyleBook for your application in NetScaler ADM, see How to Create Your Own StyleBooks.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler hybrid-mode device package into Cisco APIC

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 NetScaler deployment in the fabric (for example, one-arm and two-arm and the same with RHI). The Hybrid Mode Device package name is **NetScaler Hybrid Mode Device package 12.0 Build 56.20**. Search for the Hybrid Mode device package in the NetScaler site, download it, and import the device package to the APIC.

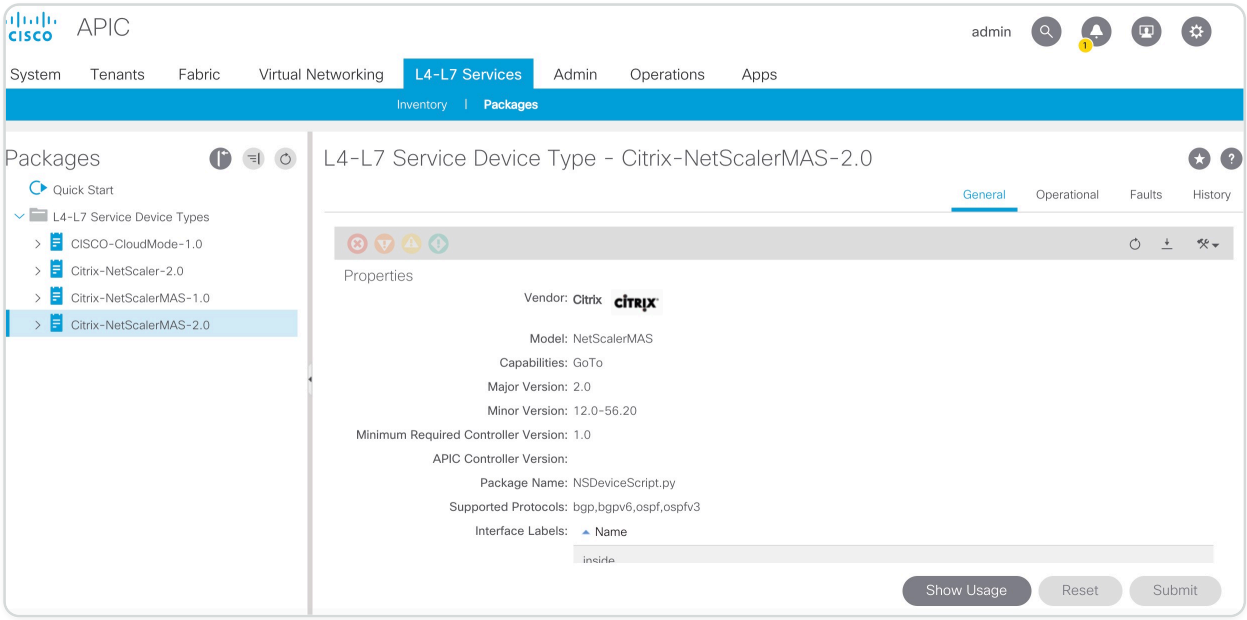
NOTE

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 NetScaler 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 the device name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

Add NetScaler ADM as device manager in Cisco APIC

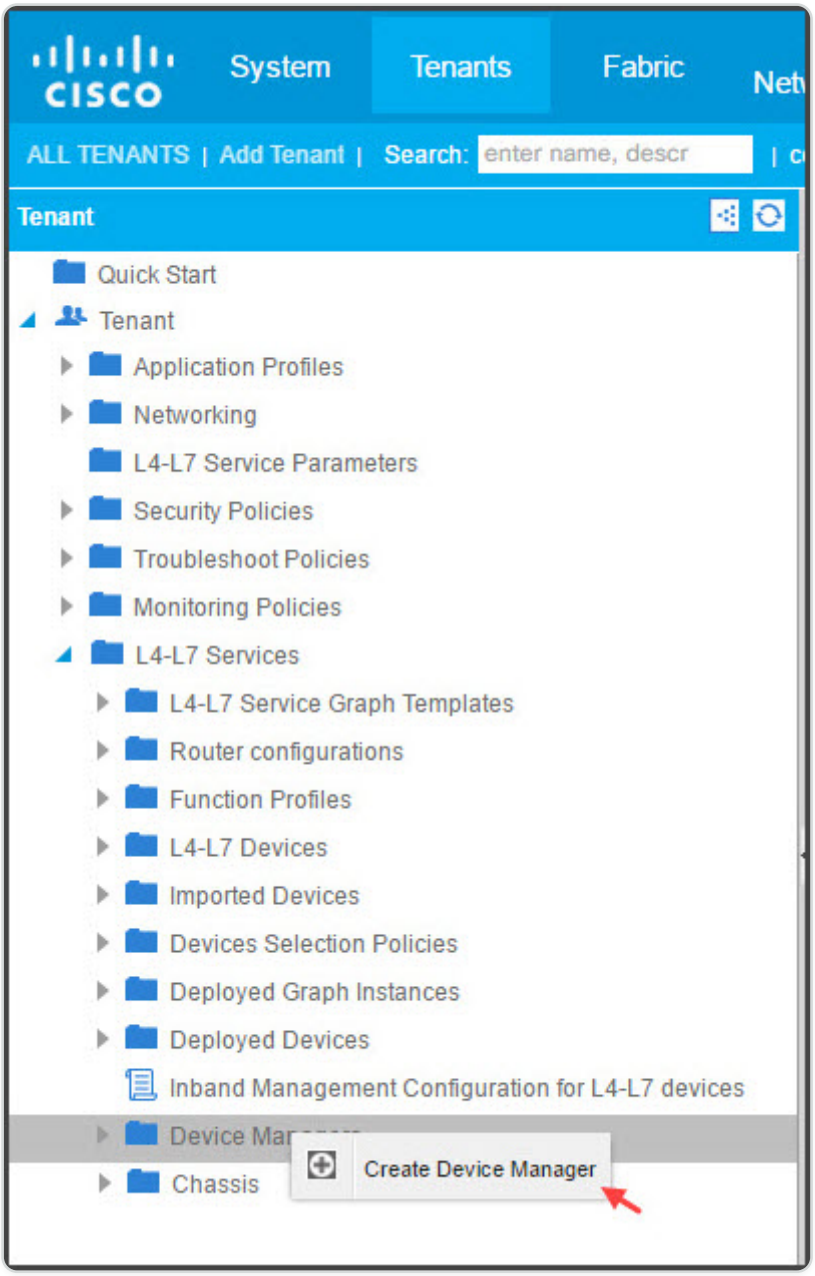
May 24, 2018

NetScaler Application Delivery Management (ADM) acts as a centralized device manager for NetScaler deployed on Cisco ACI. You need to add NetScaler ADM as a device manager in the Cisco APIC.

To add NetScaler ADM as a device manager in the APIC 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**.
4. Right-click on **Device Managers** and click **Create Device Manager**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. In the **Create Device Manager** dialog box, do the following:

   a. In the **Device Manager Name** field, enter a name for the NetScaler ADM deployment that you want register as a device manager.

   b. In the **Management EPG** drop-down list, select the management EPG.

   c. In the **Device Manager Type** drop-down list, select **Citrix-DevMgr-1.0**.

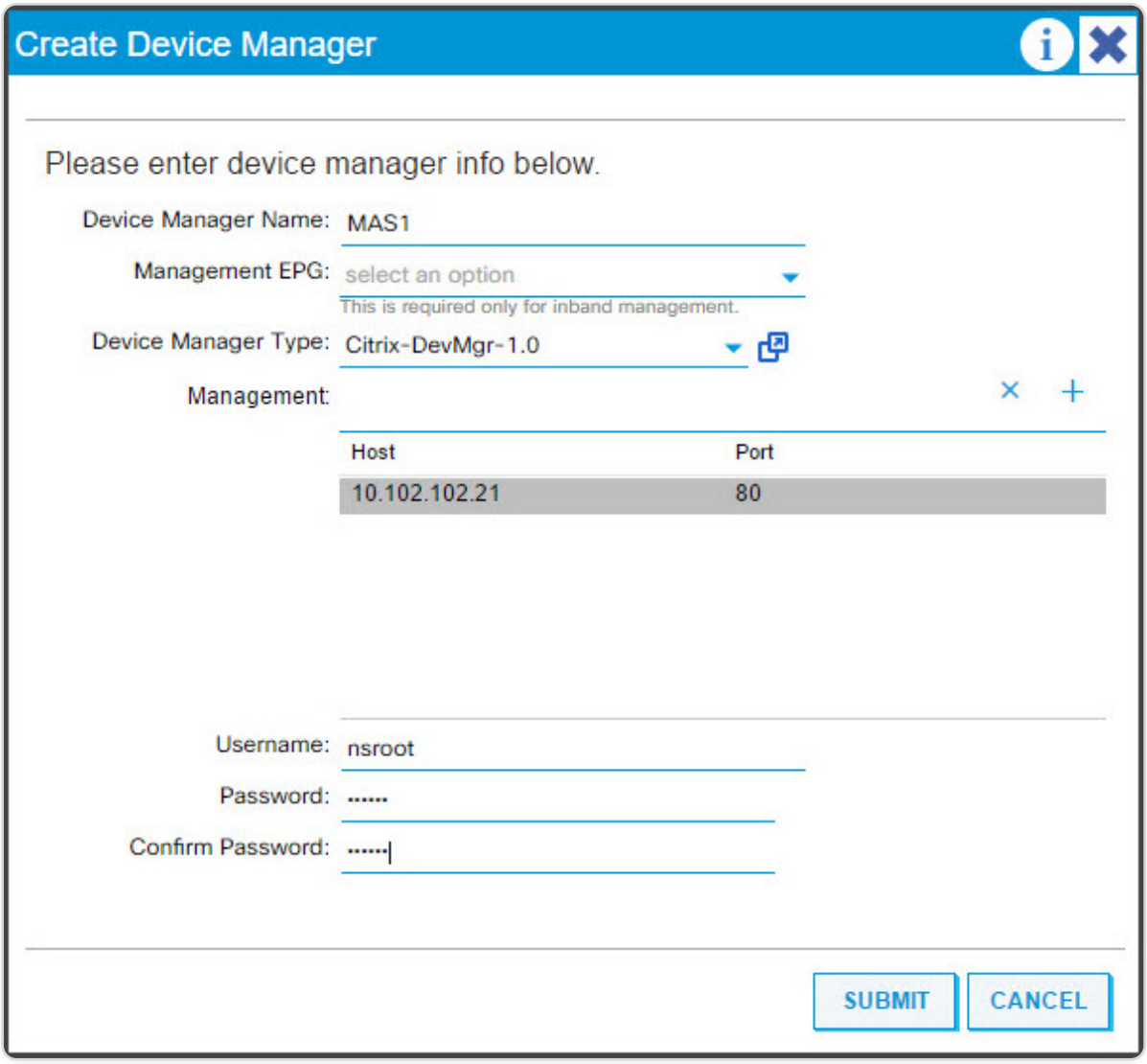
   d. In the **Management** field, click **+** and add the IP address and port details of the NetScaler ADM deployment.

   e. In the **Username** field, enter the user name to access NetScaler ADM.

   f. In the **Password** and **Confirm Password** fields, enter the password to access NetScaler ADM.

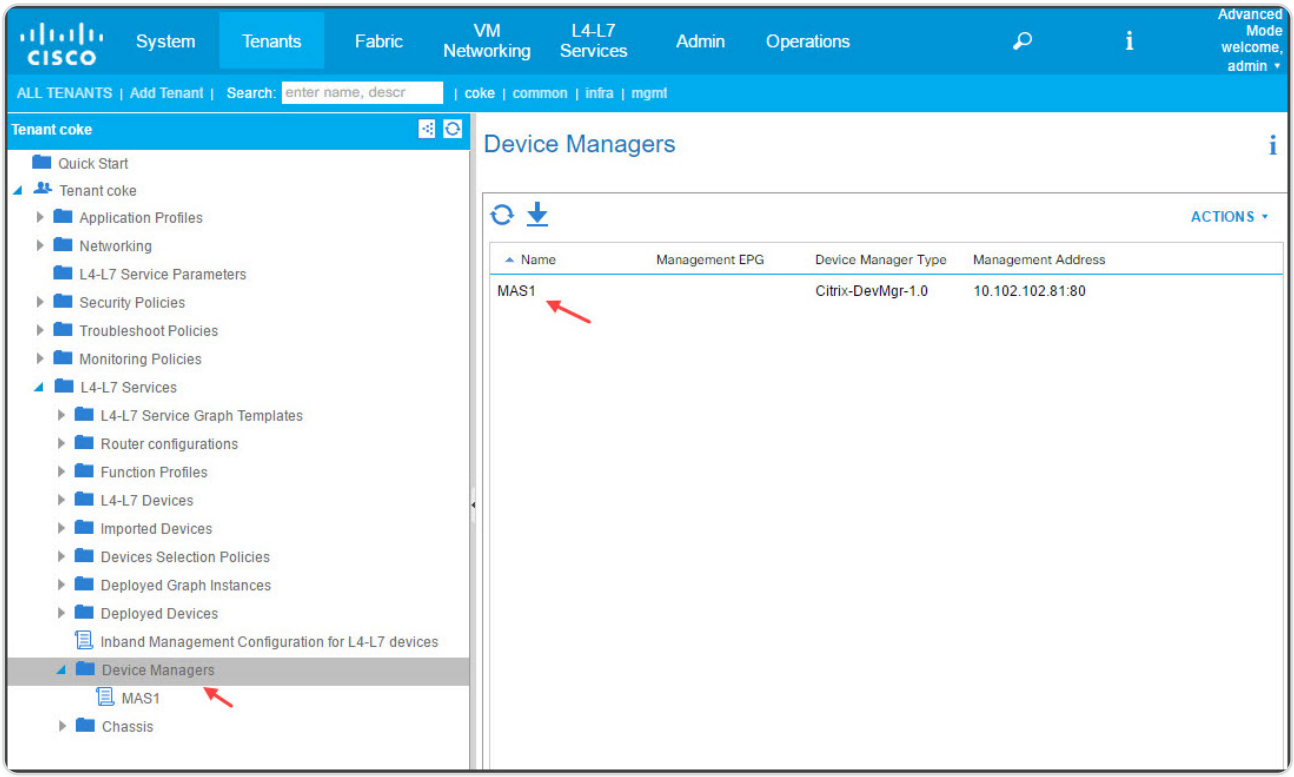
© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. Click **SUBMIT**.



Once the NetScaler ADM is successfully registered as a device manager in the APIC, the device manager is added and is displayed in the **Navigation** pane. To view the registered device manager, in the Navigation pane, go to ***tenant_name* \> L4-L7 Services \> Device Manager**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

Make sure that there are no connectivity issues between the Cisco APIC and NetScaler ADM and that you provide the same credentials that you use to access the NetScaler ADM. Also make sure that the account has admin privileges.

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.

You can also register NetScaler ADM as a device manager by using APIs. Following is a sample XML payload that shows how you can use APIs to add NetScaler ADM as a device manager.

```
&lt;polUni>

    &lt;fvTenant name="coke">

        &lt;vnsDevMgr name="MAS1">

            &lt;vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-
DevMgr-1.0" />

            &lt;vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            &lt;vnsCCred name="username" value="nsroot"/>

            &lt;vnsCCredSecret name="password" value="*****("/>

        &lt;/vnsDevMgr>

    &lt;/fvTenant>

&lt;/polUni>
```

Add NetScaler as a device in Cisco ACI using APIC

You need to add a NetScaler as an L4-L7 device to the APIC for the network automation. The APIC performs network stitching between Leaf and the NetScaler device, based on the deployed service graph. You need to configure the basic settings of the device configuration, such as configuration management IP addresses, device manager, and credentials.

To register the NetScaler as a device in the APIC 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 Devices**.
4. In the Work pane, select **Actions \> Create L4-L7 Devices**.
5. In the **Create L4-L7 Devices** dialog box, in the **General** section, do the following:
   a. Select the **Managed** check box.
   b. In the **Name** field, enter a name for the device.
   c. In the **Service Type** drop-down list, select **ADC**.
   d. In the **Device Type** field, select **Physical**.

      NOTE

      Make sure that for VMware ESX, you select Virtual and associate the respective Virtual Machine Manager (VMM) domain.

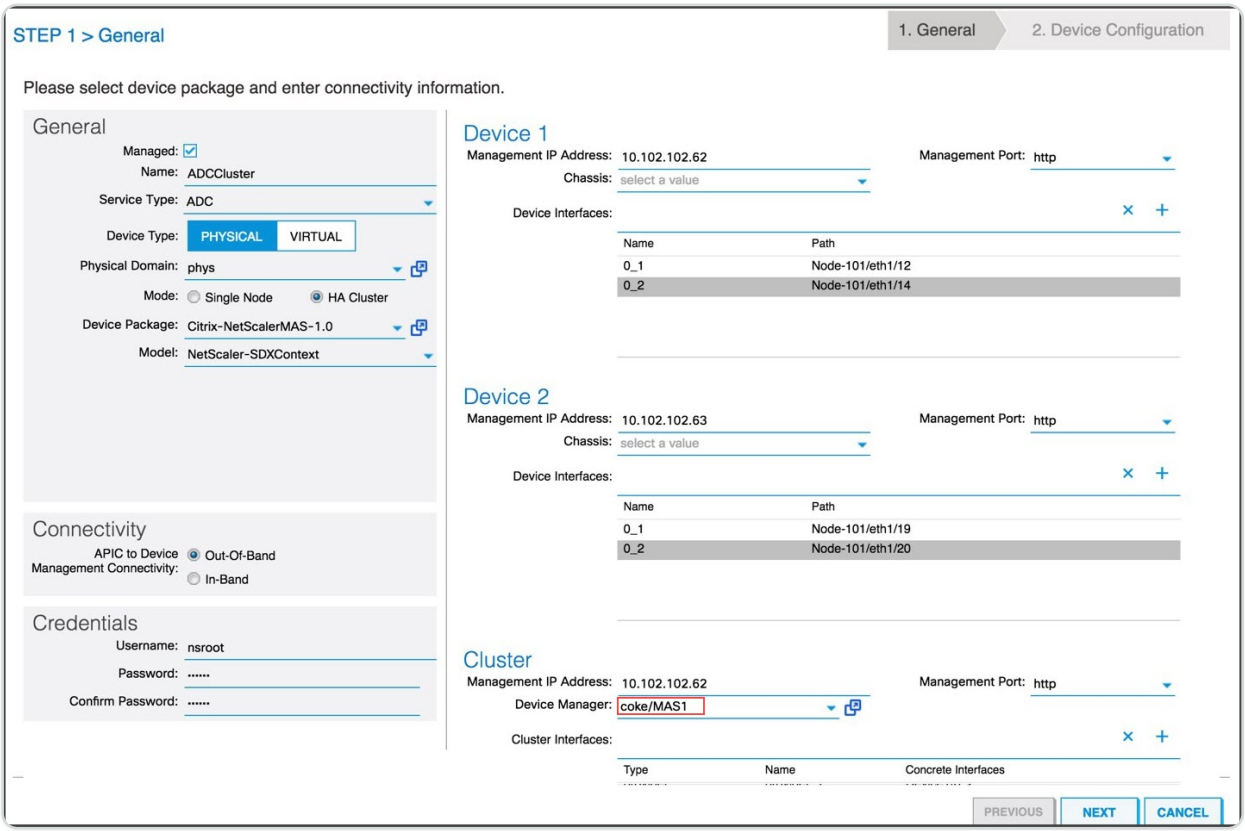
   e. In the **Physical Domain** drop-down list, select the physical domain.
   f. In the **Mode** field, select **Single Node** or **HA Cluster**, depending on your requirement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. In the **Device Package** drop-down list, select **Citrix-NetScalerMAS-1.0**.

h. In the **Model** drop-down list, select the device model. For example, NetScaler-MPX, or NetScaler-VPX.

6. In the **Connectivity** section, select **Out-Of-Band** or **In-Band** in the **APIC to Device Management Connectivity** field, depending on how NetScaler is configured in the fabric.
7. In the **Credentials** section, specify the user name and password for access to the device.
8. In the **Device 1** and **Device 2** section, respectively, complete the management related configuration.
9. In the **Cluster** section, complete the management related configuration for the cluster. Make sure that in the **Device Manager** drop-down list, you select the device manager you created in Adding NetScaler ADM as a Device Manager in Cisco APIC

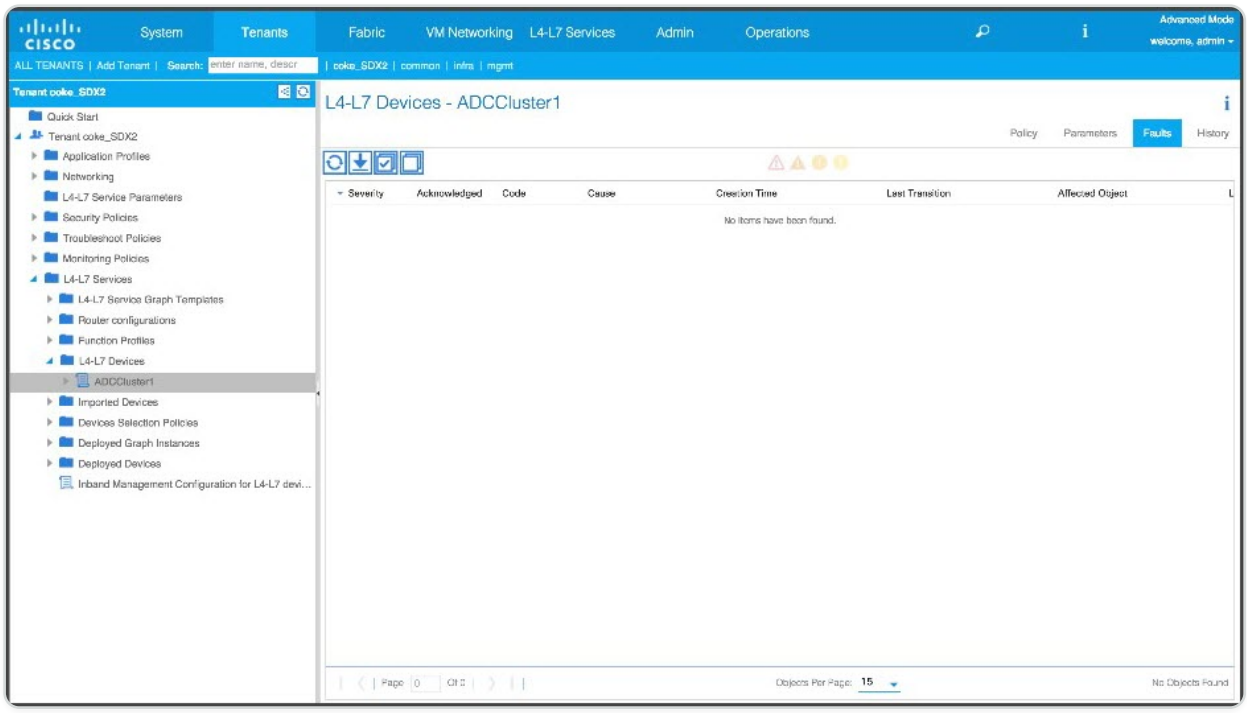


10. Click **NEXT**. The Device Configuration page appears. The hybrid mode device package does not provide device and cluster specific configuration details such as high-availability, enable/disable features and modes, configuration for NTP, SNMP, SNMP Alarms, and so on. These configurations must be done by using NetScaler ADM.
11. Click **FINISH**. When you have successfully registered the device in the APIC, the device is added and is displayed in the Navigation pane. To view the registered device, in the Navigation pane, go to ***tenant_name* \> L4-L7 Services \> L4-L7 Devices \> device_name**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

After you register the device, make sure that there are no faults in the APIC. You can view the faults by clicking the **Faults** tab in the **Work** pane.



You can also register a NetScaler device by using APIs. The following is a sample XML payload for adding L4-L7 Device:

```
&lt;polUni>


    &lt;fvTenant name="coke">


    &lt;vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">


     &lt;vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />


     &lt;vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    &lt;vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

    &lt;vnsCCred name="username" value="nsroot"/>

    &lt;vnsCCredSecret name="password" value="****"/>

    &lt;vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

    &lt;vnsCDev name="ADC1" devCtxLbl="C1">

    &lt;vnsCIf name="1_1">

    &lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/33]"/>

    &lt;/vnsCIf>

    &lt;vnsCIf name="1_2">

    &lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/35]"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    &lt;/vnsCIf>

    &lt;vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>

    &lt;vnsCCred name="username" value="nsroot"/>

    &lt;vnsCCredSecret name="password" value="****"/>

    &lt;/vnsCDev>

    &lt;vnsCDev name="ADC2" devCtxLbl="C1">

    &lt;vnsCIf name="1_1">

    &lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/34]"/>

    &lt;/vnsCIf>

    &lt;vnsCIf name="1_2">

    &lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/36]"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    &lt;/vnsCIf>

    &lt;vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>

    &lt;vnsCCred name="username" value="nsroot"/>

    &lt;vnsCCredSecret name="password" value="****"/>

    &lt;/vnsCDev>

    &lt;vnsLIf name="outside">

    &lt;vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
mIfLbl-outside"/>

    &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
cIf-1_1"/>

    &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
cIf-1_1"/>

    &lt;/vnsLIf>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    &lt;vnsLIf name="inside">


    &lt;vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
mIfLbl-inside"/>


    &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
cIf-1_2"/>


    &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
cIf-1_2"/>


    &lt;/vnsLIf>


    </vnsLDevV


    &lt;/fvTenant>


    &lt;/polUni>
```

Create and deploy a service graph

You have to use Cisco APIC service graph templates in APIC to create and deploy the NetScalers. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

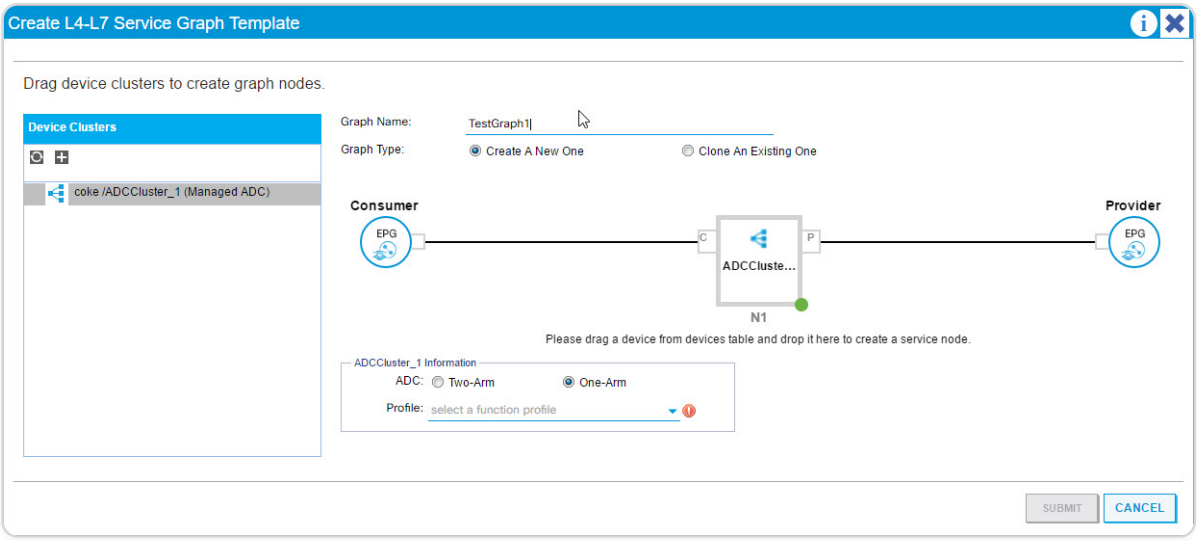
To create a service graph by using the APIC GUI:

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.

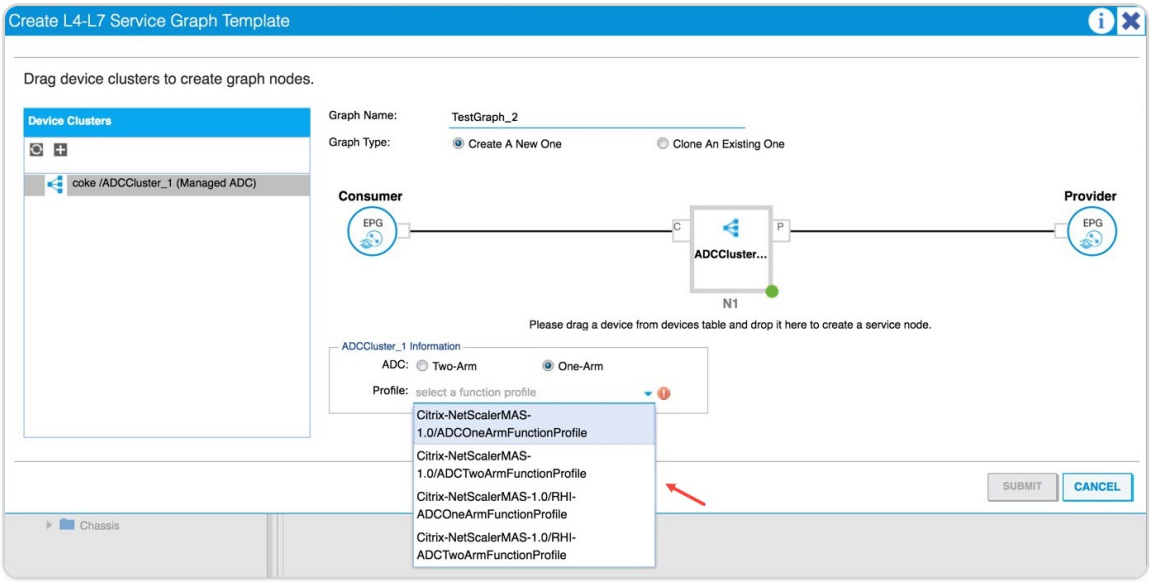


   d. In the \<***L4-L7device_name information***\> section, do the following:

      i. In the **ADC** field, select **One-Arm** or **Two-Arm**, depending on how the NetScaler is deployed in the fabric.

      ii. In the **Profile** drop-down list, select the function profile provided in the device package.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

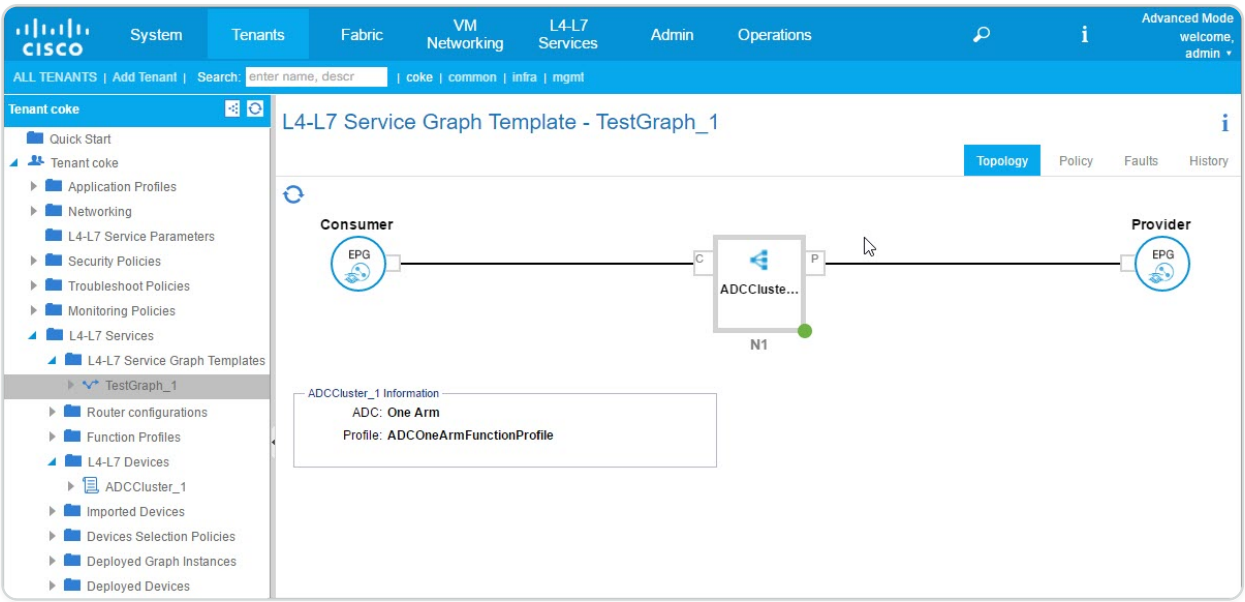


iii. Click **SUBMIT**.

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.



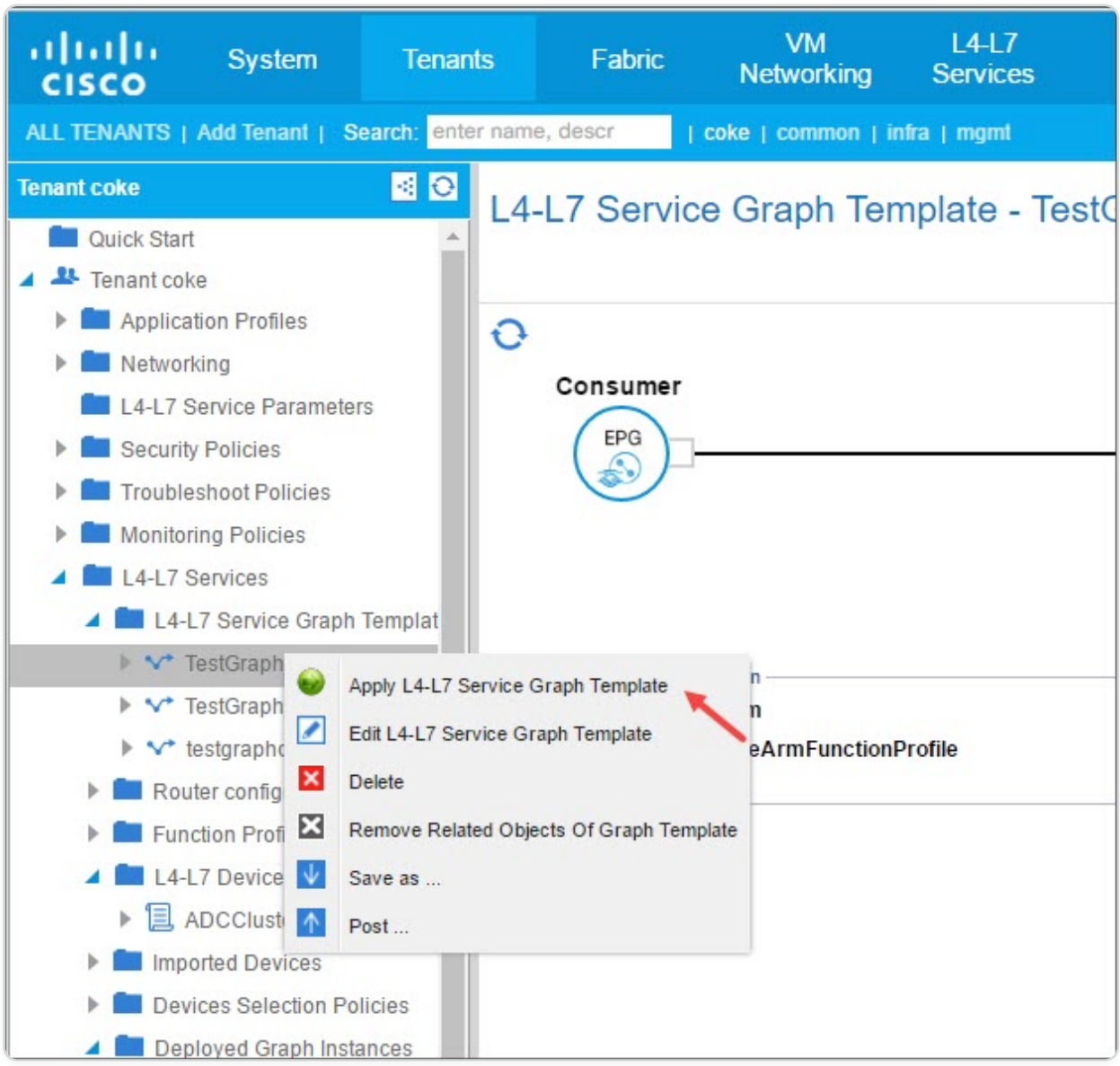
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



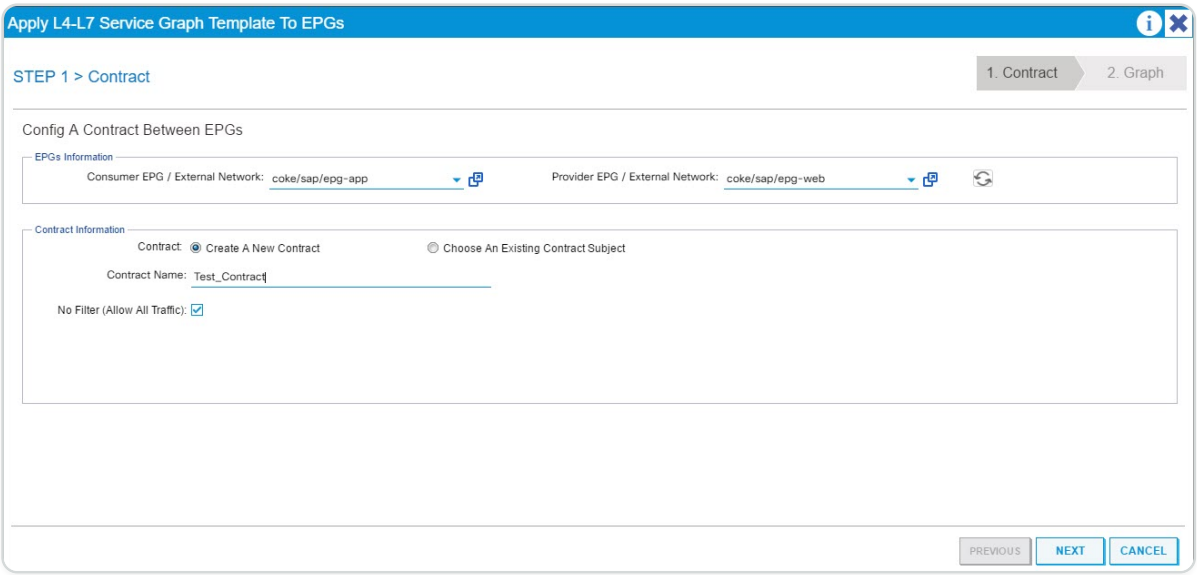
5. In the **Apply L4-L7 Service Graph Template To EPGs** dialog box, in the **EPG Information** section, complete the following fields:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Informatio**n 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:

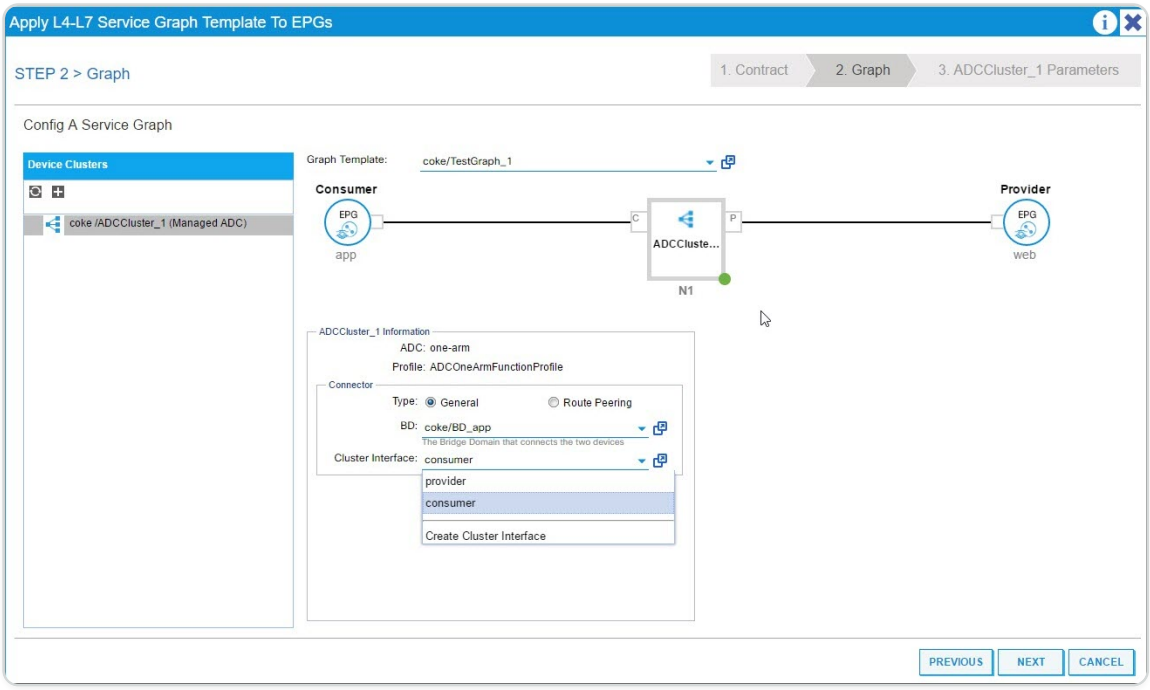
   i. In the **Type** field, select General.

   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 NetScaler device and the fabric as required by the selected service graph template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



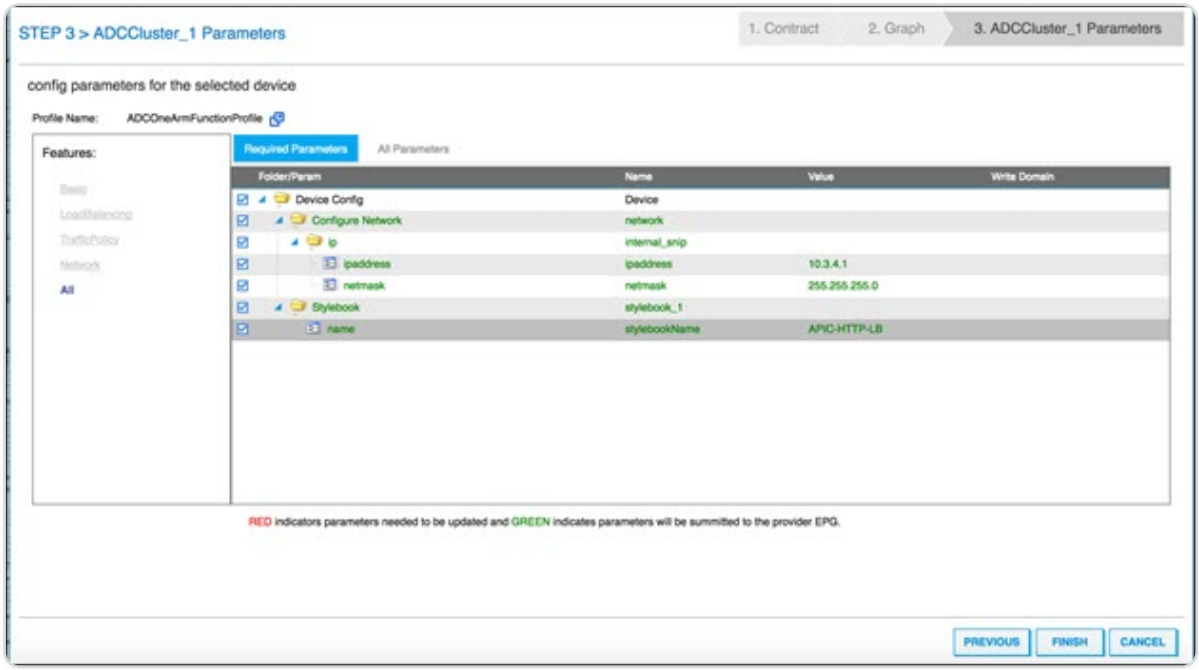
iv. Click **Next**.

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 NetScaler Application Delivery Management (ADM), or you can provide the name of the SytleBook that you created in Creating a StyleBook for the Application Using NetScaler ADM

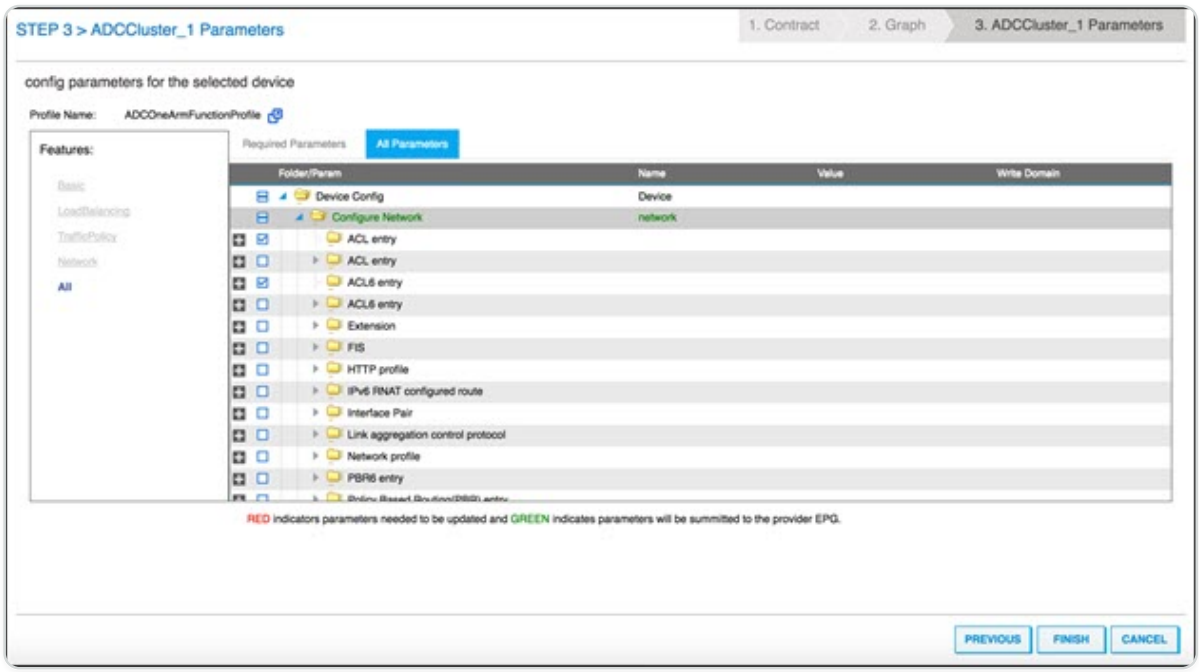
NOTE

The StyleBook name links the Service Graph details with the L4-L7 configuration created with NetScaler ADM for a given application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

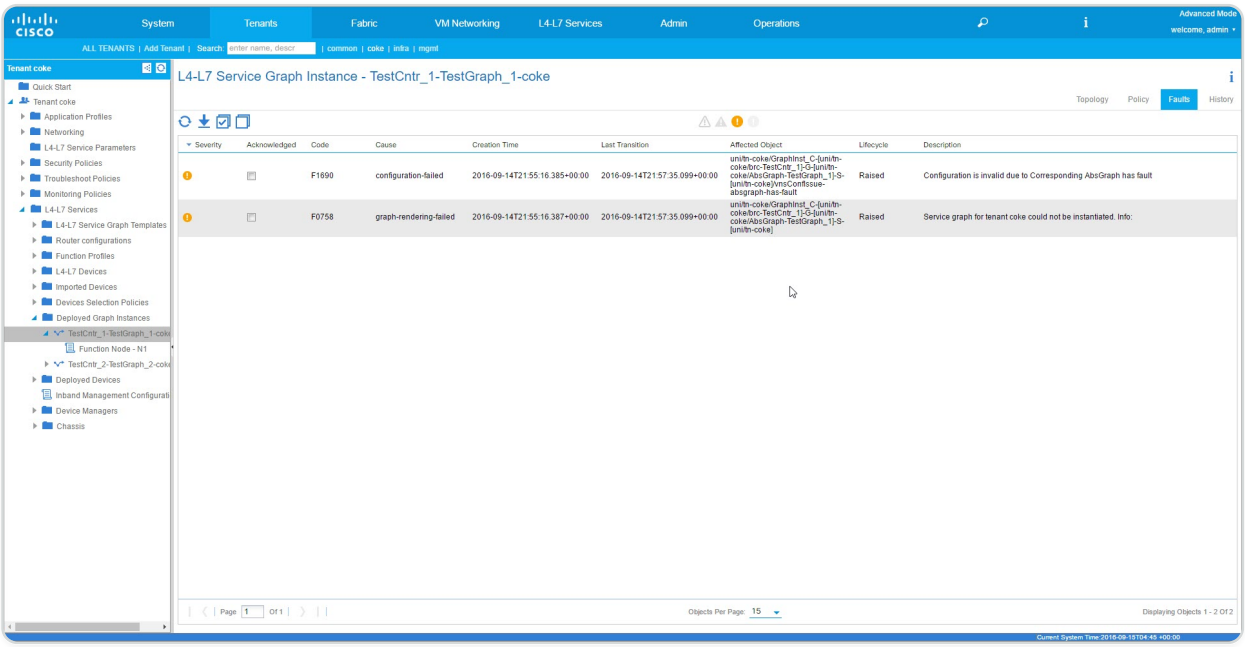
NOTE

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 NetScaler. 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 NetScaler ADM. The NetScaler ADM internally processes these configurations to the respective NetScaler and returns the response to the APIC. A successful graph deployment will have no fault, and the NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler specific entities, attributes, and their values. In the following sample XML payload, NetScaler-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" />

                <!-- --------- CONFIG PAYLOAD ---------------- -->

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network"
name="Network">

                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">

                        <vnsParamInst key="ipaddress" name="ip1"
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">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    <vnsParamInst name="stylebookName" key="name"
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_1">

                    <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"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            </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:

```
<polUni>

    <fvTenant name="coke">

        <vnsAbsGraph name = "Graph1">

            <vnsAbsTermNodeProv name = "Input1">

                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>

            </vnsAbsTermNodeProv>

            <vnsAbsNode name="ADC" funcType="GoTo">

                <vnsAbsFuncConn name = "outside" attNotify="true">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    <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"/>

                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph-
Graph1/AbsTermNodeProv-Input1/outtmnl"/>

                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
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" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            </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>

    </fvTenant>

</polUni>
```

Following is a sample XML payload for attaching the service graph to a contract:

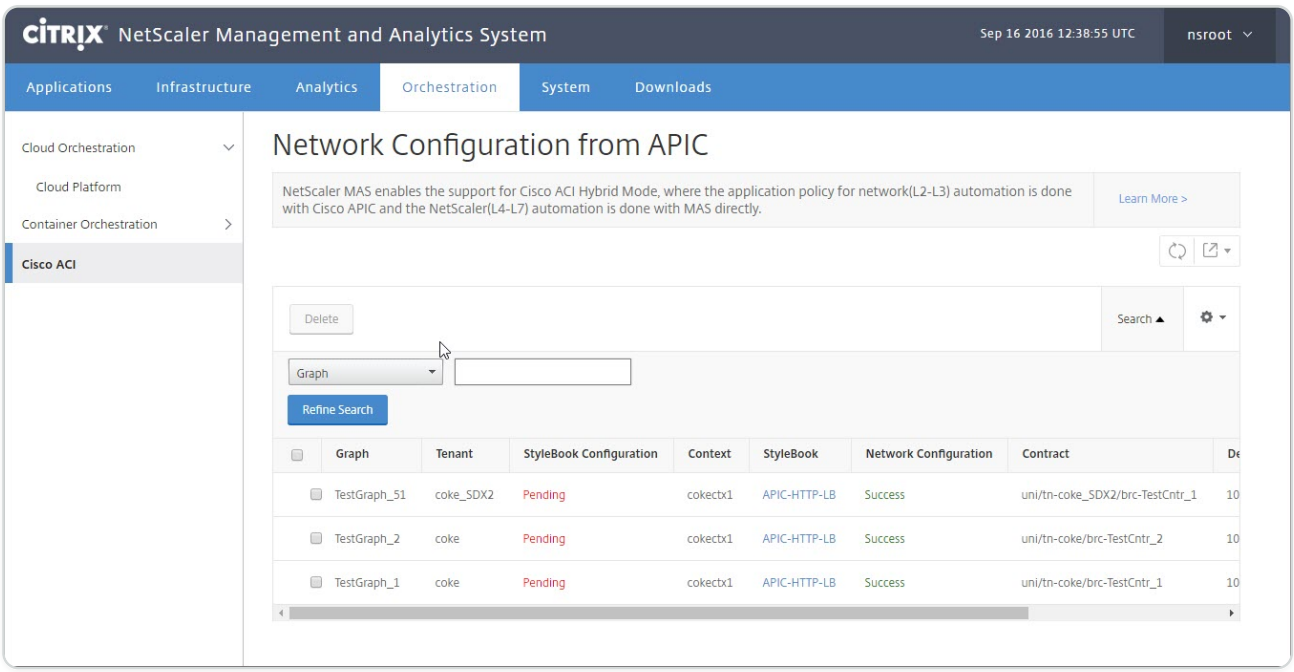
```
<polUni>

    <fvTenant name="coke">

        <vzBrCP name="Ctrct1">

            <vzSubj name="http">

                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>

            </vzSubj>

        </vzBrCP>

    </fvTenant>

</polUni>
```

Configure L4-L7 parameters from NetScaler ADM using StyleBook

May 24, 2018

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In NetScaler 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.

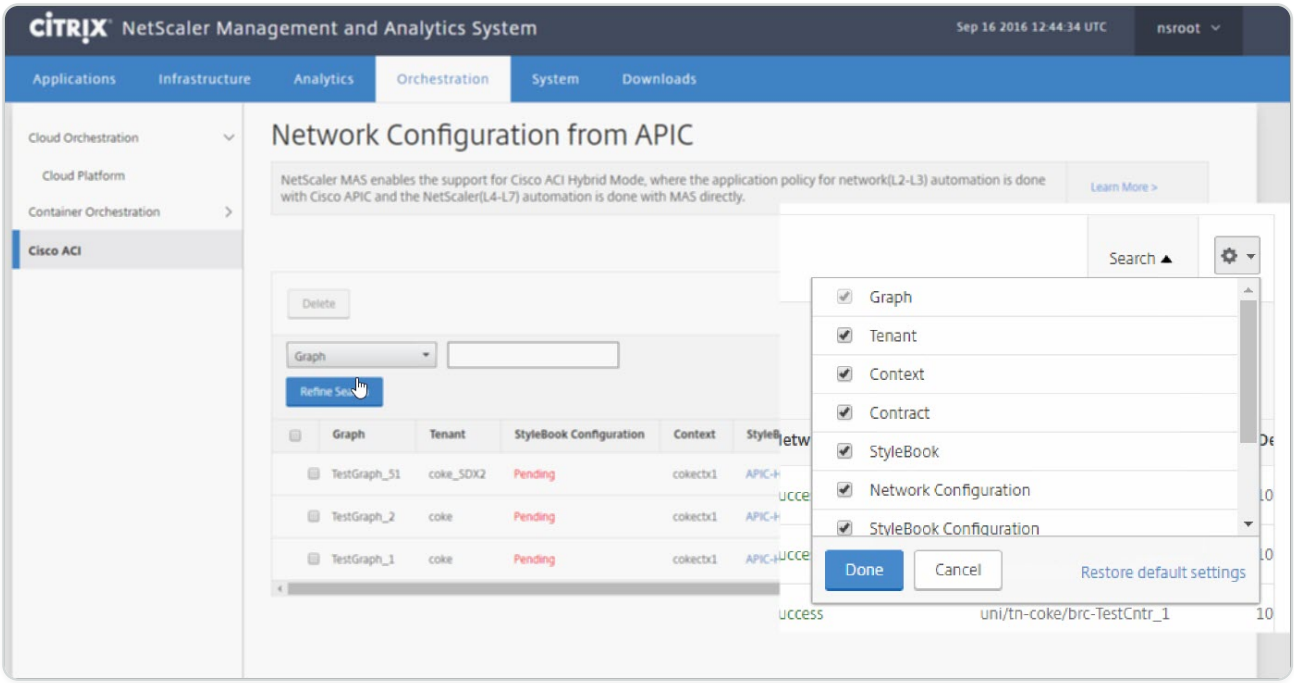


NOTE

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:

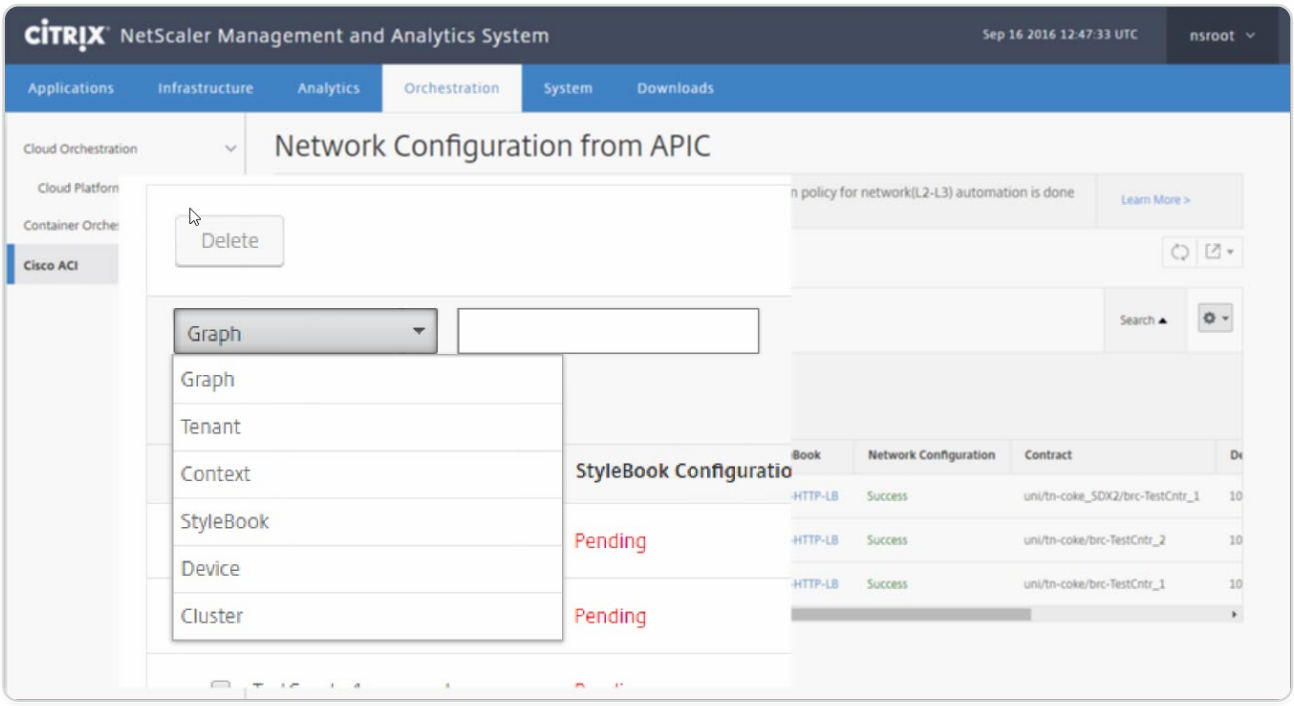
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

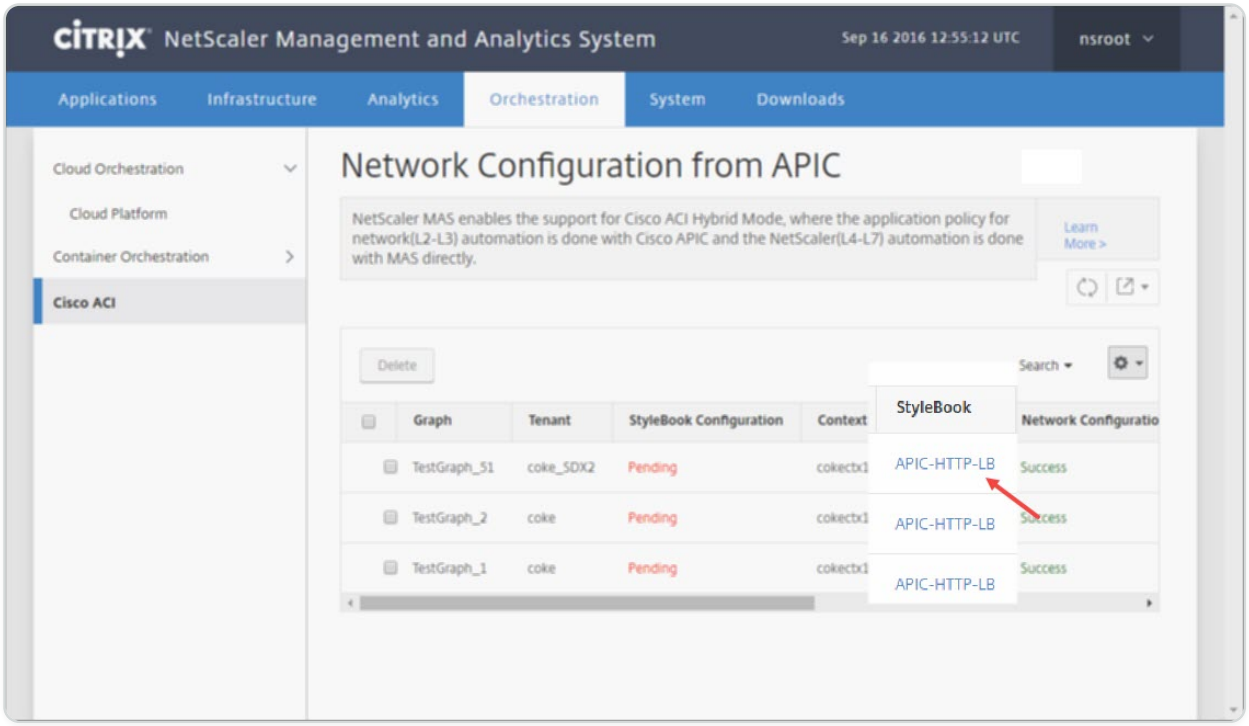
The Search functionality is case-sensitive, and you must provide the exact search criteria.



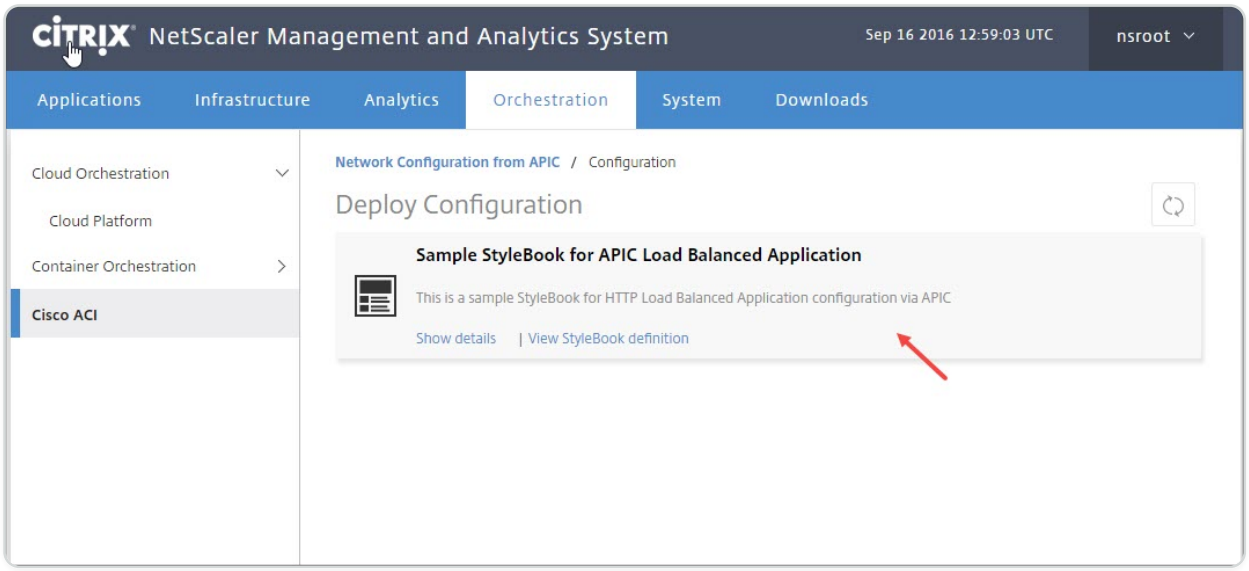
To deploy L4-L7 configuration by using StyleBook in NetScaler ADM:

1. Click the StyleBook name that appears as a URL in the tabular view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In the Configuration window, double-click **StyleBook**.

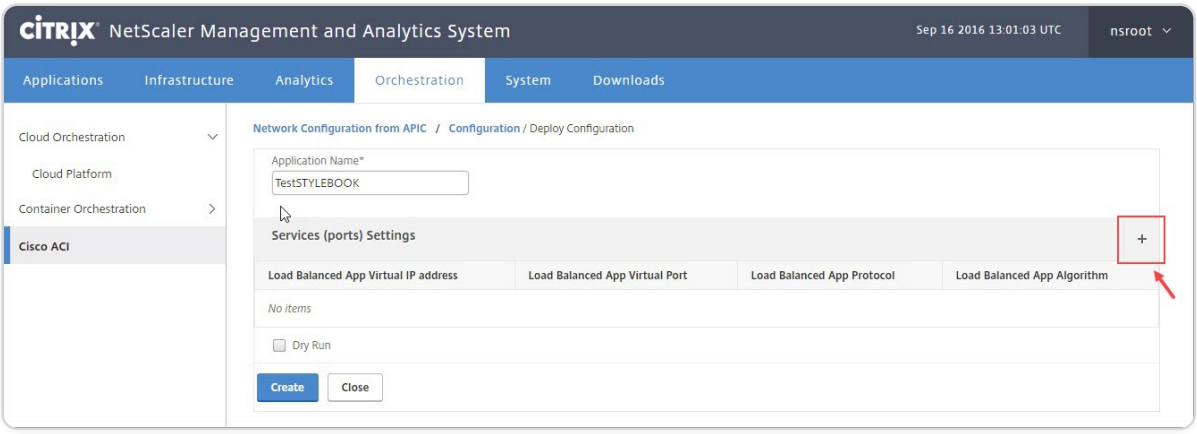


3. In the Deploy Configuration window, do the following:

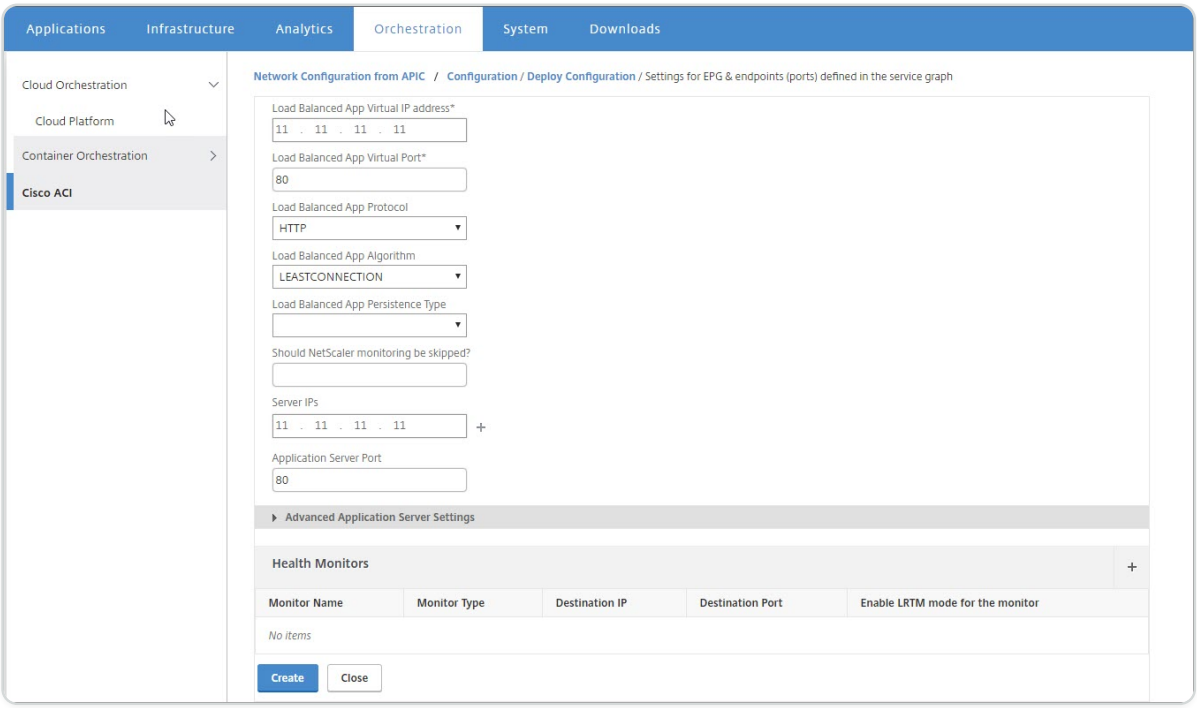
   a. In the **Application Name** field, enter the name for the ADC feature configuration that corresponds to the application's service graph in the APIC.

   b. In the Service (ports) Settings section, click **+**.

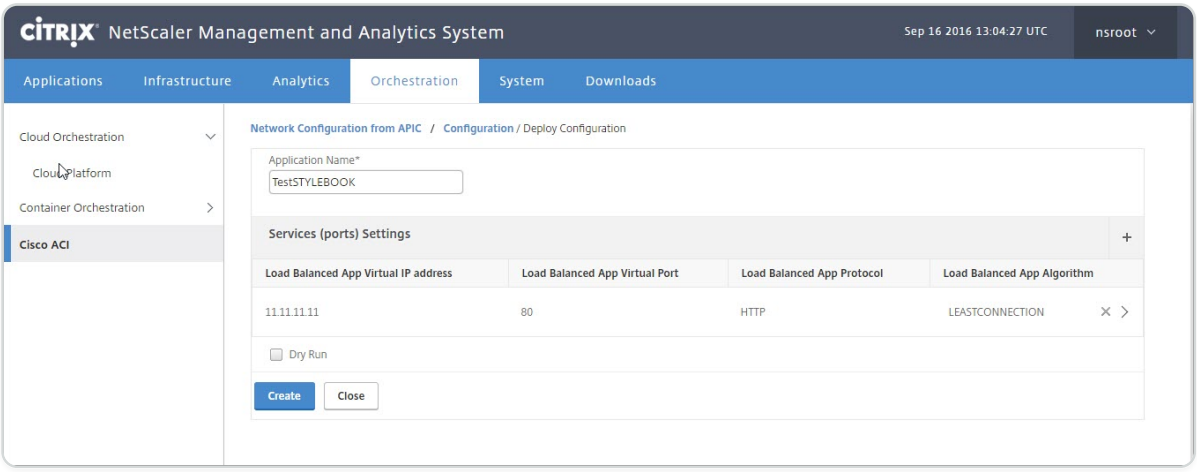
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

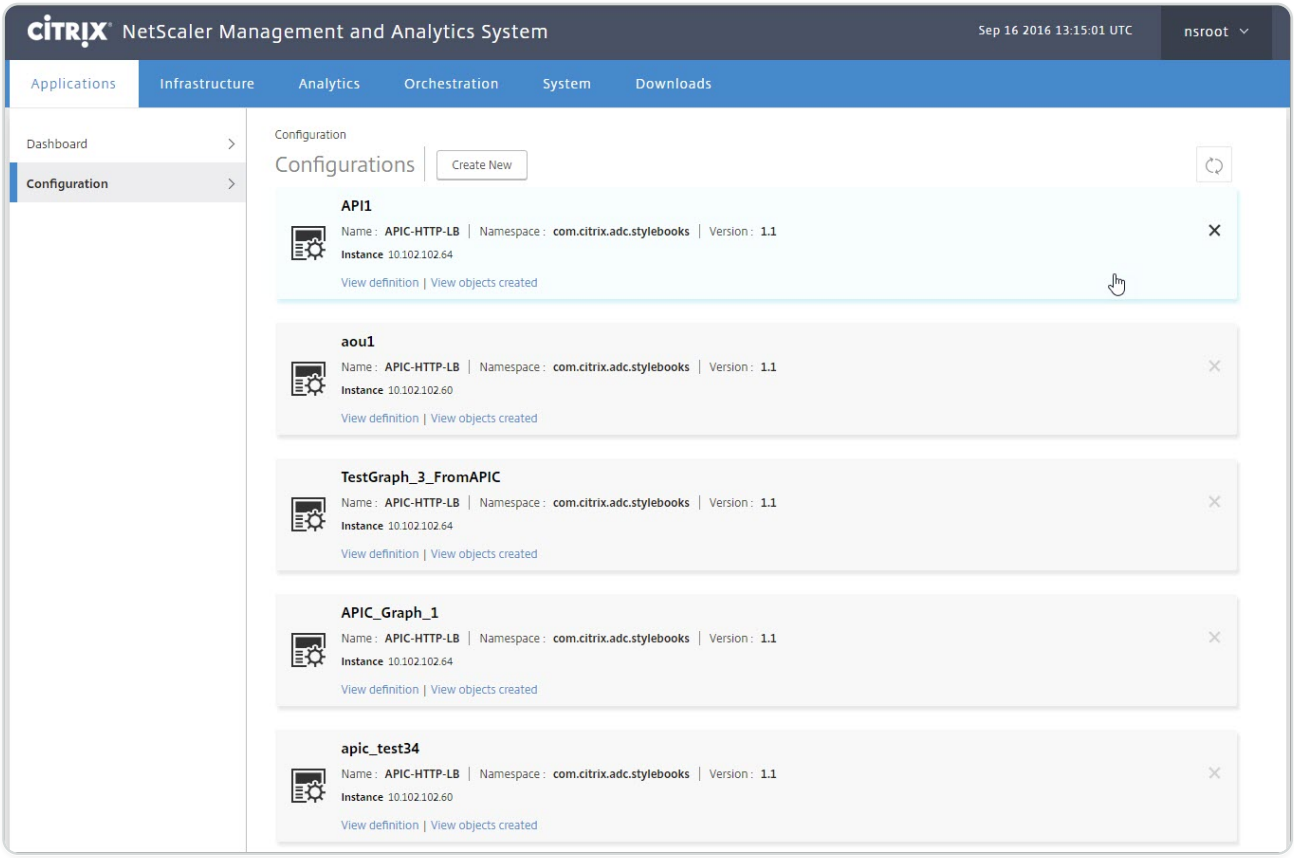


d. Click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The L4-L7 configuration specified in the StyleBook is deployed, in NetScaler ADM. You can view the StyleBoook configuration from the **Application** tab, by navigating to **Application \> Configuration**.



Attach and detach endpoint events from APIC

The hybrid-mode solution implicitly handles attach or detach endpoint events from the Cisco APIC. When the Cisco APIC triggers an attach endpoint event, the servicegroup_servicegroupmember_binding is automatically triggered by the StyleBook in NetScaler Application Delivery Management (ADM), and the endpoint is unbound during the detach endpoint event.

Additionally, if you have not deployed the L4-L7 configuration in NetScaler ADM before the attach or detach endpoint event gets triggered in Cisco the APIC, the solution will retain the attach IP addresses in the database. These IP addresses are bound to the corresponding service group after the service group is created through StyleBook.

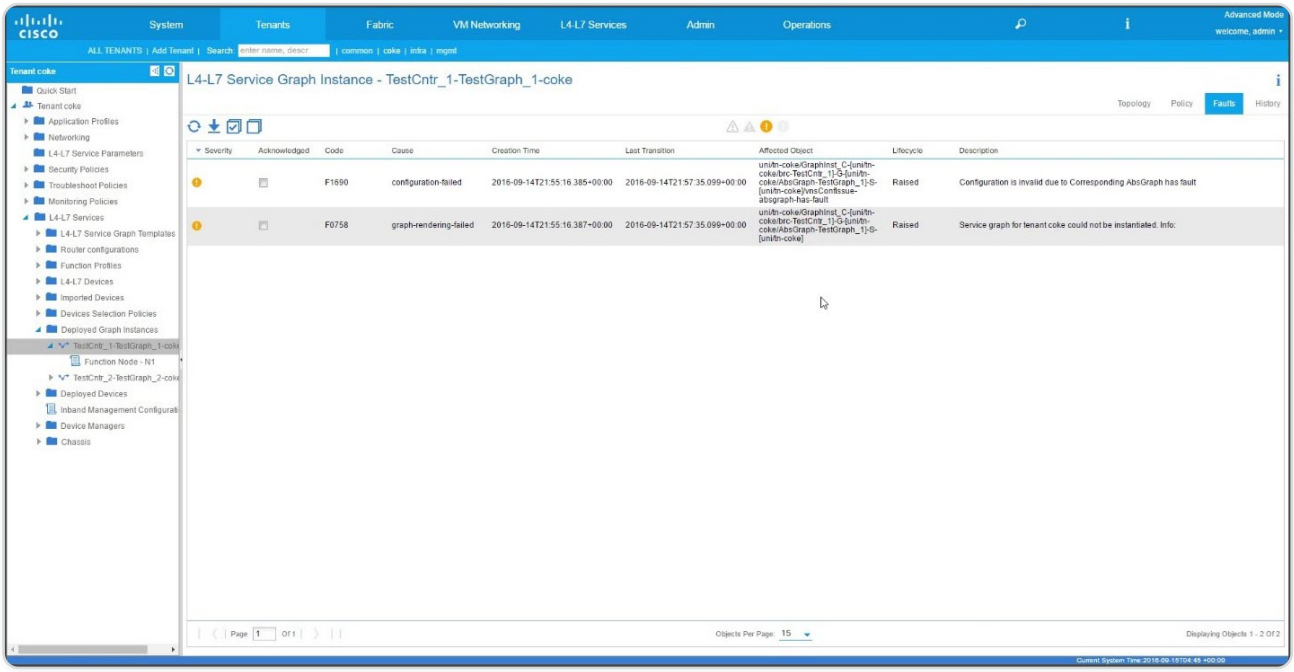
APIC fault reports

When you deploy a NetScaler 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/`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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 NetScaler® ADM

NetScaler 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 NetScaler ADM and use the shell to navigate to the NetScaler ADM directory structure. Following is a sample snippet of a NetScaler ADM log for an APIC's graph deployment.

```
2016-06-29 10:58:33,816 DEBUG APIC Config  = {(0, '', 5230): {'dn': u'uni/
vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-
cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant':
'coke_SDX2', 'ctxName': 'cokectx1', 'value': {(10, '',
'ADCHybridMode_1_Consumer_1'): {'state': 1, 'transaction': 0, 'cifs':
{'ADCHybridMode_1_Device_1': '1_1'}, 'ackedstate': 0}, (7, '',
'2129920_32778'): {'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0,
'transaction': 0}, (1, '', 5790): {'transaction': 0, 'ackedstate': 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'):
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{'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}}}}}}, 'state': 1, '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': {(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'uni/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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-29 10:58:33,833 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":"10.102.102.8
1","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 +++++++++ getContextAwareFlag = True

2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from Config ++
++++

2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {'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, '',
5230), (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 = []
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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" }, sessionId =
##D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7ED
F27646B2509164EEFBCB549EDAB6E6168ED0AEA68452DED6D30ACBED4BC34998DE818F7290
C9B44342054168DFB89DF1AFA9A4378F1DB07F03BF6C9B4F6A7A38E6A5F1BFED70C7225318
1397E305B14FF490861C3F8114948538

2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {'10.102.102.62':
{'10.102.102.62': {u'errorcode': 0, 'status_code': 201, u'message':
u'Done', u'severity': u'NONE', 'operation_name': 'add_op'}}, (7, '',
'2129920_32778'): {'vlan': {u'errorcode': 0, 'status_code': 201,
u'message': u'Done', u'severity': u'NONE', 'operation_name': 'add_op'}},
(((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, 'internal',
'provider')), 'nsip'): {'vlan_nsip_binding': {u'errorcode': 0,
'status_code': 201, u'message': u'Done', u'severity': u'NONE',
'operation_name': 'bind_op'}}, (((0, '', 5230), (4, 'Network',
'network')), (4, 'nsip', 'internal_snip')): {'nsip': {u'errorcode': 0,
'status_code': 201, u'message': u'Done', u'severity': u'NONE',
'operation_name': 'add_op'}}, (): {}, (8, '',
'ADCHybridMode_1_Consumer_1_2129920_32778'): {'vlan_interface_binding':
{u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
u'NONE', 'operation_name': '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 = add_op, erMsg =
Done, statusCode = add_op

2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op, erMsg =
Done, statusCode = bind_op

2016-06-29 10:58:44,238 DEBUG +++++++++++++++ ServiceAudit response =
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{'faults': [], 'state': 0, 'health': []}

2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {'graphDN': u'uni/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 10:58:44,242 DEBUG Journal Processing: Database task: create
apic_graph

2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2

2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2

2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector collection from
Config with type 22 for attach & detach event ++++++

2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {0: [], 1:
[], 3: []}

2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList = []

2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = []
dettachIpList = []

2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row =
{'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni/
vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-
cokectx1', 'apicGraphState': None, 'serviceGroupName': None,
'configPackId': None, 'tenantName': u'coke_SDX2', 'styleBookName': u'APIC-
HTTP-LB', 'graphInstanceName': u'HybridModeGraph_1', 'context':
u'cokectx1', 'serviceGroupPort': None, 'graphInstanceId': 5790,
'createDate': None, 'serviceGroupIP': None}
```

Logs generated by hybrid-mode device package

The NetScaler 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 = {'state': 1,
'transaction': 0, 'ackedstate': 0, 'value': {(5, 'name', 'stylebookName'):
{'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'}}}

2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62, 24063]
NMAS collection styleBookName= APIC-HTTP-LB

2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62, 24063]
NMAS collection retCol= {'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '',
5230), (4, 'Stylebook', 'stylebook_1'))}

2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62, 24063]  +
+++ devMgrStyleBookUrl = http://10.102.102.81/stylebook/nitro/v1/config/
stylebooks/com.citrix.adc.stylebooks/1.1/APIC-HTTP-LB

2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62, 24063]  +
+++ Response from styleBookresCode serviceAudit = {u'stylebook':
{u'uses_builtin_namespaces': {u'netscaler.nitro.config': u'10.5'},
u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace':
u'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-
LB\nnamespace: 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"\nimport-stylebooks: \n  - \n    namespace:
netscaler.nitro.config\n    prefix: ns\n    version: "10.5"\n  - \n
namespace: "com.citrix.adc.stylebooks"\n    prefix: "stlb"\n    version:
"1.1"\nparameters-default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n
lb-name(appname, port): $appname + "-" + str($port) + "-lb"\n  sg-
name(appname, port): $appname + "-" + str($port) + "-sg"\n
healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n  -
\n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$parameters.app-services\n    repeat-item: app\n    properties: \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        name: lbvserver-svg-binding\n        type:
ns::lbvserver_servicegroup_binding\n        properties: \n          name:
$substitutions.lb-name($parameters.appname, $app.virtual-port)\n
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\noutputs: \n  - \n    name: lbvservers\n    value:
$components.lbvserver\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 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62, 24063]  +
+++ Dev Mgr request details devMgrUrl = http://10.102.102.81/admin/v1/apic

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':
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
'close', 'date': 'Wed, 29 Jun 2016 10:58:33 GMT', 'x-frame-options':
'SAMEORIGIN', 'content-type': 'application/json; charset=utf-8'}

2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62, 24063] ++
++++++++++++ pollingURL = http://10.102.102.81/admin/v1/journalcontexts/
ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea

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'2016-06-29T10:58:33.760565', 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'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'2016-06-29T10:58:33.760565', 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 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62, 24063] ++
++++++++++++ pollingStatus = True, pollingTime = 2

2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62, 24063] ++
++++++++++++ pollingResponse json = {u'journalcontext': {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'2016-06-29T10:58:33.760565', 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', u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea',
u'replication_status': u''}}

2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62, 24063]
Attempts 1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62, 24063]
Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0, '', 5230)),
transaction: 0

2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62, 24063]
Attempts for {'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>'}}, 'version': '11.0', 'host': '10.102.102.62', 'port': 80,
'creds': {'username': 'nsroot', 'password': '<hidden>'}}}, 'manager':
{'hosts': {'10.102.102.81': {'port': 80}}, 'name': 'NMAS_1', 'creds':
{'username': 'nsroot', 'password': '<hidden>'}}, '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 (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0, '', 5230))

2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62, 24063]
pending: False, delete: False, txId: None

2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62, 24063]
Faults: []

2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62, 24063]
Health: []

2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62, 24063]
Send num: 761, type: 220, len: 382
```

NetScaler device package in Cisco ACI's cloud orchestrator mode

With Application Policy Infrastructure Controller (APIC) version 3.1 Citrix NetScaler, and Cisco ACI expand the joint integration portfolio to provide a new solution addressing customer’s needs. The new integration mode, ACI Cloud Orchestrator Mode*,* simplifies L4-L7 integrations by abstracting configuration complexity through standardized parameters. The solution works seamlessly to automate L4-L7 services, achieving the goals of agile application deployments, operational flexibility, and simplicity.

The Cisco ACI cloud orchestrator mode by using NetScaler solution provides the following benefits:

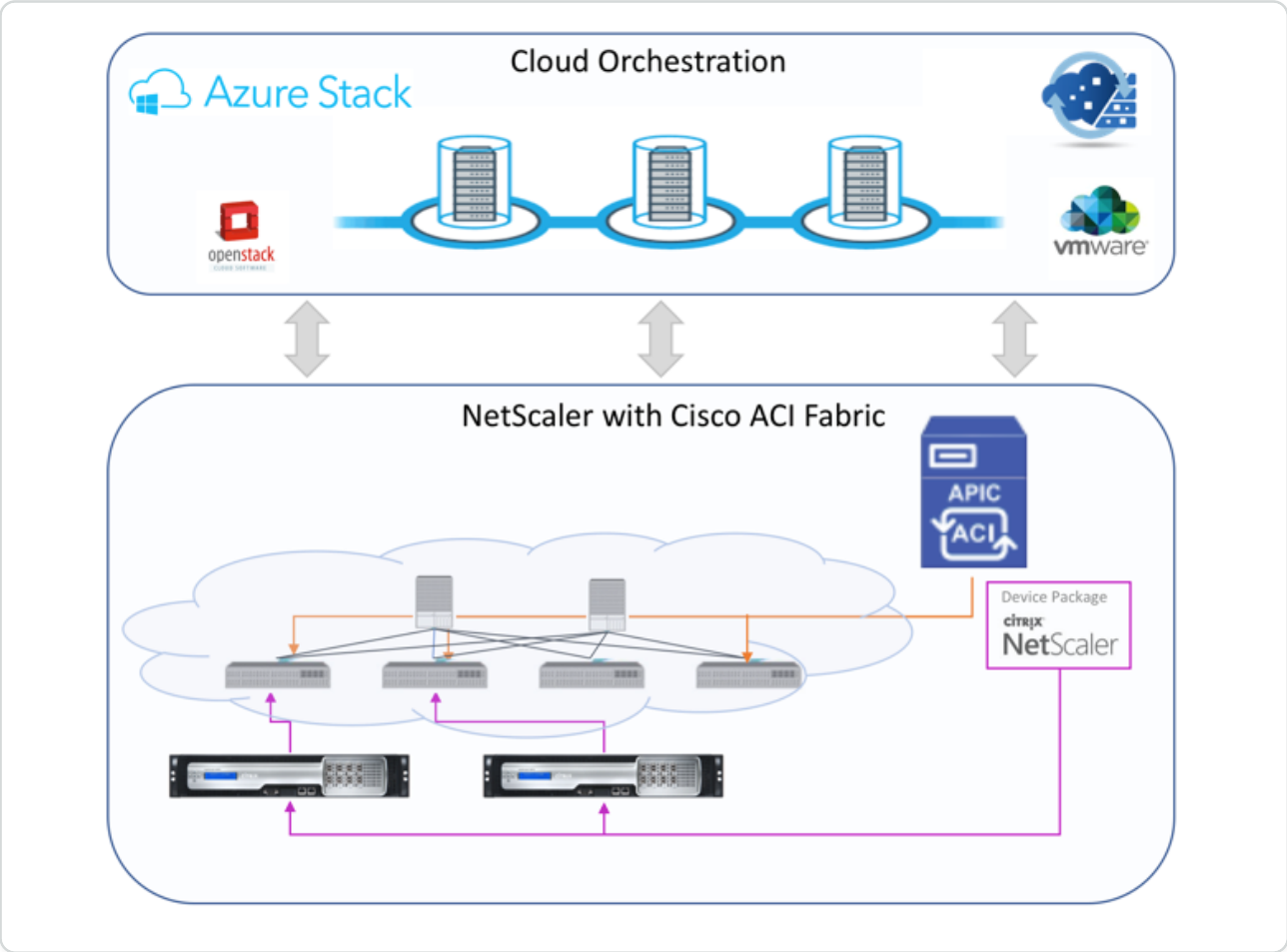
- Automation of L4-L7 services reduces the human error.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The pre-built integration of Cisco ACI solution helps you in reducing the deployment time, and increases the performance of applications, such as web applications, virtual machines, and SQL.
- Fully integrated visibility into the health of applications such as web applications, virtual machines, and SQL across physical and virtual network components.

The ACI cloud orchestrator mode now gives you more choices to utilize the new simplified APIC GUI directly or by selecting any cloud orchestrator, such as Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize, or any other based on your preference. This new change is achieved by exposing a set of ADC attributes as ADC schema. These attributes are mapped in the device packages function profiles. You can provide values for these attributes while provisioning the ADC service by the cloud orchestrator (Cisco Cloud Center or Wireless Application Protocol (WAP)).

The following illustration provides an overview of NetScaler in a cloud orchestration solution:



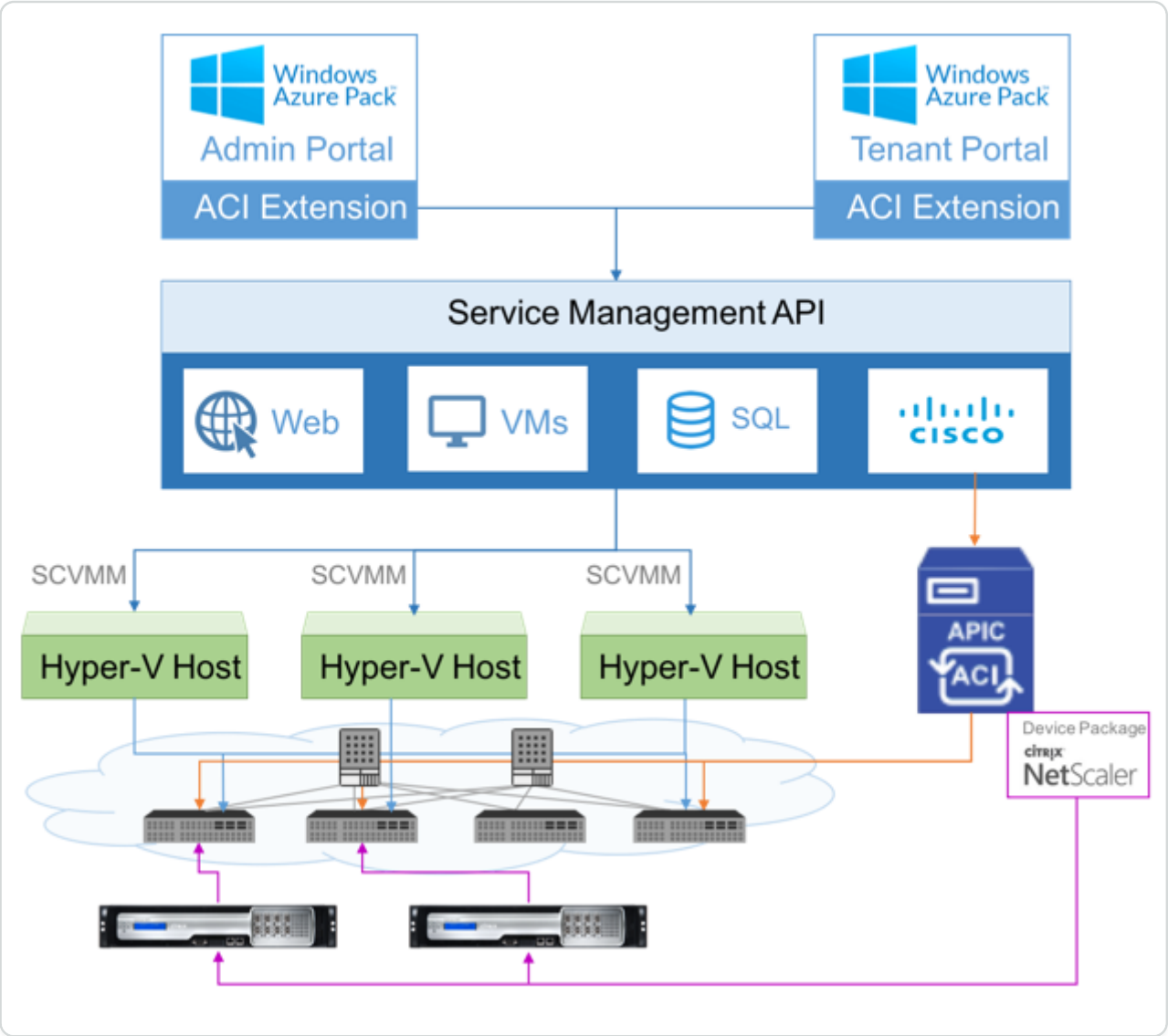
The cloud orchestrator mode solution using Microsoft Azure Pack involves many integration points, such as Azure Pack to Cisco APIC, Cisco APIC to System Central virtual machine Manager (SCVMM), and Cisco APIC to NetScaler. As a tenant in the private cloud, you can enable NAT, provision network services, and can add a load balancer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure Pack supports tenant and administrator portals, and each of them has their own set of operations that can be performed.

- As an administrator, you can perform administrative tasks such as ACI registration, VIP range, NetScaler device association with virtual machine cloud, and tenant user account creation.
- As a tenant, you can perform tasks such as log on to the Azure Pack tenant Portal and configure the network, bridge domains, and Virtual Routing and Forwarding (VRFs), and can use the NetScaler load balancing and RNAT features.

The following illustration provides an overview of Azure Pack in a cloud mode solution:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- Cloud administrator can facilitate with L4-L7 schema supported by APIC and any additional changes can be done by APIC administrator directly in the APIC. This allows you to configure and deploy NetScaler at par with the supported feature set.
- Tenants can deploy multiple VIP addresses with different ports for the same network. You must ensure that the IP and port combination is unique.
- The NetScaler device package supports only single-context deployment. Each tenant gets a dedicated NetScaler instance.
- Wireless Application Protocol (WAP) supports NetScaler MPX appliances and NetScaler VPX appliances (includes NetScaler VPX instances deployed on the NetScaler SDX platform).

The cloud orchestrator mode device package supports both fully managed mode and service manager mode. The fully managed mode package supports a wide variety of function profiles, such as simple load balancing, content switching, SSL offload, and other profiles. These function profiles cover a complete feature set and deployment mode of the NetScaler. Similarly, service manager mode device package supports one-arm and two-arm configuration and deployment of NetScaler using APIC. The NetScaler Application Delivery Management (ADM) acts as service manager for APIC and you can use NetScaler ADM to configure NetScaler L4-L7 parameters.

NOTE

In service manager mode (hybrid mode), you cannot reuse or reassign the same server IP address, which is already present in the NetScaler appliance.

Cloud orchestrator mode function profile has a set of parameters mapped to APICs ADC schema and the orchestrator uses these parameters. The cloud orchestrator provides the values for ADC parameters (VIP, while provisioning the NetScaler through APIC). The orchestrator communicates with APIC's APIs and passes the ADC specific details as part of the payload for a specific function profile. Internally, APIC extracts the values and passes them to the device package which configures the NetScaler internally.

For more information on the complete list of ADC schema's, which are supported by Cisco APICs, see Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x and earlier).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The fully managed mode device package supports the following function profiles:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

The service manage mode device package supports the following cloud mode function profiles:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler supports the above-mentioned function profiles. The APIC supports a subset of these parameters in the ADC schema. If there are any unsupported attributes by Cisco ACI present in the function profile, you have to clone the cloud orchestrator mode function profile and provide the values for all unsupported attributes by APIC and must save the attributes. Later, the orchestrator can use the newly cloned function profile.

Citrix Cloud Mode Device Package supports NetScaler 12.0 and service manager mode uses NetScaler ADM 12.0 as well. Device package has changed the model version from 1.0 to 2.0 and can be used as a new install. Cloud orchestrator Mode Device package cannot be upgraded from previous device package versions since the model version is changed.

Cloud orchestrator Mode device packages can be used in regular deployment as well. The package does not mandate user to provision NetScaler through any cloud orchestrator. The device package is compatible with just APIC and APIC with cloud orchestrator.

Manage the Kubernetes Ingress configuration in NetScaler® ADM

Kubernetes (K8s) is an open source container orchestration platform that automates the deployment, scaling, and management of cloud-native applications.

Kubernetes provides the Ingress feature which allows client traffic outside the cluster to access microservices of an application running inside the Kubernetes cluster. ADC instances can act as the Ingress to applications running inside a Kubernetes cluster. ADC instances can load balance and content route North-South traffic from the clients to any microservices inside the Kubernetes cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- NetScaler ADM supports the Ingress feature on the clusters with Kubernetes version 1.14–1.21.
- NetScaler ADM supports NetScaler VPX and MPX appliances as Ingress devices.
- In the Kubernetes environment, the NetScaler instance load balances only the "NodePort" service type.

You can configure multiple ADC instances to act as Ingress devices on the same cluster or different clusters or namespaces. After you configure the instances, you can assign each instance to different applications based on the Ingress policy.

You can create and deploy an Ingress configuration using Kubernetes `kubectl` or APIs. You can also configure and deploy an Ingress from NetScaler ADM.

You can specify the following aspects of Kubernetes integration in ADM:

- **Cluster** – You can register or unregister Kubernetes clusters for which ADM can deploy Ingress configurations. When you register a cluster in NetScaler ADM, specify the Kubernetes API server information. Then, select an ADM agent that can reach the Kubernetes cluster and deploy Ingress configurations.
- **Policies** – Ingress policies are used to select the ADC instance based on cluster or namespace to deploy an Ingress configuration. Specify the cluster, site, and instance information when you add a policy.

Before you begin

To use NetScaler instances as Ingress devices on Kubernetes clusters, ensure you have:

- Kubernetes cluster in place.
- Kubernetes cluster registered in NetScaler ADM.

Configure the NetScaler ADM with a secret token to manage a Kubernetes cluster

For NetScaler ADM to be able to receive events from Kubernetes, you need to create a service account in Kubernetes for NetScaler ADM. And, configure the service account with the necessary RBAC permissions in the Cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Create a service account for NetScaler ADM. For example, the service account name can be `citrixadm-sa`. To create a service account, see Use Multiple Service Accounts.
2. Use the `cluster-admin` role to bind the NetScaler ADM service account. This binding grants a `ClusterRole` across the cluster to a service account. The following is an example command to bind a `cluster-admin` role to the service account.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   After binding the NetScaler ADM service account to the `cluster-admin` role, the service account has the cluster-wide access. For more information, see `kubectl` create `clusterrolebinding`.
3. Obtain the token from the created service account.

   For example, run the following command to view the token for the `citrixadm-sa` service account:

   ```
   kubectl describe sa citrixadm-sa
   ```
4. Run the following command to obtain the secret string of the token:

   ```
   kubectl describe secret <token-name>
   ```

Add the Kubernetes cluster in NetScaler ADM

After you configure a NetScaler agent and configure static routes, you must register the Kubernetes cluster in NetScaler ADM.

To register the Kubernetes cluster:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

   a. **Name** - Specify a name of your choice.

   b. **API Server URL** - You can get the API Server URL details from the Kubernetes main node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. On the Kubernetes main node, run the command `kubectl cluster-info`.

```
root@kmaster:[redacted]# kubectl cluster-info
Kubernetes master is running at https://10.[redacted]:6443
KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/
services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

ii. Enter the URL that displays for **"Kubernetes master is running at."**

c. **Authentication Token** - Specify the authentication token string obtained while you configure NetScaler ADM to manage a Kubernetes cluster. The authentication token is required to validate access for communication between the Kubernetes cluster and NetScaler ADM. To generate an authentication token:

i. On the Kubernetes main node, run the following commands:

```
kubectl describe secret <token-name>
```

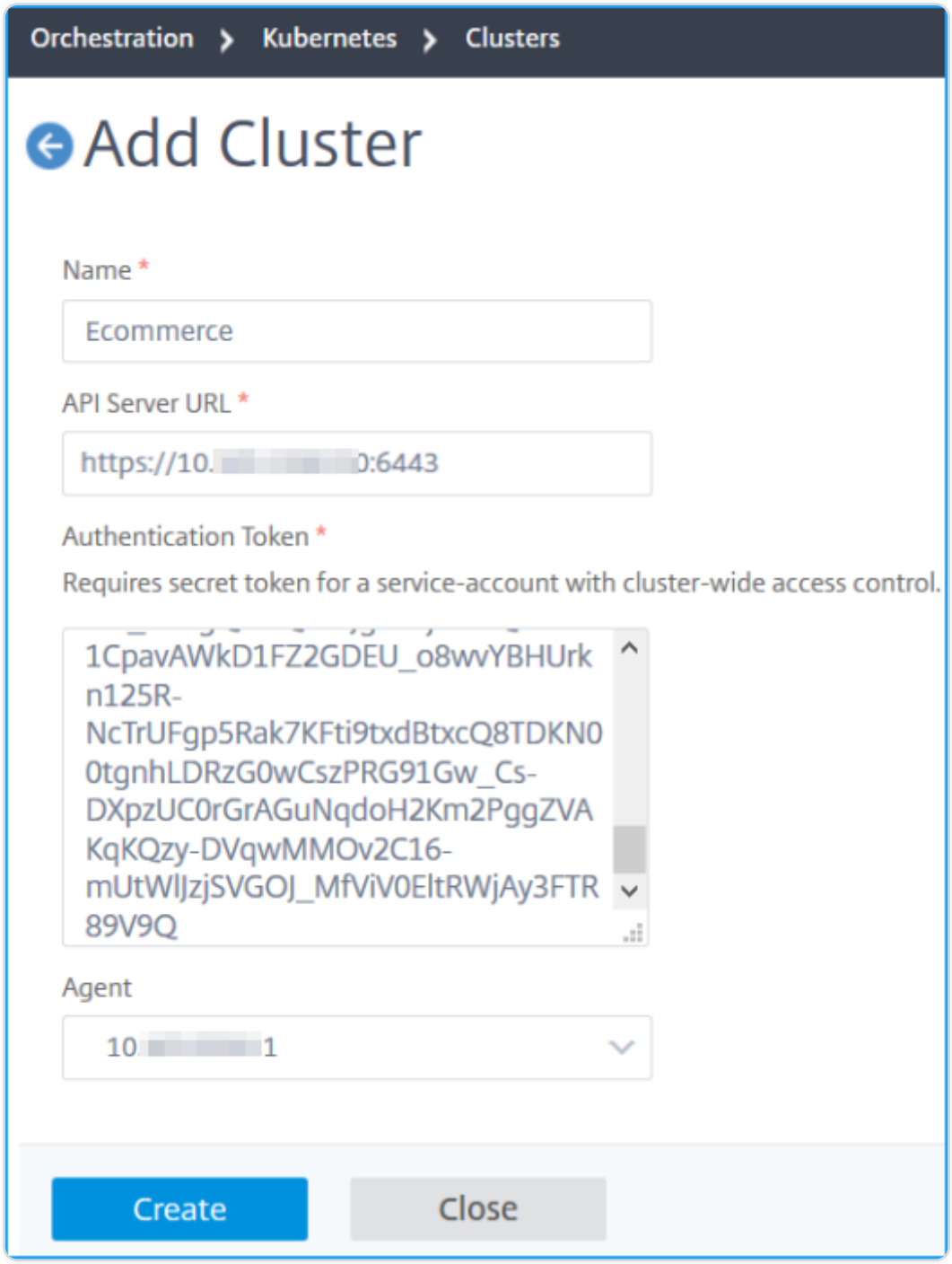
ii. Copy the token that is generated and paste it as the Authentication Token

For more information, see Kubernetes documentation.

d. Select the agent from the list.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Video Insight

The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by NetScaler appliances to improve customer experience and operational efficiency, providing benefits such as:

- Manage the network during congestion in peak hours.
- Improve video play consistency and reduce video stalling.
- Enable new video service offerings (for example, Binge-on video services).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enable customers to select the best sustainable video quality.
- Provide a consistent user experience for the subscriber.

While optimizing the video traffic, the NetScaler appliance uses a special mechanism to dynamically pace the video bit-rate and a random sampling technique to estimate the savings from the optimization technique. For more information about the NetScaler Video Optimization feature, see Video Optimization. When you integrate NetScaler appliance with NetScaler Application Delivery Management (ADM), it collects key information from the video data flowing through the NetScaler appliance. You can use this information to compare the optimized and unoptimized performance of the ABR video traffic, determine the savings due to optimization and so on.

NOTE

The statistics of the unoptimized sessions provided in NetScaler ADM corresponds to the sessions that you had selected of random sampling in NetScaler appliance. For more information about Random Sampling, see Video Optimization.

Video Insight in NetScaler® ADM provides metrics for the following types of video traffic:

- Progressive Download (PD) videos over HTTP
- ABR videos over HTTP
- ABR videos over HTTPS
- YouTube ABR videos over QUIC

Configuring Video Insight

NOTE

Video Insight is supported on NetScaler instances with NetScaler Premium license. The NetScaler Premium license is supported for NetScaler Telco platforms (VPX T1000 and VPX-T).

To configure Video insight on a NetScaler instance, first enable the AppFlow feature, configure an AppFlow collector, action, and policy, and bind the policy globally. When you configure the collector, you must specify the IP address of the NetScaler ADM server on which you want to monitor the reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure video insight on a NetScaler instance, run the following commands to configure an AppFlow profile and policy and bind the AppFlow policy globally.

add appflow collector \<name\> **-IPAddress** \<ipaddress\> **-port** \<port_number\> **-Transport** logstream

set appflow® param -**videoInsight** ENABLED

add appflow action \<name\> **-collectors** \<string\> **-videoAnalytics** ENABLED

add appflow policy \<name\> \<rule\> \<action\>

bind appflow global \<policyName\> \<priority\> \[\<gotoPriorityExpression\>\] \[**-type** \<type\>\]

enable ns mode `ulfd`

enable feature AppFlow

Sample

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -Transport
logstream

set appflow param -videoInsight ENABLED

add appflow action act1 -collectors col1 -videoAnalytics ENABLED

add appflow policy appol true act1

bind appflow global appol 1

enable ns mode ulfd

enable feature appflow
```

Viewing the Video Insight metrics in NetScaler ADM

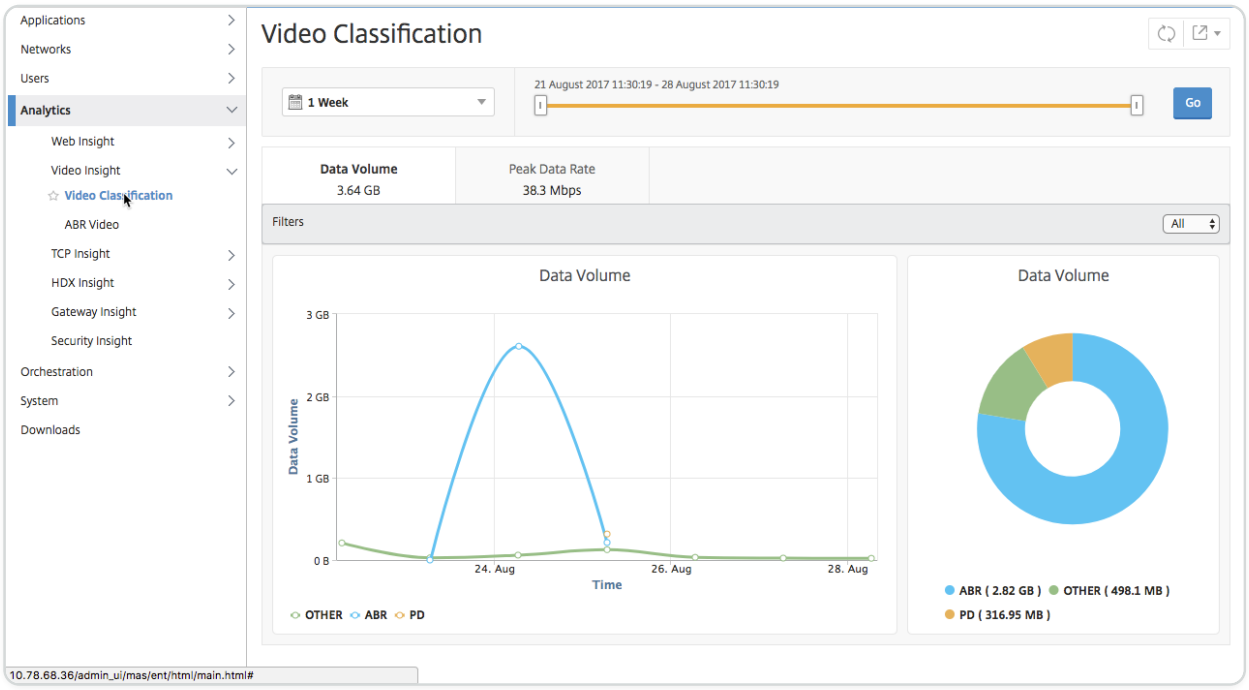
After enabling Video Insight in NetScaler ADM, you can view video optimization metrics such as, video classification, data volume, peak data rate, and ABR video plays. These metrics help you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

analyze your network and optimize the videos for improved subscriber experience, operational efficiency, and other performance criteria.

To view the Video Insight metrics in NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM virtual appliance (for example, `<http://192.168.100.1>`).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Analytics \> Video Insight**.



NOTE

The values provided by the legend **OTHER** in the charts represent the non-ABR and non-PD data in the video traffic depending on the filter you have selected:

- **All** – Sum of non-ABR (HTTP, HTTPS, and QUIC) and non-PD (HTTP) data in the video traffic.
- **HTTP** – Sum of non-ABR and non-PD data in the video traffic.
- **HTTPS** – Sum of non-ABR video data in the video traffic.
- **QUIC** – Sum of non-ABR video data in the video traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

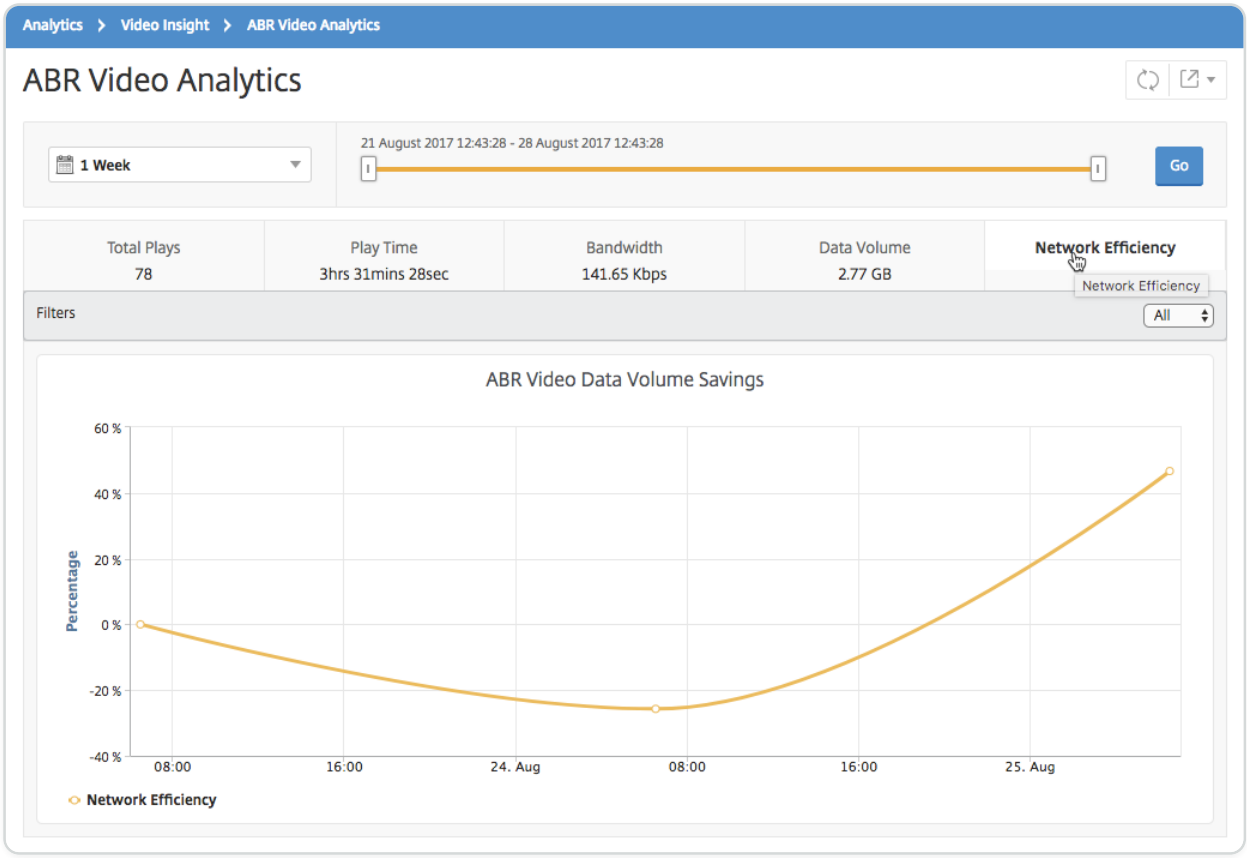
View network efficiency

For a given time frame, NetScaler® Application Delivery Management (ADM) provides a graph that shows the ratio of optimized to unoptimized video sessions in the time frame. It also displays the percentage of bandwidth saved by optimization. The percentage of bandwidth saved is calculated with the following formula:

Percentage of bandwidth saved = **Average optimized ABR video Data Volume / Average of unoptimized ABR Video Data Volume**.

To see the percentage of bandwidth saved by optimization:

1. Navigate to **Analytics \> Video Insight**, and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select the **Network Efficiency** tab.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

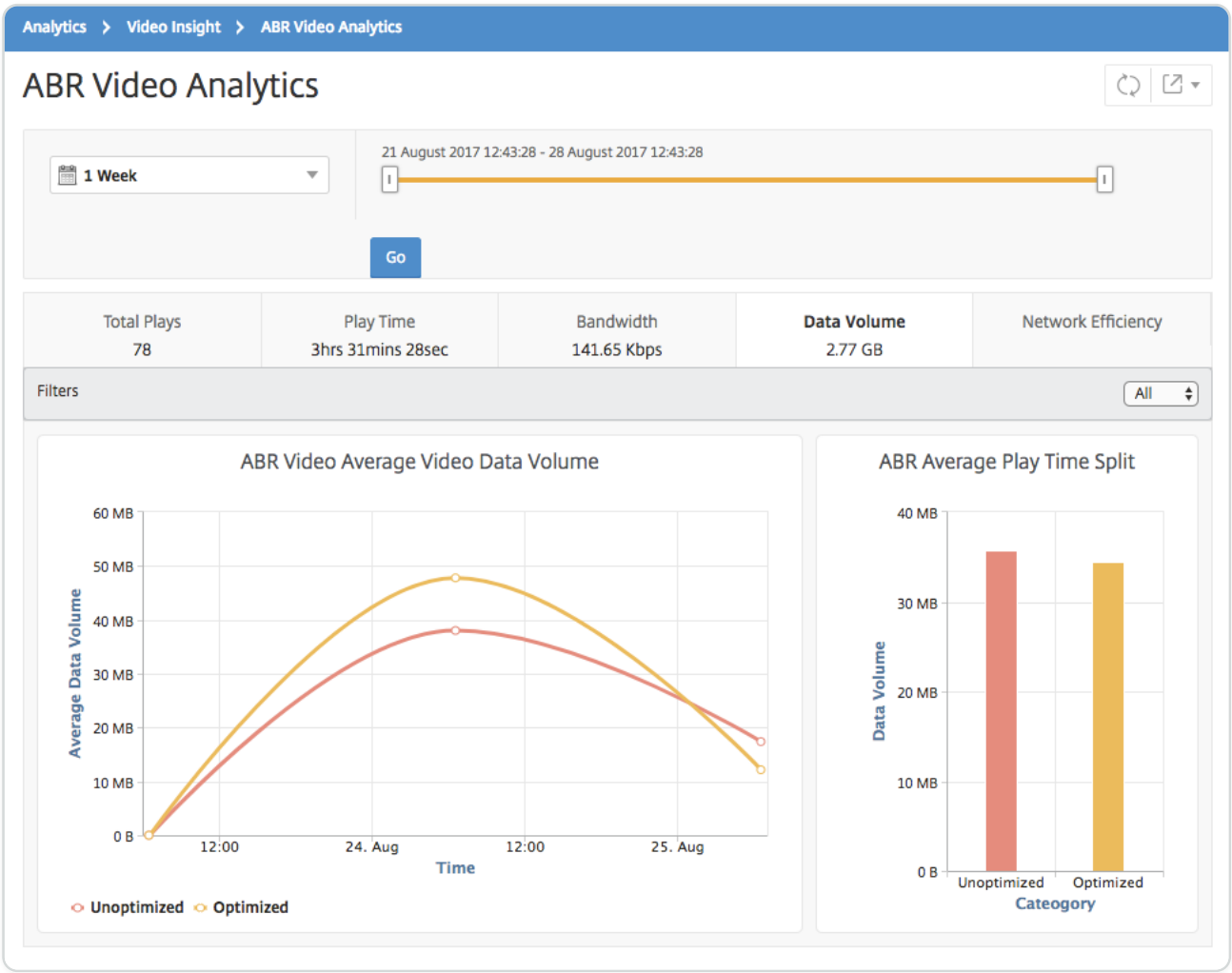
Compare the data volume used by optimized and unoptimized ABR videos

For a given time frame, NetScaler® Application Delivery Management (ADM) shows the data volume used by optimized and unoptimized ABR videos, so that you can compare the two volumes.

To see the data volume used by ABR videos:

1. Navigate to **Analytics \> Video Insight**, and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select the **Data Volume** tab.

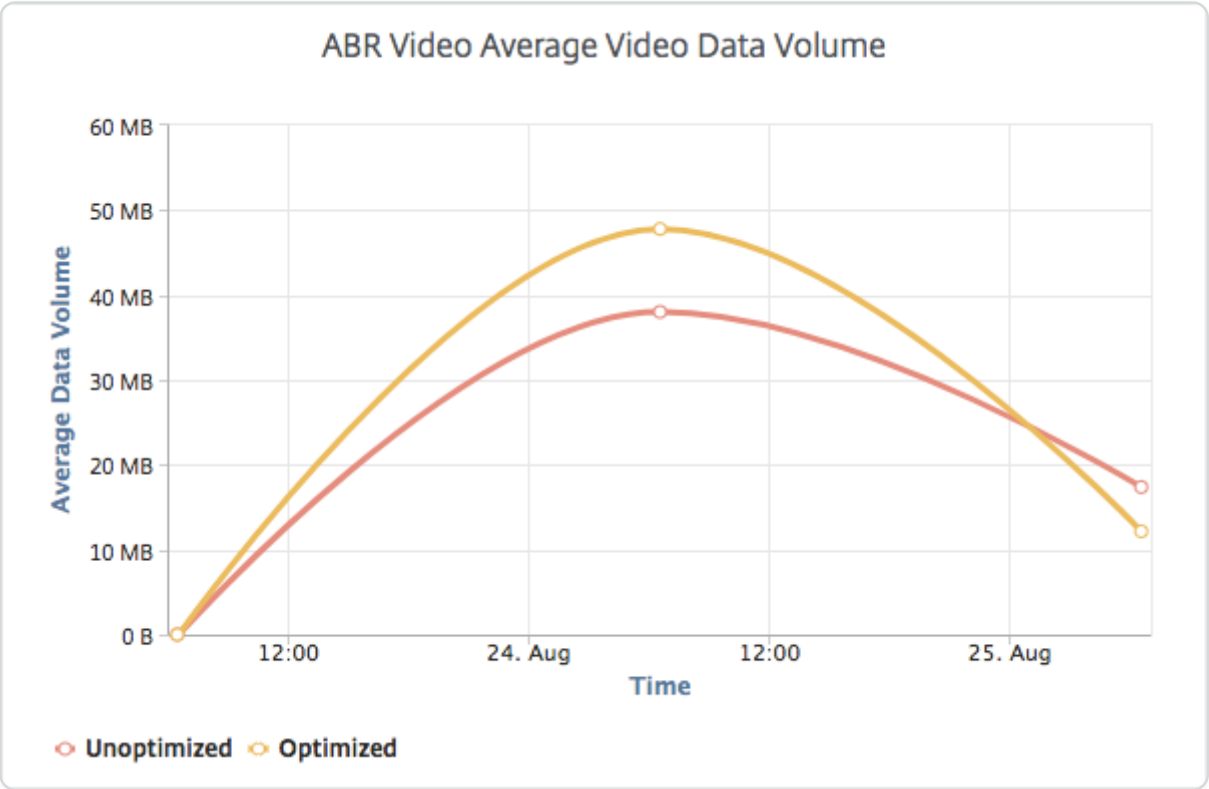
You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



The **Data Volume** tab provides a line graph and pie chart describing the average data volume used by ABR videos, and the data volume consumed by optimized and unoptimized ABR videos

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

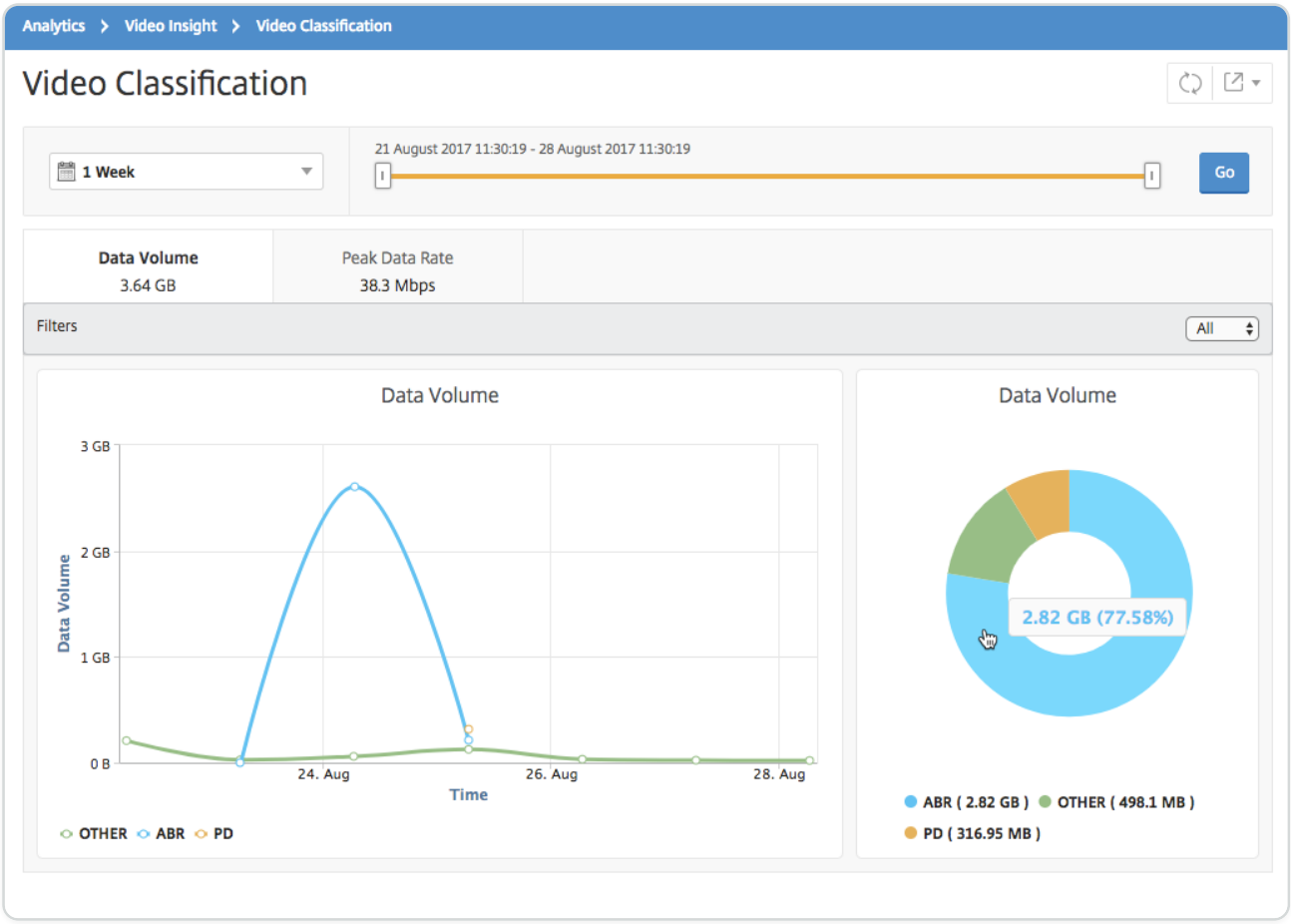
The NetScaler appliance detects the encrypted or unencrypted video traffic in your network and the type of video streaming (PD or ABR). NetScaler Application Delivery Management (ADM) displays these metrics and the data volume consumed by the video traffic for a defined time frame.

To see the types of videos and the consumed data volume:

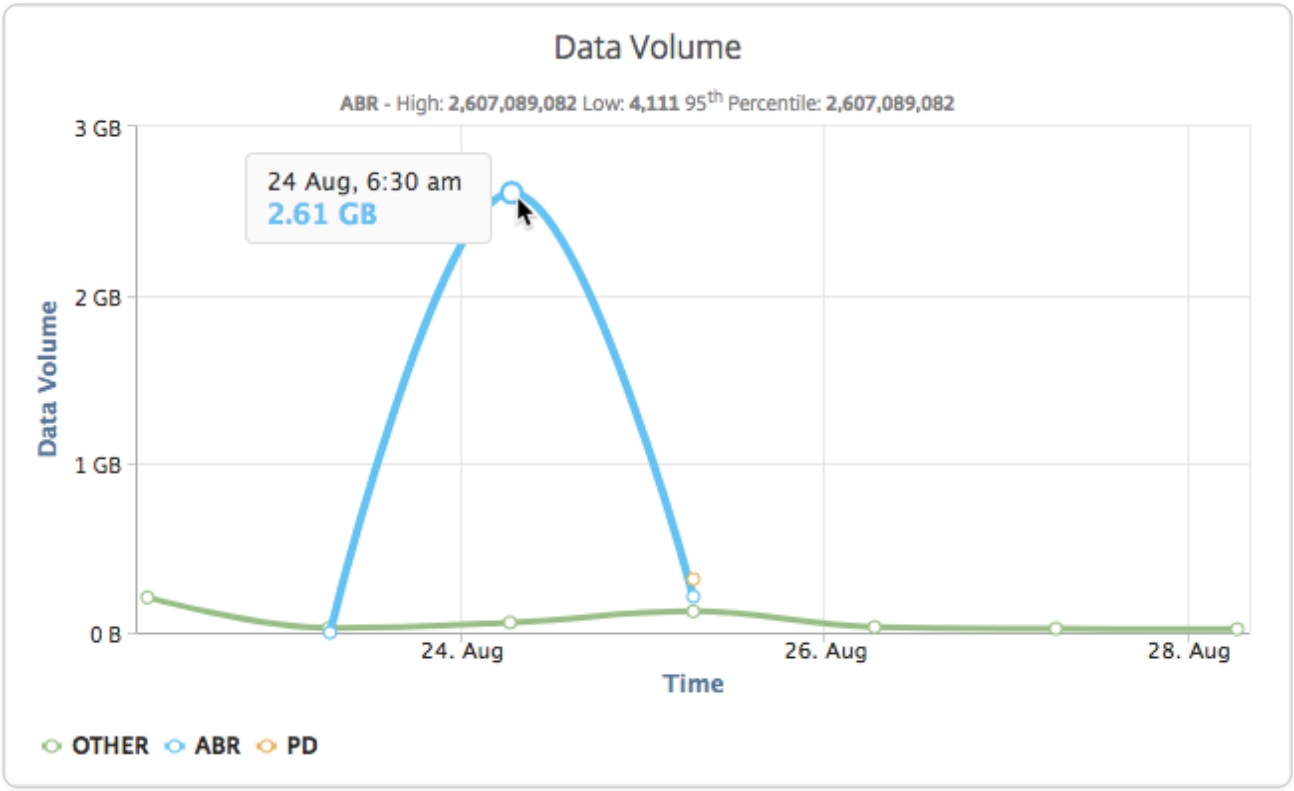
1. Navigate to **Analytics \> Video Insight** and click **Video Classification**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go**.

You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

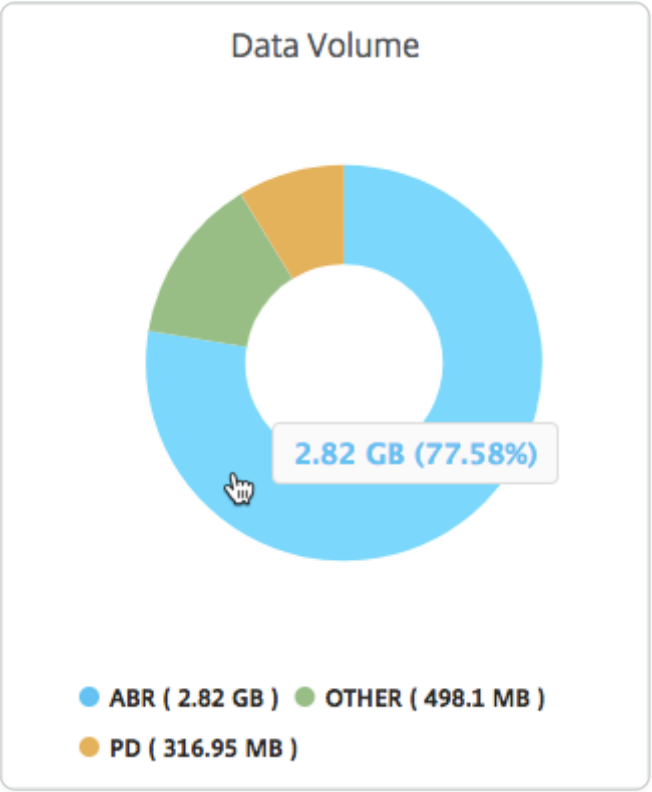


The **Data Volume** tab provides a line graph and pie chart showing the types of video traffic streaming from your network and the data volume consumed by your network. You can hover your mouse pointer on the line graph to view the data consumed during a particular time frame:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

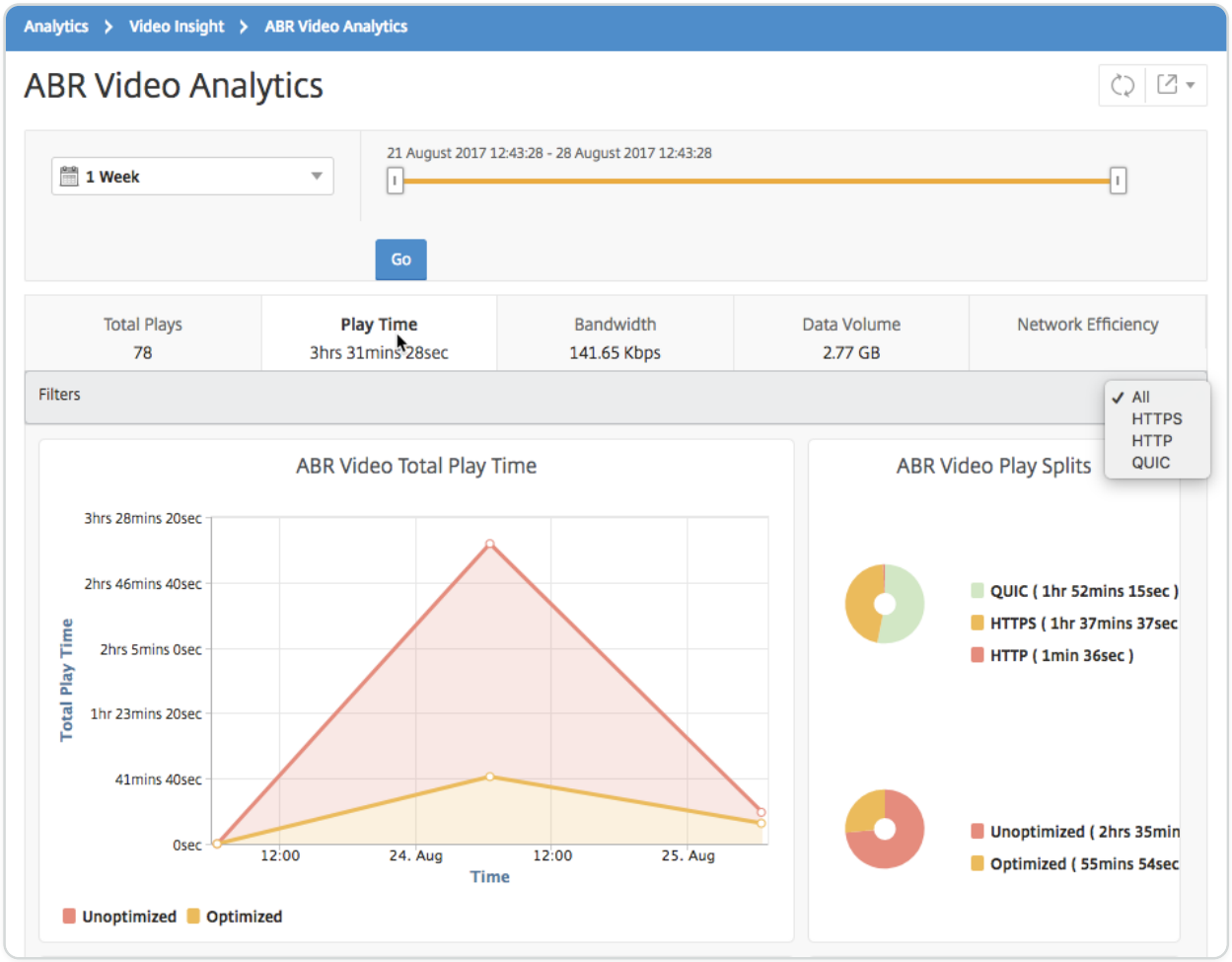
For a given time frame, NetScaler® Application Delivery Management (ADM) provides the play time of ABR videos and also enables you to compare the play time of optimized and unoptimized ABR videos in your network.

To view the play time:

1. Navigate to **Analytics \> Video Insight** and click **ABR Video**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Play Time** tab.

   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.

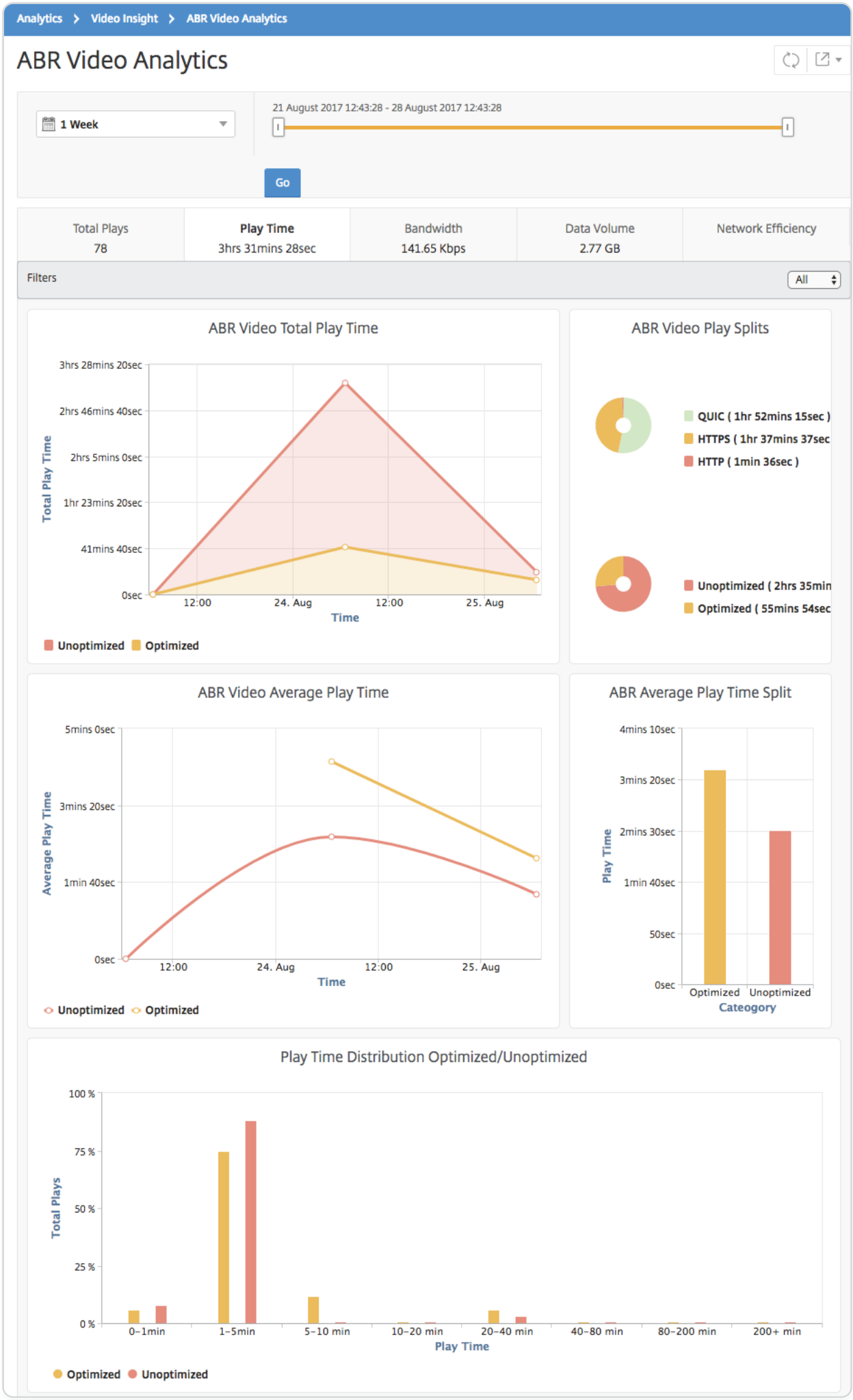
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Analytics > Video Insight > ABR Video Analytics
ABR Video Analytics
1 Week
21 August 2017 12:43:28 - 28 August 2017 12:43:28
Go
Total Plays
78
Play Time
3hrs 31mins 28sec
Bandwidth
141.65 Kbps
Data Volume
2.77 GB
Network Efficiency
Filters
All
ABR Video Total Play Time
3hrs 28mins 20sec
2hrs 46mins 40sec
2hrs 5mins 0sec
1hr 23mins 20sec
41mins 40sec
0sec
Total Play Time
12:00
24. Aug
12:00
25. Aug
Time
Unoptimized
Optimized
ABR Video Play Splits
QUIC (1hr 52mins 15sec)
HTTPS (1hr 37mins 37sec
HTTP (1min 36sec)
Unoptimized (2hrs 35min
Optimized (55mins 54sec
ABR Video Average Play Time
5mins 0sec
3mins 20sec
1min 40sec
0sec
Average Play Time
12:00
24. Aug
12:00
25. Aug
Time
Unoptimized
Optimized
ABR Average Play Time Split
4mins 10sec
3mins 20sec
2mins 30sec
1min 40sec
50sec
0sec
Play Time
Optimized
Unoptimized
Cateogory
Play Time Distribution Optimized/Unoptimized
100 %
75 %
50 %
25 %
0 %
Total Plays
0–1min
1–5min
5–10 min
10–20 min
20–40 min
40–80 min
80–200 min
200+ min
Play Time
Optimized
Unoptimized

Compare bandwidth consumption of optimized and unoptimized ABR videos

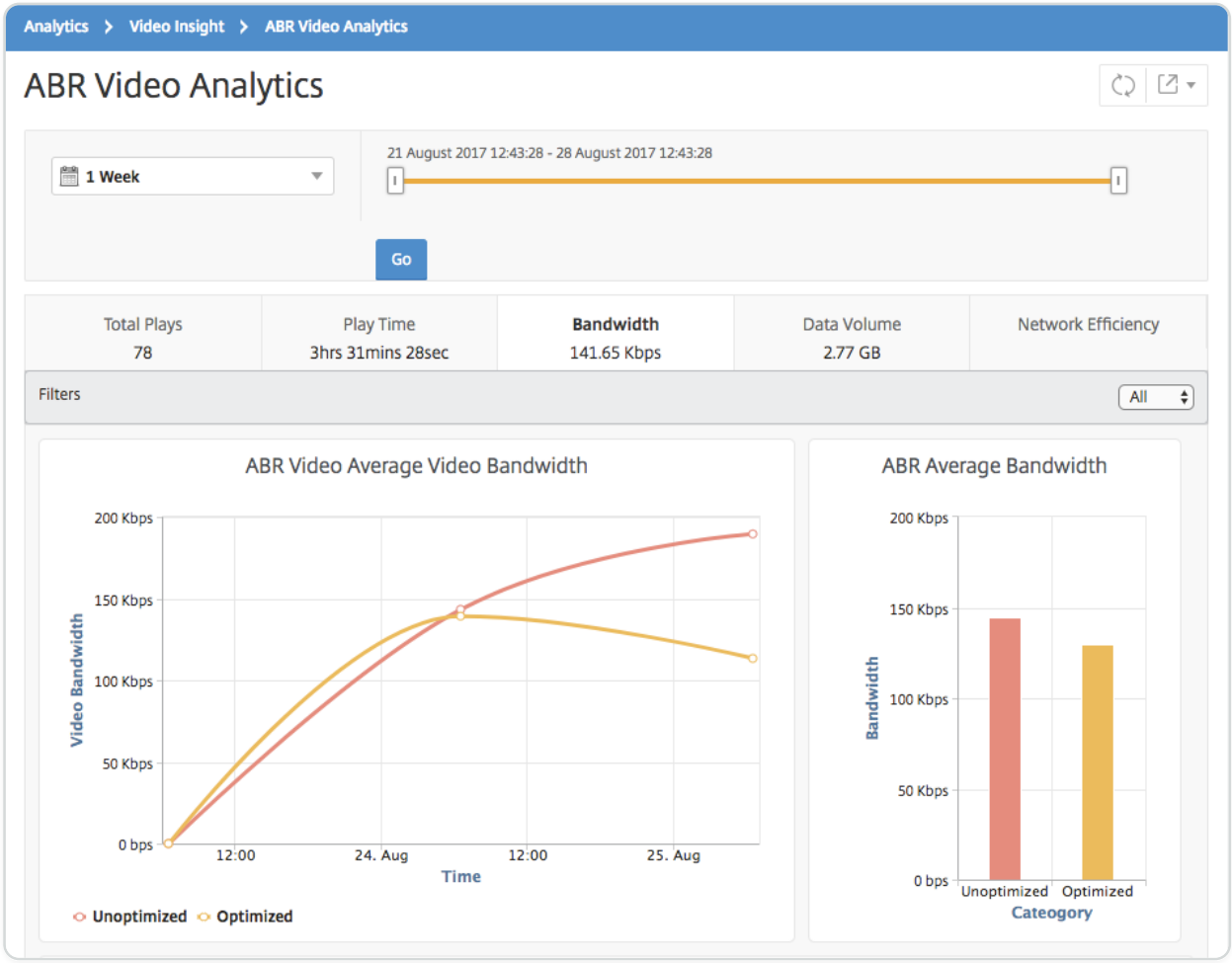
For a given time frame, NetScaler® Application Delivery Management (ADM) provides the bandwidth consumed by optimized and unoptimized of ABR videos and also enables you to compare the bandwidth consumed by optimized and unoptimized ABR videos in your network based on:

- Play Time
- Data Volume

To view the bandwidth consumption:

1. Navigate to **Analytics \> Video Insight** and click **ABR Video Analytics**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Bandwidth** tab.

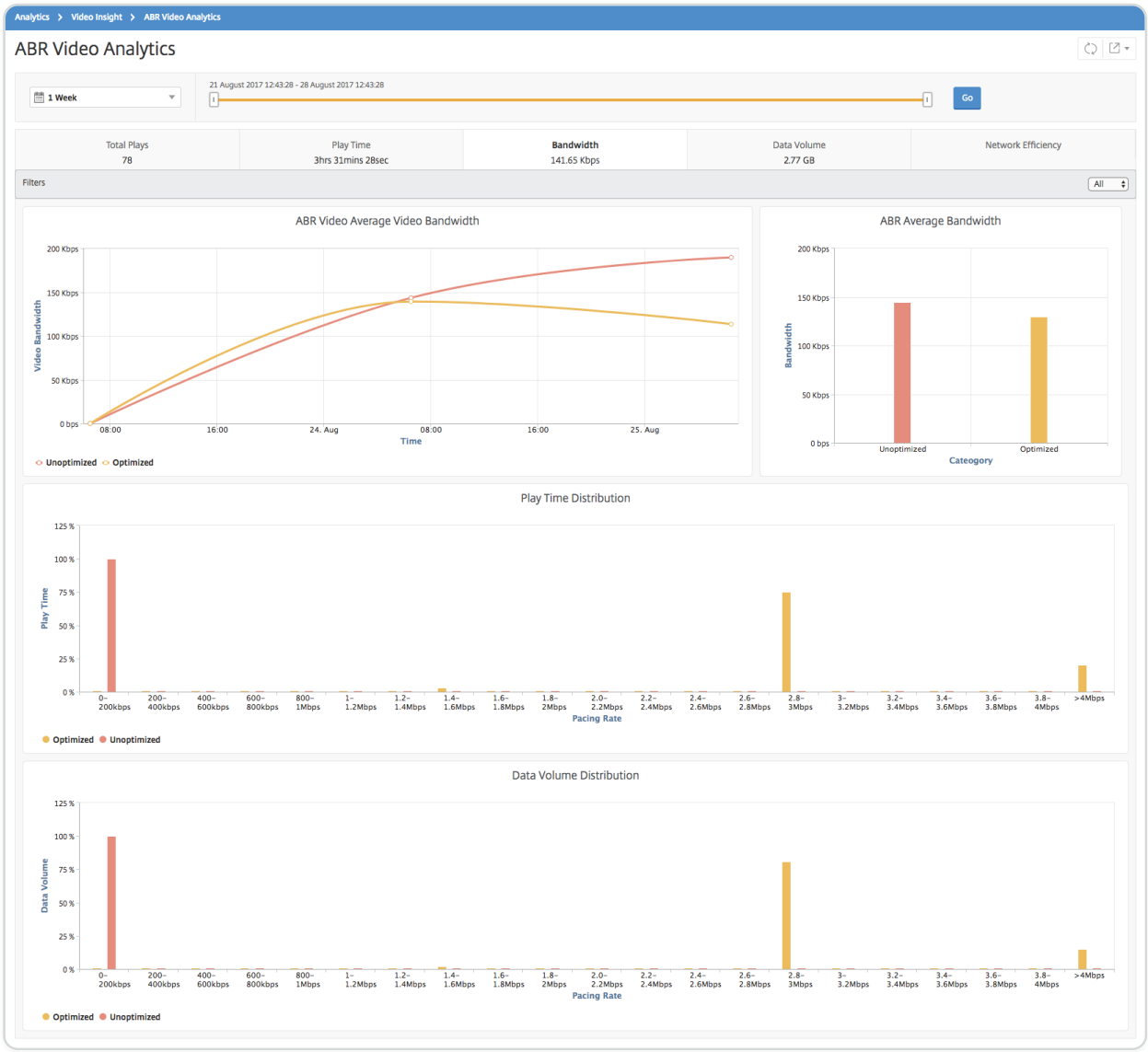
   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

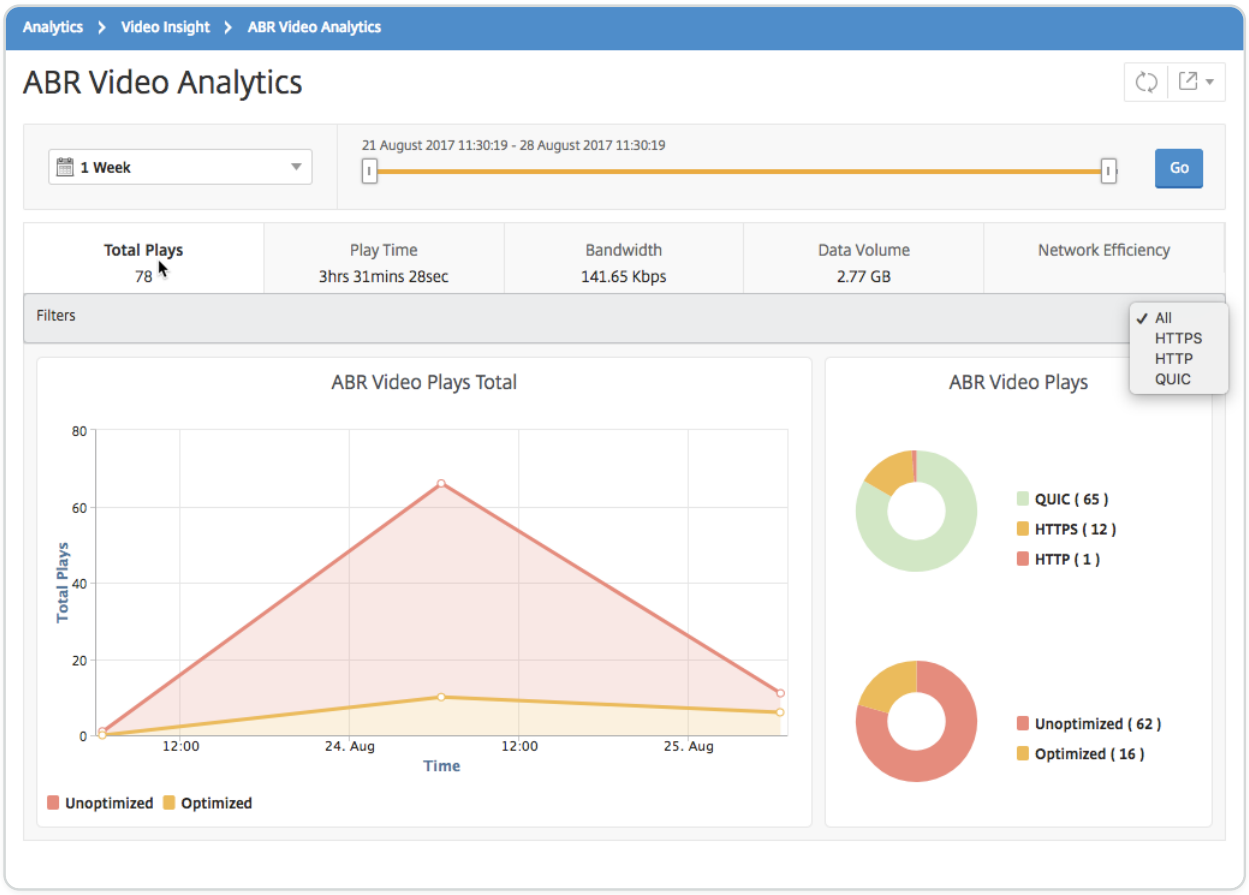
For a given time frame, NetScaler® Application Delivery Management (ADM) shows the number of plays of ABR videos and enables you to compare the number of optimized and unoptimized plays in your network.

To see the number of plays:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

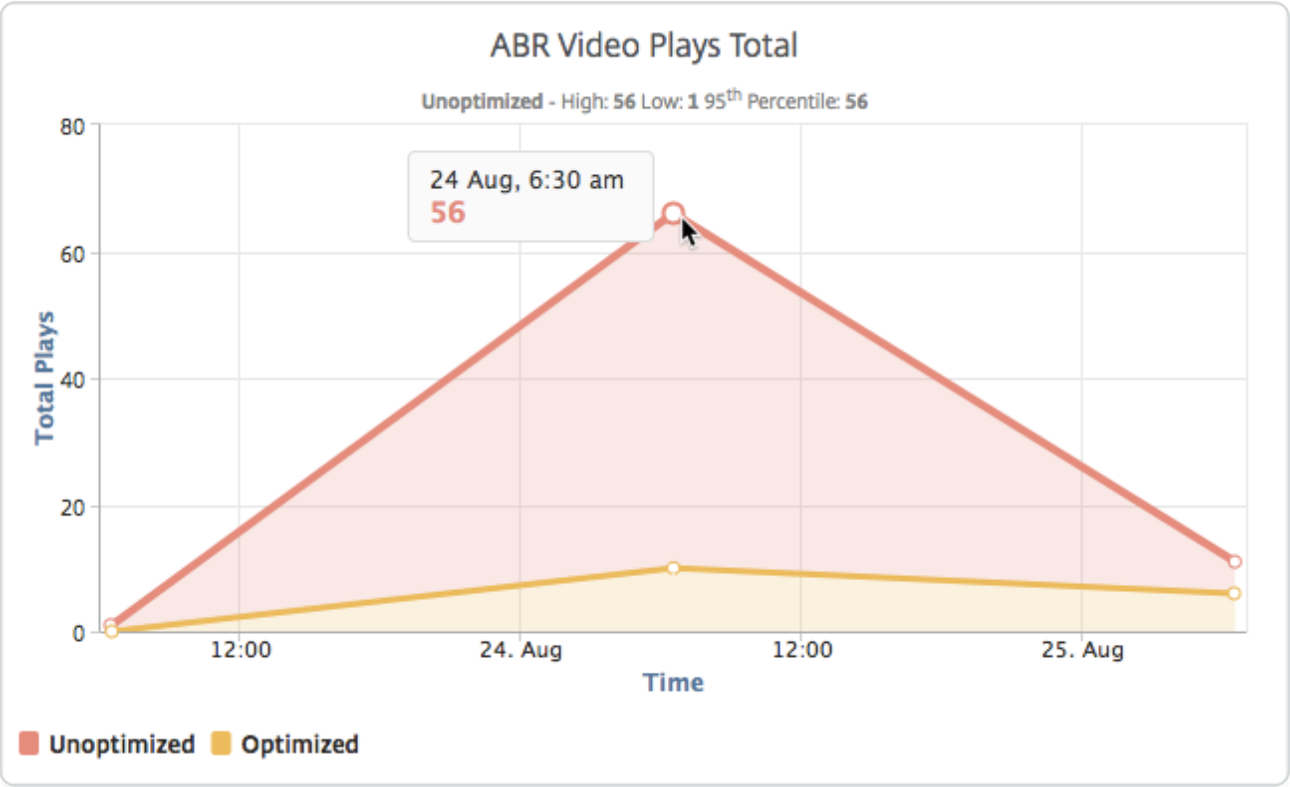
1. Navigate to **Analytics \> Video Insight**, and click **ABR Video Analytics**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **# of Plays** tab.

   You can use the **Filters** list to select the HTTP, HTTPS, or QUIC ABR videos.

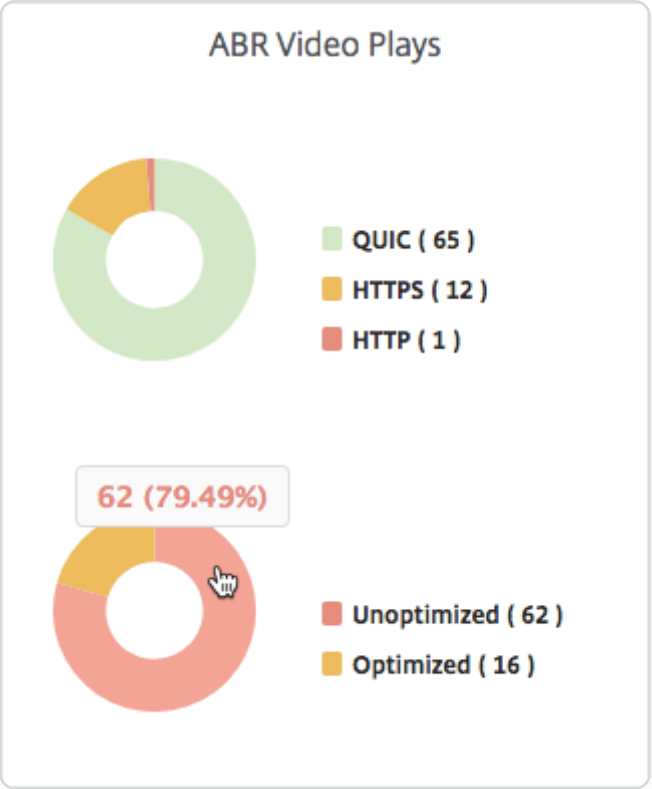


The **# of Plays** tab provides a line graph and pie chart describing the number of plays of ABR videos from your network, and the number of optimized and unoptimized plays of ABR videos from your network for the selected time frame. You can hover your mouse pointer on the line graph to view the number of plays during a particular time frame:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Also, you can hover your mouse pointer on the pie chart to the show the percentage of optimized and unoptimized plays and the percentage of encrypted and unencrypted ABR videos for the selected time frame.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

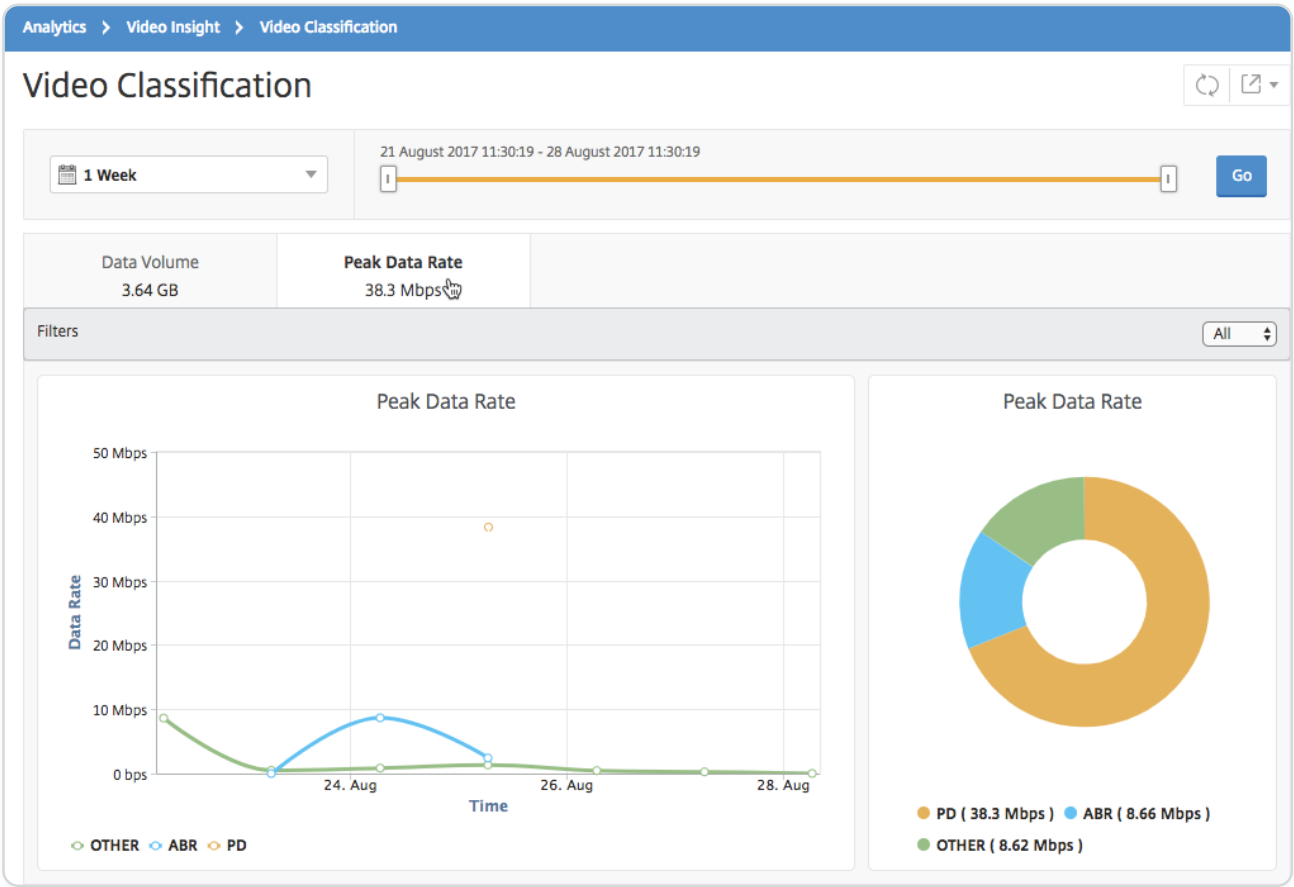
View peak data rate for a specific time frame

NetScaler® Application Delivery Management (ADM) shows you the peak throughput or data rate of the video traffic in your network.

To see the peak data rate of the video traffic:

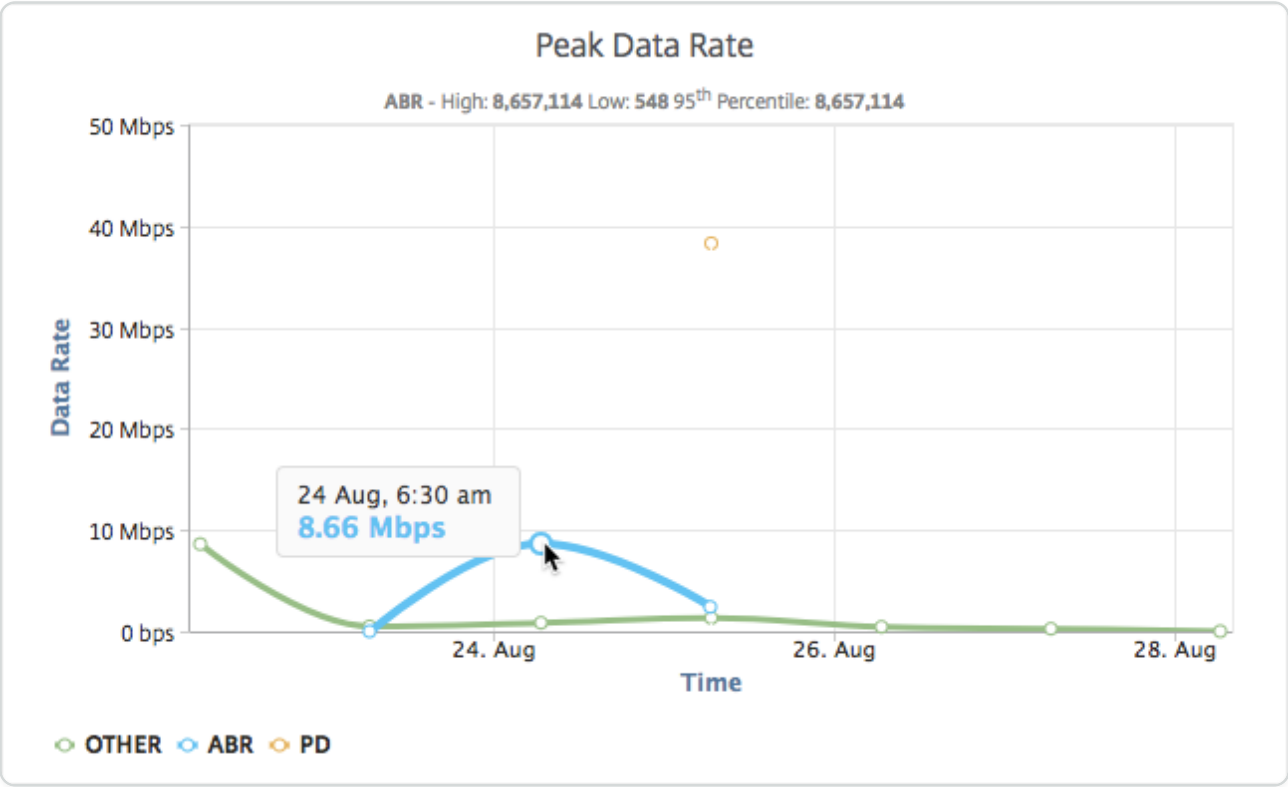
1. Navigate to **Analytics \> Video Insight**, and click **Video Classification**.
2. In the right pane, select a time frame from the list. You can further customize the time frame by using the time-frame slider.
3. Click **Go** and select **Peak Data Rate** tab.

You can use the **Filters** list to select the HTTP, HTTPS, or QUIC traffic.

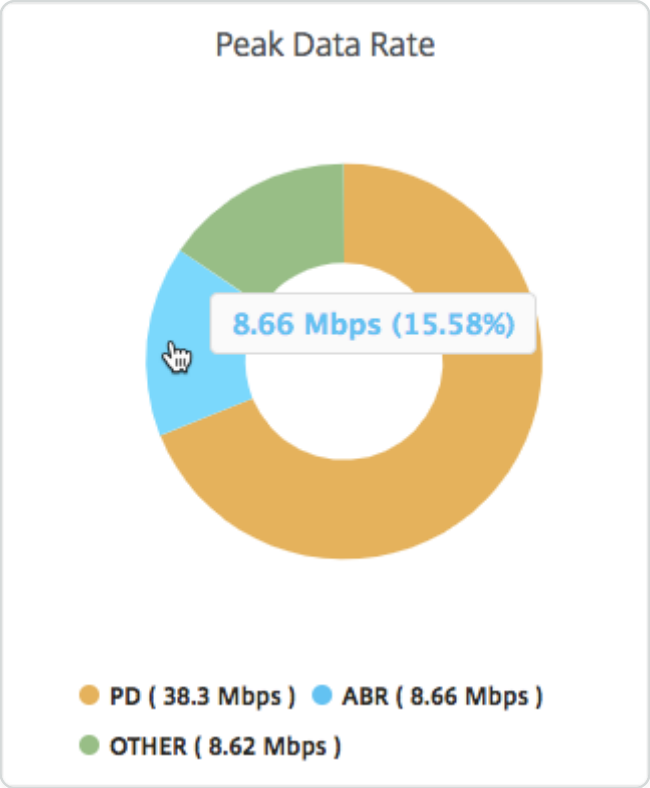


The **Peak Data Rate** tab provides a line graph and pie chart describing the peak data rate of the type of video traffic streaming from your network and the peak data rate of the video traffic on your network during the selected time frame. You can hover your mouse pointer on the line graph to show the peak data rate during a particular time frame.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Also, you can hover your mouse pointer on the pie chart to the show the percentage of the peak data rate consumed by the type of video traffic streamed during the selected time frame.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure IP address management (IPAM)

ADM IPAM provides you an ability to auto-assign and release IP addresses in ADM managed configurations. You can assign IP addresses from networks or IP ranges defined using the following IP providers:

- ADM built-in IPAM provider.
- Infoblox IPAM solution. For more information, see Infoblox DDI.

Currently, you can use ADM IPAM in:

- **StyleBooks**: Auto-Allocate IPs to virtual servers when you create configurations.
- **Kubernetes Ingress**: Auto-assign a virtual IP address to an Ingress configuration in a Kubernetes cluster.

You can also track the allocated and available IP addresses in each network or IP range managed by ADM.

Add an external IP address provider

ADM has a built-in IPAM provider to manage IPs and IP ranges. If you want to add an external IP provider solution in ADM, perform the following steps:

1. Navigate to **Infrastructure > IPAM**.
2. In **Providers**, click **Add**.
3. Specify the following details to add an IP provider:
    - **Name** - Specify the IP provider name to use in ADM.
    - **Vendor** - Select an IP address vendor from the list.
    - **URL** - Specify the URL of the IPAM solution that assigns IP addresses in ADM environment.
    - **User Name** - Specify the user name to log in to IPAM solution.
    - **Password** - Specify the password to log in to IPAM solution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Add**.

Add a network

Add a network to use IPAM with ADM managed configurations.

1. Navigate to **Infrastructure > IPAM**.
2. In **Networks**, click **Add**.
3. Specify the following details:

   - **Network Name** - Specify the network name to identify the network in ADM.
   - **Provider** - Select the provider from the list.

     This list displays the providers added in ADM.
   - **Network Type** - Select **IP range** or **CIDR** from the list based on your requirement.
   - **Network Value** - Specify the network value.

     NOTE

     ADM IPAM supports only IPv4 addresses.

     For **IP range**, specify the network value in the following format:

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Example:

     ```
     10.0.0.20-10.0.0.100
     ```

     For **CIDR**, specify the network value in the following format:

     ```
     <IP-address>/<subnet-mask>
     ```

     Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10.70.124.0/24
```

4. Click **Create**.

View allocated IP addresses

To view more details about allocated IP addresses from the IPAM network, do the following steps:

1. Navigate to **Infrastructure > IPAM**.
2. In the **Networks** tab, click **View All Allocated IPs**.

   This pane displays IP address, provider name, provider vendor, and description. It also displays the resource details that reserved this IP address:

   - **Module**: Displays the ADM module that reserves the IP address. For example, if the IP address is reserved by StyleBooks, this column displays StyleBooks as the module.
   - **Resource Type**: Displays the resource type in that module. For the StyleBooks module, only the configurations resource type uses the IPAM network.
   - **Resource ID**: Displays the resource ID with a link. Click this link to access the resource that uses the IP address. For the configuration resource type, the resource ID is displayed as the configuration pack ID.

NOTE

If you want to release the IP address, select the IP address that you want to release and click **Release Allocated IPs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use ADM audit logs for managing and monitoring your infrastructure

You can use the NetScaler® ADM service to track all events on ADM and syslog events generated on ADM-managed ADC instances. These messages can help you manage and monitor your infrastructure. But log messages are a great source of information only if you review them, and ADM simplifies the way of reviewing log messages.

You can use filters to search ADM syslog and audit log messages. The filters help to narrow down your results and find exactly what you are looking for and in real time. The built-in Search Help guides you to filter the logs. Another way to view log messages is to export them in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses at various intervals.

You can review the following types of log messages from the ADM GUI:

- ADC instance related audit logs
- ADM related audit logs
- Application audit logs

ADC instance related audit logs

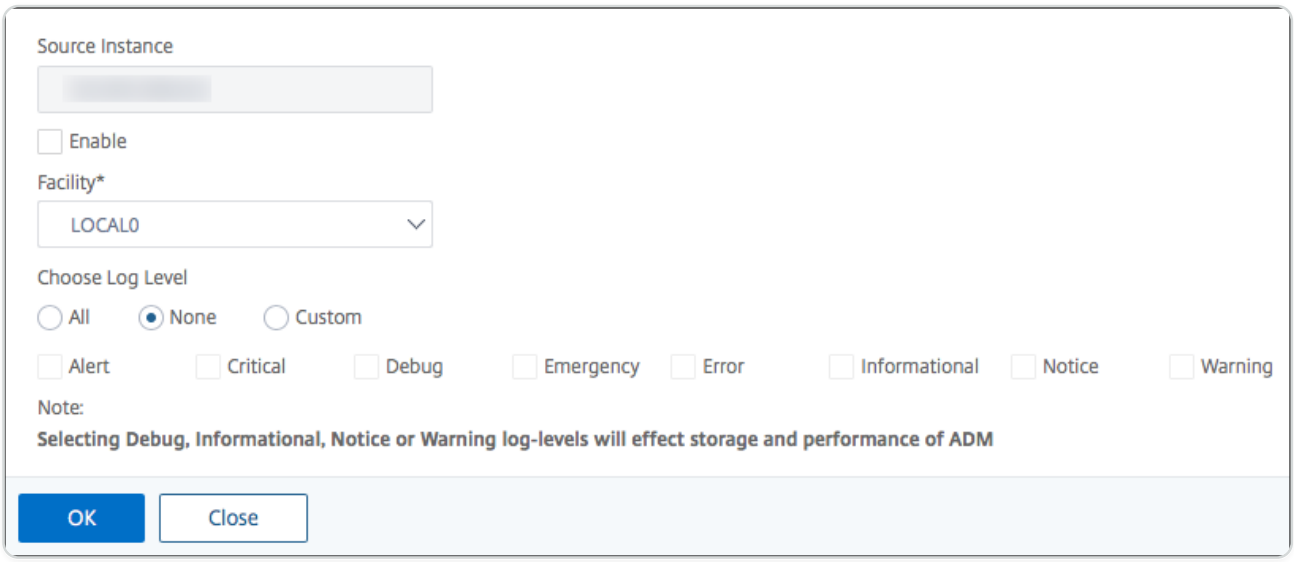
Before you can view ADC instance-related syslog messages from ADM, configure the NetScaler ADM service as the syslog server for your NetScaler instance. After the configuration is complete, all syslog messages are redirected from the instance to ADM.

Configure the ADM service as a syslog server

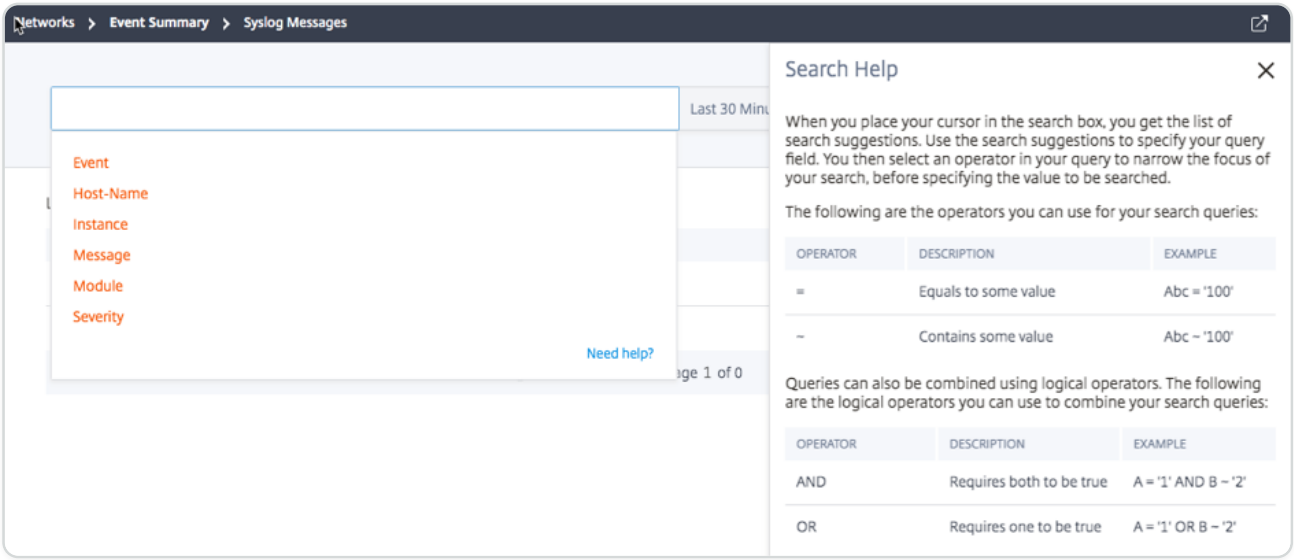
Follow these steps to configure ADM as the syslog server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From the ADM GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler ADM.
3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.



These steps configure all the syslog commands in the NetScaler instance, and NetScaler ADM starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**. Click **Need Help?** to open the built-in search help. For more information, see View and export syslog messages.



To export the log messages, click the arrow icon on the upper right corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Next, click **Export Now** or **Schedule Export**. For more information, see View and export syslog messages.

ADM related audit logs

Based on preconfigured rules, ADM generates audit log messages for all events on, helping you monitor the health of your infrastructure. To view all audit log messages present in the ADM, navigate to **Settings > ADM Audit Log Messages**.

To export the log messages, click the arrow icon on the upper right corner.

Application related audit logs

You can view the audit log messages for all ADM applications or for a specific application.

- To view all audit log messages for all applications present in the ADM, navigate to **Infrastructure > Network Functions > Auditing**.
- To view audit log messages for any specific application in the ADM, navigate to **Applications > Dashboard**, click a virtual server and select **Audit Log**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage instance licenses

NetScaler ADM enables you to manage and allocate licenses to your NetScaler instances. The following topics help you manage instance licenses:

- NetScaler pooled capacity
- NetScaler VPX check-in and check-out licensing
- NetScaler virtual CPU licensing

NetScaler pooled capacity

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
The NetScaler pooled capacity allows you to share bandwidth or instance licenses across different ADC form factors. For virtual CPU subscription-based instances, you can share virtual CPU license across instances. Use this pooled capacity for the instances that are in the data center or public clouds. When an instance no longer requires the resources, it checks the allocated capacity back into the common pool. Reuse the released capacity to other ADC instances that need resources.

You can use pooled licensing to maximize the bandwidth utilization by ensuring the necessary bandwidth allocation to an instance and not more than its need. Increase or decrease the bandwidth allocated to an instance at run time without affecting the traffic. With the pooled capacity licenses, you can automate the instance provisioning.

How NetScaler pooled capacity licensing works

NetScaler pooled capacity has the following components:

- NetScaler instances, which can be categorized into:
  - Zero-capacity hardware
  - Standalone VPX instances or CPX instances or BLX instances
- Bandwidth pool
- Instance pool
- NetScaler ADM configured as a license server

Zero-capacity hardware

When managed through NetScaler pooled capacity, MPX and SDX instances are referred to as "zero-capacity hardware" because these instances cannot function until they check resources out of the bandwidth and instance pools. Thus, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware requires a platform license to be able to check out bandwidth and an instance license from the common pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- Instance license subscription is not required for MPX instances. See table 1 in this page, for supported pooled capacity for MPX and SDX instances. See table 5 for license requirement for different MPX and SDX form factors.
- The zero capacity license installation works the same way as other NetScaler local licenses. For more information about how to obtain and install a zero capacity license, see Licensing guide for NetScaler.

Manage and install platform licenses

You must install a platform license manually, by using the hardware serial number or the license access code. After a platform license is installed, it is locked to the hardware and cannot be shared across NetScaler hardware instances on demand. However, you can manually move the platform license to another NetScaler hardware instance.

NetScaler MPX instances running the ADC software release 11.1 build 54.14 or later and NetScaler SDX instances running 11.1 build 58.13 or later support ADC pooled capacity. For more information, see **Table 1. Supported pooled capacity for MPX and SDX instances**.

Standalone NetScaler VPX instances

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 and later on the following hypervisors supports pooled-capacity:

- VMware ESX 6.0
- Citrix Hypervisor™
- Linux KVM

NetScaler VPX instances running NetScaler software release 12.0 Build 51.24 and later on the following hypervisors and cloud platforms supports pooled-capacity:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX instances running NetScaler software release 13.0 and 13.1 (all versions) on the following hypervisors and cloud platforms support pooled-capacity:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NOTE

To enable communication between NetScaler ADM and Microsoft Azure or AWS, an IPSEC tunnel has to be configured. For more information, see Add NetScaler VPX Instances Deployed in Cloud to NetScaler ADM. Unlike zero-capacity hardware, VPX does not require platform license. To process traffic, it must check out bandwidth and an instance license from the pool.

Standalone NetScaler CPX instances

NetScaler CPX instances deployed on a Docker host support pooled-capacity. Unlike zero-capacity hardware, CPX does not require a platform license. A single CPX instance consuming up to 1 Gbps throughput checks-out only 1 instance and no bandwidth from the license pool. For example, consider that you have 20 CPX instances with 20 Gbps bandwidth pool. If one of the CPX instances consumes 500 Mbps throughput, the bandwidth pool remains 20 Gbps for the remaining 19 CPX instances.

If the same CPX instance starts to consume 1500 Mbps throughput, the bandwidth pool has 19.5 Gbps for the remaining 19 CPX instances.

For pool licensing, you can add more bandwidth only in multiples of 10 Mbps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standalone NetScaler BLX instances

NetScaler BLX instances support pooled-capacity licenses. A NetScaler BLX instance does not require a platform license. To process traffic, a NetScaler BLX instance must check out bandwidth and an instance license from the pool.

Bandwidth Pool

The bandwidth pool is the total bandwidth that can be shared by NetScaler instances, both physical and virtual. The bandwidth pool comprises separate pools for each software edition (Standard, Advanced, and Premium). A given NetScaler instance cannot have bandwidth from different pools checked out concurrently. The bandwidth pool from which it can check out bandwidth depends on its software edition for which it is licensed.

Instance pool

The instance pool defines the number of VPX instances or CPX instances or BLX instances that can be managed through NetScaler pooled capacity or the number of VPX instances in an SDX-Z instance.

When checked out from the pool, a license unlocks the MPX-Z, SDX-Z, VPX, CPX, and BLX instance's resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

NOTE

The Management Service of an SDX-Z does not consume an instance.

NetScaler ADM license server

NetScaler pooled capacity uses the NetScaler ADM configured as a license server to manage pooled capacity licenses: bandwidth pool licenses and instance pool licenses. You can use the NetScaler ADM software to manage pooled capacity licenses without an ADM license.

When checking out licenses from bandwidth and instance pool, NetScaler form factor and hardware model number on a zero-capacity hardware determines

- The minimum bandwidth and the number of instances that a NetScaler instance must check out before being functional.
- The maximum bandwidth and the number of instances that a NetScaler can check out.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The minimum bandwidth unit for each bandwidth check-out. The minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if the minimum bandwidth unit of a NetScaler is 1 Gbps, 1000 Mbps can be checked out, but not 200 Mbps or 150.5 Gbps. The minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check out more bandwidth with the minimum bandwidth unit.

Tables 1, 2, 3, and 4 summarize the maximum bandwidth/instances, minimum bandwidth/instances, and minimum bandwidth unit for all supported NetScaler instances. Table 5 summarizes the license requirement for different form factors for all supported NetScaler instances:

Table 1. Supported pooled capacity for MPX and SDX instances

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
MPX 5900Z	10	1	N/A	N/A	1 Gbps
MPX 8900Z	30	5	NA	NA	1 Gbps
MPX 9100Z	30	10	NA	NA	1 Gbps
MPX 8900Z FIPS	33	5	NA	NA	1 Gbps
MPX 14000Z series	100	20	NA	NA	1 Gbps
MPX 14000Z 40G series	100	20	N/A	N/A	1 Gbps
MPX 14000Z FIPS series	100	20	N/A	N/A	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
MPX 14000Z 40S series	100	20	N/A	N/A	1 Gbps
MPX 15000Z series	120	20	N/A	N/A	1 Gbps
MPX 15000Z FIPS series	120	20	N/A	N/A	1 Gbps
MPX 15000Z 50G series	120	20	N/A	N/A	1 Gbps
MPX 16000Z series	200	30	N/A	N/A	1 Gbps
MPX 22000Z series	120	40	N/A	N/A	1 Gbps
MPX 24000Z series	150	100	N/A	N/A	1 Gbps
MPX 25000Z 40G	200	100	N/A	N/A	1 Gbps
MPX 25000ZA	200	100	N/A	N/A	1 Gbps
MPX 26000Z series	200	100	N/A	N/A	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
MPX 26000Z 100G series	200	100	N/A	N/A	1 Gbps
MPX 26000Z 50S series	200	100	N/A	N/A	1 Gbps
SDX 8900Z	30	10	2	7	1 Gbps
SDX 9100Z	95	20	4	7	1 Gbps
SDX 14000Z series	100	10	2	25	1 Gbps
SDX 14000Z 40G series	100	10	2	25	1 Gbps
SDX 14000Z 40S series	100	20	10	25	1 Gbps
SDX 14000Z FIPS series	100	10	2	25	1 Gbps
SDX 15000Z 50G	120	10	2 (Note: 5 instances for versions lower than 13.0 47.x)	55	1 Gbps
SDX 15000Z	120	10	2 Note: 5 instances for versions lower than 13.0 47.x)	55	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 16000Z series	200	15	10	55	1 Gbps
SDX 22000Z series	120	20	20	80	1 Gbps
SDX 25000Z 40G	200	50	10	115	1 Gbps
SDX 25000ZA	200	50	10	115	1 Gbps
SDX 26000Z 100G	200	50	10	115	1 Gbps
SDX 26000Z	200	50	10	115	1 Gbps
SDX 26000Z 50S	200	50	10	115	1 Gbps
SDX 24000Z series	150	50	10	80	1 Gbps

Note

> The minimum bandwidth and instances are applicable to SDX instances running the following releases and higher: 11.1 64.x, 12.0 63.x, 12.1 54.x, and 13.0 41.x.

The minimum purchase quantity is different from the minimum system requirement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 2. Supported pooled capacity for CPX instances

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
CPX	10	10	1	1	10 Mbps

Table 3. Supported pooled capacity for VPX instances on Hypervisors and Cloud services

HYPERVISOR/CLOUD SERVICE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

Note

> The minimum purchase quantity is different from the minimum system requirement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 4. Supported pooled capacity for BLX instances

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
BLX	100	10	1	1	10 Mbps

Table 5. License requirement for different form factors

PRODUCT LINE	ZERO CAPACITY HARDWARE PURCHASE	BANDWIDTH AND EDITION SUBSCRIPTION	INSTANCE SUBSCRIPTION
MPX	License required	License required	-
SDX	License required	License required	License required
VPX	-	License required	License required
CPX	-	-	License required
BLX	-	License required	License required

Configure NetScaler pooled capacity

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

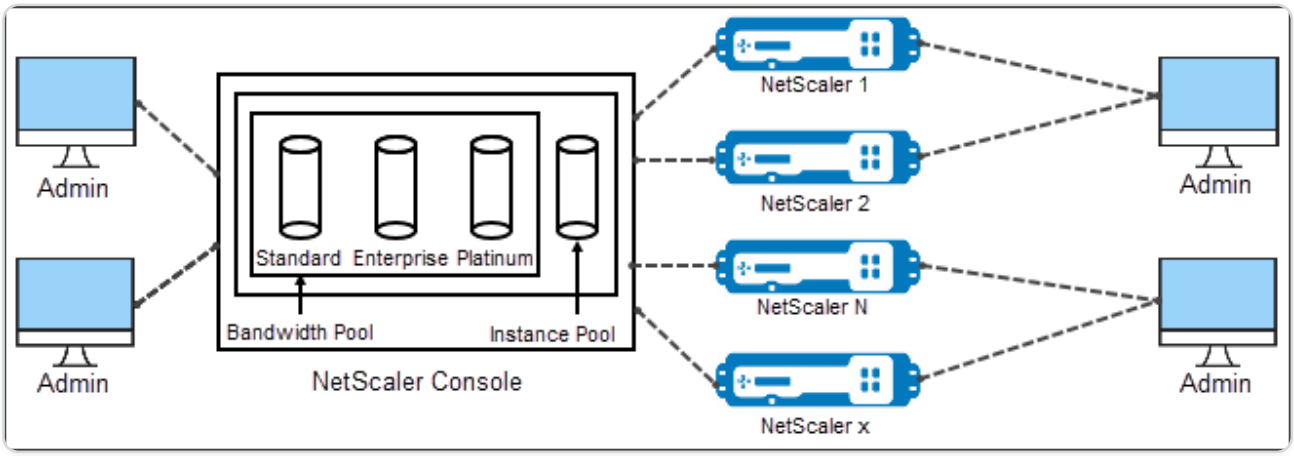
- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
To use ADC pooled capacity, configure NetScaler ADM as a license server to the required ADC instances. ADC instances check in and check out licenses from the ADM. You can perform the following tasks in the ADM GUI:

- Upload the pooled capacity license files (bandwidth and instance pool) to the license server.
- Allocate licenses from the license pool to NetScaler instances on demand.
- Check out the licenses from NetScaler instances (MPX-Z /SDX-Z/VPX/CPX/BLX) based on the minimum and maximum capacity of the instance.
- Configure pooled capacity for NetScaler FIPS instances to check in or check out licenses.



Supported hardware and software versions

For supported hardware and software versions for pooled capacity, see NetScaler pooled capacity.

ADC pooled capacity states

The pooled capacity states indicate the license requirement on an ADC instance. The ADC instances configured with pooled capacity display one of the following states:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Optimum**: Instance is running with proper license capacity.
- **Capacity mismatch**: Instance is running with a capacity less than the user configured.
- **Grace**: Instance is running on a grace license.
- **Grace & Mismatch**: Instance is running on grace but with a capacity less than the user configured.
- **Not available**: Instance is not registered with ADM for management, or NITRO communication from ADM to the instances is not working.
- **Not allocated**: License is not allocated in the instance.

Step 1 - Apply licenses in ADM

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Files** section, select **Add License File** and select one of the following options:
   - **Upload license files from a local computer**. If a license file is already present on your local computer, you can upload it to ADM.
   - **Use license access code**. Specify the license access code for the license that you have purchased from Citrix. Then, select **Get Licenses**. Then select **Finish**.

   NOTE

   At any time, you can add more licenses to ADM from **License Settings**.

3. Click **Finish**.

   The license files are added to ADM. The **License Expiry Information** tab lists the licenses present in the ADM and the remaining days to expiry.
4. In **License Files**, select a license file that you want to apply and click **Apply licenses**.

   This action enables ADC instances to use the selected license as a pooled capacity.

   For more information on how to apply pooled licenses to NetScaler ADM, see the related video Clickhere.

Step 2 - Register NetScaler ADM as a license server

To register ADM as a license server to a NetScaler instance, follow one of the procedures:

- Use GUI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use CLI

Use GUI to register ADM as a license server

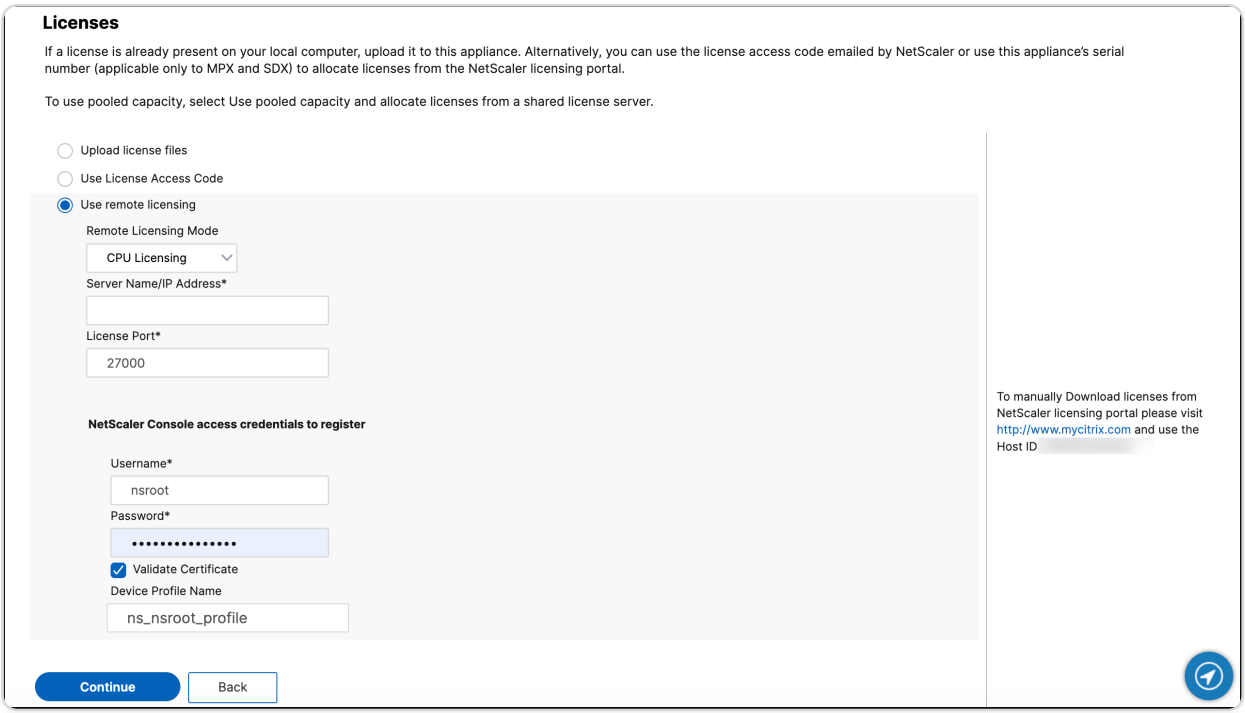
In the ADC GUI, register the ADM server as a license server.

1. Log in to NetScaler GUI.
2. Navigate to **System** > **Licenses** > **Manage Licenses**.
3. Click **Add New License**.
4. Select **Use remote licensing** and select the remote licensing mode from the list.
5. In the **Server Name/IP address** field, specify the ADM server's IP address.

   For a HA deployment, use a floating IP. For more information on configuration, see Configure High Availability Deployment.

   > For a deployment which uses a standalone ADM or an agent, seeLicensing overview

6. Select **Register with NetScaler ADM**.
7. Enter your ADM credentials to register an instance with NetScaler ADM and click **Continue**.



8. In **Allocate licenses**, select the license edition and specify the required bandwidth.

   For the first time, allocate licenses in NetScaler. You can later change or release the license allocation from the ADM GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Click **Get Licenses**.

IMPORTANT:

Warm restart the instance if you change the license edition. The configuration changes do not take effect until you restart the instance.

Use CLI to add ADM as a license server

If an ADC instance has no GUI, use the following CLI commands to add the ADM server as a license server:

1. Log in to the ADC console.
2. Add the ADM server IP address:

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
```

For more information, see Licensing overview.

3. View the license bandwidth available in the license server.

```
> sh ns licenseserverpool
```

This command lists the licenses based on the specified license mode while adding the license server.

Example-1:

If the specified license mode is `CICO`, the output contains only CICO licenses.

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                    : 1
        VPX8000P Available                : 1
```

Example-2:

If the specified license mode is `Pooled`, the output contains only pooled capacity licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                      : 40
        Instance Available                  : 38
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
```

Example-3:

If the specified license mode is `vCPU`, the output contains only virtual CPU licenses.

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

To view all the licenses together, run the following command:

```
> sh ns licenseserverpool -getallLicenses
```

Example output:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. Allocate the license bandwidth from the required license edition:

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify-amount-license-bandwidth> -edition <specify-license-edition>
```

The license edition can be **Standard** or **Enterprise** or **Platinum**.

IMPORTANT

Warm restart the instance if you change the license edition.

`reboot -w`

The configuration changes does not take effect until you restart the instance.

Step 3 - Allocate pooled licenses to ADC instances

To allocate pooled capacity licenses from the ADM GUI:

1. Log in to NetScaler ADM.
2. Navigate to **Infrastructure > Licenses > Bandwidth Licenses > Pooled Capacity**.

   The FIPS instance capacity appears only if you upload FIPS instance licenses to ADM.
3. Click the license pool that you want to manage.

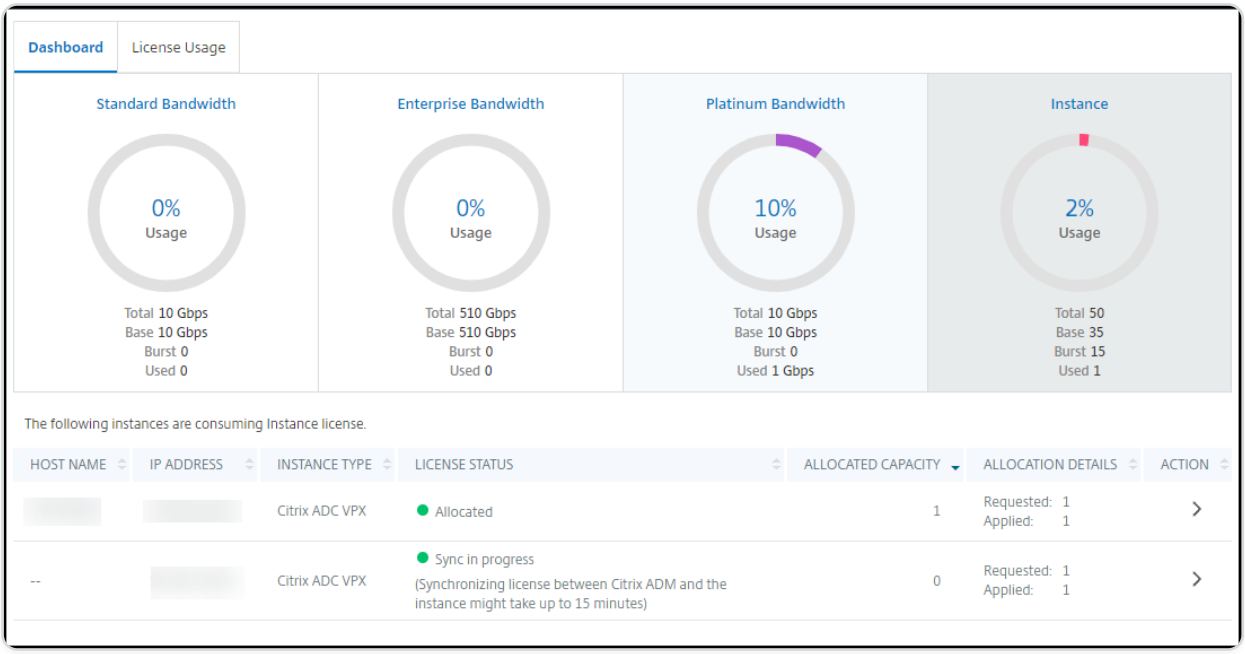
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The **Allocated Capacity** field does not reflect the changed bandwidth immediately. The bandwidth change takes effect after the ADC warm restart.

In **Allocation Details**, the **Requested** and **Applied** fields are updated when you change the instance's bandwidth allocation.

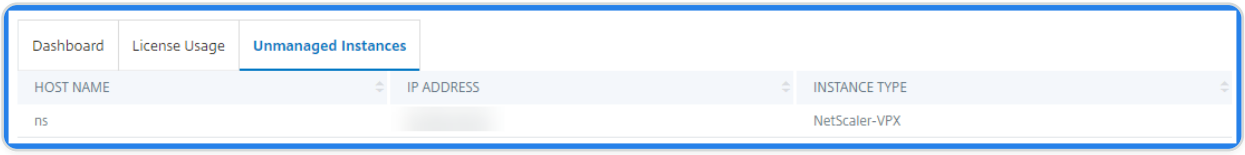
4. Select an ADC instance from the list of available instances by clicking the **>** button.



The **LICENSE STATUS** column displays corresponding license allocation status messages.

NOTE:

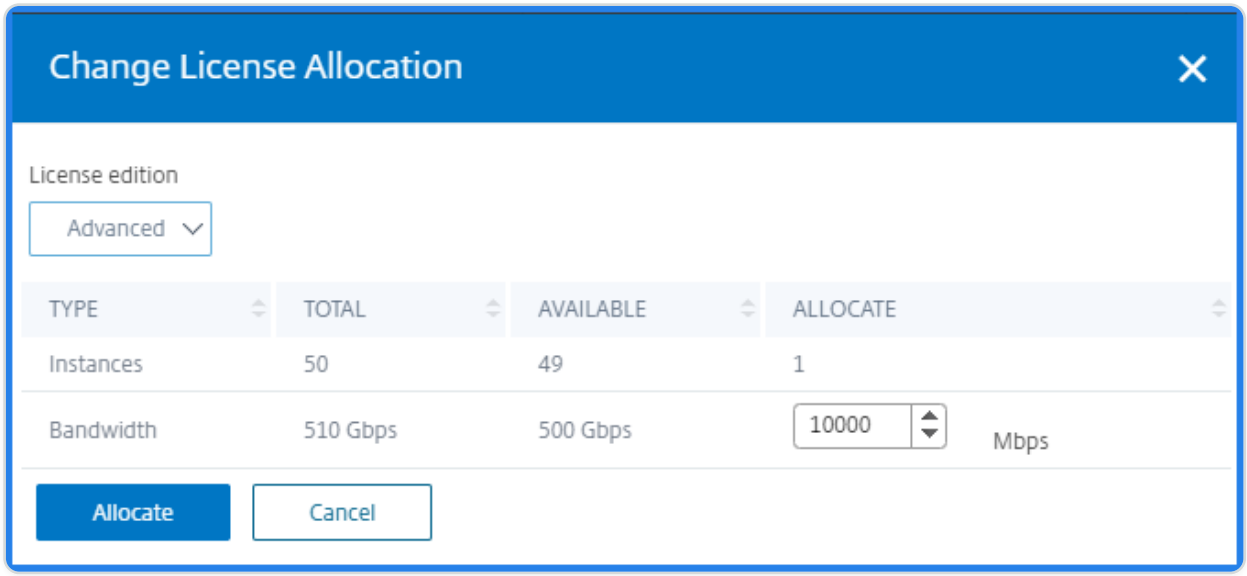
The **Unmanaged Instances** tab displays the instances that are discovered but not managed in NetScaler ADM.



5. Click **Change allocation** or **Release allocation** to modify the license allocation.
6. A pop-up window with the available licenses in the License Server appears.
7. You can choose the bandwidth or instance allocation to the instance by setting the **Allocate** list options. After making your selections, click **Allocate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. You can also change the allocated license edition from the list options in the **Change License Allocation window**.



NOTE

Warm restart an instance if you change the license edition.

For more information on how to change the bandwidth allocation, see the related video Clickhere.

Configure pooled capacity on ADC instances

You can configure pooled capacity licenses on the following ADC instances:

- NetScaler instances
- NetScaler VPX™ instances
- NetScaler high-availability pair

NetScaler MPX™ instances

MPX-Z is the pooled capacity enabled NetScaler MPX appliance. MPX-Z supports bandwidth pooling for Premium, Advanced, or Standard edition licenses.

MPX-Z requires platform licenses before it can connect to the License Server. You can install the MPX-Z platform license by either of the following:

- Uploading the license file from a local computer.
- Using the instance's hardware serial number.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The License Access Code from the **System** > **Licenses** section of the instance's GUI.

If you remove the MPX-Z platform license, the pooled-capacity feature is disabled. The instance licenses are released to the license server.

You can dynamically modify the bandwidth of an MPX-Z instance without a restart. A restart is required only if you want to change the license edition.

NOTE:

When you restart the instance, it automatically checks out the pooled licenses required for its configured capacity.

NetScaler VPX instances

A pooled capacity enabled NetScaler VPX instance can check out licenses from a bandwidth pool (Premium/Advanced/Standard editions). You can use the ADC GUI to check out licenses from the License Server.

You can dynamically modify the bandwidth of a VPX instance without a restart. A restart is required only if you want to change the license edition.

NOTE:

When you restart the instance, the configured pooled capacity licenses are automatically checked out from the ADM server.

NetScaler high-availability pair

Before you begin, ensure that the ADM server is configured as a license server. For more information, see Configure ADM as a license server.

For ADC instances configured in a high availability mode, you have to configure pooled capacity on each node of the high availability pair. For both the primary and secondary nodes, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity to each node.

To allocate pool license to each node in the pair, follow the steps given in Allocate pooled licenses to ADC instances. First allocate license to the first node and then repeat the same steps to allocate license to the second node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure an ADM server only as the pooled license server

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
As an administrator, you can configure an ADM server only as the pooled license server. With this configuration, the ADM server only receives licensing data from ADC instances.

Sometimes, you might have the regulatory mandate that requires restricting ADC instances’ data from leaving the regulatory zone. In such situations, you can deploy a local instance of an ADM on-prem server in your regulatory zone to use management, monitoring, and analytics capabilities. When you follow the same approach to use the pooled licenses feature, you have to split pooled licenses across various ADM license servers. This approach does not provide you the flexibility to allocate pooled licenses across your globally deployed ADC instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Therefore, configure the ADM server only as the pooled license server. The ADM server receives only licensing data from all ADC instances. So, you can adhere to the regulatory mandate and dynamically allocate pooled capacity licenses across globally deployed ADC instances.

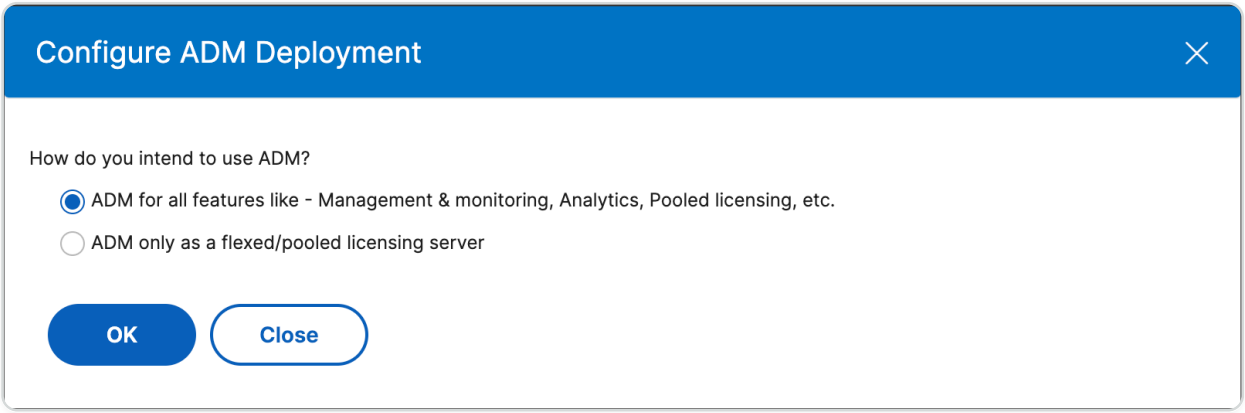
This document explains how to configure an ADM server only as the pooled license server.

How to configure an ADM server only as the pooled license server

Before you begin, ensure no ADC instances are added to an ADM server. Add the ADC instances only after you complete step 4.

Do the following to configure an ADM server only for the pooled license server:

1. Navigate to **Settings > Administration**.
2. In the **System Configurations** section, select **System Deployment**.
3. In **ADM Deployment**, select **ADM only as a pooled licensing server**.



4. Click **OK**.

   This action retains only the pooled licensing feature and disables the following ADM features:

   - ADM backup
   - Event management
   - SSL certificate management
   - Network reporting
   - Network functions
   - Configuration audit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

By default, the ADM analytics feature is disabled. Make sure to disable this feature if you have enabled it.

In the confirmation box, click **Yes**.

The ADM GUI now displays only the pooled licensing feature. And, the remaining features do not appear.

5. After you configure ADM only for the licensing feature, add ADC instances in the **Infrastructure > Instances** page.

NOTE

- You can add an ADC instance in one or more ADM servers. When you change the password of such ADC instances, ensure to update the password on all ADM servers where the instance is discovered.
- A user can still do some operations of the disabled features in the ADM GUI. For example, event polling and ADC backup. As a super administrator, If you want to restrict such operations, disable user accesses for other administrators using an appropriate access policy. For more information, see Configure Access Policies on NetScaler ADM.

Upgrade a perpetual license in NetScaler VPX to NetScaler pooled capacity

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
NetScaler VPX instances with perpetual license can be upgraded to ADC pooled capacity license. Upgrading to pooled capacity license enables you to allocate licenses from the license pool to the VPX instances on demand. You can also configure pooled capacity license for ADC instances configured in a high availability mode. To configure pooled capacity license for VPX instances in high availability mode, see Upgrading the Perpetual License in NetScaler VPX High Availability Pair to NetScaler Pooled Capacity.

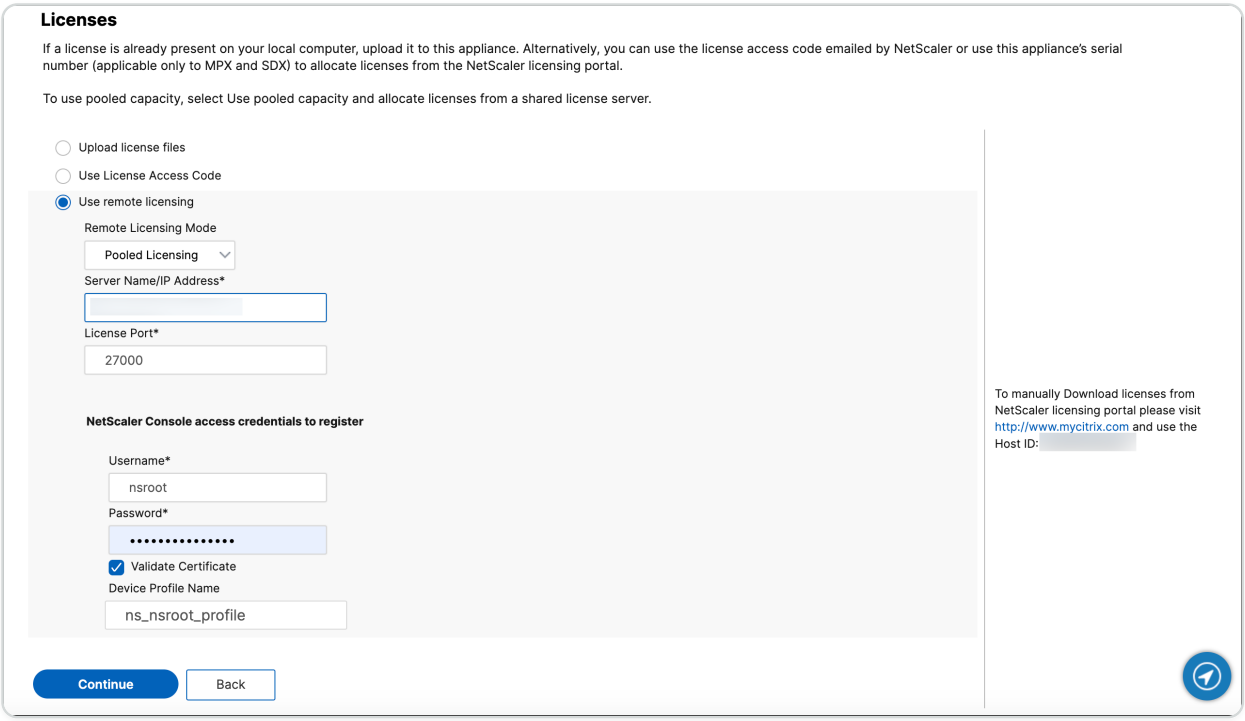
Prerequisites

Ensure that you upgrade the VPX instance to version 12.0.56.x.

To upgrade to NetScaler pooled capacity:

1. In a Web browser, type the IP address of the VPX instance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the **Configuration tab**, navigate to **System \> Licenses** and click **Manage Licenses**.
5. On the **Licenses** page, click **Add New License**.
6. On the **Licenses** page, choose **Use remote licensing** and do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.

b. In the **Server Name/IP Address** field, Enter the details of the license server.

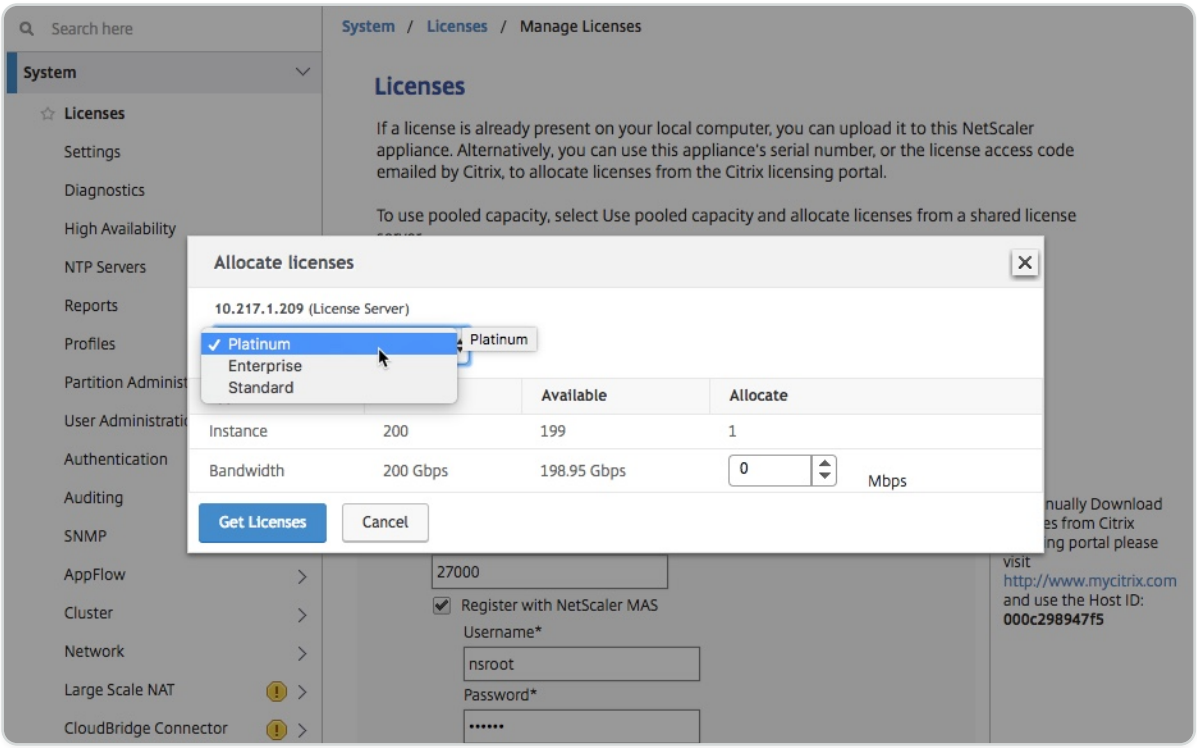
c. Make sure that the **Register with NetScaler ADM** check box is selected and enter NetScaler ADM credentials, if you want to manage your instance's pool licenses through ADM.

d. Click **Continue**.

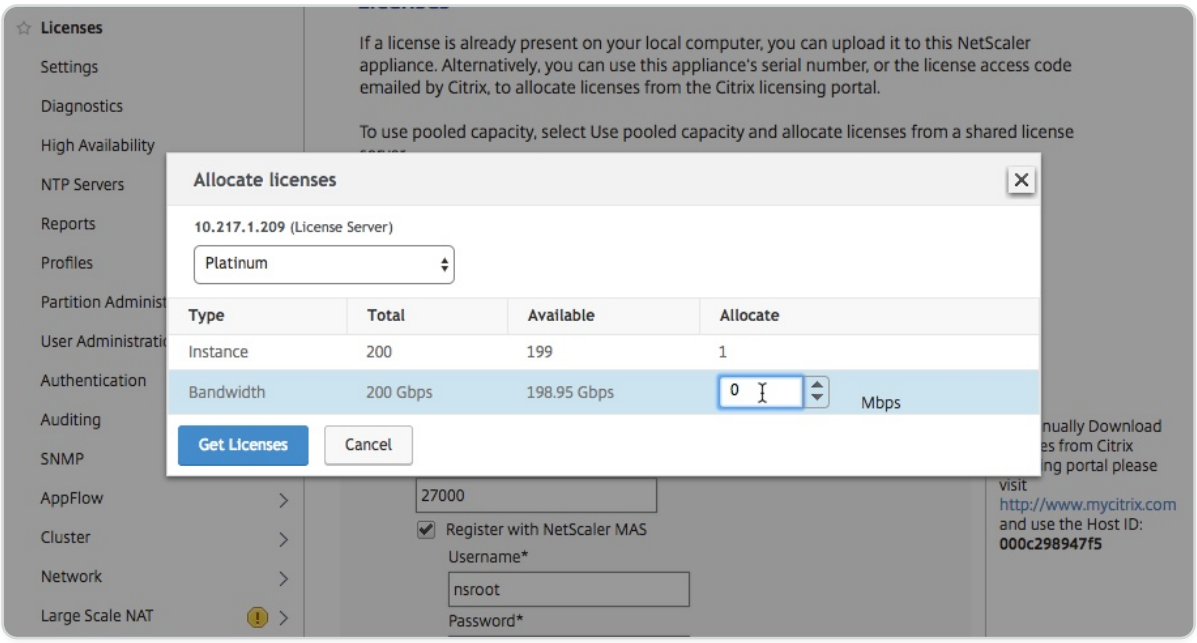
7. In **Allocate licenses**, do the following:

   a. Select the license edition from the drop-down list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

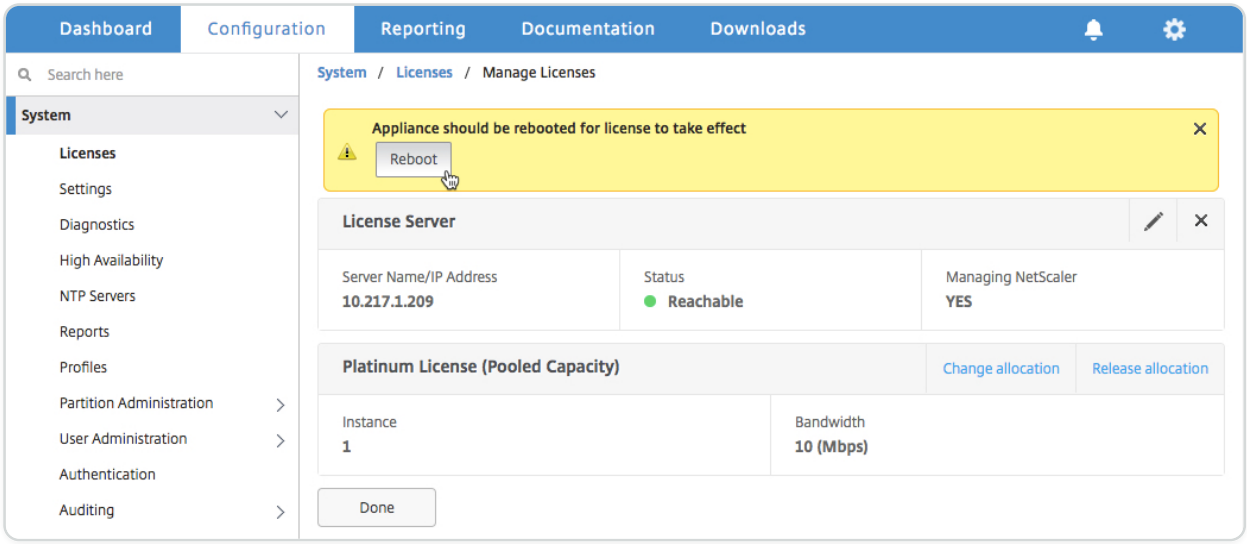


b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



8. When prompted, click **Reboot** to reboot the appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. In the Confirm dialog box, click **Yes**.
10. After the VPX instance restarts, log on to the instance. On the **Welcome** page, click **Continue**.

    The **Licenses** page displays all the features that are licensed on the NetScaler VPX appliance. Click **X**.

11. Navigate to **System \> Licenses** and click **Manage Licenses**.

    On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

Upgrade the Perpetual License in NetScaler VPX high availability pair to NetScaler pooled capacity

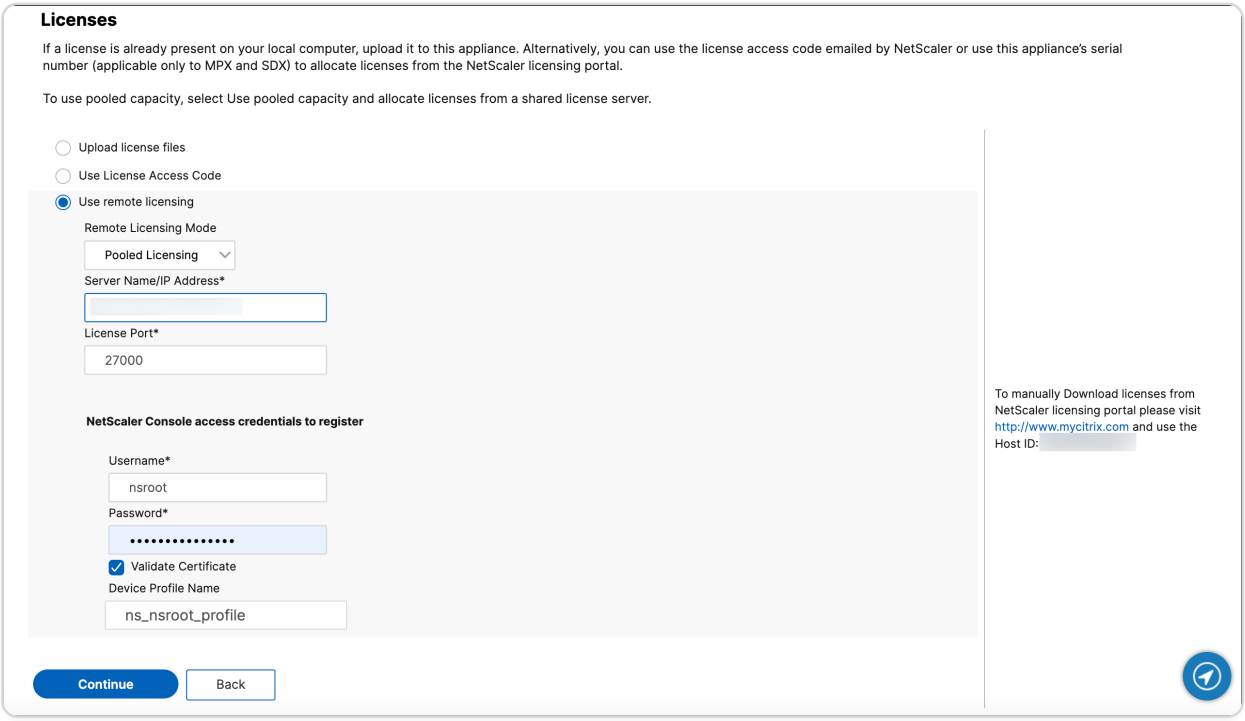
For VPX instances configured in a high availability mode, you have to configure pooled capacity on both the primary and secondary instances in the HA pair. For both the primary and secondary instances, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity each to the primary and secondary instances in the HA pair.

To upgrade an exisiting NetScaler VPX HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary VPX (node 2) instance. In a Web browser, type the IP address of the NetScaler appliance, such as `http://192.168.100.1`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the Configuration tab, navigate to **System** > **Licenses** and click **Manage Licenses**.

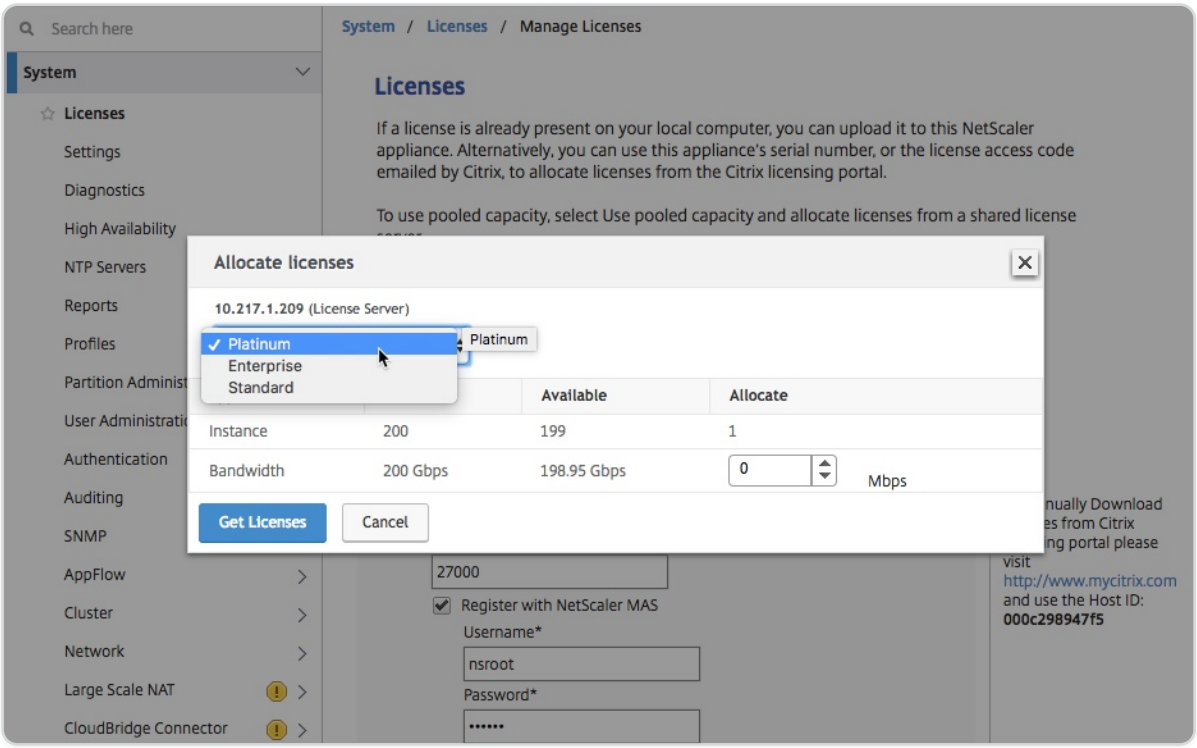
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Licenses** page, click **Add New License**.
6. Choose **Use remote licensing** and do the following:

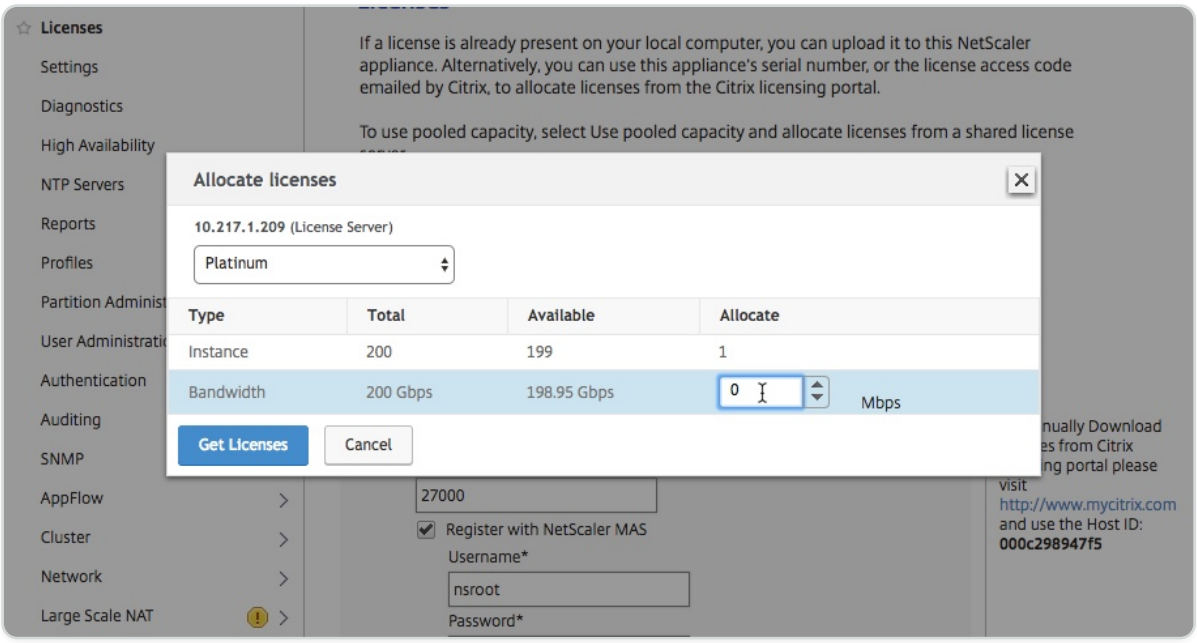


   a. In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.
   b. In the **Server Name/IP Address** field, Enter the details of the license server.
   c. Make sure that the **Register with NetScaler ADM** check box is selected and enter the ADM credentials, if you want to manage your instance's pool licenses through NetScaler ADM.
   d. Click **Continue**.
7. In **Allocate licenses**, do the following:
   a. Select the license edition from the drop-down list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

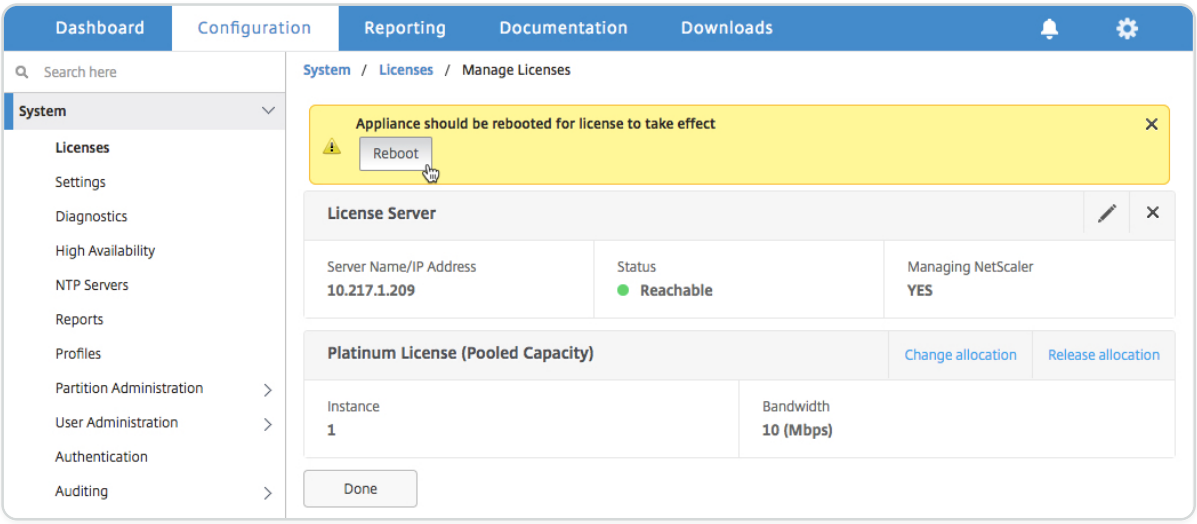


b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c. When prompted, click **Reboot** to warm restart the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. In the **Confirm** dialog box, click **Yes**.

   The VPX instance reboots.

   When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

9. After the failover, log on to the new secondary VPX instance (node 1) and repeat the same process to add the new secondary to the pool.

   If you want to change the primary and secondary instance in the HA pair to your original HA pair configuration, force a failover. Run the following command on any instance in the HA pair:

   ```
   > force ha failover
   ```

10. To verify that the VPX instance is upgraded to pooled capacity license, log on to the primary and secondary instances and complete the following steps.

    a. On the **Welcome** page, click **Continue**.

    b. On the Configuration tab, navigate to **System \> Licenses** and click **Manage Licenses**. On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrading a Perpetual License in NetScaler MPX to NetScaler Pooled Capacity

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
NetScaler MPX appliance with perpetual license can be upgraded to NetScaler Pooled Capacity license. Upgrading to NetScaler Pooled Capacity license enables you to allocate licenses from the license pool to NetScaler appliances on demand. You can also configure NetScaler Pooled Capacity license for NetScaler instances configured in high availability mode. To configure NetScaler Pooled Capacity license for NetScaler MPX instances in high availability mode, see Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler pooled capacity

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Conversion from a perpetual license to a pooled capacity license is a one-way process for license entitlement. You can't revert the pooled capacity license to perpetual. **Important**

For upgrading NetScaler MPX appliance to NetScaler Pooled Capacity license, you need to upload the MPX-Z license to the appliance.

To upgrade to NetScaler Pooled Capacity:

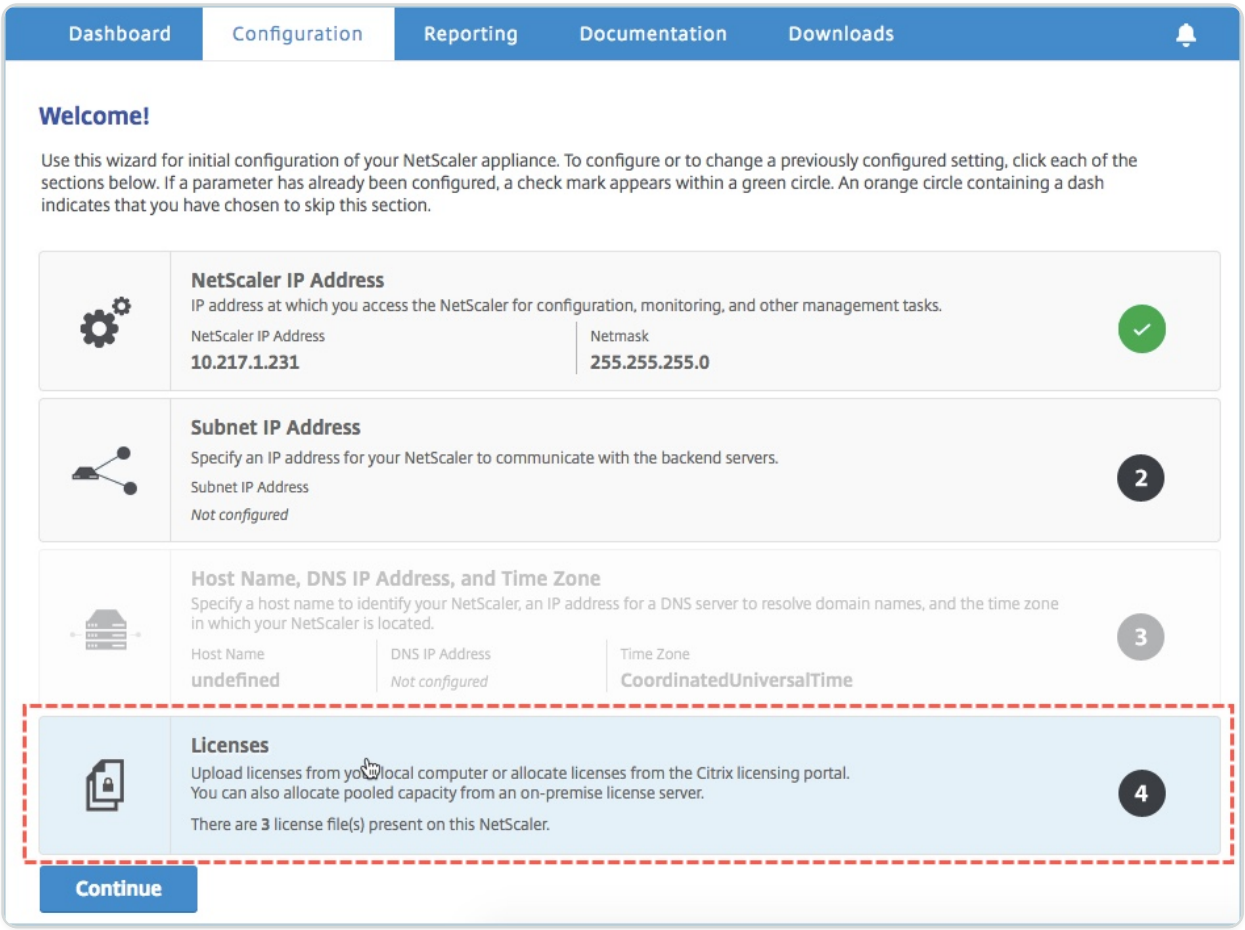
1. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the Configuration tab, navigate to **System** \> **Licenses**.
5. In the details pane, click **Manage Licenses**, click Add **New License**.
6. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.
7. After the license is uploaded, click **Reboot** to reboot the appliance.

   WARNING

   After applying the MPX-Z license, the features including SSL offloading on the appliance become unlicensed. The appliance stops processing HTTPS requests.

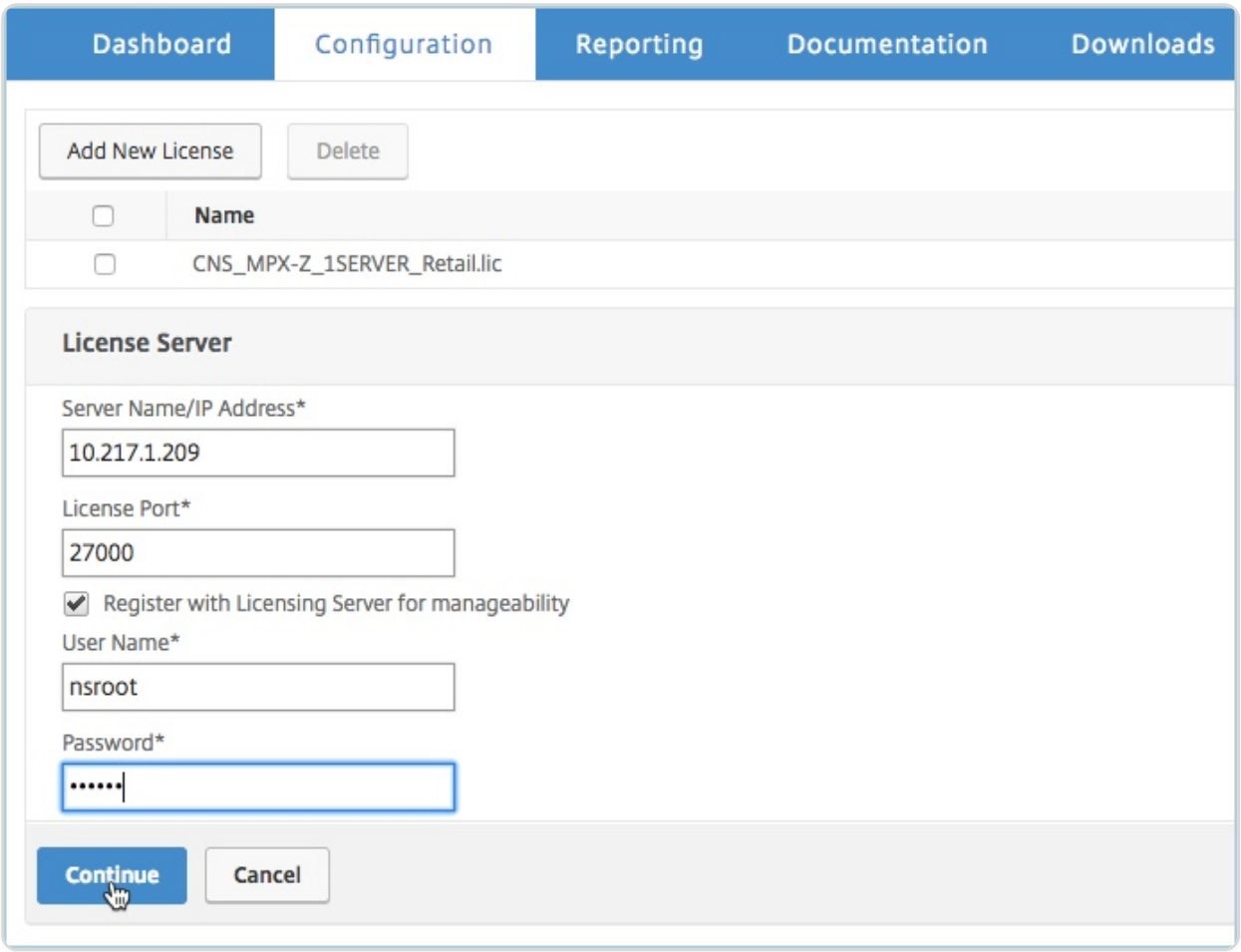
   If the **Secure Access Only** option is enabled on the appliance before the upgrade, you can't connect to the appliance through NetScaler ADM GUI, by using HTTPS.
8. On the **Confirm** page, click **Yes**.
9. After the appliance reboots, logon to the appliance.
10. On the Welcome page, click the **Licenses** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. In the **License Server** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Server Name/IP Address** field, enter the license server details.

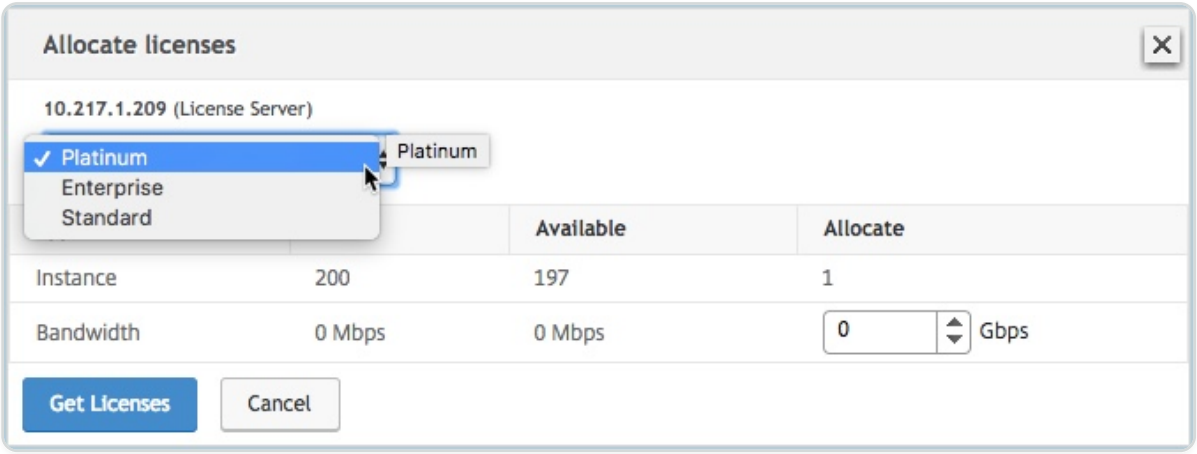
b. In the **License Port** field, enter the license server port. Default value: 27000.

c. If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

d. Click **Continue**.

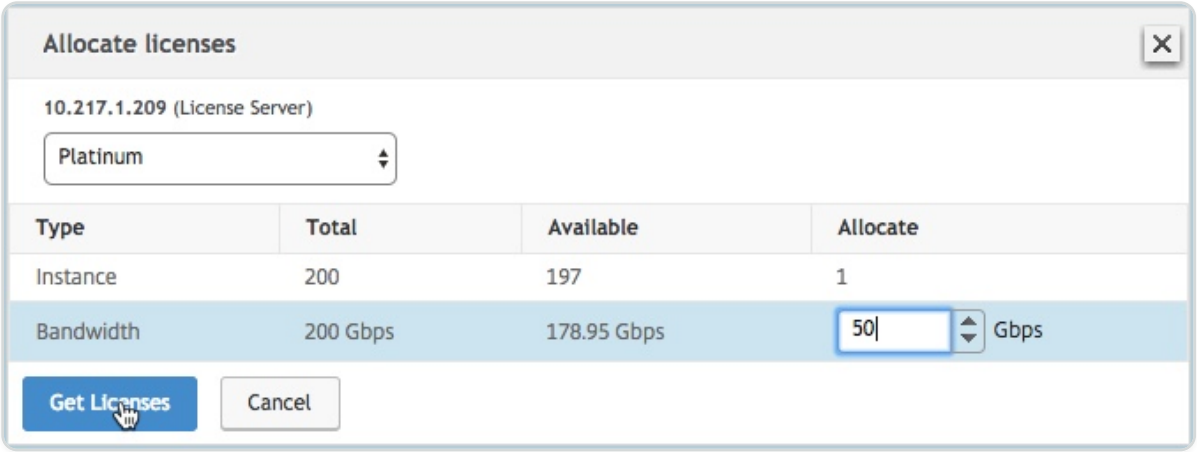
12. In **Allocate licenses**, do the following:

a. Select the license edition from the drop-down list.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



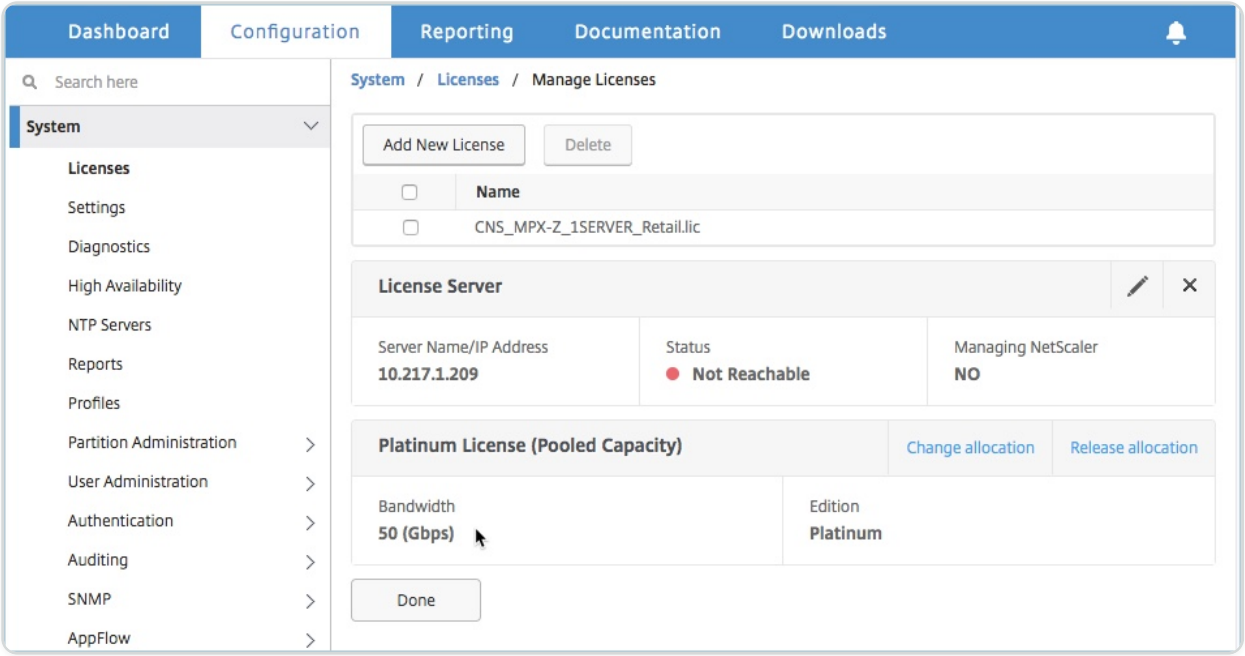
c. When prompted, click **Reboot** to reboot the appliance.

13. Once the NetScaler MPX appliance reboots, logon to the NetScaler MPX appliance. On the **Welcome** page, click **Continue**.

    The **Licenses** page lists all the licensed features.

14. Navigate to **System \> Licenses** and click **Manage Licenses**.

    On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated bandwidth.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler pooled capacity

For the MPX appliances configured in high availability mode, you have to configure pooled capacity on both the primary and secondary ADC instances in the HA pair. Allocate licenses of the same capacity to both the primary and secondary NetScaler instances in the HA pair. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need to allocate 2 Gbps capacity from the common pool. With 2 Gbps capacity, you can allocate 1 Gbps each to the primary and secondary NetScaler instances in the HA pair.

IMPORTANT

For upgrading NetScaler MPX appliance to use NetScaler Pooled Capacity license, you need to upload the MPX-Z to the appliance.

Prerequisites

Make sure that you upload the MPX-Z license to both the primary and secondary instances in the HA pair.

To upload the MPX-Z license to the NetScaler MPX instances in the HA pair:

1. In a Web browser, type the IP address of the appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the **Configuration** tab, navigate to **System \> Licenses**.
5. In the details pane, click **Manage Licenses**, click **Add New License**.
6. In **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.

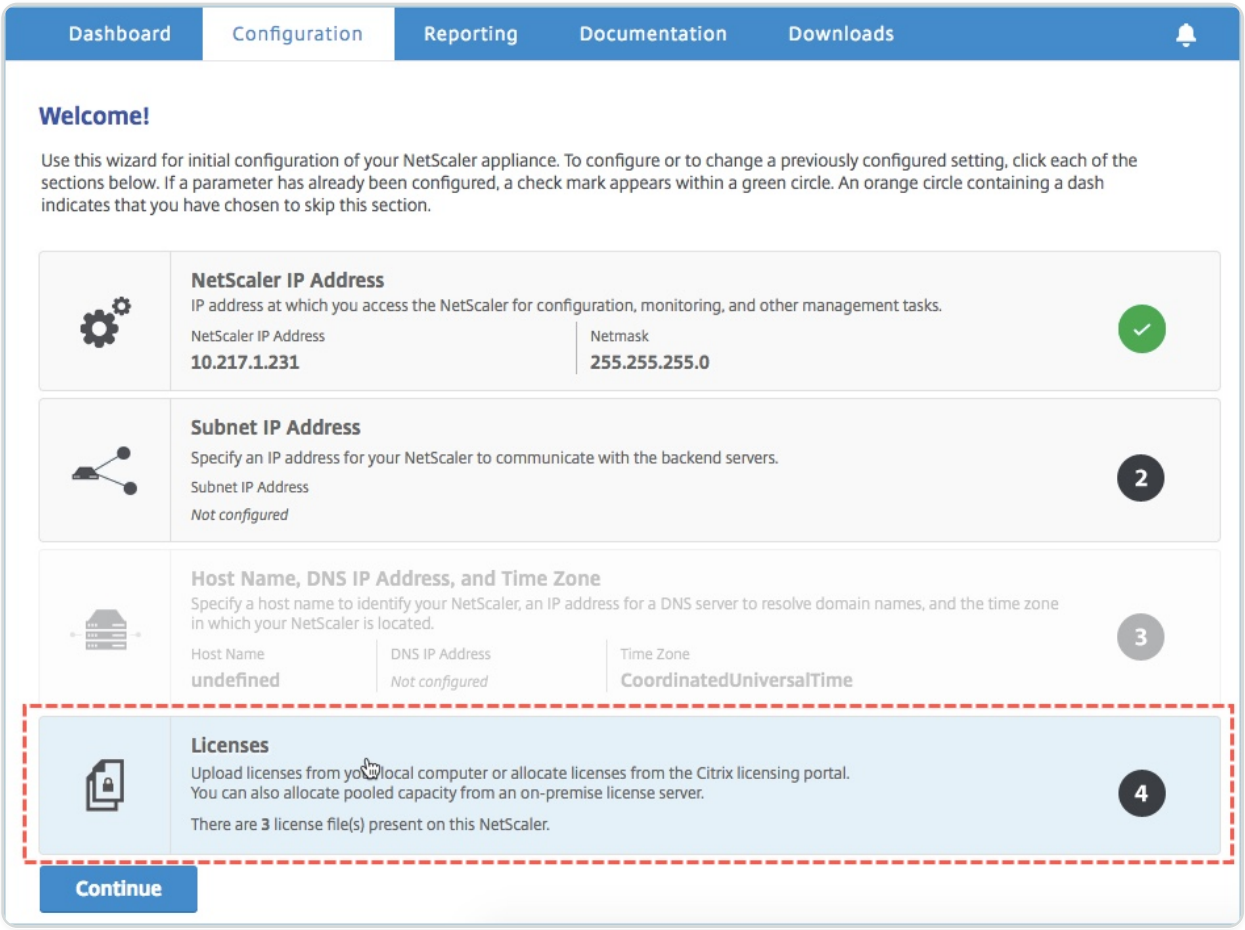
   Once the license is uploaded you are prompted to reboot the appliance.
7. Click **Reboot** to reboot the appliance.
8. On the **Confirm** page, click **Yes**.

To upgrade an exisiting HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary NetScaler MPX Instance. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.

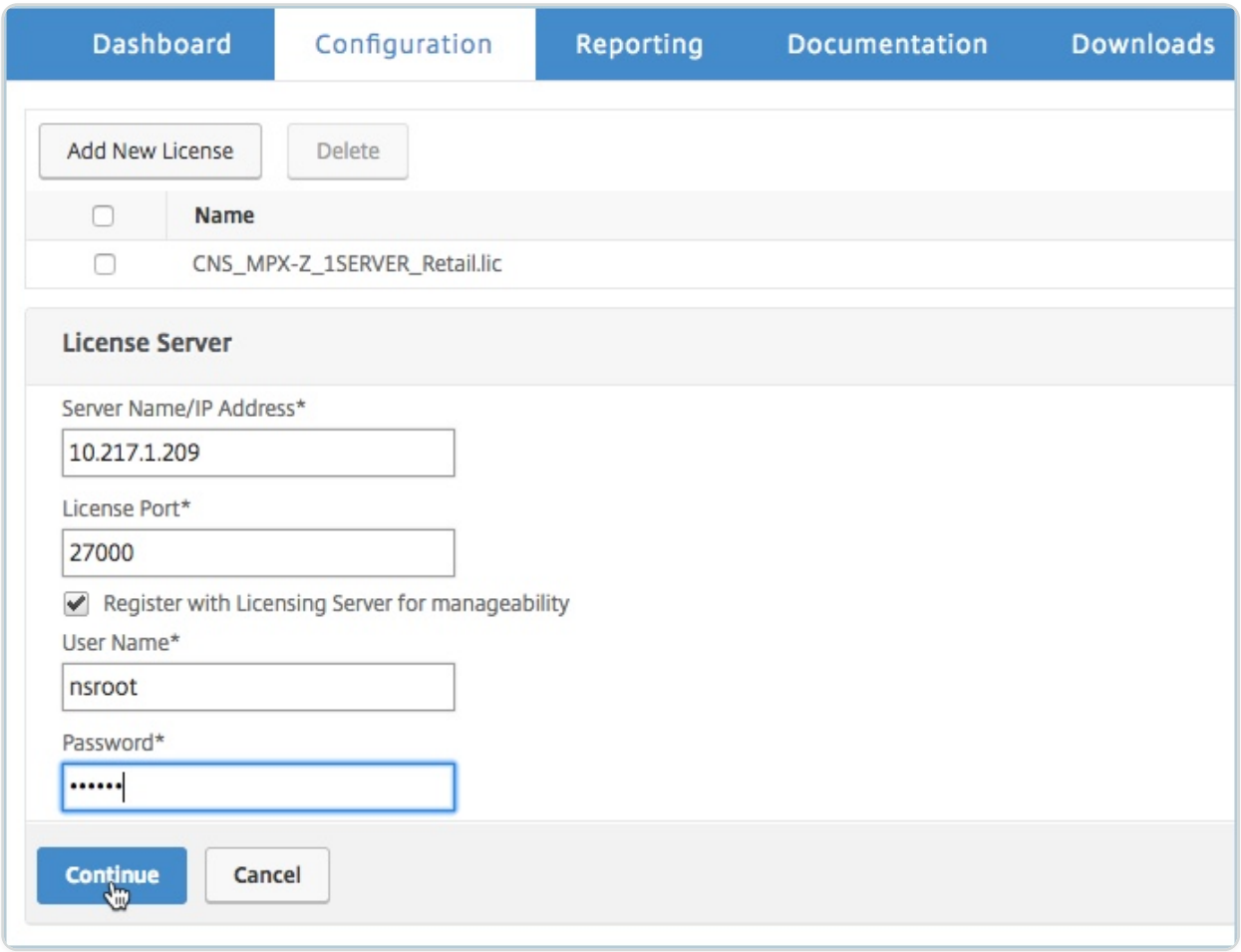
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click the **Licenses** section.



4. In the **License Server** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Server Name/IP Address** field, enter the license server details.

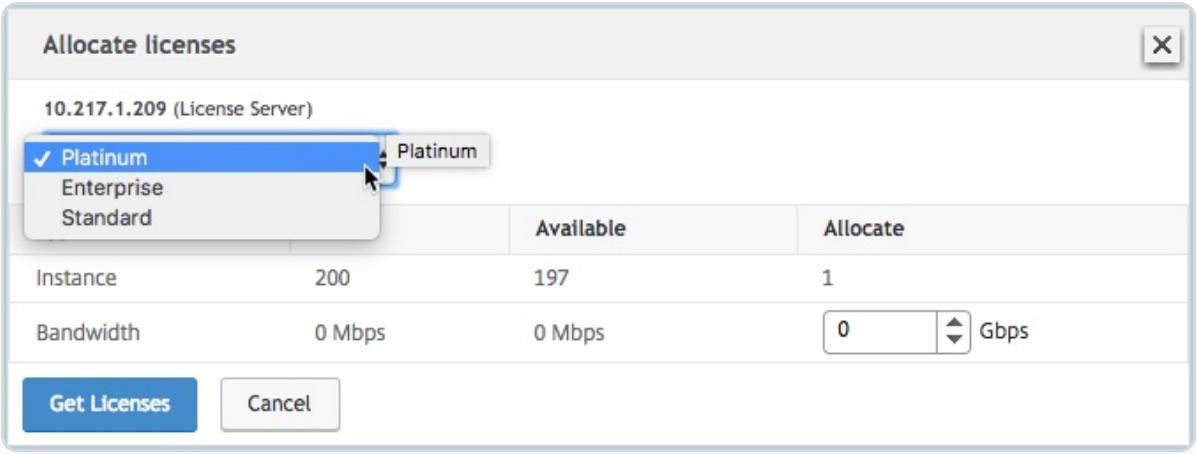
b. In the **License Port** field, enter the license server port. Default value: 27000.

c. If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with Licensing Server for manageability** check box and enter ADM credentials.

d. Click **Continue**.

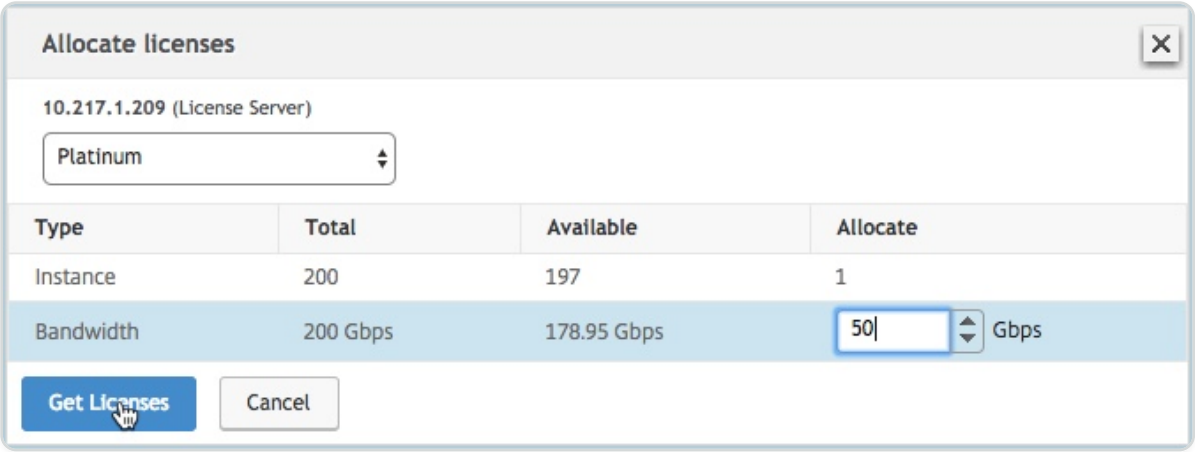
5. In **Allocate licenses**, do the following:

   a. Select the license edition from the drop-down list.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c. When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

6. Log on to the existing primary NetScaler MPX appliance and reboot the appliance. Perform the following:

   a. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.

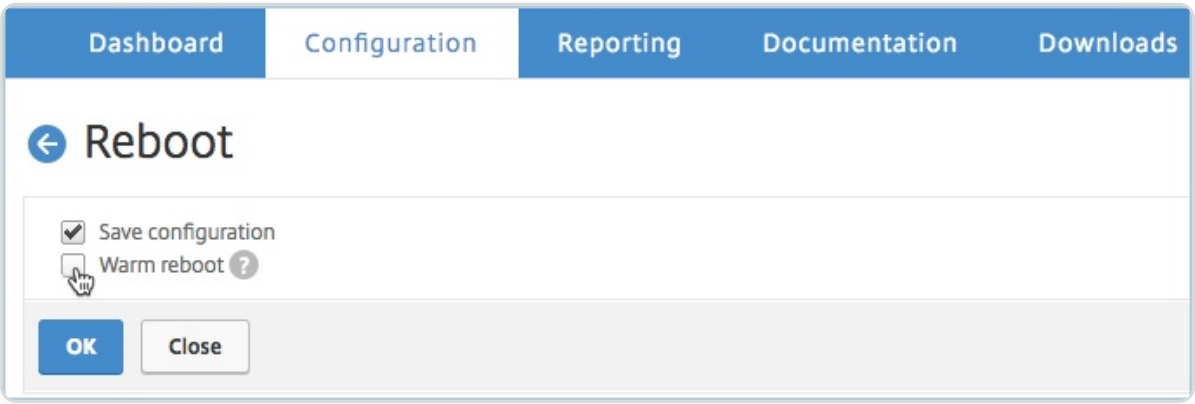
   b. In **User Name** and **Password** fields, type the administrator credentials.

   c. On the **Welcome** page, click **Continue**.

   d. On the **Configuration** tab, click **System**.

   e. On the **System** page, click **Reboot**.

   f. On the **Reboot** page, select **Warm reboot** and click **OK**.



After the primary NetScaler MPX appliance reboots, it becomes the secondary NetScaler MPX appliance in the HA pair. If you want to change the primary and secondary instance in the HA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pair to your original HA pair configuration, force a failover. Run the following command on any instance in the HA pair:

```
> force ha failover
```

Upgrade a perpetual license in a NetScaler SDX to NetScaler pooled capacity

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
A NetScaler SDX appliance with perpetual license can be upgraded to NetScaler Pooled Capacity license. Upgrading to NetScaler Pooled Capacity license enables you to allocate licenses from the license pool to NetScaler appliances on demand. You can also configure the ADC Pooled Capacity license for NetScaler instances configured in high availability mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

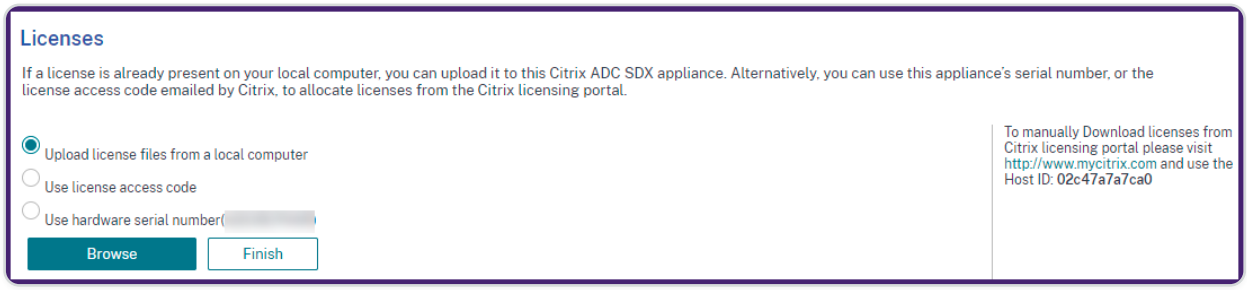
IMPORTANT

Conversion from a perpetual license to a pooled capacity license is a one-way license entitlement process. You cannot revert the pooled capacity license back to perpetual.

- For upgrading the SDX appliance to NetScaler Pooled Capacity license, you must upload the SDX-Z license to the appliance.
- Ensure you have the permission to add ADC instances in ADM.
- To ensure that there is no impact on the current licenses, customer has to allocate the same number of instances and bandwidth that is available as part of the perpetual license.

To upgrade to NetScaler Pooled Capacity:

1. In a Web browser, type the IP address of the SDX appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero-capacity license. On the Configuration tab, navigate to **System** \> **Licenses**.
5. On the **Manage Licenses** page, click **Add License File**.
6. In **Licenses** page, select **Upload license files from a local computer** and click **Browse** to select the zero-capacity license from your local machine. Then, click **Finish**.



Once the zero-capacity license is applied successfully, **Pooled Licenses** section appears on the **Licenses** page.

NOTE

To remove the old license file, you don't have to reboot your SDX appliance so there is no downtime. For more help, contact NetScaler support Team.

7. In the **Pooled licenses** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. In the **Licensing Server Name or IP Address** field, enter the license server details.

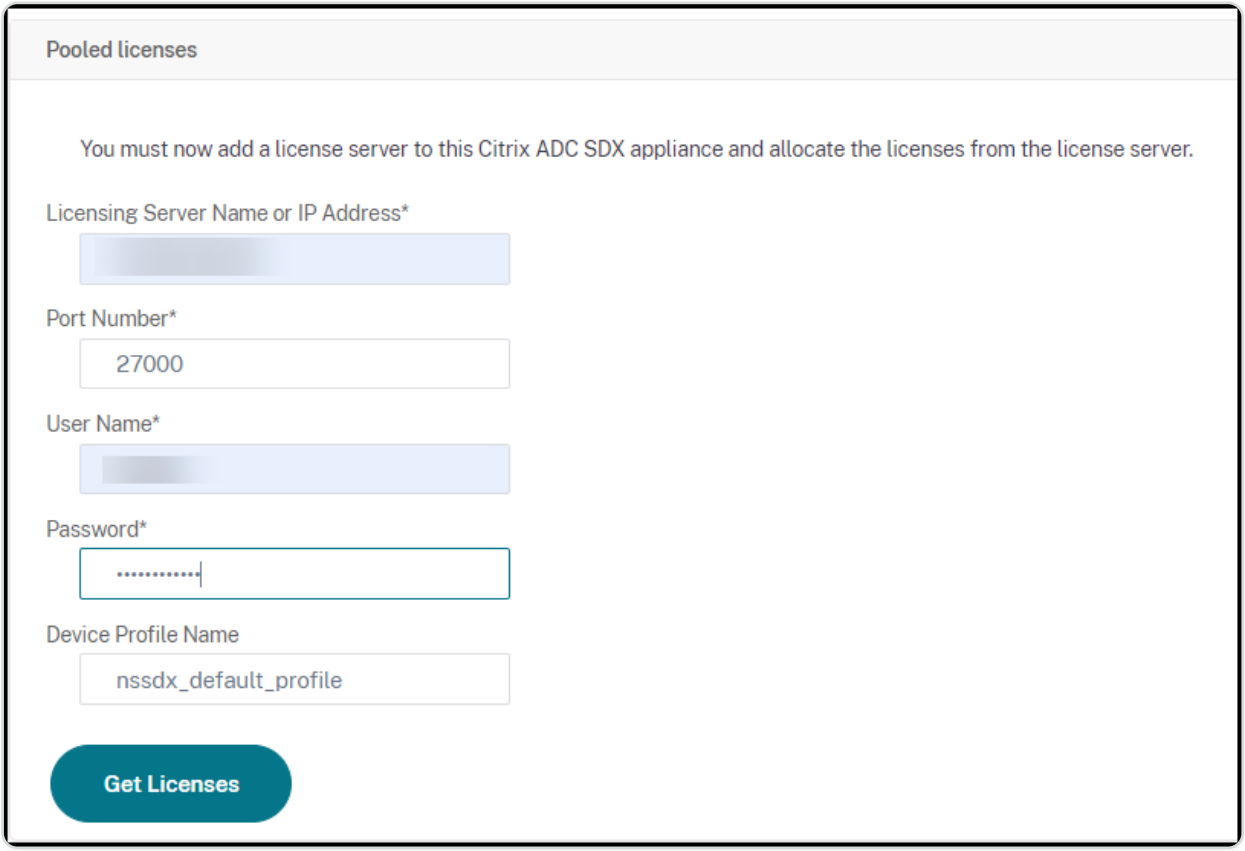
- If you want to configure ADM server as a license server, specify ADM server's IP address.
- If you are using an agent to communicate with the ADM server, specify ADM agent's IP address.

b. In the **Port Number** field, enter the license server port. Default value: 27000.

c. Specify **User Name** and **Password** of the licensing server.

- For the ADM server, enter the administrator credentials.
- For the ADM agent, enter the agent credentials.

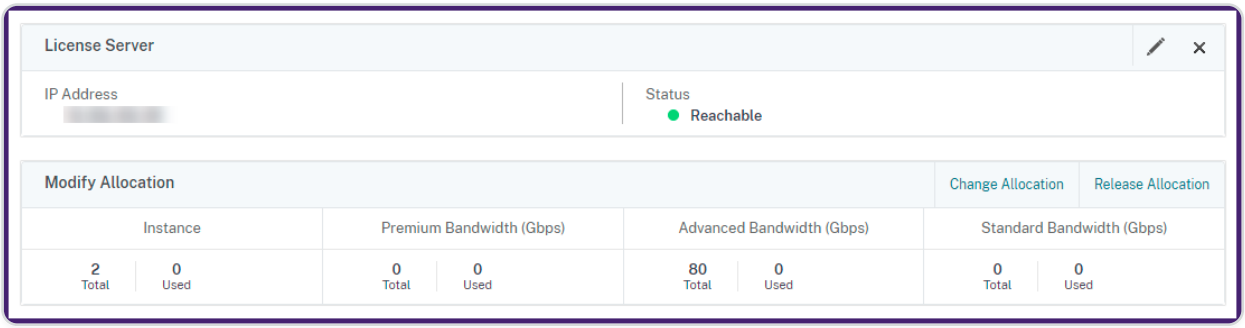
d. Click **Get Licenses**.



8. In the **Allocate Licenses** window, specify the required instances and bandwidth and click **Allocate**.

   On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated instances and bandwidth from the pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

Upgrading a perpetual license to pooled capacity does not require restarting the SDX appliance.

NetScaler pooled capacity on NetScaler instances in cluster mode

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions. LAS based licenses may not be available to customers where prohibited by law or regulations. If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

You can configure NetScaler pooled capacity on the NetScaler instances configured as a cluster. The following are the prerequisites for configuring pooled capacity on NetScaler instances in cluster mode:

- Instances are individually running in a pooled-capacity license mode to form the cluster.
- All the instances must be running with same bandwidth.
- All the instances checked out the pooled capacity from the same NetScaler Application Delivery Management (ADM).
- New instances cannot be added to an existing NetScaler cluster unless their capacity and NetScaler ADM configurations are same as those of the existing instances in the cluster.

Any capacity check-out from the NetScaler cluster assigns same capacity to all the cluster nodes and the checkout Bandwidth = Bandwidth provided * number of nodes.

For example, if you check-out 50 Mbps of bandwidth from the NetScaler cluster, and the cluster includes 12 instances, each instance automatically receives 50 Mbps. And, 600 Mbps is checked out from the pool.

NOTE

If one or more instances in the cluster become unresponsive, the cluster continues to process the traffic with the remaining instances' capacity.

Allocate ADC Pooled capacity to an ADC cluster

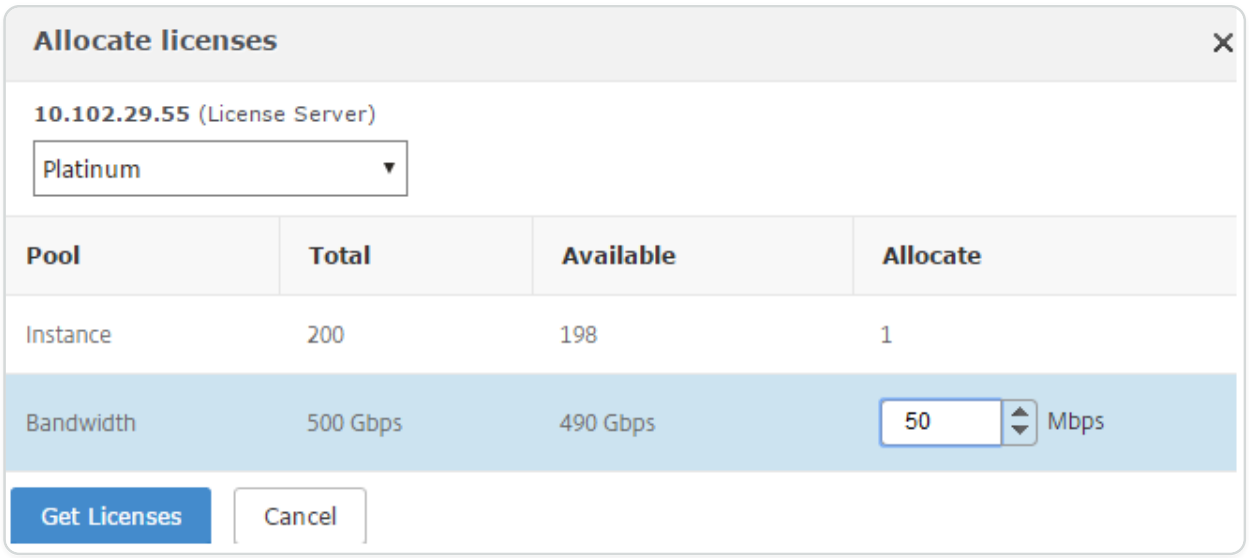
Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

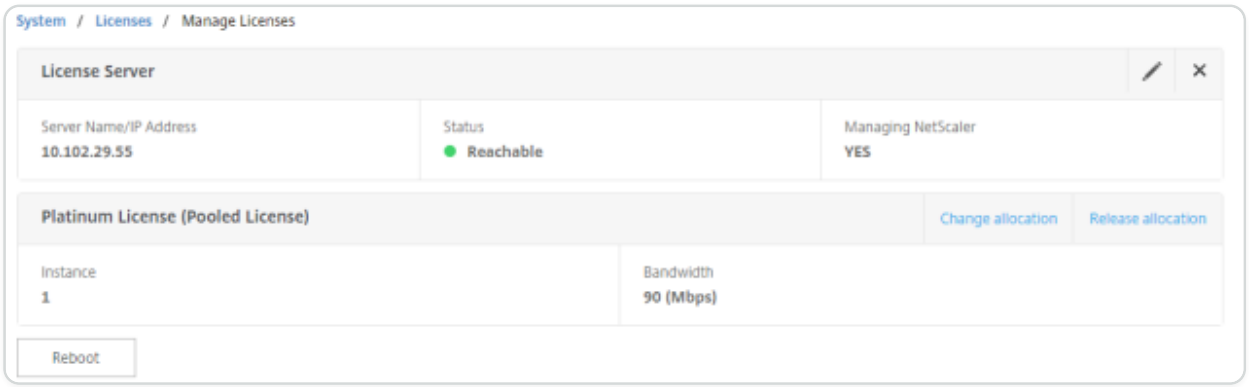
1. In a web browser, type the NetScaler IP address (NSIP). For example, `http://192.168.100.1`.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **Configuration** tab, navigate to **System \> Licenses \> Manage Licenses**, click **Add New License,** and select **Use Pooled Licensing**.
4. Enter the name or address of the license server in the **Server Name/IP Address** field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. If you want to manage your instance's pool licenses through NetScaler ADM, select the **Register with NetScaler ADM for manageability** check box and enter the ADM credentials.
6. Select the license edition and the required bandwidth, and click **Get Licenses**.



7. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.

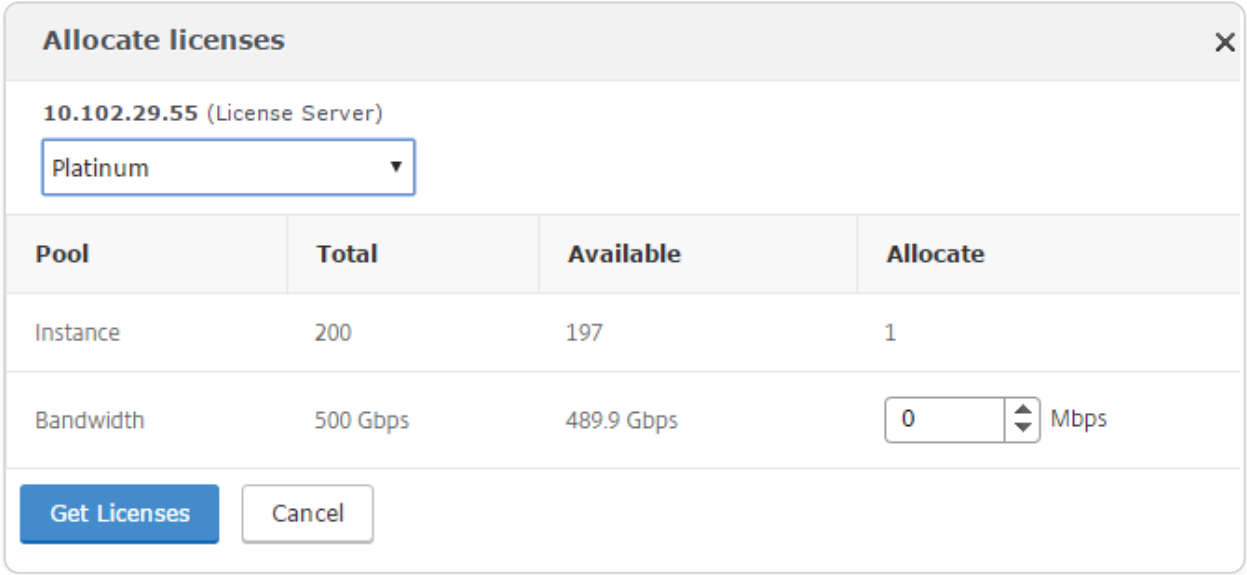


8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

NOTE

Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.
10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

> **NOTE**
>
> A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.

Allocate ADC Pooled capacity to an ADC cluster using CLI

Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

1. In an SSH client, enter the NetScaler IP address (NSIP), and log in by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                    : 0
        Instance Available                : 0
        Standard Bandwidth Total          : 0 Mbps
        Standard Bandwidth Availabe       : 0 Mbps
        Enterprise Bandwidth Total        : 0 Mbps
        Enterprise Bandwidth Available    : 0 Mbps
        Platinum Bandwidth Total          : 0 Mbps
        Platinum Bandwidth Available      : 0 Mbps
        VPX25S Total                      : 1
        VPX25S Available                  : 1
        VPX200E Total                     : 1
        VPX200E Available                 : 1
        VPX1000S Total                    : 1
        VPX1000S Available                : 1
        VPX8000E Total                    : 2
        VPX8000E Available                : 1
 Done
```

4. To assign a license to the NetScaler VPX appliance, enter the following command:

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Health monitoring

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
The license server continuously monitors the health of the NetScaler pooled-capacity enabled instance. The instances communicate through periodical messages to the license server. If few consecutive messages are not received, the license server reports that connectivity has been lost.

You can create custom notifications to supplement the default alarms.

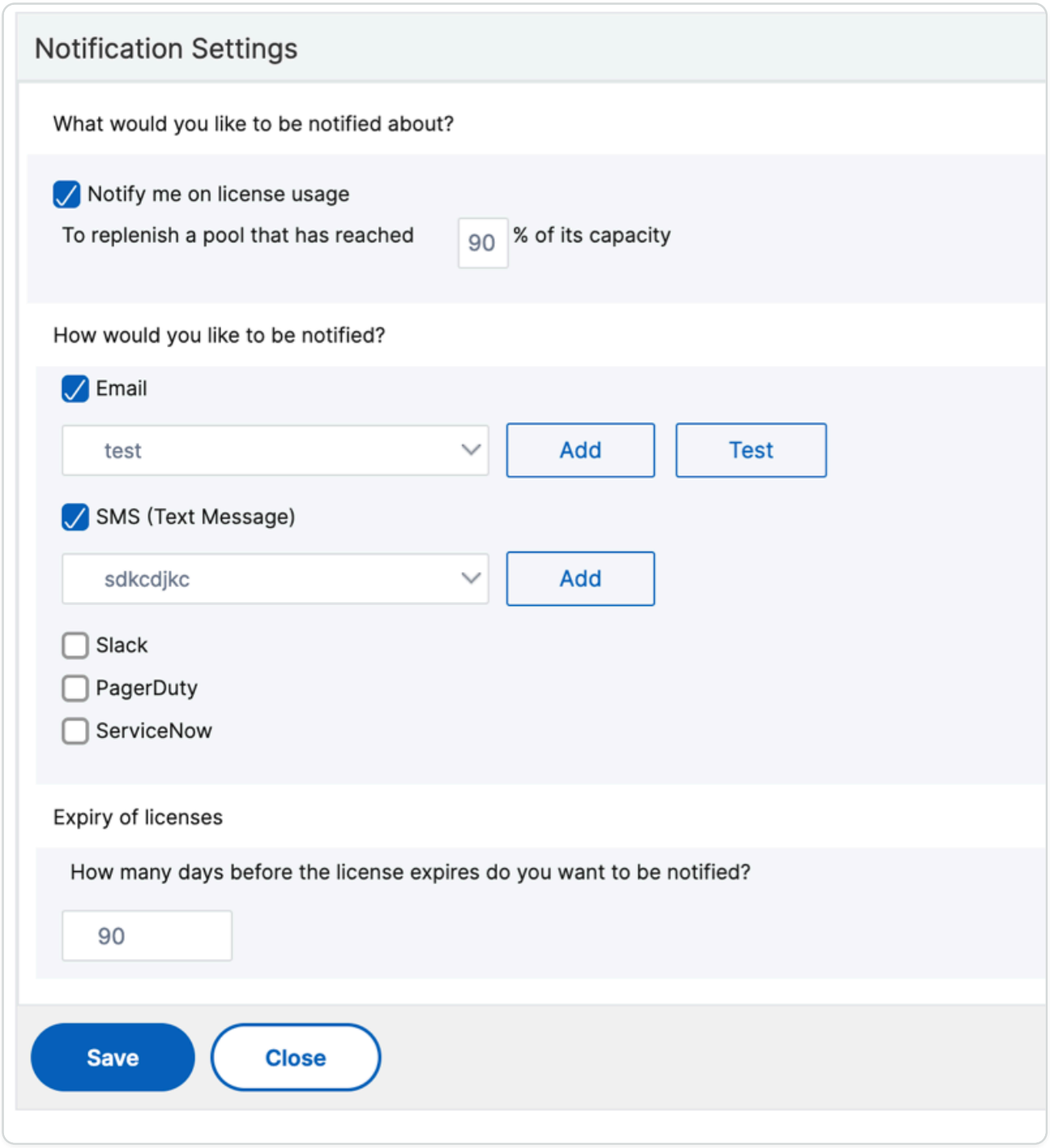
Grace Period

When a NetScaler pooled-capacity enabled instance is in a healthy state and the license server stops responding, the instance continues to operate with the current capacity for 30 days. If the connectivity to the license server is not restored after 30 days, the instance loses its capacity and stops processing traffic.

Notifications and Alarms

Notifications can be enabled from NetScaler Application Delivery Management (ADM) for any action performed on the instance. Apart from the custom notification settings, some alarms are configured by default. For example: To configure an alarm for replenishing a pool that has depleted a certain percentage of its capacity, navigate to **Infrastructure > Pooled Licensing** and under **Notification Settings**, click the edit icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expected behaviors when issues arise

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
Following are the expected behaviors of the license servers and NetScaler instances when they experience the issues described:

License Server stops responding

WARNING

The license Server is not responding. NetScaler continues to operate with the current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the NetScaler loses its current capacity and stops processing traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the license server stops responding, the NetScaler instance enters the Grace Period until connectivity is restored.

NetScaler pooled-capacity enabled instance stops responding

If the NetScaler pooled-capacity enabled instance stops responding and the license server is in a healthy state, the license server checks in all the NetScaler instance's licenses after 10 minutes. When the instance reboots, it sends a request to check out all the licenses from the licensing server.

Both license server and NetScaler pooled-capacity enabled instance stop responding

If both the license server and the NetScaler pooled-capacity enabled instance restarts and reestablishes the connection, the license server checks-in all its licenses after 10 minutes, and the NetScaler pooled capacity enabled instances automatically check out the licenses after the reboot is completed.

The NetScaler pooled-capacity enabled instance shuts down gracefully

During a graceful shutdown, you can choose to check the licenses in or keep the licenses that were allocated before the graceful shutdown. If you choose to check the licenses in, the NetScaler pooled-capacity enabled instance is unlicensed after it restarts. If you choose to keep the licenses, they are checked in to the licensing server when the instance shuts down. After the instance restarts, it reestablishes the connection with the licensing server and checks out the licenses as specified in the saved configuration.

If the system reboots and the checkout fails due to no capacity available in the pool, the NetScaler checks the inventory of NetScaler Application Delivery Management (ADM) pool licenses and checks out any available capacity. An SNMP alarm is raised to notify this condition to the user if the NetScaler is not running with full capacity as per configuration. If no capacity is available in the bandwidth pool, the pool capacity enabled instance becomes unlicensed.

Network loses connectivity

ERROR MESSAGE (SYSLOG)
License Server is not responding.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the license server and NetScaler pooled-capacity enabled instances are in healthy states but network connectivity is lost, the instances continue to operate with their current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the instances lose their capacity and stop processing traffic, and the license server checks-in all its licenses. After the license server reestablishes connectivity with the NetScaler instances, the instances check the licenses out again.

Configure expiry checks for pooled capacity licenses

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
You can now configure license expiry threshold for NetScaler pooled capacity licenses. By setting thresholds, NetScaler Application Delivery Management (ADM) sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification is also sent when the license has expired on NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler ADM.

To configure license expiry checks:

1. Navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
   - **Feature**: Type of license that is going to expire.
   - **Count**: Number of virtual servers or instances that will be affected.
   - **Days to expiry**: Number of days before license expiry.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.
4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
   a. **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
   b. **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.
5. Then, specify when you want to send the notification in terms of number of days before license expiry.
6. Click **Save**.

NOTE

When you add new licenses to the pool, the NetScaler instances use the new licenses on expiry of their existing licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Check in and check out NetScaler VPX and BLX licenses

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
You can allocate VPX and BLX licenses to NetScaler instances on demand from NetScaler Application Delivery Management (ADM). The ADM software stores and manages the licenses, which have a licensing framework that provides scalable and automated license provisioning. An instance can check out the license from the NetScaler ADM when it is provisioned. When an instance is removed or destroyed, the instance checks back in its license to the NetScaler ADM software.

Prerequisites

Make sure that the following prerequisites are met:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You are using a NetScaler VPX image running software version 12.0.For example: NSVPX-ESX-12.0-xx.xx_nc.zip
- You have installed NetScaler ADM running version 12.0.For example: MAS-ESX-12.0-xx.xx.zip

NOTE

To manage existing VPX licenses by NetScaler ADM, you need to rehost the licenses to NetScaler ADM.

Installing Licenses in NetScaler ADM

NOTE

Before installing licenses, restart the NetScaler ADM virtual appliance if you have changed the software edition or bandwidth.

To install license files on NetScaler ADM:

1. In a web browser, type the IP address of the NetScaler ADM (for example, `<http://192.168.100.1>`).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to **Infrastructure > Pooled Licensing**.
4. In the **License Files** section, select one of the following options:
   - **Upload license files from a local computer** - If a license file is already present on your local computer, you can upload it to the NetScaler ADM.To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   - **Use license access code** - Citrix emails the license access code for the licenses that you purchase.To add license files, enter the license access code in the text box and then click **Get Licenses**.

   NOTE

   Make sure you are connected to internet before using license access code for installing the licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

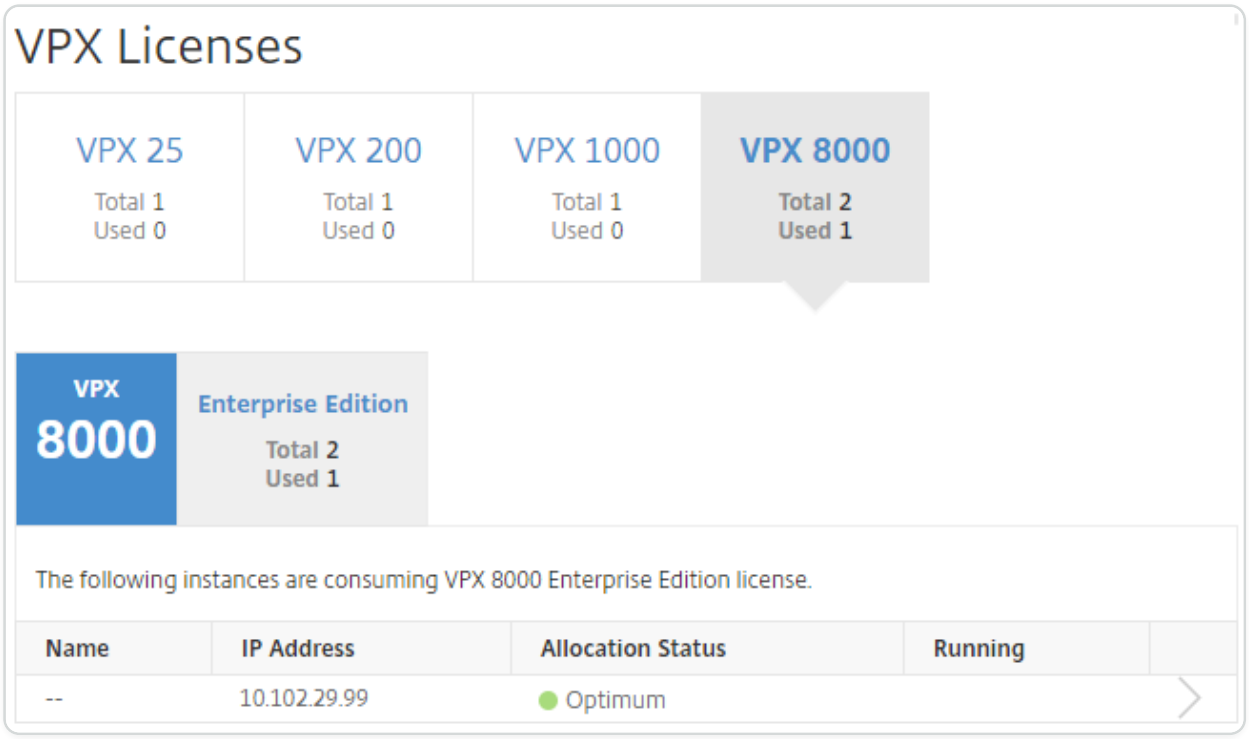
At any time, you can add more licenses to the NetScaler ADM from the **License Settings** page.

Verification

You can view the available and allocated licenses in the NetScaler ADM GUI.

To display the licenses:

1. In a web browser, type the IP address of NetScaler ADM (for example, `<http://192.168.100.1>`).
2. In **User Name** and **Password**, enter the administrator credentials.
3. On the Configuration tab, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**.



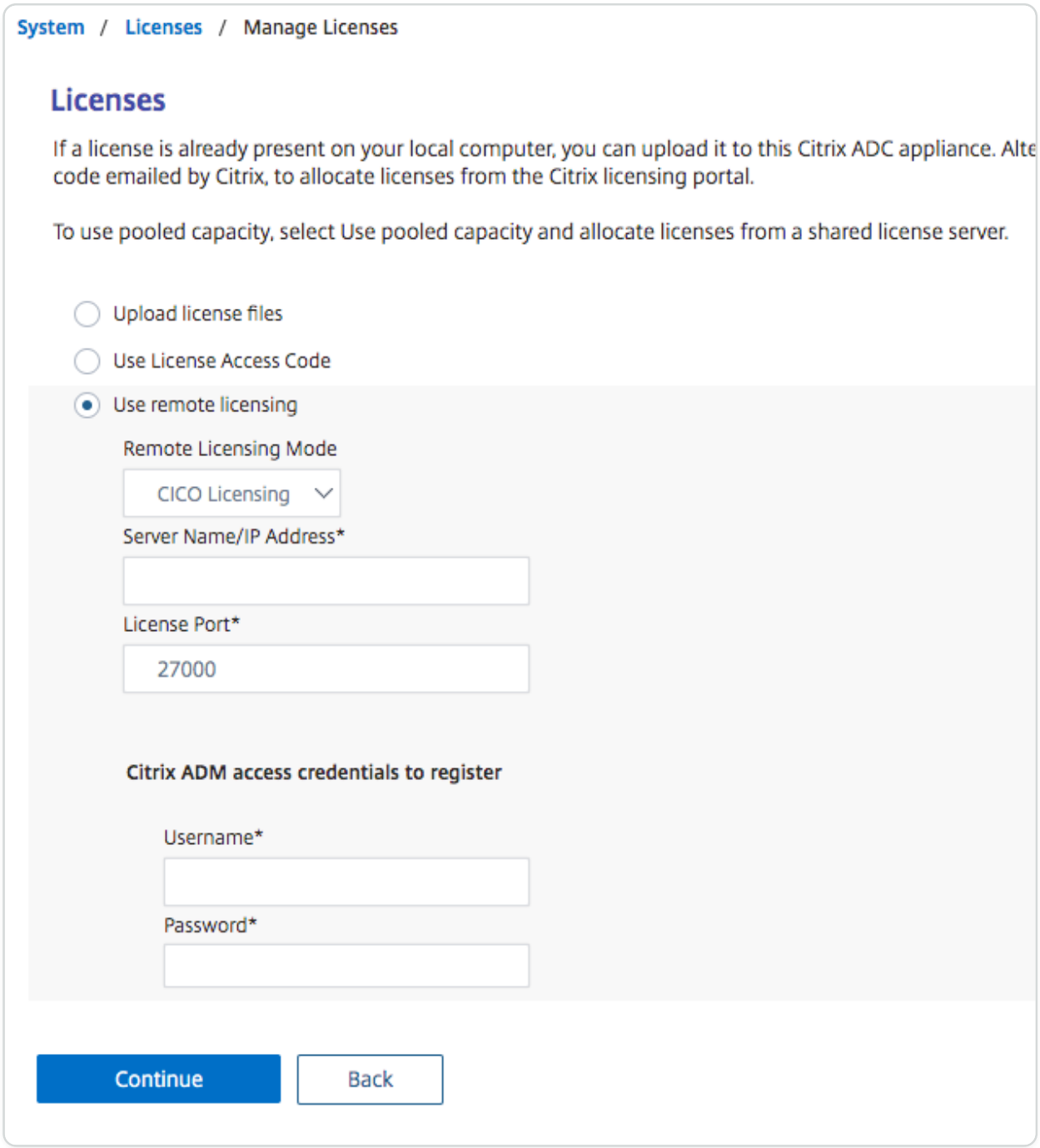
4. You can view the allocated licenses in the table under the available licenses section.

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler GUI

1. In a web browser, type the IP address of the NetScaler instance (for example, `<http://192.168.100.1>`).
2. In the **User Name** and **Password** fields, enter the administrator credentials.

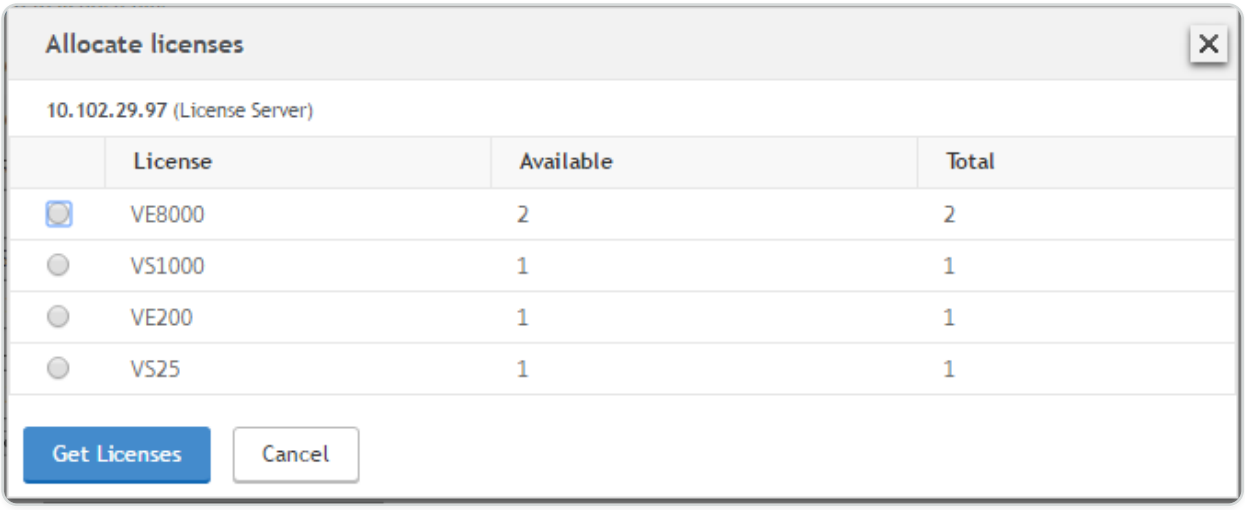
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the Configuration tab, navigate to **Settings > Licenses > Manage Licenses**, click **Add New License**, and select **Use Remote Licensing > CICO Licensing**.
4. Enter the details of the license server in the **Server Name/IP Address field**.
5. In the **Username** and **Password** fields on the above screen, enter NetScaler ADM credentials and click **Continue**.

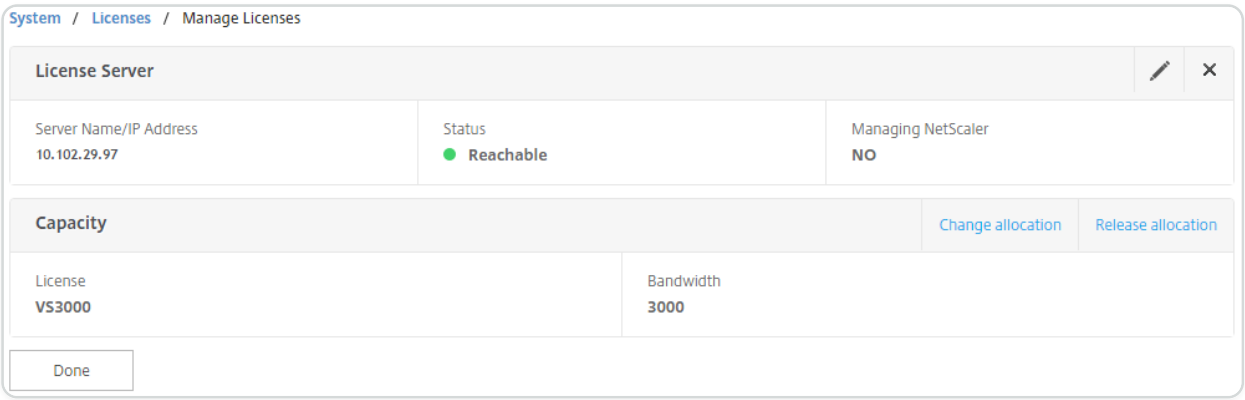


6. Select the license edition with the required bandwidth, click **Get Licenses**.

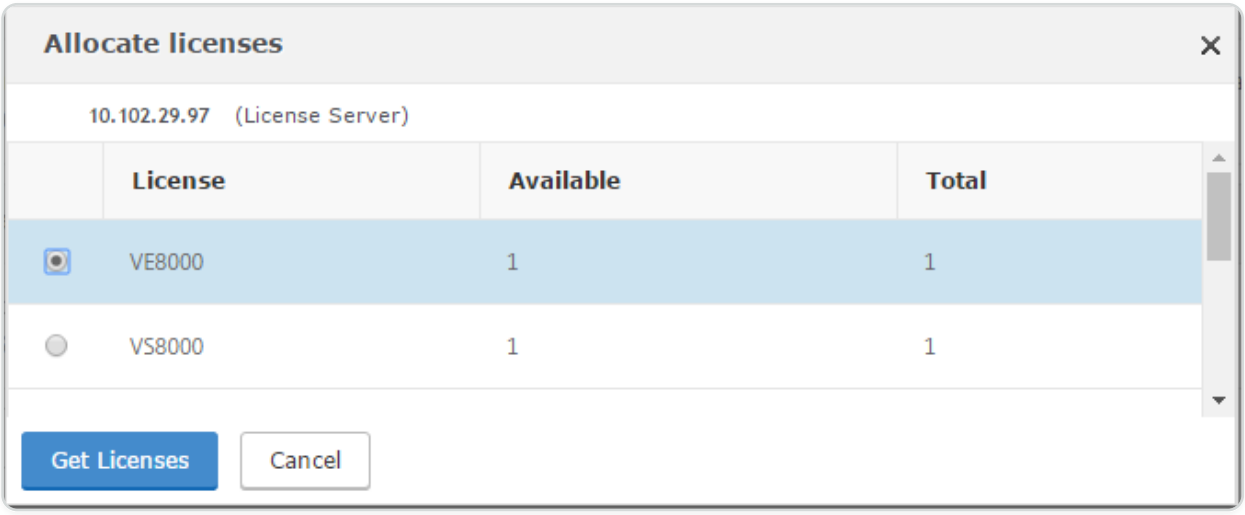
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Click **Reboot**, your NetScaler instance reboots.
8. You can change or release the license allocation by navigating to **System** \> **Licenses** \> **Manage Licenses**, and selecting **Change allocation** or **Release allocation.**



9. If you click **Change allocation**, a pop-up window shows the licenses available on the license server. Select the required license, click **Get Licenses**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler CLI

1. In an SSH client, enter the IP address of the NetScaler instance, and log on by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
```

```
> 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
```

```
> sh licenseserverpool
        Instance Total                    : 0
        Instance Available                : 0
        Standard Bandwidth Total          : 0 Mbps
        Standard Bandwidth Availabe       : 0 Mbps
        Enterprise Bandwidth Total        : 0 Mbps
        Enterprise Bandwidth Available    : 0 Mbps
        Platinum Bandwidth Total          : 0 Mbps
        Platinum Bandwidth Available      : 0 Mbps
        VPX25S Total                      : 1
        VPX25S Available                  : 1
        VPX200E Total                     : 1
        VPX200E Available                 : 1
        VPX1000S Total                    : 1
        VPX1000S Available                : 1
        VPX8000E Total                    : 2
        VPX8000E Available                : 1
 Done
```

4. To assign a license to the NetScaler appliance, enter the following command:

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Allocate VPX and BLX Licenses to an ADC instance by using API

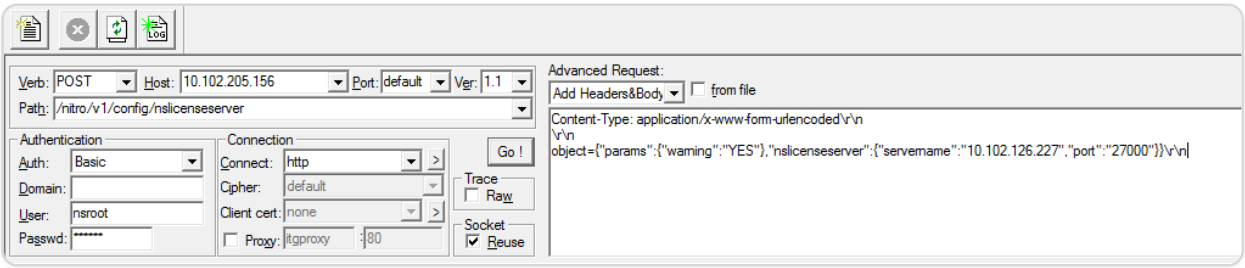
In a web browser or an API client, log on to the NetScaler instance by using the administrator credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

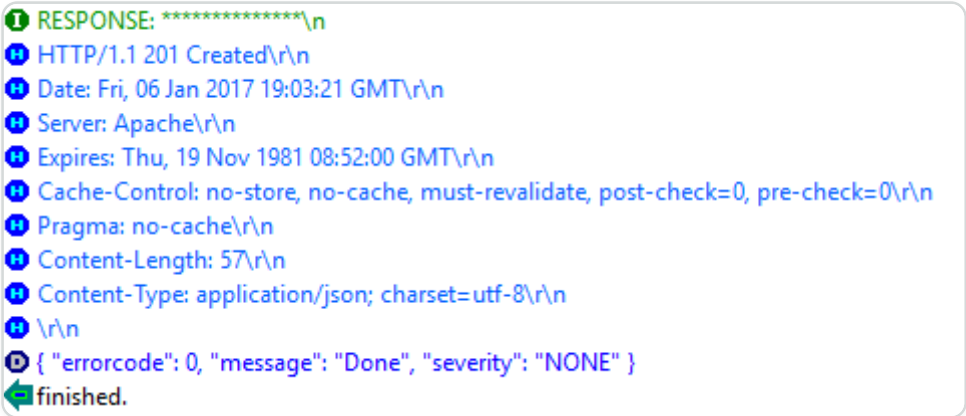
To add a licensing server:

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nslicensingserver.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

object= {“params”;{warning”:”yes”},”nslicensing server”;
{servername”:”\<NetScaler ADM IP\>”, “port”:”27000”}}\\r\\n
```



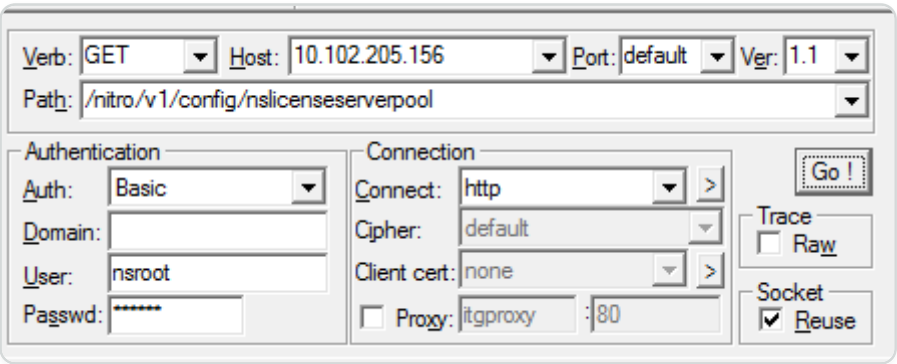
NetScaler ADM responds to the request. The following sample response shows success.



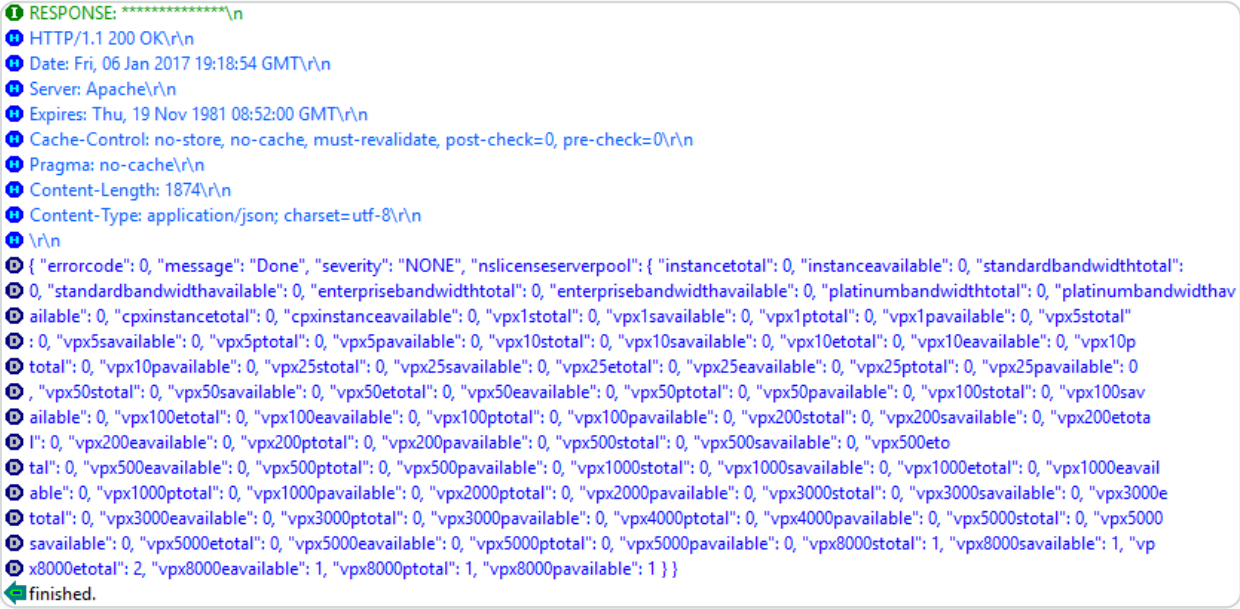
To view the available licenses on the licensing server:

1. Set the request type to **Get**.
2. Set the path to /nitro/v1/config/nslicenseserverpool

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler ADM responds to the request. The following sample response shows success, and the list of available licenses on the license server.

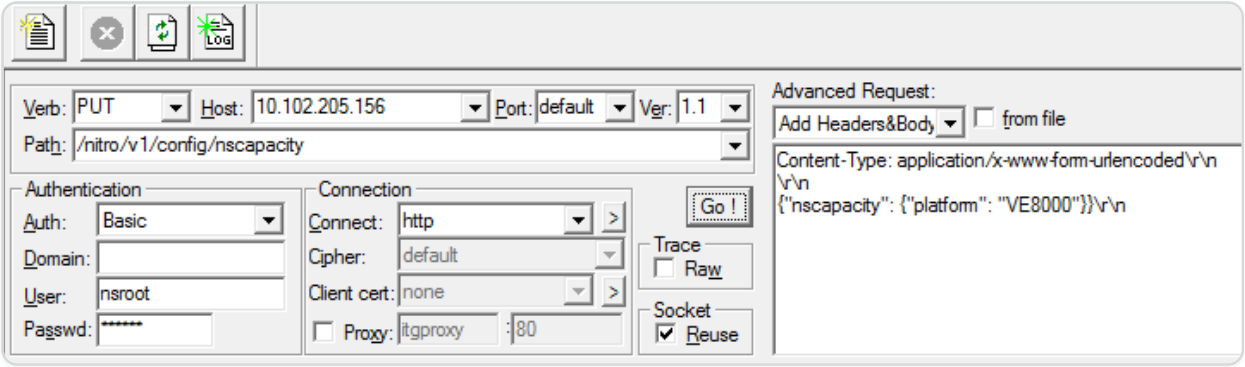


To assign a license to the NetScaler appliance:

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nscapacity.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

{“nscapacity:{“platform”:”VE8000”}}\\r\\n
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler ADM responds to the request. The following sample response shows success.

Update a licensing server IP address

You can update the licensing server IP address in the VPX and BLX instances, without any impact on the allocated license bandwidth on the instance and data loss.

Update using the CLI: To update the licensing server IP address using the CLI, type the following command on the instance:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and release the resources associated with the previous licensing server.

Update using the GUI: To update the licensing server IP address using the GUI, navigate to **System > Licenses > Manage Licenses**, click **Add New License** For more information, see Allocate VPX and BLX Licenses to an ADC instance by using the NetScaler GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Expiry Checks for NetScaler VPX and BLX Check-In and Check-Out Licenses

You can now configure license expiry threshold for NetScaler VPX and BLX licenses. By setting thresholds, NetScaler ADM sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification are also sent when the license has expired on NetScaler ADM.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler ADM.

To configure license expiry checks:

1. Navigate to **Infrastructure > Pooled Licensing**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
   - **Feature**: Type of license that is going to expire.
   - **Count**: Number of virtual servers or instances that are affected.
   - **Days to expiry**: Number of days before license expiry.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of pooled licenses capacity to be used to notify administrators.
4. Choose the type of notification you want to send by selecting the appropriate check box. The notification types are as follows:
   a. **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
   b. **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.
5. Then, specify when you want to send the notification in terms of number of days before license expiry.
6. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler virtual CPU licensing

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: will support LAS from early September.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
Read the following note before procededing further.

NOTE:

vCPU license is no longer available for purchase. For more information, see Licensing.

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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Network functions virtualization (NFV)
- Network virtualization (NV)
- Micro-services

Such a movement also needs the software requirements to be dynamic, flexible, and agile to meet the ever-changing business needs. Licenses are also expected to be managed by a central management tool with full visibility into the usage.

Virtual CPU licensing for NetScaler VPX

Earlier, NetScaler VPX licenses were allocated based on the bandwidth consumption by the instances. A NetScaler VPX is restricted to use a specific bandwidth and other performance metrics based on the license edition that it is bound to. To increase the available bandwidth, you must upgrade to a license edition that provides more bandwidth. In certain scenarios, the bandwidth requirement might be less, but the requirement is more for other L7 performance such as SSL TPS, compression throughput, and so on. Upgrading the NetScaler VPX license might not be suitable in such cases. But you might still have to buy a license with large bandwidth to unlock the system resources required for CPU-intense processing. NetScaler ADM now supports allocating licenses to NetScaler instance based on the virtual CPU requirements.

In the virtual CPU-usage-based licensing feature, the license specifies the number of CPUs that a particular NetScaler VPX is entitled to. So, the NetScaler VPX can check out licenses for only the number of virtual CPUs running on it from the license server. NetScaler VPX checks out licenses depending on the number of CPUs running in the system. NetScaler VPX does not consider the idle CPUs while checking out the licenses.

Similar to pooled license capacity and CICO licensing functionalities, the NetScaler ADM license server manages a separate set of virtual CPU licenses. Here also, the three editions managed for virtual CPU licenses are Standard, Advanced, and Premium. These editions unlock the same set of features as those unlocked by the editions for bandwidth licenses.

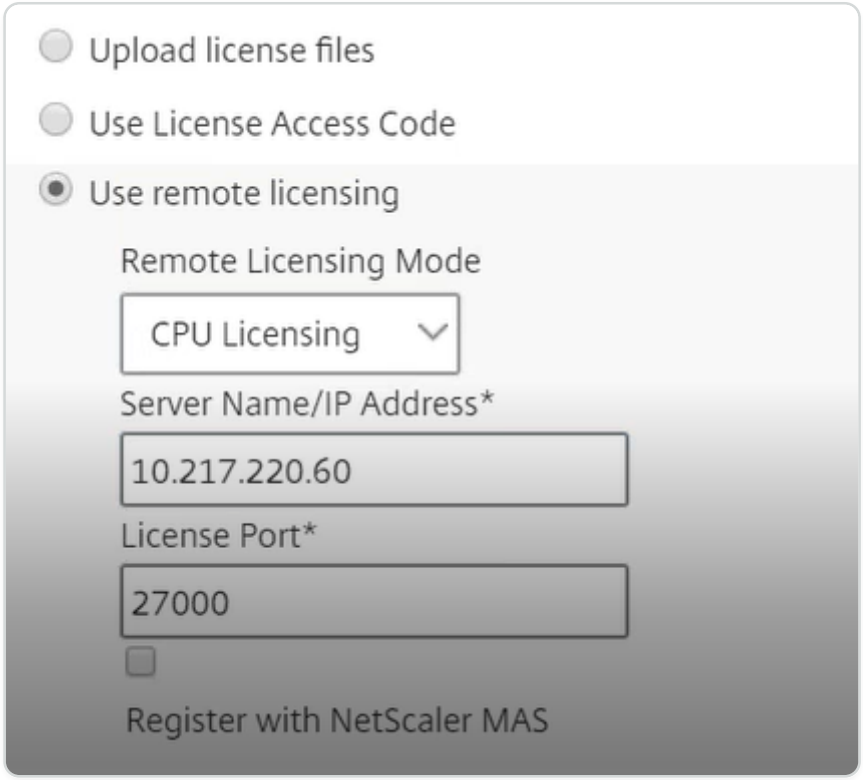
There might be a change in the number of virtual CPUs or when there is a change in the license edition. In such a case, you must always shut down the instance before you initiate a request for a new set of licenses. Restart the NetScaler VPX after checking out the licenses.

To configure licensing server in NetScaler VPX using GUI:

1. In NetScaler VPX, navigate to **System** \> **Licenses** and click **Manage Licenses**.
2. On the **License** page, click **Add New License**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Licenses** page, select the **Use remote licensing** option.
4. Select **CPU licensing** from the **Remote Licensing Mode** list.
5. Type the IP address of the license server and the port number.
6. Click **Continue**.

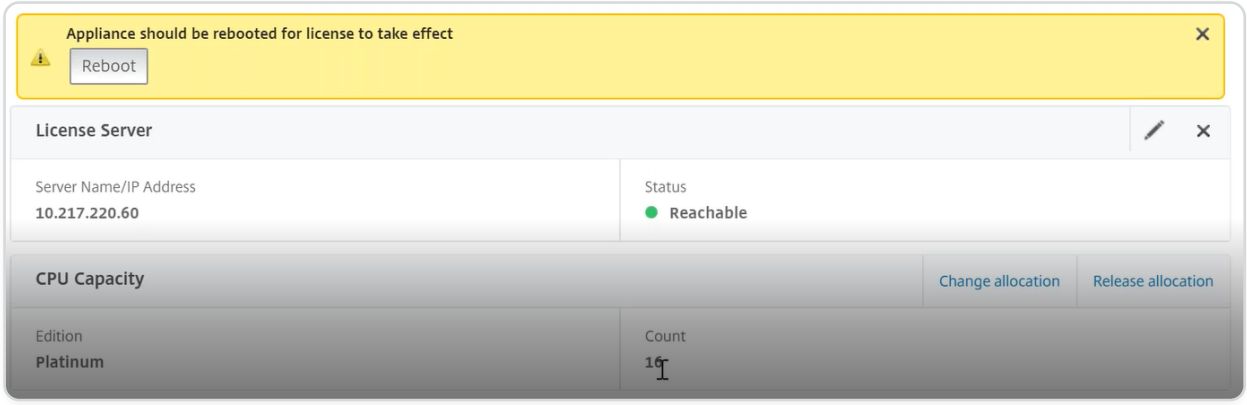


NOTE

You must always register NetScaler VPX instance with NetScaler ADM. If not done already, enable **Register with NetScaler ADM** and type NetScaler ADM login credentials.

7. In the **Allocate licenses** window, select the type of license. The window displays the total and the available virtual CPUs and also the CPUs that can be allocated. Click **Get Licenses**.
8. Click **Reboot** on the next page to apply for the licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

You can also release the current license and check out from a different edition. For example, you are already running Standard edition license on your instance. You can release that license and then check out from Advanced edition.

Configuring licensing server in NetScaler VPX license using CLI

In the NetScaler VPX console, type the following commands for the following two tasks:

1. To add the licensing server to the NetScaler VPX:

   ```
   add licenseserver <IP address of the license server>
   ```

2. To apply for the licenses:

   ```
   set capacity -vcpu - edition premium
   ```

   When prompted, reboot the instance by typing the following command:

   ```
   reboot -w
   ```

Update a licensing server IP address

You can update the licensing server IP address in the VPX instance, without any impact on the allocated license bandwidth on the instance and data loss. To update the licensing server IP address, type the following command on the VPX instance:

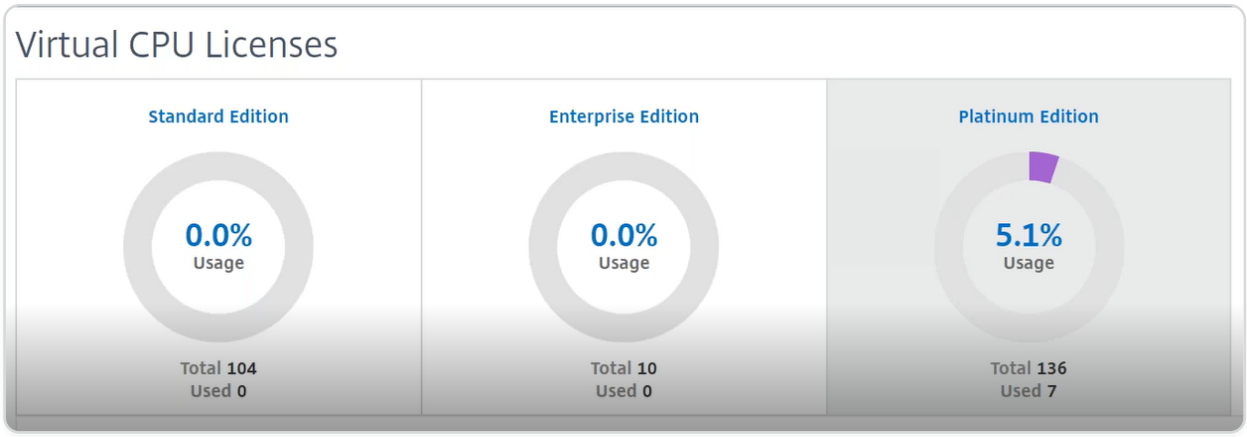
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and release the resources associated with the previous licensing server.

Managing virtual CPU licenses on NetScaler ADM

1. In NetScaler ADM, navigate to **Infrastructure > Pooled Licensing > Pooled VCPU**.
2. The page displays the licenses allocated for each type of license edition.
3. Click the number within each donut to view the NetScaler instances that are using this license.



Virtual CPU licensing for NetScaler CPX

While provisioning the NetScaler CPX instance, you can configure the NetScaler CPX instance to check out licenses from the license server depending on the CPU usage on the instance.

NetScaler CPX relies on the license server, running on NetScaler ADM, to manage the licenses. NetScaler CPX checks out the licenses from the license server when it is starting up. The licenses are checked in back to the license server when the NetScaler CPX shuts down.

You can download the NetScaler CPX image from the Quay container registry using the 'docker pull' command and deploy it on your environment.

There are three license types available for CPX licensing:

1. Virtual CPU subscription licenses supported for CPX and VPX
2. Pooled Capacity licenses
3. CP1000 licenses that support single to multiple vCPUs for CPX only

To configure vCPU subscription licenses while provisioning the NetScaler CPX instance:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Specify the number of vCPU licenses that the NetScaler CPX instance uses.

- This value is entered as an environment variable through Docker, Kubernetes, or Mesos/Marathon.
- The target variable is “CPX_CORES.” The CPX can support from 1 to 16 cores.

To specify 2 cores, you can perform the docker run command as follows:

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2
```

While provisioning a NetScaler CPX instance, define the NetScaler Licensing Server as an environmental variable in the **docker run** command as shown below:

```
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 NetScaler Licensing Server.
- *\<LS_PORT\>* is the port of the NetScaler Licensing Server. By default, the port is 27000.

NOTE

By default, the NetScaler CPX instance checks out the license from the vCPU subscription pool. The CPX instance checks out an "n" number of licenses if the instance is running with "n" CPUs.

To configure NetScaler Pooled Capacity or CP1000 licenses while provisioning the NetScaler CPX instance:

If you want to check out licenses for the CPX instance using the pooled licensing (bandwidth-based) or the CPX private pool (CP1000 or private-pool-based), you must provide the environment variables accordingly.

For example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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 NetScaler CPX instance then retrieves "n" number of instances for "n" number of cores specified for CPX_CORES. The most common use case is to specify n = 1 for a checkout of a single instance. Multicore CPX use cases check out “n” vCPUs (where “n” is from 1 to 7).

```
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 Premium bandwidth pool yet enables CPX to run up to 2000 Mbps. In Pooled Licensing, the first 1000 Mbps is not charged.

NOTE

Specify the corresponding number of vCPUs for the desired target bandwidth when checking out from the bandwidth pool as detailed in the following table:

NUMBER OF CORES (VCPU)	MAXIMUM BANDWIDTH
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage system settings

The following table describes the list of options available under **Settings** > **Administration**:

Network Configurations

NETWORK CONFIGURATIONS	OPTIONS	DESCRIPTION
IP Address, Second NIC, Host Name and Proxy Server	IP address	Displays the NetScaler ADM network configuration IP address details that are used to deploy NetScaler ADM
	Second NIC	Enables you to configure a second NIC to isolate NetScaler ADM management access. For more information, see Configure a dual NIC to access NetScaler ADM
	Host name	Enables you to assign a host name to NetScaler ADM. For more information, see Assign a host name to a NetScaler ADM server
	Proxy Server	Enables you to configure ADM as a proxy server. For more information, see NetScaler ADM as an API proxy server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Configurations

SYSTEM CONFIGURATIONS	OPTIONS	DESCRIPTION
System, Time zone, Allowed URLs and Message of the day	Basic Settings	Enables you to modify system settings such as enable `nsrecover` login, enable session timeout, and so on
	Time Zone	Enables you to modify the timezone to be used in NetScaler ADM. The default timezone is UTC
	Allowed URL List	Enables you to configure URLs to send uninterrupted requests to ADM. You can configure it with the value "none" if no URL to be added
	Message of the day	Enables you to create a welcome message in NetScaler ADM. You can use this feature to set reminder messages for yourself or the user who logs on to NetScaler ADM. Click **Enable Message**, type the message in the message box, and click **Save**
View ADM Fingerprint		Enables you to copy the unique NetScaler ADM fingerprint ID to get started with service graph
Configure Customer Identity		Enables you to protect the network resources by permitting only authenticated customers or users to access its network. For more

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SYSTEM CONFIGURATIONS	OPTIONS	DESCRIPTION
		information, see Data Governance
CUXIP Settings		If you select this check box, usage statistics are collected for the sole purpose of improving the GUI. The received data is used only by Citrix engineers and is not shared with anyone

System Maintenance

SYSTEM MAINTENANCE	DESCRIPTION
Upgrade NetScaler ADM	Enables you to upgrade the NetScaler ADM through GUI. For more information, see Upgrade
Reboot NetScaler ADM	Enables you to reboot NetScaler ADM
Shut Down NetScaler ADM	Enables you to shut down NetScaler ADM
Disaster Recovery	Enables you to view disaster recovery node information. For more information, see Configure Disaster Recovery

Data Pruning

DATA PRUNING	OPTIONS	DESCRIPTION
System and Instance Data Pruning	System	Enables you to limit the amount of reporting data being stored in NetScaler ADM server database. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATA PRUNING	OPTIONS	DESCRIPTION
		more information, see Configure system prune settings
	Instance Events	Enables you to limit the event messages reporting data stored in NetScaler ADM
	Instance Syslog	Enables you to limit the amount of syslog data stored in the database. For more information, see Configure instance syslog prune settings
	Network Reporting	Enables you to limit the network reporting data stored in NetScaler ADM

Backup

BACKUP	OPTIONS	DESCRIPTION
Configure System and Instance backup	System	Enables you to configure the initial backup settings before doing a system backup. For more information, see System Backup Settings
	Instance	Enables you to configure settings on NetScaler ADM to back up a selected NetScaler instance or multiple instances. For more information, see Configure instance backup settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Notifications

EVENT NOTIFICATIONS	OPTIONS	DESCRIPTION
Configure Event Notification and Digest	Event Notification	You can send notifications to select groups of users for several system-related functions. These system functions are organized into event categories such as SystemReboot, StatusPoll, SystemState, and so on. You can configure NetScaler Application Delivery Management (ADM) to send you notifications either through Email, SMS, or Slack. This ensures that you are notified of any system-level activities such as exceeding of data storage or backup failure.
	Event Digest	Enables you to get a consolidated report of important system and feature events

SSL Settings

SSL SETTINGS	DESCRIPTION
Install SSL Certificate	Enables you to install SSL certificate and SSL Key file
View SSL Certificate	Enables you to view the SSL certificate details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL SETTINGS	DESCRIPTION
Configure SSL Settings	For more information, see Configure SSL settings
SSL Certificates	Enables you to upload, download, or delete an SSL certificate or SSL Key file
Cipher Groups	For more information, see Configure a Cipher Groups

Configure Features

CONFIGURE FEATURES	DESCRIPTION
Disable or enable features	You can enable or disable features in NetScaler ADM. For more information, see Enable or disable ADM features

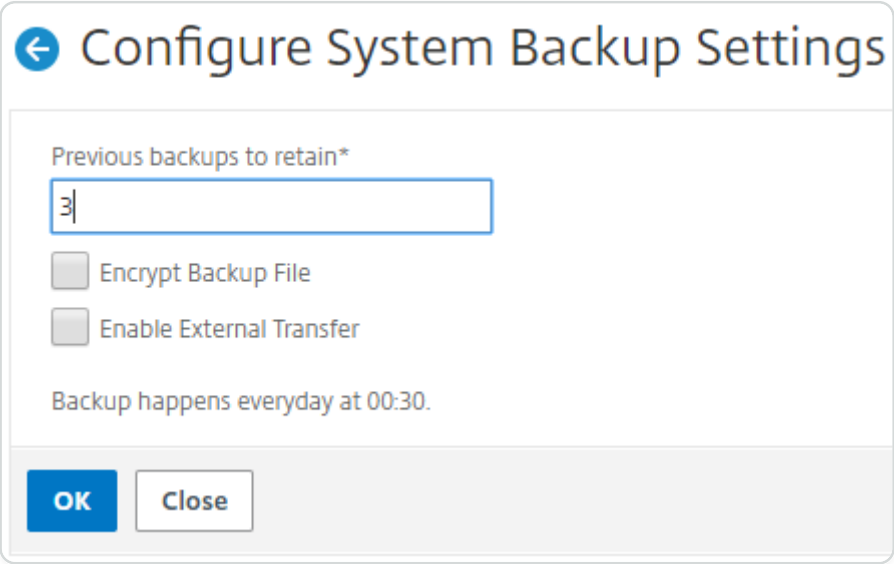
Configure system backup settings

Set your initial System Backup Settings before you need to back up and restore the NetScaler® Application Delivery Management (ADM) system.

1. Navigate to **Settings > Administration**. Under **Backup**, click **Configure System and Instance backup**.
2. On the **Backup > System** page, specify the following:
   - Previous backups to retain. You can only retain up to 10 backups.
   - Select **Encrypt Backup File** to encrypt the backup files.
   - Select **Enable External Transfer** to transfer a copy of your backup file to another system. When you want to restore the configuration, you have to first upload the file to the NetScaler ADM server and then perform the restore operation. Specify the server, user name and password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see Transfer a NetScaler ADM Backup File to an External System.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **OK**.



Configure an NTP server

You can configure a Network Time Protocol (NTP) server in NetScaler® Application Delivery Management (ADM) to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server on NetScaler ADM:

1. Navigate to **Settings > NTP Servers**, and then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
   - **Server Name/IP Address** – Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - **Minimum Poll Interval** – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2\^6, enter 6.
   - **Maximum Poll Interval** – Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2\^8, enter 8.
   - **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.
   - **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.

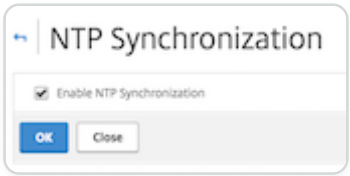
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.

To enable NTP synchronization on NetScaler ADM:

1. Navigate to **Settings > NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** check box.
3. Click **OK**.



Note

> You can find the NTP logs messages in the /var/log directory in the file `/var/log/ntpd.log` file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade NetScaler® Application Delivery Management (ADM)

Each NetScaler ADM release offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read the release notes before you upgrade the software. It is important to understand the licensing framework and types of licenses before you start to upgrade.

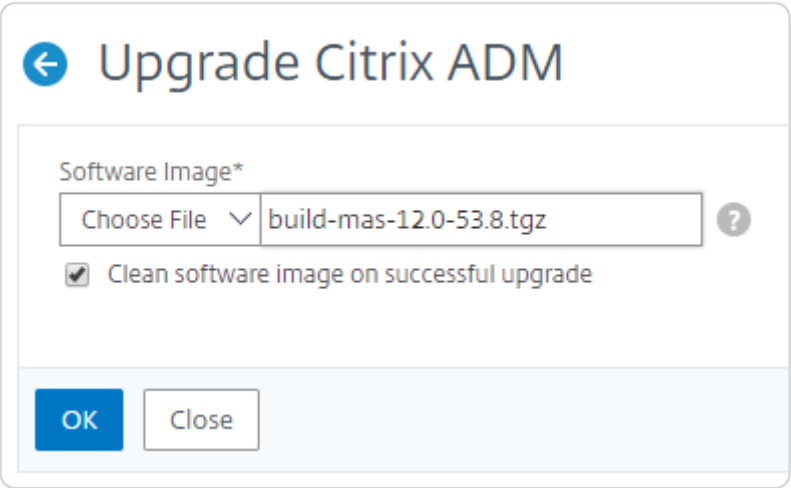
To upgrade NetScaler ADM:

1. Navigate to **Settings > Administration**. Under **System Maintenance**, click **Upgrade NetScaler ADM**.
2. On the Upgrade NetScaler ADM page, upload a new image file by selecting either **Local** (your local computer) or **Appliance**.

   NOTE

   When you select **Appliance**, ensure that the upgrade image is available at `/var/mps/mps_images` in NetScaler ADM.

   By default, the software image is cleaned up after a successful upgrade.
3. Click **OK**.



How to reset the password for NetScaler® ADM

The procedure to reset the password for NetScaler ADM might differ on hypervisors where it is hosted. If you have changed your default password and want to reset to default password, you can reset the password by rebooting the NetScaler ADM node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Hypervisor™ using XenCenter:

1. Log on to Citrix Hypervisor using XenCenter.
2. Select the NetScaler ADM node, right-click, and select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900

Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
\
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 2 seconds...
```

4. Run **boot -s** command at the OK prompt.

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900

Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
\
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 1 second...

Type '?' for a list of commands, 'help' for more detailed help.
OK _
```

NetScaler ADM reboots and displays the following message:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
talk_to_backend: xn_num_q 1 max_q 16  err 0
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
```

5. Press **Enter** to get the /u@ prompt.

```
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
u@
```

6. Mount the flash partition using the following command:

```
mount /dev/da0s1a /flash
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@
```

7. Create a file using the following command:

   `touch /flash/mpsconfig/.recover`

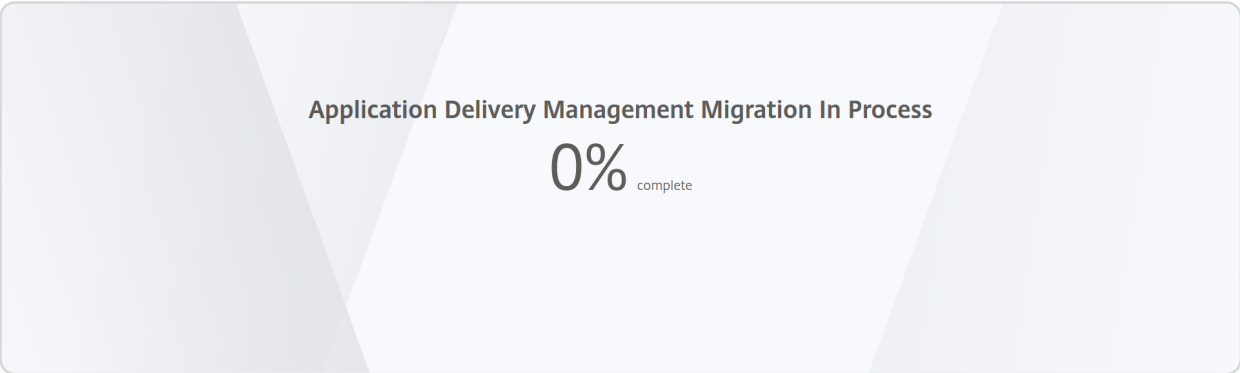
   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler ADM.

```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. Access the NetScaler ADM GUI and wait until the reboot is complete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hypervisor.

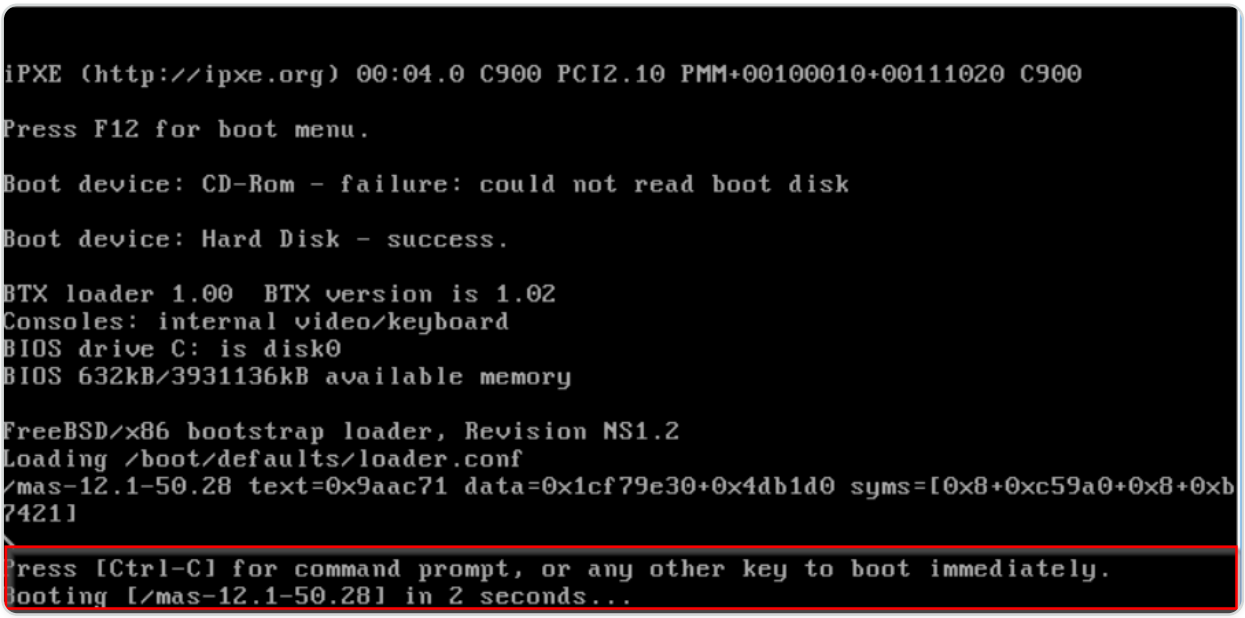
Note

> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:

- `rm /flash/mpsconfig/master.passwd`
- `rm –rf /etc/passwd`

Esx using vSphere:

1. Log on to ESX using vSphere.
2. Select the NetScaler ADM node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.



4. Run **boot -s** command in the OK prompt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The NetScaler ADM reboots.

5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

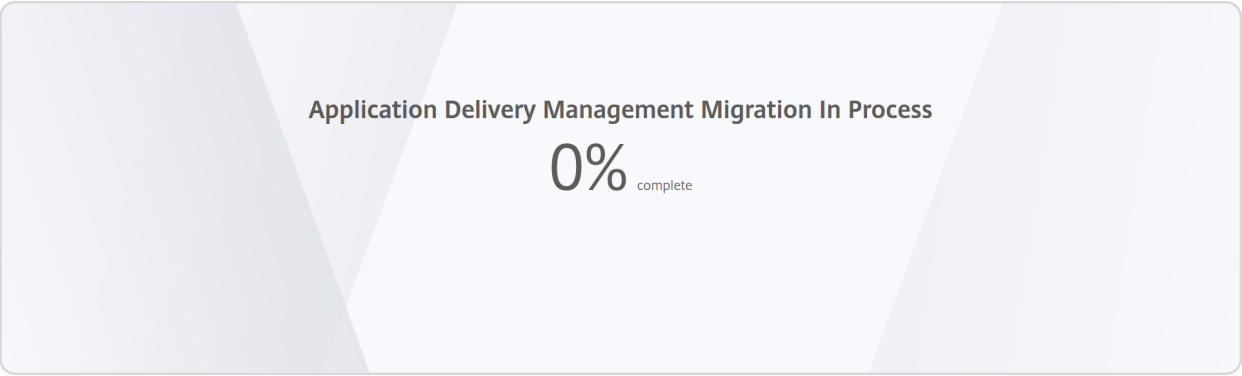
   `mount dev/da0s1a /flash`

7. Create a file using the following command:

   `touch /flash/mpsconfig/.recover`

   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler ADM.
9. Access the NetScaler ADM GUI and wait until the reboot is complete.

   You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from ESX server.

   Note

   > After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

Hyper-v using Hyper-v manager:

1. Log on to hyper-v using hyper-v manager.
2. Select the NetScaler ADM node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900

Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]

Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 2 seconds...
```

4. Run the **boot -s** command at the OK prompt.

   The NetScaler ADM reboots.

5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

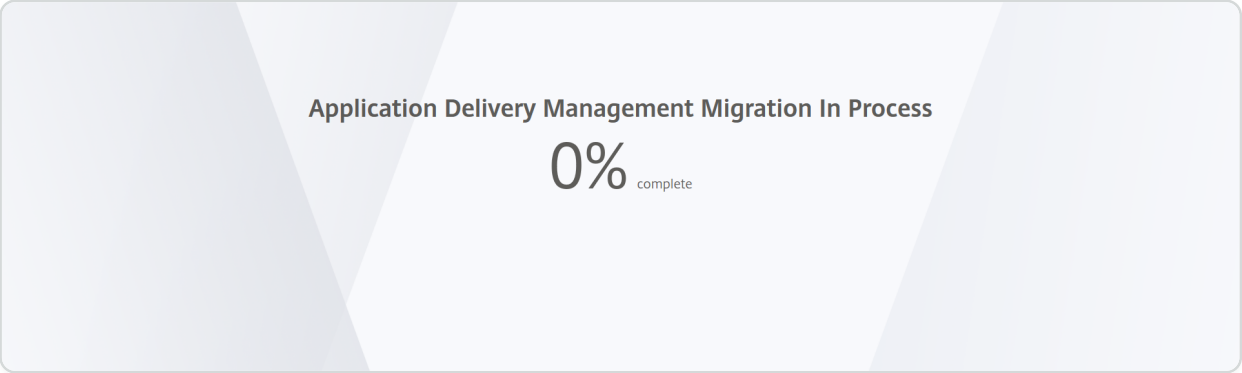
   `mount dev/ad0s1a /flash`

7. Create a file using the following command:

   `touch /flash/mpsconfig/.recover`

   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler ADM.
9. Access the NetScaler ADM GUI and wait until the reboot is complete.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hyper-v manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note

After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:

- `rm /flash/mpsconfig/master.passwd`
- `rm –rf /etc/passwd`

Linux KVM server (SSH to KVM Server by using any SSH client):

1. Log on to NetScaler ADM using an SSH client to the KVM server.
2. Reboot NetScaler ADM.
3. Press **CTL + C** to interrupt the boot sequence shortly after the **Loading /boot/defaults/loader.conf** message is displayed.
4. At the OK prompt, run the following command:

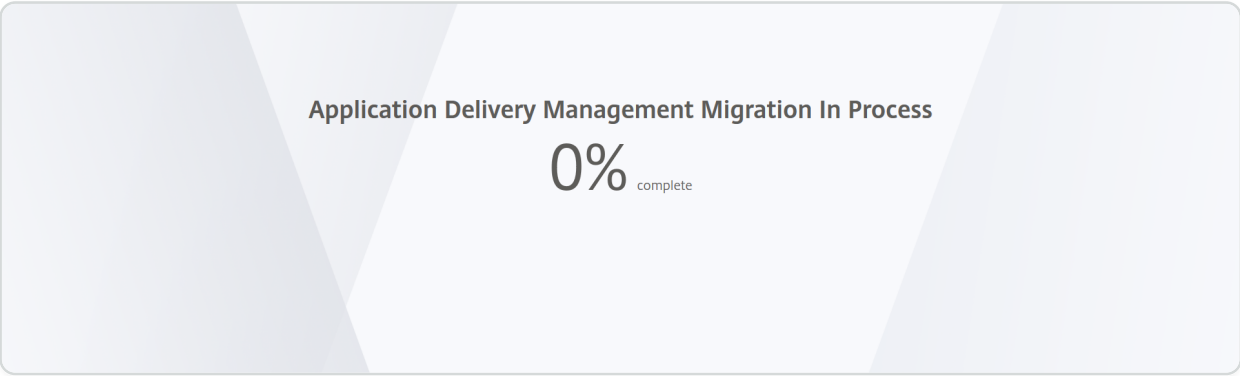
   `set console='comconsole,vidconsole'`
5. Run the **boot -s** command to reboot NetScaler ADM.
6. After the **Enter full path of shell or RETURN for /bin/sh:** message is displayed, press **Enter** to get the /u@ prompt.
7. Mount the flash partition using the following command:

   `mount dev/vtbd0s1a /flash`
8. Create a file using the following command:

   `touch /flash/mpsconfig/.recover`

   The password is now reset to default password.
9. Run the **Reboot** command to reboot NetScaler ADM.
10. Access the NetScaler ADM GUI and wait until the reboot is complete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from the SSH console.

Note

> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler ADM:

- `rm /flash/mpsconfig/master.passwd`
- `rm –rf /etc/passwd`

Configure a secondary NIC to access NetScaler® ADM

You can configure a second NIC for isolating management access to NetScaler ADM. Using this second NIC feature, depending upon your requirement, you can choose how you want to isolate the traffic that is received and sent through the NetScaler ADM.

Consider a scenario in which you want to isolate the traffic to:

- Have all communications between NetScaler ADM and its managed NetScaler instances in one network.
- Have management access to NetScaler ADM in another network.

In this scenario, as an administrator, you can:

- Configure one IP address for the traffic between NetScaler ADM and its managed NetScaler instances.
- Configure another IP address for managing the NetScaler ADM software to perform all administrative tasks in the software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If NetScaler ADM is configured as an HA pair, the management IP address configured on the second NIC is associated with the primary node.

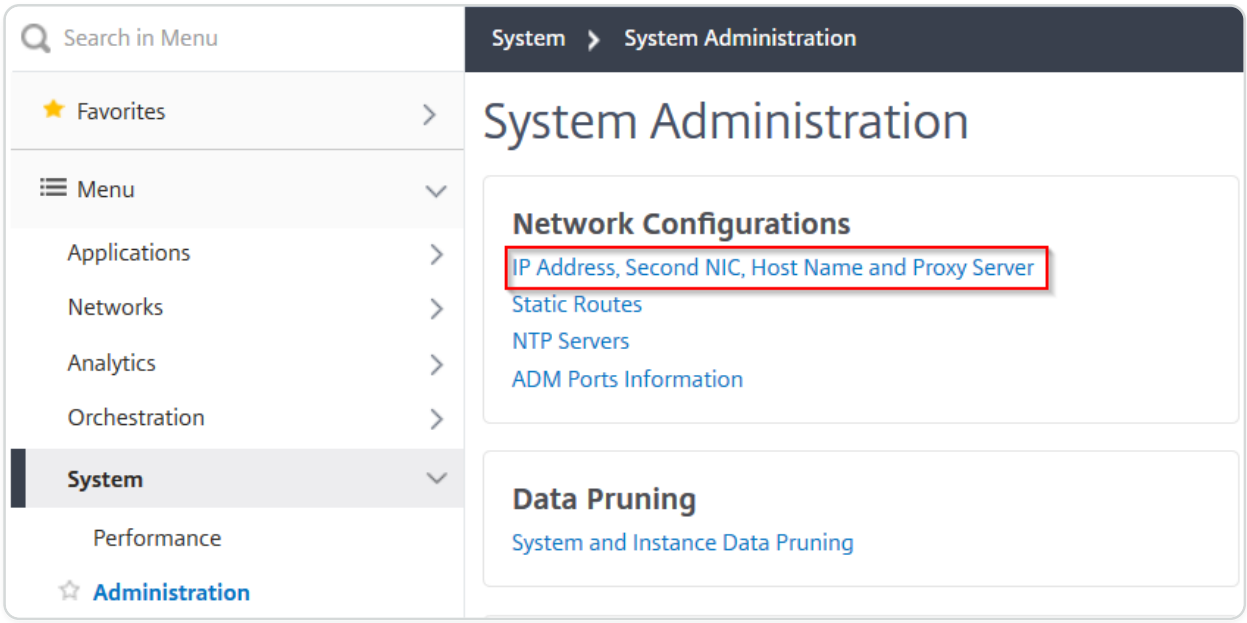
Prerequisites

- Ensure you have deployed and configured **NetScaler ADM 13.0 Build 47.x or later** on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).
- Ensure you have added the second NIC on the hypervisor (Citrix Hypervisor™, Microsoft Hyper-V, Linux KVM, or VMware ESXi).

To assign an IP address to a NIC on a Citrix Hypervisor and create a secondary interface, see Assign an IP Address to a NIC.

Configure a second NIC in NetScaler ADM

1. Log on to ADM GUI.
2. Navigate to **Settings > Administration**.
3. Under **Network Configuration**, click **IP Address, Second NIC, Host Name and Proxy Server**.



The **Network Configuration** page is displayed.

4. Click the Second NIC tab and configure the following parameters:

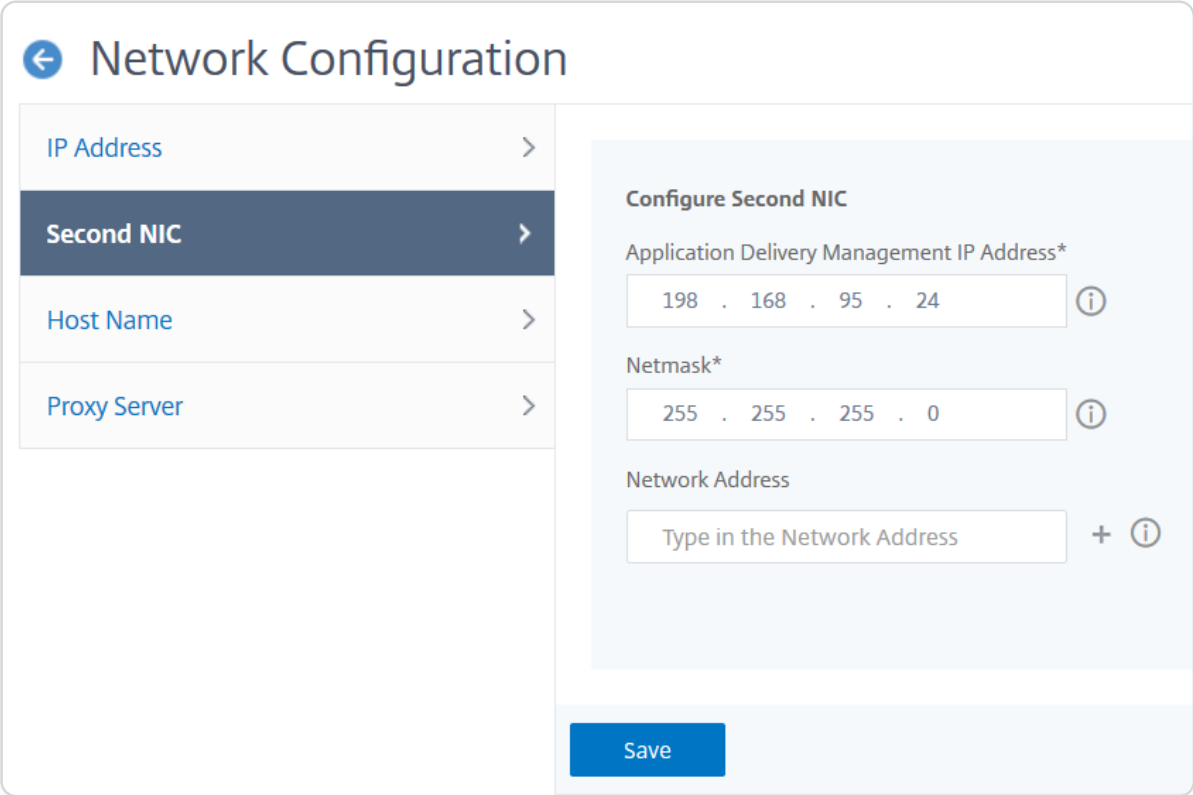
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Application Delivery Management IP Address** – Enter a valid IP address to access NetScaler ADM. You can use this IP address to access NetScaler ADM, apart from the existing management IP address.

b. **Netmask** – Enter the netmask address to specify the network host. The default address is 255.255.255.0.

c. **Network Address** – Enter an IP address to add a route entry for NetScaler ADM. Click **+** to add more IP addresses. This field is optional.

d. Click **Save**.



Configure a secondary NIC to access ADM agent

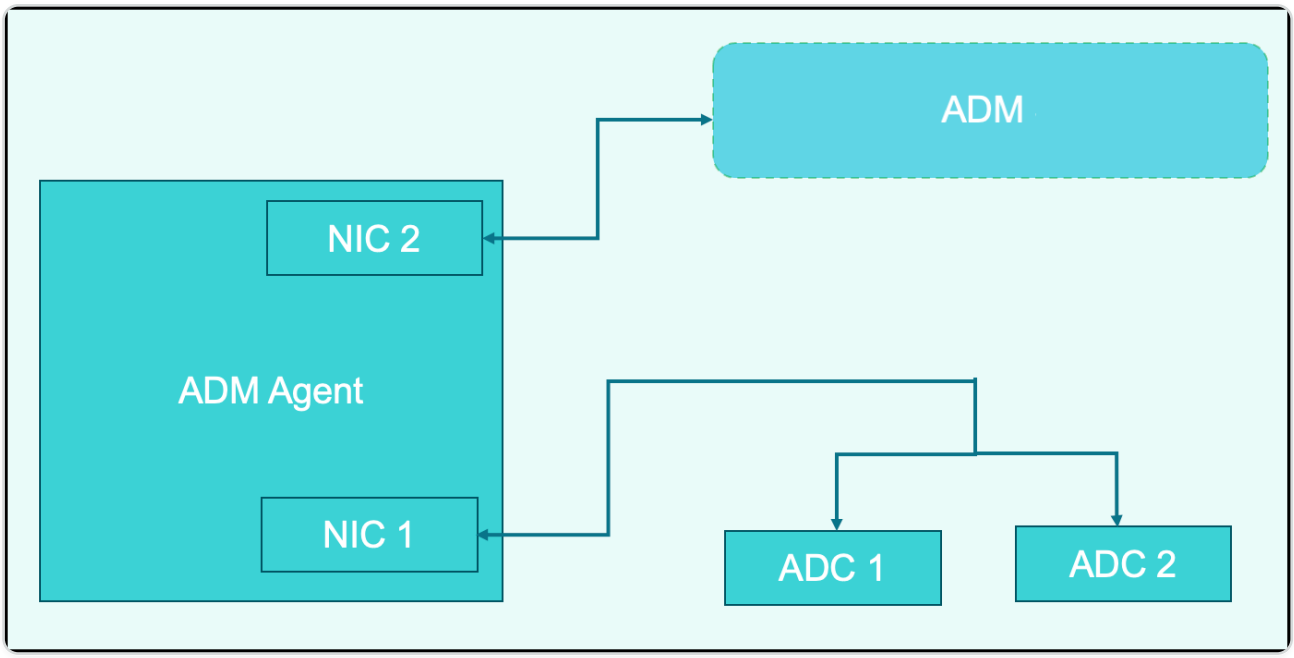
You can configure two NICs on an ADM agent. Using the Dual NIC architecture, ADM agent will be able to:

- Establish communication between ADM agent and ADC instances - You can use the first NIC to isolate the traffic that is received and sent through the NetScaler ADM and also to communicate between NetScaler ADM and its managed NetScaler instances in another network.
- Establish communication between ADM agent and NetScaler® ADM - You can use the second NIC to manage the NetScaler ADM that is on a network and perform administrative tasks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You cannot interchange the functionality and configuration of both the NICs.



In this scenario, as an administrator, you can:

- Configure IP address for the traffic between NetScaler ADM and its managed NetScaler instances.
- Configure IP address for managing the NetScaler ADM software to perform all administrative tasks in the software.

NOTE

It is not mandatory to configure Dual NICs for an ADM agent. It is optional and is required only when traffic between ADM agent, NetScaler ADM and ADCs needs to be separated.

Modify the IPV4 NIC network addresses using CLI

1. Open an SSHconnection to the NetScaler agent console by using an SSH client, such as PuTTY.
2. Log in using the **nsrecover/nsroot** credentials and switch to the shell prompt.
3. Run the command **ifconfig**. You can see the details of the two NICs that you have configured -
    - NIC 1 – For communication between ADM Agent to ADC Communication

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NIC 2 – For communication between ADM Agent to NetScaler ADM

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Run the command **networkconfig**. A menu appears which allows you to set or modify the IPV4 network addresses.

```
bash-3.2# /mps/networkconfig

--------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Agent Host Name [ns]:
      2. Citrix ADM Agent IPv4 address [10.102.103.247]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.103.1]:
      5. DNS IPv4 Address [10.102.166.70]:
      6. Second NIC IPv4 address [10.102.103.250]:
      7. Second NIC Netmask [255.255.255.0]:
      8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
      9. Second NIC Gateway IPv4 address [10.102.103.2]:
     10. Cancel and quit.
     11. Save and quit.
```

NOTE

Second NIC Network address can take multiple IP values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select a menu item to modify. Save and quit the settings.

Configure syslog purging interval

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the Citrix Application Delivery Controller (ADC) instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the NetScaler instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

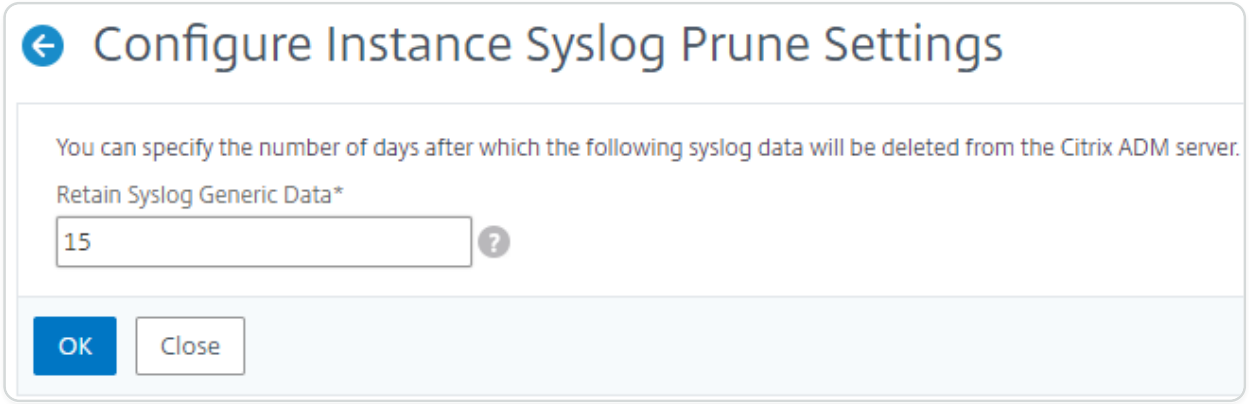
To limit the amount of syslog data stored in the database, you can specify the interval at which you want to prune syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler® Application Delivery Management (ADM):

- Generic Syslog Data
- AppFirewall Data
- NetScaler Gateway Data

You can also configure the NetScaler Gateway prune interval by syslog type. This prune interval takes precedence over the rune interval configured to retain NetScaler Gateway data.

To configure syslog prune interval settings for NetScaler ADM:

1. Navigate to **Settings > Administration**. Under **Data Pruning**, click **System and Instance Data Pruning** and then click **Instance Syslog**.
2. In **Configure Instance Syslog Prune Settings** page, specify **Retain Syslog Generic Data(days)**. Type the number of days for which NetScaler ADM retains generic syslog messages.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure system prune and event prune settings

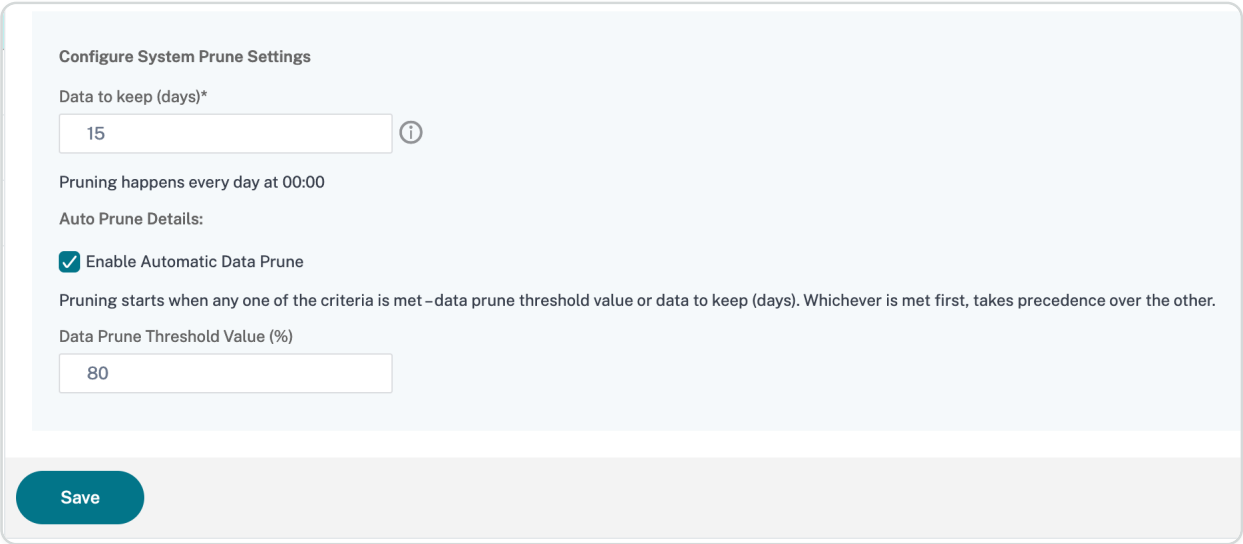
To limit the amount of reporting data being stored in your NetScaler Application Delivery Management (ADM) software database, you can prune it. You can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

NOTE

The value you specify can't be more than 30 days or be less than 15 days.

To configure system prune settings for performance reports:

1. Navigate to **Settings** > **Administration**. Under **Data Pruning**, click **System and Instance Data Pruning**.
2. In the **Configure System Prune Settings** page, specify the following:
   - Number of days to keep the data
   - Percentage of disk space (pruning threshold)
3. Click **OK**.



You can enable automatic pruning by selecting the **Enable Automatic Data Prune** check box. An alarm is triggered and an email is sent when disk usage breaches the configured **Data Prune Threshold Value**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

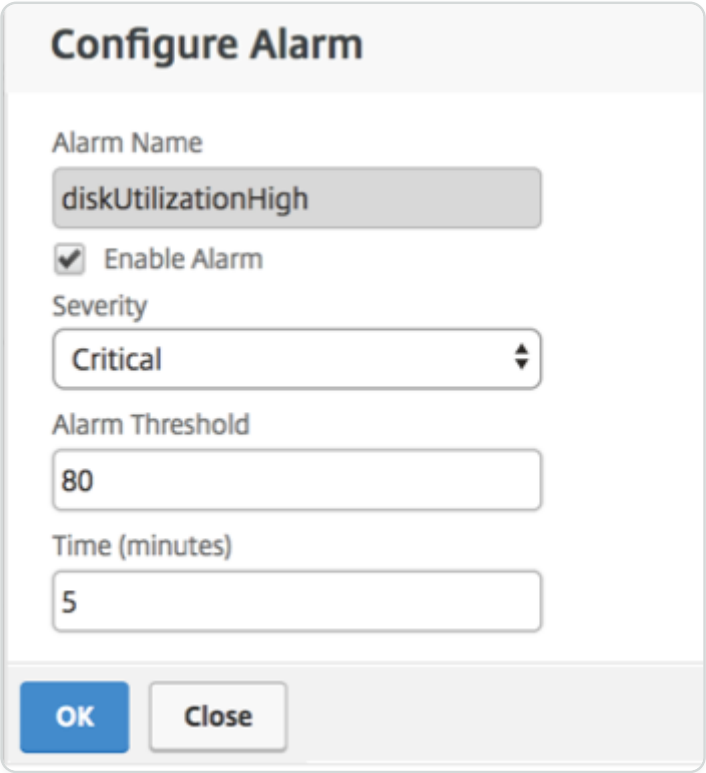
NOTE

Pruning starts when any one of the criteria is met – data prune threshold value or data to keep (days). Whichever is met first, takes precedence over the other.

To configure and enable alarm settings:

1. Navigate to **Settings** > **SNMP**. Click **Alarms** on the upper-right corner.
2. Select the alarm that you want to configure (for example, diskUtilizationHigh) and click **Edit**.
3. In the **Configure Alarm** page, specify the following:

- **Severity**—Select the severity level.
- **Alarm Threshold**—Type the value for which the event severity is calculated.
- **Time**—Type the time (in minutes) after which you want to trigger the alarm.



Configure Events Prune Settings by Using NetScaler® ADM

To limit the amount of event messages data being stored in your NetScaler ADM database, you can specify the interval for which you want NetScaler ADM to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Administration > Data Pruning** and click **System and Instance Data Pruning**. Click **Instance Events**.
2. Enter the time interval, in days, for which you want to keep the data on the NetScaler ADM server and click **Save**.

Enable shell access for non-default users

You can enable shell access for non-default users in NetScaler® Application Delivery Management (ADM). You can use this feature to enable and set up communication mode with instances.

NOTE

By default, shell access is disabled for non-default users.

To enable shell access for non-default users in NetScaler ADM:

1. In NetScaler ADM, navigate to **System** \> **System Administration**.
2. In **System Settings**, click **Change System Settings**.
3. On the **Modify System Settings** page, configure the following parameters:
   - **Communication with instances** - Select the communication protocol.
   - **Secure Access** - Enable secure access for NetScaler ADM.
   - **Enable Session Timeout** - Specify the time period for which to retain an inactive session.
   - **Allow Basic Authentication** - Allow Management Service to accept credentials given using Basic Authentication Protocol.
   - **Enable nsrecover Login** - Enable `nsrecover` login on Management Service.
   - **Enable Certificate Download** - Enables you to download certificates from the added NetScaler.
   - **Enable Shell access for non-nsroot User** - Enable shell access for non-default users in NetScaler ADM.
   - **Prompt user credentials for instance login** - Allow users to enter their user credentials while logging on to instances from NetScaler ADM.
4. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Recover inaccessible NetScaler® ADM servers

NetScaler Application Delivery Management (ADM) now provides a database maintenance tool to perform cleanup of the system database. You can now launch the NetScaler ADM utility tool to connect to the file system, delete a few components, and make the database accessible. NetScaler ADM recovery script is a tool that helps to recover space in the file system by clearing old or unused database tables and files. The tool assists you to navigate through the database tables and files in successive steps and shows the current space occupied on the filesystem by respective items. Once you have selected the database tables and files to be deleted, the tool deletes those from the filesystem after confirmation.

How to Use NetScaler ADM Database Recovery Script for a NetScaler ADM Standalone Deployment

Use the following procedure in a single server NetScaler ADM deployment to connect to the file system, delete a few components, and make the database accessible, and then perform the recovery operations.

1. Using an SSH client or your hypervisor's console, logon to NetScaler ADM and type the following command:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. When the screen displays a caution message for stopping a few NetScaler ADM processes, type "y" and press the **Enter** key.

   The following screen appears while the system determines which components of the database you can delete without affecting the system's core files.

```
-------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
-------------------------------------------------------------------------------

        This utility helps you gain disk space by performing cleanup.


                    Checking whether DB is accessible...

                              DB is accessible.

            Please wait. Gathering data. This will take some time.


                              <----------->
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. The screen displays the list of files in the database. Type "y" and press the Enter key to begin the cleanup process.

```
---------------------------------  SUMMARY  ----------------------------------

                    DB component                Current size
                    ------------                ------------

                    Analytics  ------------------  184.58 MB
                    Perf Reports  ----------------  43.73 MB
                    App Summary  -----------------  12.03 MB
                    App Health Summary  -----------  6.33 MB
                    App Counter Data  -------------  5.30 MB
                    Device Syslogs  --------------  56.00 KB
                    Device Events  ---------------  40.00 KB

                    Filesystem component        Current size
                    --------------------        ------------

                    Citrix ADM Images  -----------  15.51 GB
                    Core Files  ----------------  718.37 MB
                    Citrix ADC Images  ----------  453.32 MB
                    Techsupport Bundles  --------  439.35 MB
                    Device Backup  --------------  131.79 MB
                    Citrix ADM Backup  -----------  35.21 KB
                  Citrix ADC VPX ESXi Images  -------  0.00 B
                    Citrix ADC SDX Images  ---------  0.00 B
                    Citrix ADC CPX images  ---------  0.00 B

-------------------------------------------------------------------------------

        Do you wish to proceed with cleanup?
        [y/n]: 
```

4. You can select the specific database component that needs to be cleaned and type the corresponding number. Press the **Enter** key.

   For example, to perform System Catalog cleanup, select option 8 in the **DB component** selection menu and type "y" and press the **Enter** key to continue with the system catalog clean up.

NOTE

NetScaler ADM includes user tables known as system catalog. The system catalog is a location in the NetScaler ADM database where a relational database management system stores schema metadata, such as information about tables and columns and internal records. The tables in the system catalog are like regular tables that can accumulate inflated and dead rows over time and therefore, need periodic cleanup for optimal performance. It is a good practice to regularly maintain these tables. The activity not only frees up disk space but also improves the overall performance of the database and therefore of the NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

                                DB components
                                -------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Analytics --------------- 184.58 MB
        [2]  Perf Reports ------------ 41.84 MB
        [3]  App Summary ------------- 11.84 MB
        [4]  App Health Summary ------ 6.09 MB
        [5]  App Counter Data -------- 5.09 MB
        [6]  Device Syslogs ---------- 56.00 KB
        [7]  Device Events ----------- 40.00 KB
        [8]  Clean System Catalog
        [9]  Select all
        [10] Continue without selecting

        Your input: 8
        Are you sure you want to CLEAN SYSTEM CATALOG tables?

        [y/n]: y
```

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."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

                              Filesystem components
                              ---------------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Citrix ADM Images ------- 15.51 GB
        [2]  Core Files -------------- 718.37 MB
        [3]  Citrix ADC Images ------- 453.32 MB
        [4]  Techsupport Bundles ----- 439.35 MB
        [5]  Device Backup ----------- 131.79 MB
        [6]  Citrix ADM Backup ------- 35.21 KB
        [7]  Citrix ADC VPX ESXi Images  0.00 B
        [8]  Citrix ADC SDX Images --- 0.00 B
        [9]  Citrix ADC CPX images --- 0.00 B
        [10] Select all
        [11] Continue without selecting

        Your input: 11
```

5. Type "y" and press the **Enter** key again in the final confirmation screen.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------
                              FINAL CONFIRMATION

                      These components will be cleaned.

                                DB components
                                -------------

                      >>  System Catalog

        No data has been deleted yet.

        If you choose to proceed, all ADM processes will be stopped
        for the remainder of the cleanup.

        Do you wish to proceed with cleanup?
        [y/n]:
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
**************************** Citrix ADM Cleanup Utility ****************************
--------------------------------------------------------------------------------
----------------------------------  SUMMARY  ----------------------------------

                                DB components
                                -------------

          Component name              Present size     Size cleared
          --------------              ------------     ------------

          System Catalog  -------------  189.15 MB  -------  0.00 B
        Cleanup complete.
        Note that even empty tables in DB may appear to occupy some
        space, this is expected.


        To prevent potential unpredictable behavior, we STRONGLY recommend
        rebooting the ADM now.

        Do you want to REBOOT the ADM?
        [y/n]: 
```

6. Type "y" and press the **Enter** key to restart NetScaler ADM.

   Ensure you restart NetScaler ADM after system clean up. Wait for about 30 minutes for internal database operations to complete after NetScaler ADM has restarted. You should then be able to connect to NetScaler ADM database. If not, run the recovery script again to free up more space. When NetScaler ADM is up and running, it should work as expected.

   NOTE

   The current size of the system catalog table is never equal to Zero after clean up. This is because only empty rows are removed from the table and the table might have some valid entries even after they are cleaned up.

How to use NetScaler ADM database recovery script for a NetScaler ADM high availability deployment

The database system for NetScaler ADM servers in a high availability deployment is in continuous synchronization mode. While using the new database recovery tool, you do not need to replicate the procedure on both the NetScaler ADM servers.

1. Using an SSH client or hypervisor's console, log on to the primary node.
2. Run the following command:

   `/mps/mas_recovery/mas_recovery.py`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

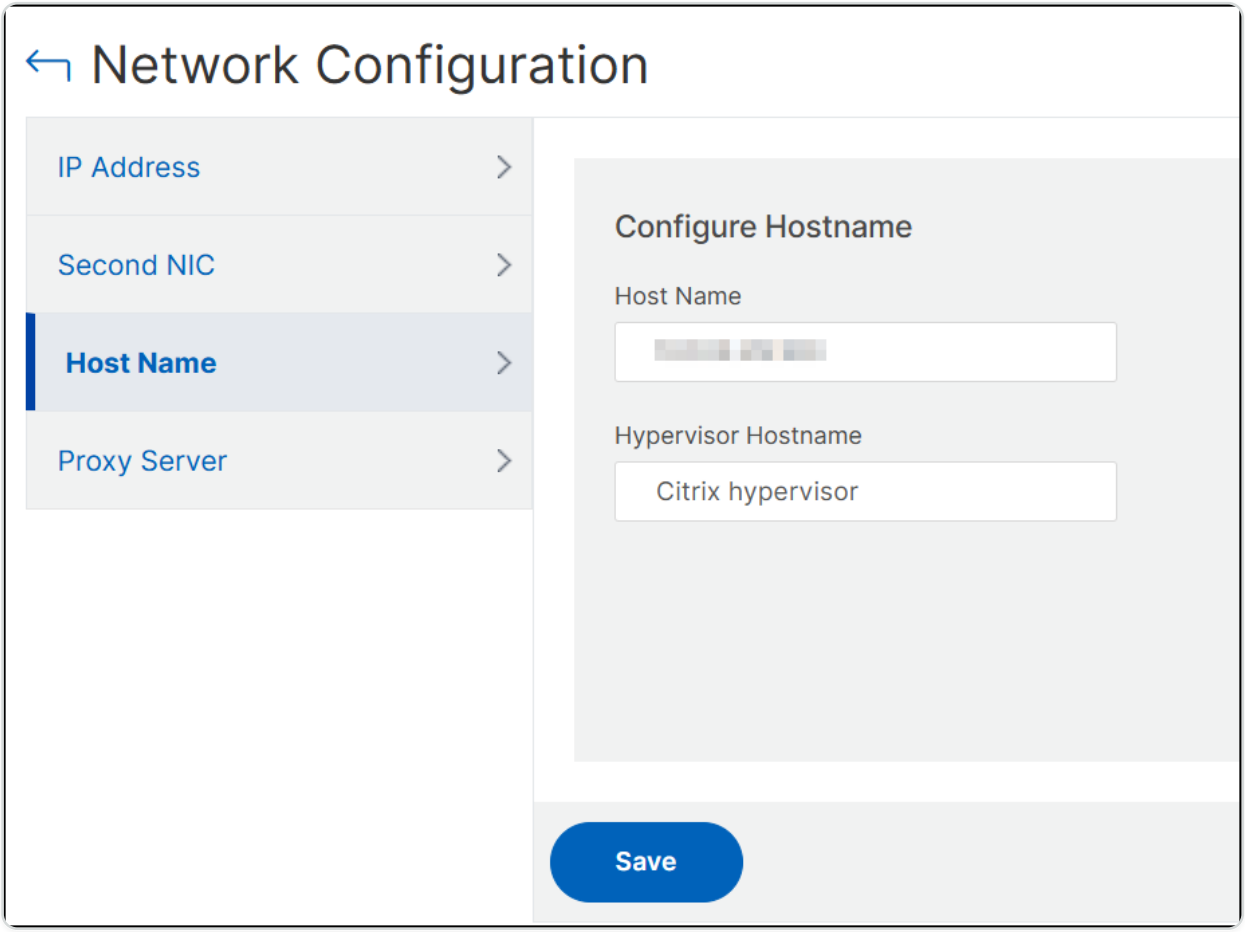
3. Follow the procedure from step 2 available for NetScaler ADM Standalone Deployment Recovery Script

Assign a host name to a NetScaler® ADM server

To identify a NetScaler Application Delivery Management (ADM) server, you can assign the server a host name. The host name is displayed on the Universal license for NetScaler ADM.

To assign a host name to a NetScaler ADM server:

1. In NetScaler ADM, navigate to **System** \> **System Administration**.
2. Under **System Settings**, click **Change Hostname**.
3. On the **Configure Hostname** page, enter a host name and click **OK**.



NOTE

You can also use the `networkconfig` command in your hypervisor and change the host name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

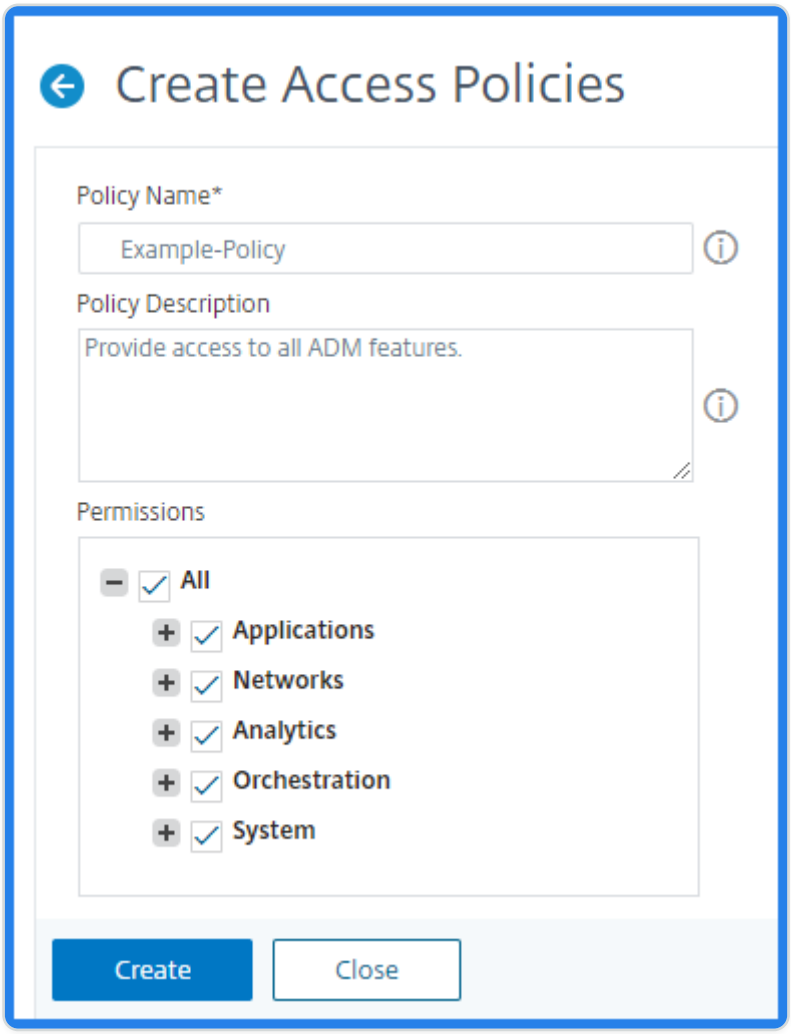
Back up and restore your NetScaler® ADM server

You can take periodic backups of your NetScaler ADM server. You can back up and restore the configuration files, instance details, system data, and so on.

IMPORTANT

Citrix recommends you to restore the ADM server using a backup of the same version. For example, if the ADM version is 13.0, use the 13.0 ADM backup to restore the server.

User access to backup and restore the ADM server is limited. The **Settings > Backup Files** page appears only to the users who have access to all ADM features. A user can access this page only if their access policy has all permissions. Typically, superusers have the access to all ADM features.



For more information, see Configure access policies.

Before you upgrade, back up the ADM server configuration files for precautionary reasons.

The backup includes the following components:

- NetScaler ADM Configuration Files:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - SNMP
  - Syslog server configuration files
  - NTP files
  - SSL certificates
  - Control Center files
- Backups of NetScaler instances that the NetScaler ADM server manages.
- Configuration audit templates.
- System data stored on the database:
  - List of tenants and users created.
  - External authentication server configuration (LDAP, RADIUS, and others).
  - Configuration jobs and job templates created.
- Infrastructure and application data stored on the database:
  - Data from added and managed NetScaler instances.
  - Instance profile details, version details, instance group details, and so on.
  - A static application (group of virtual servers) created by the administrator.
- SNMP settings.

NOTE

Analytics data, events, ADM licenses, and syslog messages are excluded from the backup.

Back up the NetScaler ADM configuration

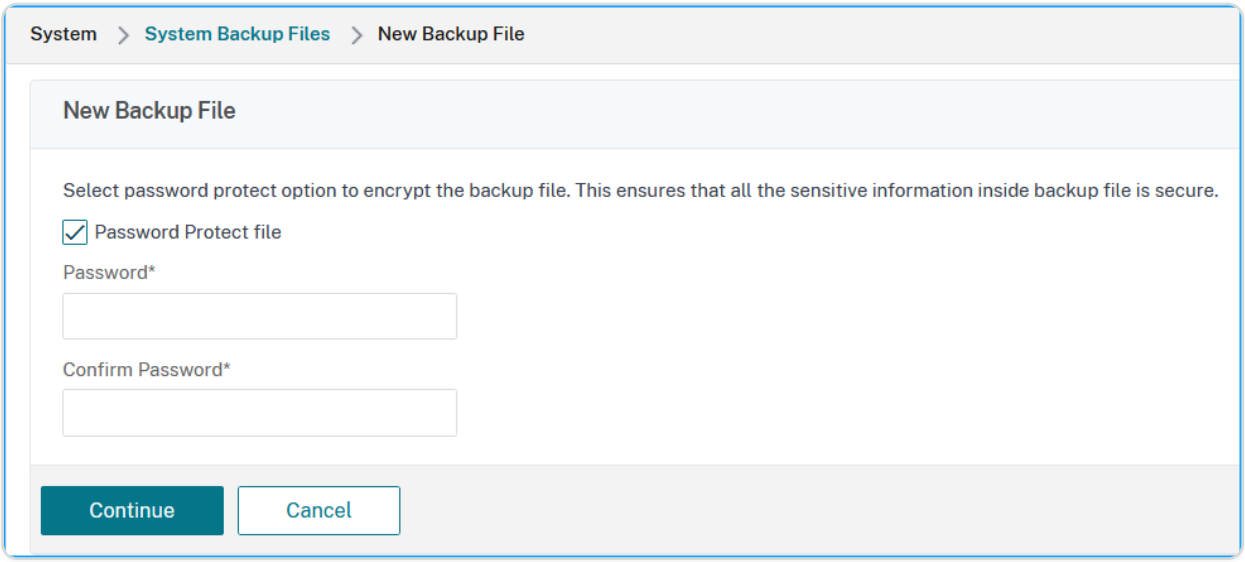
By default, the NetScaler ADM server backs up the configuration every 24 hours (at 00.30 hours). You can also schedule and select the time for the backup. Further, you can move a copy of the backed-up file to another system.

The backup is stored as a compressed TAR file that can also be encrypted. By default, three backup files are retained in the server. To avoid any low disk space issues, you can store a maximum of 10 backup files on your NetScaler ADM server. However, Citrix recommends that you store some copies of your backup files on the server or transfer the files to another system as a precautionary measure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To backup a NetScaler ADM configuration:

1. Navigate to **Settings > Backup Files**, and then click **Back Up**.
2. To encrypt the backup file, select the **Password Protect file** check box, and then provide a password to encrypt the file.



Transfer a NetScaler ADM backup file to an external system

You can transfer a copy of the backup file to another system as a precautionary measure. When you want to restore the configuration, first upload the file to the NetScaler ADM server and then perform the restore operation.

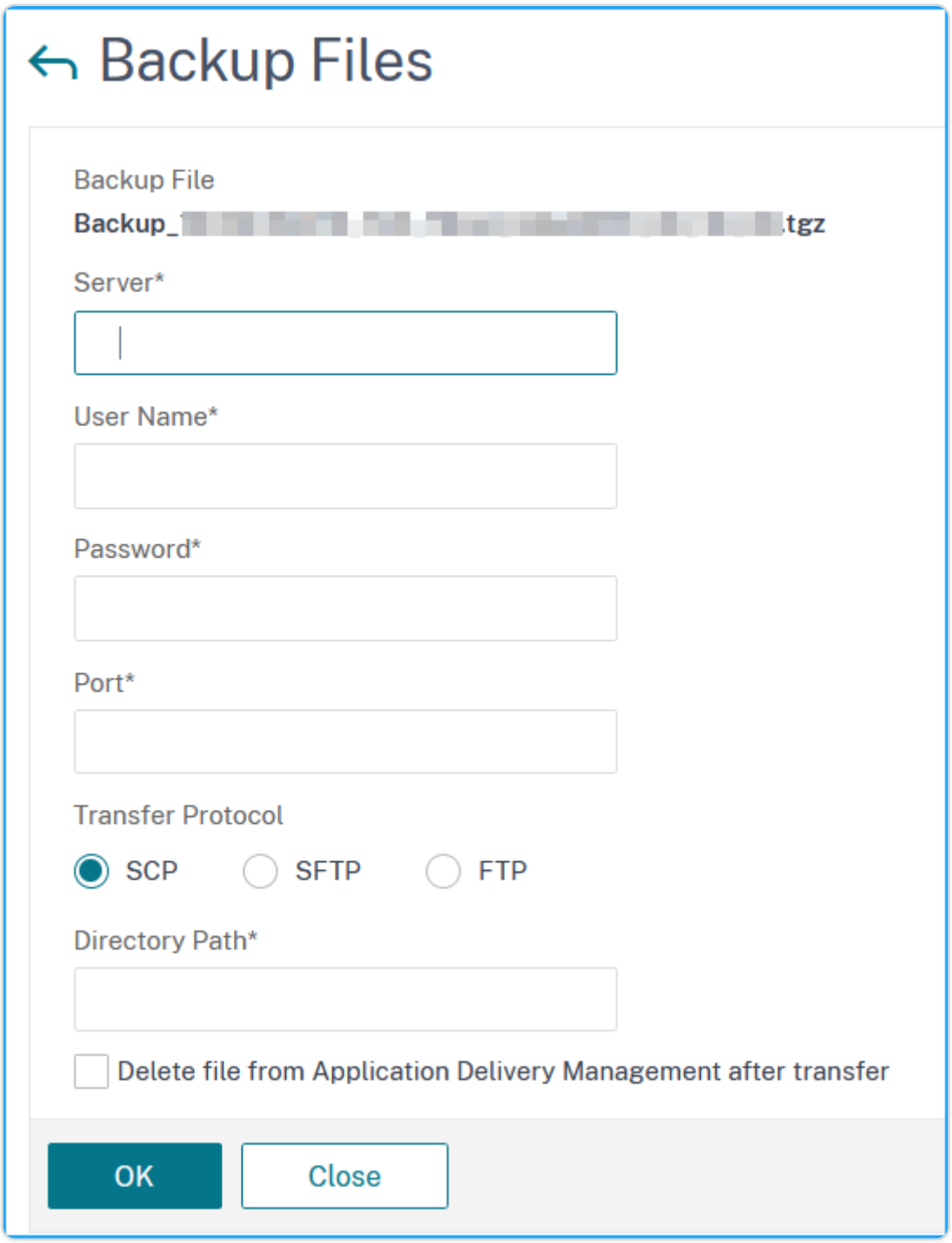
To transfer a NetScaler ADM backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to move to another system, and then click **Transfer**.
3. On the **Backup Files** page, specify the following parameters:
   - **Server** - IP address of the system where you want to transfer the backed-up file.
   - **User Name and Password** - User credentials of the new system where the backed-up files are being copied.
   - **Port** - Port number of the system the files are being transferred to.
   - **Transfer Protocol** - Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the backed-up file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Directory Path** - The location where the backed-up file is being transferred to on the new system.

4. You can delete the backup file from NetScaler ADM after transfer by selecting the **Delete file from Application Delivery Management after transfer** check box.
5. Click **OK** to make the transfer.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

To save a copy of the backup file in your local system, navigate to **Settings > Backup Files**, select the file you want to copy, and then click **Download**.

Restore the NetScaler ADM configuration from a backup file

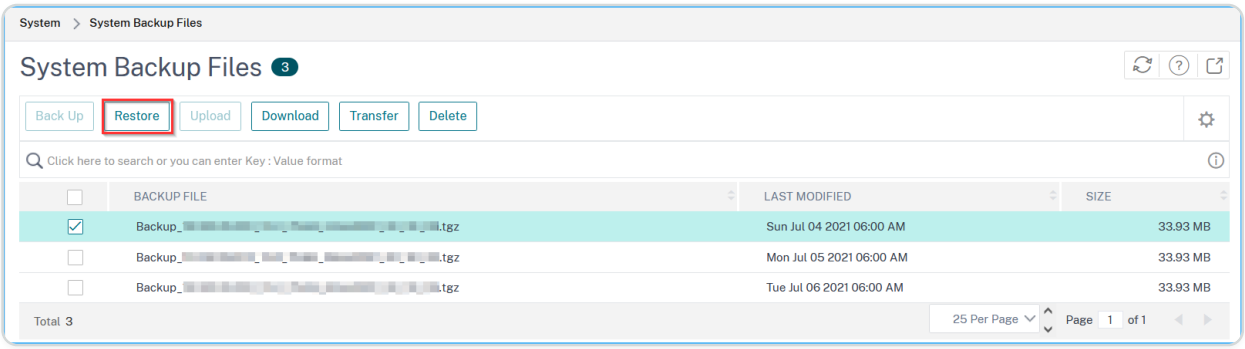
When you restore the NetScaler ADM configuration from a previously backed up file, the restore operation untars the backup file and then restores the configuration. The restore operation deletes the existing configuration and replaces it with the configuration in the backup file.

NOTE

The restore operation fails if the backup file is renamed or if the backup file contents are modified.

To restore a NetScaler ADM configuration from a backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to restore, and then click **Restore**.



3. On the confirmation dialog box, click **Yes**.

NOTE

To restore the configuration from a backup file stored in an external system, upload the backup file to the ADM server before performing the restore operation. To upload the file, navigate to **Settings > Backup Files**, and then click **Upload**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VM snapshots of NetScaler® ADM in high availability deployment

You can take snapshots of NetScaler ADM servers in the HA deployment before starting your upgrade. Snapshots capture the entire state of the virtual machine at the time that you take them.

Take a snapshot of NetScaler ADM servers

Use the following sequence to take snapshots of the NetScaler ADM servers:

1. NetScaler ADM secondary server
2. NetScaler ADM primary server

To take a snapshot of NetScaler ADM servers:

1. On your hypervisor, select the NetScaler ADM secondary server from the list of virtual machines.
2. Take a VM snapshot.
3. Give the snapshot a meaningful name and enter a description, if needed.

   The snapshot is stored in the default VM directory.
4. Repeat the same steps for the primary server.

NOTE:

You don't have to power off the VM while taking a snapshot.

Restore a snapshot of NetScaler ADM servers

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot.

Use the following sequence to restore snapshots of the NetScaler ADM servers:

1. NetScaler ADM primary server
2. NetScaler ADM secondary server

To restore the snapshot of NetScaler ADM servers:

1. On your hypervisor, select the NetScaler ADM primary server from the list of virtual machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Right-click the VM and revert the snapshot.

   The virtual machine is reverted to the most recent snapshot.

3. Repeat the same steps for the NetScaler ADM secondary server.

View auditing information

Audit logs have records with certain information for a specific duration such as user details, operations, and actions performed. You can view syslog messages for the following example scenarios:

- If your NetScaler® ADM is a HA pair and if there is any latency issue in the database replication between the primary and secondary nodes, you can view details as an event.
- If there are any invalid login attempts (user name or password error) or successful logins, you can view details as an event.

As an administrator, you can use these logs for maintaining security and for recovering lost transactions.

To configure a syslog server on NetScaler ADM:

1. Navigate to **Settings > ADM Audit log messages > Syslog Servers**.
2. In the **Syslog Server** page, click **Add**.
3. On the **Create Syslog Server** page, enter the following values:
   - **Name** - Name for the syslog server.
   - **IP Address** - IP address of the syslog server.
   - **Port** - Syslog server port.
4. Choose the log levels (All, None, or Custom).
5. Click **Create**.

To configure the syslog date and time format on NetScaler ADM:

1. Navigate to **Settings > ADM Audit log messages > Syslog Servers**.
2. In the **Syslog Server** page, select a syslog server, and then, click **Syslog Parameters**.
3. On the **Configure Syslog Parameters** page, specify the date and time format.
4. Click **OK**.

To view syslog messages on NetScaler ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Navigate to **Settings > ADM Audit log messages**.

You can also apply filters from the following filters and view the system log messages:

- Event
- Message
- Module
- Severity
- Source

For more information, see Syslog message references.

Configure SSL settings

SSL (Secure Socket layer) and TLS (Transport Layer Security) are commonly used security networking protocols that provide encrypted communication between users and servers. You can configure SSL settings on NetScaler® Application Delivery Management (ADM) and specify the type of clients that connect to the system.

To configure SSL settings for NetScaler ADM:

1. Navigate to **System** \> **System Administration**. Under **System Settings**, click **Configure SSL Settings**.
2. On the **SSL Settings** page, review the current protocol settings and the cipher suites applied to the system.
3. To modify the protocol settings, navigate to **Edit Settings** \> **Protocol Settings** and make the changes that you want.
4. To modify the applied cipher suites, navigate to **Edit Settings** \> **Cipher Suites** and make the changes that you want.
5. Click **OK**, and then click **Close**.

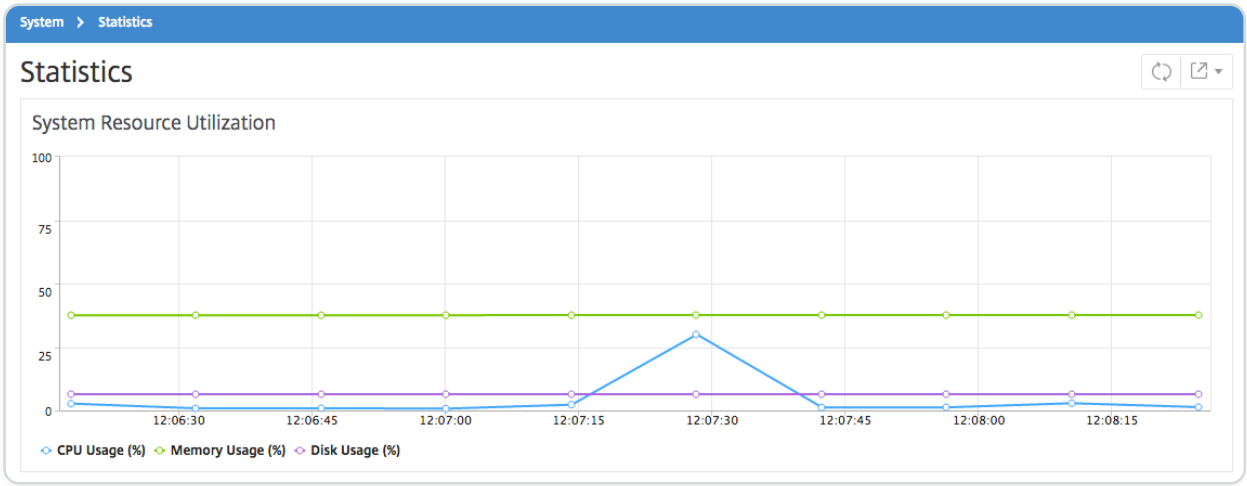
Monitor CPU, memory, and disk usage

You can use the information maintained in logs and statistics. This information is also displayed in reports that helps you to configure and maintain NetScaler® Application Delivery Management (ADM).

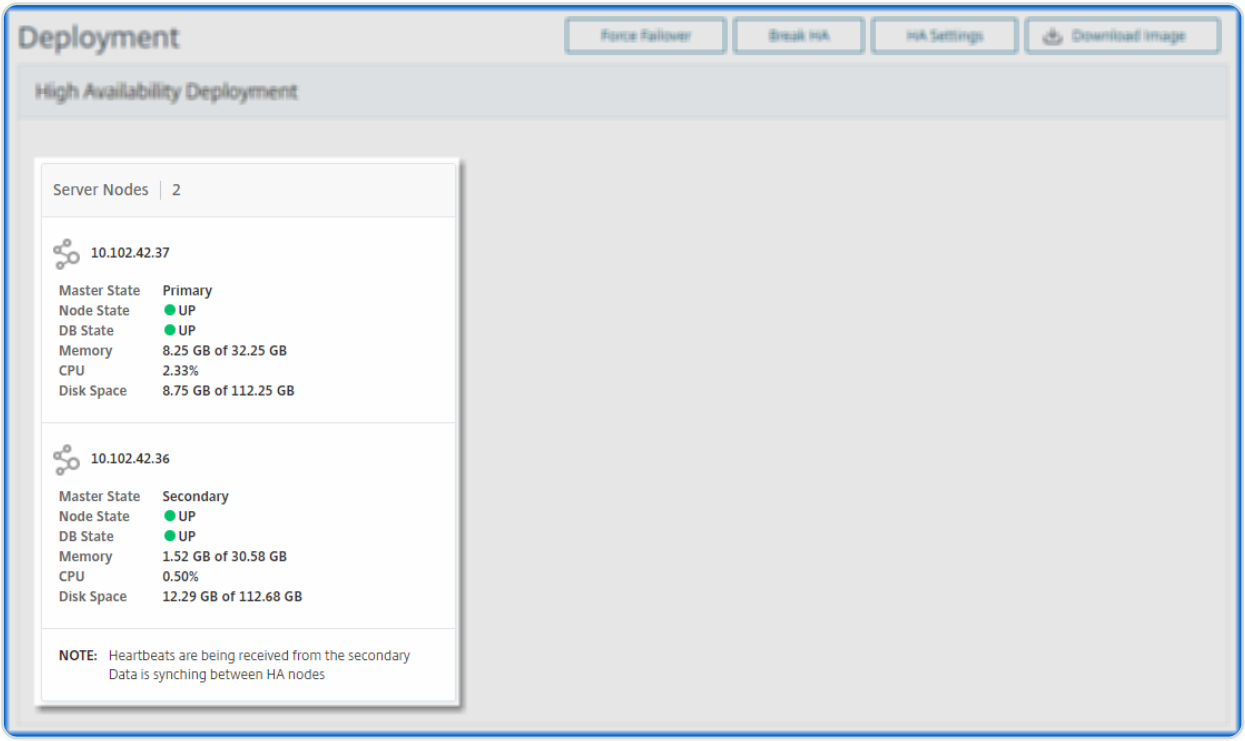
To monitor CPU, memory, and disk usage,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Standalone deployment.** Navigate to **System** \> **Statistics**. You can view real-time CPU, memory, and disk utilization charts.



- **High availability deployment.** Navigate to **Settings > Deployment**. The statistics for memory, CPU, disk space, and managed instances are displayed numerically as shown in the following figure:



Configure notification settings

You can select a notification type to receive notifications for the following features:

- **Events** – List of events that are generated for NetScaler instances. For more information, see Add event rule actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Licenses** – List of licenses that are currently active, about to expire, and so on. For more information, see The NetScaler ADM license expiry.
- **SSL Certificates** – List of SSL certificates that are added to NetScaler instances. For more information, see The SSL certificate expiry

ADM supports the following notification types:

- Email
- SMS
- Slack
- PagerDuty
- ServiceNow

For each notification type, the ADM GUI displays the configured distribution list or profile. The ADM sends notifications to the selected distribution list or profile.

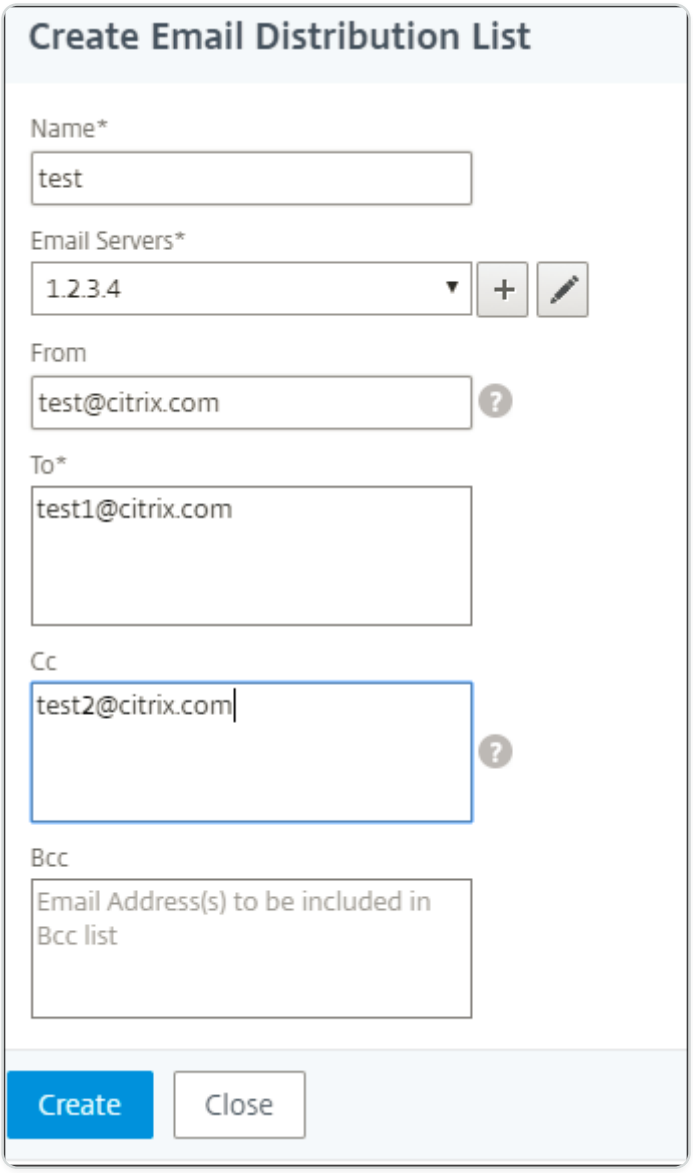
Create an email distribution list

To receive email notifications for ADM functions, you must add an email server and a distribution list.

Perform the following steps to create an email distribution list:

1. Navigate to **Settings > Notifications**.
2. In **Email**, click **Add**.
3. In **Create Email Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **Email Server** - Select the email server that sends email notification. If you want to add an email server, click **Add**.
    - **From** - Specify the email address from which ADM has to send messages.
    - **To** - Specify the email addresses to which ADM has to send messages.
    - **Cc** - Specify the email addresses to which ADM has to send message copies.
    - **Bcc** - Specify the email addresses to which ADM has to send message copies without displaying the addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Create**.

Repeat this procedure to create multiple email distribution lists. The **Email** tab displays all the email distribution lists present in ADM.

Create an SMS distribution list

To receive SMS notifications for ADM functions, you must add an SMS server and phone numbers.

Perform the following steps to configure SMS notification settings:

1. Navigate to **Settings > Notifications**.
2. In **SMS**, click **Add**.
3. In **Create SMS Distribution List**, specify the following details:
   - **Name** - Specify the distribution list name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SMS Server** - Select the SMS server that sends SMS notification.
- **To** - Specify the phone number to which ADM has to send messages.

4. Click **Create**.

Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in ADM.

Create a Slack profile

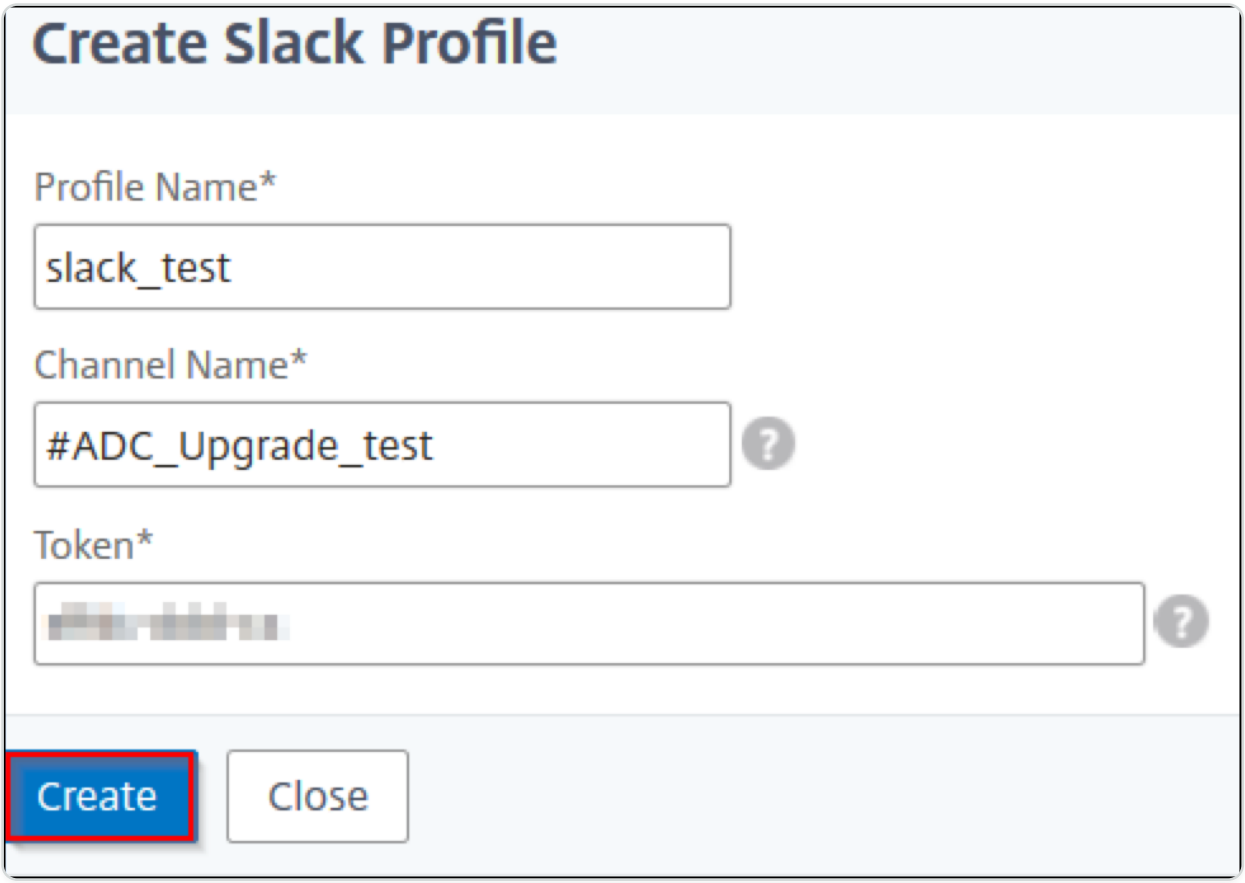
To receive Slack notifications for ADM functions, you must create a slack profile.

Perform the following steps to create a Slack profile:

1. Navigate to **Settings > Notifications**.
2. In **Slack**, click **Add**.
3. In **Create Slack Profile**, specify the following details:

   - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
   - **Channel Name** - Specify the Slack channel name to which ADM has to send notifications.
   - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. And, all event notifications are sent to this URL are posted on the designated Slack channel. An example of webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in ADM.

Create a PagerDuty profile

You can add a PagerDuty profile to monitor the incident notifications based on the PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in NetScaler ADM, ensure you have completed the required configurations in PagerDuty. To get started with PagerDuty, see PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. Navigate to **Settings > Notifications**.
2. In **PagerDuty**, click **Add**.
3. In **Create PagerDuty Profile**, specify the following details:
    - **Profile Name** - Specify a profile name of your choice.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal. When creating a service in PagerDuty for integration, use the **Generic Events API Integration** option.

4. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

Repeat this procedure to create multiple PagerDuty profiles. The **PagerDuty** tab displays all the PagerDuty profiles present in ADM.

View the ServiceNow profile

When you want to enable ServiceNow notifications for NetScaler events and ADM events, you must integrate NetScaler ADM with the ServiceNow using ITSM connector. For more information, see Integrate NetScaler ADM with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. Navigate to **Settings > Notifications**.
2. In **ServiceNow**, select the **Citrix_Workspace_SN** profile from the list.
3. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   If you want to view ServiceNow tickets in the NetScaler® ADM GUI, select **ServiceNow Tickets**.

Generate a tech support file

Citrix recommends that you generate an archive of NetScaler® Application Delivery Management (ADM) data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

NOTE

For NetScaler ADM servers in a high availability mode, you can generate a technical support file from either of the servers. Citrix advises you to not use the load balancing virtual server IP address to generate the technical support file.

To configure and send a technical support file from NetScaler ADM:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **System** \> **Diagnostics** \> **Technical Support**, and then click **Generate Technical Support File**.
2. On the **Generate Support File** page, select the following options:

- **Collect Debug Logs** – Select this option to collect `afdecoder` logs.
- **Duration** – Enter the duration for which debug logs must be collected. You will only see this option, if you enable the **Collect Debug Logs** option.
- **Collect Data Distribution** – Select this option to collect distinct and diverse logs from the database.

```
 The archive file is created as a TAR file.



 For example, the archive file that is created might be named as
follows:
Citrix_ADM_&lt;ADM_IP_address>_&lt;DDMMYY>_&lt;time_stamp>.tar.gz
```

1. You can send the technical support files to the support team in two ways:

   a. You can download the file from the ADM GUI to your local storage and then use a web browser to upload to Citrix Insight Services(CIS).

   b. You can also upload the technical support files to the CIS website by running a script on the ADM console.

      i. Using SSH, log on to the ADM console.

      ii. Switch to the Shell prompt and type:

      /mps/collector_upload.pl

The full command is given below with the attributes you need to provide:

```
/mps/collector_upload.pl [-proxy
[<proxy_user>:<proxy_password>@]<proxy_host>:<proxy_port>] [-user <user>]
[-password <password>] [-sr <sr>] [-description <description>] [-debug]
<file>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The advantage of running the Perl script is that you don't have to download the technical support file from ADM to your local system and then upload it to CIS. As an option, you can upload the file to CIS directly by using a proxy from the ADM console.

Ensure that you have an account on CIS. You can use your Citrix account credentials to upload files to CIS.

What if you don’t have a proxy server? Or what if you are facing some issues with SSL forward proxies? (This can happen if the Perl script does not trust the proxy server’s root certificate.) You can still upload the file directly from the ADM shell to CIS.

NOTE

You can still download the file and email them to the Citrix technical support team in a situation where ADM fails to upload the file to CIS from the console. Or, you can download the file from ADM to your local storage and then use a web browser to upload to CIS.

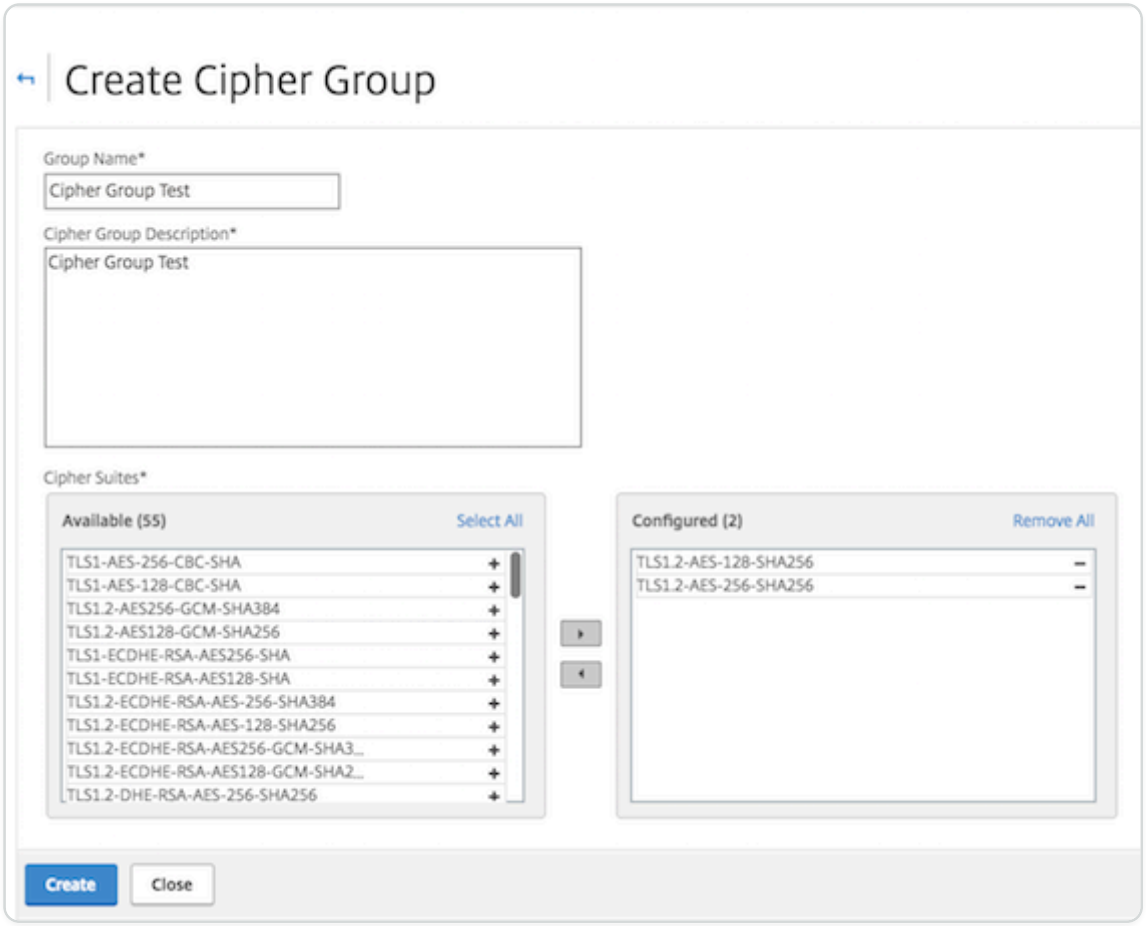
Configure a cipher group

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the Citrix Application Delivery Controller (ADC) instance. A cipher suite comprises a protocol, a key exchange (`Kx`) algorithm, an authentication (`Au`) algorithm, an encryption (`Enc`) algorithm, and a message authentication code (`Mac`) algorithm.

To add a cipher group on NetScaler® ADM:

1. Navigate to **Settings > Administration**
2. Under **SSL Settings**, click **Cipher Groups**
3. Click **Add**
4. On the **Create Cipher Group** page, enter the following details:
   - **Group Name** - Name for the cipher group.
   - **Cipher Group Description** – Provide a description for your cipher group.
   - **Cipher Suites** – Click Add to select cipher suites from the Available list, and then move the selected (or all) cipher suites to the Configured list.
5. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create SNMP trap destination, manager community, and users

Whenever an abnormal condition occurs on the NetScaler® ADM, an SNMP trap is generated. The traps are then sent to a remote device called a trap destination server or the *SNMP trap destination*. Here, NetScaler ADM is configured as the trap destination. You can query the SNMP agent for system-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

To create an SNMP trap destination on NetScaler ADM:

1. Navigate to **System** \> **SNMP** \> **Trap Destinations**.
2. Under **SNMP Traps**, click **Add** to create an SNMP trap, and then specify the following details:
    - **Version.** Select the SNMP version to use.
    - **Destination Server.** Name or IP address of the trap destination.
    - **Port.** Enter the trap destination's port. The port is set to 162 by default.
    - **Community.** Specify the community string to use when sending a trap to the trap listener.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

You can enable and configure a set of Alarms to monitor the health of your NetScaler® Application Delivery Management (ADM) servers. You must configure system alarms to make sure you are aware of any critical or major system issues. For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, **loginFailure**), a message is recorded in the system and you can view the message as syslog message. You can further set notifications to receive an email or SMS corresponding to your alarm settings.

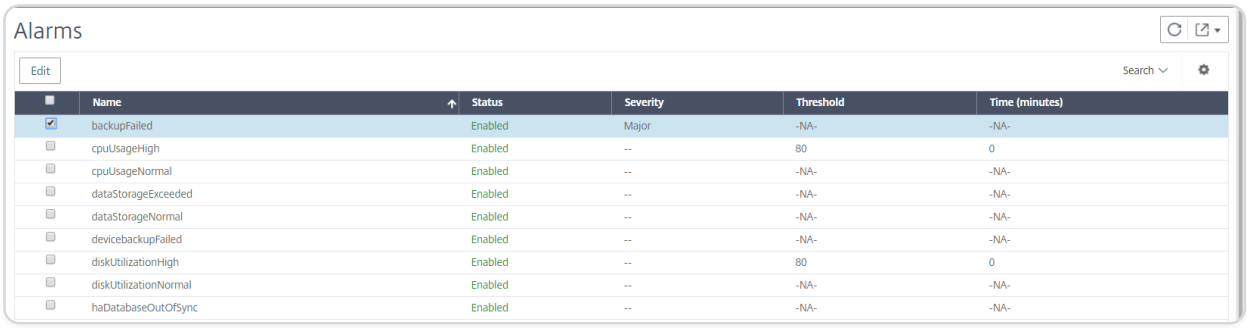
You can assign or modify the severity of an alarm. The severity levels that you can assign are Critical, Major, Minor, Warning, and Informational.

Consider a scenario where you want to monitor whenever there is a failed back up attempt. You can enable the backupFailed alarm and assign a severity, such as Major, to it. Whenever NetScaler ADM attempts to back up the system files and when the attempt fails, an alarm is triggered. You can view the message on the NetScaler ADM or get notifications through email or SMS.

To configure the alarm, you must select the backupFailed alarm and specify the severity level as Major. The alarm is enabled by default.

To configure and view a system alarm by using NetScaler ADM:

1. Navigate to **Settings > SNMP**. Click **Alarms** on the upper-right corner.



Name	Status	Severity	Threshold	Time (minutes)
backupFailed	Enabled	Major	-NA-	-NA-
cpuUsageHigh	Enabled	--	80	0
cpuUsageNormal	Enabled	--	-NA-	-NA-
dataStorageExceeded	Enabled	--	-NA-	-NA-
dataStorageNormal	Enabled	--	-NA-	-NA-
devicebackupFailed	Enabled	--	-NA-	-NA-
diskUtilizationHigh	Enabled	--	80	0
diskUtilizationNormal	Enabled	--	-NA-	-NA-
haDatabaseOutOfSync	Enabled	--	-NA-	-NA-

2. Select the alarm you want to configure (for example, backupFailed) and click **Edit** to modify its settings.
3. The alarm is enabled by default. Assign a severity level (example: Major), and then click **OK**.

NOTE

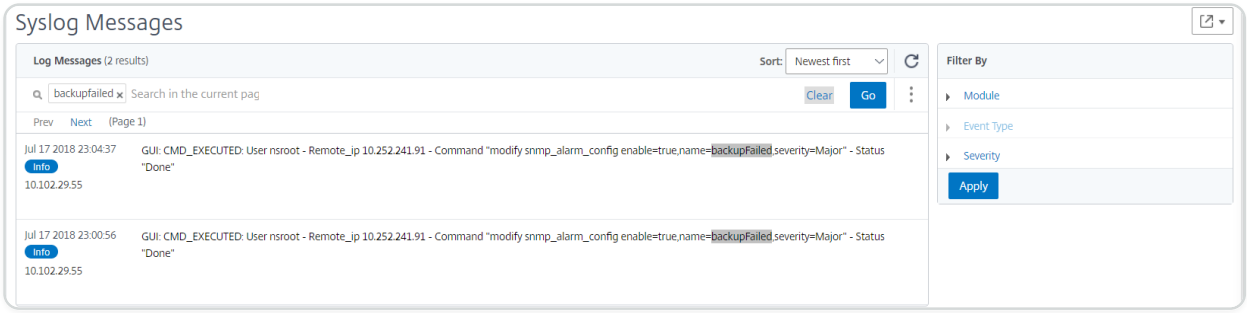
For a few alarms, you cannot set a threshold. When the alarm is triggered, you can view the generated event as a syslog message.

To view the event generated by the backupFailed alarm by using NetScaler ADM:

1. Navigate to **System** > **Auditing**.
2. In the **Auditing** page, under **Audit Messages**, select **Syslog Messages**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the search field, type in the name of the alarm.In this example, you can see that an event was generated for a failed back up attempt.



You can also set notifications to send you either an email or an SMS (Short Message Service) text when an alarm is triggered. For information about how to configure system notifications, see How to Configure System Notification Settings of NetScaler ADM.

Create SNMP managers and users for NetScaler agent

You can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

You can add an SNMP manager to query a NetScaler agent. The manager complies with SNMP V2 and V3. If you specify one or more SNMP managers, the NetScaler agent does not accept SNMP queries from any hosts except the specified SNMP managers.

Add an SNMP v2 manager

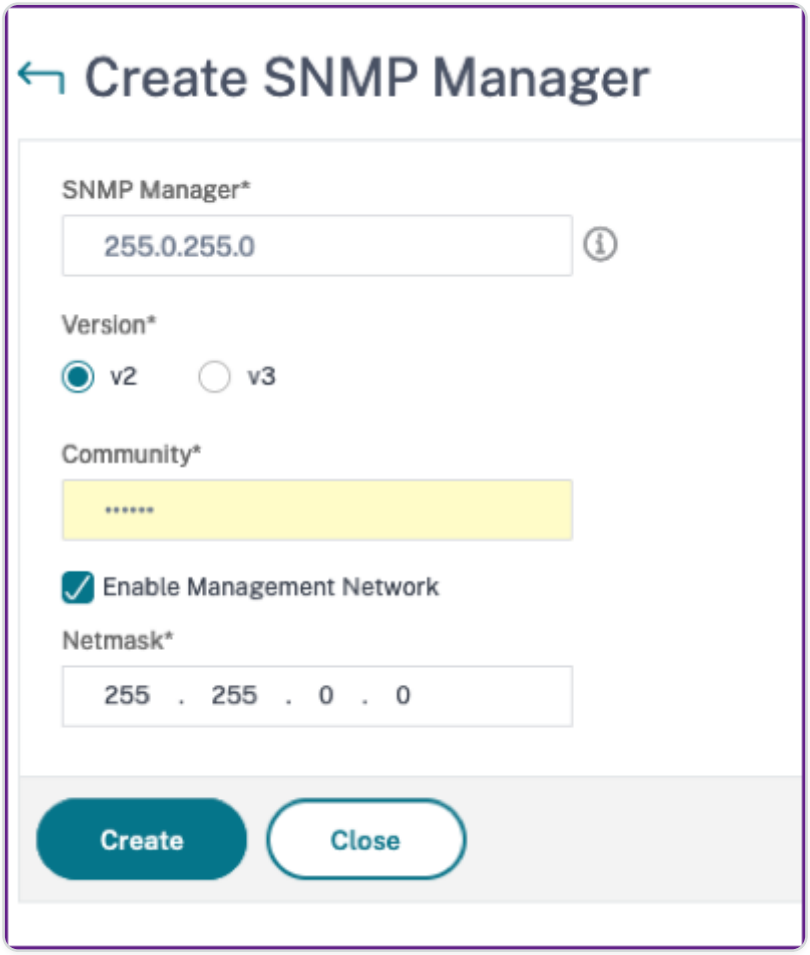
To add an SNMP v2 manager for the NetScaler agent:

1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
   - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
   - **Version**. Select v2.
   - **Community**. Enter a community name. An SNMP community configuration authenticates SNMP queries from SNMP managers.
   - **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Netmask**: Enter the subnet mask associated with an IP address.

4. Click **Create**.



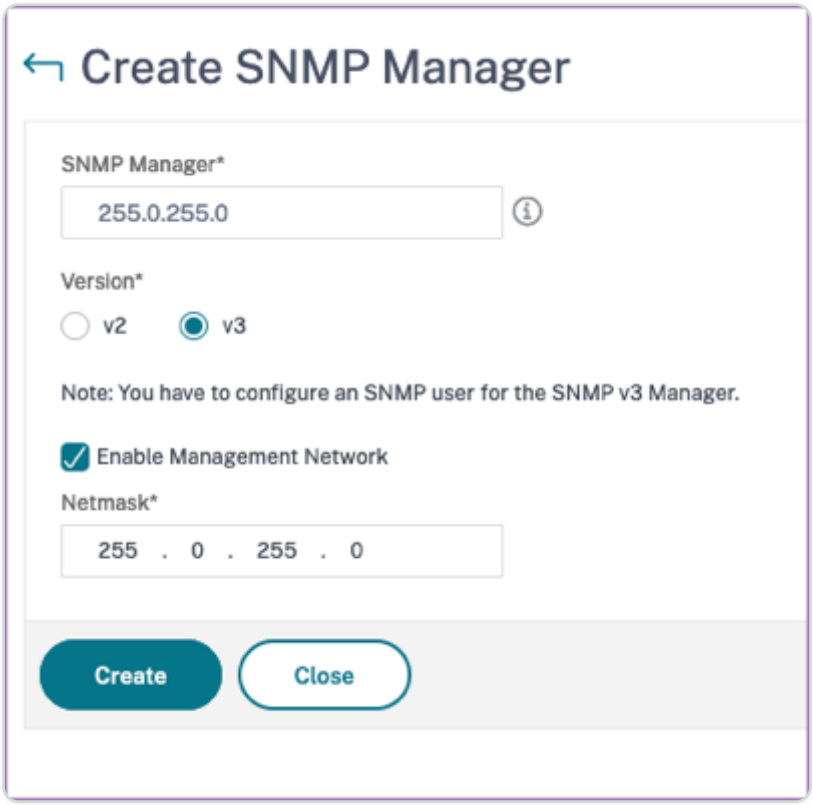
Add an SNMP v3 manager

To add an SNMP v3 Manager for the NetScaler agent:

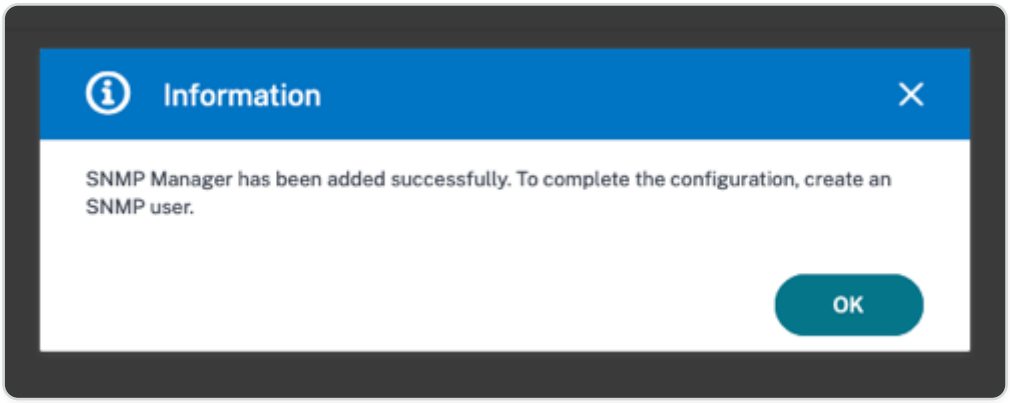
1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
   - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
   - **Version**. Select v3.
   - **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.
   - **Netmask**: Enter the subnet mask associated with an IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Create**.



A dialog box appears confirming that an SNMP manager is created and prompting you to configure an SNMP user.



NOTE

You must configure an SNMP user for an SNMP v3 manager. To configure the SNMP user, go to **SNMP > SNMP User**.

Add an SNMP user

Add an SNMP user to respond to the SNMP v3 queries from an SNMP manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

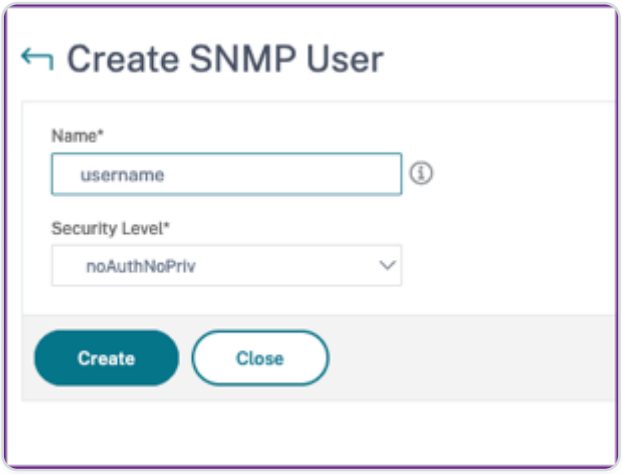
To add an SNMP user for the NetScaler agent:

1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP User** tab, click **Add**.
3. In the **Create SNMP User** page, add the following details:

   - **Name**. Enter the user name.
   - **Security Level**. Security level required for communication between the NetScaler agent and the SNMP manager.

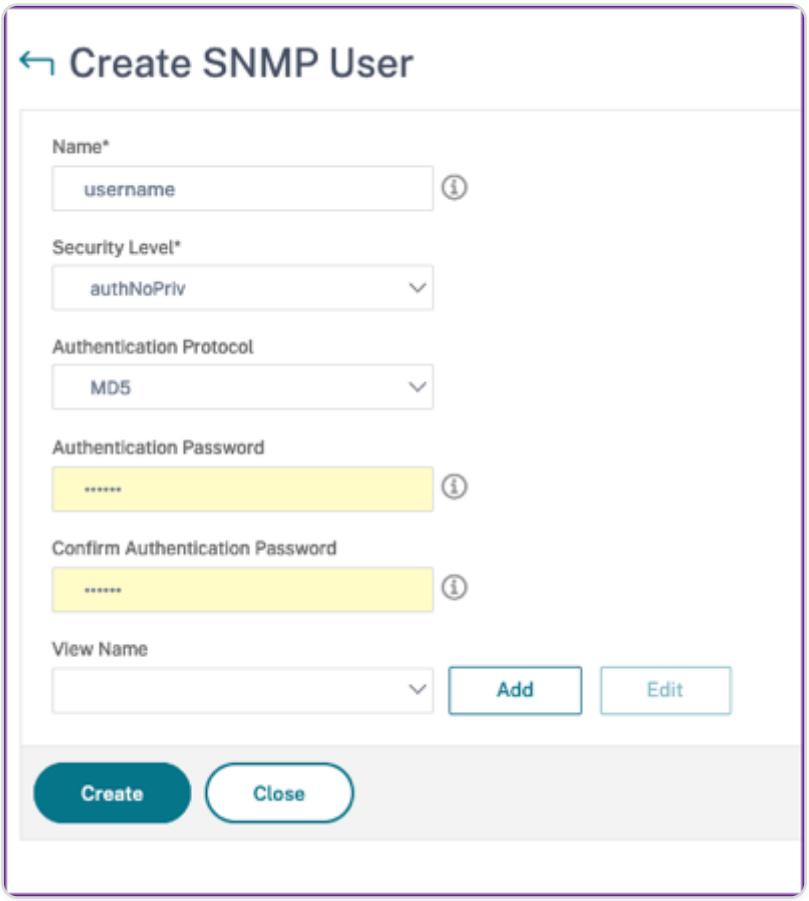
     Select one of the following security levels:

   - **noAuthNoPriv**. Require neither authentication nor encryption.



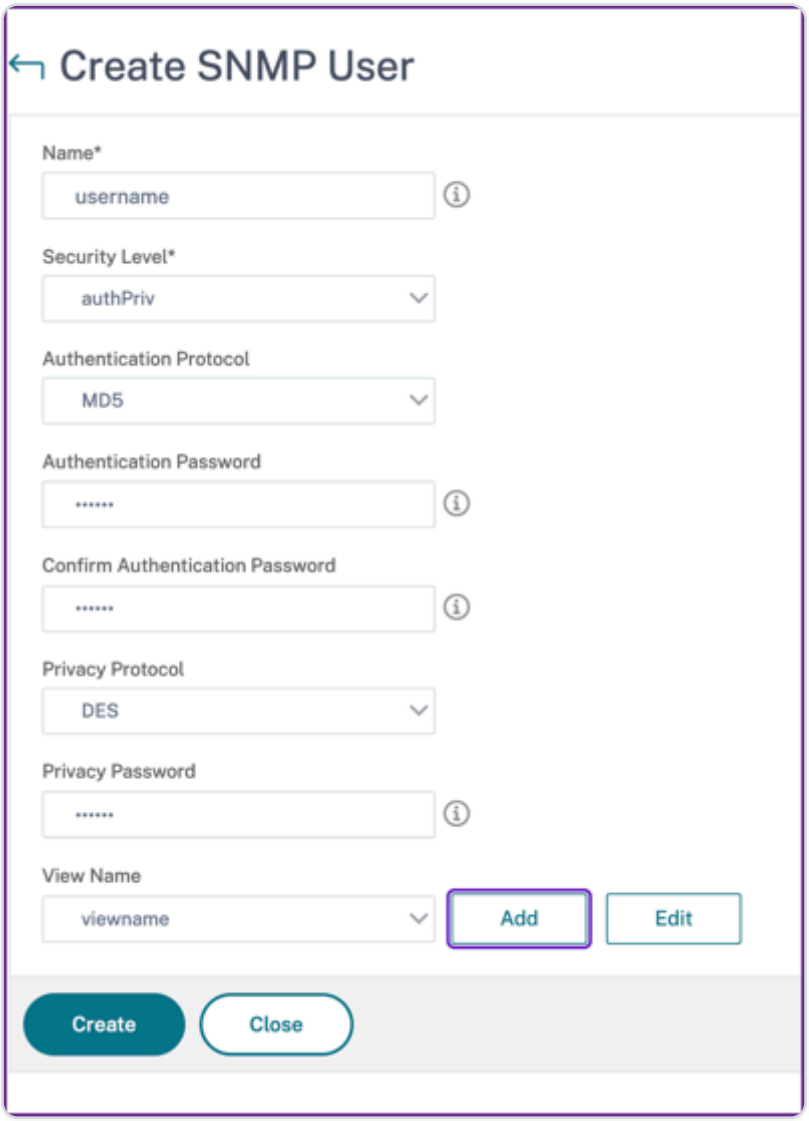
   - **authNoPriv**. Require authentication but no encryption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **authPriv**. Require authentication and encryption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Based on the security level you've assigned to the user, provide extra authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.

Managing SNMP views

SNMP views are used to implement access control for an SNMP user. The SNMP views restrict the user access to specific portions of MIB.

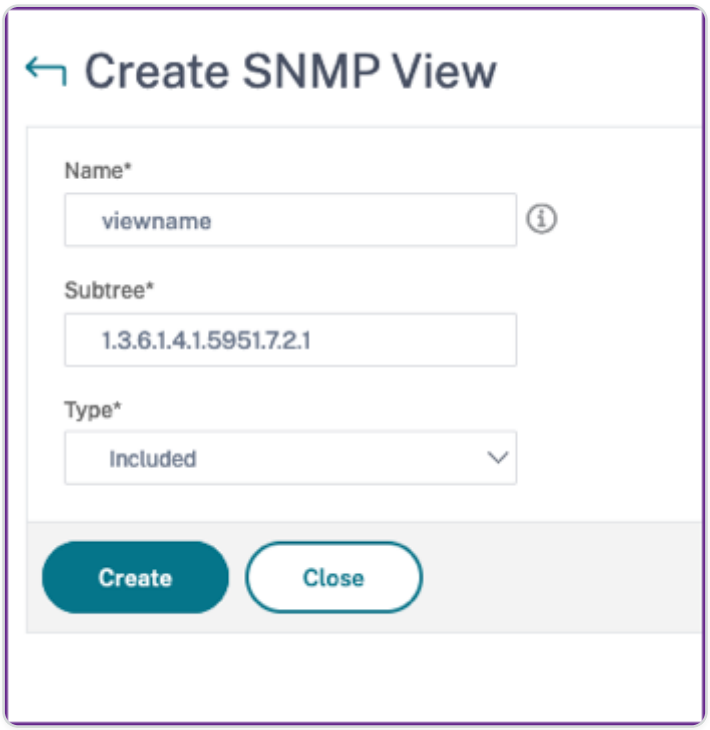
To allow or restrict an SNMP OID for the NetScaler agent:

1. Navigate to **Infrastructure > Agents > Manage SNMP** and in the **SNMP View** tab, click **Add**.
2. In the **Create SNMP View**, enter the following details:
   - **View Name**: A name for the SNMP view. An instance can have many SNMP views with the same name, differentiated by the subtree parameter settings.
   - **Subtree**: A particular branch (subtree) of the MIB tree that you want to associate with this SNMP view. You must specify the subtree as an SNMP OID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Type**: This field allows you to include or exclude subtrees from a view.

3. Click **Create**.



Configure agent settings

You can modify the NetScaler® ADM agent's keep-alive interval and password change requirements.

Set agent's keep-alive interval

NetScaler ADM server and agent maintain the same TCP connection for the specified keep-alive interval. An agent uses this connection to send the managed instances data to the NetScaler ADM server.

1. Navigate to **Settings > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.
3. In **Basic Settings > Agent Settings**, specify the keep-alive interval between 30–120 seconds.
4. Click **Save**.

Change agent's password without the current password

You can allow agent passwords to be changed without their current password.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.
3. In **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change** check box, you can do the following:
   - Select the check box to remove the **Current password** field in the **Change Agent Password** page.
   - Clear the check box to keep the **Current password** field in the **Change Agent Password** page.
4. Click **Save**.

NOTE

To view the **Change Agent Password** page, navigate to **Infrastructure > Instances > Agents**, select an agent, and click **Select Action > Change Password**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® ADM as an API proxy server

In addition to being able to receive NITRO REST API requests for its own management and analytics functionality, NetScaler Application Delivery Management (NetScaler ADM) can function as a REST API proxy server for its managed instances. Instead of sending API requests directly to the managed instances, REST API clients can send the API requests to NetScaler ADM. NetScaler ADM can differentiate between the API requests to which it must respond and the API requests that it must forward unchanged to a managed instance.

As an API proxy server, NetScaler ADM provides you with the following benefits:

- **Validation of API requests**. NetScaler ADM validates all API requests against configured security and role-based access control (RBAC) policies. NetScaler ADM is also tenant-aware and ensures that API activity does not cross tenant boundaries.
- **Centralized auditing**. NetScaler ADM maintains an audit log of all API activity related to its managed instances.
- **Session management**. NetScaler ADM frees API clients from the task of having to maintain sessions with managed instances.

How NetScaler ADM Works as an API Proxy Server

When you want NetScaler ADM to forward a request to a managed instance, you configure the API client to include any one of the following HTTP headers in the API request:

HEADER VALUES	DESCRIPTION
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Name of the managed instance.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	IP address of the managed instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HEADER VALUES	DESCRIPTION
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID of the managed instance.
_MPS_API_PROXY_TIMEOUT	Timeout value for a NITRO API request. Set the timeout value in seconds. When you set a proxy timeout, ADM waits for the specified duration before it times out the request.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	User name to access the managed ADC instance.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Password to access the managed ADC instance.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Session ID to access the managed instance.

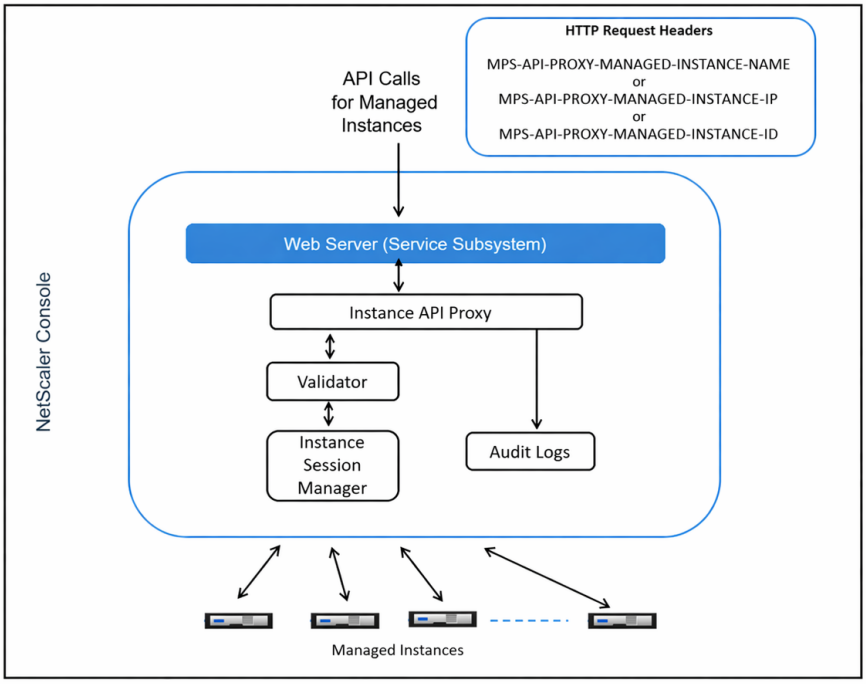
NOTE

In **Settings > Administration >** System Configurations **> Basic Settings**, if you select **Prompt Credentials for Instance Login**, ensure to configure user name and password of a managed instance. Alternatively, you can also specify the instance session ID.

The presence of any of these HTTP headers helps NetScaler ADM identify an API request as one that it must forward to a managed instance. The value of the header helps NetScaler ADM identify the managed instance to which it must forward the request.

This flow is depicted in the following figure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



As shown in the above figure, when one of these HTTP headers appears in a request, NetScaler ADM processes the request as follows:

1. Without modifying the request, NetScaler ADM forwards the request to the instance API proxy engine.
2. The instance API proxy engine forwards the API request to a validator and logs the details of the API request in the audit log.
3. The validator ensures that the request does not violate configured security policies, RBAC policies, tenancy boundaries, and so on. It performs extra checks, such as a check to determine whether the managed instance is available.

If the API request is valid and can be forwarded to the managed instance, NetScaler ADM identifies a session that is maintained by the instance Session Manager and then sends the request to the managed instance.

NOTE

Ensure the **Prompt Credentials for Instance Login** option is disabled. To do so:

1. Navigate to **Settings > Administration**.
2. In **System Configurations**, select **System, Time zone, Allowed URLs and Message of the day**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use NetScaler ADM as an API proxy server

The following examples show REST API requests that an API client sends to a NetScaler ADM server that has an IP address of 192.0.2.5. NetScaler ADM is required to forward the requests, unchanged, to a managed instance with IP address 192.0.2.10. All examples use the _MPS_API_PROXY_MANAGED_INSTANCE_IP header.

Before sending NetScaler ADM the API requests, the API client must:

- Log in to NetScaler ADM
- Obtain a session ID
- Include the session ID in subsequent API requests.

The logon API request is of the following form:

```
POST /nitro/v1/config/login

Content-Type: application/json



{

    "login": {

        "username":"nsroot",

        "password":"nsroot"

     }

}
```

NetScaler ADM responds to the logon request with a response that includes the session ID. The following sample response body shows a session ID:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {

      "tenant_name": "Owner",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "permission": "superuser",

        "session_timeout": "36000",

        "challenge_token": "",

        "username": "",

        "login_type": "",

        "challenge": "",

        "client_ip": "",

        "client_port": "-1",

        "cert_verified": "false",

        "sessionid":
"##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",

        "token": "b2f3f935e93db6a"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }


  ]


}
```

Example 1: Retrieve load balancing virtual server statistics

The client must send NetScaler ADM an API request of the following form:

```
GET /nitro/v1/stat/lbvserver

Content-type: application/json

_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Where the value of the Cookie Header is the Session ID returned from the login API call. And the value of the _MPS_API_PROXY_MANAGED_INSTANCE_IP is the IP address of the ADC.

Example 2: Create a load balancing virtual server

The client must send NetScaler ADM an API request of the following form:

```


    POST /nitro/v1/config/lbvserver/sample_lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Content-type: application/json

Accept-type: application/json

_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

     "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 NetScaler ADM an API request of the following form:

```
PUT /nitro/v1/config/lbvserver

Content-type: application/json

Accept-type: application/json

_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

   "lbvserver":{

        "name":"sample_lbvserver",

        "appflowlog":"DISABLED"

   }

}
```

Example 4: Delete a load balancing virtual server

The client must send NetScaler ADM an API request of the following form:

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver

Accept-type: application/json

_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Example 5: Download the CLI running config on the ADC

The client must send NetScaler ADM an API request of the following form:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
GET /nitro/v1/config/nsrunningconfig

Accept-type: application/json

_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs

This section provides the FAQ on the following NetScaler® Application Delivery Management (NetScaler ADM) features. Click a feature name in the following table to view the list of FAQs for that feature.

ANALYTICS	AUTHENTICATION	CONFIGURATION MANAGEMENT
Certificate Management	Deployment	Deployment (Disaster recovery)
Event Management	Instance Management	StyleBooks
System Management		

Analytics

Is it required to enable EUEM virtual channel on NetScaler Gateway instances deployed in single-hop mode?

EUEM virtual channel data is part of HDX™ Insight data that the NetScaler ADM receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If the EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler ADM.

The EUEM virtual channel is a default service running on Citrix Virtual Desktop applications (VDA). If it is not running, start the "Citrix End User Experience Monitoring" process in VDA services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How do I enable NetScaler ADM to monitor web-application and virtual-desktop traffic?

1. Navigate to **Infrastructure** \> **Instances** \> **NetScaler**, and select the NetScaler instance on which you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. In the **Configure Analytics** page, select all the virtual servers on which you want to enable analytics, and click **Enable AppFlow**. For more details, see How to Enable Analytics on Instances.

Note

> For NetScaler instances of 11.0 release, 65.30 build and later, there is no option on NetScaler ADM to enable Security Insight explicitly. Ensure that you configure the AppFlow parameters on the NetScaler instances, so that NetScaler ADM starts receiving the Security Insight traffic along with the Web Insight traffic. For more information on how to set the AppFlow parameters on NetScaler instances, see To set the AppFlow parameters by using the configuration utility.

After I add the NetScaler instances, does NetScaler ADM automatically start collecting analytical information?

No. Enable analytics on the virtual servers hosted in NetScaler instances that are managed by NetScaler ADM. For more details, see How to Enable Analytics on Instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Is it required to access the individual NetScaler appliance for enabling analytics?

No. All configurations are done from the NetScaler ADM user interface, which lists the virtual servers hosted on the specific NetScaler instance. For more details, see How to Enable Analytics on Instances.

What are the types of virtual servers that can be listed on a NetScaler instance to enable analytics?

Currently, the NetScaler ADM user interface lists the following virtual servers for enabling analytics:

- Load balancing virtual server
- Content switching virtual server
- VPN virtual server
- Cache redirection virtual server

How do I attach an extra disk to the NetScaler ADM?

To attach an extra disk to NetScaler ADM:

1. Shut down the NetScaler ADM virtual machine.
2. In the hypervisor, attach an extra disk of the required disk size to the NetScaler ADM virtual machine.

   For example, Let us consider that you want to increase the disk space to 200 GB, in a NetScaler ADM virtual machine of 120 GB. In this scenario, you must attach a disk space of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, NetScaler ADM log files. The existing 120 GB disk space is used to store core files, Operating System Log files, and so on.

3. Start the NetScaler ADM virtual machine.

What do you mean by collectors are not configured on NetScaler instances?

A collector receives AppFlow records generated by the NetScaler appliance.

NetScaler ADM receives Security Insight and Web Insight traffic from the NetScaler instances when the AppFlow feature is enabled. When you enable the AppFlow feature on a NetScaler instance, you must specify at least one collector to which the AppFlow records are sent. If the collectors are not configured on the NetScaler instances, NetScaler ADM does not receive the traffic from the instances.

For example, five NetScaler instances are added to NetScaler ADM. If collectors are not specified for two instances, no traffic flows to NetScaler ADM. Self-service diagnostics detects the issue and displays the issue as "Collectors are not configured on 2 instances."

For more information about how to configure the AppFlow Feature, see Configuring the AppFlow Feature.

What does enabling client-side measurements do?

With client side measurements enabled, ADM captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication

What is load balancing of authentication requests?

The authentication-server load balancing feature enables NetScaler ADM to load balance the authentication requests that are directed to the external authentication servers. Load balancing the authentication servers ensures that the authentication load is split across multiple authentication servers and thus avoid an authentication server from being overloaded. You can create an authentication service to connect with and get user information from your existing external authentication server using the authentication protocols like LDAP, RADIUS, or TACACS.

Why do we need to cascade external authentication servers?

Cascaded external authentication servers provide uninterrupted authentication processing, allowing access to legitimate users if an authentication server fails. There is no limitation on which types of authentication servers you can cascade. You can have all RADIUS servers, or all LDAP servers, or a combination of RADIUS and LDAP servers.

How many external authentication servers can I cascade?

You can cascade up to 32 external authentication servers in NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Do I have an alternative when external authentication fails?

There can be a situation when external authentication completely fails, even when you have cascaded several servers. For example, the external servers can become unreachable, or a new user's credentials might not have been entered in any of the external authentication servers. To prevent locking users out in such a situation, you can enable fallback local authentication. For more details, see Fallback Local Authentication.

What is fallback local authentication?

Fallback local authentication is an option to authenticate your users locally when external authentication fails. If external authentication fails, NetScaler ADM accesses the local user database to authenticate your users.

In NetScaler ADM, navigate to **Settings > Authentication > Authentication Configuration**. On this page, you can add multiple external authentication servers in a cascade, and you can select the **Enable fallback local authentication** option.

What is an extraction of external user groups?

If you have added external servers for authenticating the users, you can import (extract) existing user groups into NetScaler ADM. You have to import user groups once and provide a group permission to a user group rather than importing individual users and giving them individual permissions. You do not have to recreate the users on NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Why do we need to assign group permissions?

When you are using the load balancing feature of NetScaler, you can integrate NetScaler ADM with external authentication servers, and import user group information from the authentication servers. Log in to NetScaler ADM and manually create the same group information in NetScaler ADM and assign permission to those groups. The user and user group permission is managed in NetScaler ADM and not in the external server. The users have different role-based access permissions on the external servers. Configure the same permissions for the users in NetScaler ADM also. Instead of configuring permissions individually for each user, you can configure a group-level permission so that the user-group members can access specific services on the load balanced virtual servers. The typical permissions that you can assign are permissions to manage NetScaler instances, NetScaler SDX instances, virtual servers, and so on, so that the users of that group can manage only those instances or virtual servers. You can later edit the permissions given to the users at the group level. You can even remove one or more user groups; other group users still function on NetScaler ADM.

Configuration Management

Can I perform configuration across multiple NetScaler instances simultaneously using NetScaler ADM?

Yes, you can use configuration jobs to perform configuration across multiple NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What are configuration jobs on NetScaler ADM?

A job is a set of configuration commands that you can create and run on one or more managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler ADM GUI. You can also convert the recorded tasks into CLI commands.

You can use the Configuration Jobs feature of NetScaler ADM to create a configuration job, send email notifications, and check execution logs of the jobs created.

Can I schedule jobs using built-in templates in NetScaler ADM?

Yes! You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can choose to run the job immediately, or schedule the job to be run later.

You can save the configuration of a job that was previously created, and run the job again after modifying the commands, the parameters, the configuration source, and targeted instances. This is useful when the same set of commands has to be run on a different instance, or when the job encounters an error and stops further execution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate Management

Does the deletion of SSL certificates from NetScaler ADM lead to the deletion of certificates from NetScaler instances?

No

Deployment

What is the default user name and password?

- After you complete the initial network configuration, you can log on to NetScaler ADM from the hypervisor or SSH console, using the default user name and password (nsrecover/nsroot).
- The default user name and password to log on from the GUI is *nsroot/nsroot*.

How to change the default password?

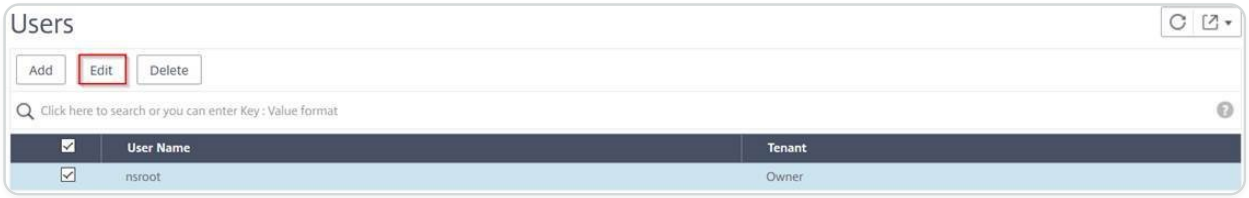
To change the password:

1. In NetScaler ADM, navigate to **Settings > User Administration > Users**.

   The **Users page** is displayed.

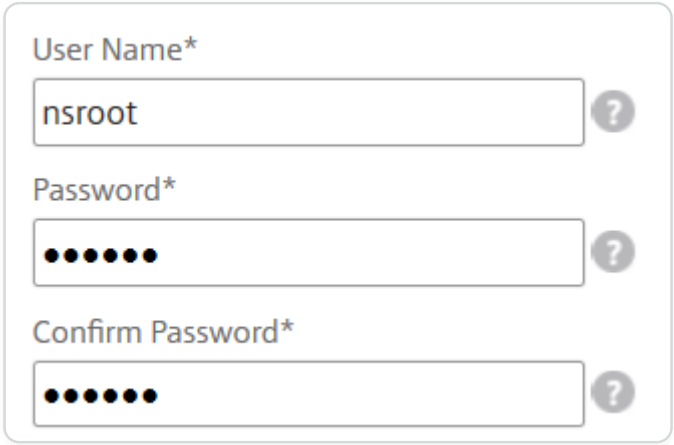
2. Select the user name **nsroot** and click **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Configure System User** page is displayed.

3. Select **Change Password** and create a password of your choice.



4. Click **OK**.

   You can now use the new password to log on from the GUI, hypervisor, or SSH console.

   Note

   > You cannot modify the user name.

How to reset the password?

You can see this documentation to reset the password.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In a HA pair, if the password is changed in the primary node and if the Break HA pair option is selected later, what is the behavior?

You can log on to both standalone nodes using your new password.

If two standalone servers have different passwords, what is the impact in deploying these two servers in HA pair?

It is recommended to have default password for both servers when you deploy two standalone servers to HA pair.

The HA configuration is complete, but the primary node GUI is not accessible. What can be the reason?

It takes a few minutes for the configuration to take effect. You can try accessing again after a few minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The HA configuration is complete, but the floating IP address GUI is not accessible. What can be the reason?

After the HA configuration, you need to first access the primary node GUI and complete the deployment. For more information, see Deploy the primary and secondary node as a high availability pair. After the deployment is complete, the server reboots and gets ready for high availability deployment. You can then access the floating IP address GUI.

What DB is supported in NetScaler ADM standalone and NetScaler ADM HA?

Both NetScaler ADM standalone and NetScaler ADM HA support PostgreSQL.

What is the potential data loss to the secondary node?

The secondary node listens to the heartbeat messages that the primary node sends through the NetScaler ADM database. If the secondary node does not receive the heartbeats for more than 180 seconds, then the secondary node performs an SSH-based check on the primary node. If the heartbeat and SSH-based check fail, the primary node is considered to be down.

In this scenario, the secondary node takes over as the primary node and the 180 seconds timeframe can be considered as the possible data loss to the secondary node.

What happens if the primary node is down?

The secondary node takes over and becomes the primary node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to reinstall the failed node?

It is recommended to install a fresh VM build. To reinstall:

1. Break the HA pair. Navigate to **Settings > Deployment**

   The deployment page is displayed. Click **Break HA**
2. Delete the failed node from the hypervisor.
3. Import the .XVA image file to the hypervisor.
4. From the Console tab, configure NetScaler ADM with the initial network configurations. For more information, see Register and deploy the first server (primary node) and Register and deploy the second server (secondary node).
5. Redeploy the HA pair.

Does NetScaler ADM support SAN Storage?

Citrix recommends you to host the NetScaler ADM VHD on a local storage. When hosted on storage devices in a SAN, NetScaler ADM might not work as expected. So, ADM deployment on SAN is not supported.

Does NetScaler ADM support an extra disk?

Yes. A new installation of NetScaler ADM HA pair allocates 120 GB of storage by default. For more than 120 GB storage, you can add one extra disk for a maximum of 3 TB storage. Adding more than one extra disk is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After disabling the HA pair, what happens to the floating IP address configured?

The floating IP address is no longer accessible and you need to redeploy the high availability pair.

Can I give a different floating IP address while redeploy?

Yes. You can configure a new floating IP address.

Why is secondary node GUI not accessible?

Secondary node is only a read-replica server and acts as a primary node only if the primary node is down for any reason. Citrix recommends accessing either the primary node GUI or the floating IP address GUI.

If the primary node is down for a long duration, can the configurations still be done using the floating IP address GUI?

Yes. You can still continue to do configurations and the configurations get saved in the secondary node. After the primary node is back, all the configurations are synchronized.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If there is a necessity to change the primary node IP address or secondary node IP address or floating IP address in the future (for example, changing it to IPv6), what are the recommended solutions to follow?

Changing the IP addresses in HA pair is not supported without breaking the HA pair.

To update the primary node or the secondary node IP address:

1. Break the HA pair. Navigate to **Settings > Deployment**.

   The Deployment page is displayed. Click **Break HA**

   a. Log on to the primary node using an SSH client or from the hypervisor.
   b. Use `nsrecover` as the user name and enter the password that you have set.
   c. Enter **networkconfig**. Perform the procedure from **step 3** available at Register and deploy the first server (primary node).

      During the initial network configuration, you can provide a different IP address.
   d. Perform the same procedure for secondary node and continue with the procedure from **step 3** available at Register and deploy the second server (secondary node).

To update the floating IP address:

1. Navigate to **Settings > Deployment**.

   The Deployment page is displayed.

   a. Click **HA Settings**.
   b. Click **Configure Floating IP Address for High Availability Mode**.
   c. Enter the floating IP address and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Does ADM support AMD processors?

AMD processor is supported in:

- **NetScaler ADM 13.1 build 4.43 or later**.
- **NetScaler agent 13.1 build 17.42 or later**.

Deployment (Disaster Recovery)

How frequent does the replication happens between the primary site and disaster recovery site?

The replication between the primary site and the disaster recovery site is real time.

After initiating the backup script at the DR site, does the DR site becomes the temporary primary site, until the primary site is recovered and fully operational?

No. The DR site will now become the primary site. To revert the HA pair as the primary site, see Revert configurations to the original primary site

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the Break HA pair option is selected, both nodes operate as a standalone server. Since DR support is not applicable for standalone server, what happens to the DR site if Break HA pair is selected?

If you select Break HA pair option, the replication between the primary site and the DR site is terminated. You need to reconfigure the DR site as part of redeploying HA pair.

Event Management

How can I keep track of all the events that have been generated on my managed NetScaler instances using NetScaler ADM?

As a network administrator, you can view details such as configuration changes, log on conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along with events and their severity on specific instances. You can use the NetScaler ADM events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What are event rules?

Using NetScaler ADM, you can configure rules to monitor specific events. Event Rules make it easier to monitor many events generated across your NetScaler ADM infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run.

The conditions for which you can create filters are severity, NetScaler instances, category, and failure objects. The actions you can assign to the events are sending an email notification, forwarding SNMP traps from managed NetScaler instances to the NetScaler ADM, and sending an SMS notification.

Instance Management

What happens if an ADC instance cannot connect to ADM after bandwidth allocation when you use NetScaler pooled capacity licensing?

If the heartbeat between the ADC instance and ADM fails, the instance enters a grace period of 30 days. And after communication is re-established, pooled capacity licensing starts working. When in grace period, ADC functions are not affected. After 30 days of grace period, the ADC instance initiates warm restart and is unlicensed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What are data centers in NetScaler ADM?

A NetScaler ADM data center is a logical grouping of the NetScaler instances in a specific geographical location. Each server can monitor and manage several NetScaler instances within a data center. You can use the NetScaler ADM server to manage data such as syslog, application traffic flow, and SNMP traps from the managed instances. For more details on configuring data centers, see How to Configure Data Centers for Geomaps in NetScaler ADM.

What are the different NetScaler ADC appliances that are supported by NetScaler ADM?

Instances are the NetScaler ADC appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler ADM. You must add these instances to the NetScaler ADM server. You can add the following NetScaler ADC appliances and virtual appliances to NetScaler ADM:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

You can add instances either while setting up the NetScaler ADM server for the first time or later.

What is an instance profile?

An instance profile is used by NetScaler ADM to access an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

An instance profile contains the user name and password for access to one or more instances. A default profile is available for each instance type. For example, the ns-root-profile is the default profile for NetScaler instances. It contains the default NetScaler administrator credentials. When you change the credentials required for access to instances, you can define custom instance profiles for those instances.

Can I rediscover multiple NetScaler VPX instances in NetScaler ADM?

Yes, you can rediscover multiple Citrix **VPX** instances in NetScaler ADM to learn the latest states and configurations of the instances.

Navigate to **Infrastructure > Instances > NetScaler > VPX**, select the instances that you want to rediscover, and in the **Action** list click **Rediscover**. For more information, see How to Rediscover Multiple VPX Instances.

Can NetScaler ADM be installed on NetScaler SDX?

No

Can I add a NetScaler instance on the ADM software by using a public IP address?

Yes, you can by using network address translation (NAT).

- For adding a single instance: use NAT IP of the public IP address of the ADC instance.
- For adding an ADC HA pair: add the NAT IP addresses of the HA pair in this format:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`

- For adding an ADC cluster: add all the NAT public IP addresses of all the instances in the cluster, each separated by a comma, and add the NAT IP of the CLUSTER IP inside parentheses or round brackets. An example format: NAT1, NAT2, NAT3,(NATIP of CLUSTERIP).

For more information, see the following topics:

- Add instances to NetScaler ADM
- Configuring Network Address Translation

How to register a disaster recovery node if the DR node credentials are changed?

Reset the disaster recovery (DR) node credentials to `nsrecover` / `nsroot` using the following command:

```
./mps/change_freebsd_password.sh <username> <password>
```

To register a DR node, follow the steps in Deploy and register the NetScaler ADM DR node using DR console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

Can StyleBooks be used to configure different NetScaler instances running on different versions of the NetScaler software?

Yes, you can use StyleBooks to configure different NetScaler instances running on different versions if there is no discrepancy between the commands across different versions.

When a StyleBook is used to configure multiple NetScaler instances at the same time, and configuration of one NetScaler instance fails, what happens?

If applying the configuration to a NetScaler instance fails, the configuration is not applied to any more instances, and already-applied configurations are rolled back.

Do NetScaler backups made through NetScaler include configurations applied through StyleBooks?

Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Management

Can I assign a host name to my NetScaler ADM server?

Yes, you can assign a host name to identify your NetScaler ADM server. To assign a host name, navigate to **System**\> **System Administration** \> **System Settings**, and click **Change Hostname**.

The host name is displayed on the Universal license for NetScaler ADM. For more information, see How to Assign a Host Name to a NetScaler ADM Server.

Can I back up and restore my NetScaler ADM configuration?

Yes, you can back up configuration files (NTP files and SSL certificates), system data, infrastructure and application data, and all your **SNMP** settings. If your NetScaler ADM ever becomes unstable, you can use the backed-up files to restore your NetScaler ADM to a stable state.

To back up and restore your NetScaler ADM configuration, navigate to **System** > **Advanced Settings** > **Backup Files**, and click **Back Up** or **Restore** as the case might be. For more information, see How to back up and Restore Configuration on NetScaler ADM.

Citrix recommends that you use this feature before performing an upgrade or for precautionary reasons.

What are Thresholds and Alerts on NetScaler ADM?

You can set thresholds and alerts to monitor the state of a NetScaler instance and monitor entities on managed instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the value of a counter exceeds the threshold, NetScaler ADM generates an alert to signify a performance-related issue. When the counter value returns to the clear value specified in the threshold, the event is cleared.

Can I generate a technical support file for NetScaler ADM?

Yes. Citrix recommends that you generate an archive of NetScaler ADM data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

You can generate a technical support file that contains debug logs, the duration for which debug logs were collected, and distinct and diverse logs from the NetScaler ADM database.

To configure and send a technical support file, navigate to **System** \> **Diagnostics** \> **Technical Support**, and then, click **Generate Technical Support File**. For more information, see How to Generate a Tech Support File for NetScaler ADM.

What is syslog purging?

Syslog is a standard protocol for logging. Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which all Generic Syslog data, AppFirewall data, and NetScaler Gateway data will be deleted from NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can I configure NTP server on NetScaler ADM?

You can configure a Network Time Protocol (NTP) server in NetScaler ADM to synchronize the NetScaler ADM clock with the NTP server. Configuring an NTP server ensures that the NetScaler ADM clock has the same date and time settings as the other servers on the network.

To configure an NTP server, navigate to **System** \> **NTP Servers**, and then click **Add**. For more information, see How to Configure NTP Server on NetScaler ADM.

From which version is the NetScaler ADM active-passive HA deployment supported?

The NetScaler ADM active-passive HA deployment mode is supported from NetScaler ADM version 12.0 build 51.24.

I had a NetScaler ADM active-active HA setup and had configured a NetScaler appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration?

After you upgrade the NetScaler ADM HA pair to active-passive mode, you have to run the following command on the NetScaler appliance to update the load balancing configuration:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\\r\\nAccept-Encoding: identity\\r\\nUser-Agent: NetScaler-Monitor\\r\\nConnection: close\\r\\n\\r\\n\\"" -recv "{\\"statuscode\\":0, \\"is_passive\\":0}" -LRTM DISABLED**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can I configure load balancing of the NetScaler ADM HA pair on a NetScaler Instance using port 443?

No, you cannot configure load balancing of the NetScaler ADM HA pair on a NetScaler Instance using port 443.

When you configure the `http-ecv` and `https-ecv` monitors on NetScaler, it does not monitor the NetScaler ADM HA nodes correctly.

Can a NetScaler ADM server backup file be used to restore the configuration of another NetScaler ADM server?

Yes

After NetScaler ADM backs up a NetScaler instance, can that backup file be used to restore the configuration of another NetScaler instance through NetScaler ADM?

Yes. Download the NetScaler ADM backup file, upload it into another NetScaler instance's backup repository, and restore that instance. Make sure that the network information and authentication information do not conflict. For example, check for IP-address or port conflicts, mismatched password profiles. Also make sure that the restored VPX instance has the same NSIP address and NetScaler license as the one that was backed up.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before restoring an instance in a high availability pair, make sure the IP addresses and state (primary or secondary) stored in the backup file match those of the original HA configuration. Also verify that the new primary and secondary have the same type of NetScaler license.

Can we force NetScaler ADM to use a SNIP address to communicate with the NetScaler instances, instead of using the NSIP address of the NetScaler ADM server?

Yes, you can add a SNIP address (with management enabled) in NetScaler ADM for communication with NetScaler instances.

When I back up NetScaler Instances in NetScaler ADM, is the result a full back-up or a basic back-up?

Backups of NetScaler instances by NetScaler ADM are full backups.

Is there a troubleshooting guide for NetScaler ADM?

Yes. See `<https://support.citrix.com/article/CTX224502>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How are NetScaler instances managed when a NetScaler ADM HA failover occurs?

If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node. All the NetScaler instances are updated with the latest primary node details as their SNMP trap destination by default.

The new primary (active) NetScaler ADM node checks to determine whether the previously active node was configured as the AppFlow® collector or syslog server, if it was, the new primary adds the AppFlow collector or syslog server details to the information sent to the instances.

For syslog it replaces the old server details.

What happens when the NetScaler ADM HA node that went down comes back up?

After returning to service, the NetScaler ADM node remains passive unless the active node fails over

How are NetScaler instances distributed across NetScaler ADM HA nodes?

All the NetScaler instances are managed by the primary NetScaler ADM node.

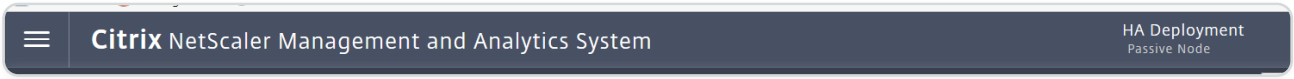
© 1997–2026 Citrix Systems, Inc. All rights reserved.

How are virtual server licenses managed if there is NetScaler ADM HA failover?

If the NetScaler ADM primary node on which virtual server licenses are applied goes down, the new primary node manages the virtual server licenses for a grace period of 30 days. Reapply the licenses on the new primary before the end of the grace period. For alternatives, contact NetScaler support.

Is a load balancer mandatory for a NetScaler ADM HA setup?

No, but if there is no load balancer, NetScaler ADM nodes must be accessed through their own IP addresses. The passive node is marked with the tag "Passive", and Citrix recommends not to create any configurations on the passive node.



Does NetScaler ADM support an external database?

No

Can a NetScaler instance that is being managed by NetScaler ADM be used as a Load balancer for NetScaler ADM HA?

Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What data is synchronized between NetScaler ADM HA nodes?

Complete NetScaler ADM database is synchronized, and the following folders are synchronized:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Configure adaptive thresholds
- Configure database summarization
- Configure SLA management
- Create thresholds and alerts
- Disable URL data collection
- Logstream overview
- Dashboards
- All Violations
- Application overview
- Network violation details
- SSL Insight
- TCP Insight
- Troubleshoot Web Insight issues
- View analytics for Web transactions
- Detailed procedures to setup dual tier or service mesh lite topology
- Detailed procedures to set up service mesh topology
- Detailed procedures to set up single tier or unified ingress topology
- Optional telemetry data for NetScaler® telemetry program
- Required telemetry data for NetScaler® telemetry program
- Data governance
- Back up and restore a NetScaler® ADM configuration in an HA pair
- Configure system notification settings
- Use jobs to upgrade NetScaler instances
- Configure sites for geomaps
- Modes of telemetry collection
- Configure adaptive thresholds

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configure database summarization
- Configure SLA management
- Create thresholds and alerts
- Disable URL data collection
- Logstream overview
- Dashboards
- All Violations
- Application overview
- Back up and restore NetScaler instances
- Network violation details
- SSL Insight
- Troubleshoot Web Insight issues
- View analytics for Web transactions
- Detailed procedures to setup dual tier or service mesh lite topology
- Detailed procedures to set up service mesh topology
- Detailed procedures to set up single tier or unified ingress topology
- Data governance (For NetScaler Console between 14.1-8.x and 14.1-21.x builds)
- Data governance (For NetScaler ADM 14.1-4.42 or earlier builds)
- Optional telemetry data for Cloud Connect
- Optional telemetry data for NetScaler® Telemetry program
- Required telemetry data for Cloud Connect
- Required telemetry data for NetScaler® Telemetry program
- Back up and restore a NetScaler Console configuration in an HA pair
- Configure system notification settings
- Configure sites for geomaps

Configure adaptive thresholds

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler® ADM

1. Navigate to **System** \> **Analytics Settings** \> **Adaptive Thresholds**, and then click **Add**.
2. On the **Create 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 summarization

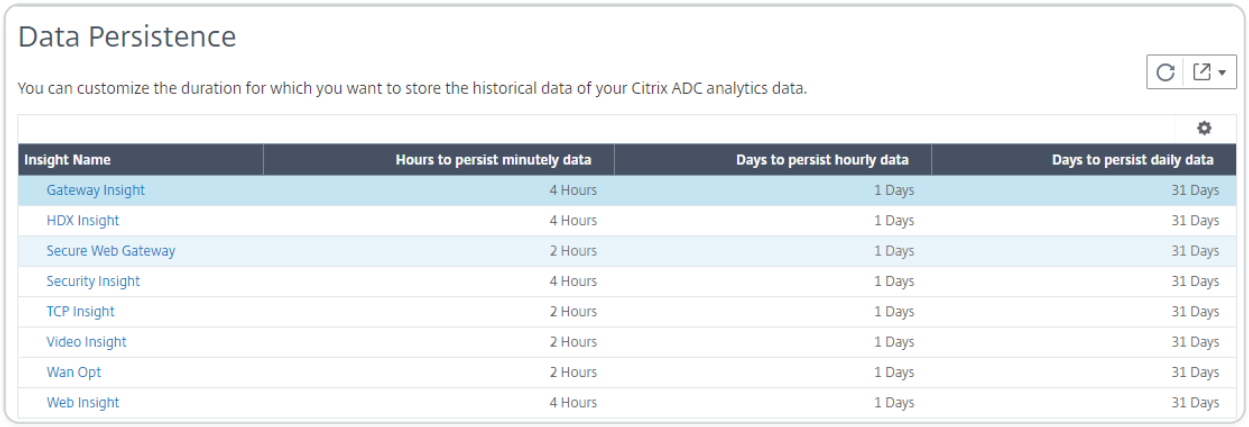
Configure Database Summarization in NetScaler® ADM allows you to customize the duration for you want to store the historical data of your NetScaler analytics data. You can choose the following database summarization types for your analytics' historical data:

- Hours to persist minutely data
- Days to persist hourly data
- Days to persist daily data

To configure database summarization

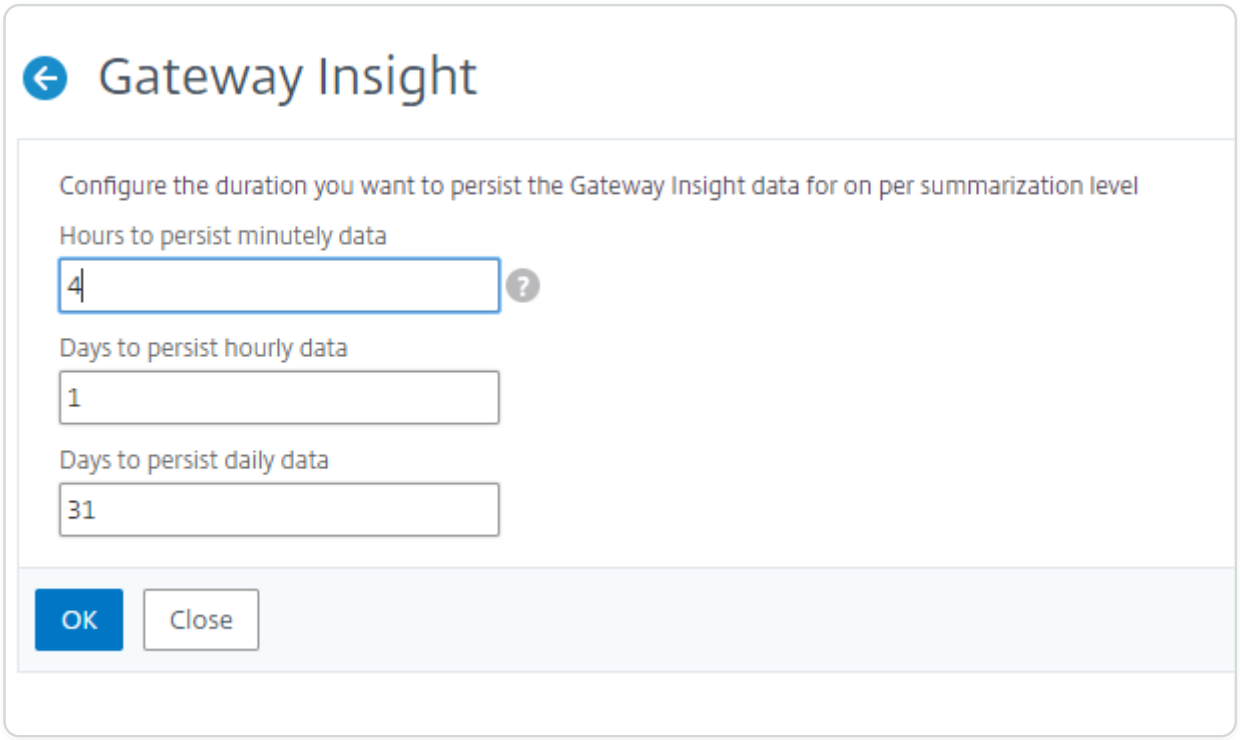
1. Navigate to **System** \> **Analytics Settings** \> **Database Summarization**.
2. Click the Insight type you want to configure the database summarization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
Gateway Insight	4 Hours	1 Days	31 Days
HDX Insight	4 Hours	1 Days	31 Days
Secure Web Gateway	2 Hours	1 Days	31 Days
Security Insight	4 Hours	1 Days	31 Days
TCP Insight	2 Hours	1 Days	31 Days
Video Insight	2 Hours	1 Days	31 Days
Wan Opt	2 Hours	1 Days	31 Days
Web Insight	4 Hours	1 Days	31 Days

3. Specify the duration for which you want to retain Insight data on NetScaler ADM. For example, for Gateway Insight, you can store your analytics' minutely historical data for 2 hours, or hourly data for 1 day.



Configure SLA management

Service Level Agreement Management feature will help you to manage SLA over Server Response Time, Hits/sec, and Bandwidth usage across your Domain usage. Configuring SLA on various breaches eases you to monitor many events generated across your NetScaler infrastructure.

You can configure SLA breach for the following:

- Server Response time
- SLA Breach Frequency for Bandwidth
- SLA Breach Frequency for Hits

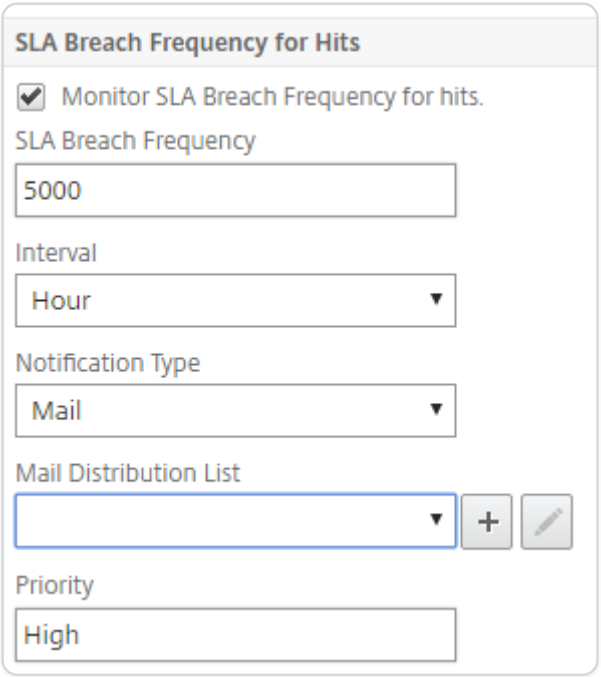
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SLA Breach Frequency for Response Time

You can configure notifications for each SLA breach whenever your appliance encounters it. You can configure the notification type as Mail, SMS, or Syslog and configure distribution lists respectively.

To configure SLA breach for a NetScaler instance

1. Navigate to **System** \> **Analytics Settings** \> **SLA Management**.
2. From the list displayed, select the NetScaler® IP address of an appliance on which you want to manage SLA.
3. Click **Add**, if you want to add a new **SLA Group** and add beach definitions to it. Alternatively, you can select a SLA group from the list if you already have added a SLA group.
4. In the **SLA Group** field, enter the name for the new SLA group.
5. Select the appropriate check boxes to enable or disable the SLA monitors.
6. Select the appropriate breach values for the selected options. For example, Maximum Server Response Time (ms)* = 22 ms.
7. Select the notification type and the interval to notify from the **Notification Type** and **Interval** lists appropriately.
8. You can select the distribution lists to send the notifications from the Mail/SMS/Syslog Distribution List menu.
9. Click **Create**, to create, and add a SLA group to your NetScaler appliance.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create thresholds and alerts

You can set thresholds and alerts to monitor the state of a NetScaler instance. You can set thresholds on counters and monitor instances and entities on managed instances.

When the value of a counter exceeds the threshold, NetScaler® 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, NetScaler 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 NetScaler ADM

1. Navigate to **System** \> **Analytics Settings** \> **Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Thresholds and Alerts** 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.
   - **Community** – Community string for each trap that is to be sent to the trap listener.
3. Optionally, configure actions such as alerts, emails notifications, and SMS notifications.
4. 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.

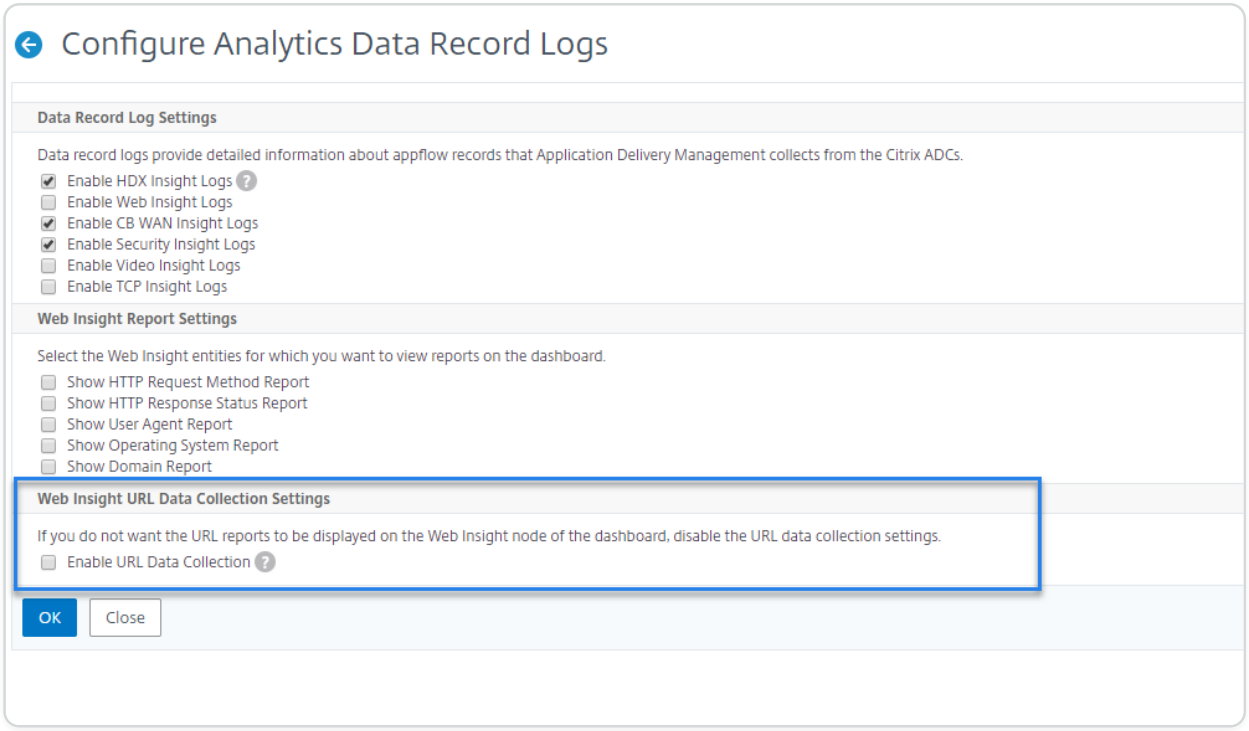
Disable URL data collection

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 NetScaler® ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To disable URL data collection from NetScaler ADM

1. Navigate to **System** \> **Analytics Settings**, and then click **Configure Data Record Settings**.
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**.



Logstream overview

NetScaler 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 NetScaler instances to NetScaler ADM. For more information, see AppFlow.

- IPFIX is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. IPFIX uses UDP protocol which is unreliable transport protocol used for data flow in one direction. Since IPFIX uses UDP protocol, adhering to IPFIX standard results in processing more resources in NetScaler® ADM.
- Logstream is a Citrix-owned protocol that is used as one of the transport modes to efficiently transfer the analytics log data from NetScaler instances to NetScaler ADM. Logstream uses reliable TCP protocol and requires lesser resources in processing the data.

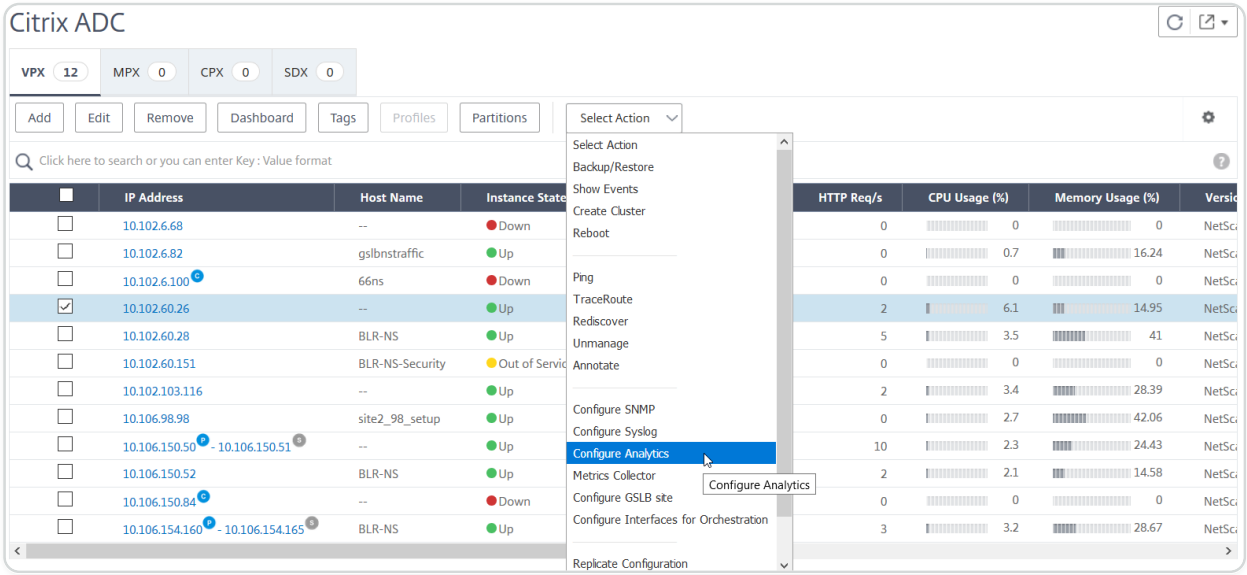
For NetScaler between **11.1 Build 47.14 and 11.1 Build 62.8**, Logstream is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

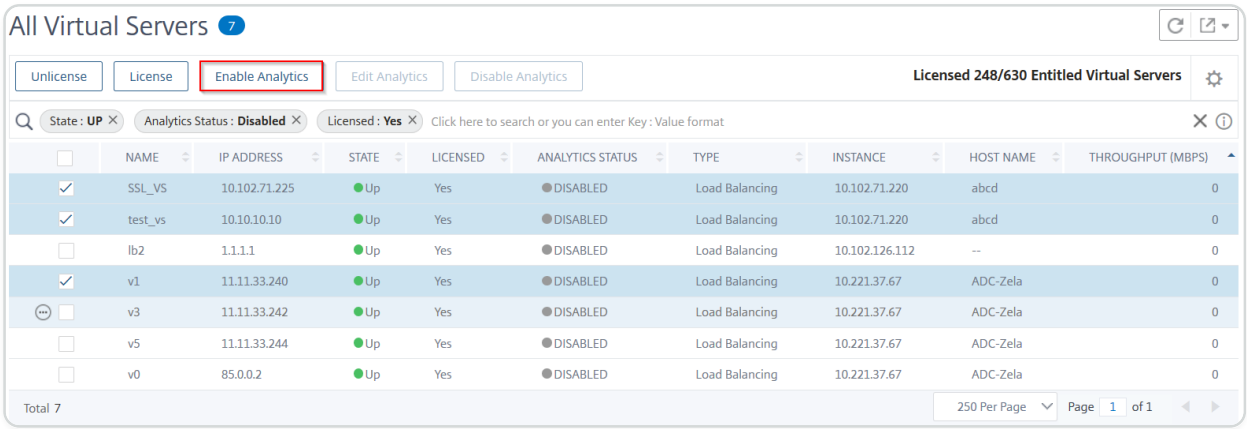
insights. For NetScaler version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

Enable Logstream as Transport Mode

1. Navigate to **Infrastructure > Instances**, and select the ADC instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.



3. Select the virtual servers and then click **Enable Analytics**.



4. On the **Enable Analytics** window:
   a. Select the insight types (Web Insight or WAF Security Violations)
   b. Select **Logstream** as Transport Mode

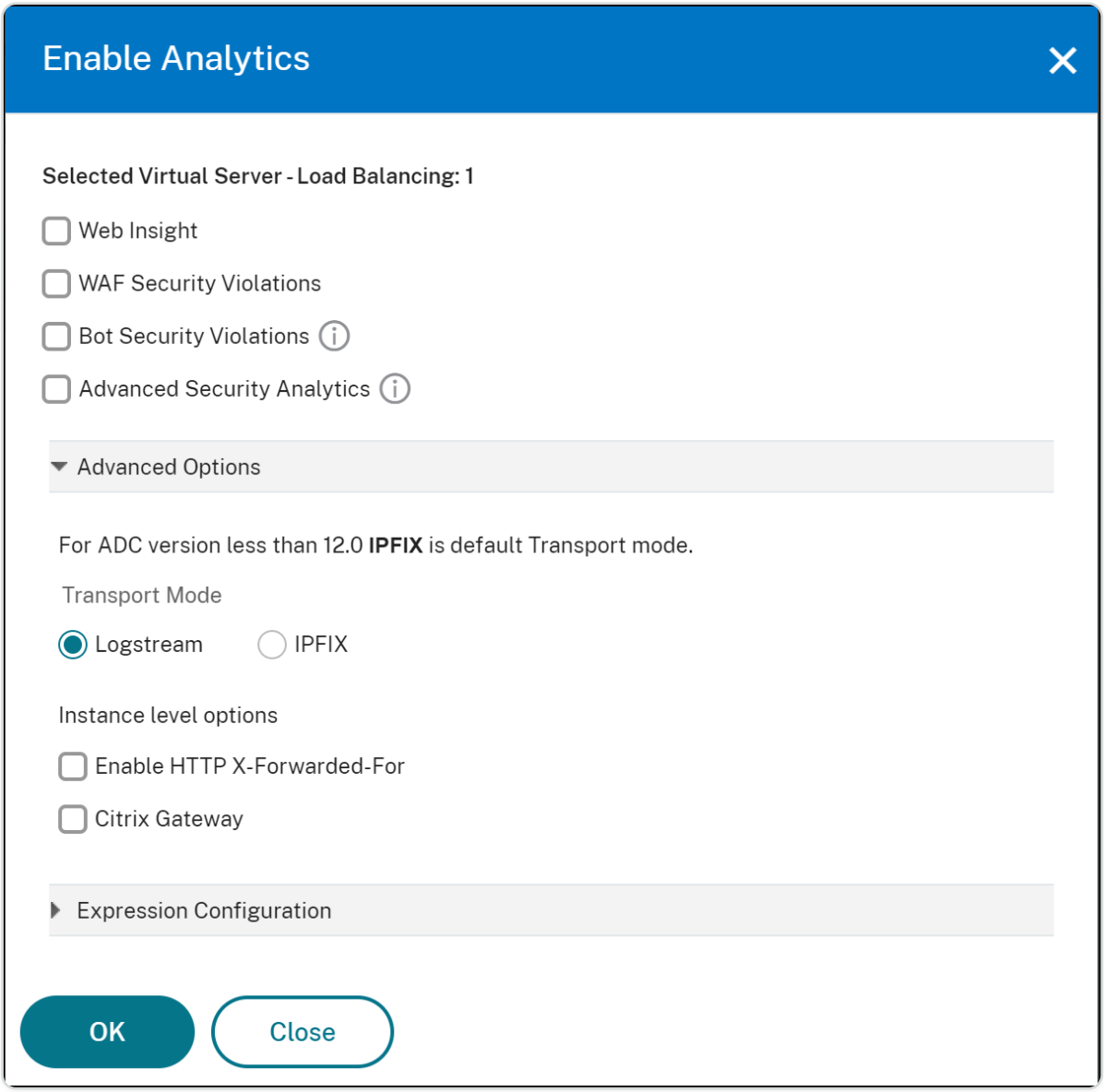
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

For NetScaler 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 NetScaler version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

c. The Expression is true by default

d. Click **OK**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- If you select virtual servers that are not licensed, then NetScaler ADM first licenses those virtual servers and then enables analytics
- For admin partitions, only **Web Insight** is supported
- For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed

The following table describes the features of NetScaler ADM that supports Logstream as the transport mode:

FEATURE	IPFIX	LOGSTREAM
Web Insight	•	•
WAF Security Violations	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

Dashboards

NetScaler® 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.

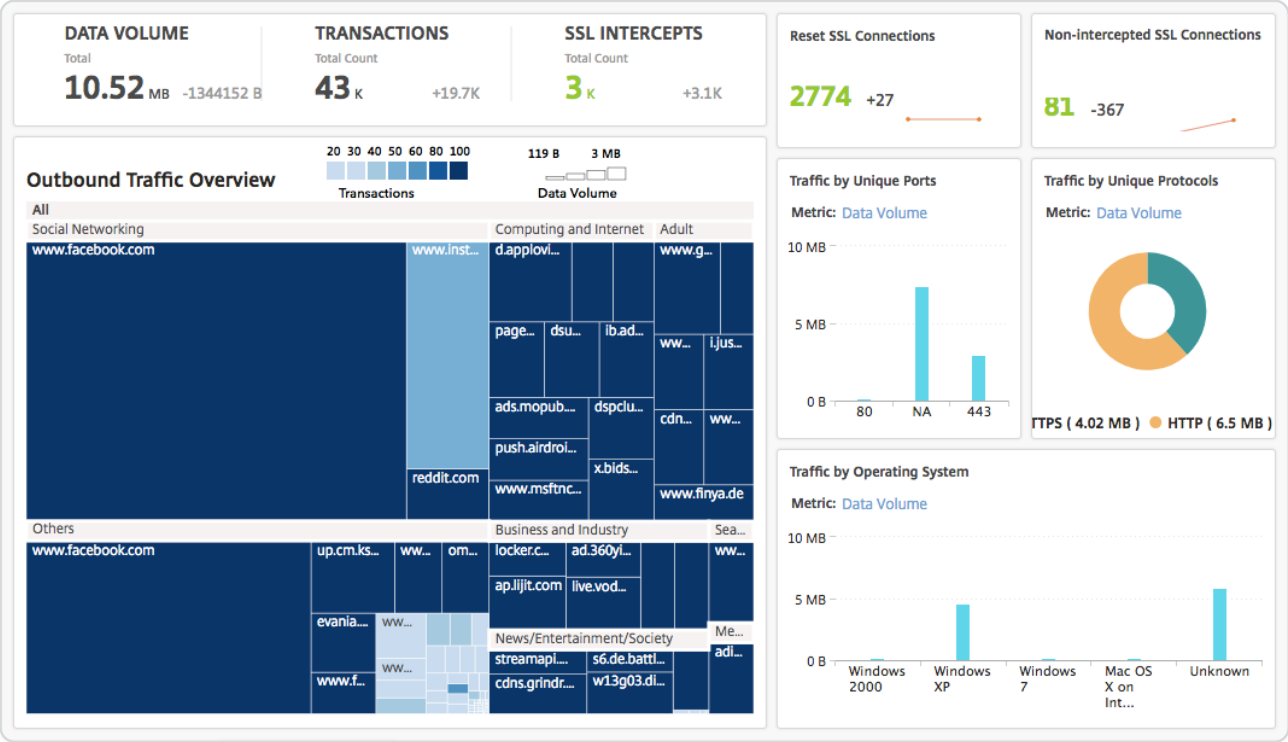
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler appliance during the transactions.
4. Number of SSL connections not intercepted by NetScaler appliance during the transactions.
5. Number of SSL connections reset by the NetScaler 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**.

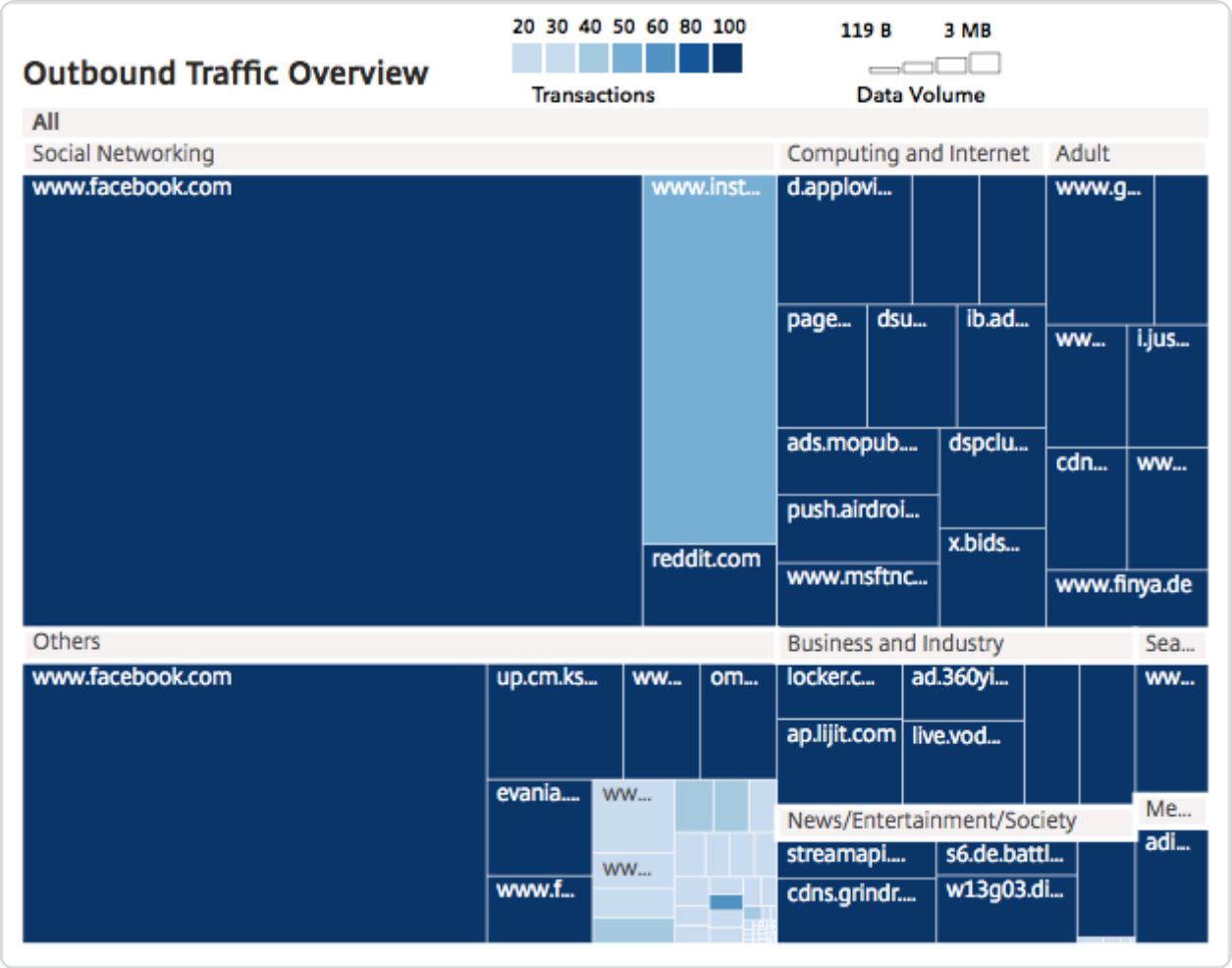


View the outbound traffic from the network

The **Outbound Traffic Dashboard** includes an **Outbound Traffic Overview** pane. In the **Outbound Traffic Overview** pane, NetScaler ADM groups the accessed URLs or domains into categories, such as Shopping, News, Social Networking, and so on. The **Outbound Traffic**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 a category to filter the charts to display details related the category for the specified time frame.

User dashboard

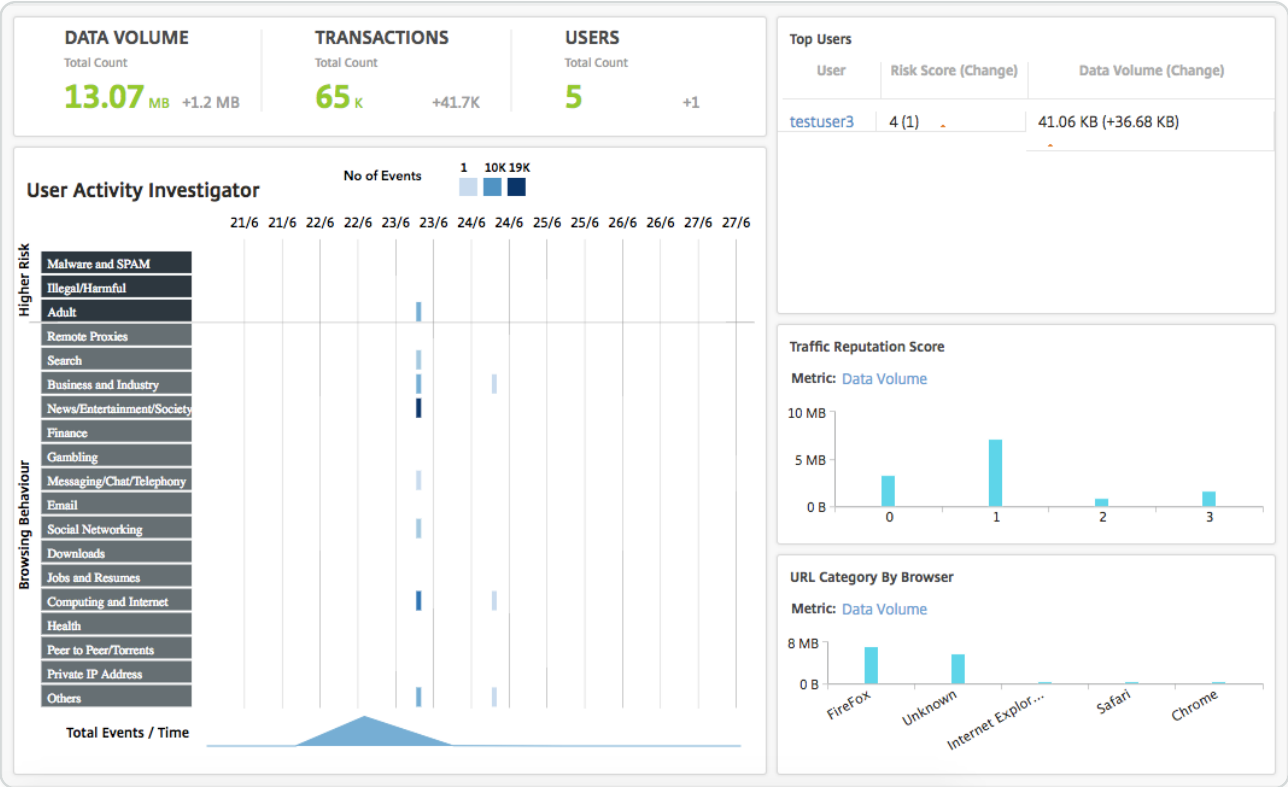
The **User Dashboard** displays a summary of the activities performed by the users in your enterprise. It provides key metrics that you can use to determine the following:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Amount web traffic generated by the users, based on the traffic reputation score.

To access the **User Dashboard**, navigate to **Users \> Dashboard**.



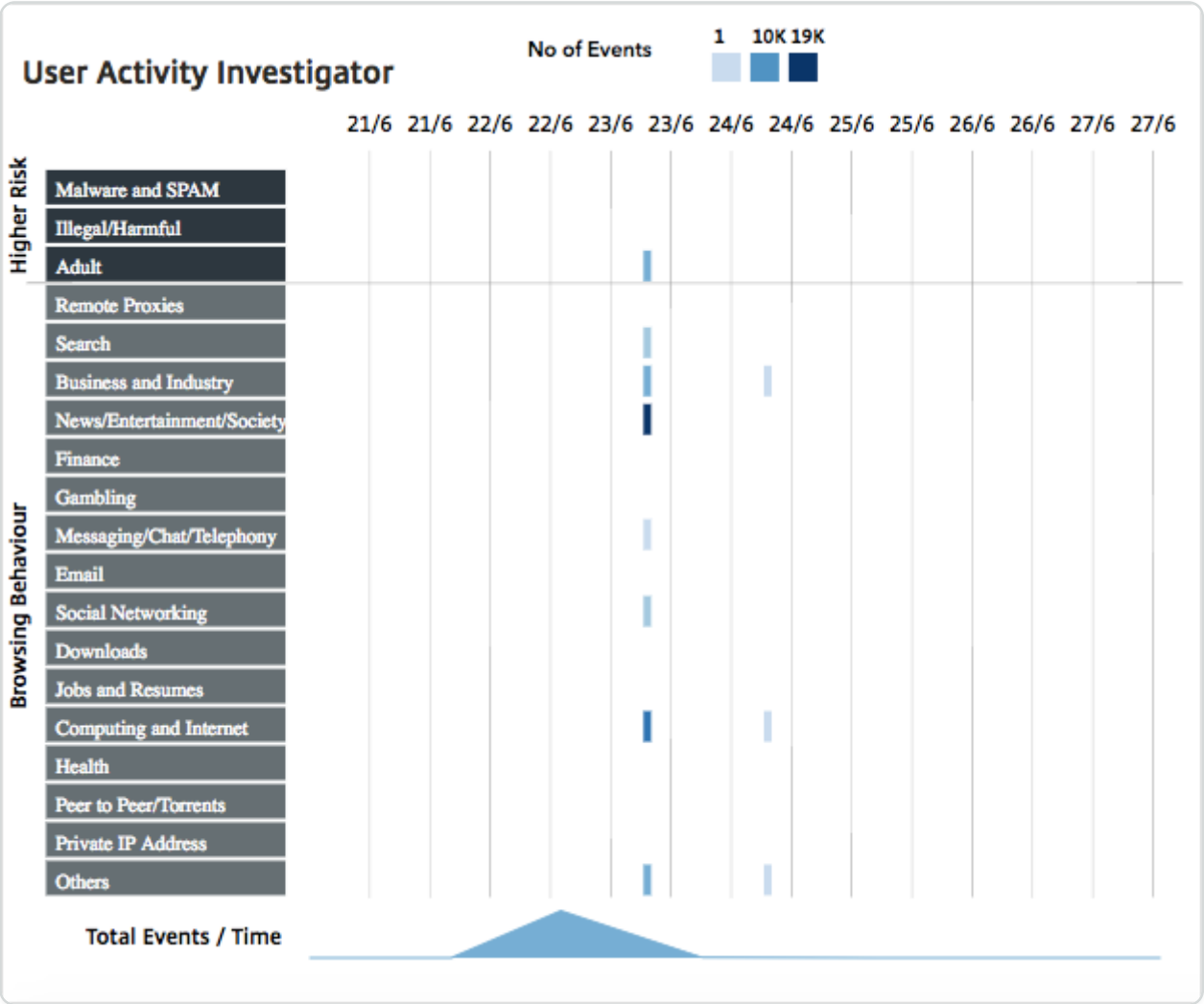
You can click a user in the **Top Users** pane to filter the charts to display details of the web activity performed by the user in the specified time frame.

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 list.

You can click the events to further drill down for the details of the transactions.

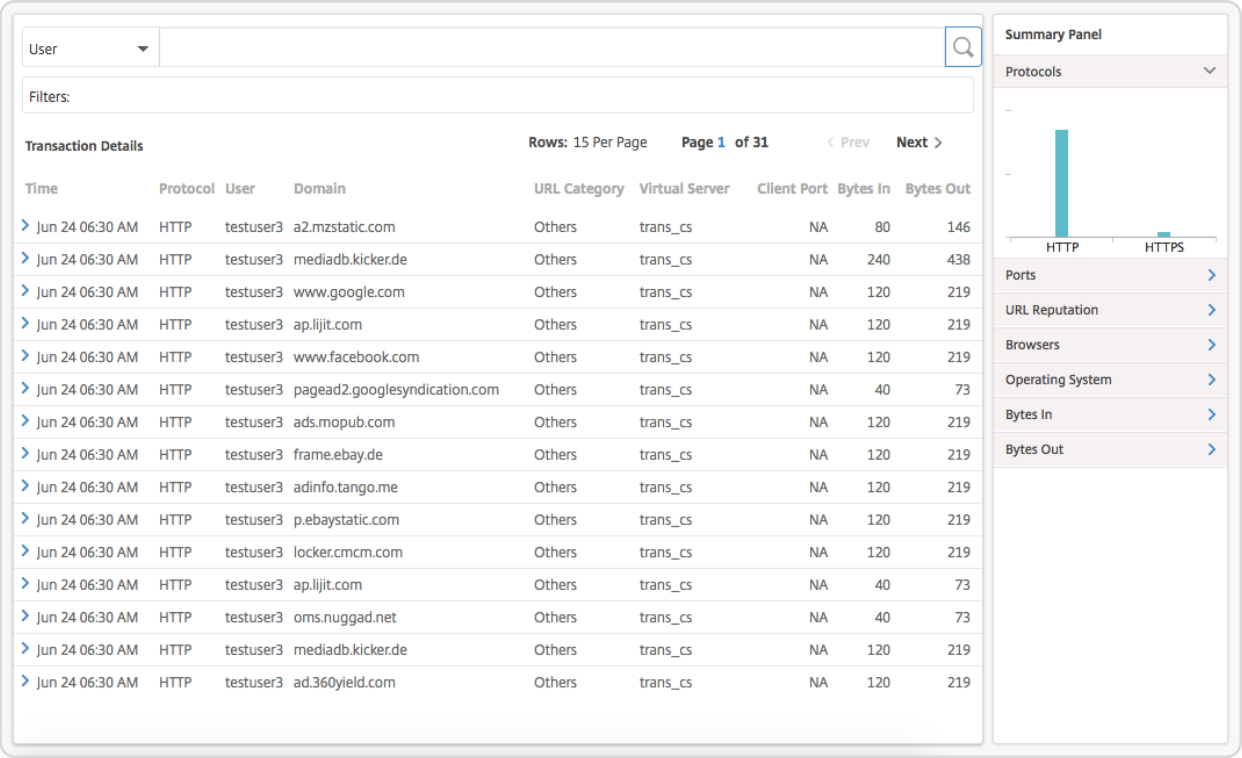
User transactions

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 accessed by the user
5. URL category

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

METRICS	DESCRIPTION
Protocols	Protocols used in the transactions
Ports	Ports used for the transactions
URL Reputation	URL reputation score
Browsers	Browsers used for the transactions
Operation System	Operating system used for the transactions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bytes In	Amount of data received through the NetScaler Appliance.
Bytes Out	Amount of data sent through the NetScaler Appliance.

Risk score

Risk Score is a scoring system used in NetScaler ADM to determine the risks associated with users in your enterprise. NetScaler ADM assigns a risk score based on the URL reputation score assigned by the NetScaler 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 NetScaler ADM.

RISK SCORE	DESCRIPTION
1	The web activity of the user has no perceived threat or is not abnormal.
2	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.
3	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.
4	Potentially compromised user.
5	The web activity of the user is abnormal and the user has accessed known malicious sites.

All Violations

The **All Violations** page displays the application security violation details based on the **Network**, **WAF**, and **Bot** categories.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Violation categories

NetScaler® ADM enables you to view the following violations. Under **Violation Details**, you can click each violation tab to view the violation details.

NETWORK	WAF	BOT
HTTP Slow Loris	CSRF Form Tagging	Marketing
DNS Slow Loris	Deny URL	Scraper
HTTP Slow Post	Form Field Consistency	Screenshot Creator
NXDomain Flood Attack	Field Formats	Search Engine
HTTP desync attack	Cookie Hijack	Feed Fetcher
Bleichenbacher Attack	Infer Content Type XML	Link Checker
Segment smack Attack	Buffer Overflow	Service Agent
SYN Flood Attack	Content Type	Site Monitor
Small Window Attack	Cookie Consistency	Speed Tester
	Safe Object	Tool
	HTML SQL Inject	Uncategorized
	Start URL	Virus Scanner
	Cross-site scripting	Vulnerability Scanner
	XML DoS	DeviceFP Wait Exceeded
	XML Format	Invalid DeviceFP
	XML WSI	Invalid Captcha Response
	XML SSL	Captcha Attempts Exceeded
	XML Attachment	Valid Captcha Response
	XML SOAP Fault	Captcha Client Muted

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	WAF	BOT
	XML Validation	Captcha Wait Time Exceeded
	Others	Request Size Limit Exceeded
	IP Reputation	Rate Limit Exceeded
	HTTP DOS	Block list (IP, subnet, policy expression)
	TCP Small Window	Allow list (IP, subnet, policy expression)
	Signature Violation	Zero Pixel Request
	File Upload Type	Source IP
	JSON cross-site scripting	Host
	JSON SQL	Geo Location
	JSON DOS	URL
	Command Injection	Crawler
	Maximum Uploads	
	Referrer Header	
	Safe Commerce	

Security violations dashboard

In the security violations dashboard, you can view:

- Total violations occurred across all ADC instances and applications. The total violations are displayed based on the selected time duration.
- Total violations.
- Total ADCs affected, total applications affected, and top violations based on the total occurrences and the affected applications.

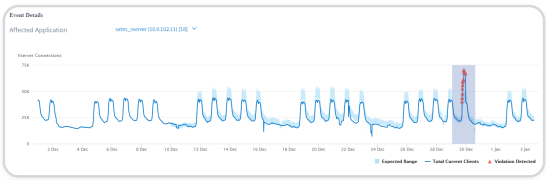
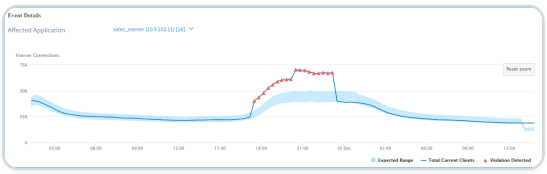
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Violation details

For each violation, NetScaler ADM monitors the behavior for a specific time duration and detects violations for unusual behaviors. Click each tab to view the violation details. You can view details such as:

- The total occurrences, last occurred, and total applications affected.
- Under event details, you can view:
  - The affected application. You can also select the application from the list if two or more applications are affected with violations.
  - The graph indicating violations.

    Drag and select on the graph that lists the violations to narrow down the violation search.

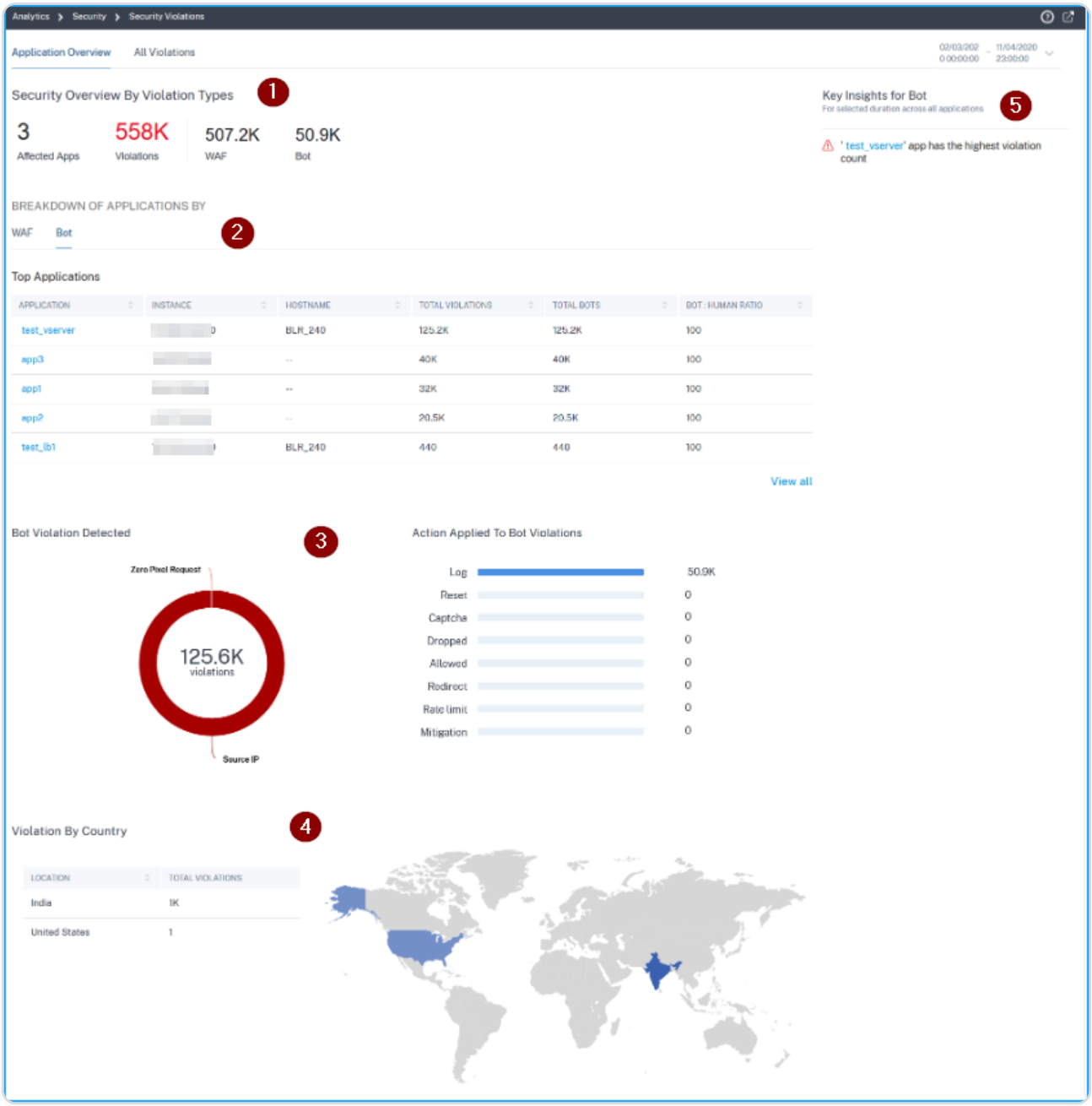
DRAG AND SELECT ON GRAPH	SEARCH RESULT
	

    Click **Reset Zoom** to reset the zoom result.
  - **Recommended Actions** that suggest you troubleshoot the issue.
  - Other violation details such as violence occurrence time and detection message.

Application overview

The **Application Overview** page displays applications with full visibility into the threat details associated in both WAF Security Violations and Bot Security Violations. You can also view information such as total violations, total WAF and Bot violations, violation by country, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – Displays the total affected applications, total violations, total WAF violations, and total Bot violations for the selected duration.

2 – Displays the WAF and Bot violation details. Click the **WAF** and **Bot** tab to view the top 5 applications based on the total violations occurred. Click **View All** to view all application details.

3 – Displays the top violations based on the occurrences and the actions applied.

4 – Displays a geo map view that provides visibility from which locations the violations have occurred.

5 – Provides information based on the violations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Violation categories

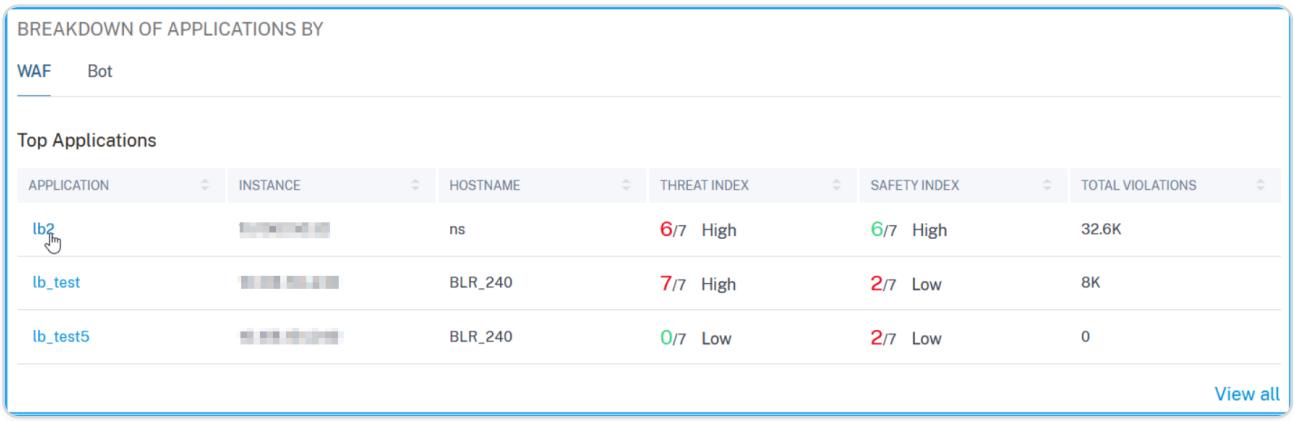
WAF	BOT
Cookie Hijack	Feed Fetcher
Infer Content Type XML	Link Checker
CSRF Form Tagging	Marketing
Deny URL	Scraper
Form Field Consistency	Screenshot Creator
Field Formats	Search Engine
Maximum Uploads	Service Agent
Referrer Header	Site Monitor
Safe Commerce	Speed Tester
Safe Object	Tool
HTML SQL Inject	Uncategorized
Start URL	Virus Scanner
Cross-site scripting	Vulnerability Scanner
XML DoS	DeviceFP Wait Exceeded
XML Format	Invalid DeviceFP
XML WSI	Invalid Captcha Response
XML SSL	Captcha Attempts Exceeded
XML Attachment	Valid Captcha Response
XML SOAP Fault	Captcha Client Muted
XML Validation	Captcha Wait Time Exceeded

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
Others	Request Size Limit Exceeded
IP Reputation	Rate Limit Exceeded
HTTP DOS	Block list (IP, subnet, policy expression)
TCP Small Window	Allow list (IP, subnet, policy expression)
Signature Violation	Zero Pixel Request
File Upload Type	Source IP
JSON cross-site scripting	Host
JSON SQL	Geo Location
JSON DOS	URL
Command Injection	Crawler
Buffer Overflow	
Content Type	
Cookie Consistency	

View WAF violation details

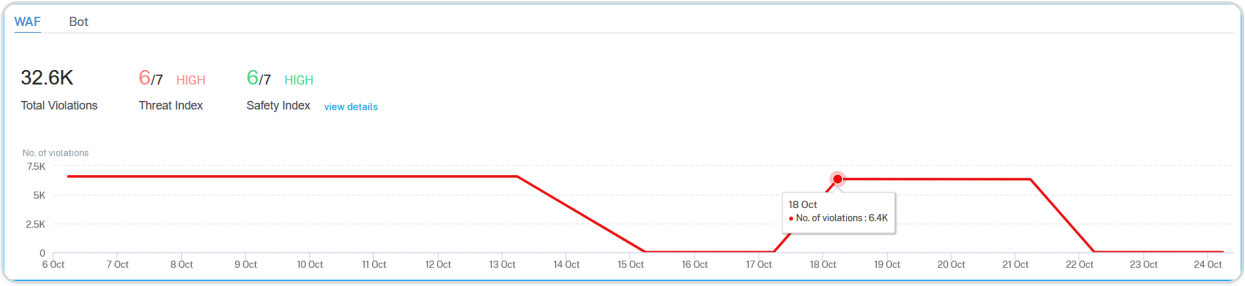
Click an application from the **Top Applications** or from the **View All** option to view the WAF details.



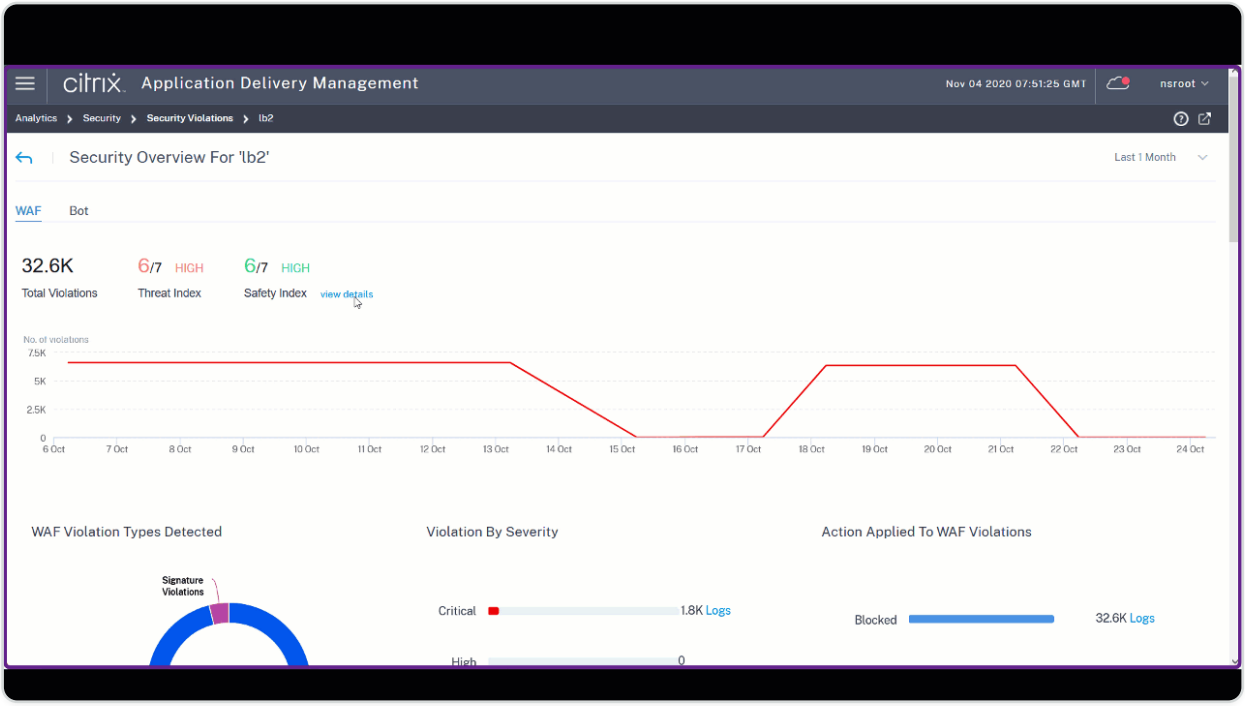
The **Security Overview** page for the selected application is displayed. Under **WAF**, you can view:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

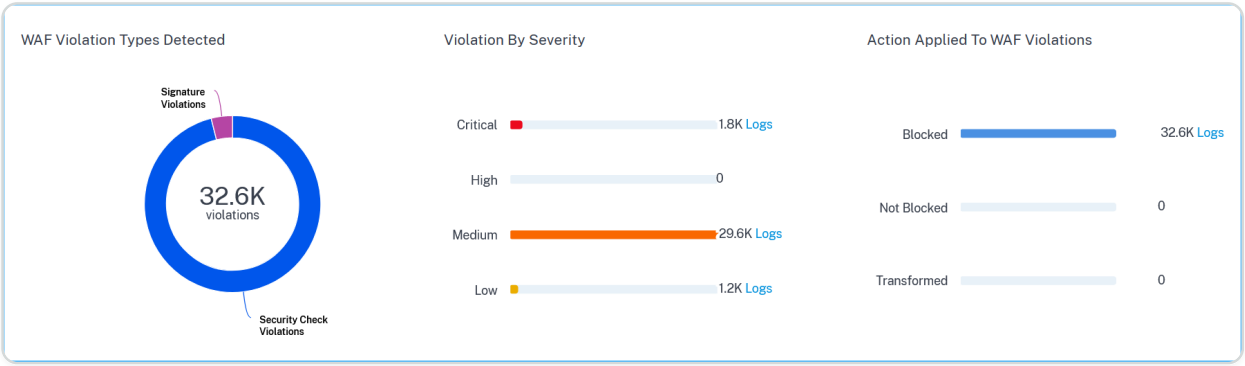
- A graph view that indicates the total violations, threat index score, safety index score for the application.



Click **View Details** to see the Application Firewall and NetScaler System Security configuration details.

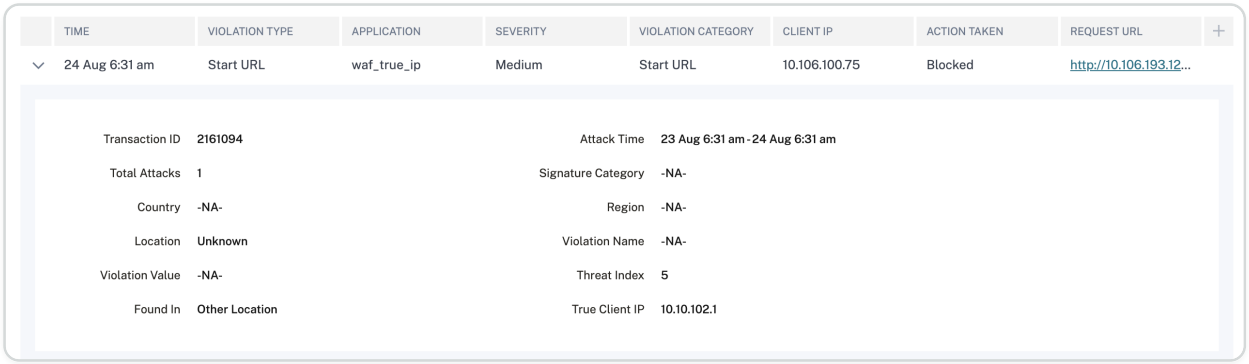


- The violations based on types, severity, and actions applied.

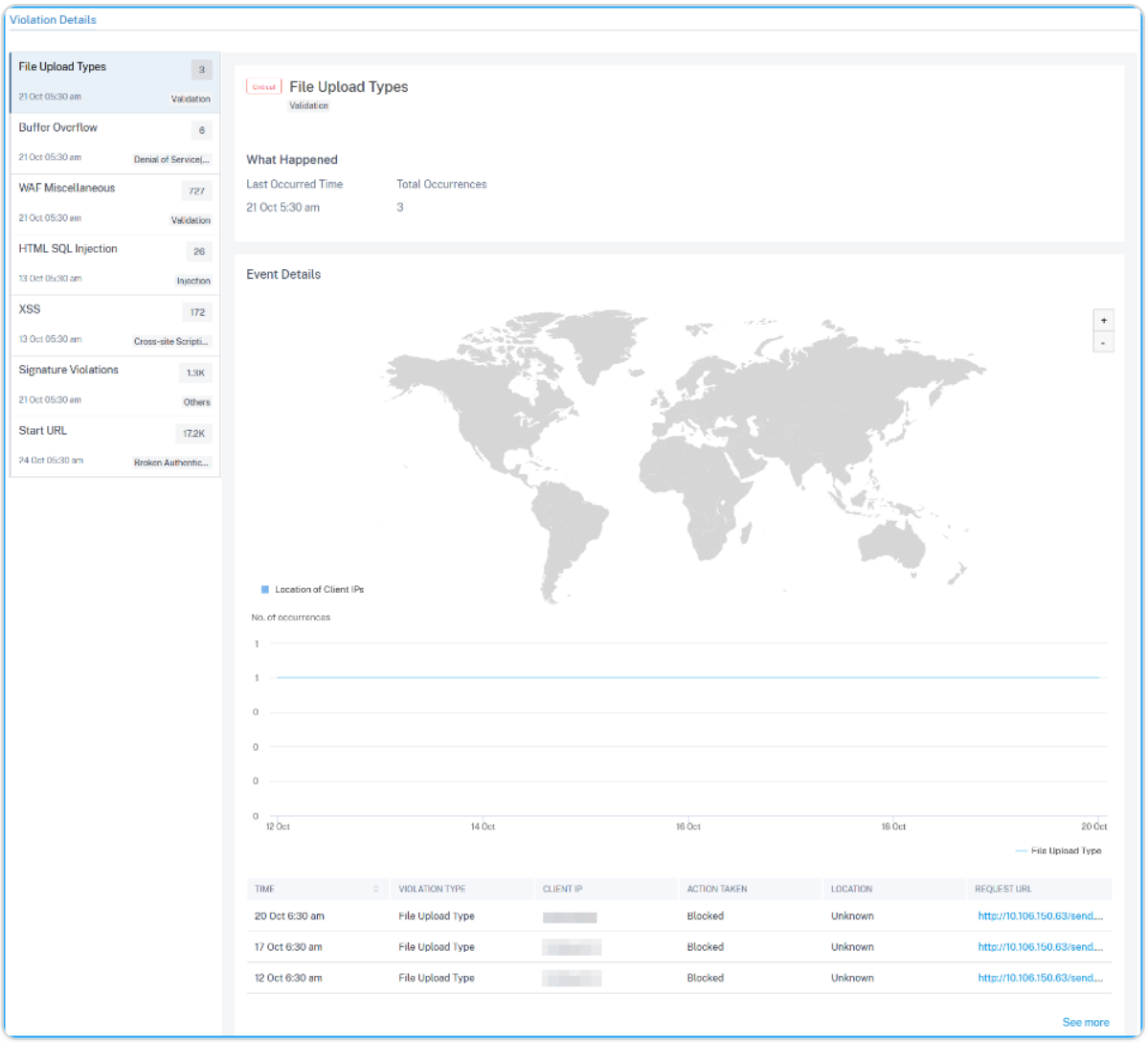


Click **Logs** to view details based on the severity or action taken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The violations affected on the application. Under **Violation Details**, you can view the affected violation details. Click each violation to view details such as:
  - **What Happened** – Indicates the total occurrences and the last occurred date and time.
  - **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.



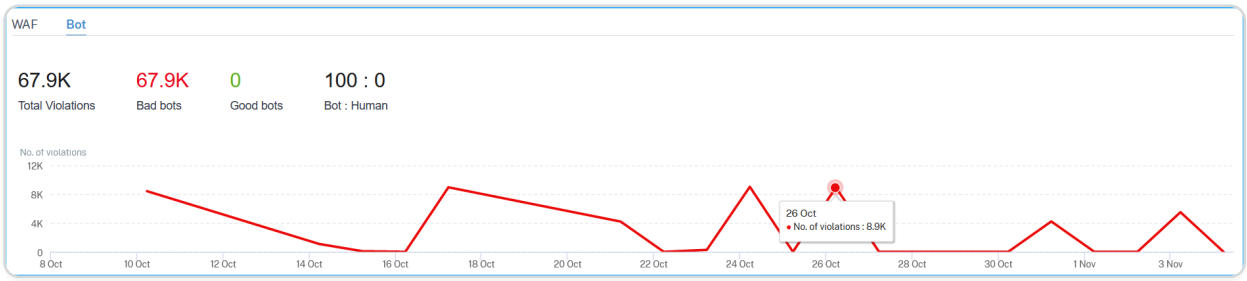
© 1997–2026 Citrix Systems, Inc. All rights reserved.

View bot violation details

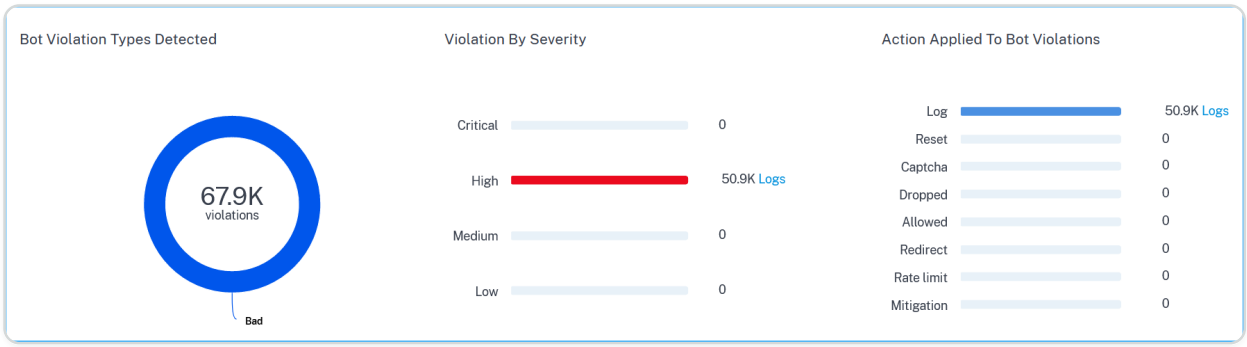
From the **Bot** tab, click an application from the Top Applications or from the **View All** option to view the bot details.

The **Security Overview** page for the selected application is displayed. Under **Bot**, you can view:

- A graph indicating total bots, total bad bots, total good bots, and total ratio between human users and bots accessing the application.

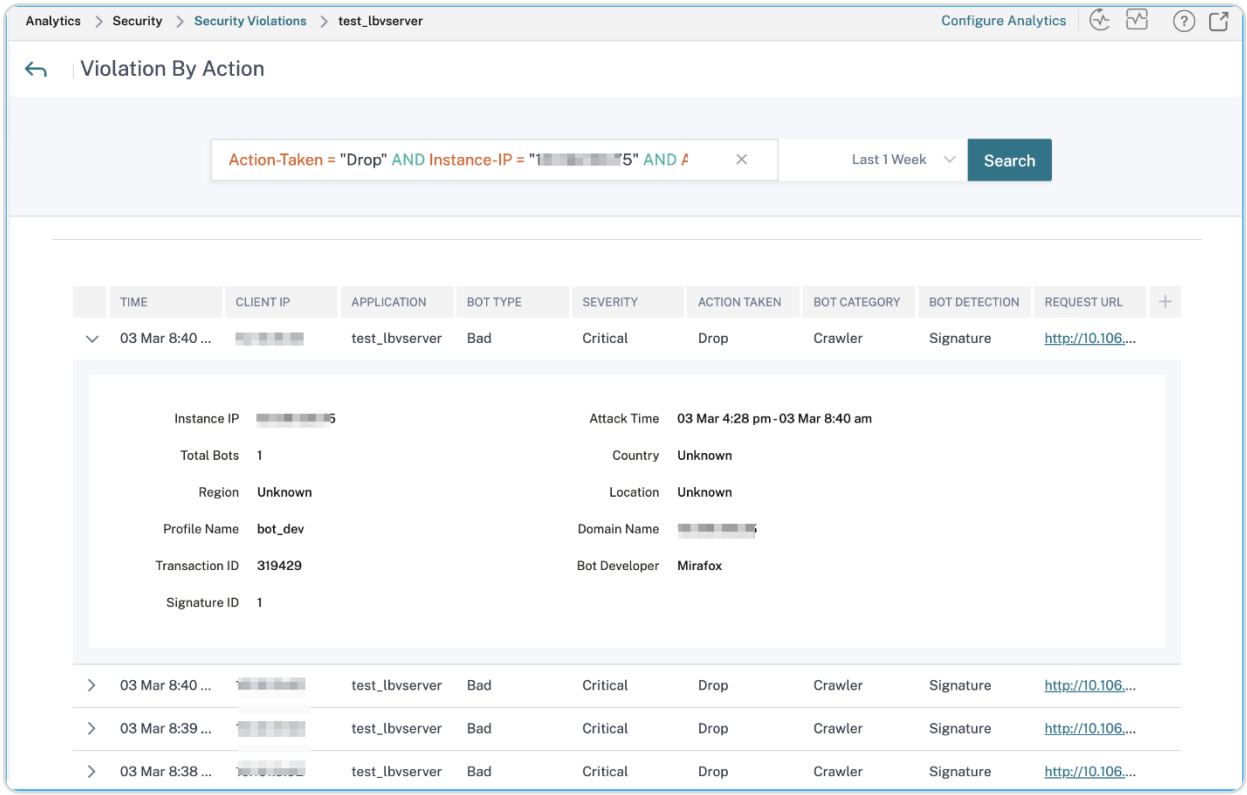


- The violations based on the bot types, severity, and actions applied.



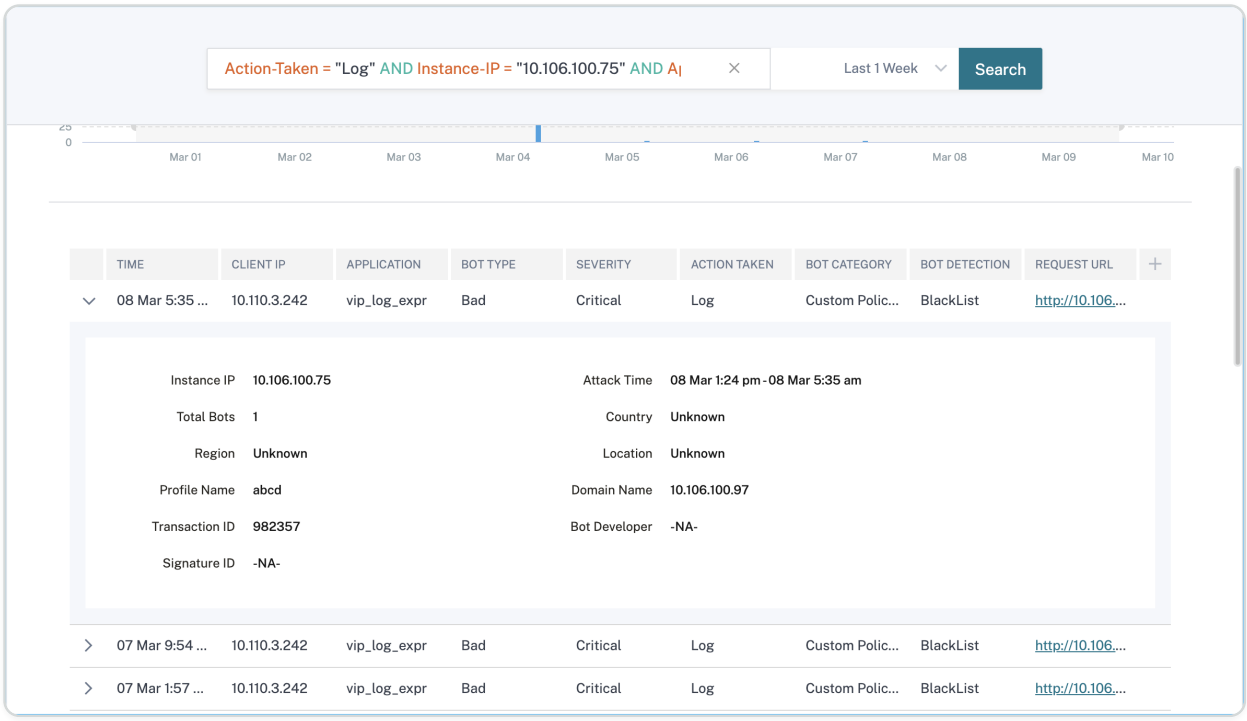
Click **Logs** to view details based on severity or actions taken. If a detected bot is a Signature type bot, you can view more details such as Bot developer and Signature ID. The Signature ID enables you to identify if the detected bot is a good bot or a bad bot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note

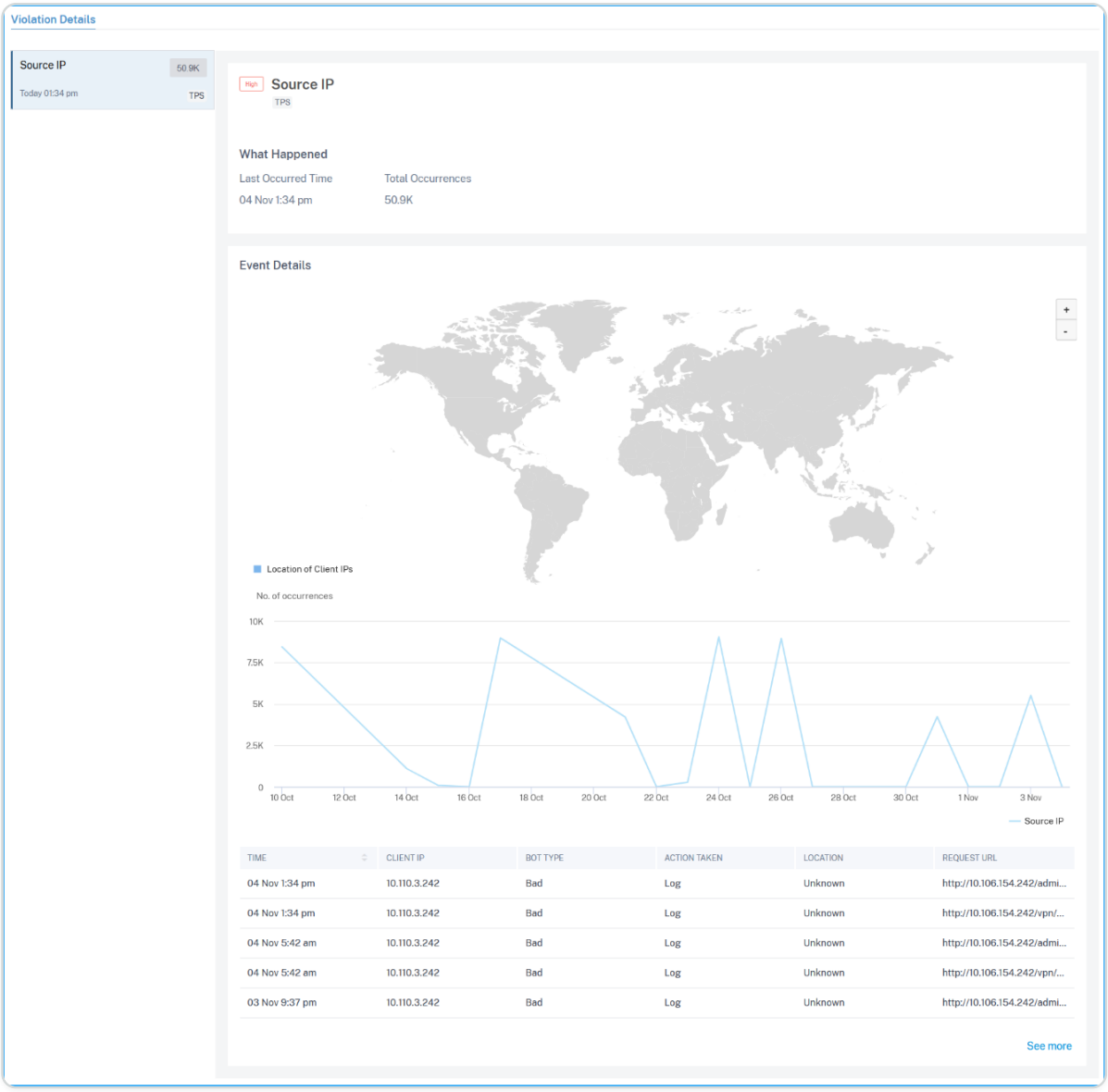
If a detected bot is any other bot type apart from Signature bot, the Signature ID and Bot developer are displayed as N/A.



- The violations affected on the application. Under Violation Details, you can view the affected violation details. Click each violation to view details such as:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

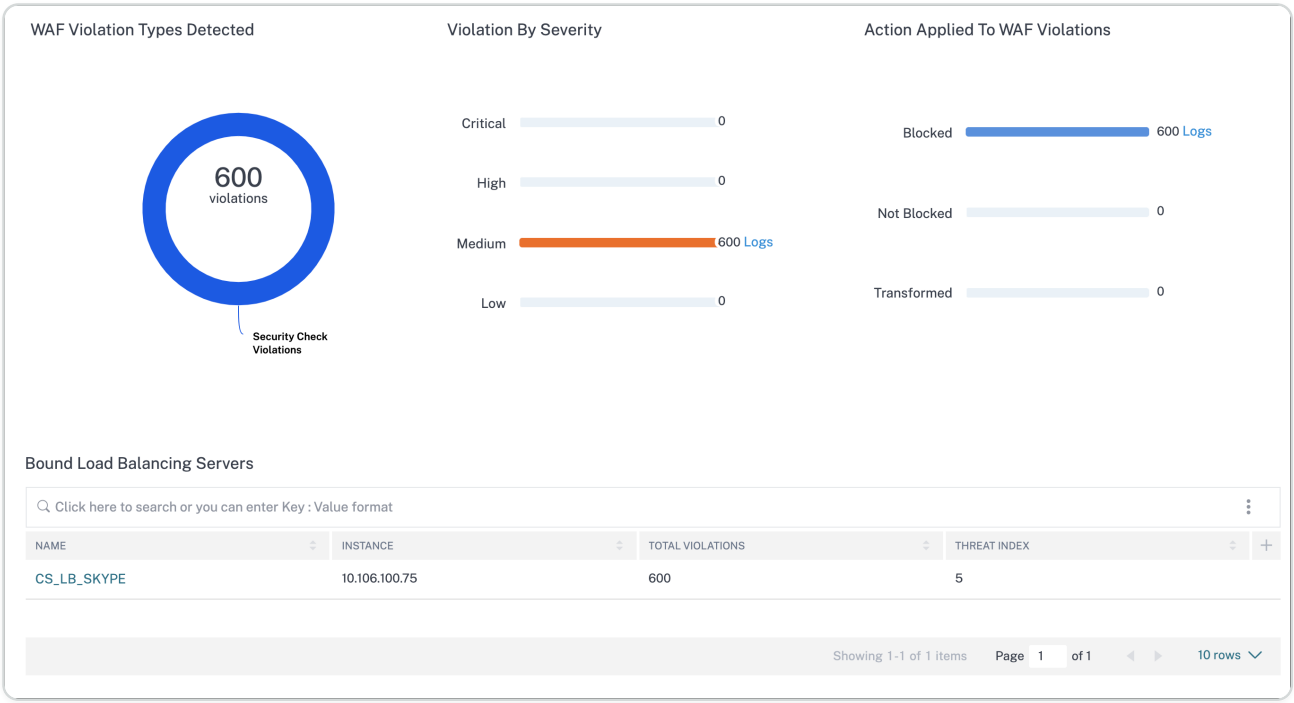
- **What Happened** – Indicates the total occurrences and the last occurred date and time.
- **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.



NOTE

Under **WAF** and **Bot**, you can view analytics for content switching virtual server that is bound with load balancing virtual servers. Click the content switching virtual server and under **Bound Load Balancing Server**, you can view the list of load balancing servers bound to the content switching virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View events history

Click the **Events** tab to view the bot and WAF events.

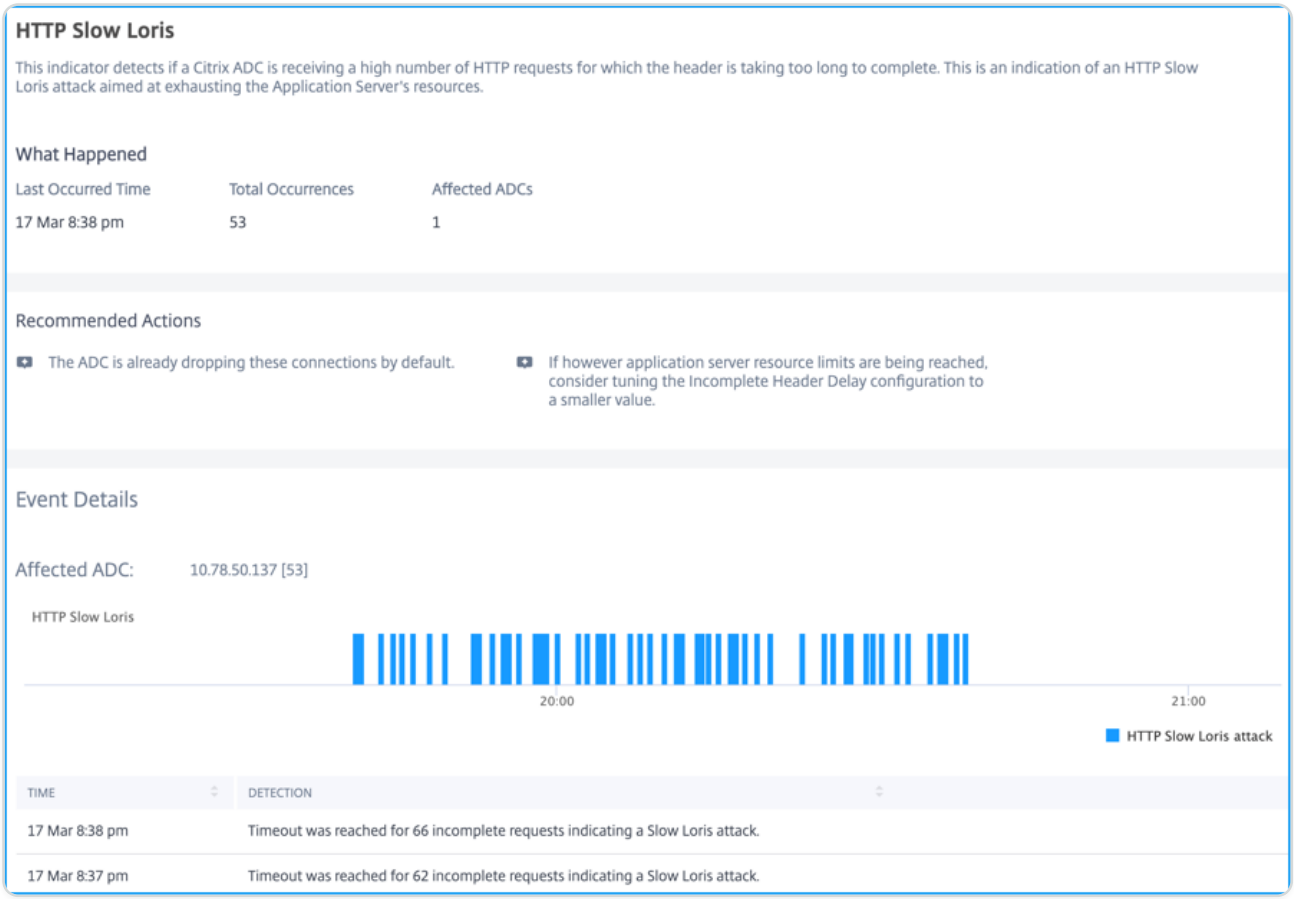
Network violation details

HTTP Slow Loris

Slow Loris is a denial-of-service attack that can send HTTP headers to the target application as slow as possible. The target application is forced to wait for headers arrival and can also quickly become unavailable to handle requests if multiple similar connections get opened. When a NetScaler instance receives a high volume of HTTP requests, the HTTP header increases and takes a long time to complete the requests. This process can exhaust application server resources and result in HTTP **Slow Loris** attack.

Using the **HTTP Slow Loris** indicator, you can analyze the requests that are resulted in **Slow Loris** attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue:

- Consider tuning the incomplete Header Delay (incompHdrDelay) configuration to a smaller value.
- By default, the NetScaler instance drops these incomplete requests.

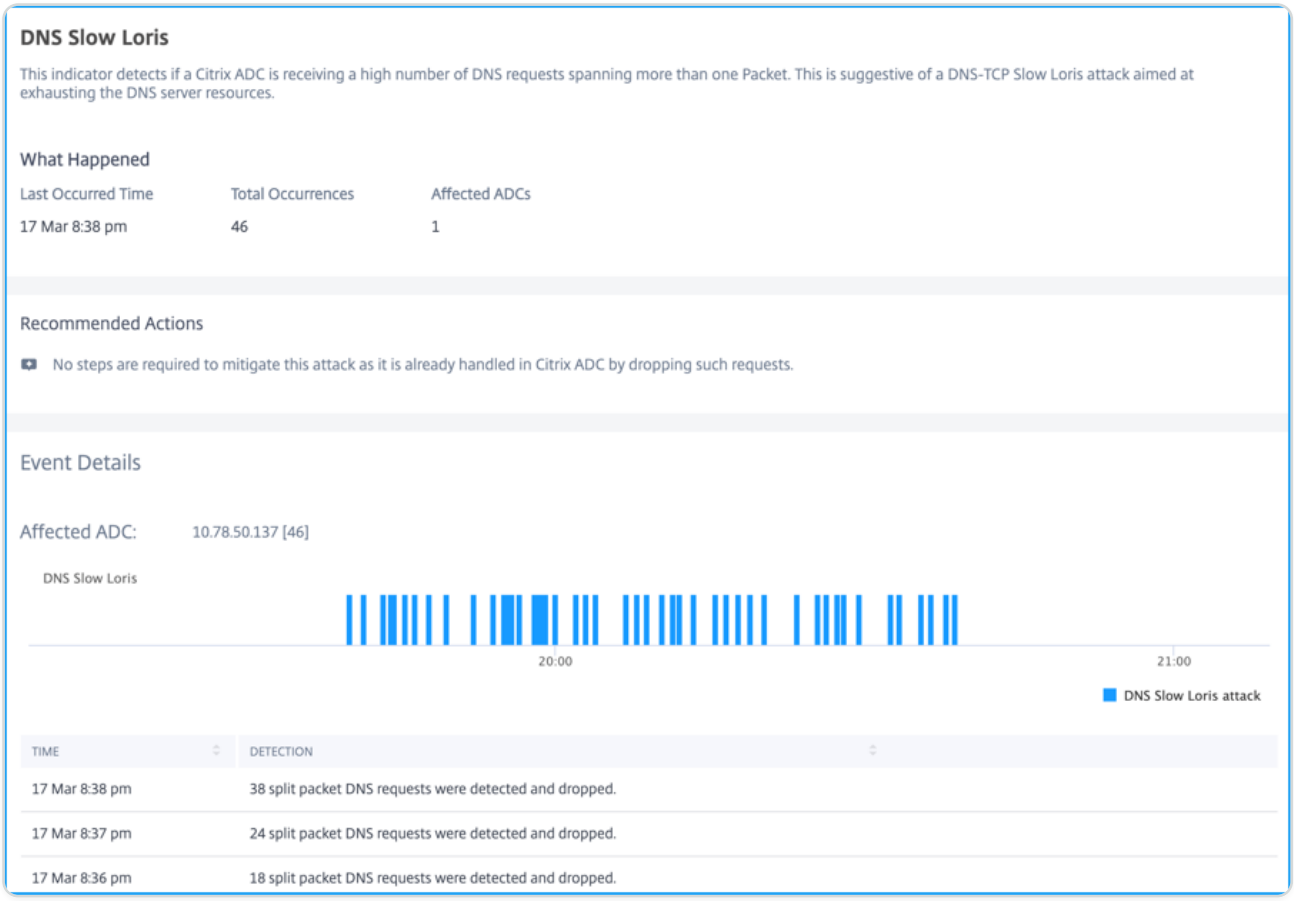
Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total incomplete requests as **Slow Loris** attack

DNS Slow Loris

The **DNS Slow Loris** indicator detects when a NetScaler receives a high number of DNS request spanning more than one packet. This process can exhaust DNS server resources and result in **DNS Slow Loris** attack. By default, NetScaler instance drops these **DNS Slow Loris** requests and no further action is required to troubleshoot this issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total DNS requests as **Slow Loris** attack

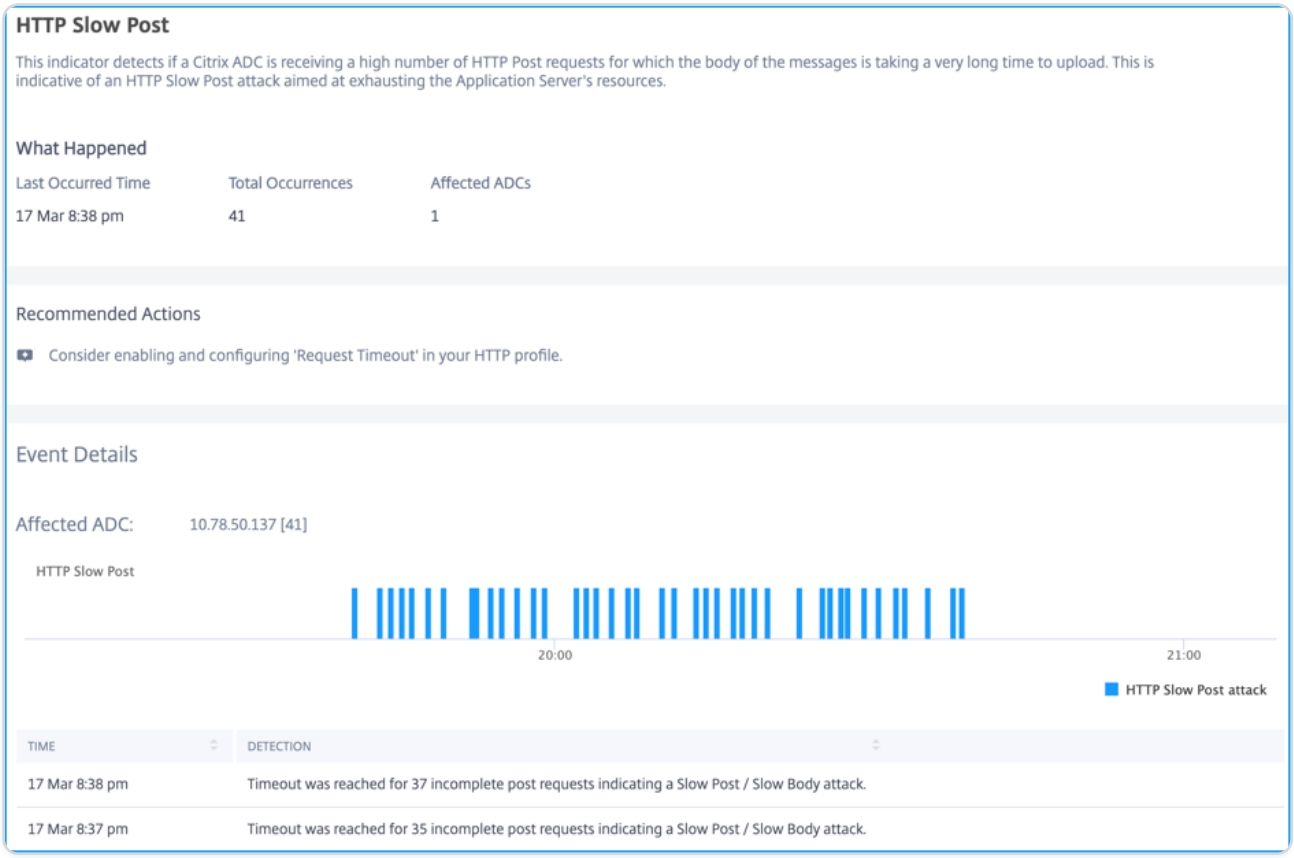
HTTP Slow Post

The Slow Post is a Denial-of-Service attack that can send HTTP POST headers to a target application. In the headers, the body message sizes are specified correct, but the message body is sent at a low speed. The target application is forced to wait and can also quickly become unavailable to handle requests if multiple similar connections get opened.

This process can exhaust application server resources and result in HTTP Slow Post attack.

Using the **HTTP Slow Post** indicator, you can analyze the requests that are resulted in slow post attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot this issue to enable and configure Request Timeout in NetScaler HTTP profile. For more information, see HTTP Configurations.

Under **Event Details**, you can view:

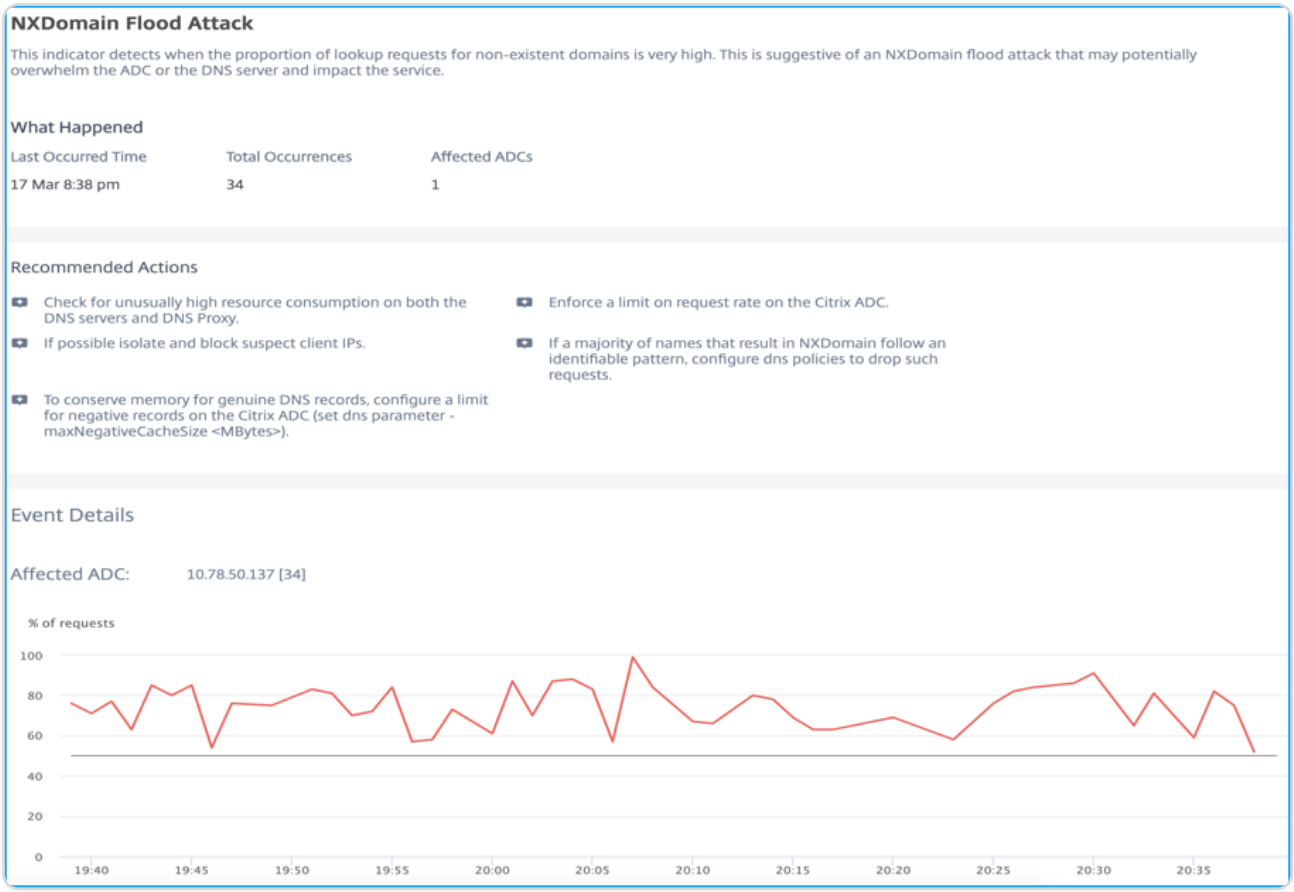
- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total POST requests as **Slow Loris** attack

NXDOMAIN Flood Attack

NXDOMAIN Flood Attack is a distributed denial-of-service (DDoS) attack that can target a DNS server or an ADC instance (that is configured as a DNS proxy server) and send a high volume of non-existence or invalid requests. This attack can impact the DNS server or ADC instance resulting in slowdown or requests not getting a response.

Using the **NXDOMAIN Flood Attack** indicator, you can analyze the requests that are resulted in NXDOMAIN attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue:

- Check for unusually high resource consumption on both DNS server and DNS proxy server.
- Enforce a limit for request rate on NetScaler instance
- Isolate and block suspect client IP addresses
- If most names result in NXDOMAIN, follow an identifiable pattern and configure DNS policies to drop such requests
- To conserve memory for genuine DNS records, configure a limit for negative records on NetScaler instance. For more information, see Mitigate DNS DDoS attacks.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations

HTTP Desync Attack

In an HTTP desync attack, a single HTTP request is interpreted as:

- A single request to the front-end server (virtual server)

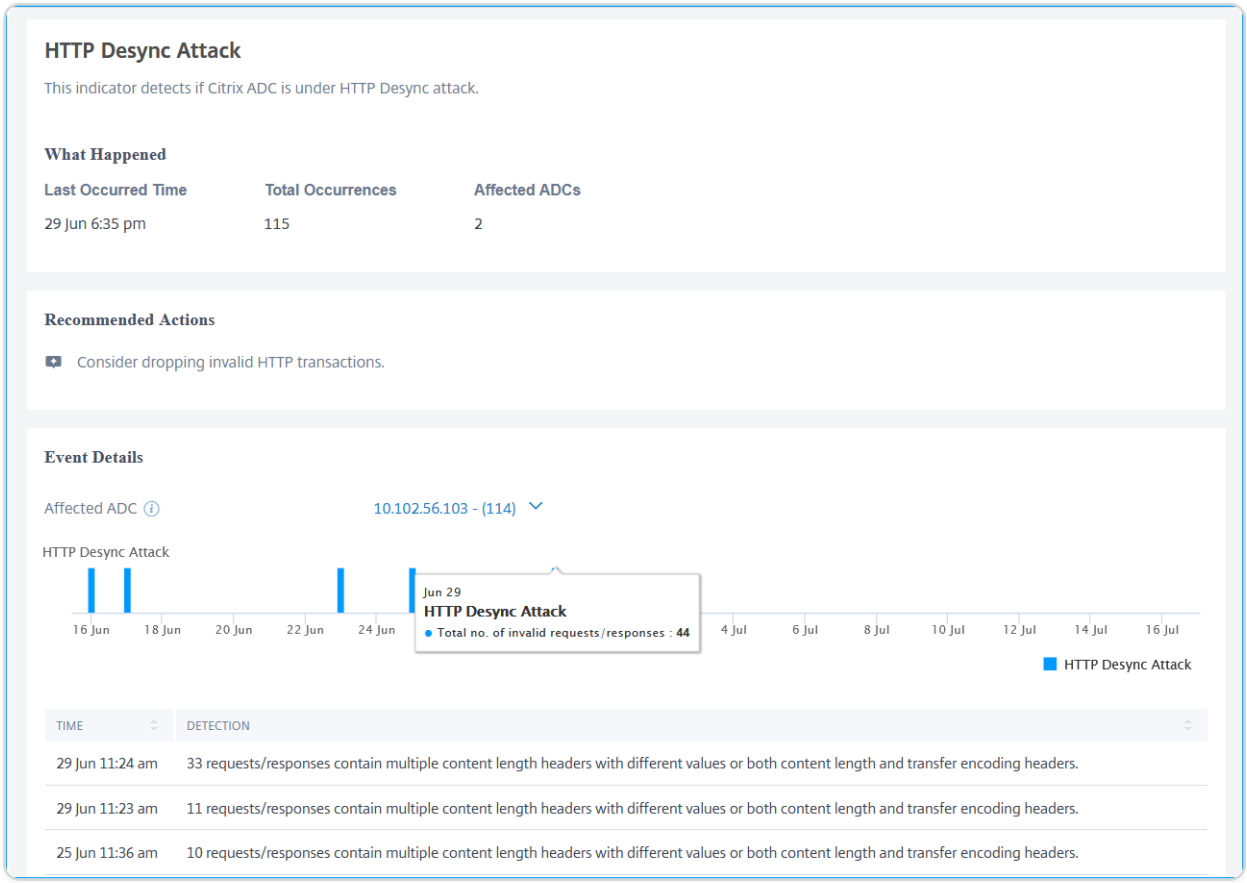
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 2 requests to the back-end server

In this scenario, the back-end server interprets the second request is from a different client. The connection between the virtual server and back-end server is reused for different requests. If the first client request is processed from a malicious client with some malicious data, the next client request can have a customized request. This activity can cause an attack by misusing the combination of two headers; content length and transfer encoding.

Using the **HTTP Desync Attack** indicator, you can analyze if the NetScaler instance might be under HTTP desync attack that has occurred due to the presence of:

- Content length and transfer encoding headers in a single HTTP transaction
- Multiple content-length headers with different values in a single HTTP transaction



The **Recommended Action** suggests you to consider dropping invalid HTTP transactions.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the violation details. Hover the mouse pointer on the bar graph to view the total invalid requests/reponses.

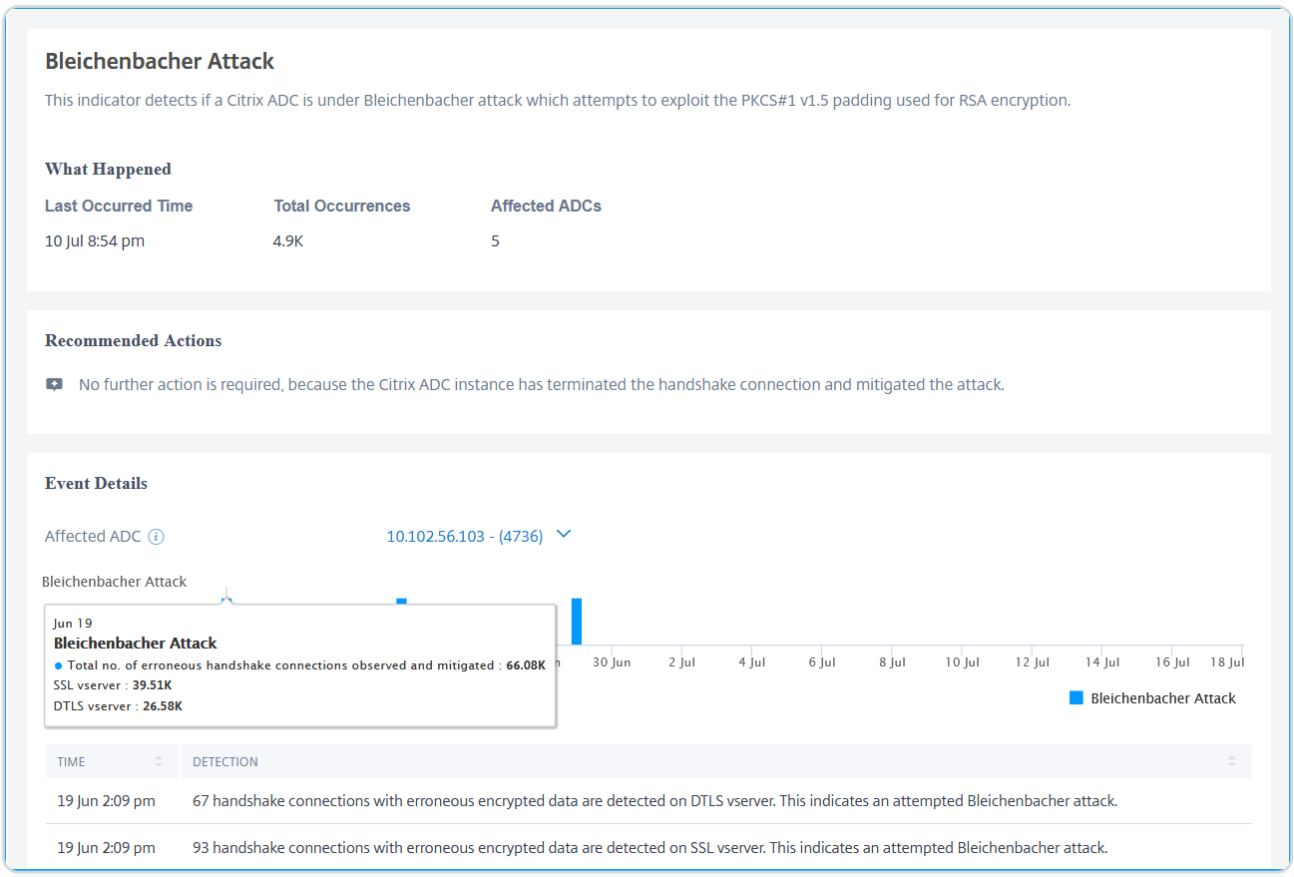
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The detection message for the violation, indicating the total requests/responses:
  - Containing multiple content-length headers with different values
  - Containing both content length and transfer encoding headers

Bleichenbacher Attack

NetScaler instance detects if a given sequence of bytes of an encrypted message has the correct padding format upon decryption.

Using the **Bleichenbacher Attack** indicator, you can analyze if the NetScaler instance receives any SSL/TLS handshake connections with erroneous encrypted data.



The **Recommended Action** indicates no further action is required because the NetScaler instance terminates the handshake connections and mitigates this attack.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the violation details. Hover the mouse point on the bar graph to view the total erroneous handshake connections detected.

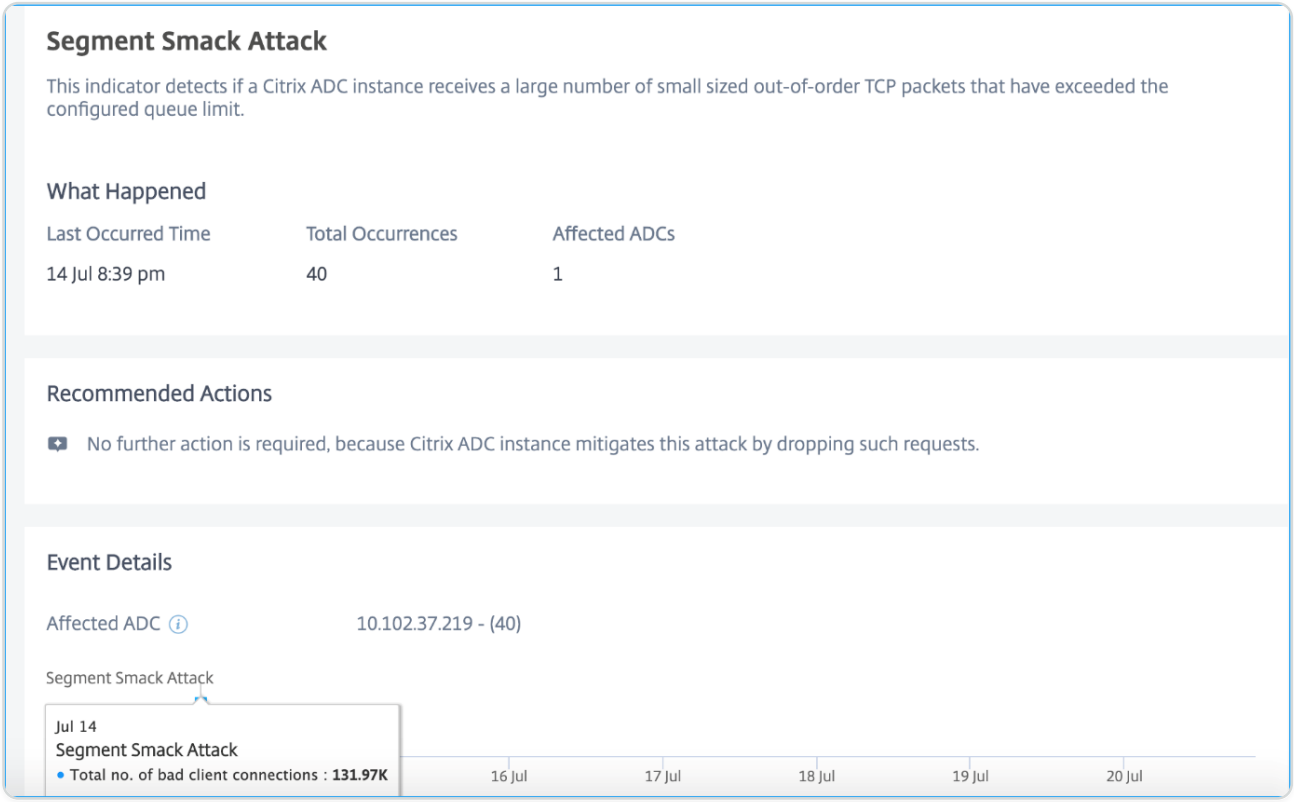
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The detection message for the violation, indicating the total handshake connections on the virtual server with erroneous encrypted data.

Segment Smack Attack

A **Segment Smack Attack** is a Denial of Service (DoS) attack, in which the attacker can send unordered small-sized packets during a TCP session. These customized TCP packets can affect the CPU and Memory, and result in a denial of service on the NetScaler instance.

Using the **Segment Smack Attack** indicator, you can analyze if a NetScaler instance has received a large number of TCP packets than the configured queue limit. For more information, see TCP configuration.

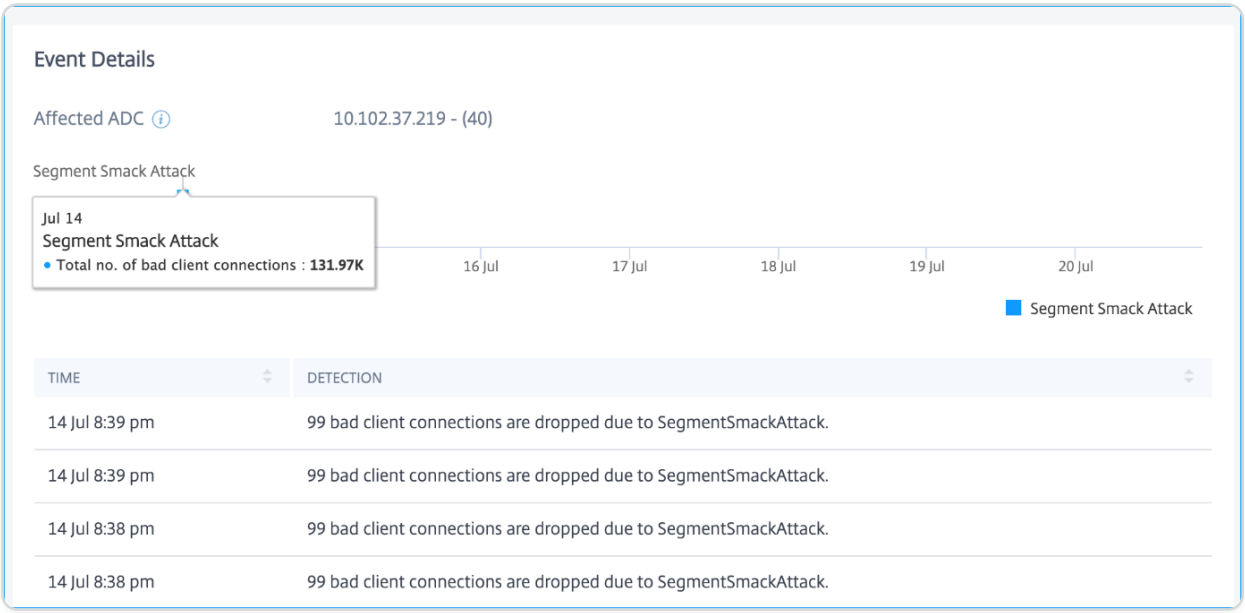


As an administrator, no further action is required because the NetScaler instance mitigates this attack by dropping all those excess TCP packets.

Under **Event Details**, you can view:

- The affected NetScaler instance
- The graph indicating the violation details. Hover the mouse point on the bar graph to view the total number of bad client connections detected.
- The detection message for the violation, indicating the total client connections dropped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



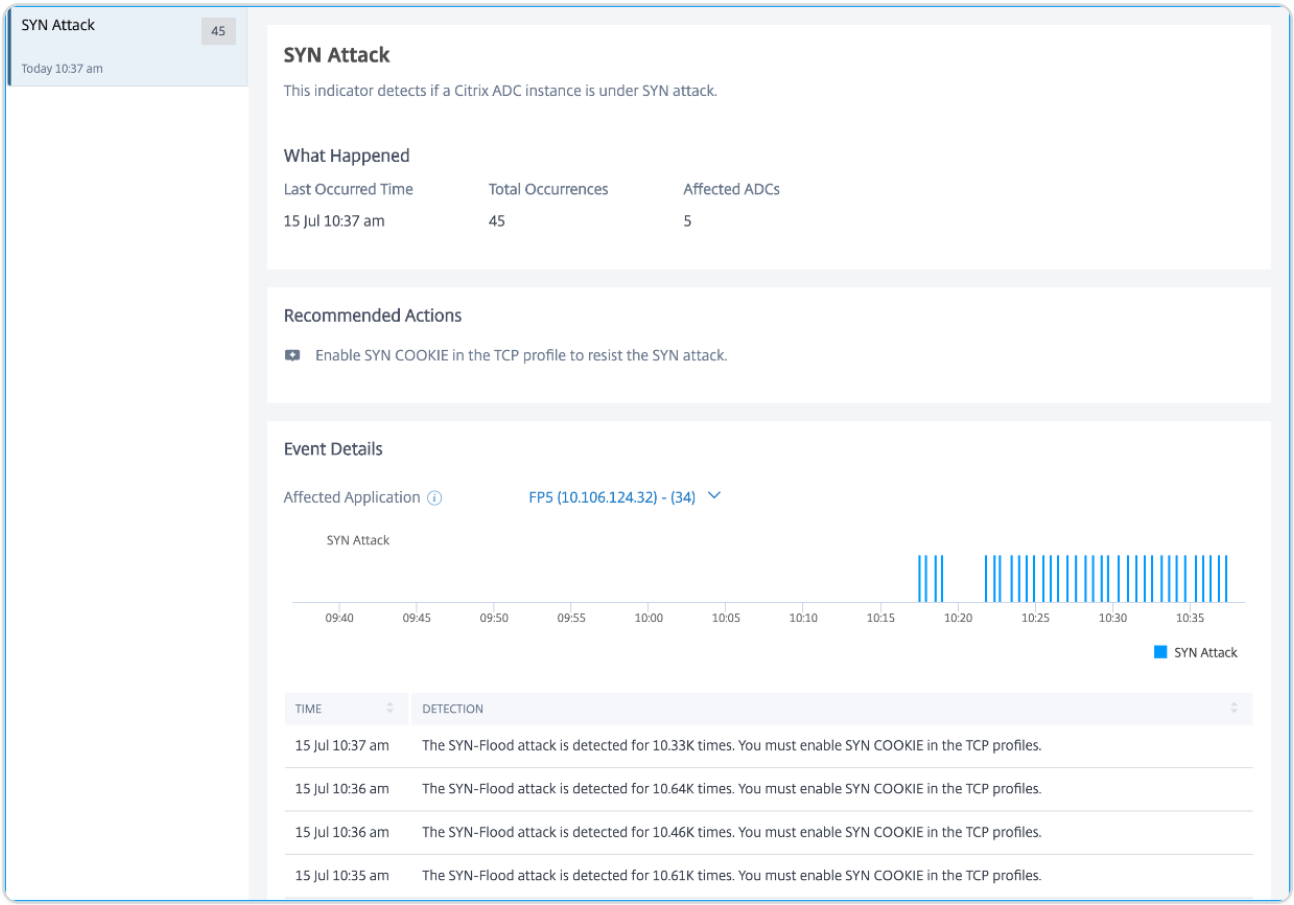
SYN Flood Attack

A SYN Flood Attack is a Denial of Service (DoS) attack that can affect the target machine, by sending thousands of connection requests using spoofed IP addresses. When a NetScaler instance is under a SYN Flood attack, the instance attempts to open a connection for each malicious request and then wait for an acknowledgment packet that never arrives.

The **SYNCOOKIE** in the TCP profile prevents SYN attacks on the NetScaler appliance. By default, the **SYNCOOKIE** on the ADC instance is enabled. The possibility for the NetScaler instance under a SYN flood attack is high only when SYNCOOKIE is disabled.

Using the **SYN Flood Attack** indicator, you can analyze if the NetScaler instance is under SYN attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



As an administrator, the **Recommended Action** suggests you to enable SYN COOKIE in the TCP profile.

Under **Event Details**, you can view:

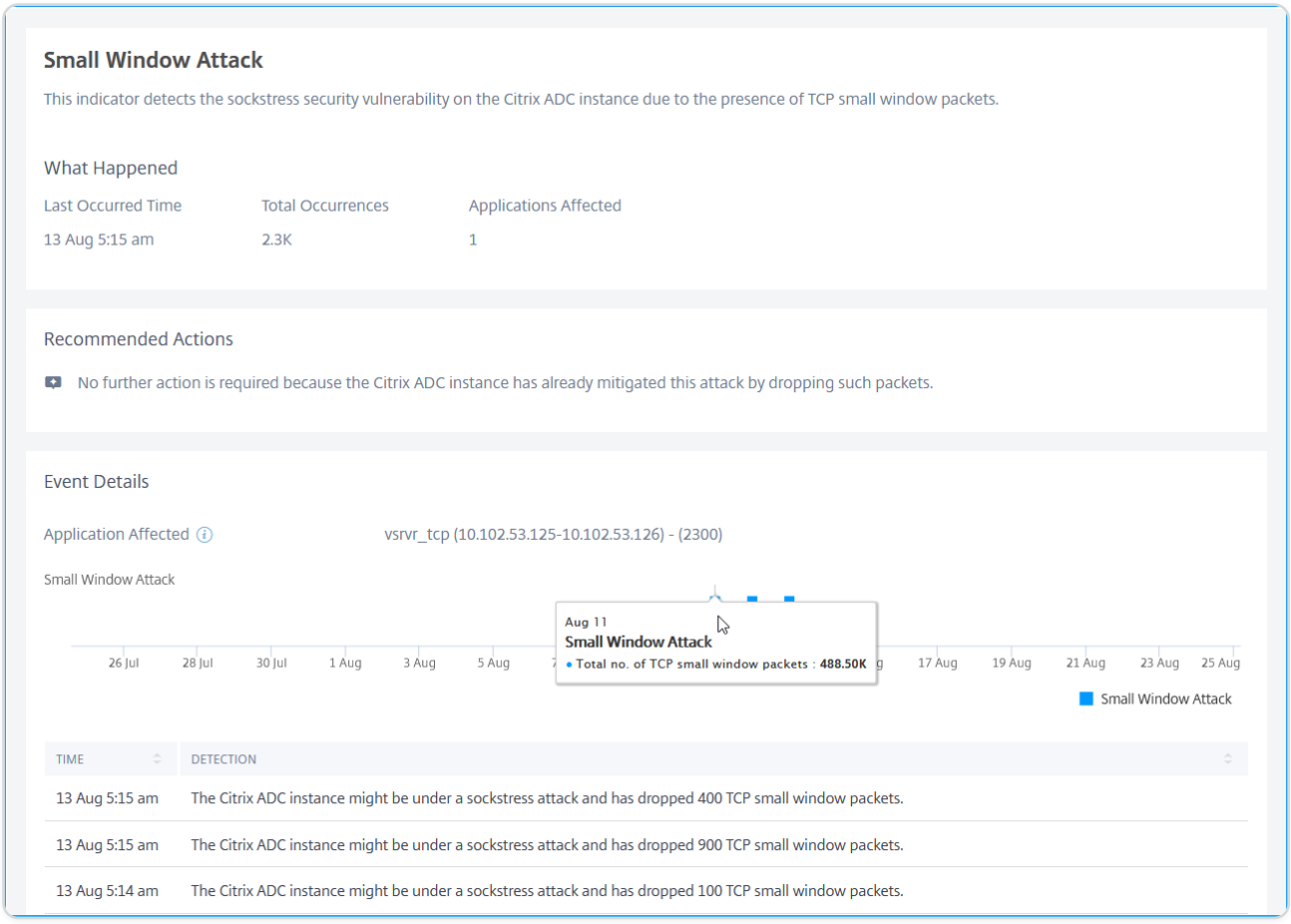
- The affected application. You can also select the application from the list if two or more applications are affected with this violation
- The graph indicating the SYN attack details
- The detection message, indicating the total number of times that the application is detected with SYN attack

Small Window Attack

A Small Window Attack is a Denial of Service (DoS) attack that can affect the target machine, by sending thousands of TCP packets with either smaller size window or window size 0. The window size 0 indicates that the target machine has to stop sending any more data until further notice. By sending as much as similar connections to the target machine, the target machine memory gets utilized to the maximum and becomes unresponsive.

Using the **Small Window Attack** indicator, you can analyze if the NetScaler instance is under the sockstress attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



By default, NetScaler instance mitigates this attack by dropping all such TCP small window packets. Hence, as an administrator, no further action is required.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the attack details. Hover the mouse point on the bar graph to view the total number of TCP small window packets detected.
- The detection message indicating the total TCP small window packets dropped.

SSL Insight

SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler by providing integrated and real-time and historic monitoring of secure web transactions. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 has transactions running on low security protocols, ciphers, or weak key strength.

When SSL Analytics is enabled on a NetScaler 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 NetScaler Application Delivery Management (ADM) Analytics.

SSL Insight provides the following critical information, which is displayed by NetScaler® ADM Analytics:

- SSL Protocol version negotiated
- Cipher negotiated, and the cipher strength
- Signature Hash algorithm of the certificate used
- Certificate Type & Size
- SSL Front-end and Back-end errors

NOTE

For successful SSL connections, SSL AppFlow® logging happens at the end of every transaction.

Prerequisites

- The NetScaler instance on which you intend to configure SSL Insight must be running NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The NetScaler ADM version and build must be equal to or higher than the NetScaler version and build. For example, if you have installed NetScaler ADM 11.1 build 61.7, then ensure you have installed NetScaler 11.1 build 60.14 or earlier.

Configure SSL Insight

SSL Insight Metrics are included in Web Insight reports if you enable the following elements:

- Enable AppFlow for Web Insight on each NetScaler instance.
- Enable ULFD mode on each NetScaler instance.
- Enable required AppFlow parameters on each NetScaler instance.

Enable the AppFlow feature

NOTE

You can enable the AppFlow feature either from NetScaler ADM or from each NetScaler instance.

To enable the AppFlow feature from NetScaler ADM:

If your NetScaler ADM is **13.0 Build 41.x or later**:

1. Navigate to **Infrastructure > Instances > NetScaler**, and select the instance type. For example, VPX.
2. Select the instance and from **Select Action** list, click **Configure Analytics**.
3. On the **Configure Analytics on Virtual Server(s)** page, select the virtual server, and click **Enable Analytics**.
4. On the **Enable Analytics** window:
   a. Select **Web Insight**
   b. Select **Logstream** as Transport Mode

   NOTE

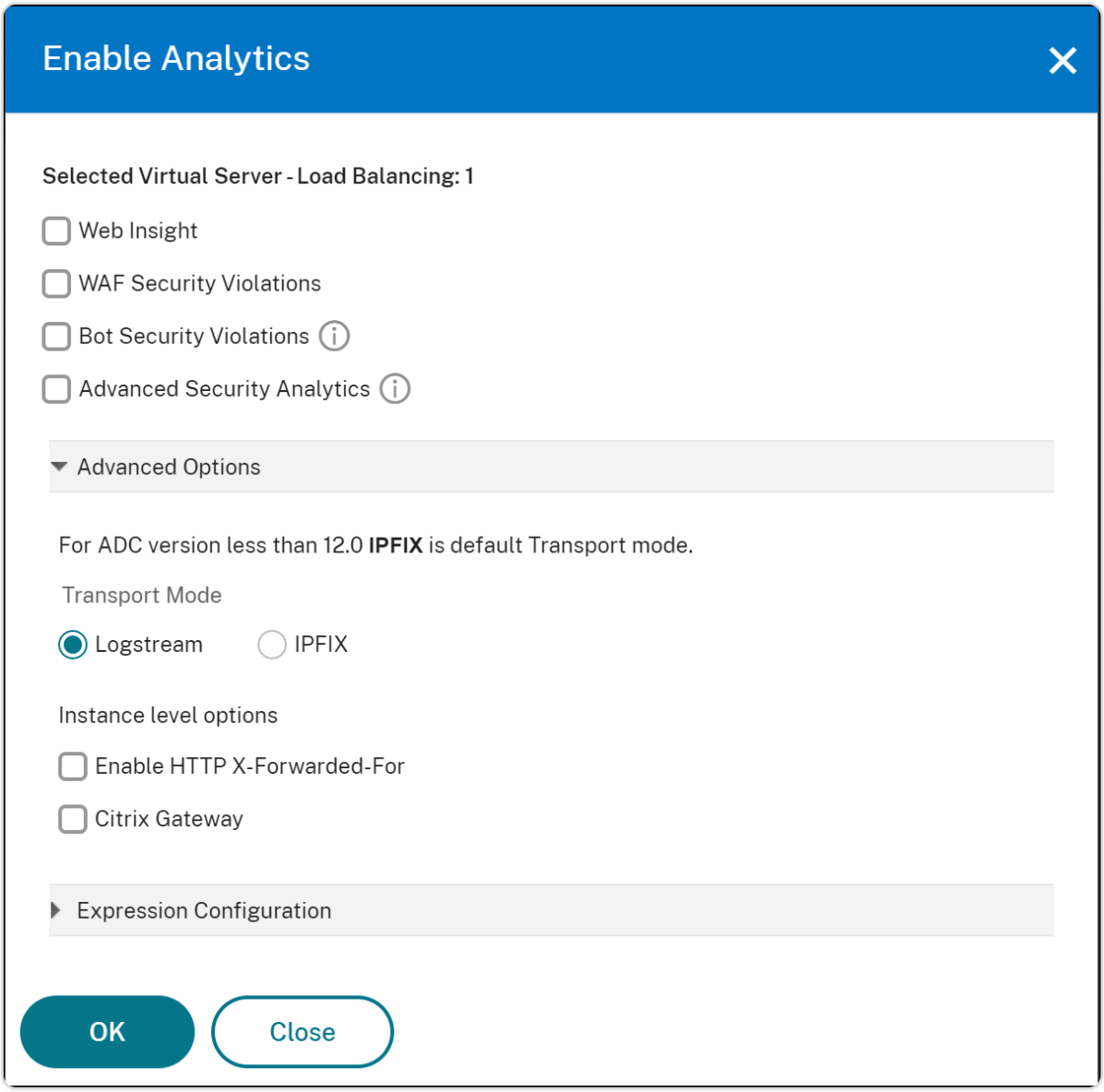
   For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about IPFIX and Logstream, see Logstream overview.

c. The Expression is true by default

d. Click **OK**



NOTE

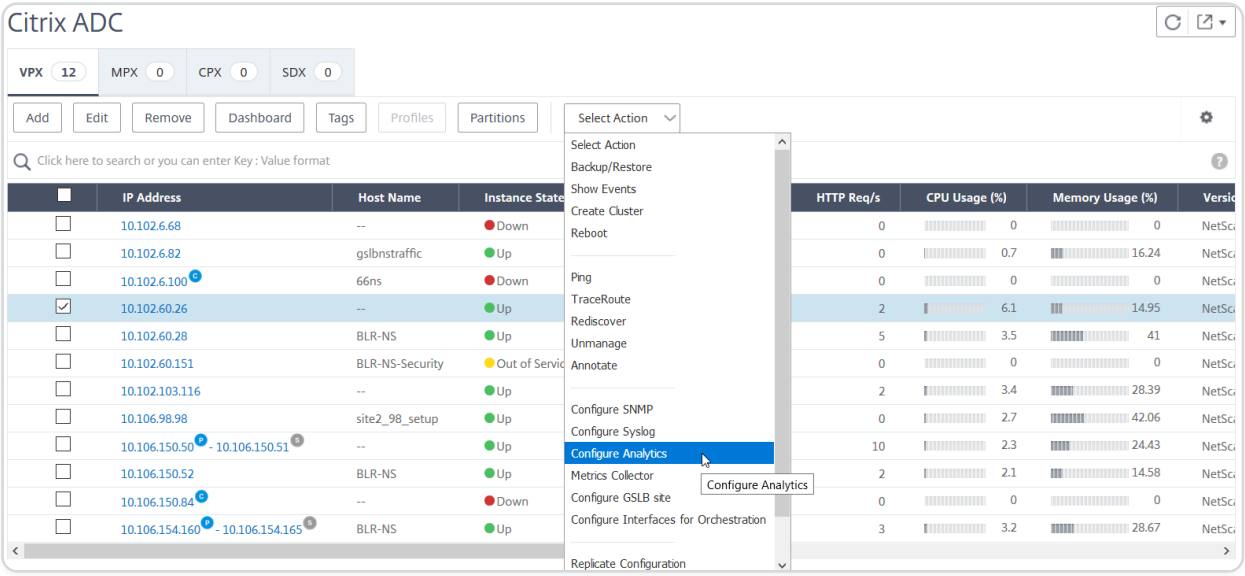
- If you select virtual servers that are not licensed, then NetScaler ADM first licenses those virtual servers and then enables analytics
- For admin partitions, only **Web Insight** is supported
- For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you click **OK**, NetScaler ADM processes to enable analytics on the selected virtual servers.

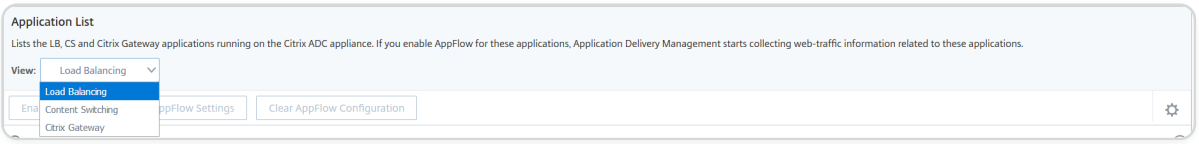
If your NetScaler ADM is **13.0 Build 36.27 or earlier**:

1. Navigate to **Infrastructure > Instances > NetScaler**, and select the NetScaler instance on which you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.

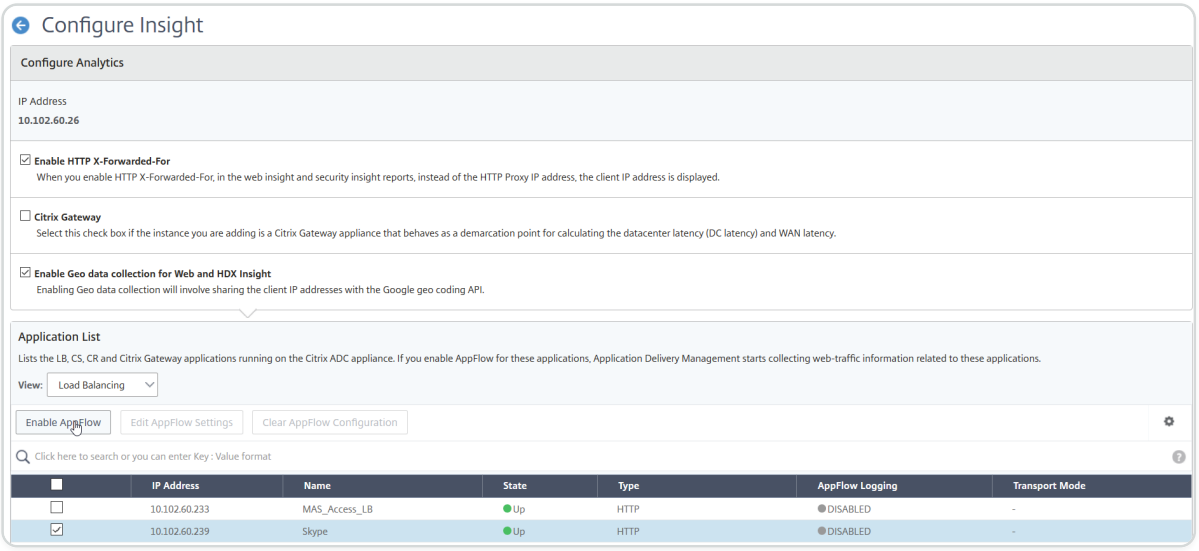


3. On the **Configure Insight** page:

   a. Select the **Application List** for either Load Balancing or Content Switching.



   b. Select the virtual server and click **Enable AppFlow**.



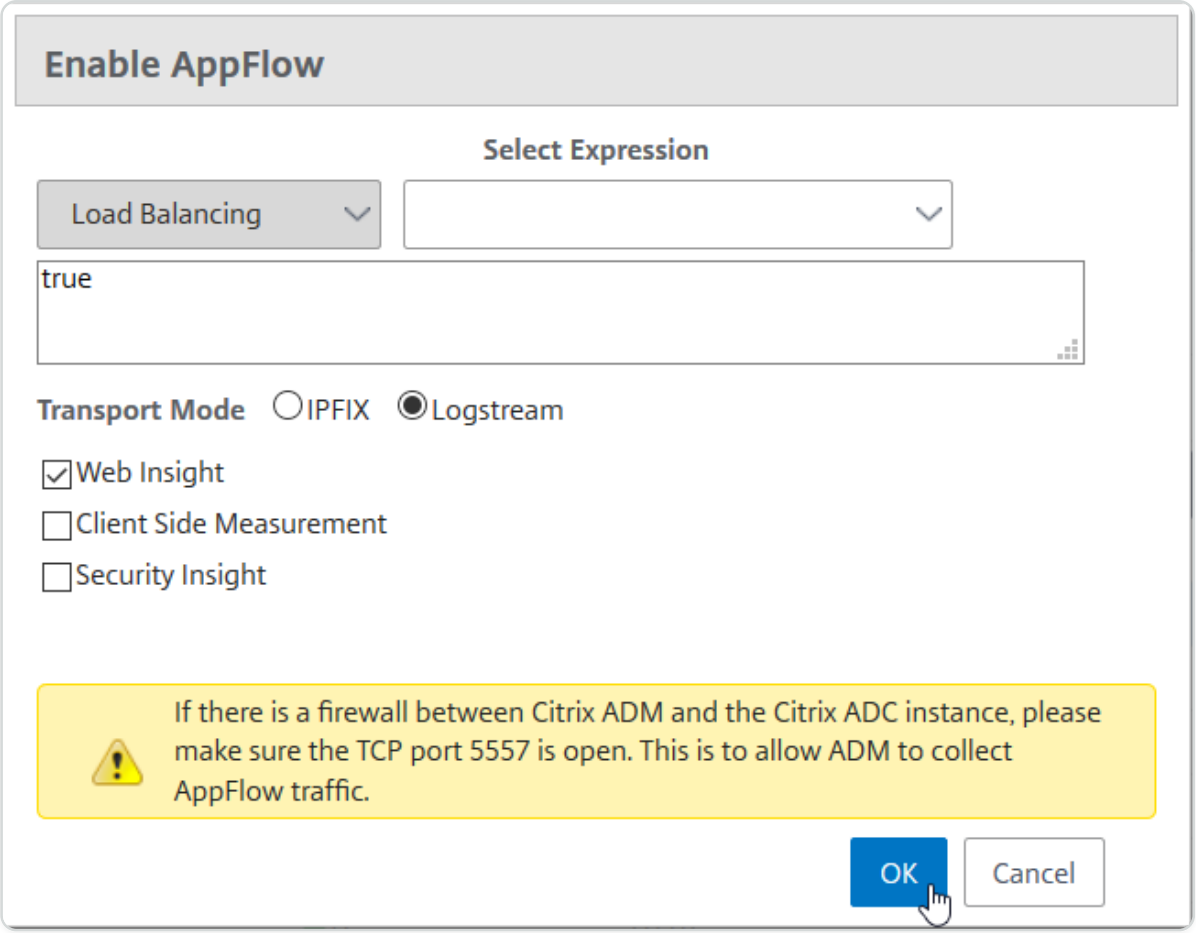
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **Web Insight** and click **OK**.



To enable the AppFlow feature by using the NetScaler GUI:

In a NetScaler instance's GUI, navigate to **Configuration** \> **System** \> **Settings**, click **Configure Advanced Features**, and select **AppFlow**.

Enable SSL Insight parameters

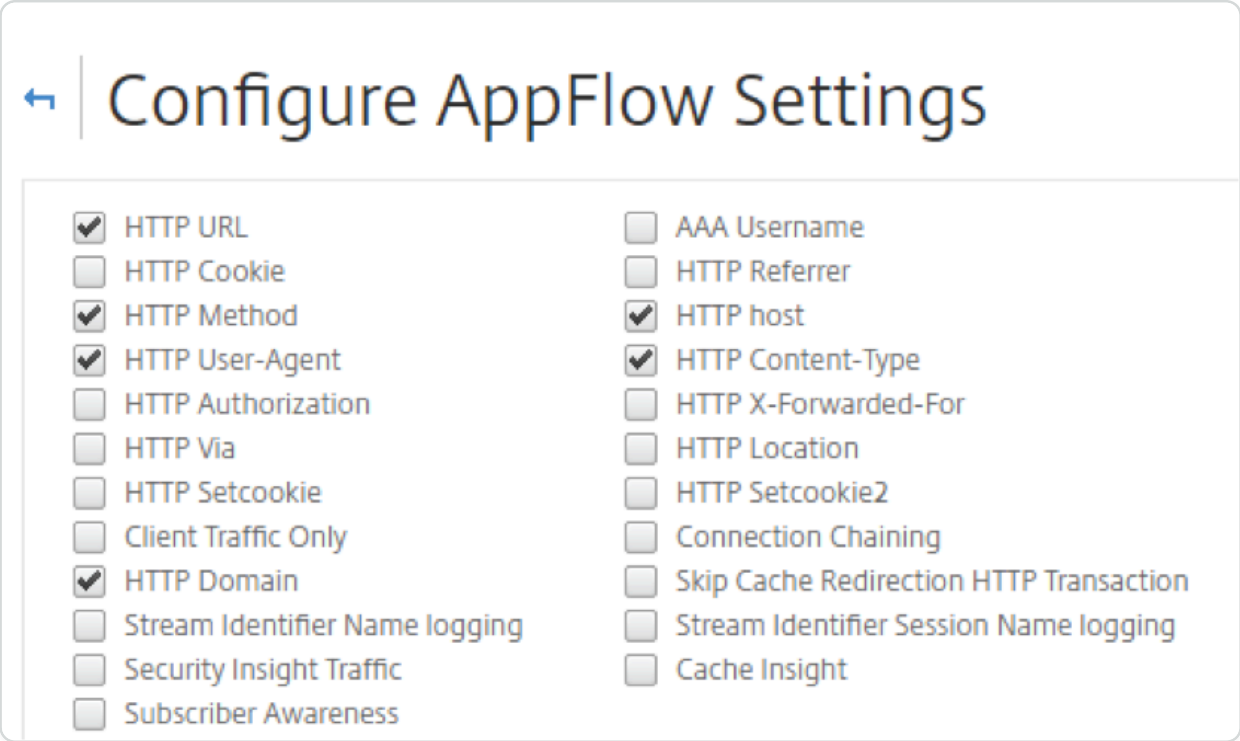
On each NetScaler instance, you have to enable some HTTP parameters to display SSL Insight records in NetScaler ADM.

To enable SSL Insight parameters from the NetScaler configuration utility:

1. Navigate to **Configuration** \> **System** \> **AppFlow**, and click **Change AppFlowSettings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the following check boxes: **HTTP Domain**, **HTTP Host**, **HTTP Method**, **HTTP URL**, **HTTP User-Agent**, **HTTP Content-Type**.
3. Click **OK**.



View the SSL Insight metrics

SSL Insight metrics in NetScaler ADM provide a detailed view of the performance of the SSL transactions served by the NetScaler 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 **NetScaler HTTPS** settings and SSL-certificate settings, and track performance issues.

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler ADM analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

To monitor SSL Insight Metrics in NetScaler ADM:

You can view SSL metrics for:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An application. Navigate to **Applications > Dashboard**, click an application, and select **Web Insight** tab to view the detailed metrics. For more information, see Application Usage Analytics.
- All applications. Navigate to **Applications > Web Insight** and click **Applications** and **Clients** tabs to view the SSL metrics.

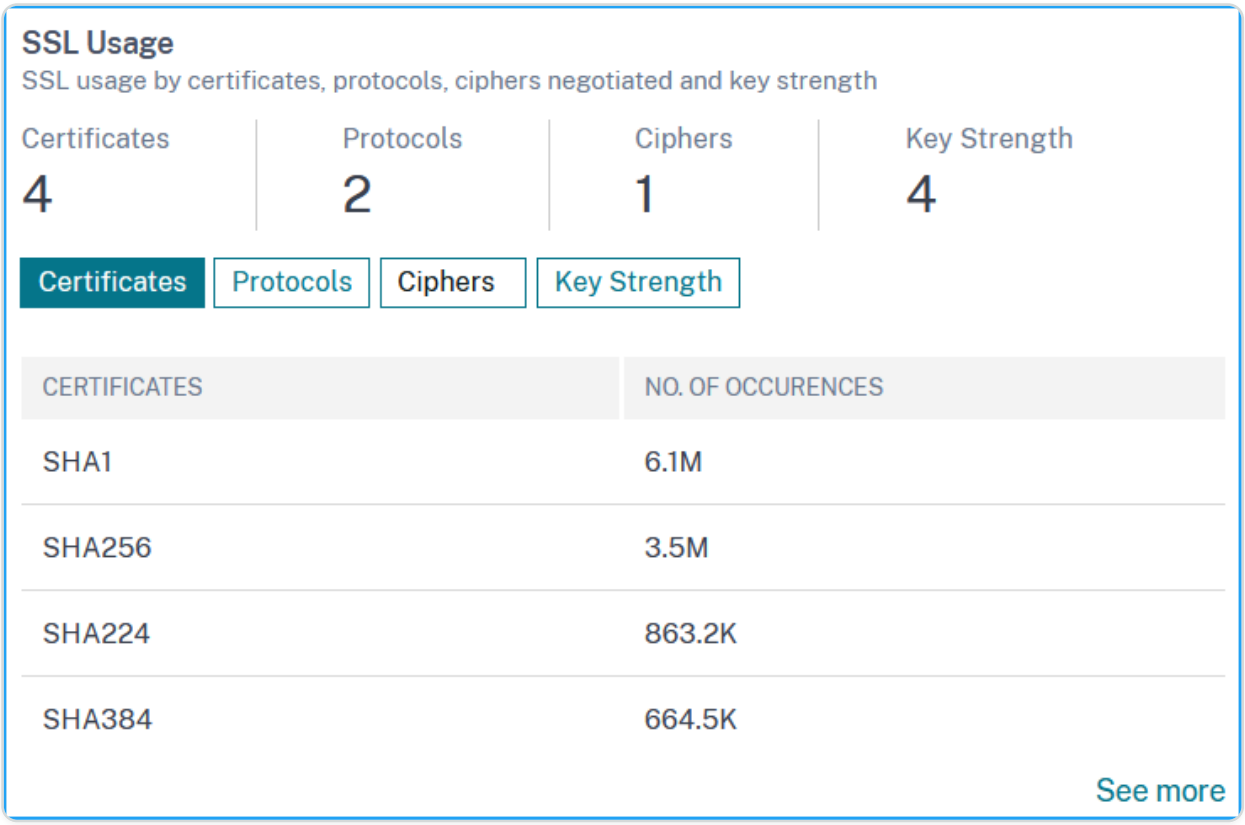
Use case: Obtain an overview of the SSL transactions

The following use case describes how you can use SSL Insight to assess the usage of various SSL Parameters and improve security measures.

Consider that you have a set of applications that are using SSL transactions (HTTPS) for communication, and you have configured NetScaler 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 **Web Insight** dashboard for an application or all applications provides a summary of following SSL parameters under **SSL Errors** and **SSL Usage**:

- SSL Certificates
- SSL Protocols
- SSL Cipher
- SSL Key Strength
- SSL Failure – Front end
- SSL Failure – Back end

© 1997–2026 Citrix Systems, Inc. All rights reserved.



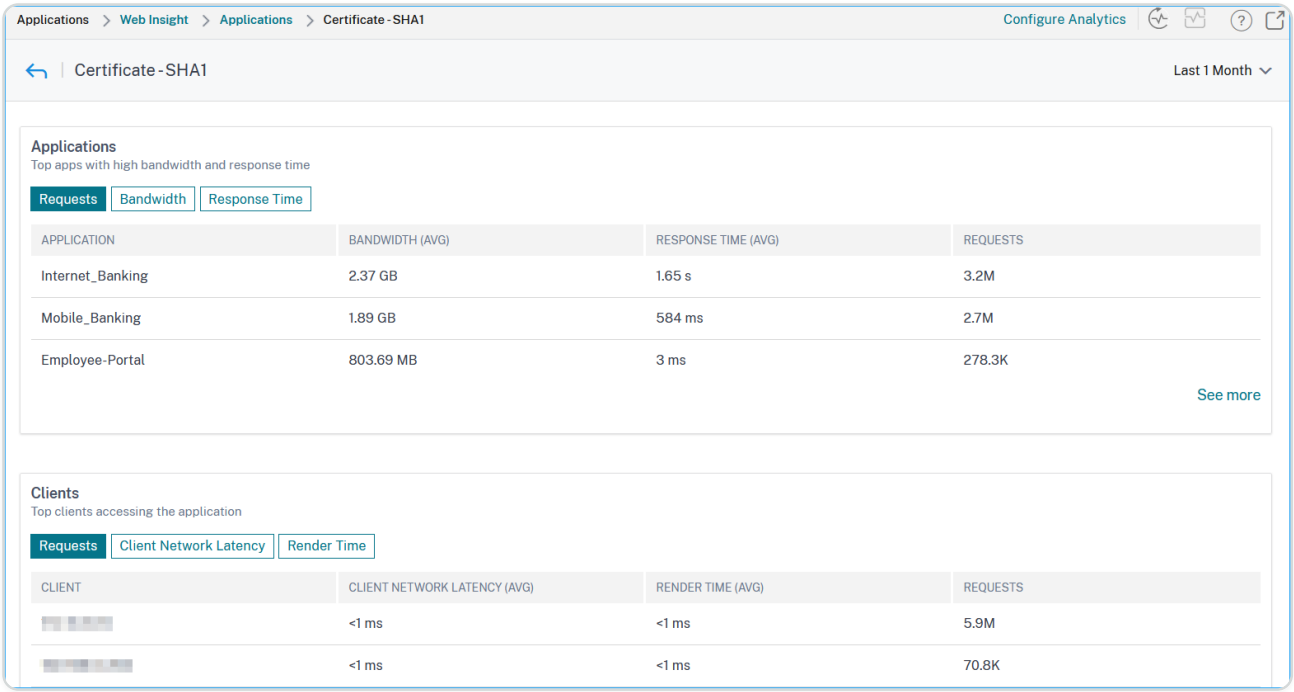
You can click each tab to view details.

Use case: SSL metrics for clients

You can see list of clients (identified by their IP addresses) and the total occurences per client. Navigate to **Applications > Web Insight** and select the **Clients** tab to view the details under **SSL Usage**.

Click a metric to view details and under **Clients**, click any client IP address to view the SSL metrics for the selected client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



TCP Insight

The TCP Insight feature of NetScaler 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 NetScaler 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 NetScaler instances and validate the benefits of TCP Optimization. Breakdowns by stream direction (from client to NetScaler and NetScaler to origin server), TCP port, and virtual LAN are provided for the above metrics.

Prerequisites

Before you begin configuring the TCP Insight feature, make sure that the following prerequisites are met:

- The NetScaler instances are running on software version 11.1 build 51.21 or later.
- You have installed NetScaler 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 NetScaler® ADM.For information about NetScaler ADM licensing, see Licensing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling TCP Insight

Before you can view the TCP Insight metrics, you must enable the feature on NetScaler ADM.

To Enable TCP Insight:

1. In a web browser, type the IP address of the NetScaler ADM virtual appliance (for example, `<http://192.168.100.1>`).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Settings > Analytics Settings**, and click **Enable Features for Analytics**.
4. On the **Enable Features for Analytics** page, select **Enable TCP Insight**.
5. In the confirmation window, click **OK**.

View the TCP Insight metrics in NetScaler ADM

After enabling TCP Insight in NetScaler 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 NetScaler ADM:

Navigate to **Infrastructure > TCP Insight**.

You can hover your mouse pointer on the bar graphs to view the data volume of the corresponding transport techniques. Also you can view the data volume, and other metrics, in the table below the graph.

NOTE

You can customize the metrics displayed in the graph by using the settings icon on the table. You can also select the time period to which the metrics pertain, and use the time slider adjust the time period.

You can also view metrics for such things as interfaces, ports, and bit rates by selecting from the **TCP Insight** list.

Use cases

The following use cases illustrate some of the ways to use TCP Insight on NetScaler appliances:

- Assess benefits of TCP optimization

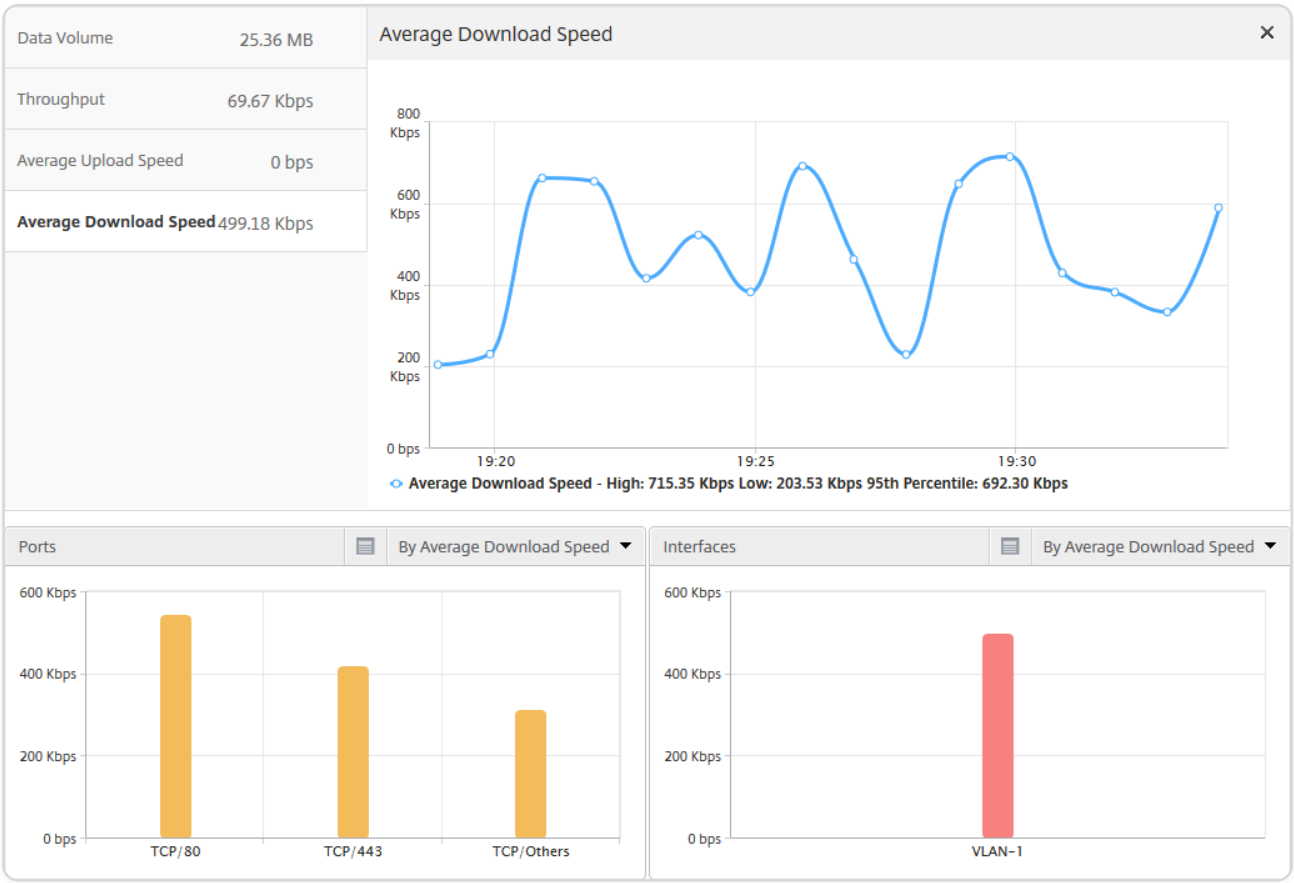
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tune TCP parameters
- Measure impact of TCP optimization on traffic volume

Assess benefits of TCP optimization

How much does NetScaler 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 NetScaler 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.



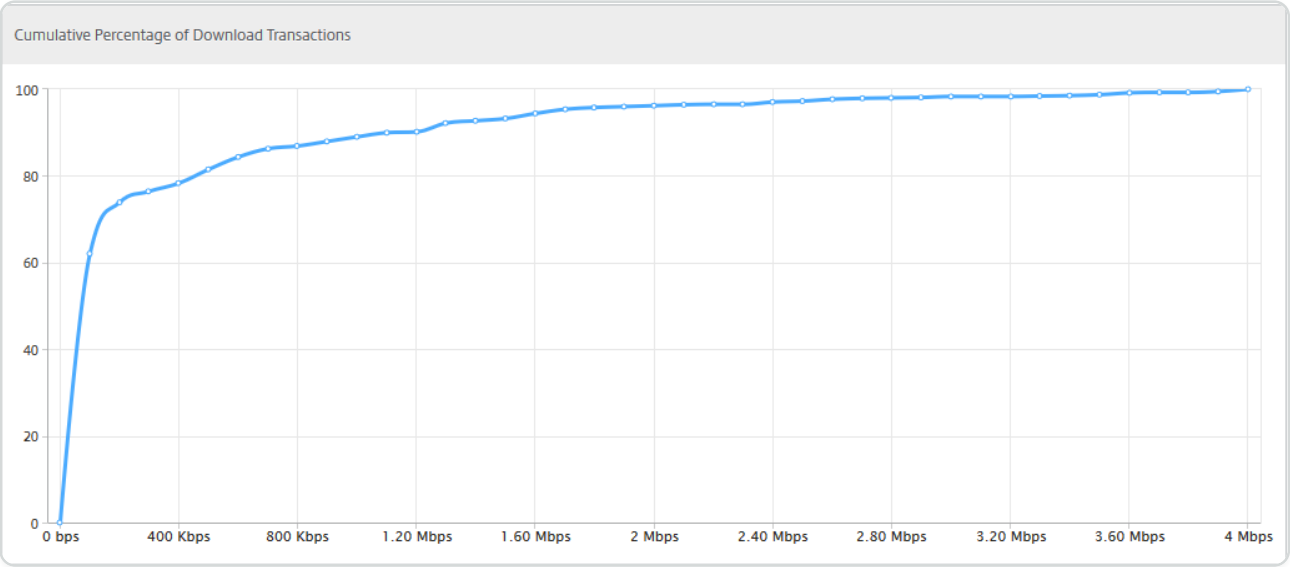
Tune TCP parameters

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 NetScaler is running different TCP optimization profiles. You can use the results to tune TCP parameters for faster

© 1997–2026 Citrix Systems, Inc. All rights reserved.

transmission, and develop a TCP profile that maximizes the user-perceived experience in a specific customer network.

To view the reports, log on to NetScaler ADM. Then, on the **TCP Insight** tab, click **Bitrates**, and select the desired bitrate from the bar graph or the table below the graph.



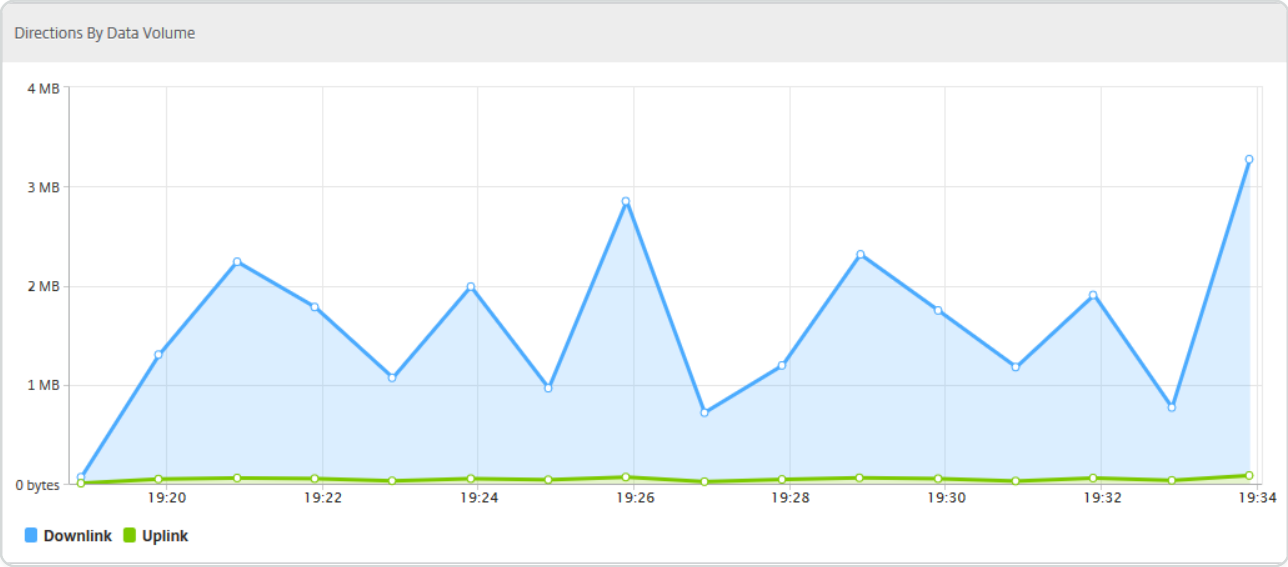
Measure impact of TCP optimization on traffic volume

Measurements of IP-layer Data Volume/Throughput handled by a NetScaler 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 NetScaler 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshoot Web Insight issues

In the Web Insight dashboard, you can visualize your application usage and monitor all applications that the NetScalers serve. Using Web Insight, the NetScalers send HTTP and SSL transaction data to the NetScaler ADM configured as an AppFlow collector. AppFlow is the flow export standard used to identify and collect application and transaction data in the network infrastructure.

This document helps you troubleshoot common Web Insight deployment issues.

Diagnostics for no data

If Web Insight does not show any data, ensure that **Web Insight** is enabled for the virtual server. For more information, see Manage licensing and enable analytics on virtual servers.

A notification with **Diagnotics for no data** is also visible if there is no data in Web Insight. You can click to view details for troubleshooting.

Issues related to Web Insight dashboard reports

If the NetScaler® ADM Web Insight dashboard (**Applications> Web Insight**) fails to display reports, the issue might be one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Web Insight configuration issue
- Connectivity issue between NetScaler and NetScaler ADM
- AppFlow data is not received from NetScaler
- License issue
- Observation point ID issue
- Missing AppFlow® parameters issue

Configuration issue

Complete the following steps to troubleshoot this issue:

1. Ensure the AppFlow feature is enabled in the NetScaler instance. For details, see Enabling AppFlow.
2. Check the Web Insight configuration in the NetScaler:
   a. Run the `show running | grep -i <appflow_policy>` command to check the Web Insight configuration on policy. Ensure the bind type is `REQUEST`. For example: `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
   b. Run the `show appflow action` command to check the Web Insight configuration on action. Ensure the `-webinsight` option is enabled
   c. Check the `appflowlog` parameter in LB/CS/CR virtual server, along with the bound services and servicegroups. Ensure this parameter is enabled in both virtual server, and bound services and servicegroups.

Connectivity issue between NetScaler and NetScaler ADM

Complete the following steps to troubleshoot this issue:

1. Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
2. On the NetScaler GUI, check if the AppFlow policies are getting hits. Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits. You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
3. Ensure that the firewall is not blocking the AppFlow data from NetScaler to NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AppFlow data not received from NetScaler

Complete the following steps to troubleshoot this issue:

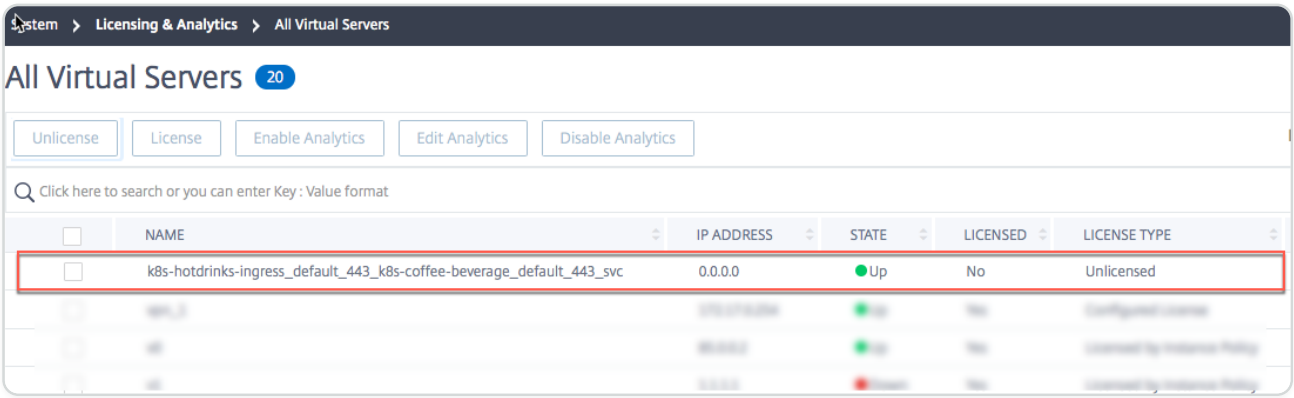
1. Ensure that there are no AppFlow configuration and connectivity issues. For more information, see the solution sections in this topic for configuration issue and connectivity issue between NetScaler and NetScaler ADM.
2. On the NetScaler, on shell prompt, run the `nsconmsg -g appflow_tmpl -d current` command and check the following counters:

   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   If any of the counters are missing, take a trace on the NetScaler. Next, confirm the transaction is complete and the response is being served from the origin server. If the transaction is complete and some counters are missing, contact the support team.

License issue

With this issue, the license for the particular virtual server for which you want to view the Web Insight report appears “No” under **Settings > Licensing & Analytics Configuration > Configure License**.



Complete the following steps to troubleshoot this issue:

1. In the NetScaler, ensure that the AppFlow policy hits are increasing and the instance is sending AppFlow records to ADM.
2. Check if the corresponding virtual server is licensed. If the virtual server is not licensed, NetScaler ADM drops the AppFlow records. As a result, Web Insight reports do not appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Observation point ID issue

This issue appears because the observation point ID is not unique.

NOTE

An observation point ID is the identifier for the NetScaler from which AppFlow records are being exported. By default, the NetScaler IP is the observation point ID.

Complete the following steps to troubleshoot this issue:

1. In the NetScaler, ensure that the AppFlow policy hits are increasing and the instance is sending AppFlow records to ADM.
2. Check if corresponding virtual server is licensed.
3. Ensure that the configuration is not copied from one NetScaler to another. When copied, the configuration might create an exporter ID issue that results NetScaler ADM to not process AppFlow records.
4. Log in to the NetScaler and run the `unset appflow param -observationpointId` command.

Missing AppFlow parameters issue

This issue appears because NetScaler ADM drops the AppFlow records due to missing data.

Complete the following steps to troubleshoot this issue:

1. Ensure in the NetScaler, the AppFlow policy hits are increasing and the instance is sending the AppFlow records to ADM.
2. Check if corresponding virtual server is licensed.
3. Ensure that the configuration is not copied from one NetScaler to another. When copied, the configuration might create an exporter ID issue that results NetScaler ADM to not process the AppFlow records.
4. Ensure the following AppFlow params are enabled on the NetScaler:
   - `HTTP method logging`
   - `HTTP domain name logging`
   - `HTTP URL logging`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `HTTP host logging`
- `HTTP Content-Type header logging`

Troubleshoot using counters

Check the following AppFlow counters for any AppFlow or Web Insight related issues.

COUNTER	DESCRIPTION
`appflow_tot_record_drop`	AppFlow records dropped due to an invalid collector. Usually happens when the collector configuration changes, and the existing connections use the old collector configuration.
`lstream_tot_trans_written`	This counter must increment for every transaction that is to be logged.
`lstream_sent`	This counter increments for every transaction log that is sent.

View analytics for Web transactions

Web transaction analytics enables you to view detailed transactions for:

- Response time > 500 ms
- 5xx errors

Note:

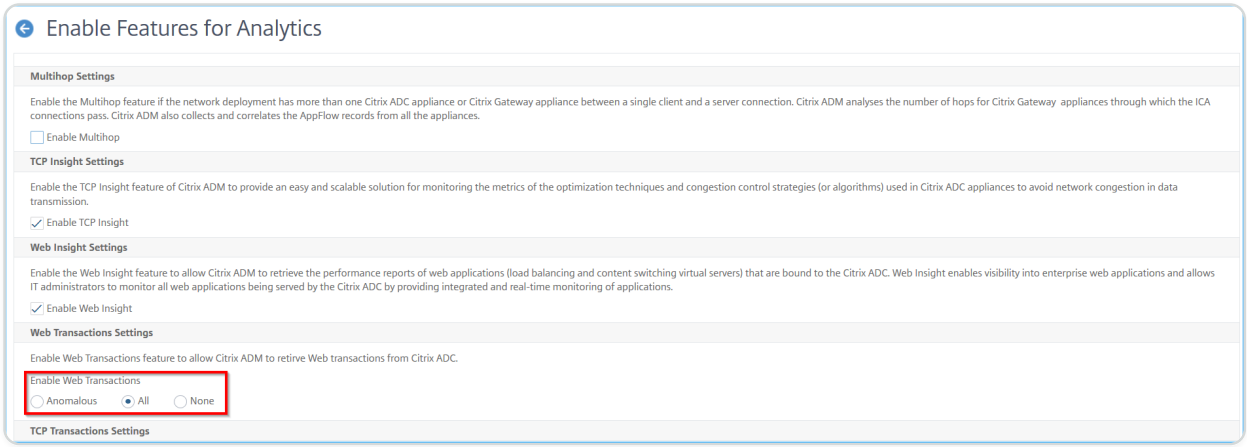
> You can view only a few sample 2xx transactions for the selected application.

Prerequisites:

To view the web transaction analytics, you must:

- Enable analytics.
- Change the **Web Transaction Settings** to get the 2xx displayed. Navigate to **Settings** > **Analytics Settings**, select **Enable Features for Analytics**, and select **All**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Detailed web transactions

This feature not only enables you to look into the detailed transactions, but also understand the response time metric split across the client, ADC, and server visually.

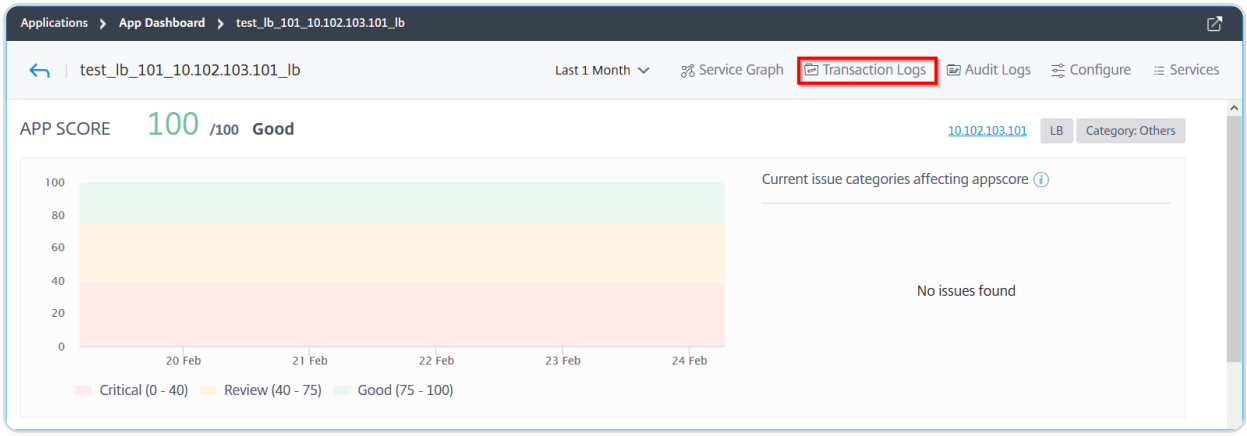
Note

> In some scenarios, NetScaler might not be able to calculate the RTT values for some transactions. For such transactions, NetScaler ADM displays the RTT values as

- **NA** – Displays when the ADC instance cannot calculate the RTT.
- **< 1ms** – Displays when the ADC instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

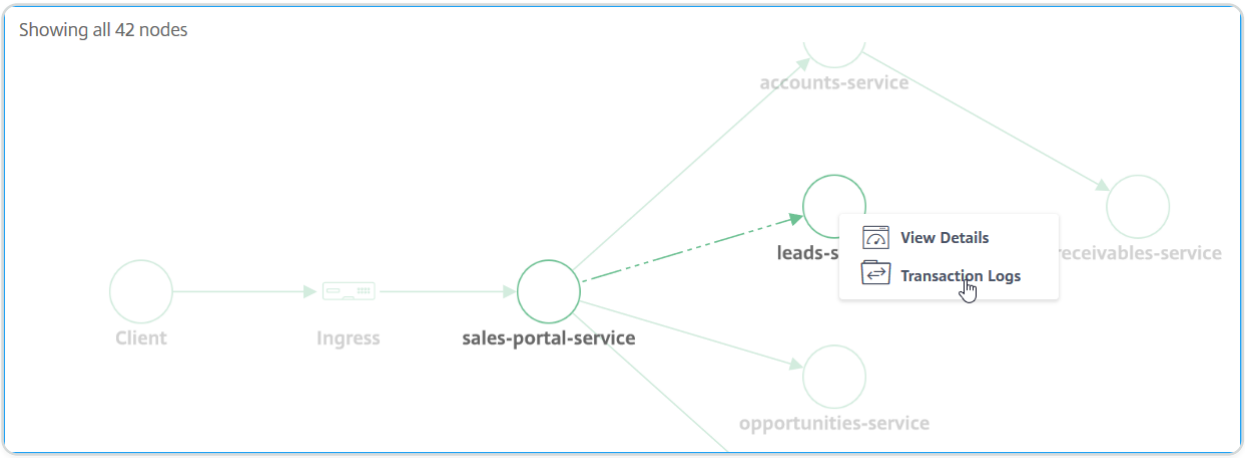
You can access the **Transaction Summary** for:

- **Applications** - Navigate to **Applications** > **Dashboard**, select an application, and Click **Transaction Log**.

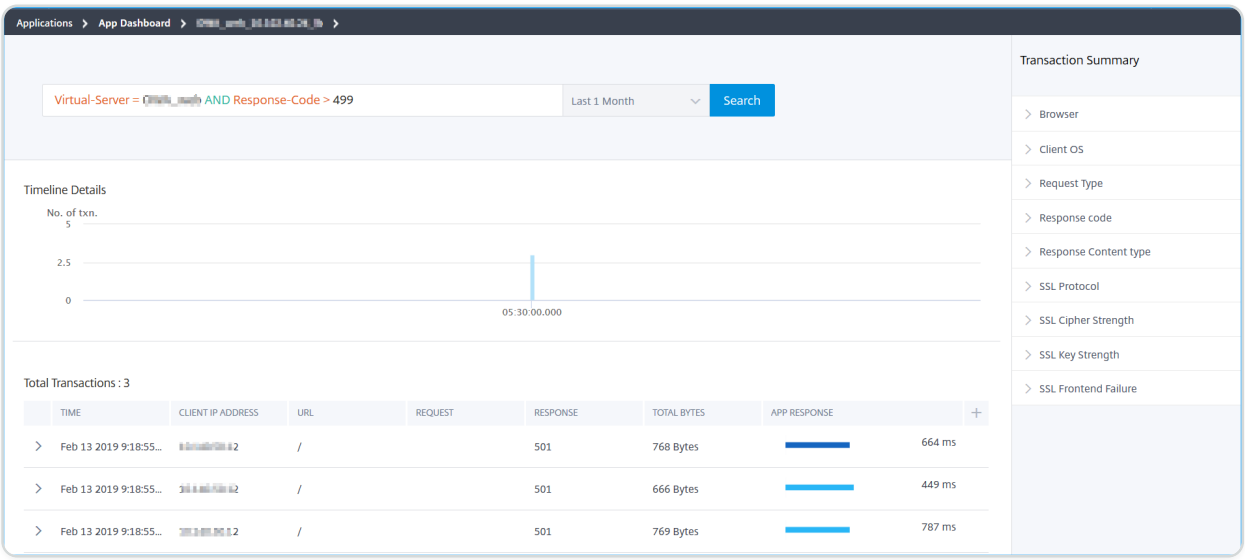


- **Kubernetes apps** - Navigate to **Applications** > **Service Graph**, and click a service and select **Transaction Logs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



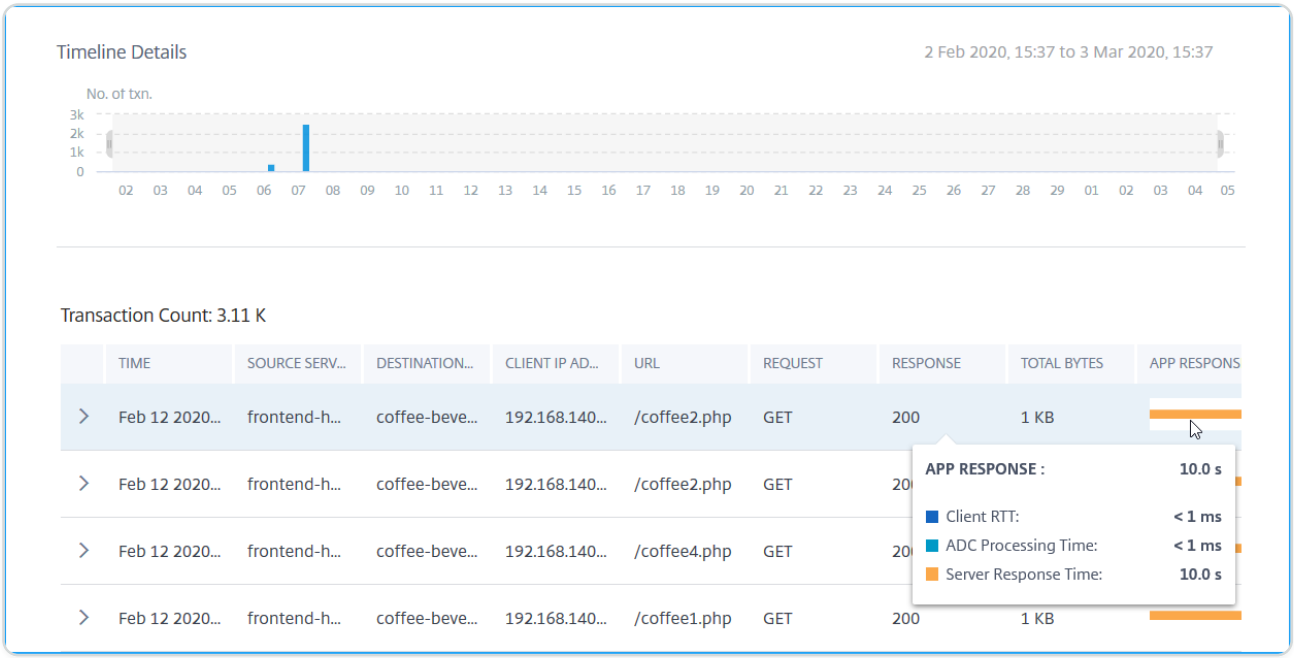
The **Transaction Summary** page is displayed for the selected application.



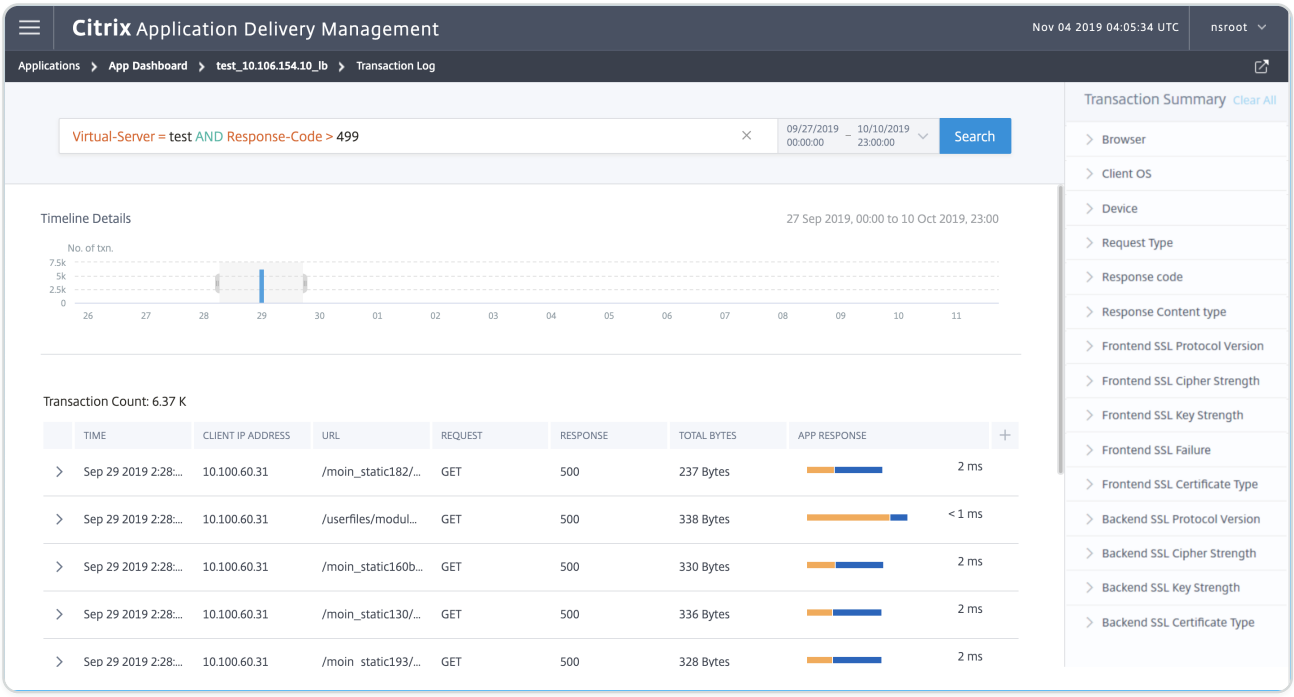
Hover the mouse pointer in **App Response** to view details such as RTT and processing time from NetScaler instance and the server.

The following example helps you analyze that the issue is from the server. The server response time indicates 10 seconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also drag and select to view the transactions for a specific duration.



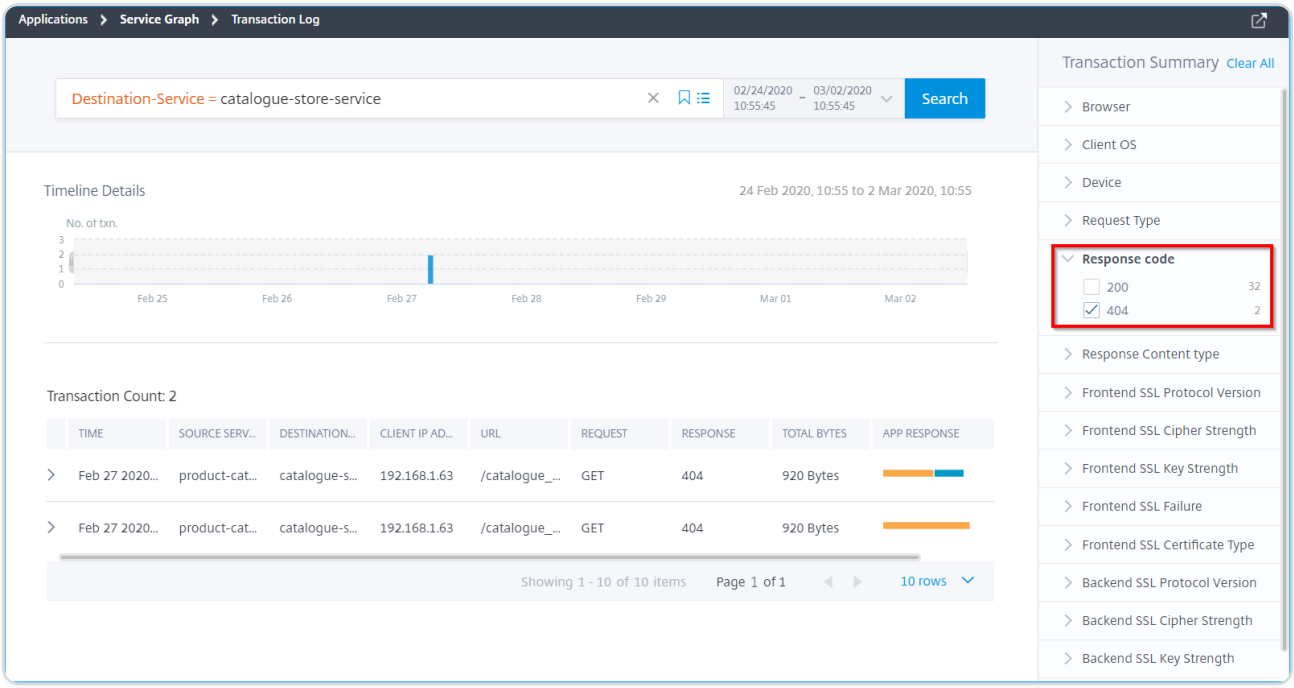
View events

You can view the detailed information about a particular event. On the **Transaction Summary** panel, you can filter results by selecting the options from each metric.

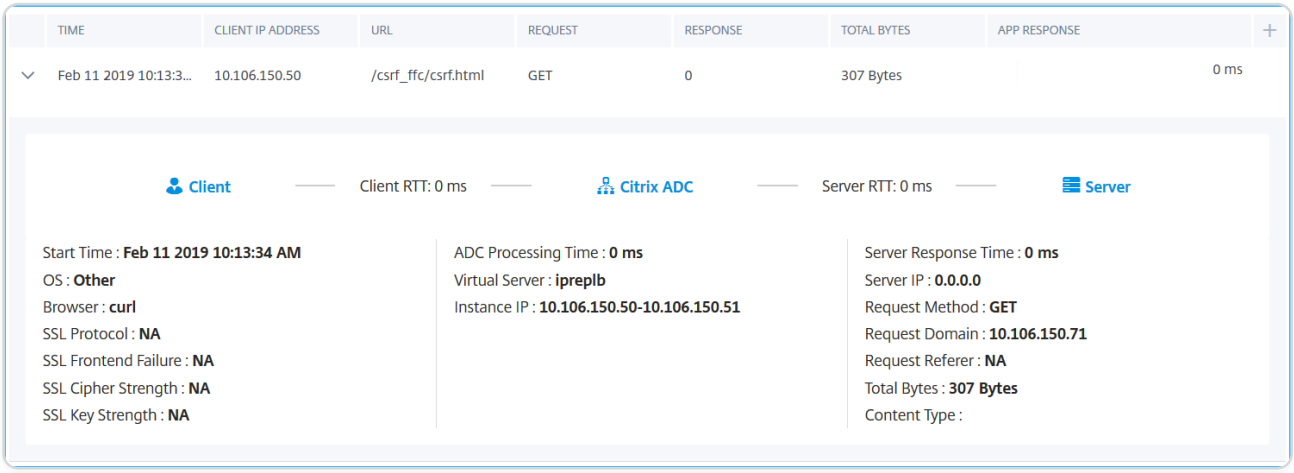
For example, consider that you want to view 4xx transactions.

On the **Transaction Summary** panel, click **Response code**, and select **404** to view the result.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



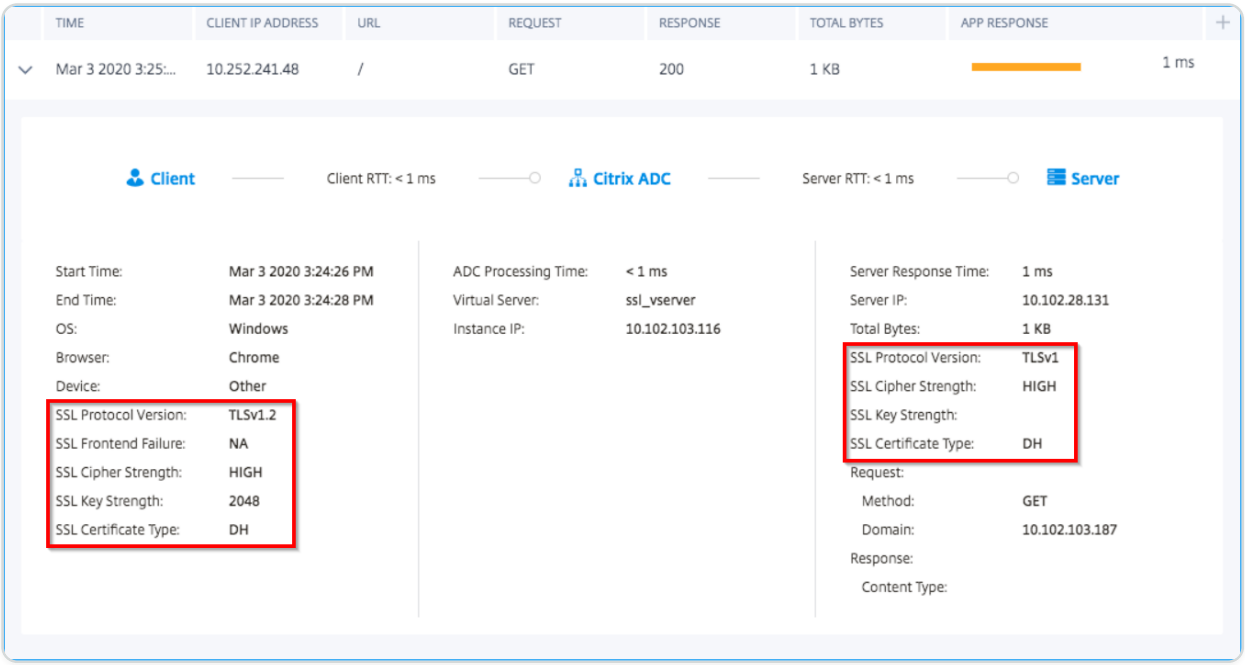
Click a transaction to view the details that display the metrics information from client to server.



For transactions that have SSL errors, the details are displayed for both client and server. The following SSL metrics are displayed:

- SSL Protocol Version
- SSL Front-end Failure
- SSL Cipher Strength
- SSL Key Strength
- SSL Certificate Type

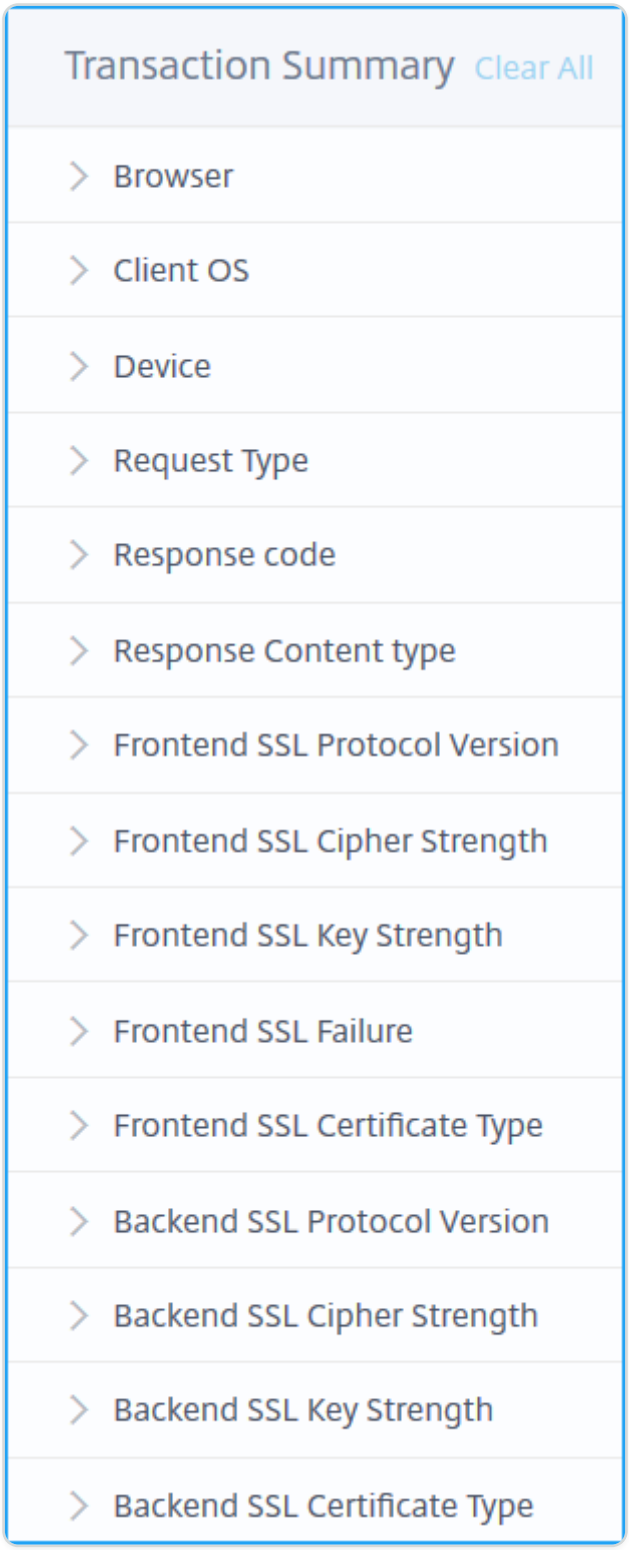
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also click the **SSL Frontend** and **SSL Backend metrics** from the **Transaction Summary** panel to filter the results.

To filter the results, select the options available under **Transaction Summary**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Browser**: The browsers types used by the clients. For example: Chrome, Firefox.
- **Client OS**: The client OS based on the User Agent details from the browser. For example: Windows
- **Device**: The devices based on the User Agent details from the browser. For example: Tablet, Mobile.
- **Request Type**: The transaction request type. For example: GET.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

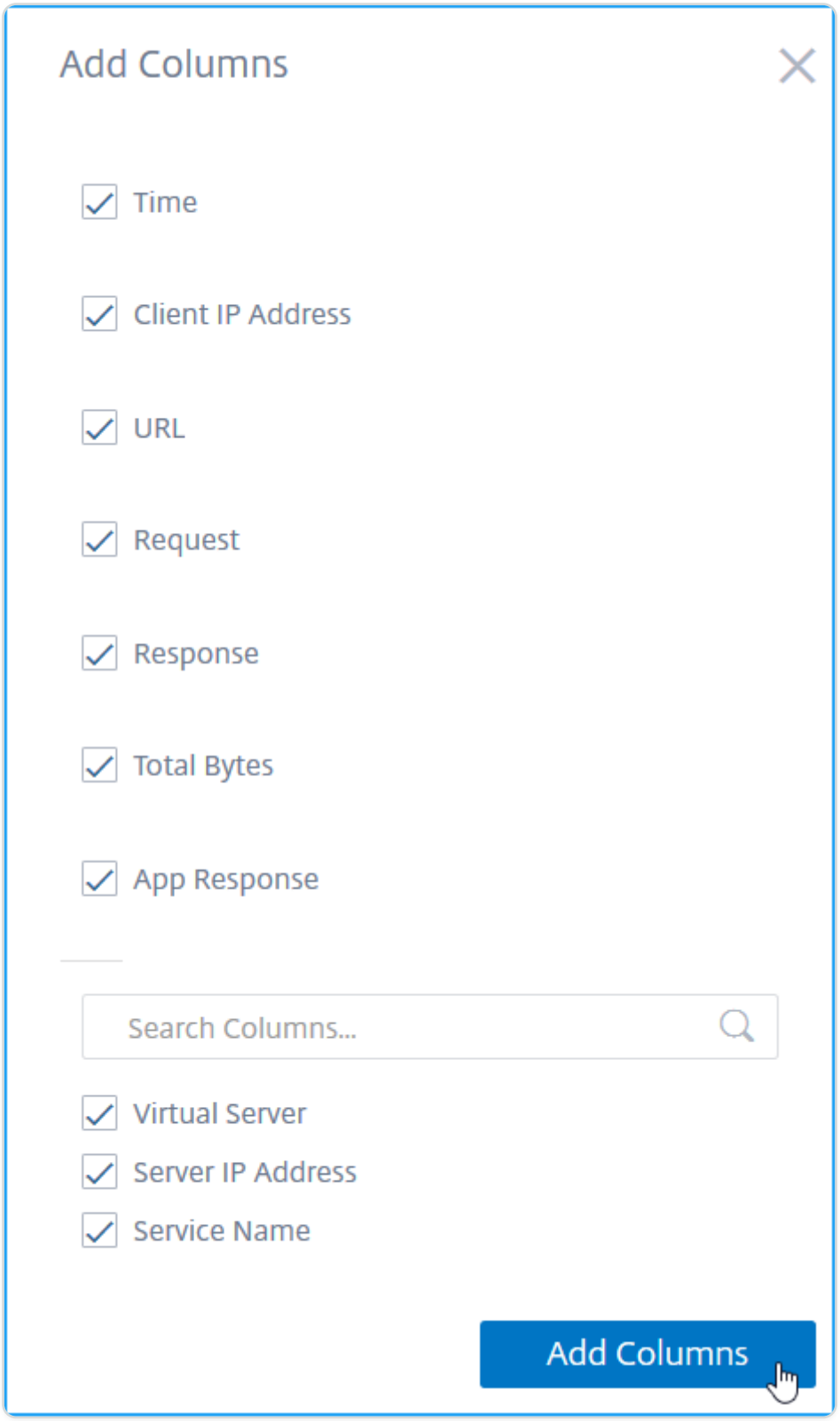
- **Response code**: The response code received from the server. For example: 501, 404, 200.
- **Response content type**: The transaction content type. If the client request is for text/html, then the response from the server must be text/html.
- **Frontend SSL Protocol Version**: The SSL protocol version used by the clients. For example: SSLv3.
- **Frontend SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **Frontend SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **Frontend SSL Failure**: The front-end SSL handshake error message. For example: SSL CLIENTAUTH FAILURE
- **Frontend SSL Certificate Type**: The certificate type used by the client. For example: RSA, DSA, ECDSA, DH.
- **Backend SSL Protocol Version**: The SSL protocols used by the server. For example: SSLv3
- **Backend SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **Backend SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **Backend SSL Certificate Type**: The certificate type used by the server. For example: RSA, DSA, ECDSA, DH.

Add columns in the event list

You can click the

button to choose the list of options and click **Add Columns** to get the details displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Advanced search

The Transaction Summary also has a search text box and time duration list, where you can view the events as per your requirement. When you place the cursor in the search box, the search box

© 1997–2026 Citrix Systems, Inc. All rights reserved.

gives you a list of search suggestions. You can also use operators in your search queries to narrow the focus of your search.

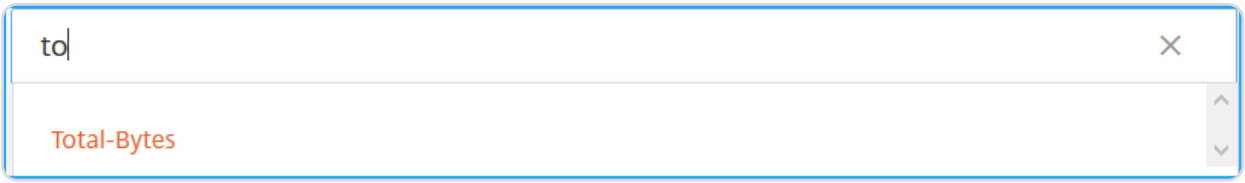
The following are the operators you can use for your search queries:

OPERATORS	DESCRIPTION	EXAMPLE	OUTPUT
=	Equals to some value	Virtual-Server = test	Displays the event for virtual server with the name "test".
>	Greater than some value	App-Response-Time > 500	Displays the events for the applications that have the app response with more than 500 ms
<	Lesser than some value	App-Response-Time < 300	Displays the events for the applications that have the app response time with less than 300 ms
>=	Greater or equal to some value	Total-Bytes >= 1024	Displays the events for the transactions with greater or equal to 1 kb
<=	Less or equal to some value	Total-Bytes <= 1024	Displays the events for the transactions with lesser or equal to 1 kb
!=	Not equal to some value	Response-code != 200	Displays the events with all transactions, except the failed transactions.
~	Contains some value	Virtual-Server ~ mas	Displays the events for the virtual servers that have the name mas.

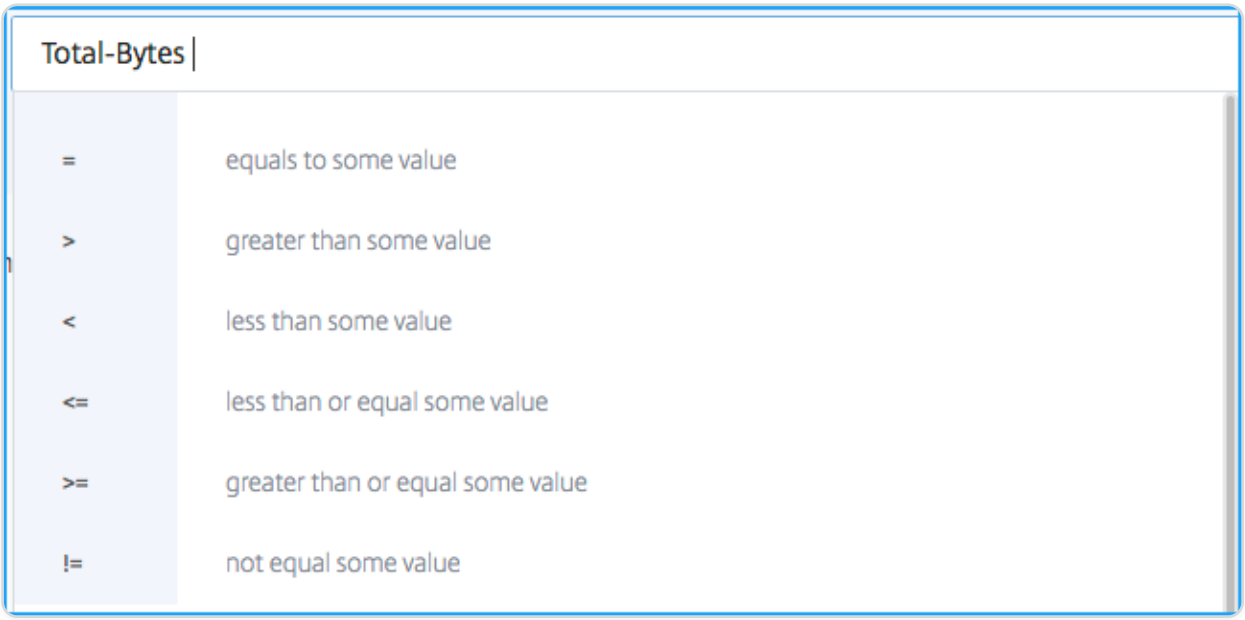
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, let us consider a scenario that you wanted to generate events for total bytes that are lesser than 300 bytes. You must specify the search queries as follows:

1. Specify the required word in the search box to get the related suggestions.



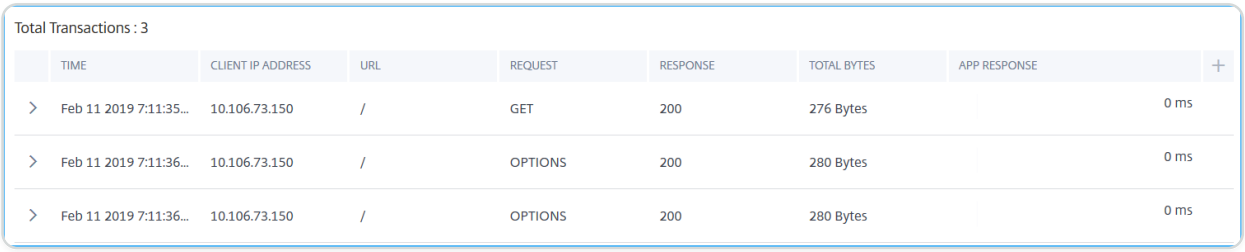
2. Select **Total-Bytes** and click again on the search text box, and select **<**.



3. Type the value 300.

4. Select the time period and click **Search** to view the events based on your search query.

   The search result is displayed.

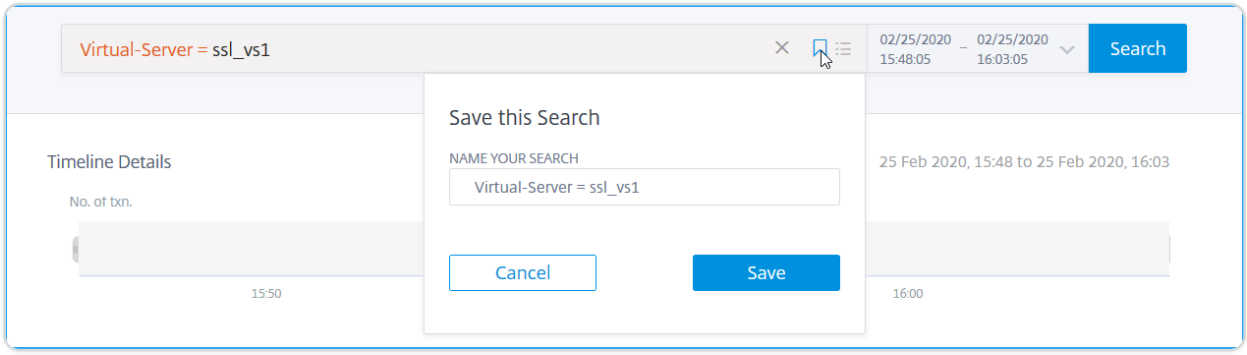


© 1997–2026 Citrix Systems, Inc. All rights reserved.

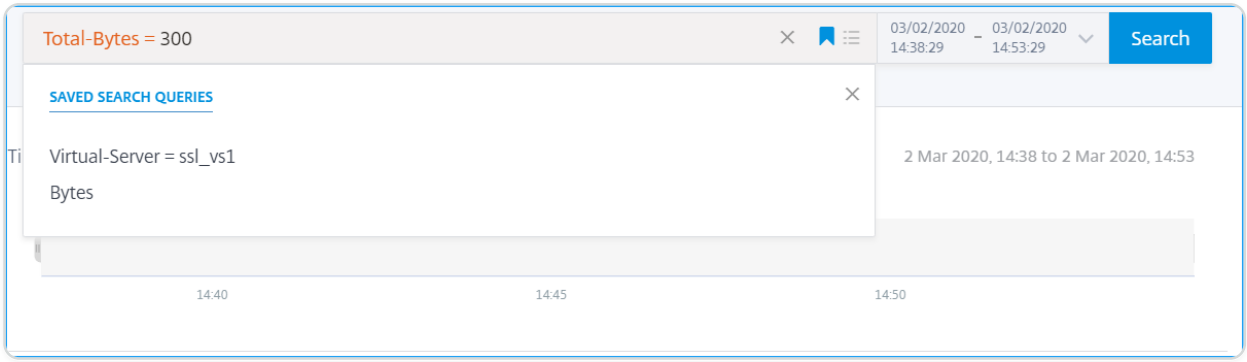
Save search

After you use the suggestions and operators, you can save the search query. You can then use it later from the list, instead of using the suggestions and operators again.

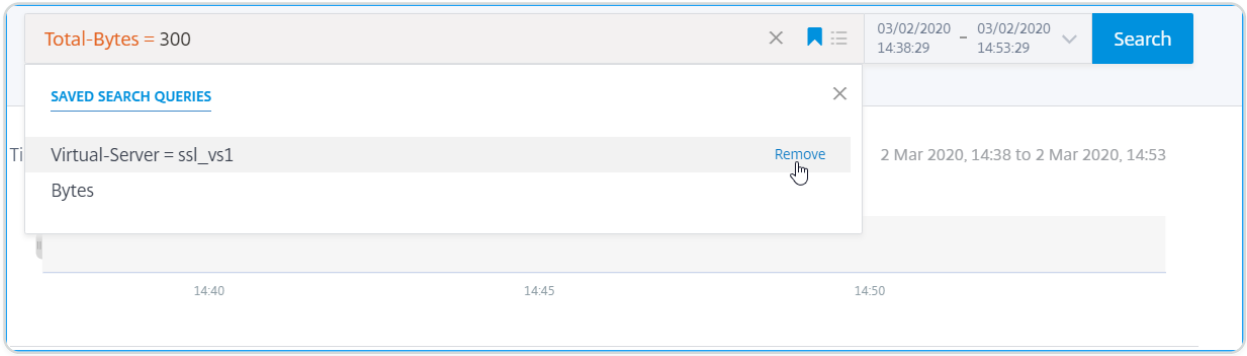
- To save a search query, click the bookmark icon, specify a name of your choice, and then click **Save**.



- To use the search query from the list, click the icon and select the search query from the list to display the results.

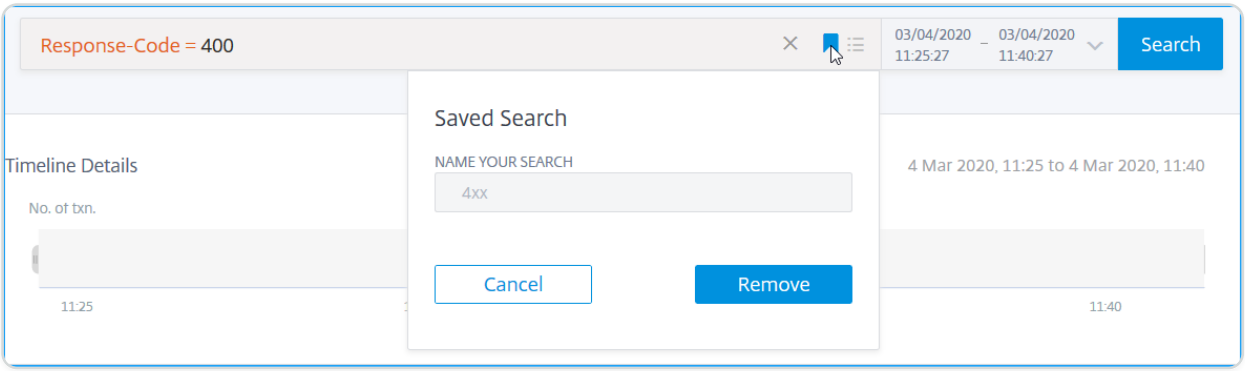


- To remove the search query, click the icon, hover the mouse pointer on the saved search query, click **Remove**.



You can also click the bookmark icon and click **Remove**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Export data

You can export the web transaction analytics data for the selected duration by clicking the **Export** icon. You can export in PDF, PNG, JPEG, and CSV formats. The **Export** option enables you to do one of the following:

- Select **Export Now** to view and export the report in PDF, JPEG, PNG, or CSV format.
- Select **Schedule Export** tab to schedule the report daily, weekly, or monthly and send the report over an email or a Slack message.

Detailed procedures to setup dual tier or service mesh lite topology

Software requirements

KUBERNETES DISTRIBUTION	KUBERNETES VERSION	CONTAINER NETWORK INTERFACES (CNI)	CPX VERSION	CIC VERSION	NETSCALER ADM VERSION	NETSCALER AGENT VERSION
Open source	v1.16.3	Flannel	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

Before you begin

You can view service graph using the following scenarios:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADM and Kubernetes cluster on the same network (for example, NetScaler ADM and Kubernetes cluster hosted on Citrix Hypervisor™).
- NetScaler ADM and Kubernetes cluster on a different network. In this scenario, you must configure an on-prem agent and register the agent on the network, where Kubernetes cluster is hosted.

To use service graph in NetScaler® ADM, ensure you have:

- Kubernetes cluster with NetScaler CPX as a proxy. For more information see, NetScaler Ingress Controller.
- Configured static routes on NetScaler ADM to enable communication between NetScaler ADM and NetScaler CPX
- Downloaded the sample deployment files from GitHub repository.
- Added required parameters in CPX YAML file to ensure successful CPX registration with NetScaler ADM.
- Added Kubernetes cluster in NetScaler ADM.
- Deployed a sample microservice application.
- Deployed NetScaler CPX and registered CPX to ADM.
- Enabled **Auto-select Virtual Servers** to license the virtual servers.
- Changed the **Web Transaction Settings** to **All** for NetScaler agent to get HTTP transactions.
- Updated the **Istream.conf** file and changed the TCP setting to **All** for NetScaler agent to get TCP metrics.

Software requirements

KUBERNETES DISTRIBUTION	KUBERNETES VERSION	CONTAINER NETWORK INTERFACES (CNI)	CPX VERSION	CIC VERSION	NETSCALER ADM VERSION	NETSCALER AGENT VERSION
Open source	v1.16.3	Flannel	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before you begin

You can view service graph using the following scenarios:

- NetScaler ADM and Kubernetes cluster on the same network (for example, NetScaler ADM and Kubernetes cluster hosted on Citrix Hypervisor).
- NetScaler ADM and Kubernetes cluster on a different network. In this scenario, you must configure an on-prem agent and register the agent on the network, where Kubernetes cluster is hosted.

To use service graph in NetScaler ADM, ensure you have:

- Kubernetes cluster with NetScaler CPX as a proxy. For more information see, NetScaler Ingress Controller.
- Configured static routes on NetScaler ADM to enable communication between NetScaler ADM and NetScaler CPX
- Downloaded the sample deployment files from GitHub repository.
- Added required parameters in CPX YAML file to ensure successful CPX registration with NetScaler ADM.
- Added Kubernetes cluster in NetScaler ADM.
- Deployed a sample microservice application.
- Deployed NetScaler CPX and registered CPX to ADM.
- Enabled **Auto-select Virtual Servers** to license the virtual servers.
- Changed the **Web Transaction Settings** to **All** for NetScaler agent to get HTTP transactions.
- Updated the **Istream.conf** file and changed the TCP setting to **All** for NetScaler agent to get TCP metrics.

Configure static routes in NetScaler ADM

Inside the Kubernetes cluster, all containerized pods use an overlay network. Establishing the communication using those private IP addresses directly is not possible. To enable communication from NetScaler ADM to Kubernetes cluster, you must configure static routing in NetScaler ADM.

Note

> If you are using an on-prem agent, ensure you configure static routes on the agent. Using an SSH client, log on to NetScaler agent and configure the static routes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consider that you have the following IP addresses for your Kubernetes cluster:

- Kubernetes master – 101.xx.xx.112
- Kubernetes worker 1 – 101.xx.xx.111
- Kubernetes worker 2 – 101.xx.xx.110

On the Kubernetes master, run the following command to identify the pod network to do the static routing:

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

The following is an example output after you run the command:

```
root@master:~# kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}
{.status.addresses[0].address}{'\n'}{end}"
podNetwork: 1[illegible]  gateway: 1[illegible]0
podNetwork: 1[illegible]4  gateway: 1[illegible]1
podNetwork: 1[illegible]  gateway: 1[illegible]2
```

1. Using an SSH client, log on to NetScaler ADM
2. Configure the static routing using the command `route add -net <public IP address range> <Kubernetes IP address>`

   For example:

   `route add -net 192.168.0.0/24 101.xx.xx.112`

   `route add -net 192.168.1.0/24 101.xx.xx.111`

   `route add -net 192.168.2.0/24 101.xx.xx.110`
3. Verify the configuration by using `netstat -rn`

```
bash-3.2# netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags     Refs      Use  Netif Expire
default            10.[illegible].1   UGS          0 20224745    1/1
10.[illegible].0/24  link#3           U            0  7002455    1/1
10.[illegible].115   link#3           UHS          0        0    lo0
127.0.0.1          link#1             UH           0  7421390    lo0
192.168.0.0/24     10.[illegible]12   UGS          0        0    1/1
192.168.1.0/24     10.[illegible]11   UGS          0   319315    1/1
192.168.2.0/24     10.[illegible]10   UGS          0    41712    1/1
```

4. Append these route commands in `/mpsconfig/svm.conf` file.

   a. In NetScaler ADM, access the **svm.conf** file using the following command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`vim /mpsconfig/svm.conf`

b. Add the static routes in **svm.conf** file.

For example, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Download the sample deployment files from GitHub

1. Use the command **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` to clone the git hub repository in the master node.
2. To access the YAMLs:

   `cd citrix-k8s-ingress-controller/example/servicegraph-demo/`

Add parameters in CPX YAML file

NOTE

If you are using CPX 58.x or later, you must use the non-nsroot password while registering to ADM agent. To ensure security, NetScaler agent 61.x or later releases need mandatory password change. If your NetScaler agent is upgraded to 61.x or latest version, you must ensure to use **CPX 58.x or later** build.

You must include the following parameters in the `cpx.yaml` file to ensure CPX registration with NetScaler ADM:

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"

- name: "NS_HTTPS_PORT"

  value: 9443"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – Indicates the NetScaler ADM IP address

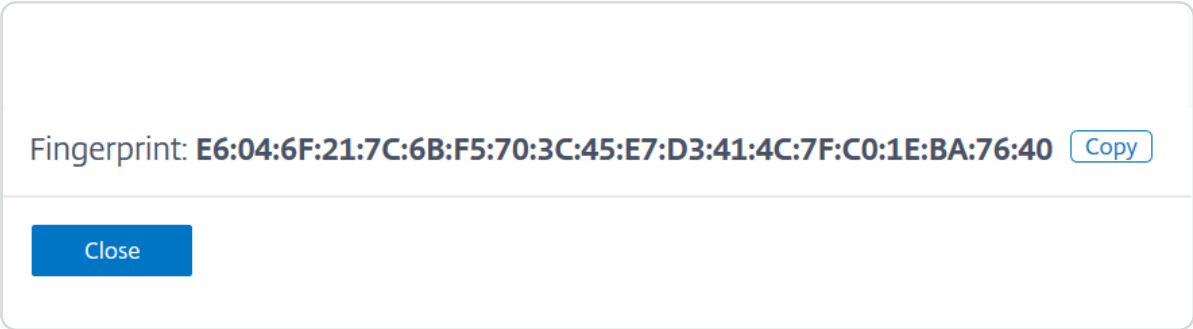
  NOTE

  If ADM agent is used, then this indicates the on-prem agent IP address.

- **NS_MGMT_FINGER_PRINT** – Indicates the authentication for CPX in NetScaler ADM. To get the fingerprint:

  a. In NetScaler ADM, navigate to **Settings > Administration**

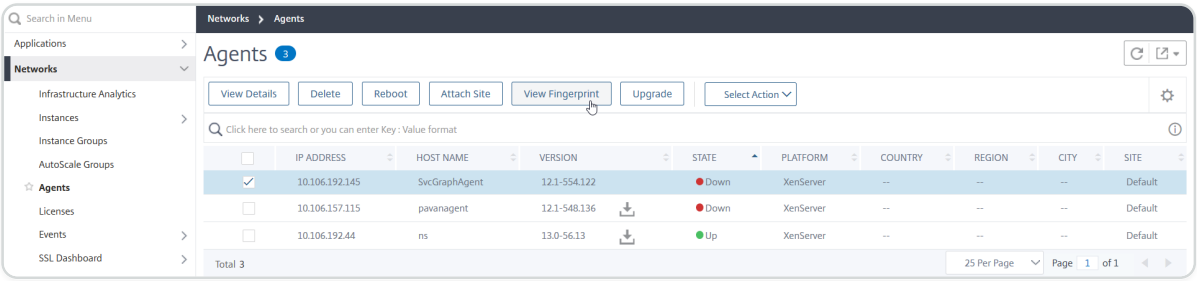
  b. Under **System Configurations**, click **View ADM Fingerprint**

  Note:

  If you have configured an on-prem agent, navigate to **Infrastructure > Instances > Agents**, select the agent, and then click **View Fingerprint**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **NS_HTTP_PORT** – Indicates the HTTP port for communication
- **NS_HTTPS_PORT** – Indicates the HTTPS port for communication
- **NS_MGMT_USER** - Indicates the user name
- **NS_MGMT_PASS** - Indicates the password. Specify a password of your choice
- **LOGSTREAM_COLLECTOR_IP** – Indicates the NetScaler agent IP address, where **Logstream** protocol must be enabled to transfer log data from CPX to ADM

Add VPX or SDX or MPX or BLX instance in NetScaler ADM

To get the tier-1 ADC instance analytics in service graph, you must add the VPX/SDX/MPX/BLX instance in NetScaler ADM and enable **Web Insight**.

1. Navigate to **Infrastructure > Instances > NetScaler**
2. Click the **Add** option to add the instance. For more information, see Add instances in NetScaler ADM
3. After adding the instance, select the virtual server and enable **Web Insight**. For more information, see Manage licensing and enable analytics on virtual servers

Add Kubernetes cluster in NetScaler ADM

To add the Kubernetes cluster:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:
   a. **Name** - Specify a name of your choice.
   b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. On the Kubernetes master node, run the command `kubectl cluster-info`.

```
root@kmaster:[redacted]# kubectl cluster-info
Kubernetes master is running at https://10.[redacted]:6443
KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/
services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

ii. Enter the URL that displays for **“Kubernetes master is running at.”**

c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler ADM. To generate an authentication token:

On the Kubernetes master node:

i. Use the following YAML to create a service account:

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

ii. Run `kubectl create -f <yaml file>`.

The service account is created.

iii. Run `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` to bind the cluster role to service account.

The service account now has the cluster-wide access.

A token is automatically generated while creating the service account.

iv. Run `kubectl describe sa <name>` to view the token.

v. To get the secret string, run `kubectl describe secret <token-name>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@kmaster:~# kubectl describe secret citrixadm-sa-token-79knw
Name:         citrixadm-sa-token-79knw
Namespace:    default
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: citrixadm-sa
              kubernetes.io/service-account.uid: 136270eb-1fe1-11ea-b603-72328a2
af136

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1025 bytes
namespace:  7 bytes
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V
hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiw
ia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImNpdHJpeGFkbS1zYS10b2t
lbi03OWtudyIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50Lm5hbWU
iOiJjaXRyaXhhZG0tc2EiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3V
udC51aWQiOiIxMzYyNzBlYi0xZmUxLTExZWEtYjYwMy03MjMyOGEyYWYxMzYiLCJzdWIiOiJzeXN0ZW0
6c2VydmljZWFjY291bnQ6ZGVmYXVsdDpjaXRyaXhhZG0tc2EifQ.JsU4JPcyFoXA6Vn5Dxa137ca_hI0
wzY1Ajv0ctHN7NeU4YC_I6H5xgNAKnqj2rJPlQEmSZQygPOrxduLDYsNBCT9fH4sv1aBdOzzpkCIDW6y
6BmX4IaC6HTFPGO54zSDzjPmuKkPzyIRa4twUSvxfhwXE6JRy99iJjgPBraL65ct99bcVXF5nMDdexro
Iw23M8lcknV5fPuD33WhieS17WbXlq_ZYEA4WaulGXi9veHczN1S9oFPUlnM3d13R7A63bZjCKvWYlnN
7W5etxd2dfLgEJysixj8lKRxUifL2f04lfWM8ucwKVb8TumsMqG7eturRF5SxSYNodmBKNNkIA
```

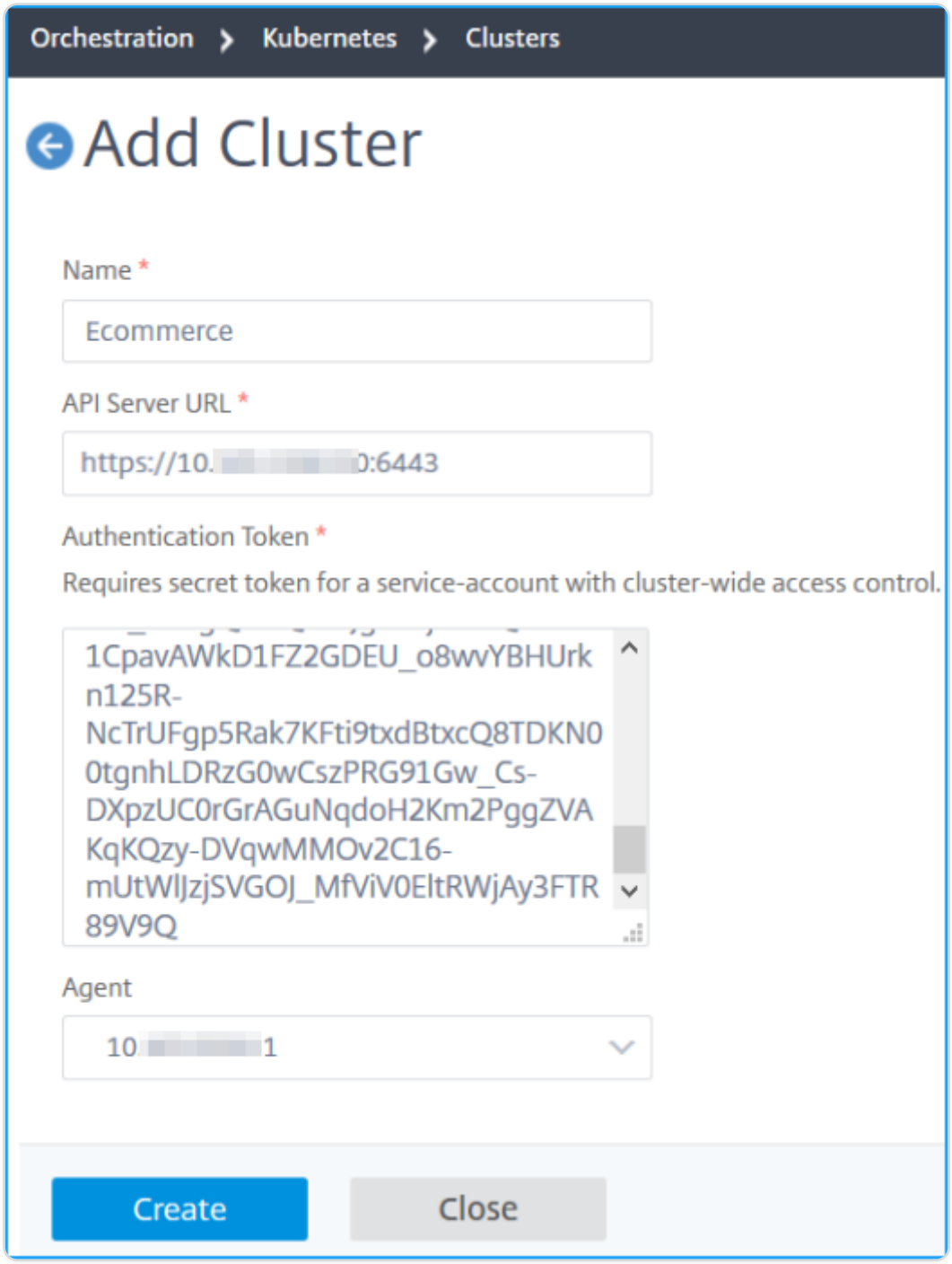
d. Select the agent from the list.

Note

> If you are using an on-prem agent, ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deploy a sample microservice application

On the master node:

1. Run `kubectl create -f namespace.yaml` to create a namespace.
2. Deploy `hotdrink` microservices, ingress, and secrets using following commands:

   `kubectl create -f team_hotdrink.yaml -n sg-demo`

   `kubectl create -f hotdrink-secret.yaml -n sg-demo`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy CPX and register CPX in ADM

1. Run `kubectl create -f rbac.yaml` to deploy cluster role and cluster binding.
2. Run `kubectl create -f cpx.yaml -n sg-demo` to deploy CPX.

After the deployment, the CPX registration is automatically done.

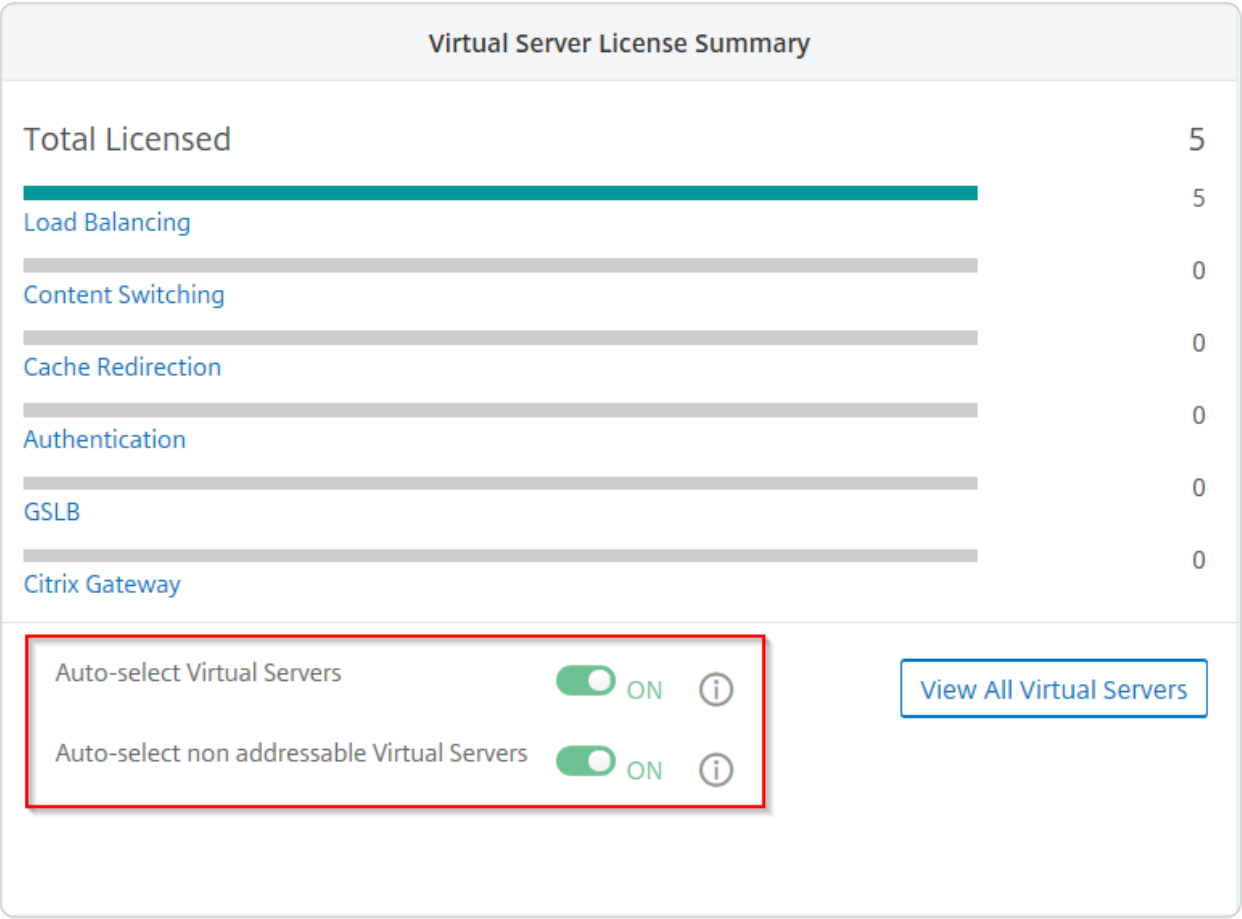
Enable auto select virtual servers for licensing

Note

> Ensure you have sufficient virtual server licenses. For more information, see Licensing

After you add Kubernetes cluster in NetScaler ADM, you must ensure to auto-select virtual servers for licensing. Virtual servers must be licensed to display data in Service Graph. To auto-select virtual servers:

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Under **Virtual Server License Summary**, enable **Auto-select Virtual Servers** and **Auto-select non addressable Virtual Servers**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

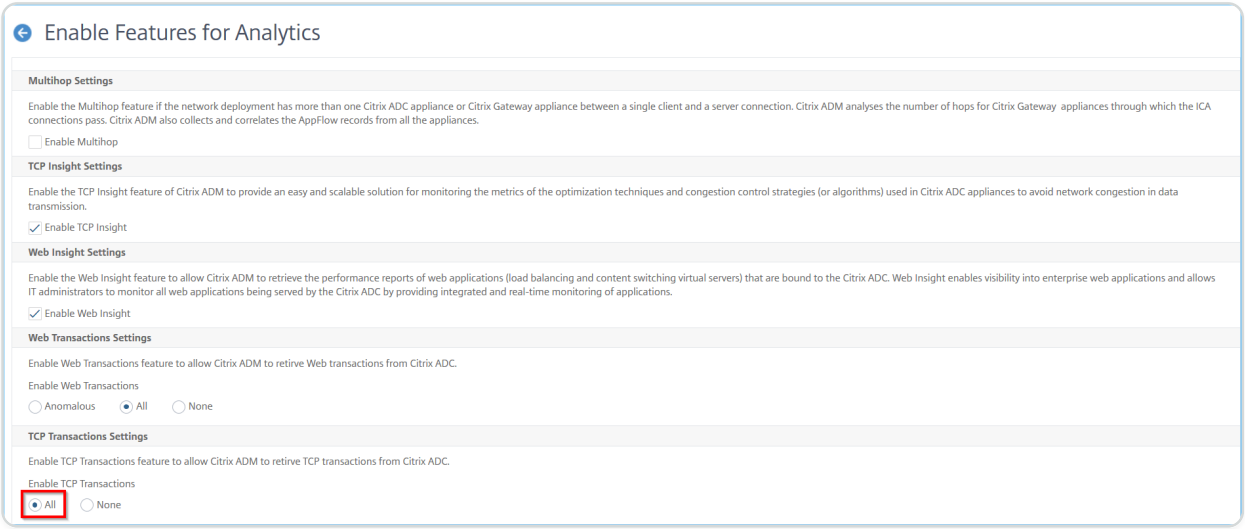
Enable Web Transaction and TCP Transaction settings

After you add the Kubernetes cluster and enable the auto-select virtual servers, change the **Web Transaction Settings** and **TCP Transactions Settings** to **All**.

1. Navigate to **Settings > Analytics Settings**.

   The **Analytics Settings** page is displayed.

2. Click **Enable Features for Analytics**.
3. Under **Web Transaction Settings**, select **All**.
4. Under **TCP Transactions Settings**, select **All**.



5. Click **OK**.

Send traffic to microservices

Next, you must send traffic to microservices to get the service graph populated in NetScaler ADM.

1. Run `kubectl get svc -n sg-demo` to expose CPX through NodePort.

```
root@adm-cic-master:~/adm# kubectl get svc -n sg-demo
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)
 AGE
coffee                  ClusterIP   10.102.13.37    <none>        80/TCP,443/TCP
 83s
coffee-beverage         ClusterIP   None            <none>        80/TCP,443/TCP
 83s
cpx-service             NodePort    10.98.190.208   <none>        80:30402/TCP,443:32042/TCP
 34s
frontend-hotdrinks      ClusterIP   None            <none>        80/TCP,443/TCP
 83s
lb-service-hotdrinks    ClusterIP   None            <none>        80/TCP,443/TCP
 33s
tea                     ClusterIP   10.103.233.53   <none>        80/TCP,443/TCP
 83s
tea-beverage            ClusterIP   None            <none>        80/TCP,443/TCP
 83s
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Edit the **etc/host** file and create a domain IP entry for `hotdrink.beverages.com`

   You can now access the microservice using `https://hotdrink.beverages.com`

Detailed procedures to set up service mesh topology

The prerequisites to deploy the service mesh topology is available at Setting up service graph.

Configure static routes in NetScaler® ADM

Inside the Kubernetes cluster, all containerized pods use an overlay network. Establishing the communication using those private IP addresses directly is not possible. To enable communication from NetScaler ADM to Kubernetes cluster, you must configure static routing in NetScaler ADM.

Note

> If you are using an on-prem agent, ensure you configure static routes on the agent. Using an SSH client, log on to NetScaler agent and configure the static routes.

Consider that you have the following IP addresses for your Kubernetes cluster:

- Kubernetes master – 101.xx.xx.112
- Kubernetes worker 1 – 101.xx.xx.111
- Kubernetes worker 2 – 101.xx.xx.110

On the Kubernetes master, run the following command to identify the pod network to do the static routing:

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

The following is an example output after you run the command:

```
root@master:~# kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}
{.status.addresses[0].address}{'\n'}{end}"
podNetwork: 1[illegible]  gateway: 1[illegible]0
podNetwork: 1[illegible]4  gateway: 1[illegible]1
podNetwork: 1[illegible]  gateway: 1[illegible]2
```

1. Using an SSH client, log on to NetScaler ADM
2. Configure the static routing using the command `route add -net <public IP address range> <Kubernetes IP address>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example:

`route add -net 192.168.0.0/24 101.xx.xx.112`

`route add -net 192.168.1.0/24 101.xx.xx.111`

`route add -net 192.168.2.0/24 101.xx.xx.110`

3. Verify the configuration by using `netstat -rn`

```
bash-3.2# netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif Expire
default            10.[redacted].1    UGS         0 20224745    1/1
10.[redacted].0/24 link#3             U           0  7002455    1/1
10.[redacted].115  link#3             UHS         0        0    lo0
127.0.0.1          link#1             UH          0  7421390    lo0
192.168.0.0/24     10.[redacted]12    UGS         0        0    1/1
192.168.1.0/24     10.[redacted]11    UGS         0   319315    1/1
192.168.2.0/24     10.[redacted]10    UGS         0    41712    1/1
```

4. Append these route commands in `/mpsconfig/svm.conf` file.

   a. In NetScaler ADM, access the **svm.conf** file using the following command:

   `vim /mpsconfig/svm.conf`

   b. Add the static routes in **svm.conf** file.

   For example, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Configure the required parameters

In the Kubernetes master:

1. Create secret with ADM Agent Credentials in every namespace where CPX as an ingress gateway / sidecar is deployed.

   `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>`

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`

3. Deploy the NetScaler CPX as an Ingress Gateway

   `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

The following table lists the configurable parameters in the Helm chart and its default values:

PARAMETER	DESCRIPTION	DEFAULT	OPTIONAL/ MANDATORY (HELM)
citrixCPX	NetScaler CPX	FALSE	Mandatory for NetScaler CPX
xDSAdaptor.image	Image of the Citrix xDS adaptor container	quay.io/citrix/citrix-istio-adaptor:1.2.1	Mandatory
ADMSettings.ADMIP	NetScaler ADM IP address	null	Mandatory for NetScaler CPX
ADMSettings.ADMFingerPrint	The NetScaler ADM Fingerprint. Navigate to **Settings > Adminstration**, and click **View Fingerprint** under **System Configurations**	null	Optional
ingressGateway.EULA	End User License Agreement(EULA) terms and conditions. If yes, then user agrees to EULA terms and conditions.	NO	Mandatory for NetScaler CPX
ingressGateway.image	Image of NetScaler CPX designated to run as Ingress Gateway	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30	Mandatory for NetScaler CPX

4. Deploy the Citrix SideCar Injector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx> citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

The following table lists the configurable parameters in the Helm chart and its default values:

PARAMETER	DESCRIPTION	DEFAULT VALUE
ADMSettings.ADMIP	The NetScaler ADM IP address	NIL
cpxProxy.image	NetScaler CPX image used as sidecar proxy	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30
cpxProxy.imagePullPolicy	Image pull policy for NetScaler	IfNotPresent
cpxProxy.EULA	End User License Agreement(EULA) terms and conditions. If yes, then user agrees to EULA terms and conditions.	NO
cpxProxy.cpxSidecarMode	Environment variable for NetScaler CPX. It indicates that NetScaler CPX is running as sidecar mode or not.	YES

5. Set the label on any Namespace that needs CPX Sidecar Injection.

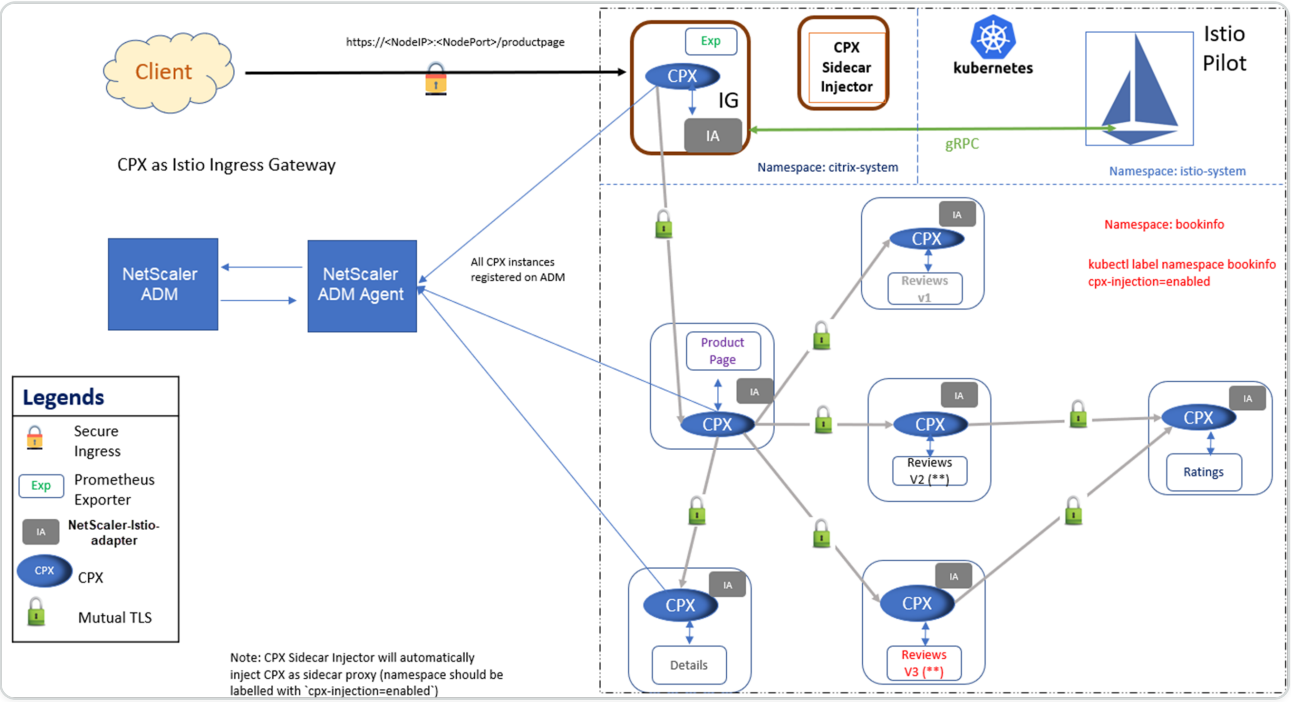
```
kubectl label namespace <app-namespace> cpx-injection=enabled
```

After performing step 3 and 5, you can see the NetScaler CPX is registered in NetScaler ADM.

Deploy a sample application

Consider that you want to deploy the following applications:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Perform the following procedure to deploy a sample application:

1. `kubectl create namespace citrix-system`
2. `kubectl create namespace bookinfo`
3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

   Note

   > You can give a user name and a password of your choice.

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   Note

   > You can give a user name and a password of your choice.

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`agent IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

Note

> You must give your ADM fingerprint and ADM agent or ADM IP address

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

   Note

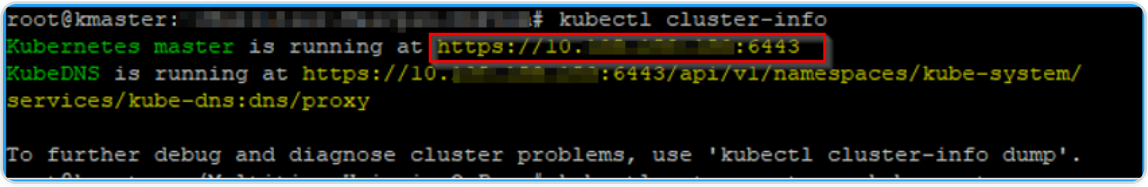
   > You must give your ADM fingerprint and ADM agent or ADM IP address

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

Add Kubernetes cluster in NetScaler ADM

To add the Kubernetes cluster:

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:
   a. **Name** - Specify a name of your choice.
   b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.
      i. On the Kubernetes master node, run the command `kubectl cluster-info`.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

ii. Enter the URL that displays for **“Kubernetes master is running at.”**

c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler ADM. To generate an authentication token:

On the Kubernetes master node:

i. Use the following YAML to create a service account:

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

ii. Run `kubectl create -f <yaml file>`.

The service account is created.

iii. Run `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` to bind the cluster role to service account.

The service account now has the cluster-wide access.

A token is automatically generated while creating the service account.

iv. Run `kubectl describe sa <name>` to view the token.

v. To get the secret string, run `kubectl describe secret <token-name>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@kmaster:~# kubectl describe secret citrixadm-sa-token-79knw
Name:         citrixadm-sa-token-79knw
Namespace:    default
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: citrixadm-sa
              kubernetes.io/service-account.uid: 136270eb-1fe1-11ea-b603-72328a2
af136

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1025 bytes
namespace:  7 bytes
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V
hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiw
ia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImNpdHJpeGFkbS1zYS10b2t
lbi03OWtudyIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50Lm5hbWU
iOiJjaXRyaXhhZG0tc2EiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3V
udC51aWQiOiIxMzYyNzBlYi0xZmUxLTExZWEtYjYwMy03MjMyOGEyYWYxMzYiLCJzdWIiOiJzeXN0ZW0
6c2VydmljZWFjY291bnQ6ZGVmYXVsdDpjaXRyaXhhZG0tc2EifQ.JsU4JPcyFoXA6Vn5Dxa137ca_hI0
wzY1Ajv0ctHN7NeU4YC_I6H5xgNAKnqj2rJPlQEmSZQygPOrxduLDYsNBCT9fH4sv1aBdOzzpkCIDW6y
6BmX4IaC6HTFPGO54zSDzjPmuKkPzyIRa4twUSvxfhwXE6JRy99iJjgPBraL65ct99bcVXF5nMDdexro
Iw23M8lcknV5fPuD33WhieS17WbXlq_ZYEA4WaulGXi9veHczN1S9oFPUlnM3d13R7A63bZjCKvWYlnN
7W5etxd2dfLgEJysixj8lKRxUifL2f04lfWM8ucwKVb8TumsMqG7eturRF5SxSYNodmBKNNkIA
```

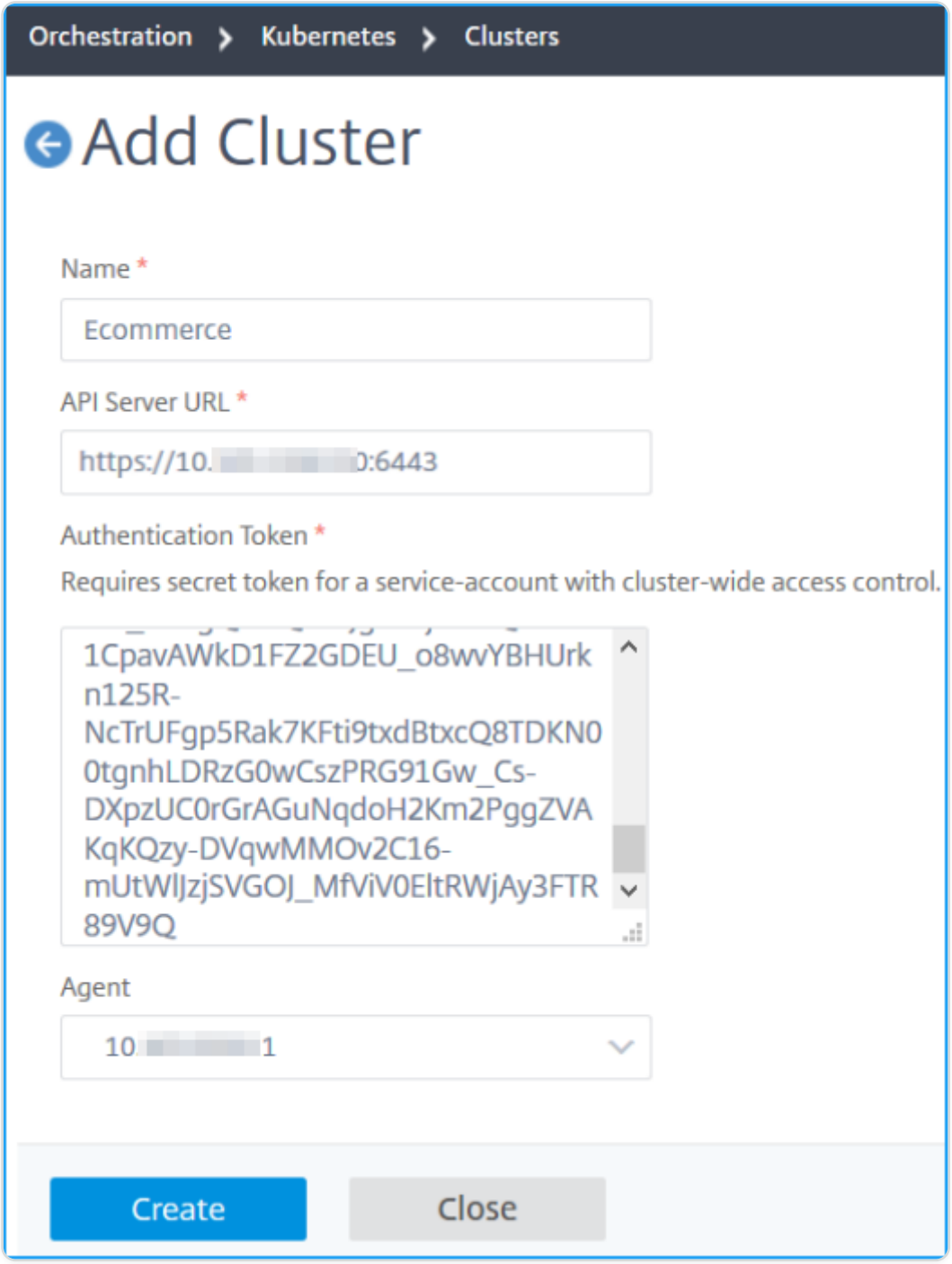
d. Select the agent from the list.

Note

> If you are using an ADM agent, ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable auto select virtual servers for licensing

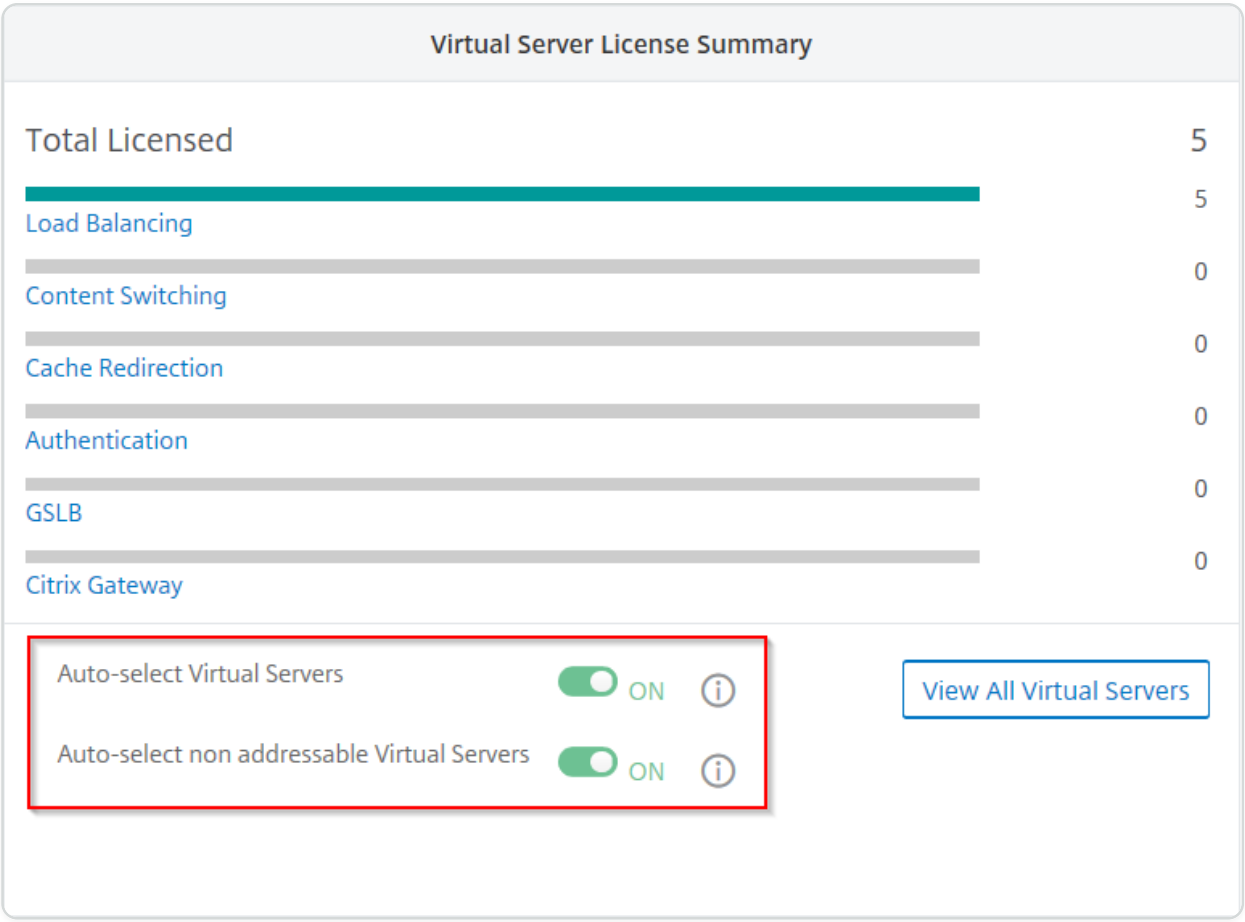
Note

> Ensure you have sufficient virtual server licenses. For more information, see Licensing

After you add Kubernetes cluster in NetScaler ADM, you must ensure to auto-select virtual servers for licensing. Virtual servers must be licensed to display data in Service Graph. To auto-select virtual servers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Under **Virtual Server License Summary**, enable **Auto-select Virtual Servers** and **Auto-select non addressable Virtual Servers**.



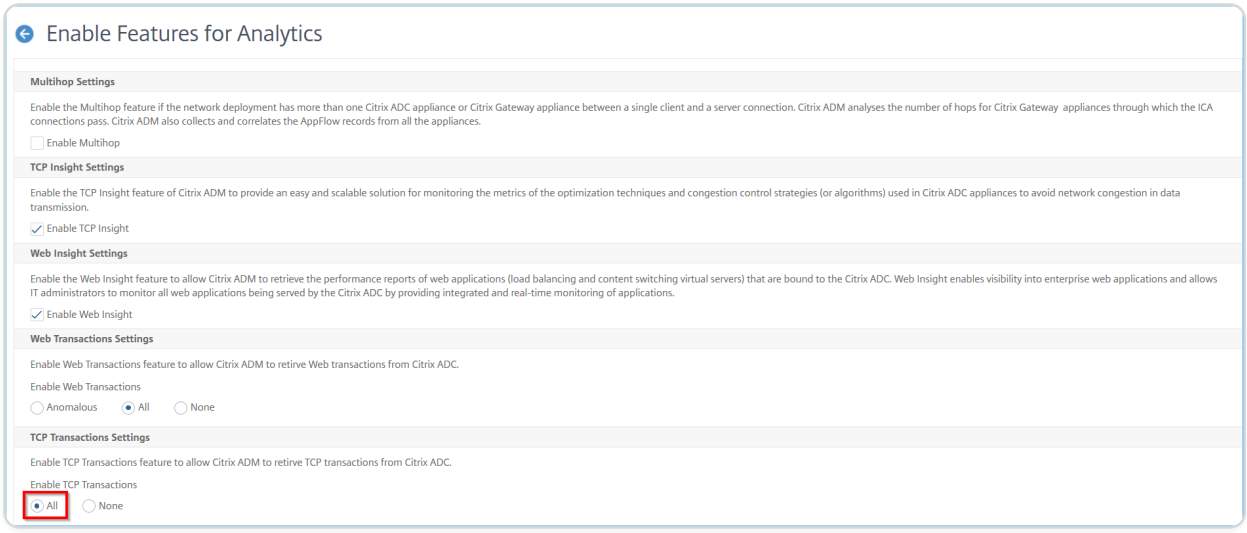
Enable Web Transaction and TCP Transaction settings

After you add the Kubernetes cluster and enable the auto-select virtual servers, change the **Web Transaction Settings** and **TCP Transactions Settings** to **All**.

1. Navigate to **Settings > Analytics Settings**.

   The **Analytics Settings** page is displayed.
2. Click **Enable Features for Analytics**.
3. Under **Web Transaction Settings**, select **All**.
4. Under **TCP Transactions Settings**, select **All**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **OK**.

Send traffic to microservices

Next, you must send traffic to microservices to get the service graph populated in NetScaler ADM.

1. Determine the Ingress IP and port

   `export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')`

   `export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')`

   `export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')`

2. Access the Bookinfo front end application using cURL. The `productpage` service must return 200 OK response.

   `curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage`

   `curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage`

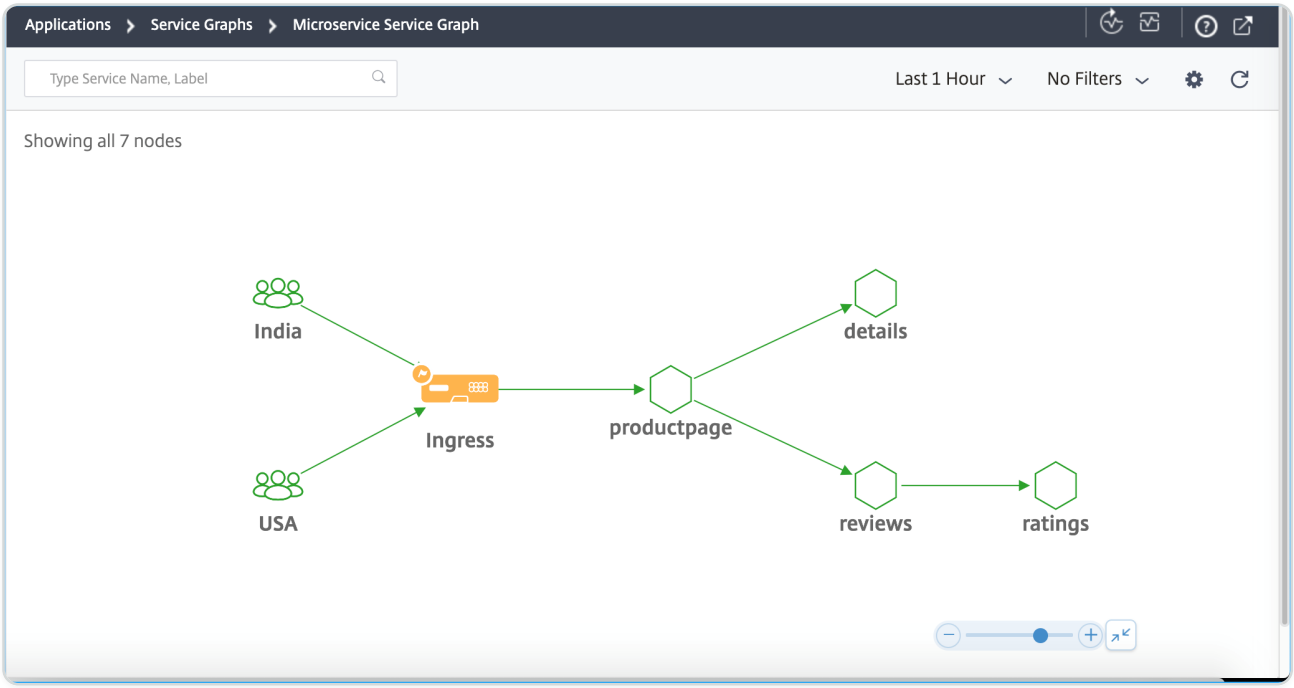
3. Visit `https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage` from a browser.

   The **Bookinfo** page is displayed.

4. Ensure that $INGRESS_HOST and $SECURE_INGRESS_PORT is replaced by an IP address and a port value.

After you send traffic to microservices, the service graph is populated approximately in 10 minutes duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Using the service graph, you can analyze various service details such as metrics, errors, and so on. For more information, see Service graph.

Detailed procedures to set up single tier or unified ingress topology

The prerequisites to deploy the single tier or unified ingress topology is available at Setting up service graph.

Add VPX or SDX or MPX or BLX instance in NetScaler® ADM

To get the tier-1 ADC instance analytics in service graph, you must add the VPX/SDX/MPX/BLX instance in NetScaler ADM and enable **Web Insight**.

1. Navigate to **Infrastructure > Instances > NetScaler**
2. Click the **Add** option to add the instance. For more information, see Add instances in NetScaler ADM
3. After adding the instance, select the virtual server and enable **Web Insight**. For more information, see Manage licensing and enable analytics on virtual servers

Add Kubernetes cluster in NetScaler ADM

To add the Kubernetes cluster:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to NetScaler ADM with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

   a. **Name** - Specify a name of your choice.

   b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.

      i. On the Kubernetes master node, run the command `kubectl cluster-info`.

      ```
      root@kmaster:[redacted]# kubectl cluster-info
      Kubernetes master is running at https://10.[redacted]:6443
      KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/
      services/kube-dns:dns/proxy

      To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
      ```

      ii. Enter the URL that displays for **"Kubernetes master is running at."**

   c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler ADM. To generate an authentication token:

      On the Kubernetes master node:

      i. Create a service account by using the YAML.

         `kubectl create -f adm_svc_account.yaml`

         The service account is created.

      ii. Run `kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa` to bind the cluster role to service account.

         The service account now has the cluster-wide access.

         A token is automatically generated while creating the service account.

      iii. Run `kubectl describe sa citrixadm-sa` to view the token.

      iv. To get the secret string, run `kubectl describe secret <token-name>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@kmaster:~# kubectl describe secret citrixadm-sa-token-79knw
Name:         citrixadm-sa-token-79knw
Namespace:    default
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: citrixadm-sa
              kubernetes.io/service-account.uid: 136270eb-1fe1-11ea-b603-72328a2
af136

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1025 bytes
namespace:  7 bytes
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V
hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiw
ia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImNpdHJpeGFkbS1zYS10b2t
lbi03OWtudyIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50Lm5hbWU
iOiJjaXRyaXhhZG0tc2EiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3V
udC51aWQiOiIxMzYyNzBlYi0xZmUxLTExZWEtYjYwMy03MjMyOGEyYWYxMzYiLCJzdWIiOiJzeXN0ZW0
6c2VydmljZWFjY291bnQ6ZGVmYXVsdDpjaXRyaXhhZG0tc2EifQ.JsU4JPcyFoXA6Vn5Dxa137ca_hI0
wzY1Ajv0ctHN7NeU4YC_I6H5xgNAKnqj2rJPlQEmSZQygPOrxduLDYsNBCT9fH4sv1aBdOzzpkCIDW6y
6BmX4IaC6HTFPGO54zSDzjPmuKkPzyIRa4twUSvxfhwXE6JRy99iJjgPBraL65ct99bcVXF5nMDdexro
Iw23M8lcknV5fPuD33WhieS17WbXlq_ZYEA4WaulGXi9veHczN1S9oFPUlnM3d13R7A63bZjCKvWYlnN
7W5etxd2dfLgEJysixj8lKRxUifL2f04lfWM8ucwKVb8TumsMqG7eturRF5SxSYNodmBKNNkIA
```

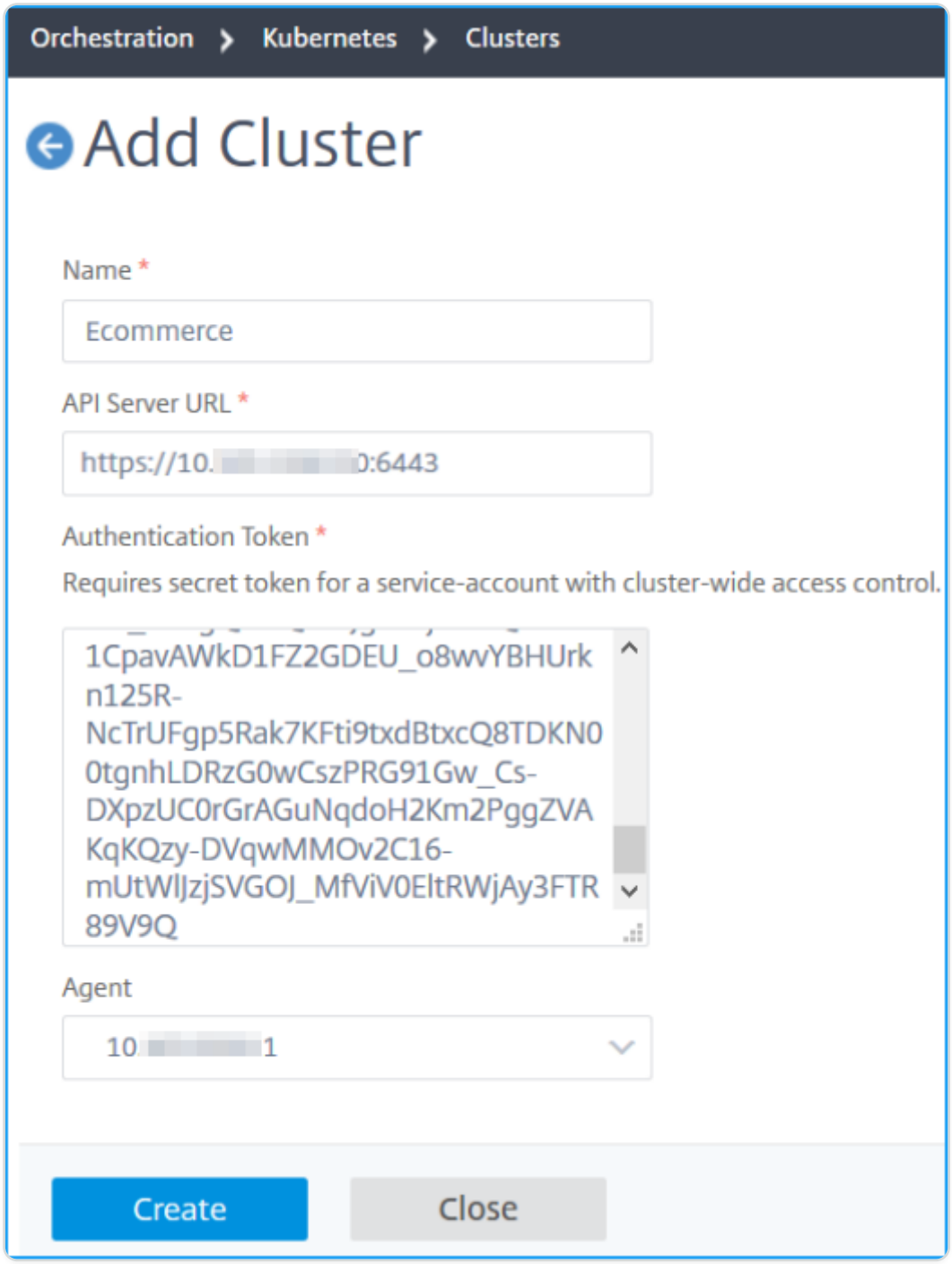
d. Select the agent from the list.

Note

> Ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Optional telemetry data for NetScaler® telemetry program

NetScaler Console feature usage

The following table displays the list of optional data collected as part of the NetScaler telemetry program:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
platform	The platform where the NetScaler Console is hosted. For example, Citrix Hypervisor
deploy	Checks if NetScaler Console deployment type is standalone or HA pair
is_agt	Checks if agent is configured or not
is_cloud	Checks if NetScaler Console deployment is NetScaler Console service or NetScaler Console on-prem
is_cntr	Checks if NetScaler Console deployment is in Kubernetes cluster
is_dr	Checks if the disaster recovery node is configured or not
t_ten	The total tenant count that is connected with NetScaler Console
num_of_ns_upgrade_jobs	The total upgrade jobs used
security_advisory_enabled	Whether Security Advisory is enabled in NetScaler Console on-prem
webinsight	Whether Web Insight is enabled in lb or cs virtual server
webinisight_usage	Whether any active hdx sessions (yes or no)
adm_analyt_hdx_apps	The total number of requests from the device that has HDX insight enabled
adm_analyt_hdx_users	The users count connected through Virtual Desktop
adm_analyt_sec_insight	The total number of requests from the device that has Security insight enabled
adm_analyt_vpn_users	The total users count connecting through VPN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
adm_analyt_webinsight	The total number of requests from the device that has Web insight enabled
anomalyinsight	Indicates whether the request feature is enabled in the lb or cs virtual server
count	The total issue count related to analytics
feature	The feature category for the identified issue. The feature can be BOT_INSIGHT, DEVICE, GATEWAY_INSIGHT, HDX_INSIGHT, SECURITY_INSIGHT, SERVICE_GRAPH, SWG_INSIGHT, WEB_INSIGHT, WEB_SECURITY_BOT_INSIGHT
feature	The analytics feature enabled on the load balancing virtual servers
feature	The analytics feature enabled on the content switching virtual servers
feature	The analytics feature enabled on the VPN virtual servers
gwinsight	Indicates whether ICA_REQUEST feature is enabled on a VPN virtual server
gwinsight_usage	Indicates whether any HDX users in the last day (yes or no)
gw_hdx_insights	The export of HDX insight and Gateway insight enabled
hdxinsight	Indicates whether ICA_Request feature is enabled in a VPN server
hdxinsight_usage	Indicates whether there is any HDX users for the last day

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
issue_type	The issue category for which the identified issue belongs to. For example, licensing, configuration
secinsight	Indicates whether the security insight is enabled in the lb or cs virtual server
secinsight_usage	Whether any security attacks found in the last day (yes or no)
sub_issue_type	The sub-issue category for the identified issue. The sub issue can be NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT, APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
total_api_discovery	The total NetScaler instances receiving API requests
total_csvserver_ft_enabled	The total content switching virtual servers where at least one analytics feature is enabled
total_lbvserver_ft_enabled	The total load balancing virtual servers where at least one analytics feature is enabled
total_vpnserver_ft_enabled	The total VPN virtual servers where at least one analytics server is enabled
total_web_transaction_analytics	The total NetScaler instances enabled with Web transaction analytics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
t_radius_svr	The total RADIUS authentication servers configured in NetScaler Console
t_ldap_svr	The total LDAP authentication servers configured in NetScaler Console
t_tacacs_svr	The total TACACS authentication servers configured in NetScaler Console
agt_pl_azure	The agent platform type
agt_pl_citrix_hypervisor	The agent platform type
agt_pl_docker	The agent platform type
agt_pl_esx	The agent platform type
agt_pl_hyper_v	The agent platform type
agt_pl_gcp	The agent platform type
agt_pl_kvm	The agent platform type
agt_pl_kubernetes	The agent platform type
agt_pl_unknown	The agent platform type
agt_pl_aws	The agent platform type
agent_id	The unique ID of the deployed agent
city	The city where agent is deployed
country	The country where agent is deployed
platform	The platform where the NetScaler Console is hosted. For example, Citrix Hypervisor
region	The region where agent is deployed
total_active_agents	The total agents that in UP state

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_agents	The total agents configured
version	The agent version
city	The datacenter city
isCloud	Whether it is on-prem or cloud
mas_platform	The NetScaler Console platform
prod	The name of the product
prodVer	The Console build version
total_k8s	The NetScaler Console hosted on the Kubernetes cluster. The total Kubernetes clusters
total_apps	The total applications in NetScaler Console
total_custom_sites	The total custom sites configured in NetScaler Console
total_managed_apps	The total managed applications in NetScaler Console
total_custom_apps	The total custom applications in NetScaler Console
root	The NetScaler Console disk utilization details in /var, /root, /flash, /var/mps directories
total	The total NetScaler Console disk space (Unit: Bytes)
used	The total utilized NetScaler Console disk space
free	The total available NetScaler Console disk space

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_api_requests	The total requests through API to NetScaler Console in the last 24 hours. This also includes remote proxy users (requests from the agent).
total_api_external_requests	The total requests through API to NetScaler Console that exclude the requests from the agent
total_gui_requests	The total users logged in to the NetScaler Console GUI in the last 24 hours
total_users	The total count of NetScaler Console local users
total_config_audit	The total Config Audit template configured in NetScaler Console
total_config_job	The total Config jobs created in NetScaler Console
total_ssl_certs	The total SSL certification that are created/ modified/deleted from NetScaler Console
total_custom_event_rules	The total custom event rules created in NetScaler Console
total_event_rules	The total event rules created in NetScaler Console
total_ingress_deployed	The total ingress controllers in Kubernetes.
total_ipam	The total IPAM providers added in NetScaler Console
total_ipam_configured	The total IPAM networks added in NetScaler Console
total_network_report	The total Network Report created in NetScaler Console
total_pager_duty_profile	The total PagerDuty profiles added in NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
gw_hdx_insights	Whether HDX insight and Gateway Insight export enabled
total_rbac_groups	The total RBAC groups configured in NetScaler Console
total_slack_profile	The total Slack profiles added in NetScaler Console
total_ssl_certs	The total SSL certification that are created/ modified/deleted from NetScaler Console
total_stylebook_config_store_count	The total config packs created in NetScaler Console
total_user_sb_stylebook_count	The total custom config packs created in NetScaler Console
configpack	The total number of stored configpack from StyleBooks
isContainer	Whether the NetScaler Console is deployed in a container platform
percent	The total disk space used for var_mps, root, flash, var

Required telemetry data for NetScaler® telemetry program

The following tables display the list of required data collected as part of the NetScaler telemetry program:

NOTE:

Some parameters are collected through a script that is pushed from NetScaler Console to NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing

PARAMETERS	DESCRIPTION
flex_vpx_inst_entitled	The total entitled VPX instances
flex_vpx_inst_allocated	The total allocated VPX instances
flex_sdx_inst_entitled	The total entitled SDX instances
flex_sdx_inst_allocated	The total allocated SDX instances
flex_mpx_inst_entitled	The total entitled MPX instances
flex_mpx_inst_allocated	The total allocated MPX instances
flex_plt_bw_entitled	The entitled platinum bandwidth
flex_plt_bw_allocated	The allocated platinum bandwidth
flex_ent_bw_entitled	The entitled enterprise bandwidth
flex_ent_bw_allocated	The allocated enterprise bandwidth
flex_std_bw_entitled	The entitled standard bandwidth
flex_std_bw_allocated	The allocated standard bandwidth
flex_vpx_fips_inst_entitled	The total entitled FIPS instances
flex_vpx_fips_inst_allocated	The total allocated FIPS instances
license_name	The license type or the feature name
peak_license_usage	The peak usage of license applied on the NetScaler instances (allocation)
peak_bandwidth_usage	The peak usage from the NetScaler instances
avg_license_usage	The average usage of license applied on the NetScaler instances (allocation)
avg_bandwidth_usage	The average usage from the NetScaler instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
license_edition	Platinum/Enterprise/Standard bandwidth
Feature Name	The license feature name
Host ID	The device host ID
License serial number	The serial number of the license
License Start Date	The start date of the license
License End Date	The end date of the license
License SA Date	The license subscription advantage date
tenantnslictype	The license type such as CPL, CUL
instance_id	The unique identifier of the instance
instance_mode	Checks if the instance is a standalone or HA pair
instance_state	The instance status (Up/Down)
is_local_license	Checks if the license is hosted in NetScaler Console
is_pooled_license	Checks if the license is a pooled license
license_edition	The license type (Platinum/Standard/ Enterprise)
license_end_date	Total number of days for the license to expire
platform	The device type
plt_license_allocation	The platinum license allocation
std_license_allocation	The Standard license allocation
ent_license_allocation	The Enterprise license allocation
nslicensingtype	The licensing type (Flexed or Fixed)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_pooled_devices	The total NetScaler instances (both managed and unmanaged) with pooled licenses
perc_discovered_vservers	The % of discovered/entitled virtual servers
perc_used_vservers	The % of used/entitled virtual servers
pool_cpxvcpu_entitled	The total pool CPX vCPUs entitled
pool_cpxvcpu_used	The total pool CPX vCPUs used
pool_entbw_entitled	The total pool Enterprise bandwidth entitled [MBps]
pool_entbw_used	The total pool Enterprise bandwidth used [MBps]
pool_entvcpu_entitled	The total pool Enterprise vCPUs entitled
pool_entvcpu_used	The total used pool Enterprise vCPUs used
pool_fips_instances_entitled	The total pool FIPS instances entitled
pool_fips_instances_used	The total used pool FIPS instances
pool_instances_entitled	The total pool instances entitled
pool_instances_used	The total used pooled instances
pool_perc_bw_used	The % of used bandwidth
pool_perc_instances_used	The % of used instances
pool_perc_vcpu_used	The % of used vCPUs
pool_pltbw_entitled	The total pool Platinum bandwidth entitled [MBps]
pool_pltbw_used	The total pool Platinum bandwidth used [MBps]
pool_pltvcpu_entitled	The total pool Platinum vCPUs entitled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
pool_pltvcpu_used	The total pool Platinum vCPUs used
pool_stdbw_entitled	The total pool Standard bandwidth entitled
pool_stdbw_used	The total pool Standard bandwidth used
pool_stdvcpu_used	The total pool Standard vCPUs Used
total_discovered_vservers	The total discovered virtual servers
total_entitled_vservers	The total entitled virtual servers
total_used_vservers	The total used virtual servers

NetScaler Gateway feature usage

The following data telemetry is collected only if your NetScaler Gateway on-prem version is **14.1-25.53 or later** / **13.1-53.22 or later** build:

PARAMETERS	DESCRIPTION
accessMode	The type of access mode. For example, ICA, VPN
bytesTransferred	The total bytes sent and received per session
epaScans	The total number of EPA scans
features	The features enabled in NetScaler Gateway
id	The unique identifier of the usage event
prod	Identification of the originating product and deployment of the usage event
prodVer	The Gateway product version
email	The gateway user email (email will be hashed)*
st	The current time of the data being pulled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
type	The event type used by CAS to identify the managed Gateway usage events
userName	The Gateway username. Note: The name will be hashed*.
ver	The version of the telemetry event

NetScaler deployment

PARAMETERS	DESCRIPTION
total_active_managed_devices	The total NetScaler instances that are in UP state
total_nsap_device	The total admin partition instances in NetScaler Console
total_managed_devices	The total managed NetScaler instances in NetScaler Console
instance_mode	Checks if the instance is a standalone or HA pair
instance_state	The instance status (Up/Down)
dev_pl_aws	The device platform type
dev_pl_azure	The device platform type
dev_pl_citrix_hypervisor	The device platform type
dev_pl_esx	The device platform type
dev_pl_gcp	The device platform type
dev_pl_hyper_v	The device platform type
dev_pl_kvm	The device platform type
dev_pl_unknown	The device platform type

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
dev_pl_vpx_on_sdx	The device platform type
total_blx_device	The total managed BLX instances in NetScaler Console on-prem
total_cpx_device	The total managed CPX instances in NetScaler Console
total_ng_device	The total managed Gateway instances in NetScaler Console
total_ngvpx_device	The total managed Gateway VPX instances in NetScaler Console
total_ns_device	The total managed MPX instances in NetScaler Console
total_nssdx_device	The total managed SDX instances in NetScaler Console
total_nsvpx_device	The total managed VPX instances in NetScaler Console
total_nswg_device	The total managed Web Gateway instances in NetScaler Console
total_nswgvpx_device	The total managed Web Gateway VPX instances in NetScaler Console
device_id	The VPX instance unique ID
device_platform	The platform where the VPX instance is hosted
state	The current status (UP or Down) of the VPX instance
aaa_vservers	The total number of AAA virtual servers
cs_vservers	The total number of content switching virtual servers
gslb_vservers	The total number of GSLB virtual servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
lb_vservers_http	The total number of HTTP LB virtual servers
lb_vservers_ssl	The total number of SSL virtual servers
version	The build version of the NetScaler instances

NetScaler feature usage

PARAMETERS	DESCRIPTION
total_aaa_devices	The total NetScaler instances configured with AAA virtual servers
aaa_as_Request_tot_blocked	The total number of HTTP requests blocked by appfw profile for AAA
aaatm_as_Request_tot_blocked	The total number of HTTP requests blocked by appfw profile for AAATM
version	The NextGen API version
as_Requests_aaatm_lb	The total number of HTTP requests processed by appfw module on behalf of aaatm_lb module
as_Requests_vpn	The total number of HTTP requests processed by appfw module on behalf of vpn module
nsapisec_builtin_tot_hits	The total number from the built-in API Security Schema for Project Shield
nsapisec_builtin_tot_validated_success	The total number of requests successfully passed the built-in API Security Schema for Project Shield
svpn_as_Request_tot_blocked	The total number of HTTP requests blocked by appfw profile for VPN
appfw.appfirewallrequests	The total number of WAF requests through the appfw profile

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
appfw.appfirewallrequestsrate	The total rate of WAF requests through appfw profile
appfwprofile.appfw_block	The total number of blocked passed per profile
appfwprofile.appfw_bypass	The total number of requests passed per profile
appfwprofile.appfw_drop	The total number of dropped passed per profile
appfwprofile.appfw_reset	The total number of reset passed per profile
bot requests	The total number of bot requests through appfw profile
bot_signature_version	The version of bot signature used
botrequestsrate	The rate of bot requests through bot profile
waf_signature_version	The version of WAF signature used
waf.as_requests	The total number of requests done through all WAF profiles that also include default profiles
waf.as_req_bytes	The total number of requests done through all WAF profiles that exclude default profiles
ingress_controllers	The total number of ingress controllers
admin_partitions	The total number of partitions
gslb_site_tot_RequestBytes	The total requests in bytes passing through the gslb profile
gslb_site_tot_Requests	The total requests pass through gslb profile
gslb_sites	The total number of gslb sites
gslb.services	The total number of gslb services
analytics.profile	The total number of analytics profile

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
appfw.policies	The total number of AppFlow policies
appfw.profiles	The total number of AppFlow profiles
bot.policies	The total number of Bot policies
bot.profiles	The total number of Bot profiles
category	The device classification. For example, Gateway
cluster.nodes	The total number of cluster nodes
cr	The total number of Cache Redirection virtual servers
cs.all	The total number of Content Switching virtual servers
cs.gw	The total number of Content Switching virtual servers used as gateway
cs.used	The total number of addressable Content Switching virtual servers not bound to localhost and of WEB or TCP protocol
deployment_type	The NetScaler deployment type (HA pair or standalone)
ha.node	The IP address of the HA pair. Note: The IP address will be hashed*.
lb.all	The total number of all load balance virtual servers
lb.gw	The total number of load balance virtual servers used as gateway
lb.used	The total number of addressable load balance virtual servers not bound to localhost and of WEB or TCP protocol

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
nsip	The NSIP of the NetScaler. Note: The IP address will be hashed*.
reason	The detailed reason for classification
servers	The total number of virtual servers
serviceGroups	The total number of ServiceGroups
services	The total number of services
services.dns	The total number of ADNS/ADNS_TCP type services
vpn	The total number of VPN virtual servers
vpn.ica	The total number of ICA VPN virtual servers
vservers.gw	The total number of LB + CS + CR virtual servers used a gateway
vservers.used	The total number of addressable LB + CS + CR virtual servers not bound to localhost and of WEB or TCP protocol
waf_protection	The waf protection type
total_cs_devices	The total NetScaler instances configured with content switching virtual servers
total_waf_devices	The total NetScaler instances that are enabled with WAF violations
total_bot_devices	The total NetScaler instances that are enabled with Bot violations
total_icaproxy_devices	The total NetScaler instances that are enabled with HDX insight
iprep_cur_ip_count	The ipreputation hits count

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_gslb_devices	The total NetScaler instances configured with Global server load balancing virtual servers
total_gw_devices	The total NetScaler instances that are enabled with SSL VPN
total_lb_devices	The total NetScaler instances configured with load balancing virtual servers
total_lb_devices_http	The total NetScaler instances configured with load balancing HTTP virtual servers
total_lb_devices_ssl	The total NetScaler instances configured with load balancing SSL virtual servers
telemetry_collected_at	The time at which the telemetry script is run
state	The current status (Up or Down) of the VPX instance
exp.events	The total number of analytics profiles used for exporting events
exp.managementlogs	The total number of analytics profiles used for exporting management logs
exp.metrics	The number of analytics profiles used for exporting metrics
exp.auditlogs	The number of analytics profiles used for exporting auditlogs to Splunk
exp.prometheus	The number of analytics profiles used for exporting to Prometheus
telemetry_collected_at	The time at which the telemetry script is run
state	The current status (Up or Down) of the VPX instance
version	The build version of the devices

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
exp.events	The total number of analytics profiles used for exporting events
exp.managementlogs	The total number of analytics profiles used for exporting management logs
exp.metrics	The number of analytics profiles used for exporting metrics
exp.auditlogs	The number of analytics profiles used for exporting auditlogs to Splunk
exp.prometheus	The number of analytics profiles used for exporting to Prometheus
gw_hdx_insights	Whether HDX insight and Gateway Insight export enabled
collected_at	The time at which the telemetry script has collected the data
total_audit_logs	The total number of audit logs configured through the NextGen API
total_backends	The total number of backends configured through the NextGen API
total_frontends	The total number of frontends configured through the NextGen API
total_health_check	Total number of health_check resources configured through the NextGen API
total_http_redirects	The total number of HTTP-redirects configured through the NextGen API
total_http_responders	The total number of HTTP-responders configured through the NextGen API
total_load_balancing_settings	The total number of load-balancing settings configured through the NextGen API

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_routes	The total number of routes (policies) configured through the NextGen API
total_tls_settings	The total number of TLS settings configured through the NextGen API
total_http_settings	The total number of HTTP settings configured through the NextGen API
total_value_set	The total number of value sets configured through the NextGen API
total_wireshark_expressions	The total number of wireshark filters used to configure through the NextGen API
last_login_time	The timestamp of the user's last login with the NextGen API
last_usage_time	The timestamp of the user's last interaction with the NextGen API
ngapi_version	The NextGen API version
state	The current NextGen API status
total_applications	The total number of applications configured through the NextGen API
total_certificates	The total number of certificates installed through the NextGen API
total_failed_commit	The total number of NextGen API requests failed at the commit stage
total_failed_install	The total number of NextGen API requests failed at the install stage
total_login	The total number of logins into the NextGen API interface
total_request	The total number of requests done through the NextGen API interface

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETERS	DESCRIPTION
total_resources	The total number of NextGen API resources (applications, certificates, health_checks, and so on) configured through the NextGen API
svpn_tot_client_type_AGENT	The total number of Citrix Secure Access clients for Windows
svpn_tot_client_type_IOS	The total number of Citrix Secure Access clients for iOS
svpn_tot_client_type_MAC	The total number of Citrix Secure Access clients for macOS
svpn_tot_client_type_ANDROID	The total number of Citrix Secure Access clients for Android
svpn_tot_client_type_CVPN	The total number of users or devices accessing the Citrix resources through clientless VPN
svpn_tot_client_type_ICA	The total number of Citrix Secure Access clients for ICA access
ns_svpn_tot_epa_failed	The total number of EPA checks failed
ns_svpn_tot_epa_quarantine	The total number of EPA checks failed with quarantine

*The information collected through telemetry, such as email addresses, user names, and IP addresses, is securely pseudonymised by hashing the information at the source using one-way hashing algorithms. As a result, Citrix cannot access or read these values. This telemetry data is used solely for logical asset-matching purposes.

Data governance

Citrix collects statistics on your NetScaler® Application Delivery Management (ADM) deployments to understand the deployment usage and scale. The statistics includes the ADM deployment health, status, and usage pattern on your premises. The statistics helps Citrix proactively troubleshoot issues on your ADM deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Create a customer identity on Citrix Cloud™** - To send important statistics about ADM health, status, and other metrics from ADM on-premises deployment to Citrix Cloud account.

  After you create a customer identity, the “Cloud Connect” establishes the connection between ADM on-prem and ADM service by creating a Citrix Cloud account. See, Configure customer identity.

- **Configure maintenance scripts** - To optimize the database. The database optimization might create tables, alter columns, and more. The same “Cloud Connect” feature is used to configure maintenance scripts. See Database optimization using maintenance scripts.
- **Customer User Experience Improvement Program (CUXIP)** - This program is enabled by default. It collects the usage-data from NetScaler ADM. This data allows optimizing the ADM experience through guided workflows, search articles, product notifications, feedback, surveys, and so on. See, Customer User Experience Improvement Program.

Configure customer identity

NetScaler 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. Provide the Citrix Cloud user credentials on the ADM GUI. For more information, see Sign up for Citrix Cloud.

There are different ways to authenticate yourself on NetScaler ADM. The following sections describe the workflows if you are a new user or an existing user on ADM.

Workflow 1 - If you are a new user

1. Complete the installation of NetScaler ADM on the selected hypervisor.
2. Configure the various required IP addresses.
3. In a web browser, type the IP address of the NetScaler ADM.
4. In the **User Name** and **Password** fields, enter the administrator credentials.

   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.

5. Click **Authenticate** and provide your email address which you have used to register on Citrix Cloud.
6. Select the check box next to **I agree to share data** for telemetry and click **Submit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workflow 2 - if you are an existing user upgrading to the latest ADM version

1. After upgrading the NetScaler ADM to the latest version, in a web browser, type the IP address of the NetScaler ADM.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
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 later in one of the following two ways:

- Navigate to **Settings > System Administration**, and click **Authentication**.
- Click 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 NetScaler ADM and using NetScaler ADM features, you agree and consent that Citrix may collect, store, transmit, maintain, process and use technical, user, or related information about your NetScaler products and services.

Information received by Citrix is always treated in accordance with Citrix.com Privacy Policy.

Diagnostics and data collection

NetScaler ADM collects the following telemetry using customer identity:

- **Actions performed in ADM**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Actions performed using the NetScaler ADM UI/API interface.
  - Actions performed using the NetScaler ADM SDK interface.
  - Count of operations in a single day. This count includes any Non-GET request from API or UI.
  - Count of ADC upgrades done by ADM.
- **NetScaler ADM license information**: Count of entitled virtual servers.
- **Key statistics**:
  - Total count of event rules.
  - Total count of and user defined stylebooks.
  - Count of managed and custom applications.
  - Count of registered agents.
  - Overall throughput across the NetScaler (Rx+Tx).
  - Count of managed instances. This count also includes admin partitions.
  - Count of admins using NetScaler ADM SaaS.
- **Geo-location of NetScaler ADM**
- **Deployment information**: This information includes deployment types such as high-availability, disaster recovery, and ADM agents.

Why data is collected?

The collected telemetry data helps to:

- Recommend correct NetScaler ADM sizing and deployment.
- Proactively troubleshoot issues on ADM on-prem deployments.

Who can use this data?

Citrix is the sole owner of the information collected. Citrix has access to/collect information that you voluntarily give us. We do not sell or rent this information to anyone. We do not share your information with any third party outside of our organization, other than as necessary to fulfill your request. Example: To ship an order or to proactively resolve issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How long we keep your data?

Typically, we store Personal/Usage data until the user is using our Services. Or, we have another purpose to do so. Afterwards, the data is no longer stored than it is required or permitted by law or necessary for internal reporting and reconciliation purposes.

All telemetry data is stored for a period no longer than 13 months or 396 days.

Database optimization using maintenance scripts

Maintenance scripts are used to resolve database related issues on ADM on-premises deployments. The ADM software automatically downloads the database maintenance scripts from ADM service, providing faster resolution for database related issues. Earlier, these issues were resolved by manually running the scripts.

With this feature, ADM on-prem deployment periodically downloads the database maintenance scripts from ADM Service. To do so, ensure to configure customer identity.

Maintenance scripts run daily and weekly. Also, the scripts might create tables or add or remove columns to improve database performance.

Customer User Experience Improvement Program

At Citrix Systems, our aim is to provide our users with an engaging product experience. **Customer User Experience Improvement Program (CUXIP)** uses Pendo to guide users through some common, yet detailed tasks by giving search articles, in-app guides and so on. We also help our users remain abreast of all the recent announcements.

What usage-data is collected over CUXIP?

Usage-data is all about user actions. Also called event-level data, usage data includes everything from the pages our users visit on a website to the number of clicks on a certain feature. Usage-data is valuable information about how users move in our applications. This data allows optimizing our user's experience.

The following are some of the usage-data we collect:

- Details of page views, time spent on every page.
- Visitor id, is a unique anonymized identifier to help identify number of unique visitors on a page.
- Survey statistics – score, views, number of submissions and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How CUXIP helps you?

We use usage-data to improve your experience with ADM. The following are some of the ways in which we intend to enhance customer user experience:

- In-app guided workflows and ability to search relevant articles.
- Participate in a survey from within the app to help improve the product.
- Stay informed about recent announcements and other notifications.
- Post a question or feedback to the product team.

How CUXIP works?

The NetScaler ADM appliance can be in the internal network. The browser must have internet connectivity to get the benefits of the guided assistance on CUXIP.

How can I disable CUXIP on my ADM?

To disable CUXIP, do the following in the ADM GUI:

1. Navigate to **Settings > System Administration**.
2. In **CUXIP Settings**, and disable CUXIP.

Changes to our Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of the changes by posting the new Privacy Policy on this page. We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on Citrix Privacy policy page.

References

Citrix Privacy Policy: `<https://www.citrix.com/about/legal/privacy/>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Back up and restore a NetScaler® ADM configuration in an HA pair

You can back up the current configuration of a NetScaler Application Delivery Management (ADM). In an HA deployment of NetScaler ADM, you can back up and restore the NetScaler 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 failover happens, the restore process fails to complete.

To back up a NetScaler 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** check box.

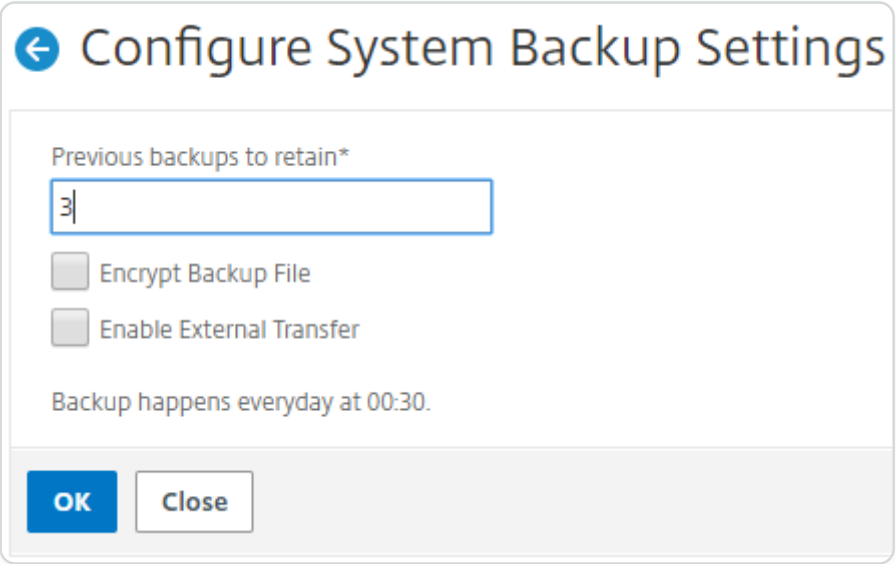
To restore a NetScaler ADM configuration from a backup file:

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 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 NetScaler ADM server and then perform the restore operation. Specify the server, user name and password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see Transfer a NetScaler ADM Backup File to an External System.
3. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure system notification settings

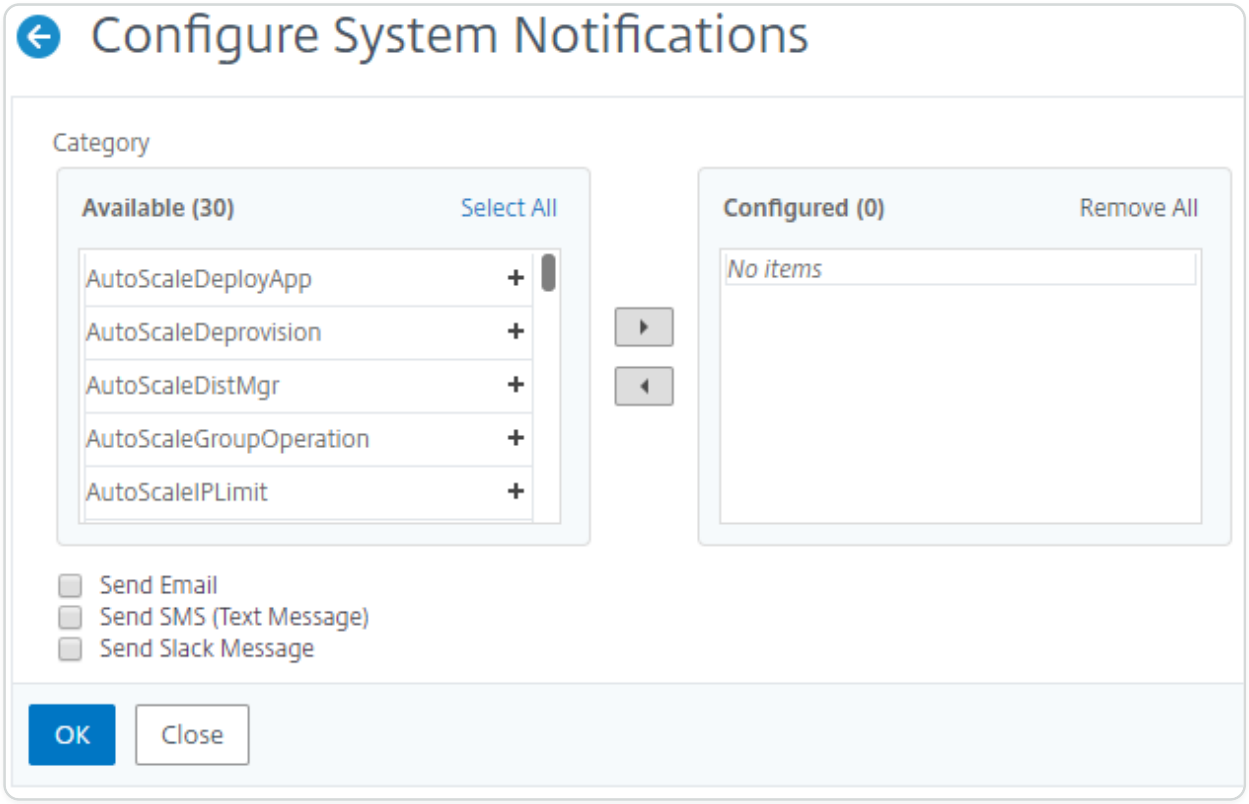
You can send notifications to select groups of users for various system-related functions. These system functions are organized into event categories such as SystemReboot, StatusPoll, and SystemState. You can configure NetScaler® Application Delivery Management (ADM) to send you notifications either through email or SMS. You have to configure an email server or Short Message Service (SMS) gateway server or both 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 NetScaler 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 NetScaler ADM:

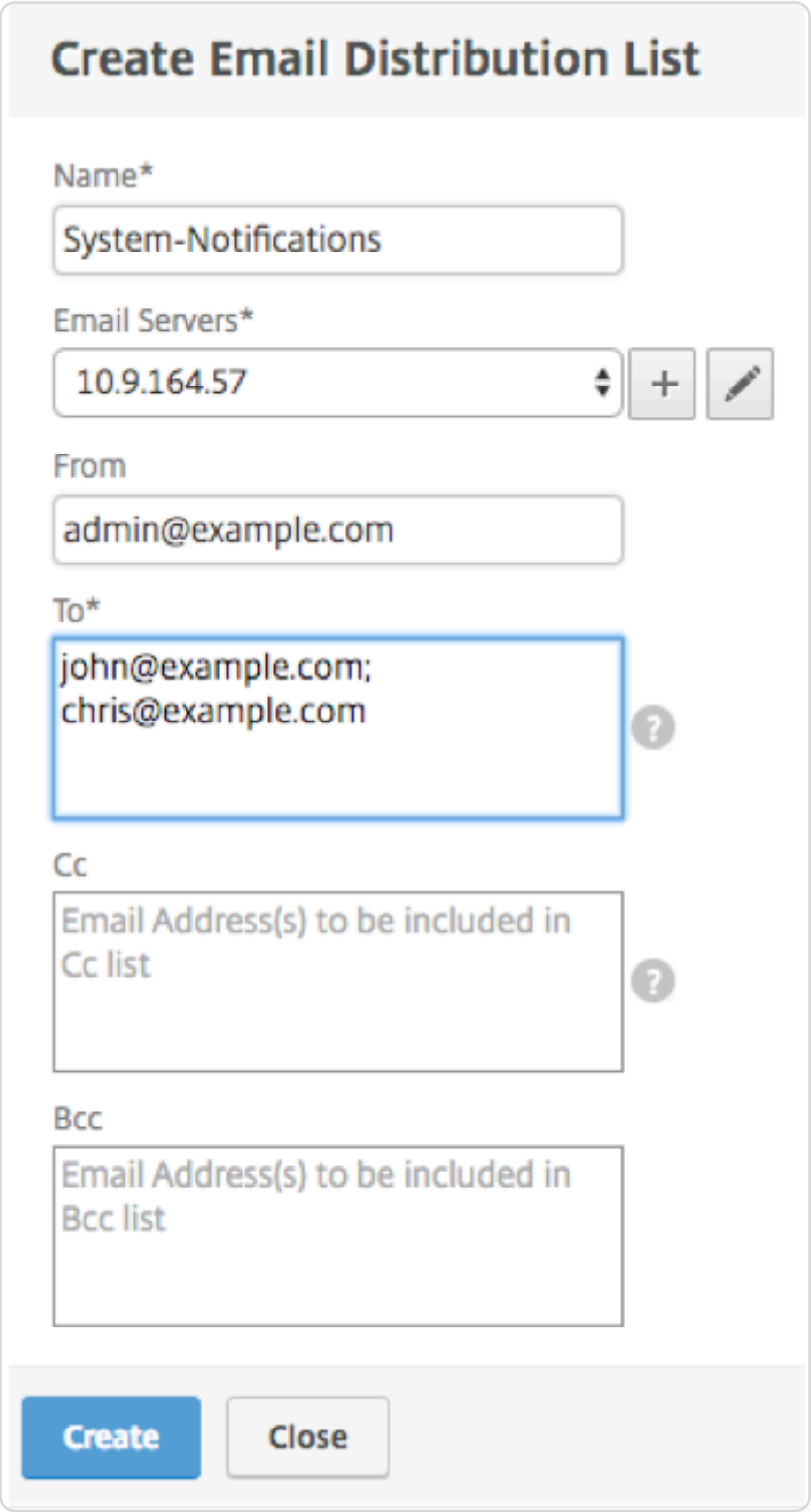
1. Navigate to **System** \> **Notifications**. Under **Settings**, click **Change Notification Settings**.
2. On the **Configure System Notification Settings** page, under **Category**, select a category such as **UserLogin**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



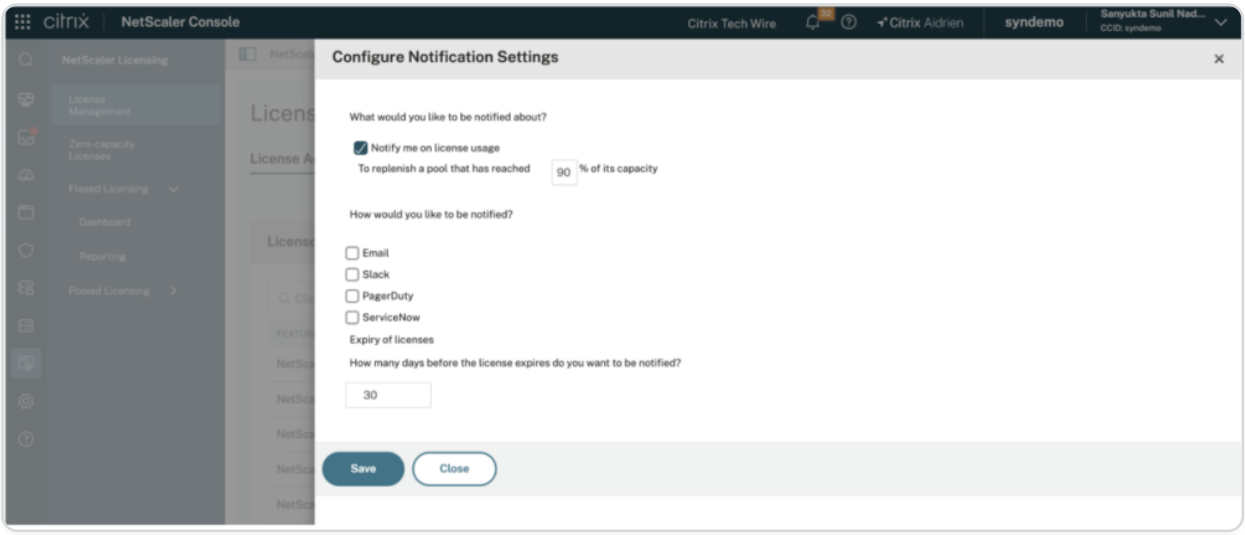
3. Select **Send Email**, and either select an email distribution from the drop-down list or click the "**+**" icon to create a new email distribution list as shown in the following figure. If you want to send text notifications, select **Send SMS (Text Message)** and create an SMS distribution list by clicking the “**+**” icon and specifying SMS server details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 notifications when a user fails to log on to NetScaler ADM by using the CLI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



System notifications are sent for the following events:

CATEGORY	CAUSE
BackupFailure	The system backup fails
DataStorageExceeded	The database storage crosses the limit specified in the license
DeviceBackupFailure	The instance backup fails
`HAMonitoring`	The system HA failover occurs, no heartbeats from a peer node, and database sync failure occurs
HealthMontoring	The CPU, RAM, or Disk utilization crosses threshold value
LicensePool	The license pool crosses the threshold value
Licenses	License fails when applied
PasswordRecovery	Password recovery fails or succeeds
PerfCounterThresholdHigh	The performance counter value exceeds the limit
PerfCounterThresholdNormal	The value of the performance counter is normal
PolicyFailed	Any of the system policies fails

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORY	CAUSE
RemoteDeviceBackupFailure	The remote instance backup fails
RemoteSystemBackupFailure	The remote system backup fails
RemoteSystemBackupNormal	The remote system backup succeeds
SSLCertThreshold	The threshold for a certificate is breached
StatusPoll	Any change in the state of an instance
SubSystemState	Any change in the subsystem state
SystemReboot	The system is rebooted
SystemState	Any change in the state of the system
TrapConfigFailure	Failure occurs when adding SNMP trap on an instance
UserLogin	User authentication fails

Use jobs to upgrade NetScaler instances

You can use NetScaler Application Delivery Management (ADM) to upgrade one or more NetScaler instances. You must know the licensing framework and types of licenses before you upgrade an instance.

When you upgrade your NetScaler instance by creating a maintenance job, perform the pre-validation check on the instances that you want to upgrade.

1. **Check for customizations** - Back up your customizations and delete them from the instances. You can reapply the backed-up customizations after the instance upgrade.
2. **Check the disk usage** - If the `/var` folder has less than 6 GB space and the `/flash` folder has less than 200 MB space, clean up the disk space. Check the following folder paths to clean the disk space:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `/var/tmp/support`
- `/var/core`
- `/var/crash`
- `/var/nsinstall`
- `/var/netscaler/nsbackup`

3. **Check for disk hardware issues** - Resolve the hardware issues if any.

You can upgrade an ADC HA pair in two stages:

1. Create an upgrade job and run on one of the nodes immediately or schedule later.
2. Schedule the upgrade job to run on the remaining node later. Ensure to schedule this job after the initial node's upgrade.

When you upgrade an ADC HA pair, note the following:

- The secondary node is upgraded first.
- Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.
- After the successful HA pair upgrade, an error message appears in the execution history. This message appears if your nodes in the HA pair are on different builds or versions. This message indicates that synchronization between primary and secondary node is disabled.

When you upgrade an ADC cluster, the ADM does pre-upgrade validation on the specified instance only. Before you upgrade, check and resolve customization, disk usage, and hardware issues on the cluster nodes.

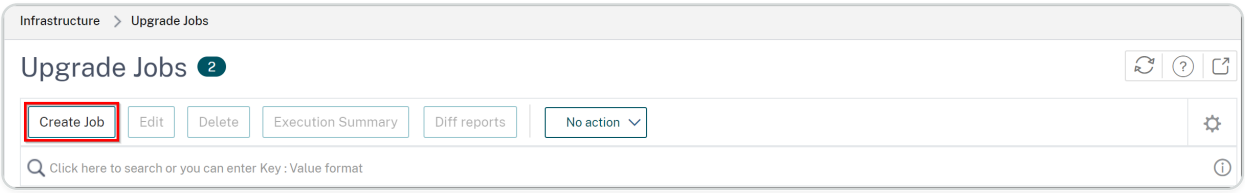
Create an upgrade maintenance job to upgrade ADC instances

NOTE

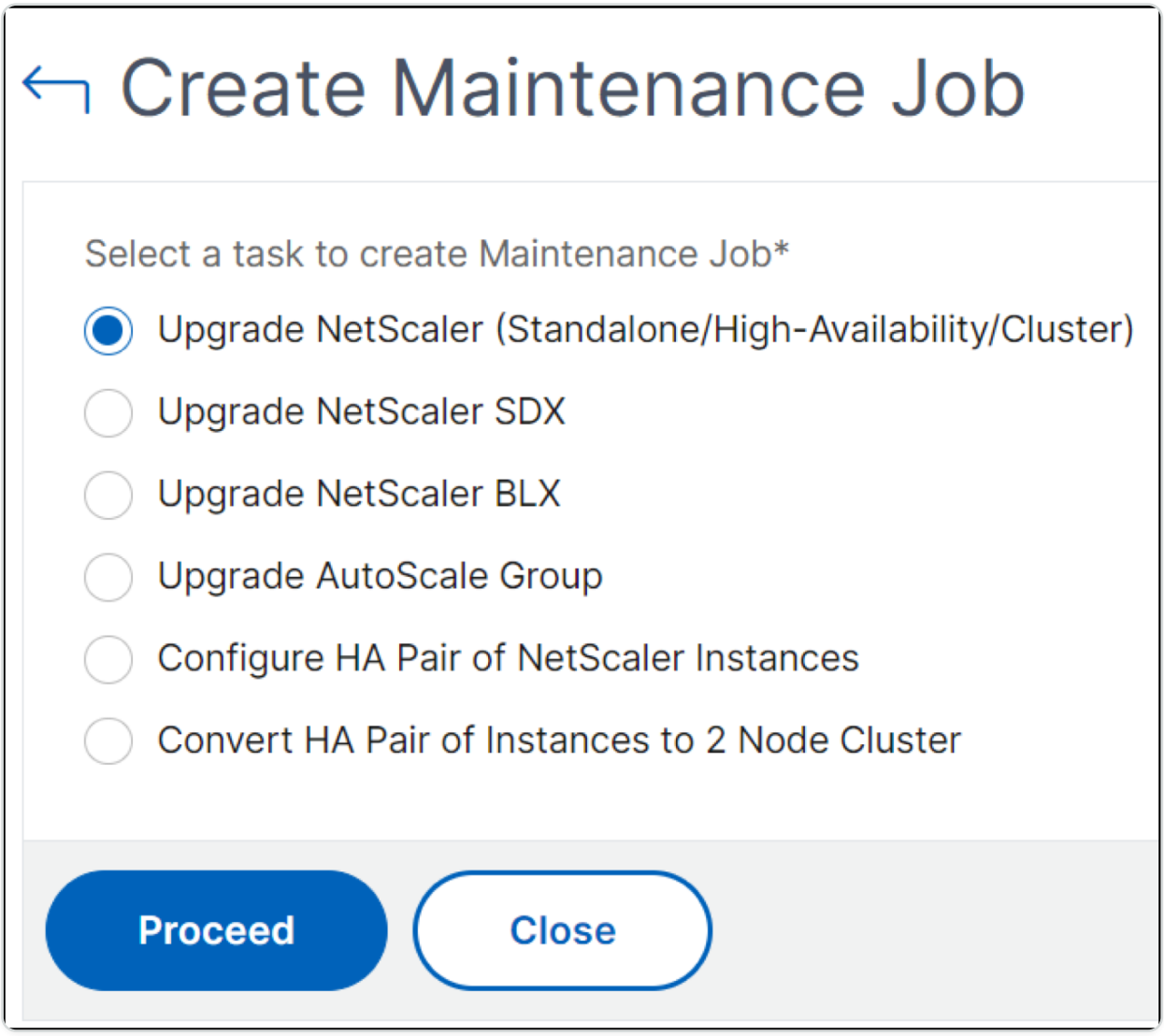
ADC upgrade from higher version to lower version is not supported. For example, if your NetScaler instance is 13.0 82.x, you cannot downgrade the ADC instance to 13.0 79.x or any other earlier versions.

1. In NetScaler® ADM, navigate to **Infrastructure > Upgrade Jobs**. Click the **Create Job** button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

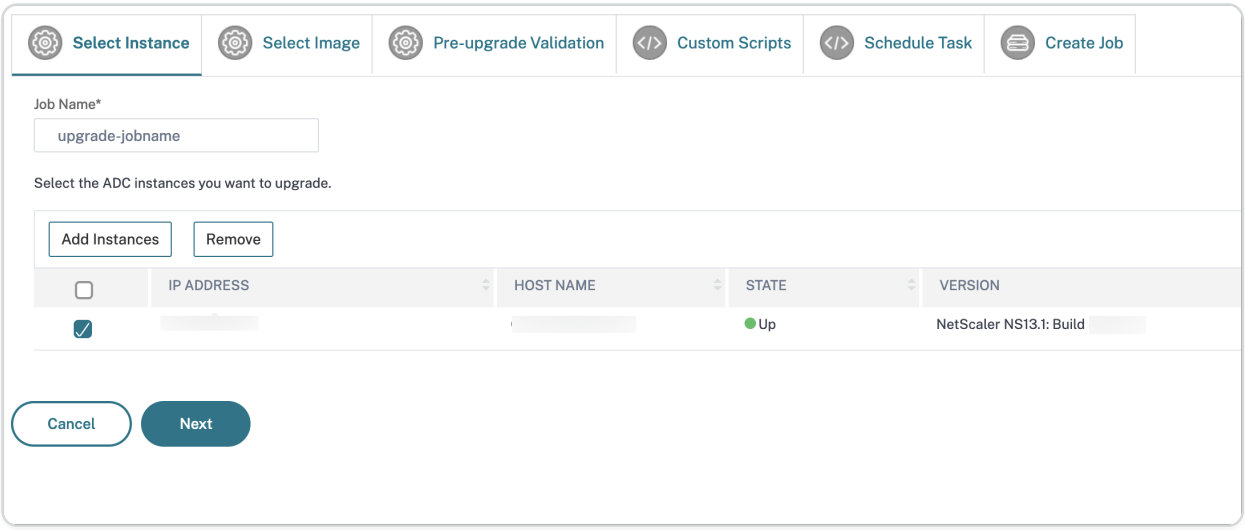


2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/Cluster)** and click **Proceed**.



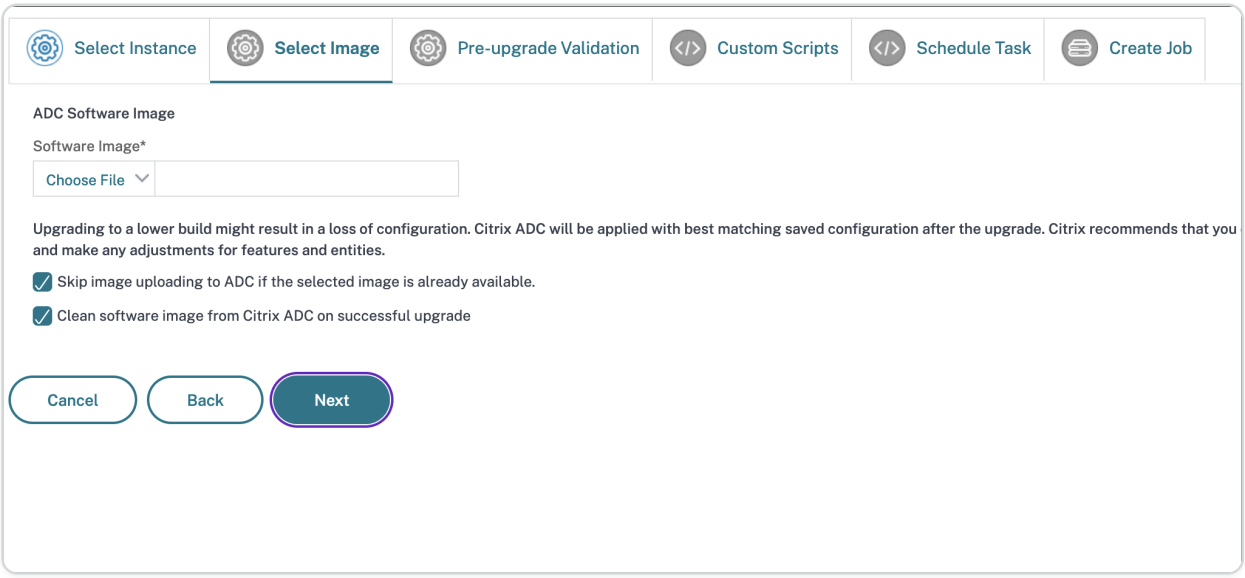
3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add ADC instances that you want to upgrade.
   - To upgrade an ADC high-availability pair, select the IP addresses of the high-availability pair (denoted by the superscript of 'S' and 'P').
   - To upgrade a cluster, select the cluster IP address (denoted by the superscript of 'C').

© 1997–2026 Citrix Systems, Inc. All rights reserved.

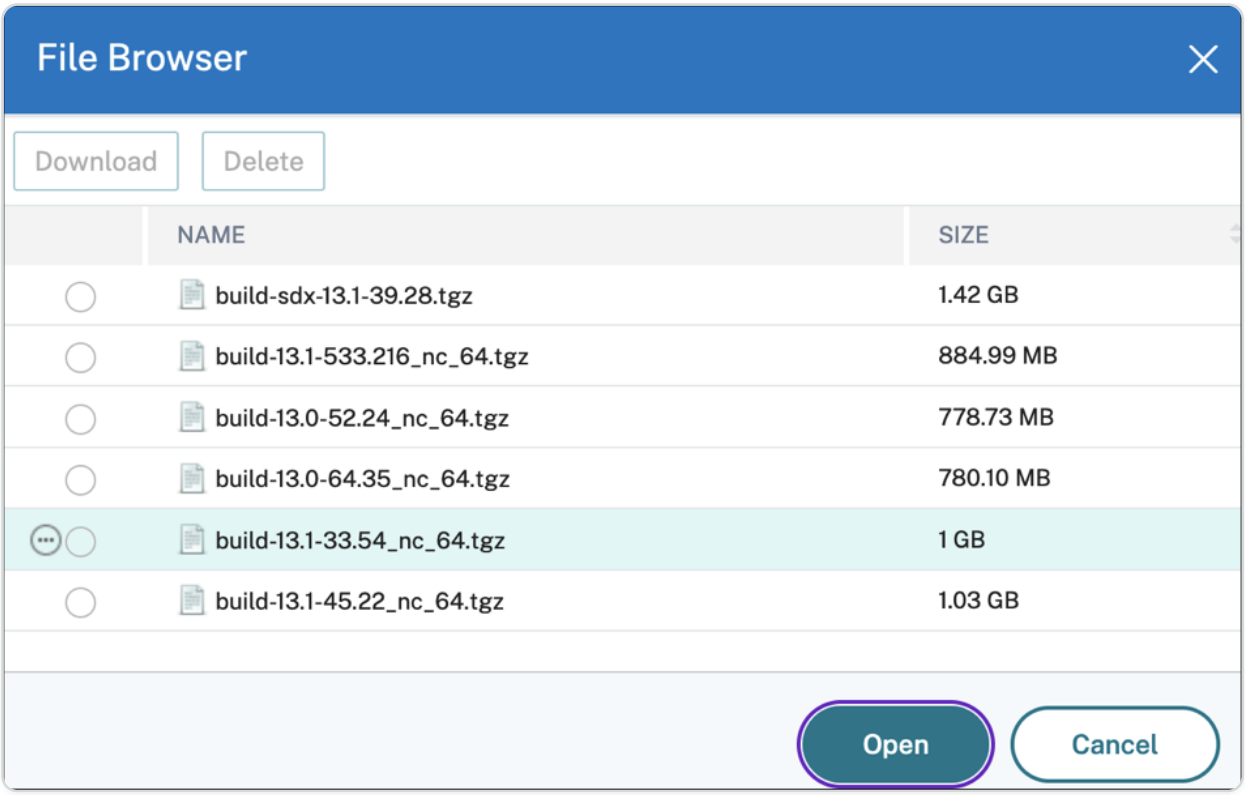


5. In the **Select Image** tab, select an ADC image from your local drive or from the build images.

   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from a NetScaler ADM file browser. The NetScaler ADM GUI displays the instance files that are present at `/var/mps/ns_images`.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Skip image uploading to ADC if the selected image is already available** - This option checks whether the selected image is available in ADC. Upgrade job skips uploading a new image and uses the image available in ADC.
- **Clean software image from NetScaler on successful upgrade** - This option clears the uploaded image in the ADC instance after the instance upgrade.

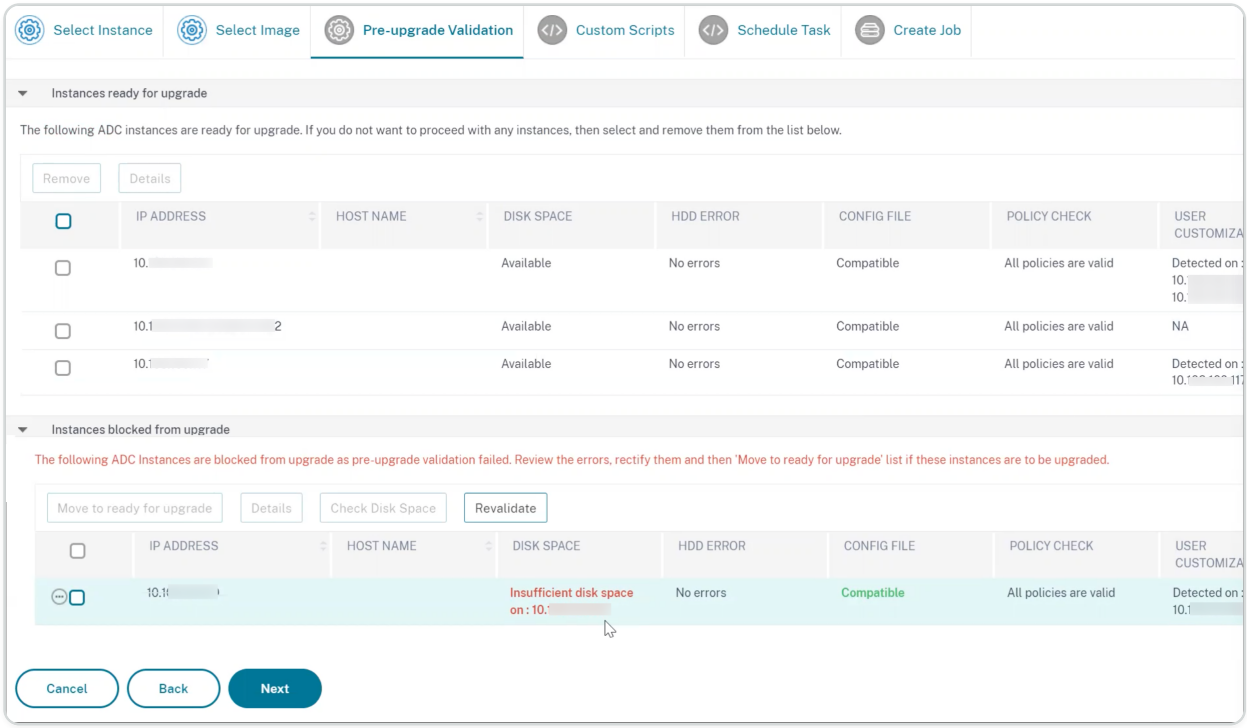
Click **Next** to start the pre-upgrade validation on the selected instances.

6. The **Pre-upgrade validation** tab displays the following sections:

   - **Instances ready for upgrade**. You can continue with the upgrade of these instances.
   - **Instances blocked from upgrade**. These NetScaler instances are blocked from upgrade because of pre-upgrade validation errors.

     You can review, rectify the errors, and then click **Move to ready for upgrade** to upgrade them. If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up ADC disk space.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Policy Check**: If NetScaler ADM finds unsupported classic policies, you can remove such policies to create an upgrade job.

IMPORTANT

If you specify cluster IP address, the ADM does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the NetScaler CLI commands:

   The custom scripts are used to check the changes before and after an ADC instance upgrade. For example:

   - The instance version before and after the upgrade.
   - The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
   - The statistics of virtual servers and services.
   - The dynamic routes.

   An instance upgrade has multiple stages. You can now specify these scripts to run in the following stages:

   - **Pre upgrade**: The specified script runs before upgrading an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Post upgrade pre failover (applicable for HA)**: This stage only applies to the high-availability deployment. The specified script runs after upgrading the nodes, but before their failover.
- **Post upgrade (applicable for standalone) / Post upgrade post failover (applicable for HA)**: The specified script runs after upgrading an instance in the standalone deployment. In the high-availability deployment, the script runs after upgrading the nodes and their failover.

NOTE

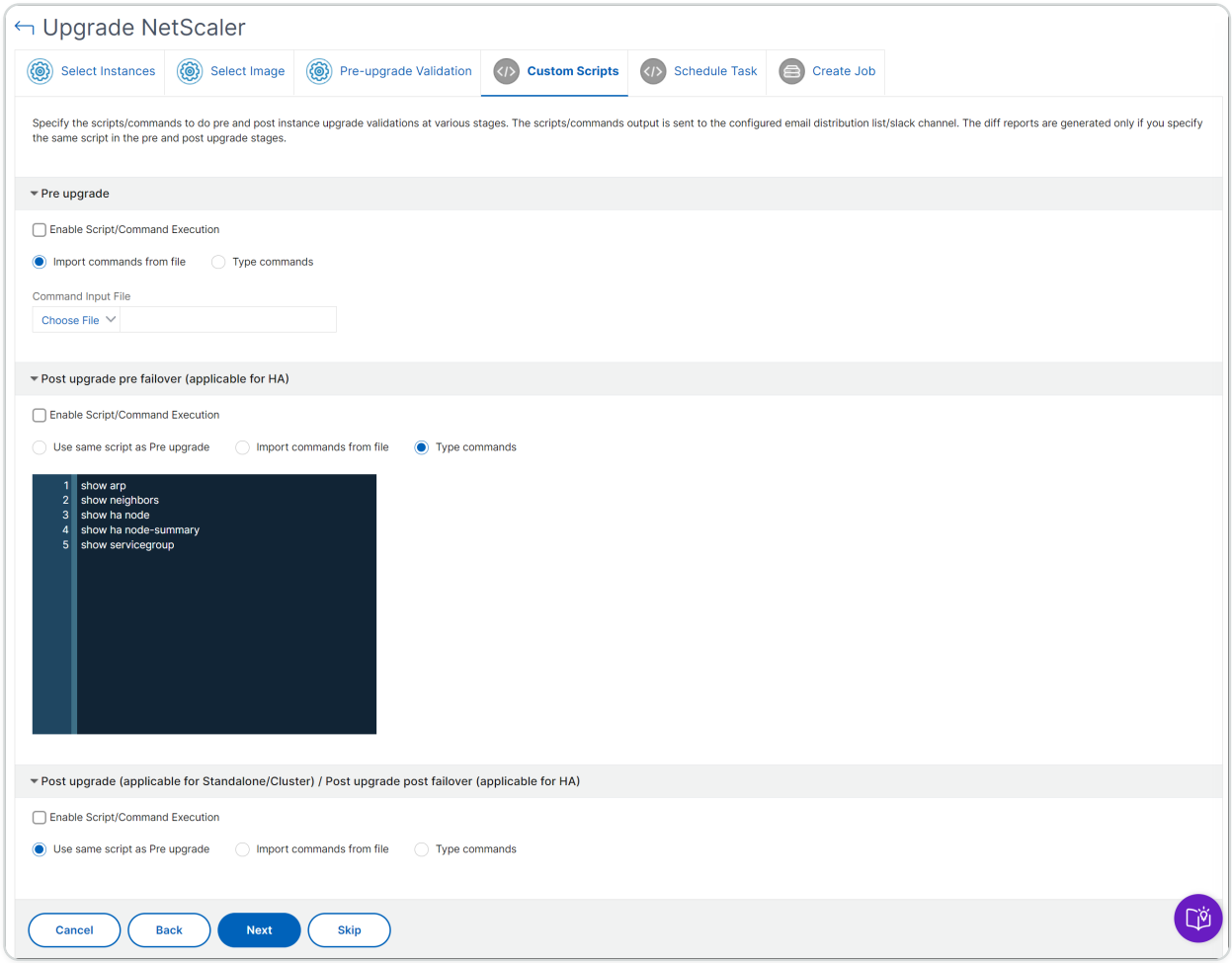
Ensure to enable script execution at the required stages. Otherwise, the specified scripts do not run.

You can import a script file or type NetScaler CLI commands directly in the ADM GUI.

- **Import commands from file**: Select the NetScaler CLI command input file from your local computer.
- **Type commands**: Enter NetScaler CLI commands directly on the GUI.

In the post upgrade stages, you can use the same script specified in the pre-upgrade stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade an ADC HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. In **Create Job**, specify the following details:

   a. Select one of the following options from the **Software Image** list:

      - **Local** - Select the instance upgrade file from your local machine.
      - **Appliance** - Select the instance upgrade file from an ADM file browser. The ADM GUI displays the instance files that are present at `/var/mps/mps_images`.

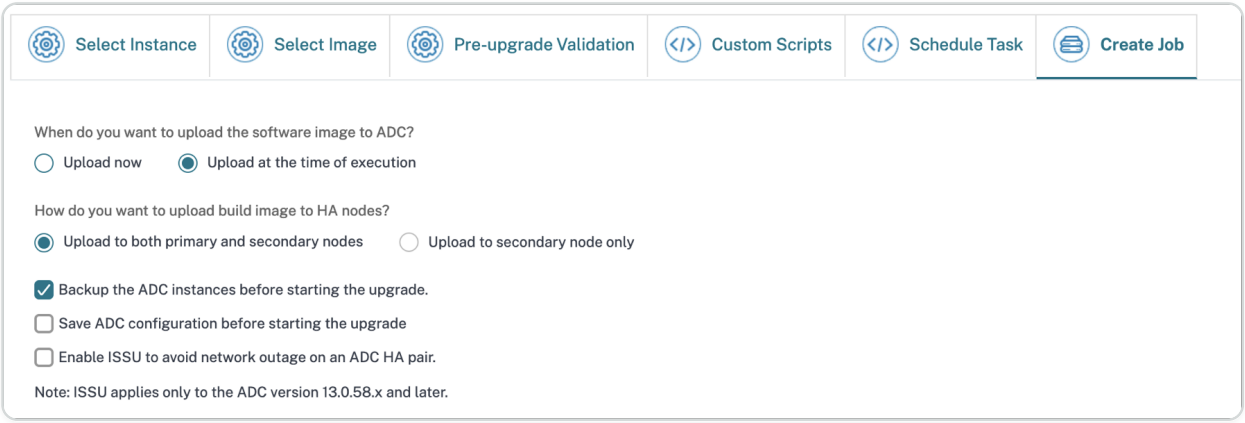
   b. Specify when you want to upload the image to an instance:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
- **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.

For high-availability pair, you can specify the nodes on which you want to upload the image:

- **Upload to both primary and secondary nodes**: Upload the build image file to both the primary and secondary nodes.
- **Upload to secondary node only**: Upload the build image file to only the secondary node. After the secondary node is upgraded, a failover occurs and the build image file is uploaded to the new secondary node which was previously, the primary node.

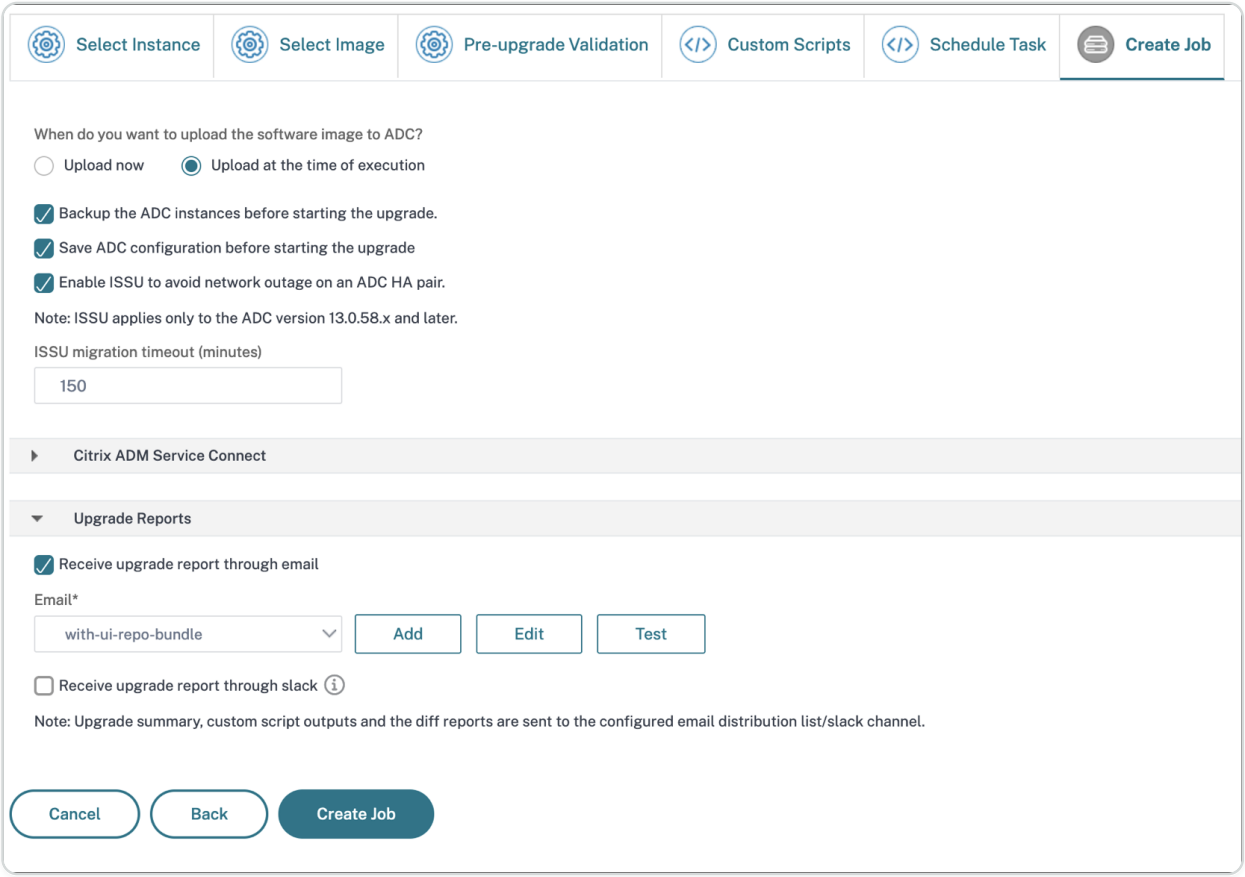


For more information on the available scheduling scenarios for high-availability pair, see Scheduling upgrade jobs for high-availability pair.

- **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the ADC instance after the instance upgrade.
- **Backup the ADC instances before starting the upgrade.** - Creates a backup of the selected ADC instances.
- **Maintain the primary and secondary status of HA nodes after upgrade**: Select this option if you want the upgrade job to start a failover after each node's upgrade. In this way, the upgrade job maintains the primary and secondary status of the nodes.
- **Save ADC configuration before starting the upgrade** - Saves the running ADC configuration before upgrading the ADC instances.
- **Enable ISSU to avoid network outage on ADC HA pair** - ISSU ensures the zero downtime upgrade on an ADC high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an ADC HA pair without downtime. Specify the ISSU migration timeout in minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.



10. Click **Create Job**.

The upgrade job appears in the **Infrastructure > Upgrade Jobs**. When you edit an existing job, you can switch to any tabs if the required fields are already filled. For example, if you are in the **Select Configuration** tab, you can switch to the **Job Preview** tab.

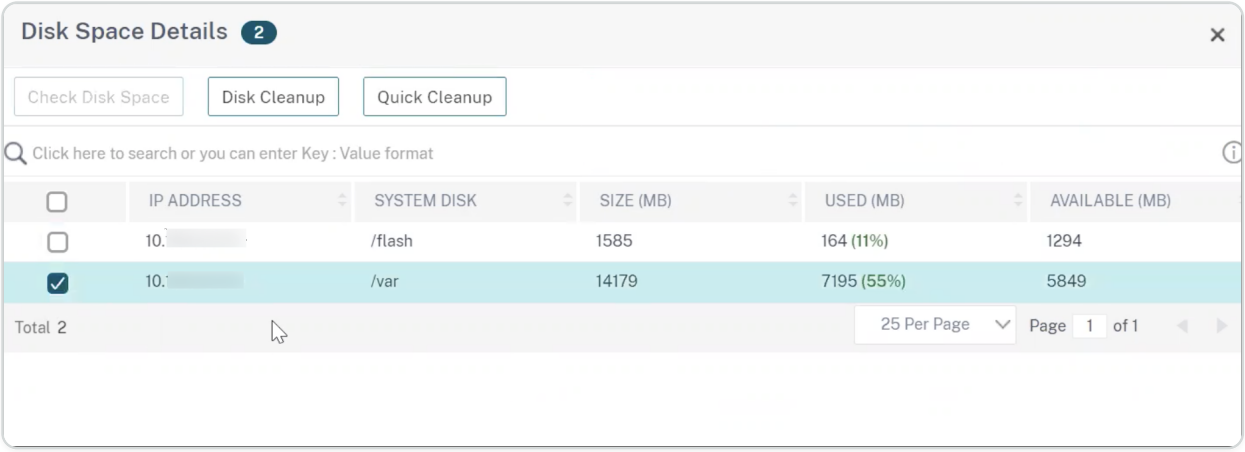
Clean up the ADC disk space

If you face the insufficient disk space issue while upgrading an ADC instance, clean up the disk space from the NetScaler ADM GUI itself.

1. In the **Pre-upgrade validation** tab, the **Instances blocked from upgrade** section displays the instances that failed the upgrade because of Insufficient disk space. Select the instance that has the disk space issue.
2. Click **Check Disk Space**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

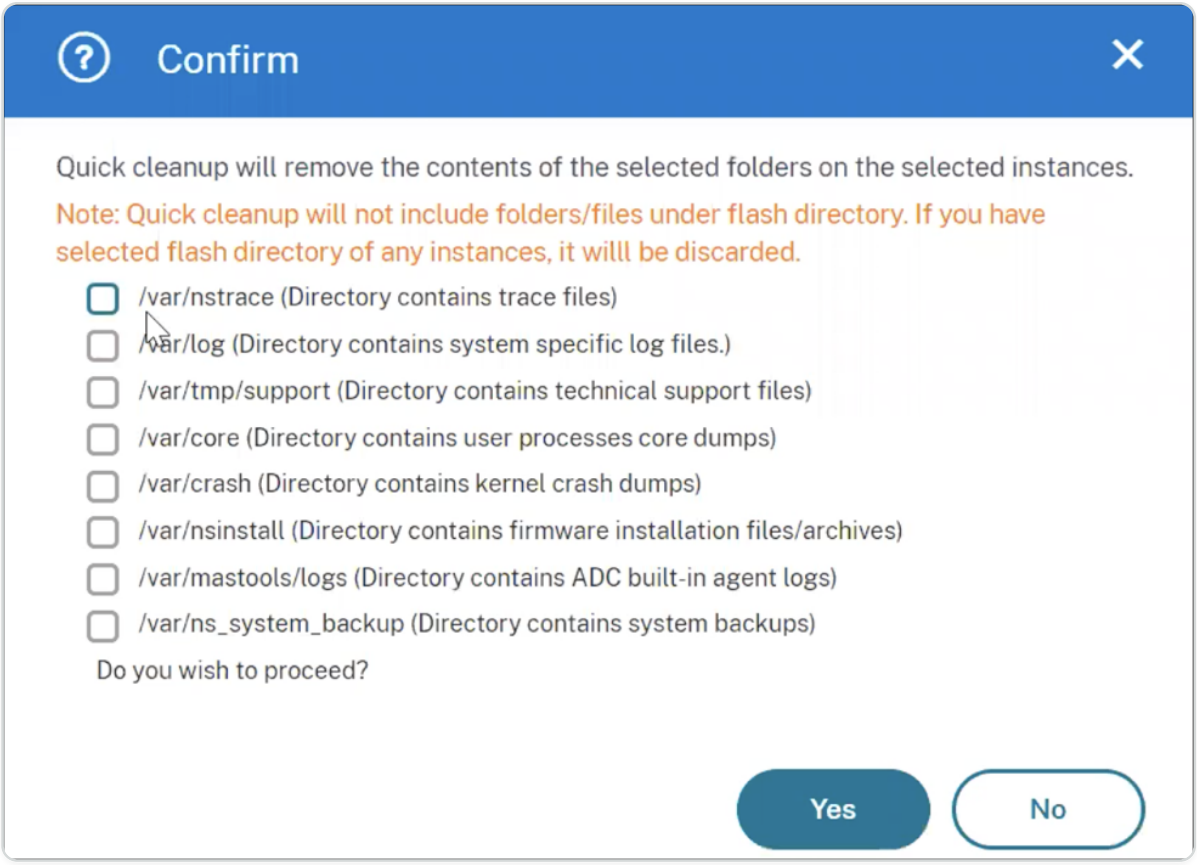
A **Disk Space Details** pane appears. This pane displays the instances, used memory, and available memory.



3. In the **Disk Space Details** pane, select the instance that requires cleanup and do one of the following:

   a. **Disk Cleanup** - Navigate to the required folders or directories and delete them to free up disk space.

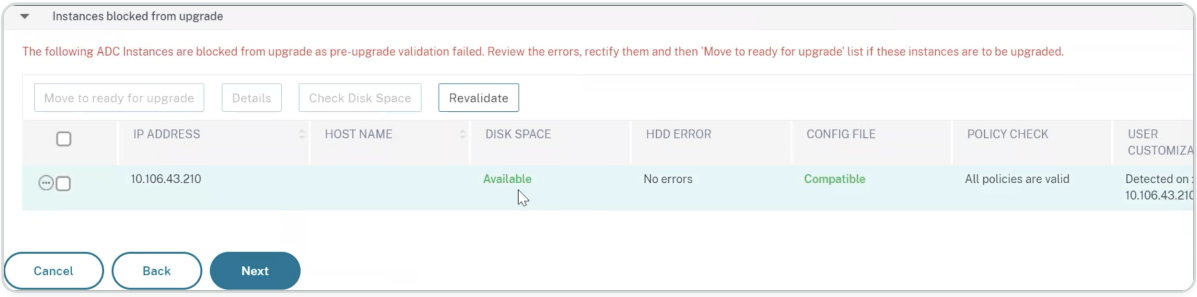
   b. **Quick Cleanup** - Quickly clear up disk space by deleting multiple folders. In the **Confirm** pane that appears, select the folders you want to delete, and click **Yes**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. After clearing up the disk space, you can check if sufficient disk space is now available to upgrade the instance. In the **Instances blocked from upgrade** section, click **Revalidate**.

   In the following example, disk space is available. You can now click **Move to ready for upgrade** to upgrade the instance or click **Next** to continue to the next step.



Scheduling upgrade jobs for a NetScaler high-availability pair

The following table lists the different scheduling scenarios in the **Schedule Task** page and the corresponding upgrade options available in the **Create Job** page:

WHEN DO YOU WANT TO EXECUTE THE UPGRADE JOB?	WHEN DO YOU WANT TO UPLOAD THE SOFTWARE IMAGE TO ADC?	HOW DO YOU WANT TO UPLOAD BUILD IMAGE TO HA NODES?
Upgrade now	Not applicable	**Upload to both primary and secondary nodes** (default option)
	Upload to secondary node only	
Schedule later	**Upload at time of execution** (default option)	**Upload to both primary and secondary nodes** (default option)
	Upload to secondary node only	
	Upload now	Not applicable
Schedule later (when **Perform two stage upgrade for nodes in HA** is selected)	**Upload at time of execution** (default option)	**Upload to secondary node only** (default and only option)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHEN DO YOU WANT TO EXECUTE THE UPGRADE JOB?	WHEN DO YOU WANT TO UPLOAD THE SOFTWARE IMAGE TO ADC?	HOW DO YOU WANT TO UPLOAD BUILD IMAGE TO HA NODES?
	Upload now	Not applicable

Download a consolidated diff report of an ADC upgrade job

You can download a diff report of an ADC upgrade job if custom scripts are specified. A diff report contains the differences between the outputs of the pre-upgrade and post-upgrade script. With this report, you can determine what changes occurred on the ADC instance post upgrade.

NOTE

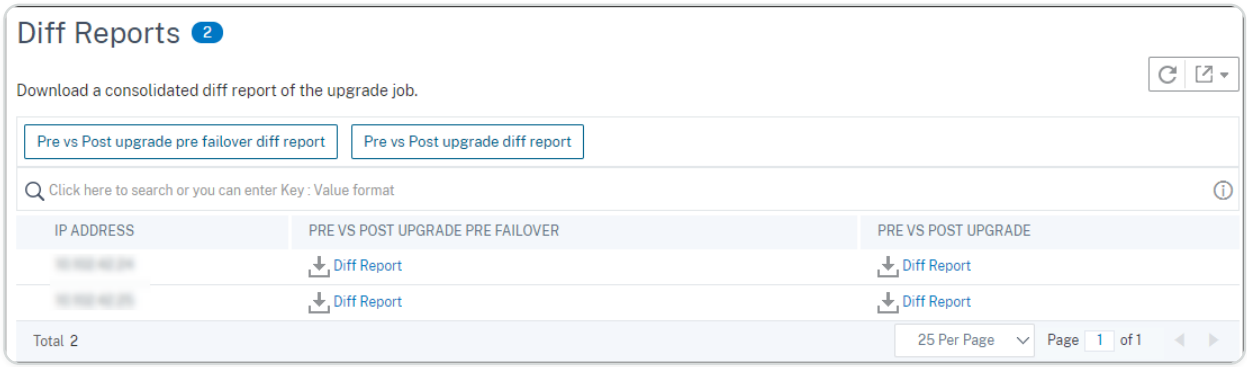
The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages.

To download a diff report of an upgrade job, do the following:

1. Navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**.
2. Select the upgrade job for which you want to download a diff report.
3. Click **Diff Reports**.
4. In **Diff Reports**, download a consolidated diff report of the selected upgrade job.

   In this page, you can download any of the following diff reports type:

   - **Pre vs Post upgrade pre failover diff report**
   - **Pre vs Post upgrade diff report**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure sites for geomaps

A NetScaler Application Delivery Management (ADM) site is a logical grouping of the Citrix Application Delivery Controller (ADC) instances in a specific geographical location. You can have several NetScaler instances within a site that can be monitored and managed by the NetScaler ADM server. You can use the NetScaler ADM server to manage data such as syslog, AppFlow, and SNMP, and others from the managed instances.

To create a Site:

1. Navigate to **Infrastructure > Instances > Sites**, and then click **Add**.
2. In the **Create Site** page, specify the following information:
   a. **Site Type**: Select **Data Center**.

      NOTE

      The site can function as the primary data center or as a branch. Choose accordingly.

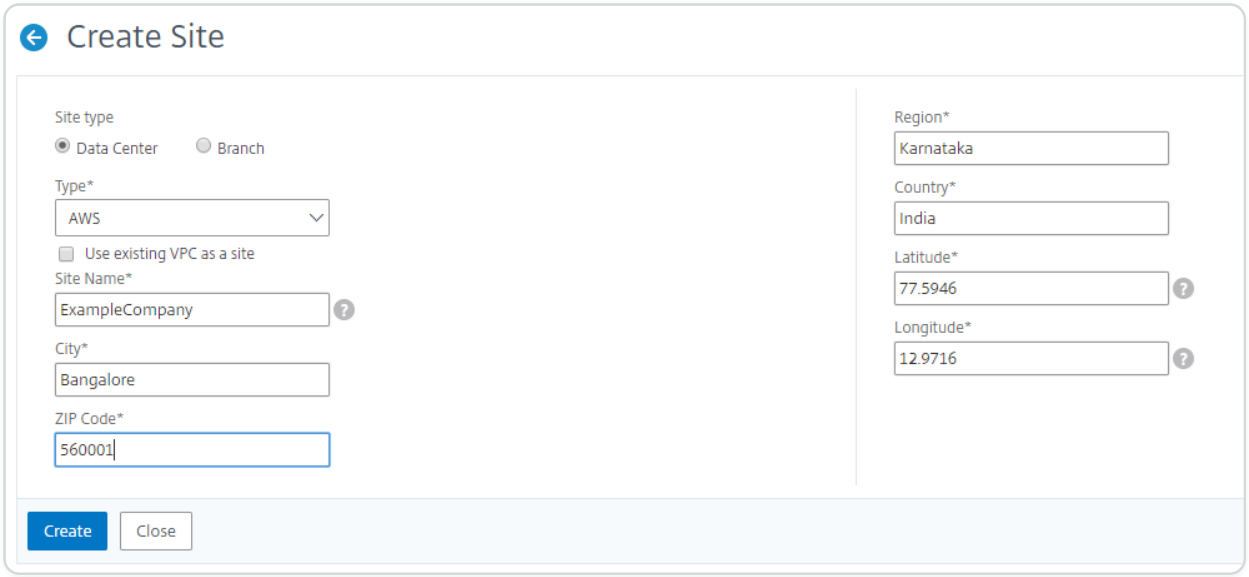
   b. **Type**: Select AWS as the cloud provider from the list.

      NOTE

      Check the **Use existing VPC as a site** box accordingly.

   c. **Site Name**: Type the name of the site.
   d. **City**: Type the city.
   e. **Zip Code**: Type the Zip Code.
   f. **Region**: Type the Region.
   g. **Country**: Type the Country
   h. **Latitude**: Type the latitude of the location.
   i. **Longitude**: Type the longitude of the location.
3. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on adding NetScaler instances to NetScaler ADM, see Adding an Instance to NetScaler ADM.

Modes of telemetry collection

Automated telemetry collection mode

This mode is enabled by default after you upgrade to NetScaler Console on-prem 14.1-25.53 / 13.1-53.22 or later build.

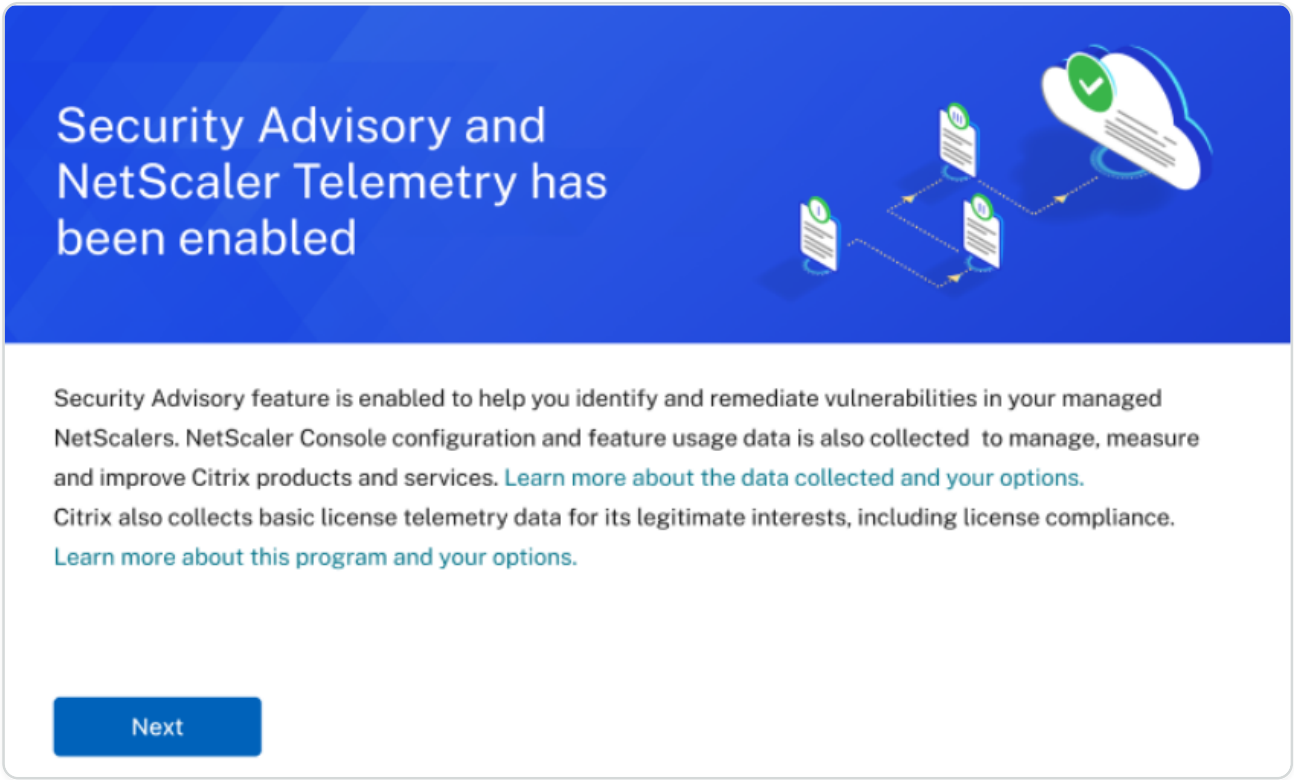
Prerequisites for the automated telemetry collection mode:

- Ensure that you have an internet connection or have a proxy server configured in NetScaler Console on-prem for Citrix Cloud™ accessibility.
- Ensure that the following endpoint URLs are reachable:
  - Download Service URL: `https://download.citrixnetworkapi.net`
  - Service URL: `https://adm.cloud.com` (required only in 13.1-57.x or earlier build).
  - Auto-enabled channel: `https://safehaven.adm.cloud.com`
- Ensure that the following port is open:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

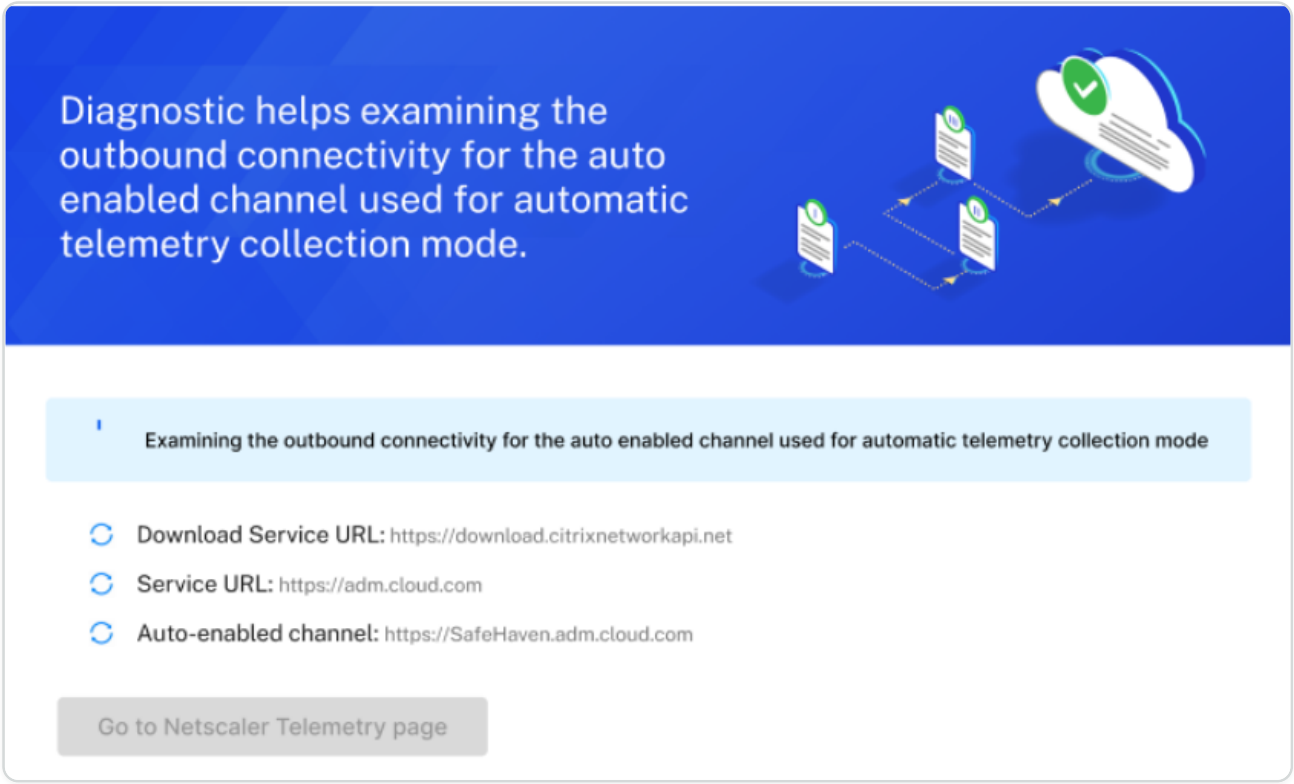
PORT	TYPE	DETAILS	DIRECT OF COMMUNICATION
5140	UDP	Port to receive NetScaler Gateway telemetry data	NetScaler to NetScaler Console

After you upgrade to 14.1-25.53 or 13.1-53.22 build and navigate to the **NetScaler Telemetry** page, click **Next** in the following pop-up window:

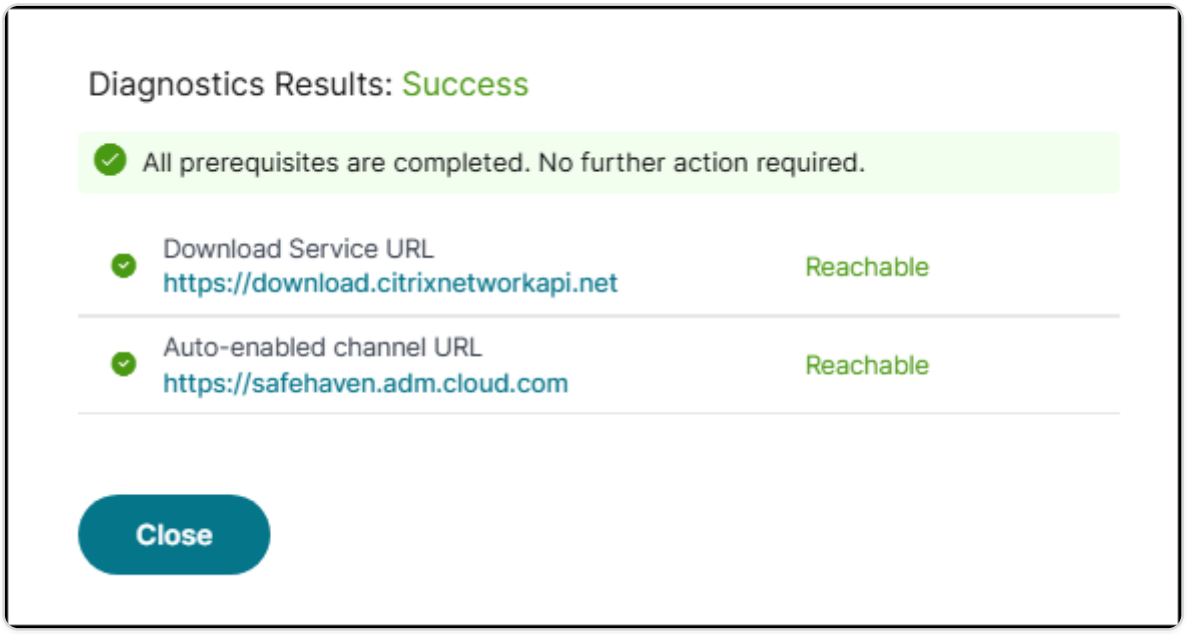


The diagnostic helps to examine the outbound connectivity to these endpoint URLs and lets you know if they are in reachable status.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

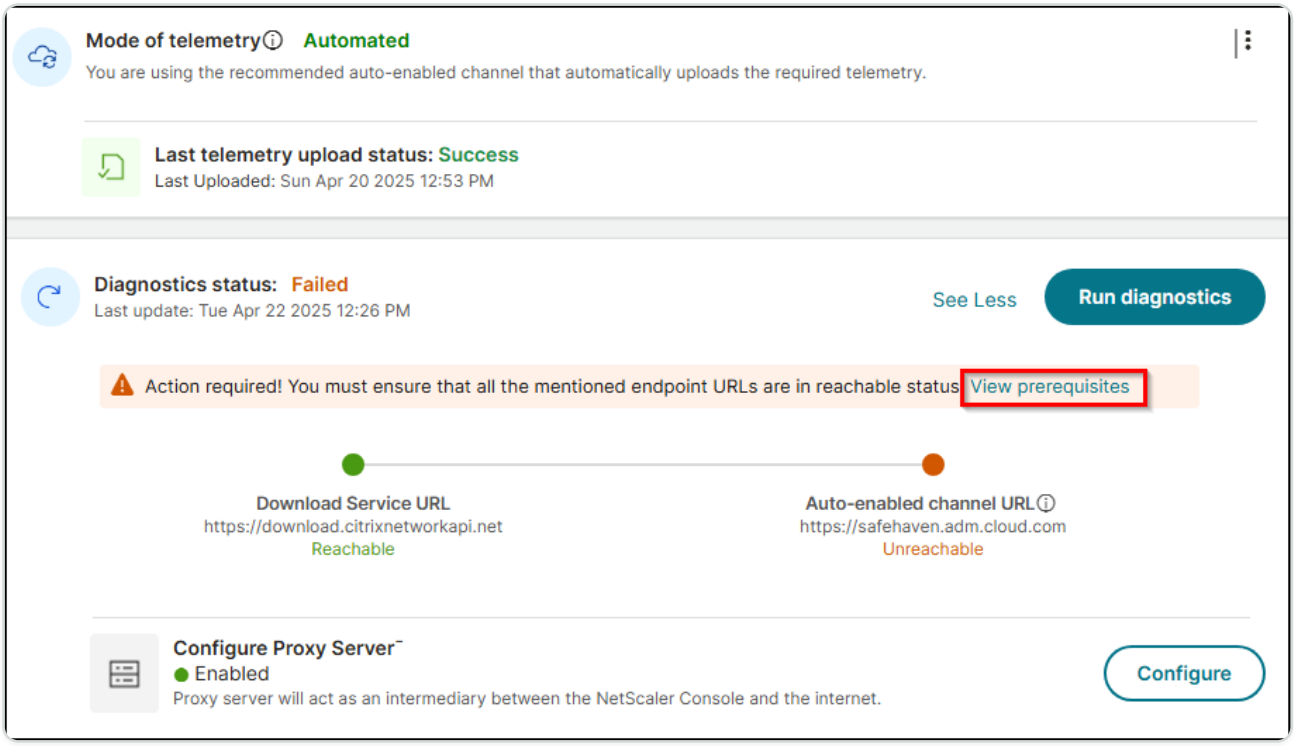


After you see the endpoint URLs in reachable status, click **Go to NetScaler® Telemetry** page.

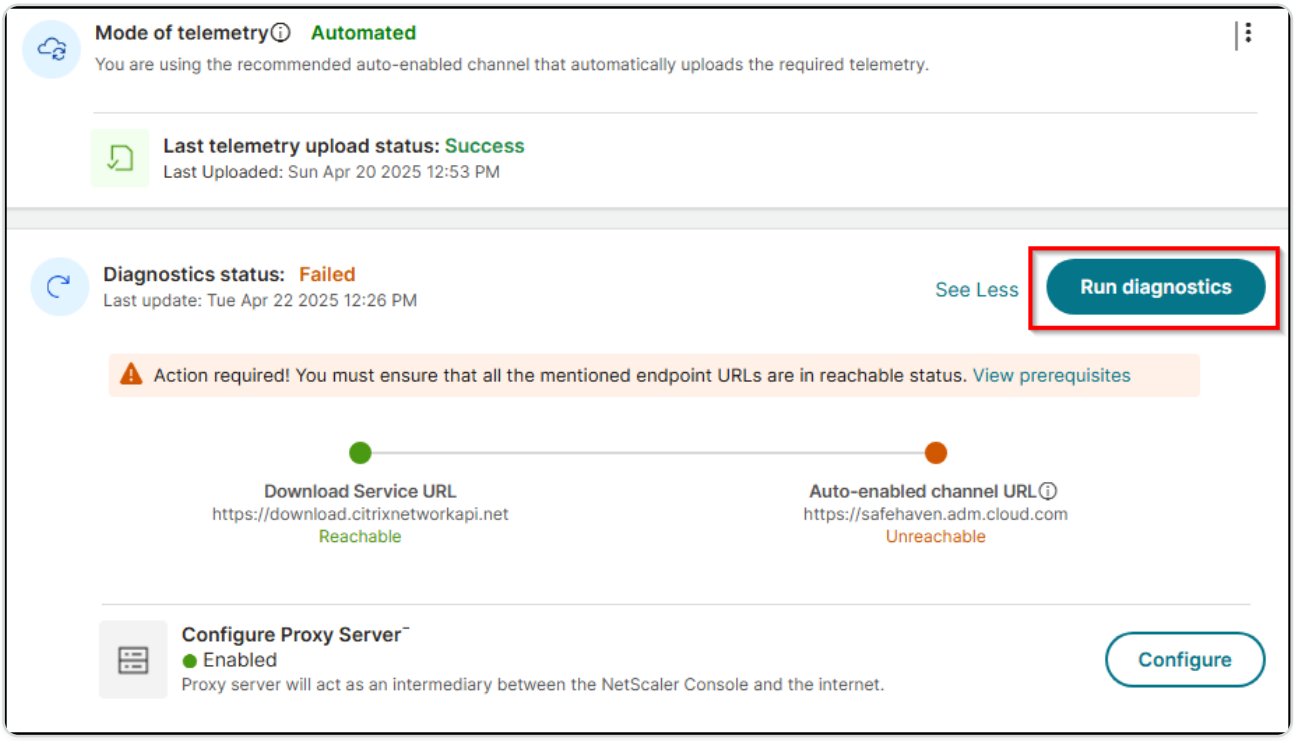


If any prerequisites fail, the diagnostic check displays the endpoints that are not reachable and you must ensure that the URLs reachable. Click **view pre-requisites** to view details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can run diagnosis by clicking **Run diagnosis** to confirm if the endpoint URLs are reachable.



If no action is taken, your NetScaler Console on-prem might be non-compliant with the NetScaler telemetry program.

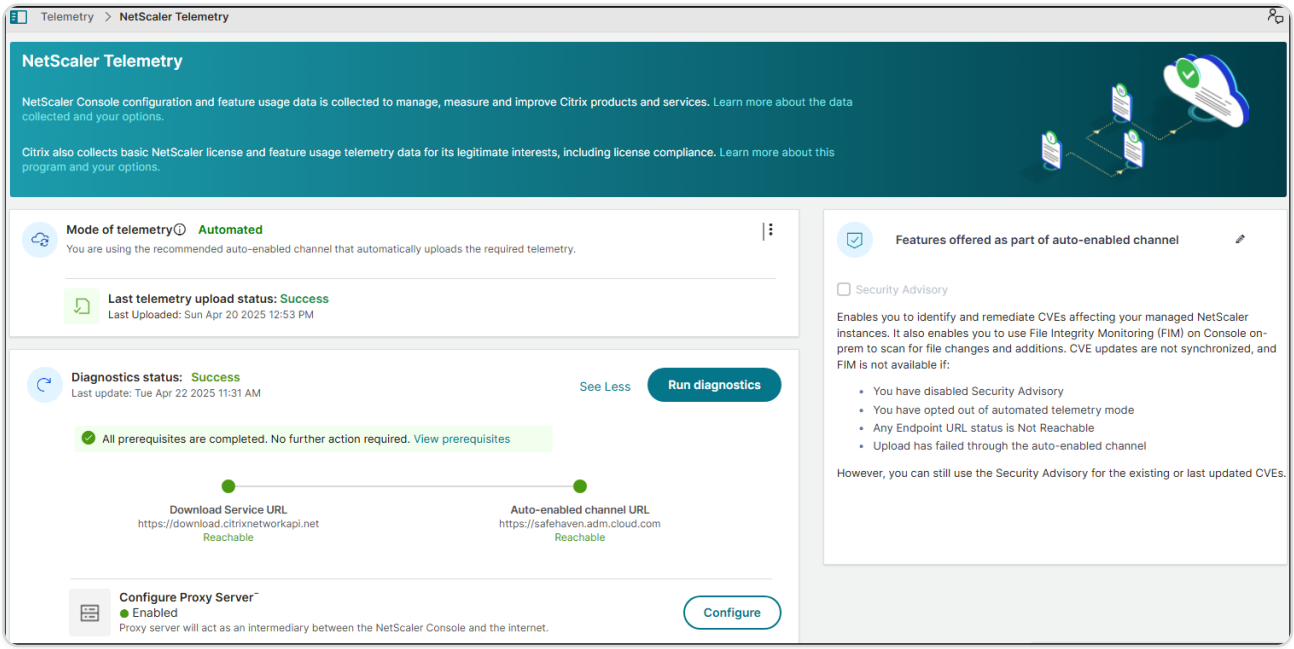
As part of the auto-enabled channel, you can use the **Security Advisory** feature with latest CVE updates in NetScaler Console on-prem. The Security Advisory feature enables you to identify the CVEs putting your NetScaler instances at risk and recommends remediations. You can view the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

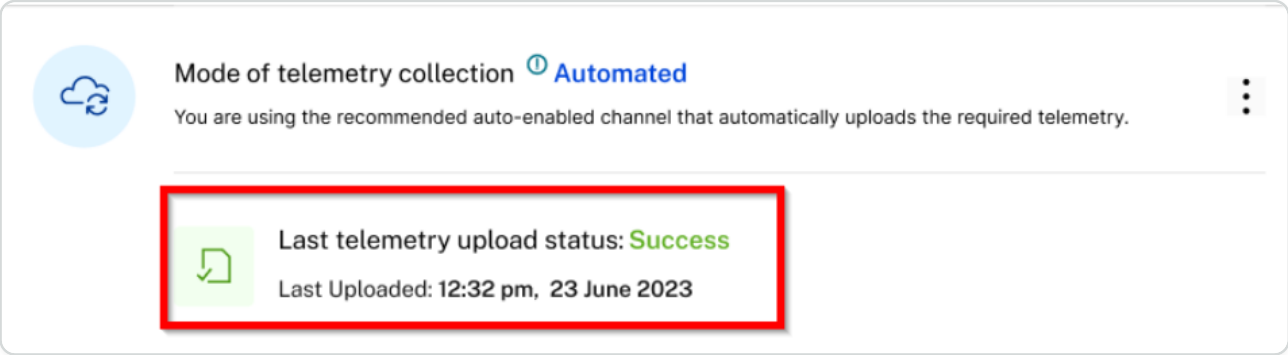
latest CVE details that are impacting your NetScaler instances in Security Advisory. For more information, see Security Advisory.

NOTE:

You can also disable Security Advisory. If you disable **Security Advisory**, or opt-out of automated telemetry mode, or any prerequisites fail, the new CVE updates are not available and you can only use the Security Advisory with the existing or the last updated CVEs.



After the automated telemetry collection is enabled successfully, the first upload happens within 24 hours. The subsequent uploads happen every 24 hours automatically. The status changes to **Success** after the upload is complete.

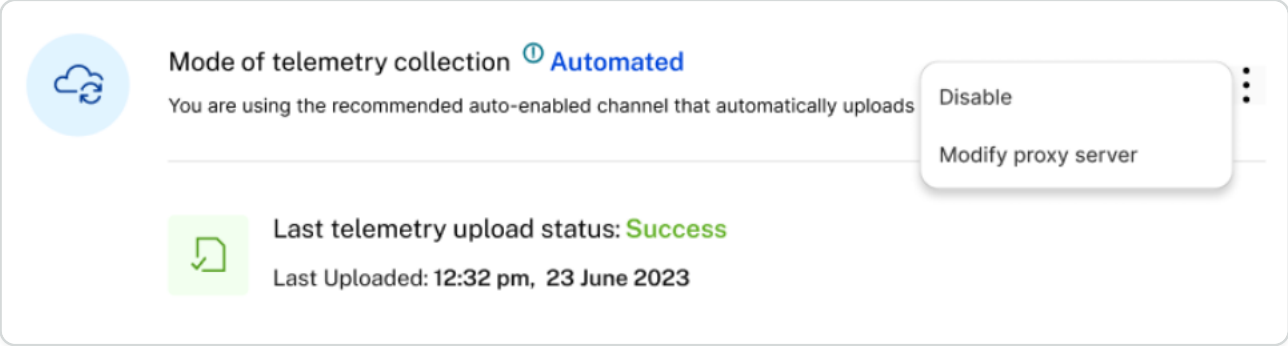


If the upload fails, ensure that the endpoint URLs are reachable. If the status indicates reachable and still the upload fails, contact Customer Care.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manual telemetry collection mode

To use the manual telemetry collection mode, you must first disable **Security Advisory** and then click the vertical ellipse and select **Disable**.



In the pop-up window, click **I agree to upload the data manually** to disable the automated telemetry collection. The mode of telemetry collection is automatically changed to **Manual**. In the Manual telemetry mode, the new CVE updates are not available and you can only use the Security Advisory with the existing or the last updated CVEs.

After you opt for manual mode, you must download the telemetry and complete the first upload in NetScaler Console service within 30 days. The subsequent uploads are to be done every 90 days thereafter.

NOTE:

A maximum of 2 GB NetScaler Console disk space is utilized to save the 90 days of telemetry data.

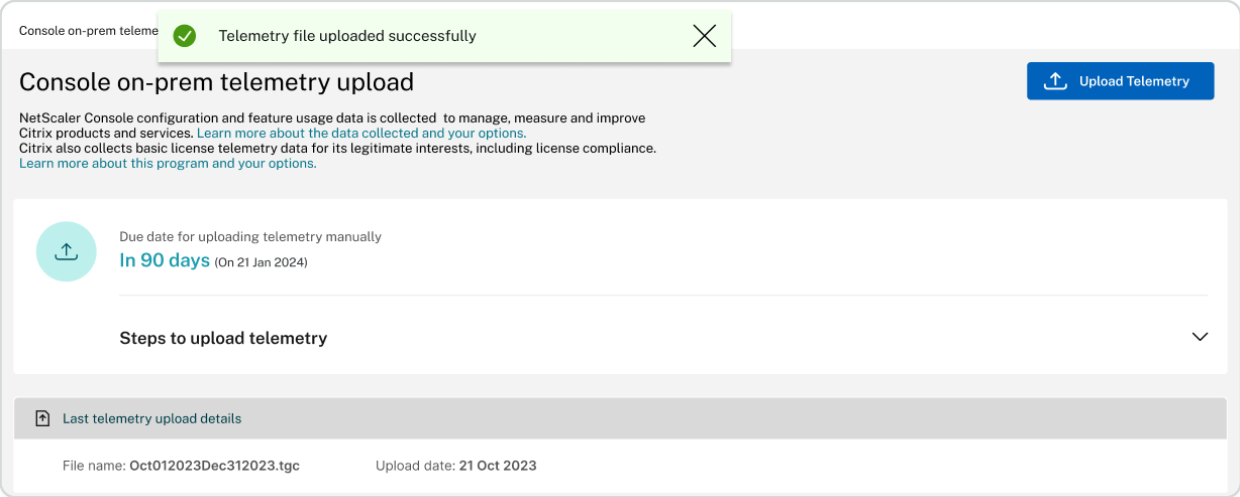
From the **NetScaler Telemetry** homepage, click **Download Telemetry** to download the bundle (.tgz) file that comprises the required telemetry data.

After you download the telemetry file, you must upload it to the NetScaler Console service. To upload in NetScaler Console service:

1. Log on to Citrix Cloud (citrix.cloud.com). If you do not have a Citrix Cloud account, sign up for a new account. For more information, see Create a Citrix Cloud account.
2. Select an account.
3. Under **NetScaler Console Service**, click **Manage**.
4. Set up a Console service account.

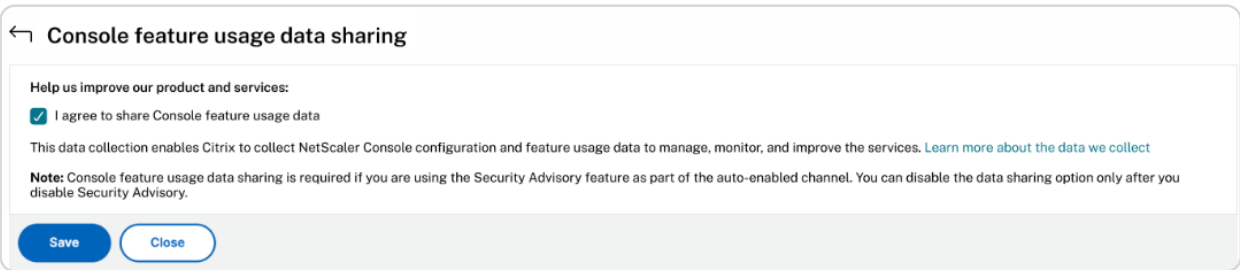
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In NetScaler Console service, navigate to **Settings > Console on-prem telemetry upload**.
6. Click **Upload Telemetry** and select the downloaded (.tgz) file to complete the upload process.
7. Complete the first upload within 30 days of selecting manual mode. Repeat the same procedure and upload the telemetry file every 90 days thereafter.



NOTES:

- The upload fails if the file is not in a valid (.tgz) format or the file does not pass the integrity checks. The recommendation is to download again and retry to upload. If the issue persists, contact Customer Care.
- You can disable uploading the optional telemetry data. To disable, you must first disable **Security Advisory** in the **NetScaler Telemetry** page, then navigate to **Settings > Administration > Enable or disable the Console feature data sharing**, and clear the **I agree to share Console feature usage data** checkbox.



- In your NetScaler Console on-prem, a reminder banner appears 7 days before the upload due date.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

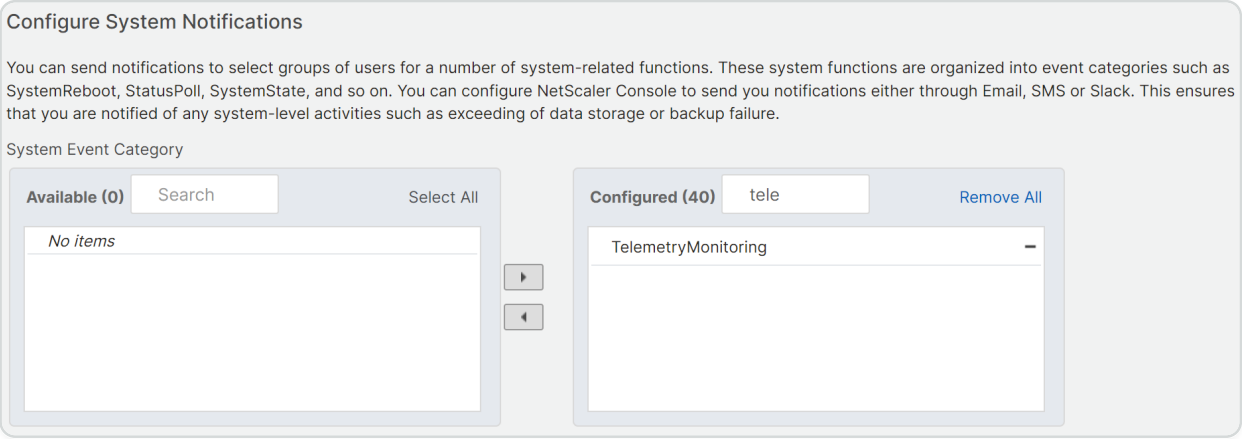
Notifications for telemetry uploads

By default, email notifications are enabled for telemetry uploads. The prerequisite to receive email notification is to configure an email distribution list. For more information, see Configure notification settings As an administrator, you receive email notifications for the following scenarios:

- **Upload failure through automated mode** - Email notification is received every 24 hours until the issue is resolved.
- **Upcoming deadline for manual upload** (only if enabled manual mode) - One email notification is received during the event and another email after the upload is complete.
- **Exceeded deadline for manual upload** (only if enabled manual mode) - One email notification is received during the event and another email after the upload is complete.

You can disable the email notification. To disable:

1. Navigate to **Settings > Administration > Configure Event Notification and Digest**.
2. In **Event Notification > Configure System Notifications**, search for **TelemetryMonitoring**, remove this notification, and click **Save**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.