Command Center 5.2

Nov 16, 2015

About this Command Center Release

FAQs

Command Center Appliance

Installing Command Center Software

Upgrading Command Center

NITRO API

About this Command Center Release

Oct 13, 2015

The release notes describe the changes or enhancements, fixed issues, and known issues in Build 44.11. The list of known issues is cumulative, that is, it includes issues that are newly found in this build and also issues from previous builds.

What's New? - The enhancement and changes released in Build 44.11.

Fixed Issues - The issues addressed in Build 44.11.

Known Issues - The issues that exist in Build 44.11.

Limitations - The list of limitations available in Build 44.11.

What's New in Previous 5.2 Builds - The enhancements and changes that were available in Command Center 5.2 releases prior to Build 44.11. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

Fixed Issues in Previous 5.2 Builds - The issues that were addressed in Command Center 5.2 releases prior to Build 44.11. The build number provided below the issue description indicates the build in which this issue was addressed.

Note

- Additional fixes in Build 49.11: 596501,603146,598053,600116
  The complete description of these issues are listed in the Fixed section
- Additional enhancement in Build 49.11: 600905
  The complete description of this issue are listed in the What's New section

Note

- This build includes fixes for 1 issues that were known issues in the previous build of the Command Center 5.2 release.
- The [# XXXXXX] labels under the issue descriptions are internal tracking IDs used by the NetScaler team.
- These release notes do not document security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

What's New?

Oct 13, 2015

The enhancement and changes released in Build 44.11.

- **Support for Administrator Base Domain Name for Active Directory/Open LDAP Authentications Servers**

  You can now specify the Administrator Base Domain Name if you configure either an Active Directory or an Open LDAP authentication server. The Administrator Base Domain Name is the administrator user name that is used to bind to the Active Directory or Open LDAP server. You can specify the Administrator Base Domain Name in the field Administrator Bind DN.

  [#557589]

- **Support for Fallback Authentication User**

  This feature allows an external user to log on to Command Center even though the configured external authentication server is down or unreachable. Command Center administrator must identify the users and enable Fallback Authentication User for those users. By default, this option is disabled for all users. Note that the default password for fallback users is public.

  To enable Fallback Authentication User for multiple users, on the Administration tab, under Security, click Fallback Authentication User, and select the user for whom you want to enable this setting.

  To enable Fallback Authentication User for a user, on the Administration tab, navigate to Security > Users, select the user and click Edit. In Configure User, select the Fallback Authentication User option.

  [#537550]

- **Preview Master Configuration Before Execution**

  You can now preview the master configuration, which is generated from the configuration template and the input file provided by the user during DeployMasterConfig task execution, before it is executed on the selected device.

  [#549991]

- **Downloading a Sample Configuration Template from Built-in Tasks**

  You can now download the sample template file and the input file for the DeployMasterConfig task from the NetScaler Built-in Tasks lists page.

  On the Configuration tab, navigate to Configuration > Built-in Tasks, select DeployMasterConfig and click Download Sample Template. A zip file containing both the sample template file and the input file is downloaded to your local machine.

  You can no longer download the sample template file and the input file from the Downloads section of Command Center.

  [#553617]

- **Restricted Access to Entities and its Bound Entities**

  If you restrict a user group to an entity, then all the users in that group can access only that entity and the entities that are bound to that entity. For example, consider there are three virtual servers configured on a NetScaler device, V1, V2, and V3, and virtual servers V1 and V2 are bound to service S1. If you restrict usergrp1 to only service S1, then all users in the group usergrp1 can access only service S1 and virtual servers V1 and V2. Users in usergrp1 cannot access virtual server V3.

  To restrict a user group to only an entity and it's bound entities, on the Administration tab, navigate to Security > Groups, select a group, and then click Advanced Settings. In the Property Name list, select an entity, and then select the Apply on bound entities also option.

  This functionality is applicable to the following entities:

  -Virtual Server Name

  -Service Name

  -Service Group Name

  -Server IP address

  Note: If you select the Apply on bound entities also option for the entities services and service groups, the servers abound to these entities might not be accessible.

  [#535029]

- **Continue Task Execution after Failure**

  If you configure a task to be executed sequentially and select the Ignore and Continue option, you can now select either of the following options:

  -Execute on current device only. Execute the task on only the current device, even though the task has partially failed on that device.

  -Execute on all selected devices. Execute the task on all the selected devices, including the current device that experiences a partial failure.

  [#549686]

- **Support for SNMPv3 Traps for NetScaler Devcies**

  Command Center now supports SNMPv3 traps. Command Center receives SNMPv3 traps once a NetScaler device is discovered with SNMPv3 credentials. SNMPv3 traps are supported for only NetScaler devices.

  [#555734]

- **Enhanced Technical Support Bundle**

  You can now generate technical support bundles of the following types:

  -Basic. A technical support bundle that includes log files, database information, and configuration settings.

  -Advanced. A technical support bundle that includes log files, database information, configuration settings, thread dumps,

and crash logs.

Command Center now stores the last ten previously generated technical support bundles. You can delete the ones that you no longer require.

Technical support bundles generated by Command Center appliances in a high availability configuration include the technical support files for both the primary and the secondary nodes.

To generate the technical support bundle by using the graphical user interface, on the Administration tab, under Diagnostics, click Technical Support.

A technical support bundle can also be generated from the Command Center command line interface. The default type is Advanced.

To generate the technical support bundle by using the command line interface, in the <CCHome>\\bin directory, execute the generate_technical_support script.

On a Windows system, run the following command:

generate_technical_support.bat

Alternatively, you can double-click the generate_technical_support.bat file.

On a Linux system, run the following command:

sh generate_technical_support.sh

[#496921, 423211, 445750]

- **Default Read-Only Permissions for All Groups**

  All groups configured on Command Center now have read-only permissions by default. In earlier releases, the default group "Users" had no permissions.

  As part of this enhancement, the Users group now has read-only permissions. A new external user is automatically added to the default Users group when that user is authenticated in Command Center. Since the Users group now has read-only permissions, the new external user does not experience an authorization failure.

  [#537546]

- **XML Schema file Included in the Sample Template Compressed File**

  The compressed file (.zip) of a sample template of built-in tasks now includes the XML schema file (.dtd) for the input XML file.

  [#583370]

- **Customizing the DeployMasterConfig Built-in Task**

  If you want to replicate the complete existing state of a NetScaler appliance on another NetScaler appliance, you must replicate the configuration, license, and certificate files. By executing the DeployMasterConfig built-in task without customizing it, you can replicate only the configuration file.

  You can customize the DeployMasterConfig built-in task to add additional commands, so that you can replicate license

and certificate files to other NetScaler devices, and execute any other commands required for your configuration.

You can customize the DeployMasterConfig built-in task to do the following:

-Add additional commands

-Modify existing commands

-Add variables to commands

-Delete commands

-Change the order of commands.

Caution: Be careful when changing the order of commands in the DeployMasterConfig built-in task.

[#586722]

- **Support for TLSv1.1 and TLSv1.2**

  Command Center now supports TLSv1.1 and TLSv1.2 protocols.

  To enable TLSv1.1 and TLSv1.2 protocols

  On the Administration tab, navigate to Settings > SSL Settings and select the Enable TLSv1.1 or Enable TLSv1.2 option.

  Note that the SSLv3 protocol is no longer supported.

  [#571448]

- The Auto rollback on failure option under Deployment Automation is now unchecked by default.

  [#600905]

- **Support for Enabling and Disabling Group Extraction**

  You now have the option to enable and disable group extraction for a RADIUS authentication server. In earlier releases, group extraction could not be disabled.

  [#556544]

- **Support for Resolving an Authentication Server by Using the Host Name**

  You can now specify either the host name or the IP address to resolve an authentication server. In earlier releases, you could only specify the IP address.

  [#586708]

- **Support for Deployment of RADIUS Authentication With Active Directory Server**

  Command Center now supports deployment of RADIUS authentication with an Active Directory server. You must enable Group Extraction and specify the group vendor identifier and the type of group attribute.

  [#571655]

- **Support for Exporting Graphs and Tables of Application Firewall Violations**

You can now export graphs and tables of Application Firewall violations from Command Center. You can choose to export either a graph or a table (CSV file), or both.

[#577318]

- **Support for Reporting for NetScaler Gateway**

  You can now view the following reports for NetScaler Gateway devices:

  -Top users by sessions

  -Top ICA applications by user access

  -Top users by bandwidth

  -Top client types

  -Top users by EPA scan failures

  -Top users by failed attempts

  You can also export NetScaler Gateway reports from Command Center. You can export them as graphs, tables (CSV files), or both. You can also schedule the Reports.

  To view NetScaler Gateway reports

  On the Reporting tab, navigate to NetScaler Gateway > Reports, select the report you want to view and then click View Graph.

  To schedule NetScaler Gateway reports

  On the Reporting tab, navigate to NetScaler Gateway > Notification Settings, and then click Schedule Report.

  [#584651]

- **Single Option to Configure Active Directory and Open LDAP Authentication Servers**

  You now have a single option, LDAP, for configuring either an Active Directory or an Open LDAP authentication server.

  On the Administration tab, navigate to Security > Authentication Settings, and select LDAP. In the Server Type list, select either Active Directory or Open LDAP, and then configure the rest of the fields as required for the authentication server you selected.

  [#571443]

- **Support for Monitoring the Command Center Database**

  You can now receive an SNMP trap if the size of the Command Center database reaches a configured threshold value. You can also receive an email notification.

  By default, the size of the Command Center database is checked once an hour. You can specify the threshold value in MB, or as a percentage (%) of the disk space allocated to the database.

  If you have configured the threshold value as a percentage, then the percentage of the used size is compared against the allocated database size and the notification is generated if the percentage exceeds the configured threshold value.

If you have configured the threshold value as a size (MB), then the used database size is compared against the configured threshold size and the notification is generated if the database size exceeds the configured threshold value.

This feature is supported for the following database servers:

-MSSQL

-MySQL

-Oracle

Note that this feature is not supported for the PostgreSQL database server.

To configure database monitoring

1. On the Administration tab, navigate to Settings > Database Monitor Settings.

2. Select the Enable Database Monitoring option and specify the threshold value as a percentage or as a size (MB).

3. If you also want to receive an email notification, select the Enable Email Notification option and then configure the email server from which to send email notifications.

[#449211, 446452]

- **Support for Viewing up to 40 Top Violations in Application Firewall Reports**

  You can now view a graph of up to 40 top violations in Application Firewall reports. You can also schedule an Application Firewall report of up to 40 top violations.

  [#547522]

- **Support for Exporting Syslogs**

  You can now export syslogs from Command Center. For Application Firewall and NetScaler Gateway syslogs, you can export the recent syslogs that appear under Logs, and you can export syslogs for the views that you have configured under Views. You can also export the syslogs that appear on the Fault tab, under Logs and Views.

  You can specify the criteria for exporting syslogs that appear under Logs. Different criteria apply to NetScaler Gateway and Application Firewall syslogs. You can limit the number of rows to be exported depending on your need. The default limit for the number of rows to be exported is 1000, and the maximum is 10000.

  You can now export all graphs (image files) and data in tabular format (CSV file) from the Application Firewall dashboard.

  [#403149]

- **Changes in the Command Center Graphical User Interface**

  Note the following changes in the Command Center graphical user interface:

  1. Fault > Syslogs

  - "Complete View" has been renamed to "Logs."

  - "Filters" has been renamed to "Suppress Logs."

2. Reporting > AppFirewall

- "Filters" has been renamed to "Suppress Logs."

- "Recent Logs" has been renamed to "Logs."

- "Views" was under "Recent Logs" which is now under "AppFirewall."

- "Schedule Report" was under "Reports" which is now under "Notification Settings."

3. Reporting > NetScaler Gateway

- "Filters" has been renamed to "Suppress Logs."

- "Recent Logs" has been renamed to "Logs."

- "Views" was under "Recent Logs" which is now under "NetScaler Gateway."

[#577325]

- **Updated Management Service Backup**

  The Management Service backup now contains only the Management Service configuration backup. This backup no longer includes the image of the NetScaler SDX appliance and NetScaler VPX instances, nor the configuration information for NetScaler VPX instances running on the NetScaler SDX appliance.

  [#526020, 526024]

Fixed Issues

Oct 13, 2015

The issues addressed in Build 44.11.

- If a NetScaler device is enabled with Common Event Format (CEF) logging for Application Firewall, Command Center fails to retrieve views for an alarm.

  [#570148]

- When OpenLDAP is used for Command Center authentication, a logon attempt with valid credentials fails.

  [#546717]

- Command center might display same host names for different devices.

  [#549935]

- User defined rollback commands are not displayed in the preview screen before task execution.

  [#550461]

- The default value of Event Cleanup Interval is now 30 days. In earlier releases, the default value was 180 days. If you had configured this value to anything other than 30 days before upgrading to the latest release, you must again set it to the value as per your need.

  [#596685]

- The arrow icon indicates that the records displayed in the Command Center graphical user interface are sorted in ascending order, but they are actually sorted in descending order.

  [#555476]

- The DeployMasterConfig task fails if the input XML file contains standard comments.

  [#581317]

- Command Center service fails to start, because of JRE corruption.

  [#555113]

- You can now specify the device group in the input file to deploy the master configuration on a NetScaler device.The variable values defined in the devicegroup tag take precedence over the global variable values and the variable values defined in the device tag take precedence over the devicegroup variable values.

  [#557664]

- All entities bound to an entity might not be displayed if you restrict a user to that entity by using Advanced Settings.

  [#583763]

- The Command Center logon page might take a long time to load.

[#556218]

- Appropriate error messages are not displayed in the execution logs if the DeployMasterConfig task fails.

  [#575339]

- After you install or upgrade Command Center, the first attempt to connect to the MSSQL database fails.

  [#566928]

- Appropriate error messages might not be logged in the task execution logs if there is an error in the input XML file.

  [#563326]

- The browse button to search users from Active Directory is now changed to a search icon.

  [#557658]

- If Command Center is configured with a custom certificate that does not have a default password, the Command Center service fails to start during an upgrade.

  [#558984]

- The DeployMasterConfig task fails if the configuration template file contains HTML tags, because Command Center uses the characters "<" and ">" to enclose the variable name. You can now use the "$" character to enclose the variables (for example, NS_IP).

  [#563404]

- Command Center now supports using the NITRO API to fetch a device list on the basis of device type.

  [#583472]

- In the NetScaler Gateway dashboard, the "Top 10 users by EPA scan failures" report displays invalid data.

  [#565270]

- The CLI commands to generate the technical support bundle have been updated as below:

  On a windows system:

  generate_technical_support.bat basic

  generate_technical_support.bat advanced

  On a linux system:

  sh generate_technical_support.sh basic

  sh generate_technical_support.sh advanced

  [#586717]

- If an Active Directory user that is a member of a group is reassigned to another group, the Command Center graphical user interface lists the user as part of the original group.

[#589898]

- On the Monitoring tab, the search functionality fails if the user belongs to two groups and advanced authorization settings are configured.

  [#594366, 590655]

- If a scheduled report generates the "Too many data points to plot" error at the same time for two different charts, graphs are not attached in the email sent to the user.

  [#594726]

- In an HA setup of a Command Center server, SSLv3 status change operations (enable or disable) are not propagated to the secondary appliance

  Workaround:

  Enable or disable SSLv3 when the secondary appliance is UP.

  [#552307]

- Command Center connections become stale because they are not refreshed.

  [#586925]

- If the Command Center logon password is longer than 15 characters, an attempt to log on to the Command Center GUI fails.

  [#600116]

- The Linux script EncryptPassword.sh throws a bad interpreter error because the script contains ^M characters.

  [#521956]

- The help text on the custom task creation screen now appears as a tool tip.

  [#583216]

Known Issues

Oct 13, 2015

The issues that exist in Build 44.11.

- Rollback of commands in the DeployMasterConfig built-in task fails.

  [#596682, 595304]

- If you configure an alarm or event trigger for a Send Trap action to send SNMP traps to an SNMP manager, SNMPv3 traps are forwarded to the manager as SNMPv2 traps.

  [#582423]

- The NetScaler dashboard always displays the CPU Usage (%) value as 0 for a NetScaler cluster.

  [#437641]

- The restore configuration option on the details page for a device does not display the log information.

  [#370810]

- When creating views for SNMP alarms and events on the Faults tab, selecting a device type on the Create View page does not load the filter criteria associated with the device type.

  [#315632, 350773]

- Rediscovery of a cluster device with an SNMP v3 profile fails after the Configuration Coordinator node restarts.

  [#390280, 413918]

- You might be unable to log onto Command Center after a fresh installation, because of a corrupted security configuration.

  Workaround: After a fresh installation, reset the Command Center configuration by re-initializing it. To do so, run the reinitialize_nms.bat or reinitialize_nms.sh script, which is located in the CCHome/bin/ folder

  [#358712]

- If you install Command Center servers in a high availability (HA) pair or upgrade Command Center servers in an HA pair to new build, one of the servers might not start.

  Workaround: Restart the server that failed to start.

  [#596501, #603146]

- You cannot generate a report by using the "RunningVsSavedconfiguration" audit policy on a NetScaler device if the device password contains a hash (#).

  Workaround: Modify the device password.

  [#443175]

- On the Citrix Network > Device Inventory > NetScaler screen, the Command Center server does not sort the System Uptime column by date but by the string value.

  [#534042]

- The Device Inventory screen does not display the IP address, platform and hostname for the CloudBridge 800 platform.

  [#551110]

- If you access the Command Center server through an Internet Explorer 8 browser, the virtual servers screen (Monitoring> NetScaler> Virtual Servers) displays an error message.

  [#515061]

- Because of security vulnerabilities in the TLSv1 SSL protocol, the default settings for Command Center no longer support TLSv1. However, CloudBridge devices currently do not support TLSv1.1 or TLSv1.2. After you upgrade to this release, Command Center's ability to discover and connect to CloudBridge models 400, 800, 1000WS, 2000, 2000WS, 3000, 4000, and 5000 is lost.

  Workaround: To discover CloudBridge devices, on the Administration tab, under settings, click SSL Settings and then select the Enable TLSv1 option.

  [#598053]

- Command Center accesses unknown DNS IP addresses.

  Workaround:

  Update the /var/cache/yum/addons/mirrorlist.txt file to remove the invalid DNS entries.

[#598040]

- Alarms are not purged if a huge number of incoming traps (around 10,000 requests per second) arrive for processing on the Command Center server.

[#538161]

- If you add a device to Command Center, sometimes, the discovery process might not proceed.

  Workaround: Restart the Command Center server.

[#380961]

- You cannot search for an execution log by specifying the status message that appeared when the task was executed.

[#552902]

Limitations

Oct 13, 2015

The list of limitations available in Build 44.11.

- The details of a security violation of type APPFW_CSRF_TAG, displayed in AppFirewall log messages, are incorrect for NetScaler devices running release 10.0.

  [From Build 44.11] [#347274]

- In the Authentication settings for Active Directory Group extraction, the option to retrieve the attributes from the Active Directory server and select the attributes from the retrieved list is not available in Command Center release 5.1 or later.

  [From Build 44.11] [#347208]

- AES based encryption is not applicable for USMTable in SNMPv3 discovery.

  [From Build 44.11] [#450079]

- The counter values for Transmit Link utilization and Receive link Utilization are incorrect.

  [From Build 44.11] [#398919]

- When you replicate a configuration on a NetScaler device, the L2 and L3 configurations are also replicated.

  [From Build 44.11] [#371907]

- The advanced search and find device features, formerly on the Home page, are not available in the Command Center release 5.2, because of migration to the new user interface framework.

  [From Build 44.11] [#290553, 337222, 353906]

- The Replicate Configuration feature is not supported for a NetScaler cluster or for NetScaler devices in a high availability pair.

  [From Build 44.11] [#370232]

- The option to export the details in the custom views of Events and Alarms is not available in Command Center release 5.2.

  The following export options are not available in Command Center release 5.2:

  * Export entire custom view data

  * Export displayed data

  * Export Annotations

  [From Build 44.11] [#354869]

- If the number of failure objects in Command Center is high and you create or modify custom views in Events and Alarms,

a script error occurs.

[From Build 44.11] [#377592]

- Command Center does not support Windows authentication mode for an MSSQL database. It only supports SQL authentication mode.

  [From Build 44.11] [#531252]

What's New in Previous 5.2 Builds

Oct 13, 2015

The enhancements and changes that were available in Command Center 5.2 releases prior to Build 44.11. The build number provided below the issue description indicates the build in which this enhancement or change was provided.

- On the graphical user interface (GUI), the Logs Settings page (Administration > Logging > Logs Settings) now displays the following details:

  - Logger: Type of log file.

  - Level: Level of log you want to generate. Select the log level for a file.

  - Appender: A link to set the file appender details.

  When you click on file name in the Appender column, you can modify the following settings:

  - File Name: Name of the log file with which the appender is associated.

  - Max Backup: Maximum number of files to be backed up when storing the logs. When this limit is reached, the log file is rolled back.

  - File Size: Maximum size of the log file.

  [From Build 40.1] [#243786]

- You can now track the configuration files downloaded during discovery of a NetScaler SDX device or a CloudBridge Advanced Platform (CloudBridge 400 or CloudBridge 800). You can back up the configurations of a device at any time.

  On the SDX Device Properties page, you can now perform the following tasks:

  - Backup Config: Initiate configuration backup.

  - Refresh: Refresh the Archived Details section.

  - Download: Download configuration and license files to your local system.

  The following details are also available for each file archived during discovery, during intervals set by the user, or for the current time:

  - Time: The date and time when the configuration and license files were archived.

  - View Files: The list of files archived. To view the list of all the license and configuration files archived and stored in the database, click View Files.

  - Comments: Details about when the files are downloaded (for example, File downloaded during discovery).

  [From Build 40.1] [#393065]

- You can use the NetScaler Dashboard to view the status of all the NetScaler devices being managed by Command Center. You can view the name, CPU usage, memory usage, throughput statistics, and HTTP requests per second data

for each discovered device.

[From Build 40.1] [#382330]

- You can now search the execution logs by task name, device, or status by using the search option on the Execution Log page.

  [From Build 40.1] [#414432]

- The CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800) can initiate discovery by Command Center, if you configure the IP address, port, and password of the Command Center server on the CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800). The appliances then use NITRO APIs to send registration requests to Command Center. The Command Center server then automatically starts the discovery process.

  [From Build 40.1] [#357041]

- You can now use Command Center to monitor and manage the states of servers across the NetScaler infrastructure.

  [From Build 40.1] [#376408, 271451]

- You can now assign Execute task Action to filter the event and alarm triggers.

  [From Build 40.1] [#363267]

- The Initial Configuration wizard enhances the first time user experience by helping you get started with Command Center efficiently and effectively, and by guiding you through the initial configurations. This ensures that you perform all the required configurations without having to navigate to GUI pages of different tabs in the Command Center GUI.

  [From Build 40.1] [#400765]

- In this release, you can now use the following built-in tasks to execute configuration changes on CloudBridge devices:

  - AddWCCPServiceGroup

  - EnableWCCP devices

  - DisableWCCP

  - SetApplication

  - SetTrafficShapingPolicy

  - AddTrafficShappingPolicy

  - AddService

  - AddLink

  For details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-tasks-conf-repeater-builtin-tasks-tsk.html.

  [From Build 40.1] [#400767]

- You can now perform the following tasks in Certificate Management:

- Display the SSL certificate links

- Link certificate(s) to CA certificates

- Unlink certificate(s) from CA certificates

For more information, see http://support.citrix.com/proddocs/topic/command-center-52/cc-mng-mon-sslcert-link-unlink-tsk.html and http://support.citrix.com/proddocs/topic/command-center-52/cc-mng-mon-sslcert-view-certs-tsk.html.

[From Build 40.1] [#412557]

- This release supports AES-based encryption of device credentials.

  [From Build 40.1] [#416593]

- You can now search for a device by device name or status, after navigating to Citrix Network > Devices > Discovery Status.

  [From Build 40.1] [#414449]

- Command Center can now discover ByteMobile Traffic Director. To begin monitoring the device, you must connect to the Command Center server and then add the ByteMobile Traffic Director for discovery. Command Center initiates the discovery process, which stores the ByteMobile Traffic Director related information in the Command Center server.

  [From Build 40.1] [#431240]

- The Deployment Automation feature provides easy automation for deployment management when deployments are going through rapid changes. This module provides smooth migration of configurations across different deployments and exposes RESTful NITRO APIs with which you can automate the entire process. For details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-tasks-devops-confmig-tsk.html

  [From Build 40.1] [#439975]

- When you view the graph for a custom report, you can now click the auto-refresh button to refresh the graph.

  [From Build 40.1] [#440571]

- Command Center now supports MSSQL 2012.

  [From Build 40.1] [#426937]

- Command Center 5.2 supports MySQL 5.6 and the Red Hat Enterprise Linux (RHEL) 6.2 operating system.

  [From Build 40.1] [#457695]

- You can now apply XenServer hotfixes on the Command Center hardware appliance. For details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-admin-apply-xenserver-hotfixes-tsk..html.

  [From Build 40.1] [#428529]

- If you have resolved any alarms, or if the alarms are no longer valid, you can either clear or delete all the alarms from the Citrix Network tab, depending on multiple severity levels.

[From Build 40.1] [#412555]

- The Configuration Management module in Command Center enables you to execute various configuration commands on multiple devices at the same time. You can create configuration profiles that are templates you can use to execute configuration tasks.

  [From Build 40.1] [#400770]

- If you create a CloudBridge Advanced Platform device profile, you no longer have to provide the CloudBridge profile and NetScaler details. Command Center internally creates CloudBridge and NetScaler profiles from the corresponding CloudBridge Advanced Platform profile.

  Also, if you create a CloudBridge device profile, you no longer have to specify the file transfer details. Command Center internally assigns the default user name transfer and assigns the same password that you specify for device login.

  [From Build 40.1] [#445849, 400903]

- Command Center now supports CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800).

  [From Build 40.1] [#430027]

- Progress of Executed Tasks

  After you provide the details for executing a built-in task or a custom task, a pop-up screen appears, stating that the task execution is in progress. You are redirected to the Execution Log page that displays the progress of the executed task.

  [From Build 40.1] [#382326]

- The Invoke CLI button is now available on the header of the Device Inventory screen.

  [From Build 41.14] [#487689]

- You can now select the columns to include in the tables on Command Center screens such as Device Inventory, Discovery Status, and Device Profiles, and you can rearrange the columns. Each user's changes persistent across his or her sessions.

  Choose the column names from the Settings drop-down list next to the Search button.

  [From Build 41.14] [#412723, 337817]

- Command Center now supports the following NetScaler counters:

  *vsvrTotalServers,1.3.6.1.4.1.5951.4.1.3.1.1.65

  *vsvrInvalidRequestResponse,1.3.6.1.4.1.5951.4.1.3.1.1.67

  *vsvrInvalidRequestResponseDropped,1.3.6.1.4.1.5951.4.1.3.1.1.68

  *vsvrEstablishedConn,1.3.6.1.4.1.5951.4.1.3.1.1.71

  *vxlanTable,1.3.6.1.4.1.5951.4.1.1.81

  *vxlanEntry,1.3.6.1.4.1.5951.4.1.1.81.1

*vxlanVNId,1.3.6.1.4.1.5951.4.1.1.81.1.1

*vxlanTotRxPkts,1.3.6.1.4.1.5951.4.1.1.81.1.2

*vxlanTotRxBytes,1.3.6.1.4.1.5951.4.1.1.81.1.3

*vxlanTotTxPkts,1.3.6.1.4.1.5951.4.1.1.81.1.4

*vxlanTotTxBytes,1.3.6.1.4.1.5951.4.1.1.81.1.5

[From Build 41.14] [#465694]

- The Execution Logs pane on the Configuration tab is now more intuitive and user friendly.

  [From Build 41.14] [#464707]

- Command Center now supports the OpenLDAP as one of the authentication servers.

  [From Build 41.14] [#448897]

- Command Center now has an autoconfiguration feature, which combines configuration profiles with the registration feature to automatically discover and configure one or multiple CloudBridge 400, 800, 1000 WS, 2000, 2000 WS, or 3000 appliances.

  For details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-pure-cs-citrix-network-auto-config-map.html.

  [From Build 41.14] [#472288]

- Command Center now supports the following NetScaler SNMP traps:

  *vridStateChange

  *portAllocFailed

  *lldpRemTablesChange

  [From Build 41.14] [#464662]

- "Show Service Bindings" and "Show Service Group Bindings" are now on the Servers screen, which is on the Monitoring tab.

  [From Build 41.14] [#462144]

- The reporting graphs are now enhanced to display the peak values and minimum values along with average values.

  [From Build 41.14] [#457254]

- Command Center now supports sending audit logs to an external syslog server.

  To add a syslog server, on the Administration tab in the details pane, under Security, click Syslog Server.

  For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-admin-conf-syslog-setting.html

  [From Build 41.14] [#452936, 449151]

- You can now select the following properties when you apply the authorization settings on a group:

  *Server IP address

  *Server Name.

  [From Build 41.14] [#486296]

- Command Center now applies a password policy to provide security against hackers and password-cracking software.

  To apply a password policy, on the Administration tab, in the details pane, under Security, click Password Policy and specify the parameters.

  [From Build 41.14] [#446593, 211955]

- Command Center now supports the following CloudBridge SNMP traps:

  *invalidBridgeConfig

  *invalidHttpCachingConfigFile

  *qosEngineError

  *MapiNtlmError

  *EthernetCrcError

  *qosLinkConfigWarning

  *MaxUnacceleratedConn

  *badHardware

  *warning

  *CheckServiceClass

  *cachingEngineMajor

  *cachingEngineMinor

  *cachingEngineWarning

  [From Build 41.14] [#477655, 478901]

- The Device Inventory screen on the Citrix Network tab now displays the nodes for device types.

  [From Build 41.14] [#476223]

- You can now use the following built-in tasks to upgrade a CloudBridge Advanced Platform appliance and its instances:

  *UploadSoftwareFile

  *UpgradeSoftware

  On the Configuration tab, in the navigation pane, navigate to Configuration > Built-in Tasks and, in the details pane,

select CloudBridge Advanced Platform.

This feature is available on CloudBridge Advanced Platforms running version 124.1353.e or later.

For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-tasks-upgrade-cb-adv-plt-builtin-con.html.

[From Build 41.14] [#425990, 472879]

- You can now enter administrator or user comments for any discovered device.

  To include comments, on the Citrix Network tab, under Device Inventory, navigate to any of the device types, Then, in the details-pane, select the device, and from the Action drop-down list select Annotate.

  Alternately, right-click the device, and then click Annotate.

  [From Build 41.14] [#412718]

- If a custom task fails, you can now choose to ignore the command failure and continue with execution of the remaining commands.

  [From Build 41.14] [#479161, 480162]

- The column customization settings drop-down list on the Device Inventory screen displays the SNMP Device Name, Description, and Location options.

  [From Build 41.14] [#479149]

- The Command Center appliance now monitors the following server conditions and generates an alarm if they occur:

  -Memory usage greater than 90%

  -CPU usage of 100%

  -Page Fault more than 1

  -Disk usage greater than 90%

  -Interface Status of Down

  -HA status

  To display this information, on the Command Center appliance, navigate to Administration, and in the left pane select Information > Server.

  [From Build 42.7] [#435030]

- You can now assign the views on the Monitoring tab to other users in a group by assigning administrator privileges to the view.

  For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-custom-view-group-assign-tsk.html.

  [From Build 42.7] [#428581]

- You can now configure ciphers in Command Center.

  For details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-faq-gen-51-con.html.

  [From Build 42.7] [#495058]

- You can configure an SNMP agent on the Command Center appliance, so that an external SNMP manager can monitor the appliance and query any of its Management Information (MIB) objects.

  To configure an SNMP agent, on the Administration tab, under Security, click SNMP Agent Configuration.

  For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-admin-conf-snmp-trap-fwd-tsk.html.

  [From Build 42.7] [#486665]

- You can now install Command Center on the 64-bit version of CentOS.

  For details on operating systems, see http://support.citrix.com/proddocs/topic/command-center-52/cc-install-os-reqmnt-ref.html.

  [From Build 42.7] [#472853]

- You can now install Command Center on the Windows server 2012 R2 platform.

  For details on operating systems, see http://support.citrix.com/proddocs/topic/command-center-52/cc-install-os-reqmnt-ref.html.

  [From Build 42.7] [#471343, 426974]

- Command Center now displays the entity's IP address and port, along with the entity name, for all the SNMP event and alarm details for entity UP, DOWN, and OUT OF SERVICE traps.

  [From Build 42.7] [#461867]

- If you use an RBAC server for authentication, Command Center groups are configured to match groups configured on authentication servers. 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 matching Command Center group.

  For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-admin-conf-authntcn-settng-4-0-tsk.html#cc-admin-conf-authntcn-settng-4-0-tsk.

  [From Build 42.7] [#440573]

- Command Center now supports the following built-in tasks for CloudBridge appliances:

  -AddVideoCachingSource

  -AddorRemoveVideoCachingPorts

  -SetVideoCaching

  -RemoveVideoCachingSource

  -RemoveAllVideoCaching

-ClearVideoCaching

-VideoCachingState

-AddVideoPrePopulationNow

-AddorUpdateVideoPrePopulation

-VideoPrePulationState

For more details, see http://support.citrix.com/proddocs/topic/command-center-52/cc-tasks-conf-repeater-builtin-tasks-tsk.html.

[From Build 42.7] [#480871, 480080]

- You can now install Command Center on a named instance of MSSQL server 2012.

  [From Build 42.7] [#490095, 496907]

- Command Center can now be configured to repeat email notifications at specified time intervals until an alarm is cleared. Navigate to Fault> SNMP> Alarms> Triggers> Add> Add Action to enable this option.

  [From Build 43.19] [#544557]

- The search functionality in Command Center is now improved to display the filter names in the search option even after performing multiple search operations by using the same filter name.

  [From Build 43.19] [#428586]

- Command Center now supports NITRO APIs for custom views.

  [From Build 43.19] [#477797]

- You can now use the DeployMasterConfig built-in task to configure parameter values across NetScaler devices by applying the global configuration template and an input file.

  [From Build 43.19] [#479155, 480154, 480159]

- If any discovered NetScaler device has an SNMP manager configured, Command Center adds itself as an SNMP manager.

  [From Build 43.19] [#486986]

- Command Center now supports the UploadXVA built-in task to upload a XenServer Virtual Appliance (XVA) image to one or more NetScaler SDX appliances.

  [From Build 43.19] [#489416]

- Command Center now supports SCP protocol to make configuration changes across NetScaler and CloudBridge devices.

  [From Build 43.19] [#491038]

- You can now enable or disable the SNMP alarm filters and schedule them (Fault> SNMP> Alarms> Triggers > Schedule a Filter.)

[From Build 43.19] [#502387]

- The Execution Log screen (Configuration> Configuration> Execution Log) now includes a Status Message column, which provides details about the progress of task execution.

  [From Build 43.19] [#508139]

- You can now discard obsolete syslog records by creating a filter.

  To configure a Syslog filter, on the Fault tab, navigate to Syslogs> Filters, and click Add.

  [From Build 43.19] [#509401]

- Command Center server now provides the option to enable or disable SSLv3 (Administration> Settings> SSLv3 Settings.) By default, SSLv3 is disabled on the Command Center server.

  [From Build 43.19] [#510806]

- You can now configure the syslog purge interval for different syslog messages.

  To configure the purge interval, on the Administration tab, in the Settings group, click Syslog Purge Settings.

  [From Build 43.19] [#512676]

- You can now search for an execution log by specifying the Start Time, End Time and Execution time of a task.

  The search by execution time works on the values displayed in the Start time and End Time columns.

  [From Build 43.19] [#517487]

- You can now abort task execution, on one or more devices, by selecting the devices and clicking the Abort button.

  [From Build 43.19] [#517495]

- Group extraction feature is now available for RADIUS authentication server.

  [From Build 43.19] [#533057]

- Command Center now supports MSSQL 2014.

  [From Build 43.19] [#533069]

- You can now discard obsolete AppFirewall or NetScaler Gateway syslog records by creating a filter.

  To configure the AppFirewall filter, on the Reporting tab, navigate to AppFirewall> Filters, and click Add.

  To configure the NetScaler Gateway filter, on the Reporting tab, navigate to NetScaler Gateway> Filters, and click Add.

  [From Build 43.19] [#537978]

Fixed Issues in Previous 5.2 Builds

Oct 13, 2015

The issues that were addressed in Command Center 5.2 releases prior to Build 44.11. The build number provided below the issue description indicates the build in which this issue was addressed.

- The sorting option after performing a search on the Monitoring tab does not work.

  [From Build 40.1] [#429631]

- On the Administration tab, after you configure the access setting values for server protocol and server port, and then upgrade Command Center, default server protocol and server port values are reset to their defaults.

  [From Build 40.1] [#407104]

- The SoftwareUpgrade task fails to upgrade CloudBridge appliances.

  [From Build 40.1] [#435675]

- You might not be able to configure a high availability (HA) setup after upgrading a Command Center hardware appliance to version 5.1 build 33.3.

  [From Build 40.1] [#446983]

- On a Command Center hardware appliance running software version 5.1 build 33.3, a failover can cause the MYSQL replication to fail, which in turn can disable high availability (HA) functionality.

  [From Build 40.1] [#451089]

- You cannot modify the device profile from the Citrix Network > Add Device > Modify icon.

  [From Build 40.1] [#366507]

- Huge NetScaler configuration files cause high disk usage.

  [From Build 40.1] [#443441]

- After you upgrade Command Center, you cannot change the Command Center password.

  [From Build 40.1] [#452151]

- You might not be able to configure a high availability (HA) setup after changing the password of a Command Center hardware appliance.

  [From Build 40.1] [#452506]

- On the Configuration tab, the task specific execution log does not display the Command Center user details.

  [From Build 40.1] [#451621]

- On the Configuration tab, after you click Add Command to add a command while adding or editing a custom task, the Command field d does not provide a scroll option for long commands.

[From Build 40.1] [#451367]

- On the Configuration tab, when you edit a custom task and click Add Task Variable to add a variable task, some fields are not displayed.

  [From Build 40.1] [#451390]

- The Monitoring tab might not display the list of polled entities for a NetScaler HA pair.

  [From Build 40.1] [#461609]

- When you add a device, the Device Profile drop-down list does not display all the available device profiles.

  [From Build 40.1] [#460486, 461822]

- If you use the Command Center graphical user interface (GUI) to change the database password for a high availability (HA) setup, the password change is not propagated to the secondary Command Center appliance.

  [From Build 40.1] [#458009]

- When you generate a technical support file, the size of the stdout.txt file increases, causing an Out Of Memory (OOM) condition. As a result, Command Center fails to generate the technical support files.

  [From Build 41.14] [#450086]

- Event severity configuration changes roll back to their default configurations after a service pack installation.

  [From Build 41.14] [#203098]

- When a secure FTP to a NetScaler device fails, an OutOfMemory (OOO) error occurs.

  [From Build 41.14] [#381157, 462974]

- If the licensing server fails, you cannot log on to Command Center.

  [From Build 41.14] [#454501]

- An IE9 browser displays long overlapping commands in the ConfigurationChangeHistory built-in audit policy reports.

  [From Build 41.14] [#464370]

- The refresh button on the Citrix Network > Maps page does not work.

  [From Build 41.14] [#465180]

- In Command Center 5.2, you cannot modify the custom logs, such as ccapiout.txt, ccapierr.txt and ccagentout.txt.

  [From Build 41.14] [#465802]

- You can create duplicate groups through the 'Add Users' option.

  [From Build 41.14] [#477690]

- If you upgrade Command Center to version 5.2, build 40.1, the SNMP community setting might become a blank string.

  [From Build 41.14] [#470841]

- If you click on the Monitoring tab, Command Center throws an undefined error.

  [From Build 41.14] [#474504]

- The AppFirewall Recent Logs Screen displays incorrect field values if the Signature category contains more than one hyphen in Signature Violations syslogs.

  [From Build 42.7] [#507310]

- The Reporting tab for Application Firewall (Reporting> AppFirewall > Recent Logs) displays incorrect values for APPFW_MAX_UPLOADS.

  [From Build 42.7] [#500465]

- After you install Command Center, you cannot add a CloudBridge 7.2.1 appliance to the Command Center inventory if the CloudBridge serial number is more than 50 characters long.

  [From Build 42.7] [#494506, 262274]

- After you upgrade a Command Center appliance, you might not be able to log on to Command Center if you have configured a syslog server with a port value other than the default.

  [From Build 42.7] [#503478]

- The entities displayed on the Monitoring tab disappear when the cleanup scheduler deletes the latest polled entities along with the older ones.

  [From Build 42.7] [#508157]

- The uninstall option functions on Command Center appliance.

  [From Build 42.7] [#489381]

- The custom task parameters are not preserved if you create a custom task by importing an xml file or if you export the custom task as an xml file.

  [From Build 42.7] [#487502, 487158]

- If, While configuring the server settings on the Administration tab (Settings > Server Settings), you select host name as the Device label, the search functionality for host name does not work across the Command Center graphical user interface.

  [From Build 42.7] [#471722]

- The following counters are defined as OCTET STRINGs in NetScaler SNMP MIB, but are actually Counter64 values and are not polled in Command Center for reporting.

  -vserverTable_vsvrClientConnOpenRate

  -nsTcpStatsGroup_tcpTotClientConnOpenRate

  -serviceGroupMemberTable_svcGrpMemberRequestRate

  -serviceGroupMemberTable_svcGrpMemberRxBytesRate

-serviceGroupMemberTable_svcGrpMemberTxBytesRate

-serviceGroupMemberTable_svcGrpMemberSynfloodRate

[From Build 42.7] [#486885]

- If an existing custom task is open when you create a new custom task, the details of the new task are replicated in the existing task.

  [From Build 42.7] [#506699]

- If you configure the root user password of a Command Center appliance to include special characters, the root user cannot use SSH to connect to the Command Center virtual machine or the XenServer virtual machine.

  [From Build 42.7] [#503379]

- If Command Center is configured with a custom certificate that does not have a default password, the Command Center service fails to start during an upgrade.

  [From Build 43.19] [#558984]

- Command Center service fails to start, because of JRE corruption.

  [From Build 43.19] [#555113]

- When OpenLDAP is used for Command Center authentication, a logon attempt with valid credentials fails.

  [From Build 43.19] [#546717]

- If you configure the autoconfiguration feature and create a configuration profile with more than 675 lines of commands, the configuration profile is not listed in the configured profile list.

  [From Build 43.19] [#492978]

- You cannot export the device inventory details for CloudBridge Accelerator and NetScaler devices.

  [From Build 43.19] [#494486]

- The Administration tab displays the following error message if Command Center does not receive enough database connections:

  'Audit Log:{ "errorcode": 400, "message": "No Custom view found with the id "AuthAudit" for user <user_name>i"}

  Workaround: Run the Update_Patch_Db.bat/.sh file file located in <CCHome>/bin/ path to solve the issue.

  [From Build 43.19] [#508371, 517512, 525343]

- The NetScaler dashboard (Monitoring > NetScaler> Dashboard) displays incorrect CPU usage percentage values for NetScaler MPX appliances.

  [From Build 43.19] [#520245, 520362]

- If a user is disabled on the Active Directory server, and a new user logs on to the Command Center server, the logs show that the user who is disabled on the Active Directory server is performing the actions of creating the new user on the Command Center server as part of authentication.

[From Build 43.19] [#509985]

- The NetScalerConfigChange trap is generated every time a NetScaler 10.5 appliance is rediscovered.

  [From Build 43.19] [#511987]

- If you sort the date columns on the Command Center server, the sort is based on the string, not the date value.

  [From Build 43.19] [#517492]

- When you search for Active Directory groups by specifying the group name characters, Command Center displays incorrect results.

  [From Build 43.19] [#522857]

- In an HA configuration, the data in the primary node is not synced with the secondary nodebecause of compression issues.

  [From Build 43.19] [#509033]

- Command Center displays an error message if you access NITRO APIs by using unsupported JRE versions.

  [From Build 43.19] [#519367]

- If you upgrade a Command Center server to release 5.2, the Command Center service does not start. It displays the "No suitable driver found" error message.

  [From Build 43.19] [#520472]

- The Linux script EncryptPassword.sh throws a bad interpreter error because the script contains ^M characters.

  [From Build 43.19] [#521956]

- The Customize button for all built-in tasks is now modified to "Save As."

  [From Build 43.19] [#517503]

- Your Command Center service account changes to a network service account after you upgrade to a release 5.2 build.

  [From Build 43.19] [#522953]

- On the device inventory screen, if you right-click a device and click Alarms, the Command Center server displays the "Error in retrieving alarms" message.

  It also does not function if you configure Command Center to display the Host Name column.

  [From Build 43.19] [#527294]

- On the Citrix Device Inventory, the View Alarms operations does not function if you configure Command Center to display the Host Name column.

  [From Build 43.19] [#527297]

- If an alarm is triggered when you assign the Execute Task action with an SNMP filter, the Command Center server

displays the "Error in retrieving Alarm Trigger" error message.

[From Build 43.19] [#527706]

- The user credentials of external users who are authenticated over the RADIUS server are stored in the Command Center server.

  [From Build 43.19] [#533061]

- If a user is present in both local server and RADIUS server, the user password gets overwritten on the Command Center server.

  [From Build 43.19] [#533618]

FAQs

Apr 11, 2016

Answers to frequently asked questions about Command Center are available in the following categories:

- General
- Installation & Setup
- Administration
- Citrix Network
- Configuration
- Fault
- Reporting
- Command Center Appliance

Q: How do I verify that Command Center service has started properly?

A: To verify that the Command Center service has started properly, you can do one of the following:

- Windows operating system: In Window Service console, see the status of the service.
- Linux: Use the /int.d/NSCCService status command to verify that the service has started.
- You can also check the status of the service in the logs/wrapper.log file. Verify that the following log entry is present at the end of the file "Please connect to web client using port <port number>."

Q:Which are the weak ciphers in Command Center and how do I remove these weak ciphers from Command Center?

A: TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA are the weak ciphers configured by default on Command Center. Because of these weak ciphers, the Command Center login page fails to load.

To remove these ciphers from a standalone Command Center

1. Stop the Command Center service.
2. Remove these ciphers from the following files:
   - <CC_Homel>/apache/tomcat/conf/backup/server.xml
   - <CC_Home>/conf/ transportProvider.conf
3. Start the command center service.

To remove these ciphers from a Command Center HA pair

1. Stop the Command Center service on the secondary node and then stop the Command Center service on the primary node.
2. Remove these ciphers from the following files on both the primary and secondary node:
   - <CC_Homel>/apache/tomcat/conf/backup/server.xml
   - <CC_Home>/conf/ transportProvider.conf
3. Start the Command Center service on the primary node and the start the Command Center service on the secondary node.

Q: I am not able to connect to the Command Center client. What are the possible causes ?

Possible Cause: Command Center service has not started properly.

Action: Check to see if the Command Center service is started. If not, start the service.

Possible Cause: You have not presented valid root-user credentials.

Action: Provide the correct credentials. If the error occurs even with the correct credentials, shut down the server and check the **securitydbData.XML** file. If it is empty, reinitialize the database.

Possible Cause: If the PostgreSQL service has not started, the Command Center service does not start.

Action: In wrapper.log file, if you see a " PostgreSQL doesn't start in timely fashion" entry, start the PostgreSOL service first and then start the Command Center server.

Possible Cause: To access the Command Center client, you are using Internet Explorer with compatibility mode enabled.

Action: Disable compatibility mode, and then access the client.

Other possible causes :

- You are using host name that contains an underscore special character.
- The Command Center client is running with a NATed IP address.
- The Firewall is blocking the ports required by Command Center. If the firewall is enabled, disable it or unblock the ports needed for communication with the client.
- The connection to the database has been lost. To check, view the log entry in the logs/wrapper.log file.
- The host name used to access the Command Center server does not resolve to the Command Center IP address.
- The browser cache was not cleared after an upgrade.
- The port you are using to access the client has been modified from the default (Https 8443 or Http 9090).

Q: I am not able to access the user interface of the secondary Command Center over port 8443.

A: You can only access the primary Command Center through the GUI when configured in HA mode. The secondary Command Center only monitors the state and is not accessible through GUI.

Q: Can Command Center be monitored through any SNMP Manger?

A: Yes, since Command Center behaves as an SNMP agent on port 8161, any SNMP manager can contact Command Center through this port. Command Center can be monitored by loading NS-CC-MIB, which is in the <CC_Home>/mibs folder on any SNMP manager.

Q: Do I need to add Command Center agent as a trap destination on the devices managed by Command Center agent ?

A: No. Command Center server adds its IP address as a trap destination in the discovered devices. Command Center Agent does not add itself as a trap destination but only does the performance data collection, syslog, and entity monitoring. Traps are still handled by the Command Center server.

Q: How do I change the default ports used by Command Center ?

A: You can change the default port (8443 or 9090) to any standard TCP port by modifying the **Server Port** details in the **Administration > Settings > Access Settings** window. The changes in access settings are effective only after a restart.

Q: Can I back up and restore data?

A: You can do a data backup and restore only on a Command Center appliance.

Q: Is a license required for evaluation-mode installation of the software version of command center?

A: No.

Q: I am not able to log on to the Command Center server. Where can I view the current Command Center version?

A: You can find the version information in the <CCHome>/conf/AboutDialogProps.xml file.

Q: Which Oracle JDBC driver version does Citrix Command Center use?

A: Command Center uses Oracle JDBC Driver version 10.2.0.3.0.

Q: What databases does Command Center support?

A: For detailed information about supported databases, see http://docs.citrix.com/en-us/command-center/5-2/cc-install-cc-wrapper-con/cc-install-plan-installation-con.html#cc-install-database-settings-ref-sh.

Q: Does Command Center support any database resiliency solution, such as mirroring, or any other replication methods that I can consider implementing?

A: You can replicate a MySQL database in Command Center. Use Command Center in an HA setup with MySQL two-way replication.

Q: How do I migrate from one type of database to another?

A: To migrate from one type of database to another, for example from MS SQL to Oracle:

1. Stop Command Center.
2. Migrate the database (for example, from MS SQL to Oracle) with the help of your database administrator.
3. In the **<CCHome>\bin** directory, execute the **database_switch.bat** (Windows) or **database_switch.sh** (Linux) script. Include an argument identifying the new database.

   Examples:

   <CCHome> \bin\database_switch.bat ORACLE
   <CCHome> \bin\ sh database_switch.sh ORACLE

4. Open the **<CCHOME>\classes\hbnlib\hibernate.cfg.xml** file in a text editor and, under **<!--For Using Oracle DB , Uncomment the below tags -->**, edit the following line to specify the host name, port number, and connection string of the new database:

   <property name="connection.url">jdbc:oracle:thin:@HOST_NAME:PORT_NUMBER:CONNECT_STRING</property>

   Example:

   <property name="connection.url">jdbc:oracle:thin:@10.102.40.248:1521:giridb52</property>

5. In the **<CCHome>\bin\admintools** directory, execute the **EncryptPassword** script and specify the user name, current password, and the new password to get the encrypted password for the new password that you specified.

   On a Windows system, enter the following command:
   <CCHome>\bin\admintools EncryptPassword.bat root *rootpassword* newpassword

   On a Linux operating system, enter the following command:
   <CCHome>\bin\admintools sh EncryptPassword.sh root rootpassword newpassword

   Examples:

   <CCHome>\bin\admintools EncryptPassword.bat root public Password123

   <CCHome>\bin\admintools sh EncryptPassword.sh root public Password123

   The system returns the encrypted version of the new password. For example:
   e8063X6

6. In the **hibernate.cfg.xml** file, under **<!--For Using Oracle DB , Uncomment the below tags -->**, copy the new encrypted password to the property name line. For example:

   <property name="connection.encryptedpassword">e8063X6</property>
7. Save the changes.

8. Restart Command Center and verify that it is using the new database.

Q: When Command Center is installed in "Evaluation" mode, what is the default DB size allocated to it?

A: For installation in "Evaluation" mode, there is no DB size limit for the internal DB. It depends on the available storage space of the system that the user installs on.

Q: When Command Center is installed in "Typical" mode, can we install the packaged PostgreSQL DB?
A: We do not recommend the usage of PostgreSQL DB in a production deployment.
Q:Can I configure ciphers on Command Center?

A: Yes, you can configure ciphers on Command Center.

A Command Center server or an appliance ships with a set of predefined ciphers. The default ciphers which are supported by Command Center are:

ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384,DHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-SHA384,ECDHE-RSA-AES128-SHA256,ECDHE-RSA-AES256-SHA,ECDHE-RSA-AES128-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-AES128-SHA256,DHE-RSA-AES256-SHA,DHE-RSA-AES128-SHA,ECDHE-RSA-DES-CBC3-SHA,EDH-RSA-DES-CBC3-SHA,AES256-GCM-SHA384,AES128-GCM-SHA256,AES256-SHA256,AES128-SHA256,AES256-SHA,AES128-SHA,DES-CBC3-SHA,HIGH,!aNULL,!eNULL,!EXPORT,!DES,!MD5,!PSK,!RC4,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AI

To use ciphers other than the predefined cipher, you have to explicitly define them in the server.xml and transportProvider.conf files.

To configure a cipher

1. Open server.xml file located in the path <CC_HOME>\apache\tomcat\conf\backup, and include one or more ciphers as follows:
   <CIPHERSUITES>ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256 </CIPHERSUITES>

   Figure 1. Server.xml

```
    -->

    <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 ## OLD
##-->
    <!-- <Connector port="WEBCONTAINER_PORT"
               enableLookups="false" debug="0"
           protocol="AJP/1.3" /> -->

       <!--For SSL Configuration Uncomment the below line -->

<Connector SSLEnabled="true" acceptCount="100"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA"
clientAuth="false" connectionTimeout="-1" debug="0"
disableUploadTimeout="true" enableLookups="false"
keystoreFile="conf/server.keystore" keystorePass="commandcenter"
maxSpareThreads="15" maxThreads="150" minSpareThreads="5"
port="SSL_PORT" scheme="https" secure="true" server="Apache"
sslEnabledProtocols="TLSv1" sslProtocol="TLS"/>

<!-- For DUAL IP Configuration Uncomment the below line-->
<!--
     <Connector port="WEBCONTAINER_PORT" address="192.168.111.190"
maxThreads="50" minSpareThreads="3" maxSpareThreads="25"
enableLookups="true" acceptCount="100" connectionTimeout="-1"
disableUploadTimeout="true" URIEncoding="UTF-8" compression="force"
compressionMinSize="1024" noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml"/>
```

Open transportProvider.conf file located in the path CC_HOME>\conf, and include one or more ciphers as follows:

<CIPHERSUITES>ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256 </CIPHERSUITES>

Figure 2. TransportProvider.conf

```
    </PROTOCOL>

     <PROTOCOL
            NAME = "RMI"
            SERVER_CLASS_NAME = "com.adventnet.management.transport.RMIServerTransportImpl"
            CLIENT_CLASS_NAME = "com.adventnet.management.transport.RMIClientTransportImpl" >

            <RMI_REGISTRY_PORT> 1099 </RMI_REGISTRY_PORT>
            <RMI_BIND_NAME> MainSocketAPI </RMI_BIND_NAME>
            <SOCKET_PORT_DIR> html </SOCKET_PORT_DIR>
            <SOCKET_PORT_FILE> NMSSocketPort.html </SOCKET_PORT_FILE>
          <DEBUG> false </DEBUG>

    </PROTOCOL>

    <PROTOCOL
            NAME = "SSL"
            SERVER_CLASS_NAME = "com.ns.ems.server.tools.CitrixTransProImpl"
            CLIENT_CLASS_NAME = "com.ns.ems.server.tools.CitrixTransProImpl" >

            <PORT_TO_LISTEN> 0 </PORT_TO_LISTEN>
            <SERVER_BACK_LOG> 300 </SERVER_BACK_LOG>
            <SOCKET_PORT_DIR> html </SOCKET_PORT_DIR>
            <SOCKET_PORT_FILE> NMSSocketPort.html </SOCKET_PORT_FILE>
            <DEBUG> false </DEBUG>

            <TRUST_STORE_FILE>conf/Truststore.truststore</TRUST_STORE_FILE>
            <TRUST_STORE_PASSWORD>commandcenter</TRUST_STORE_PASSWORD>
            <KEY_STORE_FILE>conf/server.keystore</KEY_STORE_FILE>
            <KEY_STORE_PASSWORD>commandcenter</KEY_STORE_PASSWORD>
            <CIPHERSUITES>TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA</CIPHERSUITES>
    </PROTOCOL>
```

Q: How do I synchronize the time zone of primary and secondary XenServer servers hosting the Command Center instance?
A: To ensure synchronization of the time zones of the primary and secondary XenServer servers, do the following:

1. In the configuration utility, navigate to Administration > Tools > Setup Wizard > System Settings and verify that a valid NTP server is configured on both the primary and the secondary Command Center instance.
2. Stop primary and secondary Command Center services.
3. Enter the following commands on both primary and the secondary Xenserver:
   /etc/init.d/ntpd stop
   ntpd -gq
   /etc/init.d/ntpd start
4. Check the time on each Command Center instance to verify that the time zones are synchronized.

Updated: 2013-07-03

Q: After installing the latest version of Command Center 5.0, I do not see the Start option under Windows Start > Programs > Command Center options. How do I start the Command Center server?

A: The Command Center server is installed and service is started automatically when you install Command Center version 5.0. You can directly access the Command Center server from the web browser by typing either of the following in the address field:

http://ComputerName:PortNumber

or

https://ComputerName:PortNumber

where:
- ComputerName is the fully qualified domain name (FQDN), host name, or IP address of the Command Center server.
- PortNumber is the port that the Command Center client and server use to communicate with each other. The default port number for HTTP is 9090, and for HTTPS it is 8443.

Q: Where do I view the installation log statements for Command Center version 5.0 or later ?

A: If installation is successful, for either Windows or Linux, the path to the logs is:
- :<CC_HOME>\ _Citrix Command Center_installation\Logs

  If you cancel the installation before the installation starts, or some error occurs during the pre-installation steps, the location depends on whether you are running windows or Linux.

- Windows:

  :<desktop_dir>\Citrix_Command_Center_Install_<mm>_<dd>_<yyyy>_<hh>_<mm>_<ss>.log

- Linux:

  <user_dir>\Citrix_Command_Center_Install_<mm>_<dd>_<yyyy>_<hh>_<mm>_<ss>.log

Q: After installing Command Center, I am unable to start it properly. Where do I look for the log statements regarding startup and shutdown?

A: A Look for the wrapper.log file in the <CCHome>/logs directory. The information in this log file includes the log statements regarding startup and shutdown. If you do not find the wrapper.log file in logs directory, check for the file in <CCHOME> directory.
Note: These logs are created only when you run Command Center as a service.

Q: After moving the MS SQL database to a new host, how to point the Command Center server to the new host?

A: The procedure to point Command Center server to new host:
1. In the <CCHOME>/classes/hbnlib/ hibernate.cfg.xml file search for the following line:

   <property name="connection.url">jdbc:sqlserver://<dbserver IP>:1433;databaseName=<database name>/property>

2. Replace the existing database server IP address with the IP address or DNS name of the new database host, and replace existing database name with new database.
3. If you have changed the encrypted password for the database, do the following:
   - To obtain the encrypted password, run the command

     EncryptPassword.bat file available under <CCHOME>/bin/admintools directory.

     The usage is shown below:

     "Usage : EncryptPassword *UserName Password EncryptPassword*"

     "UserName - CC UserName with admin privileges, say root"

     "Password - Password of the User"

     "EncryptPassword - The password to be encrypted."

     Example:

     <CCHome>\bin\admintools>EncryptPassword.bat root public mynewpassword

     Encrypted Password for password "mynewpassword" is: ceMv9Me6gF5h6Cn1

   - In the < CCHOME>/classes/hbnlib/ hibernate.cfg.xml file copy the new encrypted.

     The usage is shown below:

     <property name="connection.driver_class">com.microsoft.sqlserver.jdbc.SQLServerDriver</property>

     <property name="connection.url">jdbc:sqlserver://1.1.1.1.:1433;databaseName=CCDB</property>

     <property name="connection.username">yourdbusername</property>

     <property name="connection.encryptedpassword"> ceMv9Me6gF5h6Cn1</property>

     <property name="dialect">org.hibernate.dialect.SQLServerDialect</property>

     <property name="databasename">MSSQL</property>
     Note: The password is copied to the tag with property name - "connection.encryptedpassword".
4. Restart the Command Center server for the changes to take effect.

Note: The above procedure only points Command Center server to the new database host. To migrate the data to the new host, use the tools provided by MS SQL. For more information about the MS SQL data migration, refer to the MS SQL documentation.

Q: How can I change MSSQL database ports for Command Center ?

A:

1. Stop the Command Center service.
2. Edit the <cc_home>/classes/hbnlib/hibernate.cfg.xml to change the port details.
   For example, to specify the port number as 1443:
   <property>com.microsoft.sqlserver.jdbc.SQLServerDriver</property>
   <property>jdbc:sqlserver://10.102.43.50:**1443**;DatabaseName=data2013</property>
   <property>sa</property>

Q: The Postgres database server does not start in a timely fashion. What can I do?

A: For Windows: From the Windows Service Manager, start the **PostgresForCommandCenter** service. Verify that the service has started, and then start the Command Center service.

If the Postgres service does not start, go to <CCHOME>/pgsql/startup-scripts and execute the following scripts to reinstall Postgres service:

- UninstallPostgres.bat
- CreatePostgresUser.bat
- InstallPostgres.bat

For Linux: In /<CC_home>/pgsql/startup-scripts directory and run the following scripts:

- su ccpostgres
- sh StopPostgresDB.sh
- sh StartPostgresDB.sh

If the Postgres database does not start even after restarting the service, check if the Zlib libraries are installed on the Linux system.

Note: Reinstalling the Postgres service does not result in any loss of data.

Q: After I upgrade to Command Center build 45.4 from build 44.11 of release 5.2, I encounter a Bad Request error when you access the GUI for the first time.

A: Clear the bowser cache and files and access the logon page again.

Updated: 2013-06-26

Q: Why am I getting a "User not authorized" message when I log on?

A: This message appears if you belongs to a group to which no permissions are assigned. Generally, a users created on the fly in an external authentication server faces this issue. To resolve the issue, the administrator has to log on to the authentication server and assign the user to a proper group.

Q: Can I control the list of tasks that are visible to the user in Command Center?

A: Yes, you can use the Custom View Scope feature in Command Center.

Q: Why am I not able to see all the groups when I use the **Browse** option of **Add Group** after choosing external Authentication?

A: The Active Directory server always returns 1000 records at a time. You can directly key in the group name in the field instead of using **Browse** and select option.

Q: After a force failover, why am I not able to log on if external authentication is set as RADIUS in a Command Center HA setup?

A: You have to log on to Command Center as a local user with Admin privileges and change the Client IP address to the current Command Center server IP address (which was the secondary IP address before the forced failover).

Q: Which are the wildcard characters supported in Custom View Scope?

A: Command Center supports '%' wildcard character for contains case only.

Q: What Active Directory versions does Command Center support?

A: Windows 2008, Windows 2008R2, and Windows 2012.

Q: How can I do a factory reset of root user authorization?

A: Run the following script:

bin/ResetSecurityAdmin.bat/.sh

Q: Does Command Center support secure LDAP?

A:No.

Q: Can users belonging to a subdomain log on to Command Center?

A: Yes. Subdomain users can log on to Command Center if subdomain LDAP is configured.

Q: NetScaler discovery is failing for one particular device. What could be the cause?

A: For successful NetScaler discovery, the SNMP Manager list must be empty or Command Center must be listed as one of the SNMP Managers. Verify the SNMP Managers configured on the device.

Q: Is it possible to view the device label as a host name or system name instead of as an IP Address?

A: Yes. In **Administration > Server Settings** change the **Device Label** value to display the System Name/Host Name.

Q: Which IP address should I use to discover an SDX device?

A: Use the SVM IP address to discover the SDX device in Command Center.

Q: When I discover a CloudBridge Advanced Platform by using the SVM IP address, the CloudBridge instances on the CloudBridge Advanced Platform are not discovered in Command Center?

A: Only the CloudBridge accelerators on a CloudBridge Advanced Platform are discovered.

Q: Are NAT, SNIP, and MIP based discovery of NetScaler devices supported in Command Center?

A: Yes. But SNIP and MIP cannot be used for the discovery of a device configured in HA mode.

Q: I changed the credentials of my device; do I have to change the credentials in Command Center also?

A: Yes, you have to update the credentials in the device profile that is used to discover that device. After you update the profile, you have to rediscover the device.

Q: How can I back up the configuration files, such as ns.conf, for a device?

A: Command Center backs up the NetScaler configuration(ns.conf, the certificates, and so on) the first time the device is discovered and at regular intervals. By Default, the archive interval is 12 hours. You can back up the configuration files on demand from the page that lists the properties of that device.

Q: Where is the ns.conf file located on my Command Center ?

A: The file is located on the database as a plain text.

Q: I am trying to discover a NetScaler device with SNMP v3 profile and the discovery fails with the following error message: **Problem in finding device HA Mode for this device. For input string: " "** . What should I do?

A: On the NetScaler device, in the SNMP v3 view, verify if you have set the subtree value to 1. If it is not set to 1, then clear the SNMP v3 configuration (SNMP view, SNMP group, and SNMP user) from the NetScaler device. Delete the device from Command Center and re-discover.

Q: I am not able to view the configuration change history for a device.

A: Check the "Configuration Changes Duration" value you have configured. You may not be able to view the history as there may not be any configuration changes in specified duration.

Q: Can I export and mail the change management reports ?

A: Yes, you can use the **Schedule** option of Audit policies to schedule export and mailing of the reports.

Q: How can I migrate a Command Center installation to a new server?

A: The following procedure moves an existing Command Center service with MSSQL as its database.

1. Stop the existing command center service on the first virtual machine.
2. Run the following query on the database:delete from CCServerConfig where PROPNAME="CODING_HASH1" OR PROPNAME="CODING_HASH2".
3. Install another Command Center copy on another virtual machine of the same build, using the same database.
4. When connecting to the same database, you are prompted for whether you want to set up the new command center copy as the secondary command center. Type yes.
5. Stop the new command center service and move the securitydbData.xml.bkup file from its current directory (\conf\CCbackup) to the directory in which you installed the copy (\conf\). Then, rename the file to securitydbData.xml.

6. In the conf folder, open the NMsProcessedBE.conf file, search for “persis_data_in_XML false” and change it to “persist_data_in_XML true.
7. In the conf directory of the new command center copy , replace the following files with files from the conf directory of the previous server (the server from which you are moving Command Center):

- "conf\alert.filters"
- "conf\BackUp.conf"
- "conf\Polling.conf"
- "conf\event.filters"
- "conf\log4j.xml"
- "conf\monitoringcertseverity.xml"
- "conf\NonPolledVariables.properties"
- "conf\Threshold.conf"
- "conf\trapport.conf"
- "conf\Authentication.xml"
- "conf\eventseverity.xml"
- "conf\DistributedPoller.xml"
- "conf\FailOver.xml"
- "conf\GlobalTrapForwardSettings.properties"
- "conf\SnmpDefaultProperties.xml"
- "conf\SMTPSettings.properties"

8. Start the Command Center server from the new location.

Updated: 2014-08-27

Q: Why is the "Send Mail" action not working?

Possible Cause: The mail server credentials might be incorrect or mail server might not be accessible from Command Center.

Action: Check the mail server credentials and verify that the mail server is accessible from command center server. If the mail server credentials are not correct, edit the settings in Administration > Mail Server Settings .

You can refer to the exception logged under logs > stderr file.

Example of log entry for this exception:

```
Exception while sending mail notification. Sending failed;
nested exception is:
class javax.mail.MessagingException: Could not connect to SMTP host: 10.102.173.25, port: 25;
nested exception is:
java.net.ConnectException: Connection refused: connect
Invalid HostName or Port, unable to connect the mail server
```

Possible Cause: The Events/Alarms fields are not configured correctly.

Action: Check if Event/Alarm fields are configured correctly. The Message field, should match or be a part of the message of any incoming Event/Alarm.

Example of log entry for this exception:

```
Failed Object, Message.
```

Q: Can I keep a historical log of SNMP alarms and events in Command Center ?

A: Currently, only 10000 events are displayed, due to user-interface restrictions, but, by default, the events/alarms from the past 6 months are stored in the database.

Q: Command Center is not receiving the traps sent by a device. What are the possible causes?

A: The possible reasons for not receiving traps could be:

- If you enable firewall on Command Center server, it does not receive the traps
- SNMP port is being used by some other application in the Command Center server system.
- Event triggers are set to suppress the action.
- Custom View Scope is set for the device.
- Triggers are set with incorrect message fields.
- Triggers have alarm age set to a high value.
- If Command Center is installed on a Linux server, the iptable configuration might cause filtering of SNMP packets.
- Traps from unmanaged devices are not processed by Command Center.
- The default Trap port has been changed by the administrator under Administration > Settings > Trap Forward Settings.

Q: Do I need to specifically enable SNMP on Command Center? if yes, how can I do so?

A: You need not enable SNMP. It is already running on port 8161. When the Command Center service is running, Command Center behaves as an SNMP agent on port 8161, and any SNMP manager can contact Command Center through this port.

Q: Can I set triggers for all of the devices?

A: Yes. In the**Add Filters** window, leave the **Devices** field empty. All the devices discovered are then selected.

Q: Alarm Triggers actions are not being initiated for the generic category of alarms.

A: Since Alarms are not updated for generic traps, such as reboot, you have to manually clear the alarm to reenable the alarm trigger action, or you have to create triggers for the generic category of events.

Q: Syslogs and AppFirewall reports are not generated. What are the possible causes?

- Syslog settings on the NetScaler are not properly configured for Command Center to receive the syslog messages.
- Syslog port 514 is occupied by other application.
- AppFirewall related syslogs are not generated for the ICA type for a specified time period.

Q: Since all traps are sent to both the Command Center agent and the main Command Center, does the Command Center agent ignore these or are they sent to the database through the SQL connection?

A: Traps are handled only by the Command Center server, which adds its IP address as a trap destination on the NetScaler device during NetScaler device discovery.

Q: How can I customize the purge interval?

A: You can specify the interval at which Command Center should purge syslog data. By default, Command Center stores syslog messages for the last 90 days. To customize the purge interval, navigate to Administration > Server Settingsand specify the number of days in theSyslog Clean interval (in days) field. Only the records older than the number of days that you specify are purged. For example, if you specify as 45 days, Command Center purges syslog messages that are older than 45 days.

Q: I am able to view unwanted IPs in Failure Objects.

A: The unwanted IP addresses are from AppFirewall Client IP. Create a filter to suppress AppFirewall alarms.

Q: Is it possible to export data from Command Center for Syslogs, Appfirewall and AGEE logs?

A: No.

Q: Why am I not able to receive the SNMP traps from the device?

A: If the wrapper.log file contains the following entry: **"WARNING : Traps cannot be received on port : 162"**, failure to receive the traps could have the following possible causes:

Possible Cause1: If any other SNMP trap service is running on port 162, which is receiving the traps, Command Center might not be able to receive the SNMP traps.

Action:

- In case of Windows, check to see if SNMP is running and, if so, stop it. Then stop the Command Center service. Check the output of netstat using the following command in the command prompt:
  C:netstat -ano| find "162"
  Sample Output:
  TCP 0.0.0.0:49162 0.0.0.0:0 LISTENING 1892
  UDP [::]:162 *:* 6340)
  If you see " UDP [::]:162 *:*" in the output, it confirms that the port 162 is being used by some other application.
- Check to see if the traps are being logged in the CC FaultOut logs under logs/fault.
- If the traps are being logged, check to see if any filter action (for example, a suppress action) is configured, or if the user has configured any custom view scope.
- In case of Linux, check to see if SNMP packets are being filtered because of iptable configuration. In this case, tcpdump still shows that the packets are reaching their destination.

Possible Cause 2: Traps from unmanaged devices are not processed by Command Center.

Action: Check if to see if the trap destination and port are correctly configured on the device.

Q: Why am I not able to view the old events?

A: *Explanation*: By default, Command Center does not display the entire database. The default is a maximum 10,000 events, no older than 6 months.

Possible Cause 1: Command Center displays only 10,000 events in client GUI.

Action: You can change this setting by modifying the value of the **EVENT_WINDOW_SIZE** parameter in the NmsProcessesBE.conf file, which is in the <CC_HOME>/conf directory.

Possible Cause 2: Events older than 6 months are deleted.

Action: By default, the interval for cleaning the events is 6 months. You can change the interval by modifying the value of the **CLEAN_EVENT_INTERVAL** parameter in NmsProcessesBE.conf file, which is in the <CC_HOME>/conf.

Q: I am not able to view "Available Failed Objects" for a particular trap category. How do I troubleshoot the problem?

A: *Explanation*: When Command Center receives a trap, the failed objects become persistent in the Command Center database. The "Available Failed Objects" popup window displays that data.

Possible Cause: If Command Center has not received a trap for that category even once, you cannot see any failed objects for that particular trap.

Action: You can edit the field manually

Sample Events/Alarms:

For an entity-related event/alarm,(entityup/down, entityNameChanged, or entityofs), configure the failed object in the event/alarm trigger:

`failedobject = $vserver_name OR $service_name OR $interface_name`

For a Threshold event/alarm

`failedobject = $counterName:$instance`

Examples:

- Rx Average bandwidth(bits/sec):LO/1
- Vserver current client connections:CC_Vsvr(10.102.31.110:8443)

Q: When I generate a report, I encounter a "No Data to Chart" message.

A: *Possible Cause 1:* Counters for polling are disabled.

Action: Check to see if you have enabled the counter for polling in the **Configure Polled Counters** interface. If you have enabled it, clear the **Exclude Zero Values** check box for that polled counter, and then see if the report is generated.

Troubleshooting

Check the `PerformanceErr` file to see if there are any error messages logged for the particular counter and device. Some of the common error messages are: *Error:* "Invalid instance... Dropping packet for instance with value."

Explanation: This error is generally observed in Command Center version 3.x.

Action: Upgrade to 4.0 should take care of this. *Error:* "Request timed Out".

Explanation: This error appears when SNMP requests to the device are timing out.

Action: You can check the network connectivity and verify the accuracy of SNMP credentials in the device profile. *Error:* "Could not poll... No such object in this MIB".

Explanation: This error occurs when a particular version of the device does not support the counter for which the report is being generated.

Q: The Command Center graphs and values from the NetScaler device do not match.

A: A rate-counter value is calculated as the difference between two successive poll values divided by poll interval. The graphs plotted with these counters do not match with the exact values collected from the device.

Updated: 2013-06-26

Q: Can Command Center appliances be monitored through any other SNMP Manager?

A: Yes, Command Center Appliance can be monitored by loading Command Center appliance MIB `NS-CC-MIB` onto any SNMP Manager. The MIB, which is in the `<CC_Home>/mibs` directory, currently supports only the `CC appliance host name` object. Contact and Location are not supported.

Note that the Command Center agent does not add itself as a trap destination; it does only performance data collection, syslog, and entity monitoring. Traps are still handled by Command Center server.

Q: Is there a process for configuring SNMP traps on a Command Center appliance?

A: No. Users cannot configure SNMP traps on a Command Center appliance.

Q: Is evaluation license supported for Command Center appliance ?

A: Yes, it is supported from Command Center version 5.0, build 35.11 onwards.

Command Center Appliance

Mar 20, 2010

The Command Center appliance provides a hardware-based turnkey solution with a preloaded database. This section of the library describes initial set-up and basic configuration of the Command Center appliance, including the following topics.

In This Section

Introduction	Provides information on external software components, hardware components, and hardware platform.
Preparing for Installation	Provides unpacking, specific site and rack requirements, and safety precautions to be followed when installing the hardware.
Installing the Hardware	Tasks for installing the hardware, including rack mounting, connecting the console cable, connecting to a power source, and connecting to a network.
Initial Configuration	Procedures for configuring a Command Center appliance for the first time.
Command Center Appliances in a High Availability Pair	Provides instructions on how to configure Command Center appliances in high availability mode.
Command Center Appliance Licenses	Describes the procedures for obtaining and upgrading appliance licenses.
Upgrading Command Center	Describes step-by-step procedure to upgrade to a later release on a standalone Command Center appliance or an HA pair.
Performing Backup and Restore Operations	Provides a conceptual reference and instructions for performing backup and restore operations.

Introduction

May 28, 2015

The Command Center appliance provides a hardware-based turnkey solution with a preloaded database. The Command Center appliance simplifies administrative tasks by providing the following capabilities:

- No external dependency for database and license
- No additional hardware required for deployment
- Reduced overall maintenance expenses on hardware and software
- Increased scalability due to advance enterprise-grade hardware
- Increased efficiency and security because it is a complete package

The Command Center appliance comprises the Citrix XenServer virtualization platform designed for efficient management of the CentOS operating system, the Command Center software, and the MySQL database. The MySQL database is packaged as part of the appliance, eliminating the need for an external database.

This topic includes the following details:

- External Software Components
- Hardware Components
- Hardware Platform

Updated: 2014-04-29

The Command Center appliance uses the following external software components.

- XenServer—XenServer is a server virtualization platform that offers near bare-metal virtualization performance for virtualized server and client operating systems. The Command Center appliance uses XenServer version 5.6. For more information about XenServer, see http://support.citrix.com/product/xens/v5.6fp1/#tab-doc
- CentOS— CentOS is a free Enterprise-class Linux Distribution. The Command Center appliance uses CentOS version 5.5. For more information about CentOS, see http://www.centos.org/
- MySQL— The Command Center appliance uses MySQL standard version 5.1.48 and 5.6. For more information about MySQL, see http://www.oracle.com/us/products/mysql/mysqlstandard/index.html

Updated: 2015-05-28

The front panel of the Command Center appliance has RS232 serial ports and 10/100/100Base-T copper Ethernet ports. The back panel provides access to the power supply, fan, CompactFlash card, and hard-disk drive.

This topic includes the following details:

- Ports
- Power Supply
- Hard Disk Drive

Ports

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

The copper Ethernet ports installed on the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

10/100BASE-T port

The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps).

10/100/1000BASE-T port

The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, ten times faster than the other type of copper Ethernet port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Note: These ports are not used in the current release.

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.
Note: Use the management port numbered 0/1 to get direct access to the appliance.
Note: This section applies to the MPX 5500, MPX 5550/5650, MPX 7500/9500, MPX 8005/8015/8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 17500/19500/21500, MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542, MPX 11515/11520/11530/11540/11542, MPX 14000, and MPX 17550/19550/20550/21550, and MPX 22040/22060/22080/22100/22120, MPX 22040/22060/22080/22100/22120, MPX 24100/24150, and MPX 25100T/25160T appliances.
The port LEDs show whether a link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Table 1. LED port-status indicators

Port Type	LED Location	LED Function	LED Color	LED Indicates
Ethernet (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Yellow	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the

Port Type	LED Location	LED Function	LED Color	LED Indicates
			Blinking green	port Traffic is passing through the port.
Management (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Amber	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid yellow	Link is established but no traffic is passing through the port.
			Blinking yellow	Traffic is passing through the port.

Power Supply

Updated: 2013-10-23

For appliances containing two power supplies, the second power supply acts as a backup. The MPX 22040/22060/22080/22100/22120 appliance can accommodate four power supplies, and require two power supplies for proper operation. The third and fourth power supplies act as backup. The MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 appliances can accommodate four power supplies, and require two power supplies for proper operation. The third and fourth power supplies act as backup.

For power-supply specifications, see "Hardware Platforms," which describes the various platforms and includes a table summarizing the hardware specifications.

The MPX 7500 appliance ships with a dual power supply configuration, including two standard power cords that each have a NEMA 5-15 plug for connecting to the power outlet on the rack or in the wall.

Table 2. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.

Power Supply Type	LED Color	LED Indicates
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.
	RED	Power supply failure.
DC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing BLUE	Power supply is in standby mode.
	BLUE	Power supply is functional.
	RED	Power supply failure.
MPX 15000 and 17000	OFF	Power supply is not plugged in to a power source. If the LED is off when the power supply is plugged in, the power supply has a malfunction.
	AMBER	Power supply has been plugged in for less than a few seconds. If the LED does not turn GREEN, the power supply has a malfunction.
	GREEN	Power supply is functioning properly.
	BLINKING	Power supply has a malfunction

Table 3. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.

Power Supply Type	LED Color	LED Indicates
		Power supply failure.

Note: The power supply on the NetScaler MPX 5500 and MPX 5550/5650 appliances is not field replaceable.

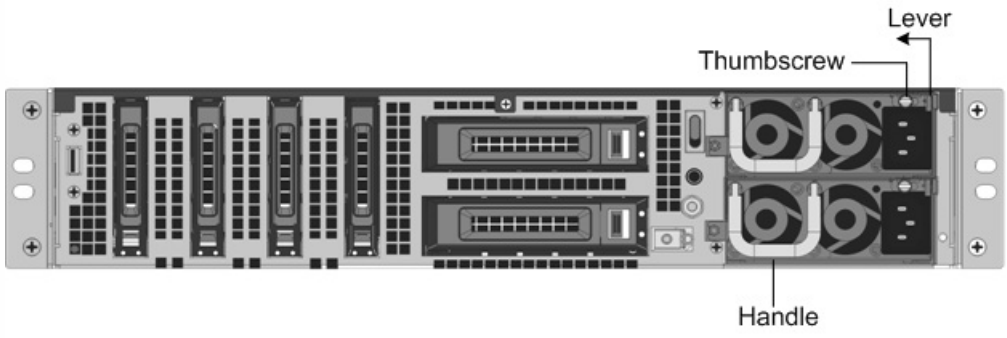
- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
- Always unplug any appliance before performing repairs or upgrades.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Citrix NetScaler MPX platforms can accommodate two power supplies, except the MPX 22040/22060/22080/22100/22120 platform which can accommodate four power supplies, except the MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the MPX 22040/22060/22080/22100/22120 platform which needs two power supplies for proper operation, except the MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 platforms which need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

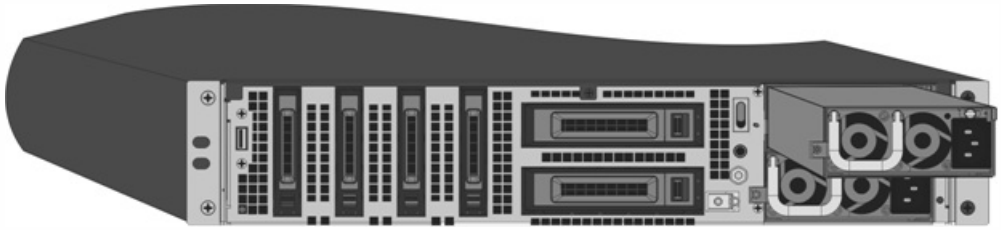
Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working, and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working, and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working.

To install or replace an AC power supply on a Citrix NetScaler appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.
   Note: The illustration in the following figures might not represent the actual NetScaler appliance.
   Figure 1. Removing the Existing AC Power Supply



2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.
   Figure 2. Inserting the Replacement AC Power Supply



5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Removable DC Power Supply is sold as an optional customer installed module.

(Citrix part number 8530019.)

Citrix NetScaler MPX platforms can accommodate two power supplies, except the MPX 22040/22060/22080/22100/22120 platform which can accommodate four power supplies, except the MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the MPX 22040/22060/22080/22100/22120 platform which needs two power supplies for proper operation, except the MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 platforms which need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

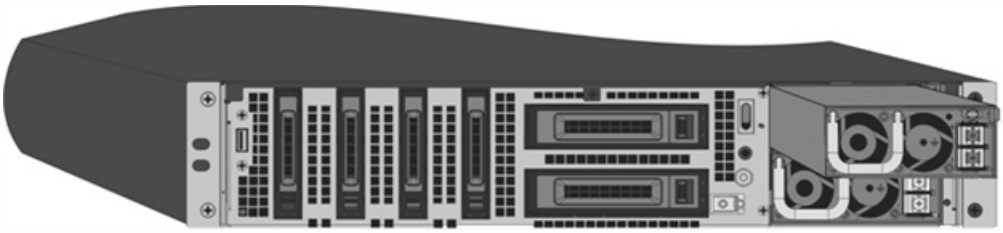
Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working, and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working, and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working.

To install or replace a DC power supply on a Citrix NetScaler applianceDC Power Supply Module Installation

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.
   Note: The illustration in the following figures might not represent the actual NetScaler appliance.
   Figure 3. Removing the Existing DC Power Supply

2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.

4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.
   Figure 4. Inserting the Replacement DC Power Supply



5. When the power supply is completely inserted into its slot, release the lever.
6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

DC Power Supply Battery Return Connection

Citrix NetScaler SDX 4x10GE SFP+8xSFP NEBS is designed to be installed in the Isolated DC Return (DC-I) configuration.

Hard Disk Drive

Updated: 2014-02-28

A hard disk drive (HDD) stores logs and other data files. Files stored on the HDD include the newnslog files, dmesg and messages files, and any core/crash files. The HDD comes in various capacities, depending on the Citrix NetScaler platform. Hard drives are used for storing files required at runtime. An HDD is mounted as /var.
The following MPX platforms support HDD:

- Citrix NetScaler MPX 9700, MPX 10500, MPX 12500, and MPX 15500
- Citrix NetScaler MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, and MPX 20500
- Citrix NetScaler MPX 11515, MPX 11520, MPX 11530, MPX 11540, and MPX 11542
- Citrix NetScaler MPX 11515, MPX 11520, MPX 11530, MPX 11540, and MPX 11542
- Citrix NetScaler MPX 15000
- Citrix NetScaler MPX 17000
- Citrix NetScaler MPX 17500, MPX 19500, and MPX 21500
- Citrix NetScaler MPX 17550, MPX 19550, MPX 20550, and MPX 21550
- Citrix NetScaler MPX 22040, MPX 22060, MPX 22080, MPX 22100, and MPX 22120
- Citrix NetScaler MPX 22040, MPX 22060, MPX 22080, MPX 22100, and MPX 22120
- Citrix NetScaler MPX 24100 and MPX 24150

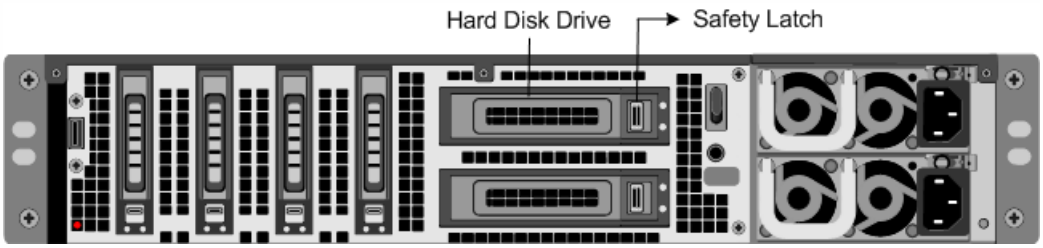
The hard disk drive contains user monitored data. It is mounted as /var.

A hard disk drive (HDD) stores log files and other user files. Collection of new log files begins upon boot-up with the new HDD. Product documentation can be downloaded from "MyCitrix.com" and reinstalled to the /var/netscaler/doc location.

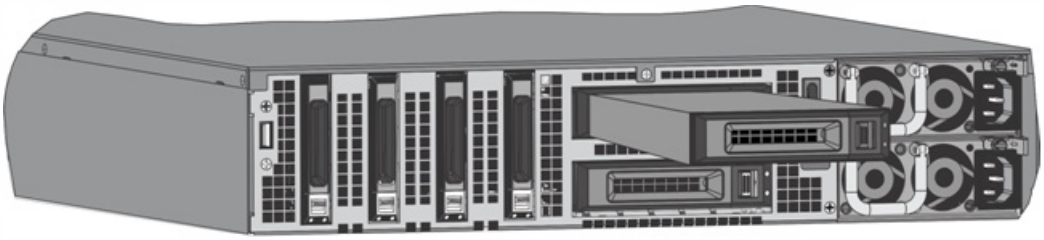
To install a hard disk drive

1. At the NetScaler command prompt, exit to the shell prompt. Type:
   shell

2. Shut down the NetScaler appliance by typing one of the following commands at the shell prompt.
   - On an MPX appliance, type:
     shutdown –p now
   - On a non-MPX appliance, type:
     shutdown
3. Locate the hard disk drive on the back panel of the appliance.
4. Verify that the replacement hard disk drive is the correct type for the NetScaler platform.
5. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.
   Note: The illustration in the following figures might not represent the actual NetScaler appliance.
   Figure 5. Removing the Existing Hard Disk Drive



6. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.
   Important: When you insert the drive, make sure that the Citrix product label is at the top.
   Figure 6. Inserting the Replacement Hard Disk Drive



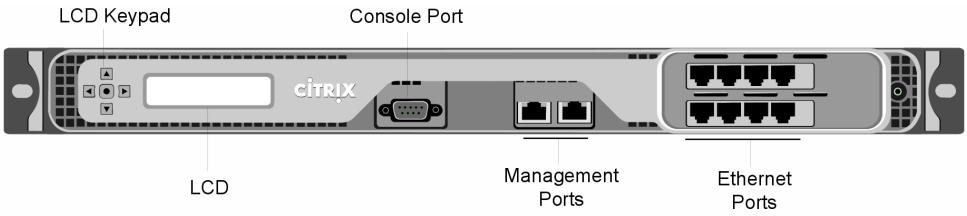
7. Turn on the NetScaler appliance. The appliance starts the NetScaler software and reads the configuration file from the CompactFlash card.

Updated: 2013-09-04

The Command Center hardware platform is the MPX™ 7500 appliance, which is a 1U appliance with one quad-core processor and 8 gigabytes (GB) of memory. The MPX 7500 appliance is available in an 8x10/100/1000Base-T copper Ethernet port configuration.

The following figure shows the front panel of the MPX 7500 (8x10/100/1000Base-T copper Ethernet ports) appliance.

Figure 7. Citrix Command Center MPX 7500(8x10/100/1000Base-T copper Ethernet ports), front panel



Note: The LCD keypad is not functional in this release.

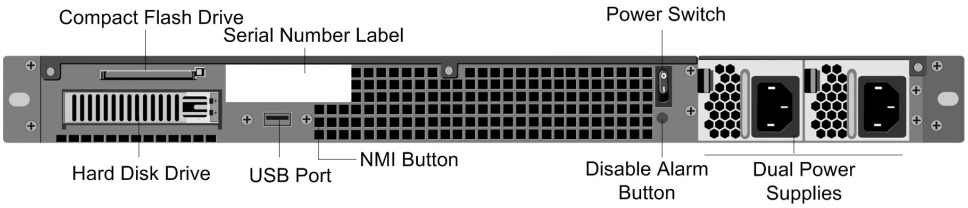
The appliance has the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports, numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
  Note: Use the first management port numbered 0/1 to connect to the appliance for system administration functions.
- Network Ports
  - MPX 7500 (8x10/100/1000Base-T copper Ethernet ports). Eight 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 on the top row from left to right, and 1/5, 1/6, 1/7, and 1/8 on the bottom row from left to right.

  Note: These ports are not used in the current release.

The following figure shows the back panel of the MPX 7500 appliance.

Figure 8. Citrix Command Center MPX 7500, back panel



The following components are visible on the back panel of the MPX 7500:

- Power switch, which turns off power to the MPX 7500, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Removable hard-disk drive (HDD) that is used to store monitored data.
- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the appliance. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Disable alarm button. This button is functional only when the appliance has two power supplies.
  Press this button to stop the power alarm from sounding when you have plugged the MPX 7500 into only one power outlet or when one power supply is malfunctioning and you want to continue operating the MPX 7500 until it is repaired.

Preparing for Installation

May 28, 2015

Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.

This topic includes the following details:

- Unpacking the Appliance
- Preparing the Site and Rack
- Cautions and Warnings

Updated: 2014-05-08

Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- The following list specifies the number of power cables included for each appliance model:
  - One power cable for the MPX 5500, MPX 5550/5650, MPX 7500/9500, and MPX 8005/8015/8200/8400/8600/8800 appliances
  - Two power cables for the 9010 FIPS, 12000-10G, MPX 15000, MPX 17000, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542, MPX 11515/11520/11530/11540/11542, MPX 14000, MPX 17500/19500/21500, and MPX 25100T/25160T, and MPX 17550/19550/20550/21550 appliances
  - Four power cables for the MPX 22040/22060/22080/22100/22120 appliance
    Note: Make sure that a power outlet is available for each cable.
  - Four power cables for the MPX 22040/22060/22080/22100/22120 and MPX 24100/24150 appliances
    Note: Make sure that a power outlet is available for each cable.

  Note: For Brazilian customers, Citrix does not ship a power cable. Use a cable that conforms to the **ABNT NBR 14136:2002** standard.
- One standard 4-post rail kit
  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network

- A computer to serve as a management workstation

Updated: 2013-07-10

There are specific site and rack requirements for the NetScaler appliance. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

Environment control

An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density

Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

Rack characteristics

Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections

At minimum, two standard power outlets per unit.

Network connections

At minimum, one Ethernet connection per rack unit.

Space requirements

One empty rack unit for the Citrix Command Center MPX 7500 appliance.

Note: You can order the following rail kits separately.

- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.

Electrical Safety Precautions

Updated: 2014-02-06

Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the

electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.
Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part that has the following label:

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no user-serviceable parts inside these components. If you suspect a problem with one of these parts, contact Citrix Technical Support.

Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.

- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.

Installing the Hardware

May 28, 2015

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

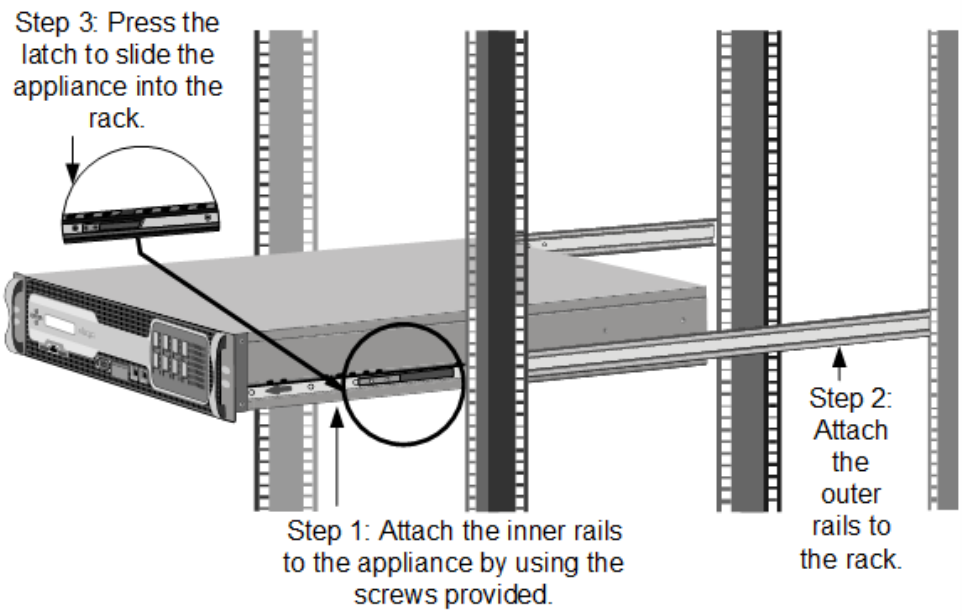
This topic includes the following details:

- Rack Mounting the Appliance
- Connecting the Cables
- Switching on the Appliance

Updated: 2015-02-12

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix Command Center appliance to a rack.

Figure 1. Rack Mounting the Appliance



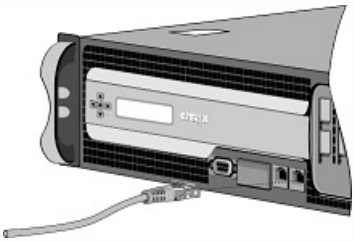
When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Danger: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Connecting the Ethernet CablesConnecting the Appliance to the Network

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

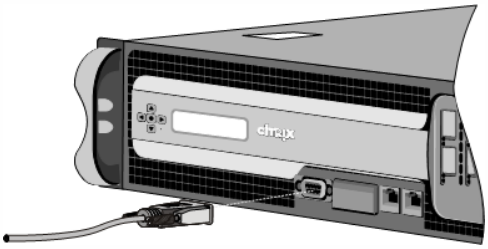
1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.
   Figure 2. Inserting an Ethernet cable



2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Note: The above Ethernet ports are not used in the current Command Center appliance release.

Connecting the Console Cable



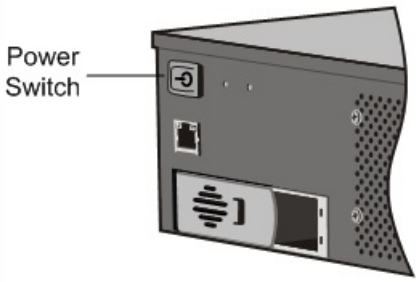
Connecting the Power Cable

Updated: 2013-10-09

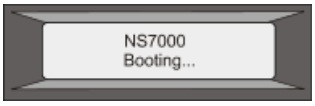
After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the back panel of the appliance.
   Figure 5. Power switch on back panel



3. Verify that the LCD on the front panel is backlit and the start message appears, as shown in the following figure.
   Figure 6. LCD startup screen



Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.

Initial Configuration

Aug 07, 2015

After you have installed your appliance in a rack, you are ready to perform the initial configuration on XenServer and Command Center appliance. Note that you will need two valid IP addresses to allot to XenServer and Command Center hardware appliance. You can configure the initial settings either by using the serial console or by changing the IP settings of your workstation or laptop and then connecting the workstation or laptop to the appliance.
Note: To locate the serial console port on your appliance, see "RS232 Serial Console Port" in Ports.

You can configure the initial settings by using the serial console and then connecting the workstation or laptop to the appliance.

To configure initial settings by using the serial console

1. Connect the console cable into your appliance. For more information, see "Connecting the Console Cable" in Connecting the Cables.
2. Use a Telnet client of your choice to access the serial console.
3. Open an SSH connection to the internal IP by typing ssh root@169.254.0.10 on the console prompt.
4. Type public as password to log into the appliance.
5. Run the Command Center appliance configuration script. At the shell prompt, type:
   sh /etc/ccnetworkconfig.sh
6. Follow the prompts and set the following parameter values to your local settings. The default values are shown within parentheses. Press Enter if you do not want to change the default value.
   - Hostname—Host name of the appliance. Change the default Hostname value. Default : cmdctr.
     Important: In an HA setup, ensure the Hostname values of the primary and secondary appliances are unique values. This is important to avoid host name resolution conflicts and ensure successful HA setup.
   - Command Center IP Address—IP address of the appliance. Default: 192.168.100.3. After initial configuration, you can access the appliance by typing this IP address in a Web browser and specifying the port as 8443. For example: https://10.102.31.69:8443/
   - XEN Server IP Address—IP address of the XenServer. Default : 192.168.100.2.
   - Enter Appliance Password—Type public as the appliance password.
   - Subnet Mask—Mask identifying the appliance's subnet. Default: 255.255.255.0
   - Gateway—IP address of the router that forwards traffic out of the appliance's subnet. Default: 192.168.100.1
   - DNS Server IP Address—IP address of the DNS server.
   - NTP Server IP Address—IP address of the NTP server.
   - Current Time zone Settings—Displays the time on the appliance. Provide the appropriate time zone.

   Note: In an HA setup, the primary and secondary appliances must have the same time stamps. This can be ensured by synchronizing both the appliances with the same NTP server and verifying that the synchronization between the appliances and NTP server is successful. This is important to ensure an accurate timeline for performance data in case of a failover.
7. When prompted to restart, select y.
8. Connect the Ethernet cable to the appliance to add the appliance to your subnet.

The appliance automatically restarts. You have now completed initial configuration of your Command Center appliance.

EXAMPLE

```
[root@NSCmdCtr ~]#
[root@NSCmdCtr ~]# ssh root@169.254.0.10
root@169.254.0.10's password:
Last login: Mon Mar 26 22:04:15 2012 from 169.254.0.1
[root@cmdctr ~]# cd /etc
[root@cmdctr etc]# sh ccnetworkconfig.sh


*** Please configure Network Settings ***

++++++++++++++++++++++++++++++++++++++++++++++++
+                                              +
+  Current values are shown within Parentheses  +
+       Press Enter to keep the current values   +
+                                              +
++++++++++++++++++++++++++++++++++++++++++++++++
Host Name (cmdctr) :CCPrimary
Command Center IP Address (192.168.100.3) :10.102.43.12
XEN Server IP Address (192.168.100.2) :10.102.43.220

Enter Appliance password :
Subnet Mask (255.255.255.0) :
Gateway (192.168.100.1) :10.102.43.1
DNS Server IP Address (127.0.0.1) :1.2.3.4
NTP Server IP Address () :10.102.1.1

Current Time Zone settings : Mon Mar 26 23:25:09 PDT 2012
Do you wish to change your Time Zone?
Enter y for yes :
```

You have an option to configure initial settings without connecting to the appliance console. You have to change the IP settings of your workstation or laptop to the default appliance subnet (192.168.100.X) and connect the workstation to the appliance by using an Ethernet cable. Connect the Ethernet cable to the first management port (from left to right,) numbered 0/1. At this point, you have an option to either run the configuration script or log on to the graphical user interface to complete the configuration.

To configure initial settings by using the graphical user interface

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY. The appliance is configured with the default IP address 192.168.100.3.
2. Log on to the appliance with the following credentials:
   - **Username**: root
   - **Password**: public
3. Logon to the Command Center client and apply the license file. For information on appliance licenses, see Command Center Appliance Licenses.
4. Under **Administration > Operations**, click **Setup Wizard**.
5. Follow the prompts and set the following parameter values to your local settings.
   - Hostname—Host name of the appliance. Change the default Hostname value. Default : cmdctr.
     Important: In an HA setup, make sure that the Hostname values of the primary and secondary appliances are unique. This is important to avoid host name resolution conflicts and ensure successful HA setup.
   - Command Center IP Address—IP address of the appliance. Default: 192.168.100.3. After initial configuration, you can access the appliance by typing this IP address in a web browser and specifying the port as 8443. For example: https://10.102.31.69:8443/
   - XEN Server IP Address—IP address of the XenServer. Default : 192.168.100.2.
   - Gateway—IP address of the router that forwards traffic out of the appliance's subnet. Default: 192.168.100.1
   - Netmask—Mask identifying the appliance's subnet. Default: 255.255.255.0

- DNS Server IP Address—IP address of the DNS server.
- NTP Server IP Address—IP address of the NTP server.
- Current Time zone Settings—Displays the time on the appliance. Provide the appropriate time zone.

6. Click **Finish**.

The appliance automatically restarts. You have now completed initial configuration of your Command Center appliance.

To configure initial setting using the configuration script

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY. The appliance is configured with the default IP address 192.168.100.3.
2. Log on to the appliance with the following credentials:
   - **Username**: root
   - **Password**: public
3. Run the Command Center appliance configuration script. At the shell prompt, type:
   sh /etc/ccnetworkconfig.sh
4. Follow the prompts and set the following parameter values to your local settings. The default values are shown within parentheses. Press Enter if you do not want to change the default value.
   - Hostname—Host name of the appliance. Change the default Hostname value. Default : cmdctr.
     Important: In an HA setup, ensure the Hostname values of the primary and secondary appliances are unique values. This is important to avoid host name resolution conflicts and ensure successful HA setup.
   - Command Center IP Address—IP address of the appliance. Default: 192.168.100.3. After initial configuration, you can access the appliance by typing this IP address in a Web browser and specifying the port as 8443. For example: https://10.102.31.69:8443/
   - XEN Server IP Address—IP address of the XenServer. Default : 192.168.100.2.
   - Enter Appliance Password—Type public as the appliance password.
   - Subnet Mask—Mask identifying the appliance's subnet. Default: 255.255.255.0
   - Gateway—IP address of the router that forwards traffic out of the appliance's subnet. Default: 192.168.100.1
   - DNS Server IP Address—IP address of the DNS server.
   - NTP Server IP Address—IP address of the NTP server.
   - Current Time zone Settings—Displays the time on the appliance. Provide the appropriate time zone.

   Note: In an HA setup, the primary and secondary appliances must have the same time stamps. This can be ensured by synchronizing both the appliances with the same NTP server and verifying that the synchronization between the appliances and NTP server is successful. This is important to ensure an accurate timeline for performance data in case of a failover.
5. When prompted to restart, select y.
6. Remove the Ethernet cable connected to the workstation or laptop. Now connect the Ethernet cable to the appliance to add the appliance to your subnet.

The appliance automatically restarts. You have now completed initial configuration of your Command Center appliance.

You can change the existing network and time zone settings of the appliance by running the Command Center appliance configuration script from the serial console.

To change the network settings by using the serial console

1. On a workstation or laptop, open a Telnet connection to the serial console of the appliance by using a Telnet client,

such as PuTTY.

2. Log on to the appliance by using the administrator credentials. In User Name and Password, type the administrator credentials. The defaults are root and public , respectively.
3. Run the Command Center appliance configuration script. At the shell prompt, type:
   sh /etc/ccnetworkconfig.sh
4. Follow the prompts and specify values for the following parameters. The default values are shown within parentheses after the parameter names. Press Enter if you do not want to change the default value.
   - Hostname—Host name of the appliance. Default : cmdctr.
     Important: In an HA setup, ensure the Hostname values of the primary and secondary appliances are unique values. This is important to avoid host name resolution conflicts and ensure successful HA setup.
   - Command Center IP Address—IP address of the appliance. Default: 192.168.100.3. After initial configuration, you can access the appliance by typing this IP address in a Web browser and specifying the port as 8443. For example: https://10.102.31.69:8443/
   - XEN Server IP Address—IP address of the XenServer. Default : 192.168.100.2.
   - Enter Appliance Password—Type public as the appliance password.
   - Subnet Mask—Mask identifying the appliance's subnet. Default: 255.255.255.0
   - Gateway—IP address of the router that forwards traffic out of the appliance's subnet. Default: 192.168.100.1
   - DNS Server IP Address—IP address of the DNS server.
   - NTP Server IP Address—IP address of the NTP server.
   - Current Time zone Settings—Displays the time on the appliance. Provide the appropriate time zone.

   Note: In an HA setup, the primary and secondary appliances must have the same time stamps. This can be ensured by synchronizing both the appliances with the same NTP server and verifying that the synchronization between the appliances and NTP server is successful. This is important to ensure an accurate timeline for performance data in case of a failover.
5. When prompted to restart, select y.
6. Remove the Ethernet cable connected to the workstation or laptop and connect it to the router to add the appliance into the network.

The appliance automatically restarts. You have now completed initial configuration of your Command Center appliance.

The default user account provides complete access to all features of the Citrix Command Center appliance. Citrix recommends changing the default password of the appliance. You can then change the password using the Change Password link provided in the Command Center interface.

To change the default password of the appliance

1. In a web browser, type the IP address of the Command Center appliance. For example: https://10.102.31.69:8443/
2. In User Name and Password, type the administrator credentials. The defaults are root and public , respectively.
3. Under **Administration > Security**, click **Change Password**.
4. Type the Current Password.
5. Type and re-type the new password.
6. Specify the password expiry value in **Password Expires In** field.
7. Click OK.

Command Center Appliances in a High Availability Pair

May 27, 2015

A high availability (HA) deployment of two Citrix® Command Center™ appliances can provide uninterrupted management of network devices. You configure one appliance as the primary node and the other as the secondary node. The primary node manages the network devices while the secondary node acts as a passive node. The secondary node becomes primary and takes over if the original primary node fails for any reason.

The primary node updates its health status at predefined intervals in a database table. Also, at predefined intervals, the secondary node checks the database for the status of the primary node. If a health check fails, the secondary node rechecks the health a predefined number of times, after which it determines that the primary node is not functioning normally. The secondary node then takes over as the primary (a process called failover). After a failover, the original secondary is the primary node. After the administrator corrects the problem on the original primary appliance and restarts it, the original primary appliance becomes the secondary node.

Important: In an HA setup, the database on the primary node must be completely in sync with the database on the secondary node. To maintain synchronization, MySQL two-way replication is configured as part of the HA setup.
This topic includes the following details:

- Prerequisites
- Configuring High Availability
- Removing Command Center Appliances from an HA Setup
- Performing a Force Failover in a High Availability Setup

A successful high availability setup depends on the following conditions:

- Both the primary and the secondary appliances should be operational and have the same build of the Command Center software.
- The primary and secondary appliances must have the same time stamps. This can be ensured by synchronizing both the appliances with the same NTP server and verifying that the synchronization between the appliances and NTP server is successful. This is important to ensure an accurate timeline for performance data in case of a failover.
- Both the primary and secondary appliances should have unique Hostname values to avoid host name resolution conflicts.
- Both the primary and secondary appliances should have the same login credentials for the root user account.

The appliance from which the configuration is initiated is designated as the primary node. Any data on the appliance designated as the secondary node is lost. During HA configuration, a number of actions, such as shutting down the server, backing up the database, and running replication commands on both databases, run in the background. The script may take from a few seconds to a few minutes to complete, depending on the size of the data that needs to be pushed from the primary appliance to the secondary appliance.

To configure Command Center appliances in high availability mode by using the graphical user interface

1. Logon to Command Center client and navigate to **Administration > Operations**.
2. Under **Operations**, click **Setup High Availability**.
3. Type the IP address of the secondary node and click **OK**.
   Note: The login credentials for the root user account on both appliances should be same.

To configure Command Center appliances in high availability mode using an SSH client

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance to be designated as the primary node. In User Name and Password, type the administrator credentials of the secondary node. The defaults are root and public, respectively.
3. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:
   sh configure_cc_ha.sh <SEC_IP> <USER_NAME>
4. When prompted, type the password.

Parameters for configuring Command Center appliances in an HA setup

SEC_IP

IP address of the secondary node.

USER_NAME

Authorized user name for the secondary node (Default is root.)

PASSWORD

Password for the secondary node (Default is public.)

You can remove Command Center appliances from an HA setup to run them as independent servers. This involves stopping the servers, stopping MySQL replication, and changing the configuration. Configuration is initiated from the primary node.

To remove Command Center appliances from an HA setup

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the primary node. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:
   sh break_cc_ha.sh <USER_NAME>
4. When prompted, type the password.

Parameters for removing a Command Center appliance from an HA setup

USER_NAME

Authorized user name for the primary node (Default is root.)

PASSWORD

Password for the primary node (Default is public.)

You might want to force a failover if, for example, you need to replace or upgrade the primary node. Force failover is always initiated from the primary node.

To perform a force failover by using graphical user interface

1. In a Web browser, type the IP address of the Command Center appliance. For example: https://10.102.31.69:8443/
2. Log on to the appliance to be designated as the primary node. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. In the Menu bar, click Administration. Under Operations, click Force Failover.
4. In the confirmation window, click **OK**.
   Note: After you confirm, the appliance is shutdown. You have to log on using the IP address of the secondary appliance. To view the status and other details, refer the log file under the logs/forcefailover_cc_ha.log directory.

To perform a force failover on a primary node in an HA setup

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance to be designated as the primary node. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:
   sh forcefailover_cc_ha.sh <USER_NAME>
4. When prompted, type the password.

Parameters for performing a force failover in an HA setup

USER_NAME

Authorized user name for the primary node (Default is root.)

Command Center Appliance Licenses

Dec 10, 2014

A Command Center appliance must be properly licensed before it can be deployed to manage and monitor Citrix application networking products. In case of an High Availability(HA) set up, both of the Command Center appliances must be properly licensed before you can start using the HA setup. All Command Center appliances are shipped with preinstalled default licenses. You can obtain a valid license (Evaluation or Retail) and upgrade the preinstalled license on the appliances to access the Command Center graphical user interface.

Evaluation licenses are used for evaluating new capabilities and when the evaluation period expires, obtain and upgrade the Retail license to access the Command Center graphical user interface.

Command Center appliances are shipped with preinstalled default licenses and the License Details window appears when you try to log on to the Command Center graphical user interface. This window provides the information you need for obtaining the licenses and upgrading the licenses on the appliances.

To obtain appliance licences when the appliance has SMTP connectivity

1. Log on to Command Center interface using the default credentials (root/public).
2. Under the I do not have Command Center Appliance licenses option, click the Click here link.
3. In the Request License window, enter the name or IP address of your mail server.
4. In the From field, type the email address at which you want to receive the license.
5. In the To field, type the email address of your Citrix contact.
6. If your mail server requires authentication, select the Mail server requires authentication option and type the required user name and password.
   Note: Do not modify the MAC address details displayed in the Message text box. Be sure to use the same MAC address details when you send a request for license generation.
7. Click OK. A confirmation message reports that your request has successfully been submitted.

After you receive the license file(s) from Citrix, you can upgrade the license(s) and access the Command Center graphical user interface.

To obtain appliance licences when the appliance does not have SMTP connectivity

1. Log on to Command Center interface using the default credentials (root/public).
2. Under the I do not have Command Center Appliance licenses option, click the Click here link.
3. Note the MAC address details displayed in the Message text box in the Request License window.
   Note: Do not modify the MAC address details displayed in the Message text box. Be sure to use the same MAC address details when you send a request for license generation.
4. Mail these details to your Citrix contact from a system with the SMTP connectivity.

After you receive the license file(s) from Citrix, you can upgrade the license(s) and access the Command Center graphical user interface.

You can upgrade the Command Center appliance licenses from the License Details window. The License Details window

appears when you try to log on to Command Center graphical user interface of an appliance that is running on a preinstalled default license or an expired Evaluation license. After you upgrade the license on the appliance, you can log on to access the Command Center graphical user interface.

To upgrade appliance license

Follow this procedure to upgrade the appliance from a preinstalled default license to an Evaluation license or a Retail license and also to upgrade an expired Evaluation license to a Retail license.

1. In the License Details window select the I have Command Center Appliance Licenses option.
2. Select the license file that you want to upload.
   Note: Each license file is unique for a specific Command Center appliance and must be installed only on that appliance. To ensure that you upload the specific license file, verify the MAC address in the license file with the MAC addresses displayed for the server in License Details window.
3. Click OK. A confirmation message reports that the license is successfully upgraded on Command Center appliance. You can now log on to access the Command Center graphical user interface.

To upgrade Command Center appliance license from an Evaluation license to a Retail license

Follow this procedure to upgrade the Command Center appliance from an Evaluation license to a Retail license. In case the Evaluation license has expired, follow the previous procedure.

1. Obtain the Retail license for the Command Center appliance from Citrix.
2. Logon to the Command Center appliance and copy the license file in the /opt/Citrix/Citrix_Command_Center/flexlm/citrix/licensing/myfiles directory by using SFTP or FTP.
3. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
4. Log on to the appliance. In User Name and Password, type the administrator credentials. The defaults are `root` and `public`, respectively.
5. Change directory to /opt/Citrix/Citrix_Command_Center. Then, at shell prompt, type: `./bin/upgradeCtxLicense.sh`
   Note: Verify the permission before you execute the script.
   The license is successfully upgraded on Command Center appliance.

Upgrading Command Center

Apr 22, 2015

You can upgrade to a later release on a standalone Command Center appliance or an HA pair. To upgrade a standalone node, first stop Command Center, upgrade the software, and then start Command Center. To upgrade an HA pair, run a script available in the /opt/Citrix/Citrix_Command_Center/bin directory. Before running the script, make sure that you know the path to the service pack for upgrading the appliance.

Note: You cannot downgrade a Command Center appliance.

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Shut down the appliance. At the shell prompt, type: `./etc/init.d/NSCCService stop`
4. Download the build file (SP_FILE) to the appliance and change the mode of the SP_FILE to executable. At the shell prompt, type: `chmod 777 ./<SP_FILE>`
5. Upgrade the appliance. At the shell prompt, type: `./<SP_FILE> -i silent`
6. Restart the appliance. At the shell prompt type: `./etc/init.d/NSCCService start`

Messages are not displayed on the console when the silent option is used.

SP_FILE

Complete path to the service pack file.

USER_NAME

Authorized user name for the primary node (Default is root.)

1. On a workstation or laptop, open an SSH connection to the primary node by using an SSH client, such as PuTTY.
2. Log on to the primary node. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:
   `sh upgrade.sh <SP_FILE> <USER_NAME>`

   The `sh upgrade.sh <SP_FILE> <USER_NAME>` command upgrades both the primary and secondary appliances.
4. When prompted, type the password.

Performing Backup and Restore Operations

May 27, 2015

You can back up Citrix Command Center appliance data and configurations either periodically to keep historical data or when upgrading Command Center software. Citrix recommends storing a copy of the backup on external storage media which can later be used to restore the backed up data.

This topic includes the following details:

You can schedule or perform an immediate backup of the database on the Command Center appliance. By default, backup is scheduled for midnight Saturday. The default directory for the backup is /var/lib/mysql/backup. Citrix recommends storing a copy of the backup on external storage media.

To backup a database by using the graphical user interface

1. In a Web browser, type the IP address of the Command Center appliance. For example: https://10.102.31.69:8443/
2. In **User Name** and **Password**, type the administrator credentials. The defaults are root and public, respectively.
3. In the Menu bar, click **Administration**.
4. Under **Tools**, click **Backup**.
5. Do one of the following:
   - To schedule a backup, click **Schedule Backup**, and perform steps 6 and 7.
   - To start a backup immediately, click **OK**. After the backup is completed, the complete path to the backup file name is displayed.
6. Under **Schedule Backup**, use the following set of options to define your backup schedule:
   - **Day(s) of Week**—Specify the days on which you want to schedule the backup process. To select more than one day, hold down the Ctrl key while clicking the days.
   - **Day(s) of month**— Select this option to schedule a backup during a range of dates. For example, if you want to schedule a backup every day between 10th and 20th of every month, type 10-20.
   - **Daily**—Select this option to run the backup process every day.
   - **Scheduled Hours**—Specify the time(s) at which to schedule the backup process, as hours in a 24-hour day. Use commas to separate multiple hours (for example, 12, 2, 4).
7. Click **OK**. The schedule is saved.

To backup a database by using the command line

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance, using the administrator credentials. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Stop the Command Center software. At the shell prompt, type:

   ./etc/init.d/NSCCService stop
4. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:

sh BackupDB.sh

5. Start the Command Center software. At the shell prompt, type:

   ./etc/init.d/NSCCService start

The backup process creates a directory whose name begins with BackUpMMDD_XXX. By default, the directory is a subdirectory of the /var/lib/mysql/backup directory. The directory contains a number of .data files. The restore operation may several minutes to complete. Stop the Command Center software before restoring the data. After the restore is complete, restart the Command Center software.
Caution: When restoring the data, the current data on the appliance is deleted.

To restore the data

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance, using the administrator credentials. In User Name and Password, type the administrator credentials. The defaults are root and public, respectively.
3. Stop the Command Center software. At the shell prompt, type:

   ./etc/init.d/NSCCService stop
4. Change directory to /opt/Citrix/Citrix_Command_Center/bin. Then, at the shell prompt, type:

   sh RestoreDB.sh <path to the directoryname in which to restore data>
5. Start the Command Center software. At the shell prompt, type:

   ./etc/init.d/NSCCService start

Updated: 2015-05-28

A backup of the database is stored by default on the Command Center appliance. You can also store a backup of the database on an external appliance and generate reports from that database. Before you can generate reports, you must install MySQL software on the external appliance, create a database, restore the backed up files, and install the same version of Command Center software that is installed on the Command Center appliance.

Prerequisites

Before you restore the backed up files on the external appliance, verify the following:

1. You are running a supported version of the Linux operating system. The following versions are supported:
   - Red Hat Enterprise Linux AS 4.0
   - Red Hat Enterprise Linux ES 4.0 and 5.1
   - Red Hat Enterprise Linux ES 5.1 64-bit edition
   - CentOS 4.0 and 5.1
2. A minimum of 2GB RAM is available.

To restore the data on an external appliance

1. Install MySQL 5.1.48 on the external appliance. At the shell prompt, type the following commands:
   rpm -i MySQL-server-enterprise-5.1.48-1.rhel5.x86_64.rpm

   rpm – i MySQL-client-enterprise-5.1.48-1.rhel5.x86_64.rpm

This operation may take a few minutes.

2. Set the administrator password. At the shell prompt, type:
   /usr/bin/mysqladmin –uroot password <mypassword>

   where <mypassword> is the new password.

3. Connect to the MySQL client and create a database named cmdctr. At the prompt, type:
   create database cmdctr;

4. Copy the backed up files under /var/lib/mysql/backup/<directoryname> on the Command Center appliance to the external appliance by using a secure file transfer utility, such as SFTP.
5. Restore each file on the external appliance. At the shell prompt, type:
   gunzip < $[<filename.gz file] | /usr/bin/mysql -u root –p[PASSWORD] cmdctr

   Repeat this command for each of the other files that are backed up.

6. Install Command Center on the external appliance. The version of Command Center software should be the same version that is running on the Command Center appliance. When prompted to start Command Center, select No.
7. Copy the configuration folder in the backed up files to the directory in which Command Center is installed on the external appliance. The default directory is /opt/Citrix/Citrix_Command_Center. Copying the folder ensures that your settings, such as alert filters, event filters, threshold, event severity, failover and security settings, on the Command Center appliance are available on the external appliance.
8. Start the Command Center software. The restore is now complete.

Example

The following commands are an example of performing steps 1–5 of the above procedure. For information about installing Command Center, see Installing the Command Center Server on Linux.

```
#rpm -i MySQL-server-enterprise-5.1.48-1.rhel5.x86_64.rpm
#rpm –i MySQL-client-enterprise-5.1.48-1.rhel5.x86_64.rpm
#/usr/bin/mysqladmin –uroot password pass1
#mysql –uroot –ppass1
mysql> create database cmdctr;
mysql> exit;
# sftp root@10.102.31.69
Connecting to 10.102.31.69...
root@10.102.31.69's password:
sftp> cd /var/lib/mysql/backup/CCBackUp_JUN30_2011_11_35
sftp> mput *.gz
sftp> bye
# gunzip< file1.gz> | /usr/bin/mysql -u root –ppass1cmdctr
# gunzip< file2.gz> | /usr/bin/mysql -u root –ppass1cmdctr
…
…
…
```

Installing Command Center Software

May 28, 2015

You can install the Command Center server on either the Windows or Linux platform. You can download the installation package for both Windows and Linux from the Citrix portal Web site: http://mycitrix.com.

There are two types of server installation: Evaluation and Typical. The installation type is specified at the start of the installation process.

Evaluation installation type enables you to quickly install the Command Center server by installing the pre-packaged PostgreSQL database and by using predefined options. Typical installation type provides more flexibility and enables you to connect to an external database; this is recommended for use in production environment. For more information on the installation types and installation steps, see

- Installing the Command Center Server on Windows
- Installing the Command Center Server on Linux

You can also configure Command Center in a distributed multi-tier architecture by installing Command Center agents that manage and monitor the Citrix devices. This architecture provides scalability and reduces the load on the server. For more information, see

- Installing Command Center Agents on Windows
- Installing Command Center Agents on Linux

The following Citrix products are supported by Command Center:

- NetScaler Standard, Enterprise and Platinum editions
- NetScaler Gateway
- NetScaler AppFirewall
- ByteMobile Traffic Director
- CloudBridge

You do not need a license to use Command Center software.

In this section:

- Before You Begin
- Installing the Command Center Server on Windows
- Installing the Command Center Server as a Windows Service
- Installing the Command Center Server on Linux
- Installing the Command Center Server as a Linux Startup Service
- Setting the Command Center Communication Mode
- Installing the Command Center Server in High Availability Mode
- Installing Certificates for Secure Communication

Updated: 2014-04-29

The following versions of Citrix Products are supported by Command Center.

- NetScaler: 7.0 and later
  Note: The Entity Monitoring feature is supported on NetScaler versions 8.0 and later.
- Repeater and Branch Repeater: 4.5.0 and later
- Branch Repeater with Windows Server (2003 and 2008): 2.0.0 or later
- Branch Repeater VPX: 5.6.0 or later
- NetScaler SDX
- ByteMobile Traffic Director

Before You Begin

Oct 21, 2015

Before you install your Command Center server, make sure that you have the minimum system requirements, such as hardware requirements, operating system requirements, and database requirements. You also need to ensure that the database settings are specified according to Command Center requirements.

This topic includes the following details:

Updated: 2014-10-17

The following table summarizes the minimum hardware requirements for the Command Center servers.

Component	Requirement
Processor type	Pentium 4
Processor speed	1.2 gigahertz (GHz)
Memory	1 gigabyte (GB) RAM
Hard disk space	20 GB

The performance management module plots graphs across three tables. By Default, the first table maintains data for 14 days, with a polling interval of 5 minutes. The second table maintains data from one poll per hour, for 30 days. The third table maintains data from one poll per 24 hours, for 365 days. At the beginning of the 15th day, the data in the first table is overwritten with new data. The data in the other two tables is overwritten on the 31st day and the 366th day, respectively. The following table lists the disk space requirements for using the performance management module in a few sample configurations.

No. of Counters	Polling Interval	No. of Devices	Disk Space Required	Unit

No. of Counters	Polling Interval	No. of Devices	Disk Space Required	Unit
100	5 minutes	10	488	MB
300	5 minutes	10	1.4	GB
500	5 minutes	10	2.4	GB
1000	5 minutes	25	11.9	GB
5000	5 minutes	50	119.1	GB
10000	2.5 minutes	50	426	GB

Updated: 2015-05-13

The following table lists the operating system requirements for installing Command Center.

Operating System	Version
Windows	• Microsoft® Windows® 2012 • Microsoft® Windows® 2012 R2 64 bit • Microsoft® Windows® 2008 • Microsoft® Windows® 2008 R2 64 bit
Linux	• CentOS 6.2 32 bit • CentOS 6.2 64 bit • CentOS 6.5 32 bit • CentOS 6.5 64 bit • Red Hat Enterprise Linux 6.2 64 bit • Red Hat Enterprise Linux 6.4 32 bit • Red Hat Enterprise Linux 6.4 64 bit

Updated: 2015-04-03

Command Center supports the following databases and their versions.

Database Type	Version
MySQL	5.1.x with InnoDB storage engine

Database Type	Version
	5.6.x with InnoDB storage engine
Oracle	10g/11g
Microsoft SQL Server	2008, 2008 R2, 2012, 2012 R2, and 2014

Note:

- Before installing Command Center to work with an MS SQL Server database, ensure that you select the SQL Server Authentication mode when installing the database. The Windows Authentication mode is not supported in Command Center.
- MSSQL2005 is not supported if you are installing CC 5.2 build 43.19. However, if you are upgrading to the CC 5.2 build 43.19 service pack build, MSSQL2005 is supported.

Updated: 2013-07-22

The following are the prerequisites for installing Command Center on Linux.

You must ensure that the hostname -i command on the system on which Command Center is installed resolves the actual IP address and not the loopback IP address (127.0.0.1). If the hostname -i command does not resolve the actual IP address, do the following:

1. Log on as root, and change to /etc directory.
2. Open the host file using a vi editor.
3. Update the line 127.0.0.1 localhost with the actual IP address, for example 10.102.41.10: 10.102.41.10 HostName
4. For Linux ES 5.1, add the following line: 10.102.41.10 localhost

Updated: 2014-08-04

The following table provides the minimum software recommendations for running the Command Center clients.

Browser	Version
Internet Explorer	IE 8, 9,10 and 11
Firefox	3.6.25 and above
Chrome	Latest
Safari	5.1.3 and above

This section covers the various ports that Command Center uses. The Command Center client and server use either HTTP or HTTPS to communicate. The HTTPS communication mode is enabled by default when you install the Command Center server.

The following table lists the ports used by the Command Center client and server to communicate with each other.

Purpose	TCP Ports
HTTPS communication between Command Center client and server.	8443
HTTP communication between Command Center client and server.	9090
Communication between Command Center High Availability (HA) servers.	6011, 2014, and 1099

The following table lists the ports used by the Citrix Command Center server to communicate with the Citrix NetScaler, NetScaler SDX, and Citrix CloudBridge.

Purpose	Port
SNMP communication between the Citrix Command Center server and the Citrix NetScaler system and Citrix CloudBridge.	161 (UDP port)
Configuration of SNMP traps between the Command Center server and the Citrix NetScaler system.	162 (UDP port)
SSH and SFTP communication between the Command Center server and the Citrix NetScaler system.	22 (TCP port)
HTTPS and HTTP communication between the Command Center server and Citrix CloudBridge.	443 and 80 (TCP ports)
HTTPS communication between the Command Center server and NetScaler SDX.	443 (TCP port)

Note: In the Command Center client, by using the Invoke Configuration Utility option, you can access the Citrix NetScaler utilities, such as the configuration utility and dashboard. To access the configuration utility and dashboard from Command Center, you must ensure that these are independently accessible from the client machine.

The following table lists the ports used for communication between the Command Center server and the Command Center agents.

Purpose	Port
Communication between the Citrix Command Center server and the Citrix Command Center agents. Note: This port should be opened on the server as well as on the agents.	1099
Remote Method Invocation (RMI) lookup. Note: This port should be opened on the server as well as on the agents.	6011
HTTPS communication between the Command Center server and the agents.	8443
HTTP communication between the Command Center server and the agents.	9090

Updated: 2014-12-23

Command Center supports the following databases:

- MySQL 5.1.x with InnoDB storage engine. For instructions on installation, see http://dev.mysql.com/doc/
- MS SQL Server 2005 and 2008. For instructions on installation, see http://msdn.microsoft.com/en-us/library/ms143516(SQL.90).aspx
  Important:
  - Before installing Command Center to work with an MS SQL Server database, ensure that you select the SQL Server Authentication mode when installing the database. The Windows Authentication mode is not supported in Command Center.
  - Also, make sure to enable SQL Server Authentication while installing the database.
- Oracle 10g and 11g. For instructions on installation, see http://docs.oracle.com/cd/B19306_01/nav/portal_2.html

After installing the database, you must configure the database user permissions and database parameters.

Database Parameters

The following table lists the parameters that you need to specify for the database settings.

Parameter	Description
Database	MySQL, Oracle, or MS SQL Server.
Host Name	IP address of the server or the server name where the database is hosted.
Port	Port number of the server where the database is hosted. The default port for MySQL is 3306, for Oracle is 1521, and for MS SQL Server is 1433.

Parameter	Description
Database Name	Name of the database.
SID	Name of the Oracle database.
User Name	Database logon user name. The default user for MySQL is root, for Oracle it is system, and for SQL Server it is sa. However, the administrator can create users and define the required permissions. For information on the user permissions, see the section "Database User Permissions."
Password	Password assigned by the database administrator.

Note: Before performing a complete installation of a new version of Command Center, you must check for and uninstall earlier versions of Command Center.

Database User Permissions

After you have created the Command Center database and the database user, you need to grant the required permissions as described in the following table.

Database	User Permissions
Oracle	GRANT CREATE SESSION to DatabaseUserName; GRANT CREATE TABLE to DatabaseUserName; GRANT ALTER DATABASE to DatabaseUserName; GRANT UNLIMITED TABLESPACE to DatabaseUserName; GRANT CREATE TRIGGER to DatabaseUserName; GRANT CREATE SEQUENCE to DatabaseUserName;
MS SQL	In the MS SQL Server Management tool, you need to set the following permissions: 1. Click Security > Logins, and then double-click DatabaseUserName. 2. In General, set Default database as the Command Center database. 3. In User Mapping, under Users mapped to this login, select the default database, and under Database role membership for, select the db_owner role membership. Note that the public role is selected by default.
MySQL	GRANT ALL ON DatabaseName.* TO DatabaseUserName@ CommandCenterIPAddress identified by 'DatabaseUserPassword'; GRANT FILE ON *.* TO DatabaseUserName@ *CommandCenterIPAddress* identified by

Database	'DatabaseUserPassword'; **User Permissions** GRANT SELECT, UPDATE on 'mysql'.'user' TO 'DatabaseUserName'@'CommandCenterIPAddress'; GRANT RELOAD, PROCESS ON *.* TO DatabaseUserName@CommandCenterIPAddress;

Installing the Command Center Server on Windows

May 09, 2012

To install the Command Center server, download the installation package from the Citrix portal: http://mycitrix.com. The installation package is an executable file with the following naming convention:

CC_Setup_ReleaseNumber_BuildNumber.exe

Example:

There are two types of server installation: Evaluation and Typical. The installation type is specified at the start of the installation process.

Evaluation installation type enables you to quickly install the Command Center server by installing the pre-packaged PostgreSQL database and by using predefined defaults, such as the HTTPS security mode. Although this installation type provides all functionality of Command Center, it is not supported in production environment. Citrix recommends you use the Evaluation installation type only for evaluation purposes.

Typical installation type provides more flexibility and enables you to connect to an external database and specify the security mode you want to use. This installation type provides all Command Center functionality and Citrix recommends you use this in production environment.

Note: You can also configure Command Center in a distributed multi-tier architecture by installing Command Center agents that manage and monitor the Citrix devices. For more information, see Installing Command Center Agents on Windows.

To install the Command Center server on Windows

1. Run the setup file and follow the instructions on the screen.
2. On the Choose Installation Type screen, select either Evaluation or Typical.
3. If you have selected Evaluation, click Next, and then click Install. This installs the packaged Postgre SQL database, and installs Command Center in the HTTPS security mode.
   If you have selected Typical, perform the following steps:
   1. On the Database Settings screen, enter the values for the database parameters, and then click Test Connection. After the connection to the database is successful, click Next
      Note: For information on the database parameters and their values, see the table in section Database Settings.
   2. Under Security Settings, select either HTTP or HTTPS.
   3. Click Next, and then click Install.

   Note: After Command Center successfully installs, the summary screen appears with a brief note about getting started with Command Center.
4. On the summary screen, click Done.
   Command Center starts and a command prompt windows appears displaying the status of the startup process. After the Command Center server starts successfully, the command prompt window displays the URL to access the Command Center server from a Web browser.

Note: The Command Center service is installed and started automatically and Command Center server can be accessed from the web browser.

In this section:

- Installing Command Center Agents on Windows
- Uninstalling the Command Center Server from Windows

Installing Command Center Agents on Windows

Updated: 2014-12-12

Consider a scenario where you use 300 NetScaler VPX devices in the development and testing stages in your production environment. To manage and monitor such large number of devices, you can set up Command Center in a distributed multi-tier architecture by configuring Command Center agents to manage and monitor the Citrix devices.

This architecture reduces the load on the Command Center server by distributing the load across the different agents. In a distributed multi-tier setup, the Command Center server performs operations, such tasks as discovery, trap processing, monitoring entities and syslog messages, and configuration. The agents are used for monitoring entities and syslog messages, for certificate management, and for polling and collecting data used for performance monitoring, such as CPU usage, resource utilization, and IP bytes transmitted. The Command Center server and the agents are connected to the same database.

The number of agents to install depends on the usage of virtual servers, services and service groups to be monitored, reporting counters to be polled, and the syslog messages received by the Command Center server.

You can also monitor the state of the agents from your Command Center client. For example, when an agent connects to the Command Center server, an event of severity clear is generate and, if an agent connected to the server goes down, an event of severity critical is generated. This alerts the user to take appropriate action.

To install the Command Center agents, use the Command Center installation package available at the Citrix portal: http://mycitrix.com. The installation package is an executable file with the following naming convention:

CC_Setup_ReleaseNumber_BuildNumber.exe

Note: You cannot install the Command Center server and the agent on the same system. Also, you cannot install more than one agent on a system.

To install Command Center agents on Windows

1. Install and start the Command Center server on a system.
2. On the system where you want to install the agent, run the setup file and follow the instructions on the screen.
3. On the installation-type screen, select Agent Setup, and then click Next.
4. Under Agent Setup, in Server IP address, type the IP address of your Command Center server, and then click Test Connection.
5. After the connection is successfully tested, click Next, and then click Install.

Uninstalling the Command Center Server from Windows

Uninstall the Command Center server by using the Add or Remove Programs option in Windows or from the Windows Start menu. If you need to perform a complete installation of a new release of Command Center server, you must uninstall the

older version before carrying out the complete installation.

Note: If you have a Command Center service pack installed, you must uninstall the service pack before you can uninstall the previous version of Command Center. You must also uninstall the Command Center service on Windows.

To uninstall the Command Center server

To uninstall the Command Center server, do one of the following:

- From the Windows Start menu: On the Windows desktop, click Start > Programs > Citrix Command Center > Uninstall. Follow the steps in the wizard to uninstall the software.
- Using Add or Remove Programs:
  1. Click Start > Settings > Control Panel. The Control Panel screen appears.
  2. Double-click Add or Remove programs. The Add or Remove Programs screen appears.
  3. Select the Citrix Command Center entry from the Currently installed programs: list and click Remove. Follow the steps in the wizard to uninstall the software.

Note: Uninstalling Command Center removes only the user-created files and folders; you must manually delete the database.

Installing the Command Center Server as a Windows Service

May 27, 2015

To use Command Center server as a Windows service, refer the related tasks:

- Installing the Service
- Running the Command Center Server as a Windows Service
- Stopping the Command Center Server from Running as a Service
- Uninstalling the Service

Installing the Service

To enable Command Center to automatically start whenever the server on which Command Center is installed restarts, you must install the service.

To install Command Center as a Windows service

1. At a command prompt, change the current working directory: cd CC_Home\bin
2. Run the batch file: InstallCCAsService.bat
   Note: This version of Command Center does not support the NSCCService -install and NSCCService -uninstall options.

Running the Command Center Server as a Windows Service

The following procedure describes how to start the Command Center server as a Windows service.

To run the Command Center server as a service

1. Click Start > Settings > Control Panel. The Control Panel screen appears.
2. Double-click Administrative Tools. The Administrative Tools screen appears.
3. Double-click Services. The Services screen of the Microsoft Management Console appears.
4. To run the server as a service, right-click Citrix Command Center and click Start.
5. To stop the server, right-click Citrix Command Center and click Stop.
   Note: Before you start the Command Center server as a service, you must start Command Center in the standalone mode to invoke the End User License Agreement (EULA) signatures.

Stopping the Command Center Server Running as a Service

To upgrade the software or to migrate from the current database to another database, you must stop the Command Center server that is running as a Windows service.

To stop the Command Center server running as a service

1. Click Start > Settings > Control Panel. The Control Panel appears.
2. Double-click Administrative Tools. The Administrative Tools pane appears.
3. Double-click Services. The Services screen of the Microsoft Management Console appears.
4. To stop the server, right-click Citrix Command Center and click Stop.

Uninstalling the Service

The following procedure describes the steps to uninstall the Command Center service.

To uninstall the Command Center service

1. At a command prompt, change the current working directory: cd CC_Home\bin
2. Run the batch file: UninstallCCAsService.bat
   Note: The Command Center Windows service is automatically uninstalled when you uninstall the Command Center server as described in Uninstalling the Command Center Server from Windows.

Installing the Command Center Server on Linux

May 27, 2015

To install the Command Center server on Linux, download the installation package from the Citrix portal: http://mycitrix.com. The installation package is a binary file with the following naming convention:

CC_Setup_ReleaseNumber_BuildNumber.bin

Example:

There are two types of server installation: Evaluation and Typical. The installation type is specified at the start of the installation process.

Evaluation installation type enables you to quickly install the Command Center server by installing the pre-packaged PostgreSQL database and by using predefined defaults, such as the HTTPS security mode. Although this installation type provides all functionality of Command Center, it is not supported in production environment. Citrix recommends you use the Evaluation installation type only for evaluation purposes.

Typical installation type provides more flexibility and enables you to connect to an external database and specify the security mode you want to use. This installation type provides all Command Center functionality and Citrix recommends you use this in production environment.

Note: You can also configure Command Center in a distributed multi-tier architecture by installing Command Center agents that manage and monitor the Citrix devices. For more information, see Installing Command Center Agents on Linux
You can install the Command Center server on Linux using either the installation wizard or the CLI.

To install the Command Center server by using the installation wizard

1. Run the setup file and follow the instructions on the screen. To run the setup file, at the Linux terminal window, type the following and press Enter.
   - For a 32-bit kernel, type ./CC_Setup_ReleaseNumber_BuildNumber.bin
   - For a 64-bit kernel, type ./CC_Setup64_ReleaseNumber_BuildNumber.bin

   Note: The commands listed above are applicable only when you install Command Center on Linux.
   Example:

   - 32-bit kernel: ./CC_SP_5.2_42_7.bin
   - 64-bit kernel: ./CC_SP64_5.2_42_7.bin
2. On the installation type screen, select either Evaluation or Typical.
3. If you have selected Evaluation, click Next, and then click Install. This installs the packaged Postgre SQL database, and installs Command Center in the HTTPS security mode.
   If you have selected Typical, perform the following steps:

   1. On the database settings screen, under Database Settings, enter the values for the database parameters, and then click Test Connection. After the connection to the database is successful, click Next
      Note: For information on the database parameters and their values, see the table in the section Database Settings.
   2. Under Security Settings, select either HTTP or HTTPS.
   3. Click Next, and then click Install.

   Note: After Command Center is successfully installed, the summary screen appears with a brief note about getting started with Command Center.

4. On the summary screen, click Done..
   Note: The Command Center service is installed and started automatically and Command Center can be accessed from the web browser.

To install the Command Center Server from the command line

1. At a command prompt, log on as root and type the following:
   ./CC_Setup_ReleaseNumber_Build Number.bin -i console

   Example:

   Note: Specifying the -i console option runs the setup file from the command line.
   The Installation Wizard starts and displays a set of numerical options.
2. To continue with the installation, follow the instructions on the screen.
3. To accept the license agreement, type 1 and press Enter, and then type 0 and press Enter to confirm.
4. When prompted, specify the complete path where you want to install the server, and then press Enter.
5. Enter one of the installation type options - Type1 for Evaluation or 2 for Typical.
   Note: For information about installing Command Center agents, see Installing Command Center Agents on Linux.
6. If you have typed 1 for Evaluation, to confirm and move to the next step, type 0 and press Enter, and then type 1 and press Enter. The packaged database and security mode details appear on the screen. Type 1 and press Enter to proceed with the installation.
   If you have typed 2 for Typical, perform the following steps:

   1. Enter one of the following database options - 1 for MYSQL, 2 for Oracle, or 3 for MS SQL.
   2. Enter the values for the following database parameters: hostname, port number, database name, username, and password.
      Note: For information on the database parameters and their values, see the table in section "Database Settings."
   3. Enter the communication mode you want to use. Type 1 for HTTP or 2 for HTTPS.
   4. View the Pre-Installation Summary and press Enter to proceed.

   After Command Center is successfully installed, the summary screen appears with a brief note about getting started with Command Center.

   Note: The Command Center service is installed and started automatically and Command Center can be accessed from the web browser.

This topic includes the following details:

- Installing Command Center Agents on Linux
- Uninstalling the Command Center Server from Linux

Installing Command Center Agents on Linux

Consider a scenario where you use 300 NetScaler VPX devices in the development and testing stages in your production environment. To manage and monitor such large number of devices, you can now set up Command Center in a distributed multi-tier architecture by configuring Command Center agents to manage and monitor the Citrix devices.

This architecture reduces the load on the Command Center server by distributing the load across the different agents. In a distributed multi-tier setup, the Command Center server performs operations, such as discovery, trap processing, and configuration using tasks. The agents are used for polling and collecting data used for performance monitoring, such as CPU usage, resource utilization, and IP bytes transmitted, and for certificate management. The Command Center server and

the agents are connected to the same database.

After the agents are installed and connected to the Command Center server, you can view the agent details on the Administration tab from the Command Center client. You can activate the agents from the client, and then assign devices to the agent to manage. For more information, see Setting Up Command Center Agents.

You can also monitor the state of the agents from your Command Center client. For example, when an agent connects to the Command Center server, an event with severity as clear is raised. And, when an agent connected to the server is down, an event with severity as critical is raised. This allows the user to take appropriate action.

To install the Command Center agents, use the Command Center installation package available at the Citrix portal: http://mycitrix.com. The installation package is an binary file with the following naming convention:

CC_Setup_ReleaseNumber_BuildNumber.bin

Example:

Note: You cannot install the Command Center server and the agent on the same system. Also, you cannot install more than one agent on a system.

To install Command Center agents on Linux

1. Install and start the Command Center server on a system.
2. On the system where you want to install the agent, run the setup file either in graphical mode or CLI mode, and then follow the instructions on the screen.
3. On the installation type screen, select Agent Setup. If you are using the CLI mode, under Choose Installation Type, type 3 for Agent Setup, and then press Enter.
4. In Server IP address, type the IP address of your Command Center server, and then test the connection. If you are using the CLI mode, enter the server IP address, type 1, and then press Enter to test the connection.
5. After the connection is successfully tested, follow the instructions on the screen to install the agent.

   Note: The Command Center Agent as a service is installed automatically, but you have to start the service manually.

Uninstalling the Command Center Server from Linux

This section describes the procedure to uninstall the Command Center server and service packs, if any. It also describes the procedure to uninstall Command Center configured to run as a service.

To uninstall the Command Center server

1. Stop the Command Center server.
2. At a command prompt, navigate to the bin subdirectory of the CC_Home directory.
3. Run the reinitialize_nms.sh shell script. This deletes the database tables created by the Command Center server.
4. Navigate to the CC_Home/_Citrix Command Center_installation directory and run Uninstall.bin file. Follow the steps in the wizard to uninstall.
   Note: Uninstalling Command Center removes only the user-created files and folders; you must manually delete the database.

Installing the Command Center Server as a Linux Startup Service

Jan 06, 2017

To use the Command Center server as a Linux Startup service, perform the following tasks:

- Installing the Service
- Running the Command Center Server as a Linux Service
- Stopping the Command Center Server from Running as a Service
- Uninstalling the Service

Installing the Service

You must install the Command Center service to start the Command Center server as a Linux service.

To install the Linux service

Use the chkconfig command to configure the Command Center server as service: **chkconfig -add NSCCService**

Running the Command Center Server as a Linux Service

You can manually run Command Center as a service, or you can set Command Center to start as a service when the system is restarted.

To run the Command Center server as a service

Use the following command to start Command Center as a service: /etc/init.d/NSCCService start

To automatically start Command Center as a service when the computer is restarted

1. Run the following command: /usr/sbin/ntsysv
2. In the screen that appears, select NSCCService.

Running the Command Center Agent as a Linux Service

You can manually run Command Center Agent as a service, or you can set Command Center Agent to start as a service when the system is restarted.

To run the Command Center server as a service

Use the following command to start Command Center as a service: /etc/init.d/CCAgentService start

To automatically start Command Center Agent as a service when the computer is restarted

1. Run the following command: /usr/sbin/ntsysv
2. In the screen that appears, select CCAgentService.

Stopping the Command Center Server from Running as a Service

To upgrade the software or to migrate from the current database to another database, you must stop the Command Center server that is running as a Linux service.

To stop the Command Center server from running as a service

Run the following command: /etc/init.d/NSCCService stop

Uninstalling the Service

The following procedure describes the steps to uninstall the Command Center service.

To uninstall the Linux startup service

1. At a command prompt, type the following to uninstall the Linux Startup service: chkconfig -del NSCCService
2. Run the following command: rm -rf /etc/init.d/NSCCService The Command Center Linux service is automatically uninstalled when you uninstall the Command Center server as described in Uninstalling the Command Center Server from Linux.

Setting the Command Center Communication Mode

Dec 23, 2009

By default, Command Center runs on HTTPS mode. You can change the communication mode from HTTPS to HTTP or HTTP to HTTPS.

To set communication mode to HTTP or HTTPS

1. At a command prompt, navigate to the bin directory of the CC_Home directory.
2. Do one of the following:
   - If HTTPS was chosen as the communication mode, type: server_mode.bat https
   - If HTTP was chosen as the communication mode, type: server_mode.bat http

Installing the Command Center Server in High Availability Mode

Mar 20, 2010

You can configure two Command Center servers to work as a high availability (HA) pair by configuring a server as primary and the other server as secondary. HA pair mode of operation allows you to ensure uninterrupted management of network devices by allowing the secondary Command Center server to take over in case the primary server fails, terminates, or shuts down.

Note: Both the primary and secondary servers should be in same time zone or with the same time settings. This is to ensure an accurate timeline for performance data in case of a failover.

To set up Command Center to work in high availability mode

1. Install Command Center on the server that you want to use as the primary HA server as described in Installing the Command Center Server on Windows or Installing the Command Center Server on Linux and connect to your database.
2. Start the Command Center server.
3. Install Command Center on the server that you want to use as the secondary HA server connecting to the same database to which the primary HA server is connected.
4. Start the Command Center server.
   Important: Citrix recommends you to start the server which you intend to assign as primary server, connect to the Command Center client to ensure that the server is started, and then start the other server, which is automatically assigned as a secondary server.
   Note: For a successful HA failover, ensure that both the primary server and the secondary server are DNS-enabled.

Installing Certificates for Secure Communication

Jan 06, 2017

You must install a certificate from a trusted certification authority to validate the server identity and to ensure secure communication between the Command Center server and the clients. For more information about the ports that must be open between clients and the Command Center server, see Port Settings.

It is assumed that you already have the certificate you want to install.

You must convert the certificate to the pkcs#12 format by using any conversion tool, such as the openssl tool.

Note: You can install default certificates by using the cccerts.p12 file, which is located in the *CC_Home* directory.

To install the certificate

1. Copy the file, which is in the pkcs#12 format, either to the root directory on the Command Center server or to your local system.
2. Log on to the Command Center client.
3. On the Administration tab, in the right pane, under Tools, click Install Certificate.
4. In File, click Local (if you have saved the .p12 file on your local system) or click Server (if you have saved the file on the Command Center server), and then click Browse to select the .p12 file.
5. In Password, specify the password that you had provided while converting the certificate to pkcs#12 format.
6. Click OK and restart the Command Center server.
   Note: Changes to the certificate are effective after you restart the Command Center server.

Upgrading Command Center

Mar 30, 2016

Command Center offers new features and improved functionality of existing features. For more information, see

Upgrading the Command Center server to release requires the installation of the Command Center service pack. This service pack installs the upgraded Command Center platform, installs JRE 1.6, and upgrades your data.

You can download the service pack for both Windows and Linux from the Citrix portal Web site: http://mycitrix.com.

Note: You cannot downgrade a Command Center software or appliance.
Important: Please see the database upgrade requirements and the upgrade scenarios and steps before you begin upgrading your Command Center server.

Database Upgrade Requirements

For Command Center release , the MySQL database version supported is 5.0 and higher with InnoDB storage engine. Also, Command Center 4.0 and later no longer supports internal MySQL that was packaged with earlier releases of Command Center.

If you are using Command Center release 3.x with internal or external MySQL database version earlier than 5.1.x and/or with MyISAM storage engine, you must migrate your data to a MySQL database running 5.1.x with InnoDB storage engine before you upgrade to Command Center .

Upgrade Scenarios and Procedures

The following table summarizes four scenarios and the upgrade steps you would follow to upgrade your Command Center in each scenario.

Scenario	Upgrade Steps
Upgrading from Command Center release 3.x with one of the following databases: o MS SQL database o Oracle database o External MySQL 5.1.x with InnoDB storage engine	1. Upgrade to Command Center 4.0 by installing the service pack CC_SP4.exe (for Windows) or, CC_SP4.bin (for Linux) For information about the installation steps, see Installing the Service Pack. 2. Upgrade to Command Center 4.1 by installing the latest version of the service pack with file naming convention: CC_SP_ReleaseNumber_BuildNumber.exe (for Windows) or, CC_SP_ReleaseNumber_BuildNumber.bin (for Linux) 3. Upgrade to Command Center 5.x by installing the latest version of the service pack with file naming convention: CC_SP_ReleaseNumber_BuildNumber.exe (for Windows) or, CC_SP_ReleaseNumber_BuildNumber.bin (for Linux) For information about the installation steps, see Installing the Service Pack.
Upgrading from Command Center release 3.x with one of the following MySQL database versions:	1. Migrate to an external MySQL database running version 5.1.x with InnoDB storage engine. For information about the migration executable and the migration steps,

o Internal MySQL o External MySQL running a version earlier than 5.1.x o External MySQL running version 5.1.x and with MyISAM storage engine.	see Migrating MySQL Database. 2. Upgrade to Command Center 4.0 by installing the service pack CC_SP4.exe (for Windows) or, CC_SP4.bin (for Linux). For information about the installation steps, see Installing the Service Pack. 3. Upgrade to Command Center 4.1 by installing the latest version of the service pack with file naming convention: CC_SP_ReleaseNumber_BuildNumber.exe (for Windows) or, CC_SP_ReleaseNumber_BuildNumber.bin (for Linux) 4. Upgrade to Command Center 5.x by installing the latest version of the service pack with file naming convention: CC_SP_ReleaseNumber_BuildNumber.exe (for Windows) or, CC_SP_ReleaseNumber_BuildNumber.bin (for Linux) For information about the installation steps, see Installing the Service Pack.
Upgrading within Command Center release 5.x	Install only the latest version of the 5.1 service pack with file naming convention: CC_SP_ReleaseNumber_BuildNumber.exe (for Windows) or, CC_SP_ReleaseNumber_BuildNumber.bin (for Linux) For information on the installation steps, see Installing the Service Pack.
Upgrading Command Center software in a High Availability (HA) setup	To upgrade Command Center software in an HA setup: 1. Stop the Secondary Command Center service. 2. Stop the Primary Command Center service. 3. Upgrade the Primary Command Center server as described in the scenarios above. 4. Upgrade the Secondary Command Center server as described in the scenarios above. 5. Start the Primary Command Center service (Make sure that all the processes in <CC_HOME>/logs/wrapper.log are in the Started state) 6. Start the Secondary Command Center service. (Verify that the Command Center server in <CC_HOME>/logs/wrapper.log comes up as a secondary server)

In this section:

- Migrating MySQL Database
- Installing the Service Pack

Migrating MySQL Database

May 09, 2012

For Command Center release 5.1, the MySQL version supported is 5.1.x with InnoDB storage engine. Also, Command Center 4.0 and later no longer supports internal MySQL that was packaged with earlier releases of Command Center.

If you are using Command Center release 3.x with internal or external MySQL database version earlier than 5.1.x and/or with MyISAM storage engine, you must migrate your data to a MySQL database running 5.1.x with InnoDB storage engine by running the Data Migration executable.

You can download the data migration executable from the Citrix portal Web site: http://mycitrix.com

The executables are:

- CC_MySQL_DM_4.0.exe (for Windows)
- CC_MySQL_DM_4.0.bin (for Linux)

The data migration tool backs up your current data and restores it to your new database.

Important:

- Data backed up in Windows cannot be restored in Linux and vice-versa.
- The minimum available disk space of the source system where the data is backed up should be the same as the size as your database.
- The minimum available disk space of the destination system where data is getting migrated should be double the size of your database.

To migrate MySQL database

1. Install MySQL 5.1.x with InnoDB storage engine.
2. Create a database for Command Center.
   Important: The parameter max_allowed_packet in the file my.ini should be set to a high value. Citrix recommends you set this parameter to 30MB. The default location of this file is MySQL_Install_Dir (in Windows) and /etc/my.cnf (in Linux).
3. When prompted for the destination directory path, specify the path to your current Command Center location.
4. When prompted for the database settings, enter the host name, database name, port, user name, and password of the new database.
5. Click Next, or type 1 and press Enter (if you are running the tool from the CLI on Linux) to start the data migration process.
   Note: The data migration may take some time depending on the amount of data that is being migrated.

Installing the Service Pack

Oct 21, 2015

You need to install the Command Center service pack to upgrade the Command Center server to release 5.2. You can download the service pack for both Windows and Linux from the Citrix portal Web site: http://mycitrix.com. The service pack is an executable or binary file.

If you are upgrading to Command Center release 5.2 from release 3.x, you must first download the following to upgrade to Command Center release 4.0:

- CC_SP4.exe (for Windows)
- CC_SP4.bin (for Linux)

Note: This service pack installs the upgraded Command Center platform, installs JRE 1.6, and upgrades your data.

- To upgrade from Command Center release 4.0 or later to release 5.2, download the following:
  - CC_SP_ReleaseNumber_BuildNumber.exe (for Windows)
  - CC_SP_ReleaseNumber_BuildNumber.bin (for Linux)

Note: Make sure that you have read the database upgrade requirements and the upgrade scenarios and steps in Upgrading Command Center.

To install the service pack on Windows

1. Shut down the Command Center server.
2. To install the service pack, double-click the executable file that you downloaded.
3. Click Next and follow the instructions in the wizard. Upon successful completion of the upgrade process, the screen displays the summary of the upgrade.
4. Click Finish. The Command Center upgrade process is complete.
   Note: The upgrade may take some time depending on the size of the data that is being upgraded.
5. Double-click the Start Citrix Command Center server icon on the Windows desktop to start the server.

To install the service pack on Linux

1. Shut down the Command Center server by navigating to \\CC_Home\bin at the Linux terminal window, and then run the ShutDown.sh shell script.
2. To run the service pack, change the attributes of the file to executable.
3. At the Linux terminal window, type one of the following commands to start the installation wizard.
   ./CC_SP4.bin

   or,

   ./CC_SP_ReleaseNumber_BuildNumber.bin

   Note: You can also run the service pack from the CLI.
4. On the Welcome screen, click Next, select the license agreement, and then click Next.
5. On the Directory Name screen, click Next.
   Note: The Directory Name field displays the default installation directory path.
6. On the Summary screen, verify the settings.
7. To start the upgrade process, click Install. Upon successful completion of the upgrade process, the Installation Complete screen appears. In addition to notifying you that the Citrix Command Center server has been installed successfully, this screen also provides a brief introduction to getting started with Citrix Command Center.

8. Click Finish. The Citrix Command Center server upgrade installation is complete.
   Note: The upgrade may take some time depending on the size of the data that is being upgraded.
9. To start the Command Center server, at the Linux terminal window, navigate to the Services Manager screen and start the service..

Getting Started with Command Center

May 28, 2015

Citrix Command Center is a management and monitoring solution for Citrix application networking products that include Citrix NetScaler, Citrix NetScaler VPX, Citrix NetScaler Gateway Enterprise Edition, Citrix CloudBridge VPX, NetScaler SDX, CloudBridge Platform, and Citrix CloudBridge. Use Command Center to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

This centralized management solution simplifies operations by providing administrators with enterprise-wide visibility and automating management tasks that need to be executed across multiple devices.

The following management tasks are simplified with Command Center:

- Quickly address and resolve device and network issues and keep the network running effectively by monitoring and managing the SNMP and syslog events generated on your devices.
- Understand the traffic patterns, gather data for capacity planning, and monitor the performance of the entire application delivery infrastructure by using historical charts and performance graphs.
- Monitor and manage the states of virtual servers, services, and service groups across the NetScaler infrastructure.
- Simplify device management and minimize configuration errors by using built-in and custom tasks to make configuration changes across devices, upgrade firmware, and replicate a device's configuration to other devices in your network.
- Set up alerts for specific instances of entities and notify administrators when configured thresholds are breached by using the advanced entity-based thresholds feature.
- Troubleshoot configuration errors or recover unsaved configuration on sudden system shutdown by running audit policies.
- Prevent server downtime from expired SSL certificates by receiving notifications for certificate expiration dates, and then updating the certificates from your management solution.
- Ensure constant availability of your management solution by setting up Command Center in a high availability active-standby mode.

To begin monitoring and managing Citrix devices, you need to connect to the Command Center server by using the HTML Web client, and then add the devices for discovery. Command Center initiates the discovery process, which stores device-related information in the Command Center server.

This topic includes the following details:

Initial Configuration Wizard

Oct 31, 2014

The Initial Configuration wizard helps you set up the Command Center configuration for the first time after installing the Command Center. This wizard enhances the first time user experience by helping a new user get started with Command Center efficiently and effectively by setting up the one time configuration for adding a device.

A dashboard is provided in the home tab to provide information about the configured settings based on the module and its usage. The dashboard also provides an option to configure the settings instantly.

You can add devices by specifying the host names of the devices, the IP addresses of each device, a range of IP addresses, and NAT HA devices. If you have configured IPv6 feature on the NetScaler device, you can add the NetScaler device using the NetScaler IP addresses in IPv6 format. You can also add devices by importing the device names from a file. Note that when you specify a range, the first three octets of the low and high addresses must be the same. Command Center can discover only 254 devices in an IP address range.

Adding a Device

To begin monitoring and managing Citrix devices, first add the device in the Command Center.

1. Under Add Device, provide the following details:
   - Select either of the following check boxes:
     - Enter Device IP: In the Devices text box, type the host names, or IP addresses, Cluster IP addresses, IP addresses in IPv6 format, ranges of IP addresses of devices, and IP addresses of NAT devices you want to discover.
       Note: When adding a NetScaler high-availability pair whose NetScaler IP (NSIP) addresses are in IPv6 format, use the pound sign (#) as a separator between the two addresses: < IPv6 address>#<IPv6 address >.
     - Import from File: Select the Import from file check box, and then click the Choose File to select a file containing the host names and/or IP addresses of the devices you want to discover.
   - From the Device Profile drop-down list, select the device family.
     Note: If the device password is not a default password, click the + icon next to the Device Profile drop-down list to create a new device profile and provide the user credentials and SNMP details.
2. Click Continue.
   If the device is discovered successfully, the Device Status Summary is displayed.
3. Click Continue.
   After the device is discovered, it is displayed in the Citrix Network tab.

   In the right pane, from the Advanced menu, you can also configure authentication settings, mail server settings, and/or disk management.

   For details about authentication settings, see Configuring Authentication Settings.

   For details about mail server settings, see Configuring Mail Server Settings.

   For details about disk management, see Configuring Server Settings.

Logging on to Command Center

May 24, 2012

You need to connect to the Command Center server by using the HTML Web client.

To log on to Command Center

1. In your Web browser address field, type one of the following:
   http://ComputerName:PortNumber
   or
   https:///ComputerName:PortNumber
   Where:
   - ComputerName is the fully qualified domain name (FQDN), host name, or the IP address of the Command Center server.
   - PortNumber is the port used by the Command Center client and server to communicate with each other. The default port number for HTTP is 9090 and for HTTPS is 8443.
2. On the Login page, in User Name and Password, type the user name and password to connect to the Command Center server, and then click Login.

   The default user name and password are **root** and **public**. However, Citrix recommends that you change the password after you install the Command Center server. For information about changing the root password, see Changing the Root Password.

   The Command Center Home page appears that provides you with a high-level view of the performance of the Citrix devices that you are managing and monitoring.

   On first log on, the Home page does not display any data because you do not have any Citrix devices discovered on your Command Center.

3. In the Start in list, select how you want to log on to Command Center. The available options are Home, Citrix Network, Fault, Monitoring, Configuration, and Reporting. For example, if you want Command Center to display the Configuration page when you log on, select Configuration in the Start in list.
4. In Timeout, type the length of time (in minutes, hours, or days) for which the session can be inactive before you must log in again. The timeout duration that you specify here is applicable only for this client. You can also specify timeout duration for all the users on the Access Settings page (Administration > Access Settings). For more information, see .
   Note: You must minimize the Alarm Summary table for the session timeout to work. If the Alarm Summary table is expanded, the session is considered to be active.
5. Click **Login** to log in to the Command Center client.

Adding Devices

May 27, 2015

Devices are Citrix appliances or virtual appliances that you want to discover and manage.

The Command Center server supports three types of devices:

- Standalone : A standalone device functions independently and is not configured in an HA setup.
- HA pair : This represents a pair of devices configured in an HA setup. The primary device in an HA setup processes the traffic. The secondary device monitors the primary and takes over the functions of the primary device if that device is unable to continue processing traffic.
- NetScaler Cluster: This represents a group of NetScaler devices working as a single device. Each device of the NetScaler cluster is called a node. A NetScaler cluster can include as few as 2 or as many as 32 NetScaler devices as nodes.

You can add devices by specifying the host names of the devices, the IP addresses of each device, a range of IP addresses, and NAT HA devices. If you have configured IPv6 feature on the NetScaler device, you can add the NetScaler device using the NetScaler IP addresses in IPv6 format. You can also add devices by importing the device names from a file. Note that when you specify a range, the first three octets of the low and high addresses must be the same. Command Center can discover only 254 devices in an IP address range.

To add devices

1. On the Citrix Network tab, in the left pane, click Device Inventory, and in the right pane, click Add.
2. Under Add Device, do one of the following:
   - In the Devices text box, type the host names, IP addresses, Cluster IP addresses, NetScaler IP addresses in IPv6 format, range of IP addresses of devices, and IP addresses of NAT devices you want to discover.
     Note: When adding a NetScaler high-availability pair whose NetScaler IP (NSIP) addresses are in IPv6 format, use the pound sign (#) as a separator between the two addresses: < IPv6 address>**#<**IPv6 address >.
   - Click the Import from file check box, and then click the Browse to select a file containing the host names and/or IP addresses of the devices you want to discover.
3. Under Device Profile, select a profile you want to use. To add a new profile, click + icon, and follow the steps described in Add Device Profiles.
4. Click Continue. The Discovery Status page displays the status of the discovery process. It also displays the status of the peer device.
5. Click Done.

Viewing the Discovery Status of Devices

Updated: 2014-10-31

Command Center lets you view the discovery status of all discovered as well as inaccessible devices.

To view the discovery status of devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and then click Discovery Status.
2. On the Discovery Status page, you can view the following details:
   - Time: Time when the step in the discovery process started.
   - Device: Device that is being discovered.
   - Operation: Step in the discovery process that is executed, such as add trap destination and enable SNMP.

- Status: Status of a step in the discovery process. The status can be STARTED, COMPLETED, and FAILED.
- Description: Message that describes the reason of the discovery process failure or the details of when the discovery process started on a particular device.

Understanding the Discovery Process

May 27, 2015

Command Center initiates the discovery process when you add the devices to the map. Command Center discovers devices based on the user credentials and/or the host names and IP addresses that you provide when adding a map or device.

After you initiate the discovery process, the device goes through a series of steps. Each step and its status in the discovery process are visible in Command Center. To view the discovery status, see Viewing the Discovery Status of Devices.

The Command Center discovery process involves the following steps:

1. **SNMP ping:** The Command Center server sends a Simple Network Management Protocol (SNMP) GET request to a Citrix system-specific object identifier (OID) (for example, 1.3.6.1.4.1.5951.1.1). If the server successfully pings the device, it sets the status of step 2 to SUCCESS and proceeds to step 3. If the GET request fails, the device is not a Citrix device, or it is a Citrix device but SNMP is disabled on it. In either fail case, the Command Center server proceeds to step 2.
2. **Find Citrix device:** The Command Center server attempts to open an SSH session to the device based on the user credentials configured when adding a map. If the SSH session fails, the device is discarded as a non-Citrix device. If the SSH session succeeds, the server issues a CLI command to check whether the device is a Citrix device. A positive result moves the device to the next step. Otherwise, Command Center discards the device as a non-Citrix device. To check the cause of failure of this step, on the Citrix Network tab, click the device, and click Status. You can also view the cause of failure on the Device Status page.
3. **Enable SNMP:** On the discovered Citrix device, Command Center executes a command to configure an SNMP community based on the details entered when configuring the map or when adding a device. This step may fail for various reasons, such as network issues or if another SNMP manager is already configured on the device.
4. **Add trap destination:** Devices communicate with Command Center by sending trap notifications. The Command Center server adds its IP address to the list of trap destinations on the discovered device. This allows Command Center to receive all events/traps generated on the Citrix device. However, this step may fail if the number of trap destinations exceeds the maximum limit of trap destinations on the Citrix device. The limit on Citrix NetScaler devices is 10. If an error occurs you must take corrective measures before you initiate rediscovery of this device.
   Note: If Command Center is behind a Network Address Translation (NAT) device, the trap destination configured on the server is its internal IP, and the events and traps generated by the Citrix device do not reach the Command Center server. To set the trap destination in this case, you must configure it from the Administration tab. For more information, see "Setting Up an SNMP Trap Destination" in the Citrix Command Center Administrator's Guide.
5. **Collect inventory:** The Command Center server collects the basic system information for the discovered devices using SNMP. You can view this information on the Device Properties page. For more information, see "Viewing Device Properties" in the Citrix Command Center Online Help. This step may fail if the SNMP manager configured on the Citrix device is not that of the server. It may also fail because of network issues or because the SNMP ports are not configured properly on the firewall. If an error occurs you must take corrective measures, and then initiate rediscovery of the device.
6. **Download files:** The Command Center server initiates a Secure File Transfer Protocol (SFTP) session based on the user credentials defined while configuring the map. Then, it downloads the configuration and license files of the device. For CloudBridge devices, it downloads only the configuration files. The Command Center server stores these files in the database. This step may fail because of the following reasons:
   - Incorrectly specified user credentials
   - Incorrectly configured SFTP ports in the firewall
   - Network issues

To check the cause of failure, on the Citrix Network tab, click the device, and click Status. You can also view the cause of failure on the Device Status page. If an error occurs, you must take corrective measures, and then initiate rediscovery of this device.

Note: If the discovery process fails, the failed step is marked as FAILED. Any subsequent steps are marked as N/A.
Upon successful discovery, the devices appear on the corresponding maps as icons with their IP addresses or device names. If the server is unable to successfully discover the devices, it marks the devices as inaccessible, generates an event, and groups the devices under the **Inaccessible Systems** node.

Provisioning NetScaler VPX Devices on XenServers

May 09, 2012

Using Command Center you can provision NetScaler VPX on XenServers and begin managing the NetScaler VPX instances.

You can install one or more instances of NetScaler VPX on a XenServer from the Command Center client by using a NetScaler VPX template. The number of instances that you can install depends on the amount of memory available on the hardware that is running XenServer.

To provision NetScaler VPX on a XenServer, first, you need to add the XenServer device and set it for discovery. After the XenServer is discovered, you can provision the NetScaler VPX devices on the XenServer from the Command Center client. Command Center implicitly deploys NetScaler VPX devices on the XenServer, and then discovers the NetScaler VPX devices for monitoring and management.

Important: Before you begin provisioning the NetScaler VPX devices, create a NetScaler VPX template on the XenServer. Make sure that the template name contains the word "NetScaler" as part of the name string, for example, "NetScaler Virtual Appliance". Command Center recognizes only template names with "NetScaler" in the string as NetScaler VPX templates.
When you provision NetScaler VPX from Command Center, you need to provide values for the following parameters, and Command Center implicitly configures these settings on the NetScaler VPX.

- NetScaler IP address (NSIP): Specifies the IP address at which you access a NetScaler VPX instance for management purposes. A NetScaler VPX can have only one NSIP. You cannot remove an NSIP address.
- Netmask: Specifies the subnet mask associated with the NSIP address.
- Gateway: Specifies the default gateway that you must add on the NetScaler VPX if you want access through SSH or the configuration utility from an administrative workstation or laptop that is on a different network.

To provision NetScaler VPX devices on a XenServer

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices.
2. In the right pane, under Device Inventory, right click on the XenServer device on which you want to provision the NetScaler VPX devices, and then click Provision VPX from the menu options.
3. Under Provision VPX, in Template Name, click the NetScaler VPX template you want to use.
4. In NetScaler IP, type the IP address you want to assign to the NetScaler VPX device.
5. In Netmask, type the IP address of the subnet mask for the subnet where the device is deployed.
6. In Gateway, type the IP address of the default gateway for the device.
7. Click **OK.**

Provisioning NetScaler Instances on NetScaler SDX Platform

May 27, 2014

Using Command Center you can provision one or more NetScaler instances on NetScaler SDX device and begin managing the NetScaler VPX devices. The number of instances that you can provision depends on type of NetScaler SDX device license.

To provision NetScaler instance on a NetScaler SDX device, first add the NetScaler SDX device and set it for discovery. After the NetScaler SDX device is discovered, you can provision the NetScaler instance on the NetScaler SDX device from the Command Center client. Command Center provisions the NetScaler instances on the NetScaler SDX device, and then discovers the NetScaler instances as NetScaler VPX devices in Command Center for monitoring and management.

Important: Before you begin provisioning the NetScaler instances, make sure that the .xva image file is uploaded and the admin profile is created on the NetScaler SDX device. Also, view the Device Properties page to check the # Maximum NetScaler Instances property and # Available NetScaler Instances property, to ensure that you do not exceed the maximum number of NetScaler instances that can be provisioned for that NetScaler SDX device.
Note: Provisioning is not enabled for NetScaler SDX Platform models 19555, 17555, 11505, and 13505.
When you provision NetScaler instance from Command Center, you need to provide values for the following parameters.

- Name: The host name assigned to the NetScaler instance.
- IP address: The NetScaler IP (NSIP) address at which you access a NetScaler instance for management purposes. A NetScaler instance can have only one NSIP. You cannot remove an NSIP address.
- Netmask: The subnet mask associated with the NSIP address.
- Gateway: The default gateway that you must add on the NetScaler instance if you want access through SSH or the configuration utility from an administrative workstation or laptop that is on a different network.
- #SSL Cores: The number of SSL cores you want to assign to a NetScaler instance.
- XVA File: The .xva image file that you need to provision.
- CPU: Assign a dedicated core or cores to the instance or the instance shares a core with other instance(s).
- Feature License: Specifies the license you have procured for the NetScaler. The license could be Standard, Enterprise, and Platinum.
- Admin Profile: The profile you want to attach to the NetScaler instance. This profile specifies the user credentials used by Management Service VM and to communicate with the instance to retrieve configuration data.
- User Name: The root user name for NetScaler instance administrator.
- Password: The password for the root user.
- Shell/Sftp/Scp Access: The access allowed to the NetScaler instance administrator.
- Total Memory (MB): The total memory allocated to the NetScaler instance.
- Throughput (Mbps): The total throughput allocated to the NetScaler instance. The total used throughput should be less than or equal to the maximum throughput allocated in the SDX license. If the administrator has already allocated full throughput to multiple instances, no further throughput can be assigned to any new instance.
- Packets per second: The total number of packets received on the interface every second.
- Interfaces: Bind the selected interfaces to the NSVLAN. This specifies the network interfaces assigned to a NetScaler instance. You can assign interfaces to an instance. For each interface, you can specify a VLAN ID. This is the network interface that is a tagged member of a VLAN.
  - If a non-zero VLAN ID is specified for a NetScaler instance interface, all the packets transmitted from the NetScaler instance through that interface will be tagged with the specified VLAN ID. If you want incoming packets meant for

the NetScaler instance that you are configuring to be forwarded to the instance through a particular interface, you must tag that interface with the VLAN ID you want and ensure that the incoming packets specify the same VLAN ID.
    - For an interface to receive packets with several VLAN tags, you must specify a VLAN ID of 0 for the interface, and you must specify the required VLAN IDs for the NetScaler instance interface.
- **VLAN ID**: An integer that uniquely identifies the VLAN. Minimum value: 2. Maximum value: 4095.
- **NSVLAN**: A VLAN to which the subnet of the NetScaler management IP (NSIP) address is bound.
- **VRID IPV4**: The IPv4 VRID that identifies the VMAC. Possible values: 1 to 255.
- **VRID IPV6**: The IPv6 VRID that identifies the VMAC. Possible values: 1 to 255.
- Tagged: Designate all interfaces associated with the NSVLAN as 802.1q tagged interfaces.
  Note: If you select tagged, make sure that management interfaces 0/1 and 0/2 are not added.

To provision NetScaler instances on a NetScaler SDX Platform

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and then click Devices.
2. In the right pane, under Devices, select the NetScaler SDX device on which you want to provision the NetScaler instances, and then do one of the following:
    - Right-click the NetScaler SDX device and then click Add NS Instance.
    - Click the Add NS Instance button at the bottom of the right pane.
3. In the Provision NetScaler Instance dialog box, specify values for the following parameters.
    - Name*
    - IP Address *
    - Netmask *
    - Gateway *
    - XVA File *
    - Feature License *
    - Admin Profile *
    - Description
4. Under Resource Allocation, specify values for the following parameters.
    - Total Memory (MB) *
    - #SSL Cores *
    - Throughput (Mbps) *
    - Packets per second *
    - CPU *
    - Reboot affected Instances if CPU cores are reassigned. You can check this option to restart the instances on which CPU cores are reassigned to avoid any performance degradation.
5. Under Instance Administration, specify values for the following parameters.
    - User Name*
    - Password*
    - Shell/Sftp/Scp Access*
6. Under Network Settings, select the check boxes next to the interfaces you want to assign, and then in the corresponding text boxes, specify the VLAN IDs for the network interfaces. Optionally select the Allow L2 Mode option to allow the L2 mode on the NetScaler instance. Select this option before you log on to the instance and enable L2 mode.
7. Under VLAN Settings, specify the VLAN ID. Optionally, select Tagged to tag packets with the specified VLAN ID. Optionally select the **NSVLAN** option if your deployment requires that the NSIP not be accessible through any interface other than the one you select in the VLAN Settings dialog box. This setting cannot be changed after the NetScaler instance is provisioned. In the Available list, click the arrow symbol to move the interface to the Configured list. The

selected interface is tagged with the specified NSVLAN ID.

8. Click OK.

Configuring a NetScaler Cluster from Command Center

Apr 17, 2014

To create a cluster from Command Center, under **Configure Cluster**, set up a cluster backplane, add the first node to the cluster from the list of discovered NetScaler devices in Command Center, and then assign a cluster IP address. After you have created the cluster, you can add more nodes to the cluster.

To configure a NetScaler Cluster

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and then click Devices.
2. In the right pane, select the device for which you want to configure a cluster, and then from the Action drop-down list click Configure Cluster.
3. Under Configure Cluster, provide the following parameters.
   - **Cluster IP** . The IP address to assign as Cluster IP address.
   - **Cluster ID** . An identification number that distinguishes the cluster from other clusters. Minimum value: 1. Maximum value: 16.
   - **Node ID** An identification number that distinguishes the node from other nodes in the cluster. Each node in the cluster must have a different node ID. Minimum value: 0. Maximum value: 31.
   - **Node IP** The IP address of the NetScaler device you intend to add as cluster node.
   - **State** . The configured state of the cluster node. Possible values: ACTIVE, PASSIVE, SPARE. Default: PASSIVE.
   - **Back Plane** . Backplane interface of the node. For example, if node 0 uses interface 1/1, the value of this parameter is 0/1/1. If node Id is 1, backplane will be 1/1/1. It is a combination of node id/interface/port number.
4. Click Create. You have created a single-node cluster. After Command Center discovers the new cluster, you can add additional nodes.

AutoConfiguration: Simplifying Remote CloudBridge Deployments

May 27, 2015

A CloudBridge solution requires the CloudBridge product to be present at both sides of the link. This imposes a deployment burden on the remote offices, especially the ones without dedicated IT staff. The autoconfiguration feature of Command Center eliminates this burden by offloading the deployment and configuration effort to the datacenters, thus reducing the effort and expertise required at the branch offices. The autoconfiguration feature eases deployments involving large number of branch offices.

With the autoconfiguration feature, Command Center automates the configuration and deployment of CloudBridge devices in the branch offices. You can use this feature to add new branch devices for either a new deployment or an existing deployment.

Points to Note:

- The autoconfiguration feature is not supported on CloudBridge 600, 700, 4000, or 5000 appliances, CloudBridge VPX instances, or Repeater 8300, 8520, or 8820 appliances.
- The autoconfiguration feature does not support IPv6 addresses.

This topic includes the following details:

Limitations

Updated: 2014-09-05

The autoconfiguration feature does not support the following configurations:

- Local licenses
- Certificate configuration (SSL/HA/GroupMode)
- Install Software command

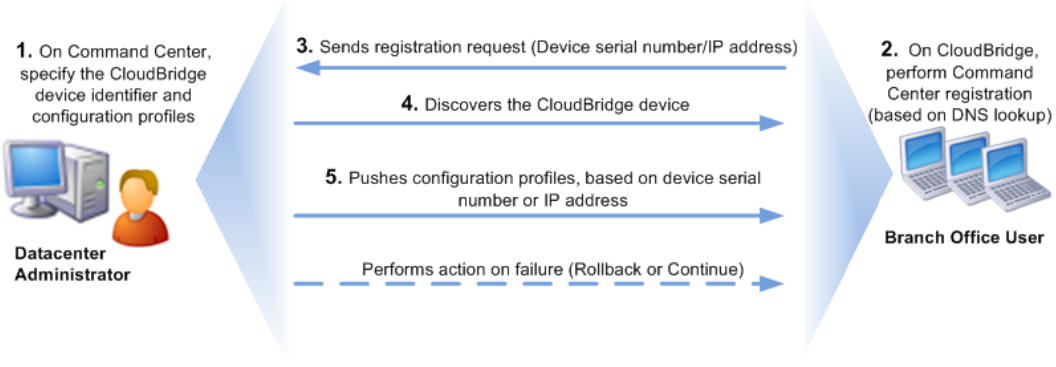
How AutoConfiguration Works

Updated: 2014-09-05

The autoconfiguration feature implicitly registers, discovers, and configures a CloudBridge device by using the CloudBridge device identifier and the configuration profile input provided by the datacenter administrator. It requires minimal manual configuration at both the datacenter and the branch offices.

The following figure shows how the autoconfiguration feature works.

Figure 1. How AutoConfiguration Works



Following is the workflow of the autoconfiguration feature:

1. The datacenter administrator configures the Command Center server with the CloudBridge device serial number or the management service IP address and the configuration profile details. The datacenter administrator then notifies the branch office user.
2. The branch office user powers on the CloudBridge device and performs the initial configuration by using the setup wizard where he provides the DNS IP address along with other network settings.
   After the initial setup of the CloudBridge device is completed, and the Command Center server IP address is resolved, the branch office user enables the device for registration with the Command Center server.
3. The CloudBridge device, then implicitly requests the Command Center server to begin registration.
4. On receiving this request, the Command Center server registers the device and starts the device discovery process.
5. After discovery is successful, the Command Center server begins the CloudBridge device configuration based on the details in the configuration profiles assigned to this device.

Note: If any command fails during configuration, the Command Center server either rolls back the entire configuration or runs the rest of the commands depending on the settings configured by the datacenter administrator.
On completion of automatic registration and configuration on the CloudBridge device, the Command Center server raises an internal event. The information about this configuration is stored in execution logs on the Command Center server. The datacenter administrator can view the progress of the automatic registration, discovery, and configuration on the Command Center graphical user interface (GUI.)

Prerequisites to Configuring AutoConfiguration

Updated: 2014-09-05

Before you begin configuration, make sure you have the following information:

Datacenter Administrator

- Serial number or management service IP address of the CloudBridge device from the purchase order of the CloudBridge device.
  Important: The datacenter administrator must use the management service IP address and not the CloudBridge IP address.
- Configuration profiles that you want to assign to the device (See Appendix for a sample.)
- Confirmation that CloudBridge registration settings status is enabled on the Command Center server (Administration > Settings > CloudBridge Registration Settings.)
  Note: If this setting is enabled, the CloudBridge device initiates the discovery process through the Command Center server.
- CloudBridge registration settings password.
- Device profile password on the Command Center server (Citrix Network > Device Inventory > Device Profile > <profile_name>.)
  Note: Password of the device profile that you specify when you enable the CloudBridge registration settings on the Command Center server.

Branch Office User

- Confirmation that the hardware installation of the CloudBridge device is completed.
- Command Center server IP address.
- DNS server is configured with a valid address record of the Command Center server. (Specify the DNS server hostname as commandcenter.yourdomain.)
- Administrator password, which is the device profile password provided by the datacenter administrator on the Command Center server.
- CloudBridge registration settings password.

Configuring AutoConfiguration

Updated: 2015-03-31

The configuration of the autoconfiguration feature requires the datacenter administrator to provide the CloudBridge device serial number or the management service IP address and the configuration profile to the Command Center server. At the branch office, the user needs to power on the device, perform initial setup, and set the device for registration with the Command Center server.

Configuration Steps Performed by the Datacenter Administrator

1. In a web browser, type the IP address of the Command Center server.
2. Navigate to Citrix Network > Device Inventory > CloudBridge Advanced Platform and, in the details pane, on the AutoConfiguration tab, click Add.
3. In the Choose Configuration Profiles page, enter values for the CloudBridge device serial number or the management service IP address, select or create configuration profiles, and choose to either roll back or continue with the configuration on command failure.
   Note:

- You can assign multiple configuration profiles to a device. The profiles will be configured on the device in the sequence specified on this page.
- Before you specify the configuration profiles, make sure that the configuration works as expected.

4. If you want to receive an email notification after the configuration is complete, specify your email address.
5. Notify the branch office user to power on the CloudBridge device and perform the initial setup on the device.

Configuration Steps Performed by the Branch Office User

1. In a web browser, type the IP address of the CloudBridge device.
2. In the Command Center wizard, (Configuration > Appliance Settings > Command Center), specify the Command Center IP address, port number and the registration password set by the datacenter administrator while configuring the CloudBridge registration settings, and click OK.

The CloudBridge device sends a registration request to the Command Center server, which automatically discovers the device and executes the commands in the configuration profile.

Verification Steps

Updated: 2014-09-05

After the configuration is complete at both the datacenter and the branch office, the datacenter administrator and the branch office user can monitor and verify the progress and success of the registration, discovery, and configuration process.

Verification at the datacenter

On the Command Center server, navigate to Citrix Network > Device Inventory > CloudBridge Advanced Platform and, in the details pane, click the AutoConfiguration tab.

You can view the registration status and the configuration status of the device in the AutoConfiguration pane, as shown in the following image.

Figure 2. Verification at the datacenter

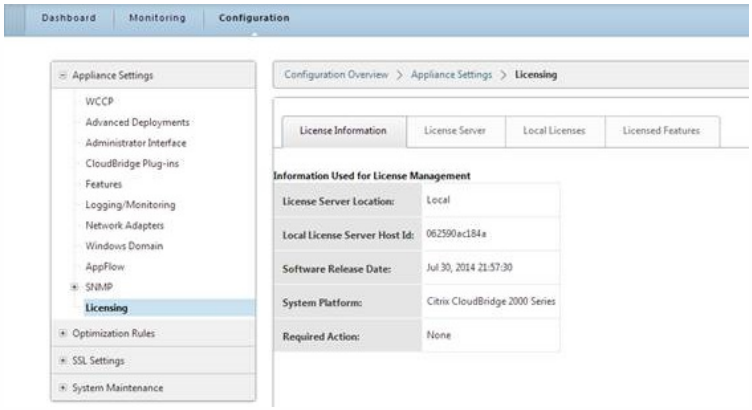
Verification at the branch office

You can apply a license to the device by using the autoconfiguration feature. In such a case, after the autoconfiguration process is completed, the device is licensed with the license file that is specified in the configuration profile.

To verify that the CloudBridge device is configured:

1. Log on to the CloudBridge device.
2. Navigate to CloudBridge > Configuration > Appliance Settings > Licensing.
   The License Information tab of the Licensing page displays the details of the license applied to the device.

Figure 3. Verification at the branch office



Note: If the device is not yet licensed, a message stating "Appliance is not licensed." is displayed as soon as you log on to the device. This message disappears after the device is licensed and after you refresh the page.

Troubleshooting Tips

Updated: 2014-09-05

If the Registration Status column or the Configuration Status column on the Command Center server (Citrix Network > Device Inventory > CloudBridge Advanced Platform and click AutoConfiguration) does not show a green check mark, check if you see one of the following status messages and take the specified action.

1. **Registration Status**: Registration request not received.
   - **Possible Causes**:
     - The Command Center server has not received a registration request from the CloudBridge device and is yet to discover the CloudBridge device. This is the initial status displayed on the AutoConfiguration tab after the datacenter administrator has specified the CloudBridge device identifier and configuration profiles.
     - The Command Center server has successfully discovered the CloudBridge device, but not the CloudBridge instance hosted on the device.
   - **Action**: The branch office user should initiate the setup wizard (System > Configuration > System > Setup Wizard) again and resend the registration request.
2. **Registration Status**: Failed device.
   - **Possible Cause**: Discovery of the CloudBridge device in the Command Center server has failed.
   - **Action**: On the Command Center server, navigate to Citrix Network > Device Inventory. Select the CloudBridge device and, from the Action list, click Status and view the discovery error status. Rectify the error and start the rediscovery. For example, if the error message says, "Unable to enable SNMP on device : Exceeded task timeout of 15000ms waiting for end prompt", check to see if SSH from the Command Center server to CloudBridge device responds within 15 seconds. If it takes longer, increase the SSH timeout in the associated device profile and restart the discovery again.
3. **Configuration Status**: Configuration request not received.
   - **Possible Cause**: AutoConfiguration by Command Center flag on the CloudBridge device is unset.
     To verify, on the CloudBridge device, after you perform the initial configuration on the setup wizard (System > Configuration > System > Setup Wizard), on the CloudBridge Registration Settings screen, check to see if the AutoConfiguration by Command Center flag is unset.
   - **Action**: On the Command Center server, from the AutoConfiguration tab, select the required row and click Retry Configuration to push the configuration profiles to the CloudBridge device.
4. **Configuration Status**: Failed and Rolled Back.
   - **Possible Cause**: Command execution on the CloudBridge device has failed and the failed commands are rolled back.
   - **Action**: On the Command Center server, from the AutoConfiguration tab (Citrix Network > Device Inventory > CloudBridge Advanced Platform), select the required row and click View Report. This lists the commands executed and their statuses. Modify the failed command in the corresponding configuration profile and, from the AutoConfiguration tab, select the required row and click Retry Configuration to push the configuration profiles to the CloudBridge device.
5. **Configuration Status**: m/n Commands Failed.
   - **Possible Cause**: One or more commands have failed to execute in the CloudBridge device.
   - **Action**: On the Command Center server, from the AutoConfiguration tab (Citrix Network > Device Inventory > CloudBridge Advanced Platform), select the required row and click View Report. This lists the commands executed and their statuses. Modify the failed command in the corresponding configuration file and, from the AutoConfiguration tab, select the required row and click **Retry Configuration** to push the configuration profiles to the CloudBridge device.

Appendix

Updated: 2014-09-04

Configuration Profile Sample

```
###########
# System Configuration
enable unit
enable acceleration
enable traffic-shaping

###########
# Link Configuration
remove link -all
add link -name "Link (apA.2)" -type WAN -max-in-bandwidth 10000000 bps -max-out-bandwidth 10000000 bps -adapters apA.2
add link -name "Link (apA.1)" -type LAN -max-in-bandwidth 1000000000 bps -max-out-bandwidth 1000000000 bps -adapters apA.1

#Set the License Server
set license-server -location remote -model 2000-050 -ip 10.102.137.44 -port 27000
```

```
#Set the apA network configuration
set adapter apa -ip 88.88.88.0 -netmask 255.255.255.0 -gateway 88.88.88.1 -vlan enable -vlan-group 75
set dns-server 10.140.50.5 -backup-dns 10.140.50.6

##########
# Date Time Configuration
add ntpserver 10.102.76.127
set timezone Asia/Kolkata


#Enable video caching.As Enable video caching takes RESTART hence above changes will take effect automatically
enable videocaching

#Add the Video sources

##########
# Video Caching Source and Listen Port List
remove videocaching -video-source -clear-enabled
remove videocaching -video-source -clear-disabled
remove videocaching -video-source -clear-excluded
remove videocaching -listen-ports -clear
add videocaching -video-source "vimeo.com" -state  enable
add videocaching -video-source "youtube.com" -state  enable
add videocaching -video-source "dailymotion.com" -state  disable
add videocaching -video-source "metacafe.com" -state  disable
add videocaching -video-source "youku.com" -state  disable
add videocaching -listen-ports "80"


#Add the Pre-population list

#Advanced Configuration
##########
# Video Caching DNS Suffix, Max Object Size
remove videocaching dns-suffix
set videocaching -dns-suffix "citrix.com"
set videocaching -max-object-size 100


##########
# SYSLOG Configuration
add syslog -ip 4.5.6.76 -port 514

# SNMP Configuration
enable snmp
add snmp-manager -community "public" -ip 10.102.203.199 -netmask 32
add snmp-trapdest -name "MYSNMP_Trap203.199" -ip 10.102.203.199 -port 162 -version v2c -community "public"
```

Viewing Inaccessible Devices

Jul 15, 2014

When any step of the discovery process fails either when adding a new device or when rediscovering an existing device, Command Center moves the device to the **Inaccessible Systems** node and notifies the administrator through an event. Subsequent successful rediscovery of the device makes it available for monitoring and managing.

To view the inaccessible devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Inaccessible Systems.
2. You can perform the following set of tasks on inaccessible devices:
   - Status::
   - Rediscover: Rediscover the device map.
   - Quick Report: View reports about the performance of a specified device.
   - Configuration Utility: Navigate to the device configuration utility.
   - Invoke CLI: Invoke the command line interface of the device.
   - Ping: Ping the device.
   - Trace Route: View the route of a packet from the server to the device.
   - Execute Task: Execute built-in and custom tasks to make configuration changes across devices, upgrade firmware, and replicate a device's configuration to other devices on your network.

Configuring Maps

May 26, 2015

Maps are logical containers that either graphically represent a group of discovered Citrix devices, or represent a group of devices configured as a NetScaler pool and are considered a single logical unit. When adding a map, you need to select the devices you want to grouped under that map. After adding a map, you can perform operations on a map, such as adding submaps and modifying maps. You can also perform operations on all the devices in a map, such as configuring audit and running reports.

This topic includes the following details:

Adding Maps

Updated: 2014-04-16

Maps are logical containers that either graphically represent a group of discovered Citrix devices considered a single logical unit. You can either add a map and group devices under it logically, such as based on features configured on your devices.

To add maps

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Maps.
2. In the right pane, click Add.
3. Under Add Map, in Name, type the name that you want to use for the new map.
4. In Description, type a brief description of the new map. Note that this step is optional.
5. In Devices click the the + icon next to the devices you want to add to the map and then click Create.

Modifying Maps

Updated: 2014-04-16

You may want to modify a map if the device login credentials or SNMP version details on your devices have changed. You can also modify a map to add more devices to that map, or remove existing devices from the map.

To modify maps

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Maps.
2. In the right pane, click the map you want to modify, and then click Edit.
3. Under Modify Map, make the required changes, and then click OK.

Deleting Maps

Updated: 2014-04-16

You can delete an existing map from the network using the delete map feature.

To remove a map

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Maps.
2. In the right pane, click the map you want to delete, and then click Delete.
3. In the confirmation dialog box, click Yes. The map is deleted.

Performing Operations on Maps

Updated: 2014-07-04

After you have grouped devices by adding maps (see Adding Maps), you can perform a set of operations on all the devices grouped under a specific map, such as run reports and execute tasks.

To perform operations on maps

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Maps.
2. In the right pane, click a map on which you want to perform an operation. either by selecting the following options from the Action drop-down list or by clicking the tabs on the top of the maps.
   - Run Report: Run a custom report on all the devices in a map or a pool to troubleshoot or analyze the behavior of the devices.
   - Execute Task: Execute a built-in or custom task on all the devices in a map or a pool.
   - Config Audit: Run configuration audits on all the devices in a map or a pool to monitor configuration changes across the devices.
   - Rediscover: Rediscover all the devices in a map.
   - View Map: View the map

Monitoring Devices

May 28, 2015

After the devices are discovered, on the Citrix Network tab you can perform various operations specific to single devices or multiple devices.

This topic includes the following details:

Viewing Device Properties

During every discovery or rediscovery of a device, Command Center downloads and stores the configuration and license files of that device. These files contain device-related information that you can view in device properties.

To navigate to device properties

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Devices.
2. In the right pane, under Devices, select the device, and then click Device Properties. Alternately, right-click the device, and then click Device Properties.

CloudBridge Device Properties

General Properties of CloudBridge Devices

The general properties of a device are:

- System Name: Specifies the name of the system.
- **CloudBridge IP**: Specifies the IP address of the system.
- Build Version: Specifies the software version of the CloudBridge device.
- System Status: Specifies the system status—Normal or Bypass.
- Boost Status: Specifies the mode of boost operation used by the device—Hardboost or Softboost.
- Uptime: Specifies the period of time, in days, hours and minutes, for which the device has been continuously in the up state.
- Host Name: Specifies the host name of the system.
- Bandwidth Mode: Specifies the mode of bandwidth set for accelerated and non-accelerated traffic—Full or Partial.
- Bandwidth Limit: Specifies the bandwidth limit value configured for the device in megabits per second (Mbps).
- HA Virtual Management IP: Specifies the virtual management IP address specified for the HA pair.
- Node State: Specifies the state of the device. The state indicates whether the device is configured in a standalone or is part of a High Availability setup. In a High Availability setup, it displays as either HA node primary or HA node secondary.
- Contact Person: Specifies the contact information of the person who configured the device. (By default, it is the webmaster.)
- Qos Status: Specifies the Qos Status for the Repeater device.
- Serial Number: Specifies the serial number of the Repeater device.
- Managed: Specifies the status of the device—whether the device is Managed or Unmanaged. The values that display are TRUE or FALSE, TRUE indicates that the device is managed and FALSE indicates that the device is not currently managed by Command Center.
- Location: Specifies the SNMP location value of the device.
- HA Peer IP Address: Specifies the IP address of the peer HA device in an HA setup.
- HA Virtual Management IP Address: Specifies the virtual management IP address of the HA pair.
- Profile Name: Specifies the device profile that is used by Command Center to access the device. To modify the device profile, click the Edit icon and select a different profile.

Monitoring Parameters of CloudBridge Devices

To view Monitoring, under Device Properties, click More. The Monitoring section displays the status of monitoring parameters and status polling options:

- Last Status Update Time: Specifies the time that the last status check was performed on the device.
- Last Status Change Time: Specifies the time that the last status change was performed on the device.
- Next Status Poll Time: Specifies the time that the next status check is scheduled for the device.
- State: Indicates whether monitoring is enabled for the device. The server has the ability to monitor the discovered devices on a periodic basis, to check for any change in state, and to update the database server with the latest changes.
- Interval in seconds: Specifies the frequency (in seconds) in which discovered devices are polled for state.
- Status Polling: You can enable or disable status polling and set the interval of polling the device for status.
  To configure status polling, click the Edit icon and configure the following parameters:
  - State: Indicates whether monitoring is enabled for the device. The server monitors the discovered devices on a periodic basis to check for any change in state and to update the database server with the latest changes.
  - Interval in Seconds: The frequency (in seconds) in which discovered devices are polled for their status.

Configuration Changes on CloudBridge Devices

Use Command Center to view the details of the archived files in the database as well as configuration files for the current

time. Under Archived Details, view the following details:

- Time: Specifies the time at which a configuration change was made.
- Restore Configuration: Click Restore Configuration against a timestamp to restore the previous version of the configuration file. On the Restore Configuration page, in Annotation, type a message to describe why you want to restore the configuration, and then click Submit.
- Comments: Specifies the comments on the configuration change.
- Download: Download the configuration files to your local system.
- Backup Config: You can download and archive the configuration and license files at the current time. To do this, click Backup Config. The files are downloaded and archived in the database. The status of this download is displayed in the table under Archived Details. The Comments column displays "File downloaded on user request".

Running Reports

You can run a custom report of any polled counters to troubleshoot or analyze the behavior of a device.

To run reports

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the devices on which you want to run a report, and from the Action drop-down list, select Run Report. Alternately, right-click the device, and then click Run Report .
   Note: You can also run a report on all devices in a map or pool. For more information, see Performing Operations on a Map.
3. Under Select Instances, provide the appropriate information about the virtual servers and services as needed.
4. In Period, select the time interval for which you want to view the specified counter. If you select Custom, select the Start Date and End Date. Note: The values specified in Period are displayed only in the top chart. By default, two other charts are plotted for hourly and daily average data for the counters selected in the previous steps. These two other charts are plotted for a time duration of 3 months and 1 year, respectively. You can change the duration using the Settings option on the View Graph page.
5. If you want to view only those counters with non-zero values, select the Exclude zero values check box, and then click OK. Note: On the View Graph page, you can perform additional tasks, such as customizing graph series, changing the scale, modifying the report settings, and refreshing the report. For more information, click Help on the View Graph page.

Viewing Events and Alarms

When the IP address of the Command Center server is added to the list of trap destinations on a discovered device, the device routes all events or traps to Command Center.
Command Center correlates the history of events to form alarms for different severity levels and displays the events as messages, some of which may require immediate attention. For more information, see Fault.

From the Citrix Network tab, you can view the events and alarms for single devices.

To view events and alarms

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Events or Alarms . Alternately, right-click the device, and then click Events or Events .

Executing Tasks

You can simplify device management and minimize configuration errors by using built-in and custom tasks to make

configuration changes across devices, upgrade firmware, and replicate a device's configuration to other devices on your network.

You can execute tasks on single or multiple devices on the Citrix Network tab.

To execute tasks on Citrix devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and from the Action drop-down list click Execute Task .
3. Under Execute Task, in Task Type, click Built-in or Custom.
4. In Task Name, click the name of the task you want to execute.
   Note: Depending on the task you select, type the required values in User Inputs and Annotation Details.
5. Click Preview if you want to preview the details of the task you are executing, and then click OK.

Running Configuration Audits

Run configuration audits on Citrix devices to monitor configuration changes across managed NetScaler devices, troubleshoot configuration errors, and recover unsaved configurations upon a sudden system shutdown. Use Audit Policies to generate audit reports based on your requirements. Using these reports, you can monitor the configuration change events for each device on which an audit policy is executed.

To run configuration audits on Citrix devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and from the Action drop-down list select Config Audit. Alternately, right-click the device, and then click Config Audit.
3. Under Config Audit, in Audit Policy Name, click the name of the audit policy you want to execute to generate the audit report.
4. Click OK.

Invoking the CLI of NetScaler Devices

You can launch the Citrix NetScaler CLI for a selected NetScaler device by using Command Center. From the CLI, you can configure and manage various features of the Citrix NetScaler system.

To invoke the CLI of NetScaler devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Invoke CLI. Alternately, right-click the device, and then click Invoke CLI.
3. On the CLI Credentials page, in User Name and Password, type the user name and password of the device, and then click Login.

Invoking the User Interface of NetScaler Devices

You can use Citrix Command Center to launch the browser-based NetScaler user interface for a selected device. You can use the user interface to launch the configuration utility, dashboard, monitoring, and reporting tools of any NetScaler device (which also includes NetScaler Gateway and NetScaler VPX devices).

To invoke the user interface of NetScaler devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Configuration Utility. Alternately, right-click the device,

and then click Configuration Utility.
Note: This option works only if the client computer is able to reach the selected Citrix NetScaler device; therefore, you must ensure that network connectivity exists between the client and the Citrix NetScaler IP (NSIP) address.

Invoking the CLI and User Interface of CloudBridge Devices

You can launch the Citrix CloudBridge CLI for a selected CloudBridge device by using Command Center. From the CLI, you can configure and manage various features of the Citrix CloudBridge device.

To invoke the CLI of CloudBridge devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Invoke CLI. Alternately, right-click the device, and then click Invoke CLI.
3. On the WS CLI Credentials page, type the user name and password of the device, and then click Login.
   You can launch the Web user interface for a selected CloudBridge device by using Command Center.

To invoke the user interface of CloudBridge devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Configuration Utility. Alternately, right-click the device, and then click Configuration Utility.

Generating the Tar Archive of Configuration Data of NetScaler Devices

You can use the Show TechSupport option to generate a tar archive of system configuration data and statistics for submission to Citrix technical support. After the tar archive file (support.tgz) is generated on the NetScaler, it is downloaded to the Command Center server with the NetScaler IP address used for the file name prefix (for example, NetScalerIP_support.tgz). You can then download the file to your local system.

To generate the tar archive of configuration data of NetScaler devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Show TechSupport. Alternately, right-click the device, and then click Show TechSupport.
3. In the Show TechSupport window, click Generate. The archive file is generated and downloaded to the Command Center server.
4. Click click here to save the tar archive file to your local system.

Replicating a NetScaler Device's Configuration to Other NetScaler Devices

You can use Command Center to replicate the configuration of a NetScaler device to multiple NetScaler devices on your network to save time and minimize configuration errors. Command Center does not propagate node- or device-specific details, such as NetScaler IP addresses.
Note: The replicate configuration functionality is not supported for a NetScaler cluster or for NetScaler devices in a high availability pair.

To replicate configuration of a NetScaler device

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the NetScaler device, right-click the device, and then click Replicate Configuration.
3. Under Replicate Configuration, in **Available Device(s)**, select the devices to which you want to replicate the selected

configuration, and then click the right arrow.

4. In Annotation, type a message describing the reason for replication, and then click OK.
5. The Replicate Configuration Status window is displayed and you can view the following details:
   - Annotation: Specifies the message describing the reason for replication, which you had typed when replicating configuration to this device.
   - Command: Specifies the configuration command that was executed during replication. Clicking the command displays the details of the command on the Execution Details page. Also, you can view and download the configuration status of the batch commands executed.
   - Device Name: Specifies the IP address of the source or destination device on which the command is executed.
   - Start Time: Specifies the time when configuration replication had started.
   - Finish Time: Specifies the time when configuration replication finished.
   - Status: Specifies the status of the configuration replication, which can be either Success or Failed.

   Note: To view the configuration of the device before replicating, click on the device and click Show Configuration from the menu.

Replicating a CloudBridge Device's Configuration to Other CloudBridge Devices

You can use Command Center to replicate the configuration of a CloudBridge device to multiple CloudBridge devices on your network to save time and minimize configuration errors. Command Center replicates only configuration commands, such as service classes and SNMP trap destinations, that may be applied to other CloudBridge devices. Command Center does not propagate node- or device-specific details, such as IP addresses.

To replicate configuration of a CloudBridge device

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the CloudBridge device, right-click the device, and then click Replicate Configuration.
   Note: You cannot replicate the configuration of a CloudBridge instance hosted on a CloudBridge Advanced Platform device.
3. Under Replicate Configuration, in **Available Device(s)**, select the devices to which you want to replicate the selected configuration, and then click the right arrow.
4. In Annotation, type a message describing the reason for replication, and then click OK.
5. Under Replicate Configuration Status, you can view the following:
   - Annotation: Specifies the message describing the reason for replication, which you had typed when replicating configuration to this device.
   - Command: Specifies the configuration command that was executed during replication. Clicking the command displays the details of the command on the Execution Details page.
   - Device Name: Specifies the IP address of the source or destination device on which the command is executed.
   - Start Time: Specifies the time when configuration replication had started.
   - Finish Time: Specifies the time when configuration replication finished.
   - Status: Specifies the status of the configuration replication, which can be either Success or Failed.

   Note: To view the configuration of the device before replicating, click on the device and click Show Configuration from the menu.

Viewing the Replication Status of Devices

You can view the status of a configuration that has been replicated from a Repeater device to one or more Repeater devices or from a NetScaler device to one or more NetScaler devices. The replication status can be viewed only for those devices from which configurations have been replicated.

To view the replication status

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Replication Status. Alternately, right-click the device, and then click Replication Status.
3. Under Replication Status, you can view the following details:
   - Settings : Opens the Settings box for specifying how often you want Command Center to update the replication status page in seconds. By default, the refresh interval is set to 10 seconds.
   - Refresh : Refreshes the replication status page at the current time.
   - Show Source Device : Selecting this check box displays the IP address and status of the source device from which the configuration was replicated.
   - Device Name : Specifies the IP address of the source and destination devices. Clicking the IP address displays the status of each command that was executed on that device during replication.
   - Start Time : Specifies the time when configuration replication had started.
   - End Time : Specifies the time when configuration replication finished.
   - Executed By : Specifies the Command Center user who executed the replication.
   - Status: Specifies the status of the configuration replication, which can be either Success or Failed.
   - Annotation: Specifies the message describing the reason for replication, which you had typed when replicating configuration from or to this device.

Viewing the Device Configuration of CloudBridge Devices

You can view the running configuration of standalone and high availability (HA) primary CloudBridge devices.

To view the device configuration of CloudBridge devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Show Configuration. Alternately, right-click the device, and then click Show Configuration.
   Note: For an HA pair, click the primary device, and then click Show Configuration.

Searching Devices from Device Inventory

You can search for any discovered NetScaler, NetScaler VPX, NetScaler Gateway, CloudBridge, CloudBridge VPX, NetScaler SDX, CloudBridge Platform, or Xen Server device on your Citrix network.

To search devices from Device Inventory

1. On the Citrix Network tab, in the left pane, click Device Inventory, or expand Device Inventory, and click the device type.
2. In the right pane, click Search.
3. In the search pane, use the drop down list to select the filter criteria. Enter the search keyword in the text box. You can also use the reserved characters to define the search keyword. To view the supported reserved characters, see Search Syntax Reference, next.

Search Syntax Reference

You can search for devices, events, alarms, syslogs, AppFirewall logs, and entities in Command Center on the basis of filters that you create. The following table lists the functions of the reserved characters that you can use to create filters.

Search Syntax		Examples	

Character Search Syntax	Definition /Usage	Pattern Examples	Sample Matches
*	Use when you want to match zero or more characters of the keyword.	Module - Device Inventory Search criterion - Type Search keyword - stand*	All the devices whose state is STANDALONE
!	Use when you want to exclude the characters of the keyword.	Module - Device Inventory Search criterion - Type Search keyword - !stand	All devices whose state is not STANDALONE
,	Use as a separator between multiple values for a filter criterion.	Module - Device Inventory Search criterion - Name Search keyword - 10*,*56	All devices whose Name starts with '10' or ends with '56'. Sample matches : 10.234.123.56 and 12.123.23.56

Restarting Devices

You can restart a device after performing tasks such as changing the configuration or upgrading the system.

To restart devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Reboot. Alternately, right-click the device, and then click Reboot.
   Note: For an HA pair, click the primary or secondary device, and then click Reboot.

Pinging Devices

You can ping a device to check whether the device is reachable from the Command Center server.

To ping devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and from the Action drop-down list click Ping. Alternately, right-click the device, and then click Ping.
3. Under Ping , you can view the ping statistics for the device.

Tracing the Route of Devices

You can trace the route of a packet from the server to a device through a network by determining the number of hops necessary to reach the device.

To trace the route of devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and from the Action drop-down list, select Trace Route. Alternately, right-click the device, and then click Trace Route.

Viewing the Discovery Status

You can view the cause of failure of the discovery of a device on the Device Status page. You can view the step that has failed and the reason why the step has failed. Depending on the type of error, you must take corrective measures, and then initiate rediscovery of the device. For information about the discovery process, see Understanding the Discovery process.

To view the discovery status of devices

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices > Discovery Status.

Rediscovering Devices

You may want to set a device(s) for rediscovery when you need to view the latest state of the device and its configuration file. Or, you may want to set a device for rediscovery if the device has moved to the Inaccessible Systems node.

During rediscovery, the Command Center server fetches the configuration and license files of the device, and archives them in its file system. By default, Command Center schedules devices for rediscovery once every hour. You can configure the rediscovery interval according to your preference. For instructions on how to set the rediscovery interval, see Configuring the Discovery Settings.

To rediscover devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and from the Action drop-down list, select Rediscover. Alternately, right-click the device, and then click Rediscover.

De-Provisioning NetScaler VPX on NetScaler SDX Platform

Using Command Center you can de-provision the NetScaler VPX instances that are provisioned on NetScaler SDX Platform.

Note: You cannot de-provision the NetScaler instances installed on NetScaler SDX models 19555, 17555, 11505, and 13505.

To de-provision NetScaler VPX devices on a NetScaler SDX Platform

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the NetScaler SDX device on which you want to de-provision the NetScaler VPX devices, and then click Device Properties. Alternately, right-click the NetScaler SDX device, and then click Device Properties.
3. Under NetScaler Instances, click the De-Provision icon for the NetScaler instance to be deprovisioned.
4. In the confirmation window, click OK.

Deleting Devices

If you do not want to manage and monitor a device, you can delete that device. Deleting a device permanently removes the device and its related details from the database of the Command Center server. With an HA pair, you can delete only the HA pair parent and not individual members.

To delete devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, and click Devices.
2. In the right pane, under Devices, select the device, and then click Delete. Alternately, right-click the device, and then click Delete.

Unmanaging Devices

You can stop managing a device and stop the exchange of information between the device and the Command Center server.

To unmanage devices

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the device, and then click Unmanage. Alternately, right-click the device, and then click Unmanage.

Performing Operations Specific to HA Devices

Command Center supports devices configured in high availability mode where the primary device processes the traffic and the secondary device monitors the primary and takes over the functions of the primary device if that device is unable to continue processing traffic. You can perform a set of operations specific to the HA devices, such as forcing a failover and forcing a secondary to stay as a secondary, described in the following two sections.

Doing a Force Failover

You can force a primary device in an HA pair to fail and a secondary device to take over as the primary system. In this mode, a secondary system runs as a hot standby to a primary. This allows the secondary system to automatically take over the functions of the primary system if the primary has a failure that prevents it from processing additional network traffic. Failover: When two devices are operating as an HA pair, one device is configured as the primary device and the other is configured as the secondary device. The secondary device sends periodic hello messages to the primary device to check whether it is operating. If the primary does not reply, the secondary device retries the connection with the primary for a specified time period. If the secondary device fails to re-establish communication, it determines that the primary system is not functioning as expected, and takes over as the new primary device. This process is known as failover

After a failover, all client connections must be re-established; however, the session persistence rules set before the failover are maintained after a failover.

To force a failover

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the HA pair, and then from the Action drop-down list, select Force Failover. Alternately right-click the HA pair, and then click Force Failover.
3. Under Confirm, click Yes to do a force failover.
   The failover starts on the HA pair. If the force failover is successful, a confirmation message appears.

Staying as Secondary on Secondary Devices

In an HA setup, you can force the secondary node to stay as a secondary node independent of the state of the primary. For example, in an existing HA setup you may need to upgrade the primary node. During the upgrade, the primary node may restart to complete the upgrade process. In such a situation, you do not want the secondary to take over as the primary node. Instead, the secondary node must remain as secondary even if there is a failure on the primary node.
To configure the secondary device

1. On the Citrix Network tab, in the left pane, expand Device Inventory, click Devices.
2. In the right pane, under Devices, select the secondary device, and from the Action drop-down list, select Stay as Secondary. Alternately, right-click the secondary device, and then click Stay as Secondary.
3. Under Confirm, click Yes.

Performing Operations Specific to NetScaler Cluster

You can now configure and manage NetScaler clusters from Command Center console. You can configure a cluster from the scratch or add a configured cluster to Command Center and then, start managing the NetScaler cluster from Command Center console. The NetScaler Cluster is represented as **NS CL** and the device type of a cluster node is represented as 'Cluster Node' in the Citrix Network page.

A NetScaler cluster is a group of NetScaler devices working together as a single device. Each device of the cluster is called a *node*. A NetScaler cluster can include as few as two or as many as 32 NetScaler nCore hardware or virtual appliances as nodes. The traffic is distributed among the cluster nodes to provide high availability, high throughput, and scalability.

You can perform various tasks to manage and monitor the device from the Command Center console:

- Discovering a NetScaler Cluster
- Adding a Nodes to the NetScaler Cluster
- Removing the Nodes from NetScaler Cluster
- Removing a Cluster Instance

Discovering a NetScaler Cluster

To add a NetScaler cluster for discovery by Command Center, you can specify the Cluster IP address or the IP address of any of nodes in the cluster. Command Center implicitly discovers the entire set of devices participating in the cluster and adds them to its database.
To discover a NetScaler Cluster

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices.
2. In the right pane, click Add.
3. Under Add Device, in the **Devices** text box, type the cluster IP address, or the host name, or IP address of any of the cluster nodes participating in the cluster configuration.
   Note: If a NetScaler cluster has more than one cluster IP address, then only one of the cluster IP address will be discovered.
4. Under Device Profile, select a NetScaler profile you want to use.
5. Click **OK**.

Adding a Node to the NetScaler Cluster

You can add additional nodes to the NetScaler Cluster from Command Center. Before you can add cluster nodes from Command Center, you must add the NetScaler devices to Command Center, and then configure these devices as nodes in the cluster.
To add a node to the NetScaler Cluster

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices .
2. In the right pane, click the NetScaler Cluster to which you want to add an additional node, and then from the Action drop-down list click Add Cluster Node. Alternately, right-click the NetScaler Cluster and click Add Cluster Node.
3. Under Create Cluster Node, set the following parameters.
   - **Node IP.** Select the IP address of the NetScaler device you intend to add as cluster node.
     Note: You can only select the NetScaler devices which have been discovered by Command Center. If you wish to add a NetScaler device as a node, first add the device to Command Center and then configure the device as a cluster node.
   - **Node ID.** A unique number that identifies the appliance on the cluster. Each node must have a different node ID. Minimum value: 0. Maximum value: 31.
   - **State**. The configured state of the cluster node. Possible values: ACTIVE, PASSIVE, SPARE. Default: PASSIVE.
   - **Back Plane**. Backplane interface of the node. For example, if node 0 uses interface 1/1, the value of this parameter is 0/1/1. If node Id is 1, back plane will be 1/1/1. It is a combination of node id/interface/port number.
4. Click Create. The NetScaler device is configured as a cluster node.

Removing the Nodes from NetScaler Cluster

If you want remove an existing cluster node from the cluster configuration, you can remove that node from Command Center console. Removing the node from the cluster removes the node from the cluster, but not from the Command Center server.

To remove a cluster node from NetScaler Cluster

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices.
2. In the right pane, do one of the following:
   - Navigate to the Device Properties page of the NetScaler Cluster and under **NetScaler Cluster Nodes**, click the remove icon for the node to be removed.
   - Select the cluster node you wish to remove from the cluster and click Remove Cluster Node. Alternately, right-click the cluster node and click Remove Cluster Node from the options.
3. Under Confirm, click OK.

After you remove a node from a NetScaler Cluster, the device is re-discovered as a standalone NetScaler device in Command Center and no longer participates in the cluster configuration. The cluster node is no longer mapped in the device properties page of NetScaler Cluster.

Removing a Cluster Instance

Removing a NetScaler Cluster from Command Center deletes the cluster configuration (Cluster IP and all the nodes) and also deletes Cluster IP from the database of the Command Center server. The nodes participating in this cluster configuration are re-discovered as standalone NetScaler devices in Command Center.

To delete a NetScaler Cluster configuration

1. On the Citrix Network tab, in the left pane, under Device Inventory , click Devices .
2. In the right pane, select the NetScaler Cluster you wish to remove, and click Remove Cluster Instance. Alternately, right-click the cluster node and click Remove Cluster Instance from the options.
3. Under Confirm, click OK.

If you want to stop managing and monitoring a NetScaler cluster, you can delete it from Command Center. Deleting a NetScaler cluster does not change the cluster configuration but only removes the device and its related details from the database of the Command Center server. To delete a device from Command Center, see Deleting Devices

Monitoring Your Network by Using the Home Page

May 26, 2015

The Command Center Home page provides you with a high-level view of the performance of your Citrix network. The Home page contains graphical and tabular representation of the following statistics about your devices on the network:

- **Alarm Summary:** An aggregate view of the alarms for all of the discovered devices in your network.
- **Inventory:** Summary of alarm status for each device category, such as NetScaler or NetScaler Gateway.
- **Active Alarms:** Graphical representation of the number of currently active alarms by their severity.
- **My Assignments:** List of alarms assigned to you. You may pick up alarms to resolve them, or you may unpick the alarms and assign them to other users.
- **System Overview:** Summary of the configurations that you have performed on Command Center.

This topic includes the following details:

Understanding the Alarm Summary

The Alarm Summary table is an aggregate view of the alarms for all the discovered devices on your network. This aggregate is based on the categories and severity of the alarms. The table is updated automatically.

The alarm details include the date and time the alarms was generated, the severity, and the actions.

For information about the color codes of the alarms, see Monitoring Active Alarms.

To view the alarm details for a particular category of alarms, click the category name in the table. On the Alarms page, you can view the following details:

- Date/Time: Specifies the date and time when the alarm was generated.
- Severity: Specifies the severity of the alarm, such as Major and Warning.
- Actions: Specifies the actions you can take on the alarms. The possible actions are Alarm Pickup and Annotate.
- Category: Specifies the alarm category, for example, vserverTxBytesRate.
- Source: Specifies the system name, host name, or the IP address of the device on which the alarm is generated.
- Failure Object: Specifies the object on which the alarm is raised.
- Description: Specifies the description of the alarm.

Monitoring Device Inventory

Updated: 2014-02-06

The Inventory view is a table listing the device types and the alarm status of all devices on the network. It also displays the total number of devices (discovered and inaccessible) managed by Command Center.

- The first column lists the device types and the number of discovered and inaccessible devices for each device type. The device types listed are: NetScaler, NetScaler Gateway, NetScaler Cluster, NetScaler SDX Platform, CloudBridge,

CloudBridge Advanced Platform, and XenServerNetScaler, NetScaler Gateway, ByteMobile Traffic Generator, NetScaler Cluster, NetScaler SDX Platform, CloudBridge, CloudBridge Advanced Platform, and XenServer. Clicking the device type displays the details of all the devices in that category.

- The second through sixth columns display the number of devices (for each device type) with the alarm severity depicted by the alarm color code. For information on alarm color code, see Monitoring Active Alarms. Clicking any of the numbers in these columns displays the details of devices with pending alarms or no pending alarms, as is applicable.
- The last column displays the number of inaccessible devices for each device type. For information on inaccessible systems, see Viewing Inaccessible Devices. Clicking a number in the last column displays the inaccessible devices for the corresponding category.

On clicking any of the columns, you can view the following details of the devices:

- **Name:** Specifies the IP addresses of the devices.
- **Status:** Specifies the status of the alarms for each device - critical, major, minor, warning, or clear.
- **Type:** Specifies the type of device, such as NetScaler VPX, NetScaler MPX or NetScaler Instance.
- **State:** Specifies the type of device, such as Standalone or Primary.
- **Build Version:** Specifies the release version, build version, and date and time of the build.
- **Host Device**: Specifies the host name on which the device is hosted.
- Host Name: Specifies the host name of the device.

Monitoring Active Alarms

The Active Alarms view is a pie chart representation of the number of currently active alarms, segmented and color coded on the basis of their severity. The following table lists the color codes of the alarms.

ALARM	COLOR CODE
Critical	Red
Major	Amber
Minor	Yellow
Warning	Cyan
Clear	Green

To view the details of the active alarms of a particular severity, click that segment of the pie chart. Under Alarms, you can view the following details:

- Date/Time: Specifies the date and time when the alarm was generated.
- Severity: Specifies the severity of the alarm, such as Major and Warning.
- Actions: Specifies the actions you can take on the alarms. The possible actions are Alarm Pickup and Annotate.
- Category: Specifies the alarm category, for example, vserverTxBytesRate.
- Source: Specifies the system name, host name, or the IP address of the device on which the alarm is generated.

- Failure Object: Specifies the object on which the alarm is raised.
- Description: Specifies the description of the alarm.

Note: Click My Assignments to view a list of alarms assigned to you. You may resolve the alarms assigned to you, or you may unpick the alarms and assign them to other users.

Monitoring Recent Alarms

The Recent Alarms view is a list of the 5 most recent alarms, represented in a table with the following details:

- Date/Time : Specifies the date and time when the alarm was generated.
- Severity: Specifies the severity of the alarm, such as Major and Warning.
- Category: Specifies the alarm category, for example, vserverTxBytesRate.
- Source: Specifies the system name, host name, or the IP address of the device on which the alarm is generated. To view the properties of the device for which an alarm appears, click the IP address of the device.
- Description: Specifies the description of the alarm. To view the alarm properties, click the alarm description.

Monitoring System Settings

Updated: 2014-04-18

The System Overview table is an aggregate view of the settings you have configured on Command Center. You can click the links to directly navigate to the modules and view the configuration pages.

To view the system overview details for a particular setting, click the setting on the table. When you click the setting you can view the details of all the settings you have configured.

Monitoring and Managing Events Generated on Citrix Devices

May 28, 2015

Use the Fault tab in Command Center to monitor and manage the SNMP and syslog events generated on the Citrix devices. Command Center identifies errors or events based on the real-time status of the devices. It further generates alarms for the identified events, thereby helping administrators to address issues immediately and keep the network running effectively. You can also configure event triggers to filter the events generated by Command Center and take actions on the filtered list of events.

In this section:

Monitoring SNMP Events and Alarms

May 26, 2015

When the Command Center server adds its IP address to the list of trap destinations on a discovered device, the device routes all events or traps generated on it to Command Center. From these SNMP trap notifications, the Command Center server automatically consolidates a list of the events that occur on the discovered devices.

Command Center correlates the history of events to form alarms of different severity levels and displays them as messages, some of which may require immediate attention. The alarms are correlated for similar kinds of events. For example, for events linkUp and linkDown of the same entity Link occurring in the same device, only one alarm is generated, stating the latest status and the severity of the event.

Each event stored in Command Center occupies approximately 250 bytes of space. Command Center stores the events of six months and displays only the latest 10,000 events and alarms.

This topic includes the following details:

- Viewing Events
- Viewing Alarms
- Configuring Views for Events and Alarms
- Searching Events and Alarms
- Scheduling a Filter

For information about NetScaler SNMP OIDs, traps, and system health counters, see NetScaler SNMP OID Reference.

Viewing Events

Updated: 2014-10-17

Events represent occurrences of events or errors on Citrix devices. For example, when a failure or fault is detected on a Citrix device, an event occurs. The Command Center server collects information about these events.

To view events

1. On the Fault tab, in the left pane, under SNMP, click Events.
2. In the right pane, under Events, view the following:
   - Severity: Specifies the severity of the event, such as critical, major, warning, minor, or clear.
   - Source: Specifies the IP address, the system name, or the host name of the device on which the event is generated ,based on the device label configuration. For more information about configuring the device label, see Configuring Server Settings.
   - Date: Specifies the date and time when the event was generated. The date format is MMM DD, YYYY HH:MM:SS AM/PM.
   - Category: Specifies the category of the device to which the event belongs, such as discovery standalone, inaccessible system, or a discovery HA pair.
   - Description: Specifies the message associated with the event, such as "Command: save ns config Authorization Status: AUTHORIZED Result: SUCCESS User: nsroot."
     For SNMP authentication failures, the message also displays the IP address and port value of the device that failed authentication.

For any entity-related UP, DOWN, or OUT OF SERVICE traps, the description also displays the entity IP address and port value along with the entity name.

Viewing Alarms

Command Center correlates the history of events to form alarms of different severity levels and displays them as messages, some of which may require immediate attention. The alarms are correlated for similar kinds of events. For example, for events linkUp and linkDown of the same entity Link occurring in the same device, only one alarm is generated, stating the latest status and the severity of the event.

You can view either all the alarms for all the events, or view the alarm associated with an event.

To view all alarms

1. On the Fault tab, in the left pane, expand SNMP, click Alarms.
2. In the right pane, under Alarms, view the following:
   - Date/Time: Specifies the date and time when the alarm was generated (that is, the latest time of the occurrence of the event associated with the alarm). The date/time format is MM DD, YYYY HH:MM:SS AM/PM.
   - Severity: Specifies the current severity of the alarm—critical, major, minor, warning, info, or clear.
   - Category: Specifies the type of alarm (for example, Entitydown or linkDown).
   - Source: Specifies the IP address or the system name of the device on which the events that caused the alarm occurred., based on the device label configuration. For more information about configuring the device label, see Configuring Server Settings.
   - Failure Object: Specifies the object that triggered the alarm (for example, entity).
   - Description: Specifies the properties (for example, alarm creation date, last updated date, and current and previous severity) of the alarm, with a detailed message.
   - Actions: Specifies the permitted actions (for example, annotate and pickup) that you can perform on the alarm.

To view alarms for an event

1. On the Fault tab, in the left pane, expand SNMP, click Events.
2. In the right pane, under Events, click the event for which you want to view the alarm, and then click Alarm. Alternately, right-click the view, and click Alarm.

Configuring Views for Events and Alarms

You can configure views to monitor specific events and alarms based on the criteria you specify.

Views make it easier to monitor a large number of events generated across your NetScaler infrastructure. For example, you can create a view to monitor all major events raised when there is a high CPU usage.

In this section:

- Adding Views for Events and Alarms
- Modifying Views
- Deleting Views

Adding Views for Events and Alarms

You can add different views for the events and alarms you monitor. These views are based on various filter criteria, such as

severity, devices, and categories.

To add views for events and alarms

1. On the Fault tab, in the left pane, under SNMP, click Events or Alarms.
2. Under Eventsor Alarms, navigate to Views and click Add .
3. Under Create Event View, in Name, type a view name. The view name is unique and user-defined.
4. In Device Type, select the type of device, such as NetScaler, CloudBridge, NetScaler VPX, and CloudBridge VPX.
5. In Severity, select the severity level of the events or alarms for which you want to add the view
6. For an alarm view, in Previous Severity, select the severity level that the alarm had earlier. Note: Due to event correlation an alarm goes through various severity levels. The Previous Severity option filters the alarms based on the previous severity level.
7. In Devices, click the icon next to the text box to select the IP address(es) of the discovered NetScaler or CloudBridge devices for which you want to define a view
8. In Categories, click the icon next to the text box to select the categories of events or alarms generated by the managed devices.
9. In Failure Objects, either type the entity instances or counters for which an event or alarm has been generated, or click the icon next to the text box to select the entity instances. Note: This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events. For threshold-related events, the instances should match the incoming traps, as described in the following table.
10. In Filter based on event description type a message that lets you further narrow the filter to events or alarms that meet specific criteria. The message should match the incoming trap. For example, if you want to view all events that are generated when a feature or entity is enabled, type Command: enable*. And, if you want to view all events generated by a particular user for the selected category, type *User: UserName. Note: If you are not sure of the format of the message to type, you can copy the format of a similar category from the Message field in the Network Events or Alarms pane.
11. In From Time and To Time, click the calendar icon to specify the date and time during which the events or alarms are generated.
12. In Event Age or Alarm Age, specify the age of the alarm based on which you want to filter the view.
13. In Refresh Period in Minutes, type the time interval after which you want Command Center to refresh the view.

Threshold Instance Formats

Group Name	Instance Format
Interface	InterfaceName Example: L0/1
Content Filters	ContentFilterName Example: Cfilter1
VLAN	VLANID Example: 102

Policy Engine **Group Name**	PolicyName **Instance Format**
	Example: Pol1
Services	ServiceName(ServiceIPAddress:ServicePort) Example: svc1(1.1.1.1:8080)
Virtual Servers	VserverName(VserverIPAddress:VserverPort) Example: vsvr(10.102.31.80:8443)
Virtual Services	(VserverName:ServiceName) Example: vsvr:svc1
Content Switch policies	(VserverName:ContentSwitchPolicyName) Example: vsvr:cspol1
Cache Redirection Policies	VserverName:CacheRedirectionPolicyName Example : vsvr1:crpol1
ACL Table	ACLName Example: acl1
CPU Usage	CPUName Example: cpu0
Service Groups	ServiceGroupMemberName(Weight:ServiceGroupMemberWeight) Example: svcg1(Weight:1)
ACL6 Table	ACL6Name(Priority:ACL6Priority) Example: aclRule1(Priority:25)
System Health	SystemHealthCounterName Example: CPUFan0Speed
System Disks	SystemHealthDiskName

Group Name	Instance Format
	Example: /var
CloudBridge Service Classes	ServiceClassName Example: HTTP (Private)
CloudBridge ICA Traffic	Priority Example: 5

Modifying Views

After creating views, you can modify the filter criteria of the views.

To modify views

1. On the Fault tab, in the left pane, under SNMP, expand Events or Alarms.
2. Under Events or Alarms, click the view you want to modify.
3. In the right pane, click Modify....
4. Under Modify View, make changes to the values as required, and then click OK.

Deleting Views

You can delete a view if you do not want to use it again.

To delete a view

1. On the Fault tab, in the left pane, under SNMP, expand Events or Alarms.
2. Under Events or Alarms, click the view you want to modify.
3. In the right pane, click Delete.

Scheduling a Filter

Updated: 2015-04-03

After creating a filter, if you do not want the Command Center server to send email notifications every time the alarm or event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals. You can specify daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your devices at different times, the devices 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 Command Center server receives these traps. If you want the server to send these email notifications during only a specific time period, you can do so by scheduling a filter.

To schedule a filter

1. On the Fault tab, in the left pane, under SNMP, click Alarms or Events, and then click Triggers.
2. In the right pane, select a trigger and click Schedule a Filter.

To view scheduled filters

1. On the Fault tab, in the left pane, under SNMP, click Alarms or Events, and then click Triggers.
2. In the right pane, select a trigger and click Scheduled Filters.

Searching Events and Alarms

Updated: 2013-07-22

You can use the search option to search for events and alarms based on different criteria that you provide.

To search for events and alarms

1. On the Fault tab, in the left pane, under SNMP, click Events or Alarms.
2. In the right pane, under Events or Alarms, click Search icon.
3. In the search pane, use the drop down list to select the filter criteria. Enter the search keyword in the text box. You can also use the logical operators to define the search keyword.
4. Click **+** icon or press Enter key to add the criteria, and then click Refine Search. The search results are displayed.

Managing SNMP Events and Alarms

May 28, 2015

You can manage the events generated on all your devices from the Command Center console. You can set a time interval for which you want Command Center to poll the events. You can assign alarms to Command Center users to analyze and resolve them. You can also print the list of events and alarms for analysis, or save the list of events and alarms to a file on your local system.

This topic includes the following details:

Assigning Alarms to Users

You can assign alarms to Command Center users who can analyze these alarms and resolve them.

To assign alarms to users

1. On the Fault tab, in the left pane, under SNMP, click Alarms.
2. In the right pane, under Alarms, select the alarms that you want to assign, and then click Assign To.
3. Under **Assign To**, select the user name to which you want to assign the alarm.
4. In Annotation, type a message describing the reason why you are assigning the alarm, and then click OK.

Viewing and Managing Alarms Assigned to a User

You can view and manage the alarms assigned to you. You may resolve the alarms, or you may unpick the alarms and assign them to other users. When you unpick an alarm, it becomes available for assignment to other users.

To view the alarms assigned to a user

1. On the Fault tab, in the left pane, under SNMP, click My Assignments.
2. In the right pane, under My Assignments, you can view the following details of the alarms assigned to you:
   - Date/Time: Specifies the date and time when the alarm was generated (that is, the latest time of the occurrence of the event associated with the alarm). The date/time format is MM DD, YYYY HH:MM:SS AM/PM.
   - Severity: Specifies the current severity of the alarm—critical, major, minor, warning, info, or clear.
   - Actions: Specifies the permitted actions (for example, annotate and pickup) that you can perform on the alarm.
   - Category: Specifies the type of alarm (for example, Entitydown or linkDown).
   - Source: Specifies the IP address of the device on which the events that caused the alarm occurred.
   - Failure Object: Specifies the object that triggered the alarm (for example, entity).
   - Description: Specifies the properties (for example, alarm creation date, last updated date, and current and previous severity) of the alarm, with a detailed message.

Printing a List of Events and Alarms

You may want to print a hard copy of the list of events or alarms.

To print a list of events and alarms

1. On the Fault tab, in the left pane, under SNMP, click Events or Alarms.
2. In the right pane, under Events or Alarms, select the events and alarms you want to print, and then click Print.

Saving List of Events and Alarms to a File

You can save a list of events and alarms to your local system in CSV format.

To save list of events and alarms to a file

1. On the Fault tab, in the left pane, under SNMP, click Events or Alarms.
2. In the right pane, under Events or Alarms, click Export.
3. Under Export, do one of the following:
   - If you want to save all the events in your view, click Export entire custom view data.
   - If you want to save only the data on the current page, click Export displayed data.

   Note: When exporting alarms, if you want the annotations to be saved to a file along with the alarms, select Export Annotations.

Assigning Severity to Events

Updated: 2014-04-18

Command Center assigns severity to the events based on default configuration. However, you can reassign severity levels to events that are generated for the devices on the Citrix network. You can configure severity for both generic and enterprise-specific events. You can define the following types of severity levels: Critical, Major, Minor, Warning, Clear, Info, and Unknown.

To assign severity to events

1. On the Fault tab, in the left pane, under SNMP, click Events.
2. In the left pane, under Events, click Severity.
3. Under Severity, click any of the tabs, click the event, and then click Configure Event Severity.
4. In Configure Event Severity, click the severity you want to assign, and then click OK.

Clearing and Deleting Alarms

Updated: 2014-04-29

If you have resolved an alarm or an alarm is no longer valid, you can either clear or delete that alarm.

To clear and delete alarms from the Fault tab

1. On the Fault tab, in the left pane, under SNMP, click Alarms.
2. In the right pane, under Alarms, select the alarms you want to clear or delete, and then click Clear or Delete.

To clear and delete alarms from the Citrix Network tab

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Devices.
2. In the right pane, select a device from the Action drop-down list, and then click Clear Alarms or Delete Alarms.

3. On the Clear Alarms page or Delete Alarms page, under Severity, select one or more check boxes to clear or delete all the alarms for the corresponding severity level.
   After the alarms are cleared, the severity level of each alarm is green.

   Note: The clear check box is selected by default.

Monitoring Syslog Events

Mar 23, 2015

You can monitor the syslog events generated on your NetScaler device if you have configured your device to redirect all syslog messages to the Command Center server. To monitor syslog events, you need to first configure Command Center as the syslog server for your NetScaler.

In this section:

For information about NetScaler Syslog messages, see NetScaler Log Message Reference.

Configuring Command Center as the Syslog Server

To enable Command Center to display syslog messages generated on NetScaler devices, you need to add your Command Center server as the syslog server on the NetScaler device.

To configure Command Center as the syslog server

1. Log on to the NetScaler device
2. To add a syslog action, at the NetScaler command prompt, type:
   add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [- tcp (
   Example
   add audit syslogAction CC_action 10.102.29.70 -serverPort 514 -logLevel ALL -dateFormat MMDDYYYY -logFacility LOCAL0 - tcp ALL -acl DISABLED -timeZone LOCAL_TIM
   Note: The value for serverIP should be the IP address of your Command Center server, and the serverPort should be 514.
3. Add a syslog policy so that all syslog messages are forwarded to the Command Center server. The policy defines the conditions under which the specified syslog server will be used for logging. To add a syslog policy, at the NetScaler command prompt, type:
   add audit syslogPolicy <name> <rule> <action>
   Example
   add audit syslogpolicy CC_pol ns_true CC_action
4. To bind the policy globally, at the NetScaler command prompt, type:
   bind system global <policyName>
   Example
   bind system global CC_pol

For more information about these commands, see Citrix NetScaler Command Reference Guide.

Viewing Syslog Messages

Updated: 2014-04-16

After you have configured your NetScaler device to forward syslog messages to the Command Center server, you can view the syslog messages from the Command Center client.

To view syslog messages

1. On the Fault tab, in the left pane, under Syslogs, click Complete View.
2. In the right pane, under Complete View, you can view the following details:
   - Date/Time: Specifies the date and time when the syslog is generated.
   - Source: Specifies the IP address of the device on which the syslog is generated.
   - Message: Specifies the syslog message that is generated on the NetScaler device (for example, "Nsconf was unable to write a complete config file to disk.").
   - EventID: Specifies the event ID for the syslog message.

Configuring Syslog Views

You can configure views to monitor specific syslog events and based on the criteria you specify.

Views make it easier to monitor a large number of syslog events generated across your NetScaler infrastructure. For example, you can create a view to monitor all critical syslog events raised on log facility local0.

In this section:

Adding Syslog Views

You can add different views for various types of syslog events that are generated on the NetScaler devices monitored on the Citrix network. These views are based on various filter criteria, such as severity, devices, and log facility.

To add syslog views

1. On the Fault tab, in the left pane, under Syslogs, click View.
2. In the right pane, click Add .
3. Under Create Syslog View, enter the following details.
   - Name: The user-defined syslog name. Type a name for the syslog view.
   - Message: The syslog message that is generated. Select the operator, such as equals, not equals, and then type the message for which you want to create the view. Note that the message should be exactly the same as it is generated on the NetScaler device.

- From Date and To Date: The date range when the syslogs are generated. Select the range for which you want to create the view.
- Severity: The log level. Select the severity for which you want to create the view. The possible values are: Alert, Critical, Debug, Emergency, Error, Info, Notice, Warning.
- Source: IP address of the device on which the syslog is generated. Select the IP addresses of the devices for which you want to create the view.
- Facility: The log facility from where the syslog is generated. Select the facility for which you want to create the view. The possible values are: local0, local1, local2, local3, local4, local5, local6, and local7.

Modifying Syslog Views

After creating views, you can modify the filter criteria of the views.

To modify syslog views

1. On the Fault tab, in the left pane, under Syslogs, click **Views**.
2. In the right pane, click the view name you want to modify, and click **Modify**.
3. Under Configure Syslog View, make changes to the values as required, and then click OK.

Deleting Syslog Views

You can delete a view if you do not want to use it again.

To delete syslog views

1. On the Fault tab, in the left pane, under Syslogs, click **Views**.
2. In the right pane, click the view name you want to delete, and then click Delete. Alternately, right click the view name and click **Delete** .

Discarding Syslogs

Updated: 2015-03-23

A large number of syslog records can occupy an excessive amount of the Command Center server space. If you do not want the Command Center server to store obsolete syslog records generated by the devices, you can create a Filter that discards those records.

After you create the filter, the Command Center server discards the syslogs that meet the criteria you specified.

To create a Filter

On the Fault tab, in the left pane, expand Syslogs, click Filters and then click Add.

Configuring Event and Alarm Triggers

Apr 22, 2014

You can filter a set of events or alarms by configuring filters with specific conditions and assigning actions to the filters. When the events or alarms generated meet the filter criteria, the action associated to the filter is executed.

Event triggers enable an administrator to filter the events generated by Command Center and take actions on the filtered list of events. Alarm triggers enable an administrator to filter the alarms generated by Command Center and take actions on the filtered list of alarms. You can also set the time interval to trigger an alarm (in seconds) and priority on a list of filters. The conditions on which you can create the filters are: status, device type, severity, source, failure object, category, and message.

You can assign the following actions to event and alarm triggers:

- Send e-mail Action: Sends an email for the events and alarms that match the filter criteria you specified.
- Suppress Action: Suppresses or drops the events and alarms for a specific time period.
- Run Command Action: Executes a command or a script on the Command Center server for events matching a particular filter criterion. By default, to search for the executable, Command Center looks in the paths defined in the environment variable PATH of the device operating system.

Table 1. Parameters for Run Command Action Script

Parameter	Description
$severity	This parameter corresponds to the state of the event, which corresponds to the severity of the Event.
$text	This parameter corresponds to the "description" field of the events received.
$message	This parameter corresponds to the "description" field of the alarms received.
$entity	The failure object is the key of the Event object. This field affects how the event is processed. Appropriate processing by the trap parser ensures that the failure object reflects the exact problem as notified. This can be used for tracking down the problems quickly and to identify the objects, instead of simply reporting raw events.
$category	This parameter corresponds to the type of traps defined under category of the filter.
$source	This parameter corresponds to the source IP of the managed device.

- Send Trap Action: Sends or forwards SNMP traps to an external trap destination. The values that you configure in Trap Forward Settings (Administration > Trap Forward Settings) are displayed by default. You can configure new values, if required.
- Execute Task Action: Executes a built-in task or a custom task (both NetScaler and CloudBridge), for the events and alarms that match the filer criteria you specified. You can specify the below parameters as task variable values for a

chosen task. During task execution, these parameters will be replaced with actual values.

Table 2. Parameters for Execute Task Action Script

Parameter	Description
$source	This parameter corresponds to the source IP of the managed device.
$failureobject	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.

To configure event and alarm triggers

1. On the Fault tab, in the left pane, under SNMP, click Events or Alarms.
2. In the right pane, under Events or Alarms, click **Triggers**.
3. Under Event Triggers or Alarm Triggers, click Add Filter.
4. Under Add Filter, in Name, type a filter name. The filter name is unique and user-defined.
5. In Status, select either Enable or Disable.
6. In Device Type, select the type of device, such as NetScaler and CloudBridge.
7. In Severity, select the severity level of the events for which you want to add the filter.
8. In Devices, click the icon next to the text box to select the IP address(es) of the discovered NetScaler or WANScaler devices for which you want to define a filter.
9. In Categories, click the icon next to the text box to select the categories of events generated by the managed devices.
10. In Failure Objects, either type the entity instances or counters for which an event has been generated, or enter a part of the entity instance along with a wildcard character, or click the icon next to the text box to select the entity instances. Note: This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events. For threshold-related events, the instances should match the incoming traps, as described in the table.
11. In Filter based on event description, type a message that lets you further narrow the filter to events or alarms that meet specific criteria. The message should match the incoming trap. For example, if you want to view all events that are generated when a feature or entity is enabled, type Command: enable*. And, if you want to view all events generated by a particular user for the selected category, type *User: UserName Note: If you are not sure of the format of the message to type, you can copy the format of a similar category from the Message field in the Events or Alarms pane.
12. Under Filter Action, click Add Action.
13. Under Filter Actions, in Action Type, select the type of action you want to associate with a filter, such as Send e-mail Action, Suppress Action, Run Command Action Send Trap Action and Execute Task Action.
    Note: Click **Test Mail** to check if the mail server credentials provided are accurate and if the mail server is accessible from command center server. If the connection to the mail server is successful, a test mail is sent to the specified email and the settings are saved.
14. In Action Name, type the name of the action, and fill values for various options depending on the action type that you select, and then click OK.

Threshold Instance Formats

Jun 04, 2013

Group Name	Instance Format
Interface	InterfaceName Example: L0/1
Content Filters	ContentFilterName Example: Cfilter1
VLAN	VLANID Example: 102
Policy Engine	PolicyName Example: Pol1
Services	ServiceName(ServiceIPAddress:ServicePort) Example: svc1(1.1.1.1:8080)
Virtual Servers	VserverName(VserverIPAddress:VserverPort) Example: vsvr(10.102.31.80:8443)
Virtual Services	(VserverName:ServiceName) Example: vsvr:svc1
Content Switch policies	(VserverName:ContentSwitchPolicyName) Example: vsvr:cspol1
Cache Redirection Policies	VserverName:CacheRedirectionPolicyName Example : vsvr1:crpol1
ACL Table	ACLName Example: acl1

Group Name	Instance Format
CPU Usage	Example: cpu0
Service Groups	ServiceGroupMemberName(Weight:ServiceGroupMemberWeight) Example: svcg1(Weight:1)
ACL6 Table	ACL6Name(Priority:ACL6Priority) Example: aclRule1(Priority:25)
System Health	SystemHealthCounterName Example: CPUFan0Speed
System Disks	SystemHealthDiskName Example: /var
CloudBridge Service Classes	ServiceClassName Example: HTTP (Private)
CloudBridge ICA Traffic	Priority Example: 5

Monitoring and Managing the Real-Time Status of Entities Configured on NetScaler Devices

May 26, 2015

Use Command Center to monitor and manage the states of virtual servers, services, and service groups across the NetScaler infrastructure. You can monitor values, such as the health of a virtual server and the time elapsed since the last state change of a service or service group. This gives you visibility into the real-time status of the entities and makes management of these entities easy when you have a large number of entities configured on your NetScaler devices.

This topic includes the following details:

Monitoring the Status of NetScaler Devices

Use the NetScaler Dashboard to view the operational status of the NetScaler devices being managed by Command Center. By default, the dashboard data is refreshed every 5 minutes, you can change it by setting the polling interval value in Command Center.

Note: The dashboard does not display the data of NetScaler devices whose state is Failed, or Unmanaged.

To use the Dashboard

1. On the Monitoring tab, in the left pane, under NetScaler, click Dashboard.
2. In the right pane, under Dashboard, you can view the following :
   - Name— The name or IP address of the device
   - CPU Usage (%)— CPU Usage (%)
   - Memory Usage (%)— Memory utilization percentage.
   - Rx (Mbps)— Number of megabytes received by the NetScaler appliance
   - Tx (Mbps)— Number of megabytes transmitted by the NetScaler appliance
   - HTTP Req/s— Total number of HTTP requests received

The dashboard data is refreshed after each polling interval, the default value is 5 minutes. To poll the device,

1. On the Monitoring tab, on the left pane, navigate to NetScaler > Dashboard.
2. Select the device you want to poll and from theActions drop-down list, select Poll Now.
3. When prompted for confirmation, click Yes.

The default interval is 5 minutes. To change the polling interval navigate to Monitoring > NetScaler > Dashboard > Configure Polling Interval page and set the value.

Monitoring Virtual Servers, Services, Servers, and Service Groups

May 28, 2015

You can monitor the real-time status of virtual servers, services, servers, and service groups using the Monitoring feature of Command Center. You can also view the services and service groups bound to virtual servers.

You can further add views to monitor specific entities based on entity names, device names, protocol types, states, and health.

This topic includes the following details:

Viewing the Status of Virtual Servers

Updated: 2014-04-15

Use Command Center to monitor the real-time values of the state and health of a virtual server. You can also view the attributes of a virtual server, such as name, IP address, and type of virtual server.

To view the status of virtual servers

1. On the Monitoring tab, in the left pane, under NetScaler, click Virtual Servers.
2. In the right pane, under Virtual Servers, view the following statistics:
   - Device Name: Specifies the name of the device on which the virtual server is configured.
   - Name: Specifies the name of the virtual server.
   - IP: Specifies the IP address of the virtual server. Clients send connection requests to this IP address.
   - Port: Specifies the port on which the virtual server listens for client connections.
   - Type: Specifies the type of virtual server (for example, load balancing). This information is available only for virtual servers configured on NetScaler release 9.0 and later.
   - **Protocol**: Specifies the service type of the virtual server. For example, HTTP, TCP, and SSL.
   - State: Specifies the current state of the virtual server. For example, UP, DOWN, and OUT OF SERVICE.
   - Health: Specifies the percentage of the services that are in the state UP and are bound to the virtual server. The following formula is used to calculate the health percentage: (Number of bound UP services * 100) / Total bound services
   - Last State Change: Specifies the time elapsed (in days, hours, minutes, and seconds) since the last change in the state of the virtual server, that is, the duration of time for which the virtual server is in the current state. This information is available only for virtual servers configured on NetScaler release 9.0 and later.

   Note: You can sort the rows in ascending or descending order by clicking the column headers. For example, clicking the

Device Name column header sorts the rows in order of the device names.

Viewing the Status of Servers

Updated: 2014-07-14

Use Command Center to monitor and manage the states of servers across the NetScaler infrastructure. This gives you visibility into the real-time status of the servers and makes management of these servers easy when you have a large number of servers.

To view the status of servers

1. On the Monitoring tab, under NetScaler, in the left pane, expand NetScaler, and then click Servers.
2. In the right pane, under Servers, view the following statistics:
   - Device Name: Specifies the name of the device on which the server is configured.
   - Name: Specifies the name of the server.
   - IP Address: Specifies the IP address of the server. Clients send connection requests to this IP address.
   - State: Specifies the current state of the server. For example, UP, DOWN, and OUT OF SERVICE.

   Note: You can sort the rows in ascending or descending order by clicking the column headers. For example, clicking the Device Name column header sorts the rows in order of the device names.
   The Show Service Bindings and Show Service Group Bindings display the respective service and service groups associated with a server.

Viewing Services and Service Groups Bound to a Virtual Server

Updated: 2014-04-15

You can monitor the real-time status of the services and service groups bound to a virtual server. This lets you check the state of the services that may cause the health percentage of a virtual server to become low, and then you can take appropriate action.

To view the services and service groups bound to a virtual server

1. On the Monitoring tab, in the left pane, under NetScaler, click Virtual Servers.
2. In the right pane, under Virtual Servers, click the name of the virtual server for which you want to view the bound services and service groups, and click Bounded Servicesor Bounded Services Groups. Alternately, right-click the name of the virtual server, and then click Bounded Services or Bounded Services Groups. For more information about the status of service groups, see Viewing the Status of Service Groups.

Viewing the Status of Services

Updated: 2014-04-15

Use Command Center to monitor the real-time values of the state of a service and the duration for which a service is in the current state.

To view the status of services

1. On the Monitoring tab, on the left pane, expand NetScaler, and then click Services.
2. In the right pane, under Services, view the following statistics:
   - Device Name: Specifies the name of the device on which the service is configured.
   - Name: Specifies the name of the service.

- IP: Specifies the IP address of the service.
- Port: Specifies the port on which the service listens.
- Protocol: Specifies the service type that determines the behavior of the service. For example, HTTP, TCP, UDP, and SSL.
- State: Specifies the current state of the service. For example, UP, DOWN, and OUT OF SERVICE.
- Last State Change: Specifies the time elapsed (in days, hours, minutes, and seconds) since the last change in the state of the service, that is, the duration of time for which the service is in the current state.

Note: You can sort the rows in ascending or descending order by clicking the column headers. For example, clicking the Name column header sorts the rows in order of the service names.

Viewing the Virtual Servers to which a Service is Bound

Updated: 2014-04-18

You can view the virtual servers to which a service is bound and further monitor the real-time status of the virtual servers.

To view the virtual servers to which the service is bound

1. On the Monitoring tab, in the left pane, expand NetScaler, and then click Services.
2. In the right pane, under Services, click the name of service for which you want to view the bound virtual servers, and click Bounded Virtual Servers.
   Alternately, right-click the service and click Bounded Virtual Servers. For more information about the status of virtual servers, see Viewing the Status of Virtual Servers.

Viewing the Status of Service Groups

Updated: 2014-04-15

Use Command Center to monitor the real-time values of the state of a service group member.

To view the status of service groups

1. On the Monitoring tab, in the left pane, expand NetScaler and click Service Groups.
2. In the right pane, under Service Groups, view the following statistics:
   - Device Name: Specifies the name of the device on which the service group is configured.
   - Name: Specifies the name of the service group.
   - IP: Specifies the IP address of the service, which is a member of the service group.
   - Port: Specifies the port on which the service group member listens.
   - Protocol: Specifies the service type that determines the behavior of the service group. For example, HTTP, TCP, UDP, and SSL.
   - State: Specifies the effective state of the service group, which is based on the state of the member of the service group. For example, UP, DOWN, and OUT OF SERVICE.
   - Last State Change: Specifies the time elapsed (in days, hours, minutes, and seconds) since the last change in the state of the service group member, that is, the duration of time for which the service group member is in the current state. This information is available only for service group members configured on NetScaler release 9.0 and later.

   Note: You can sort the rows in ascending or descending order by clicking the column headers. For example, clicking the Name column header sorts the rows in order of the service group names.

Viewing the Virtual Servers to which a Service Group is Bound

Updated: 2014-04-15

You can view the virtual servers to which a service group is bound and further monitor the real-time status of those virtual servers.

To view the virtual servers to which the service group is bound

1. On the Monitoring tab, in the left pane, expand NetScaler and click Service Groups.
2. In the right pane, under Service Groups, click the name of the service group for which you want to view the bound virtual servers, and then click Bounded Virtual Servers. Alternately, right-click the name of the service group, and then click Bounded Virtual Servers.

Configuring Views

Updated: 2015-05-28

You can add views to monitor specific entities based on entity names, device names, protocol types, states, and health. Views make it easier to monitor a large number of entities configured across your NetScaler infrastructure. For example, you can create a view to monitor virtual servers with protocol type as AAA.

The views you create are associated with your Command Center user account. If you want to assign these views to other groups of users, you must assign administrator privileges to the view.

This topic includes the following details:

- Adding Views for Virtual Servers
- Adding Views for Services
- Adding Views for Service Groups
- Modifying Views
- Deleting Views
- Assigning Views

Adding Views for Virtual Servers

You can add different views for the virtual servers you monitor. These views are based on various filter criteria, such as the virtual server name, device name, protocol type, state, and health.

To add views for virtual servers

1. On the Monitoring tab, in the left pane, under NetScaler, expand Virtual Servers, and then click Views.
2. In the right pane, under Views, click Add.
3. Under Create Virtual Server View, in Name, type a name for the view you want to create.
4. In Virtual Server Names, type the name(s) of the virtual server(s) for which you want to create the view.
   Note: Use a comma to separate multiple virtual server names.
5. In Virtual Server IPs, specify the IP address of the virtual servers for which you want to filter in the view.
6. In Devices, select the device(s) and click **+** and select the devices from the available list
7. In Protocols, select the protocols.
8. In States, select the state(s) of the virtual server.
9. In Health, choose the operator, and in the Value text box, type the health percentage, and then click Create.

Adding Views for Services

You can add different views for the services you monitor. These views are based on various filter criteria, such as the service

name, device name, protocol type, state, and last state change.

To add views for services

1. On the Monitoring tab, in the left pane, under NetScaler expand Services, and then click **Views.**
2. In the right pane, under Views, click Add.
3. Under Create Service View, in Name, type a name for the custom view you want to create.
4. In Service Names, type the name(s) of the service(s) for which you want to create the custom view. Use a comma to separate multiple service names.
5. In Service IPs, type the IP address of the service for which you want to filter in the view.
6. In Devices, click **+** and select the device(s) from the list.
7. In Protocols, select the protocol type(s).
8. In States, select the state(s) of the service(s).
9. In Last State Change, choose the operator, type the time period, and choose the time interval, and then click Create.
   Note: The Last State Change field defines the time elapsed (in days, hours, minutes, and seconds) since the last change in the state of the service, that is, the duration of time for which the service is in the current state.

Adding Views for Service Groups

You can add different views for the service groups you monitor. These views are based on various filter criteria, such as the device name, protocol type, and state. Note that views you create are associated with your Command Center user account.

To add views for service groups

1. On the Monitoring tab, in the left pane, under NetScaler, expand Service Groups, and then click **Views.**
2. In the right pane, under Views, click Add.
3. Under Create Service Group View, in Name, type a name for the custom view you want to create.
4. In Service Group Names, type the name(s) of the service group(s) for which you want to create the custom view. Use a comma to separate multiple service names.
5. In Service Group IPs, type the IP address of the service for which you want to filter in the view.
6. In Devices, click +, and then select the device(s) from the list.
7. In Protocols, select the protocol type(s).
8. In States, select the state(s) of the service, and then click Create.

Adding Views for Servers

You can add different views for the servers you monitor. These views are based on various filter criteria, such as the server name, device name and state.

To add views for virtual servers

1. On the Monitoring tab, in the left pane, under NetScaler, expand Servers, and then click Views.
2. In the right pane, under Servers, click Add.
3. Under Create Server View, in Name, type a name for the view you want to create.
4. In Server Names, type the name(s) of the server(s) for which you want to create the view.
   Note: Use a comma to separate multiple server names.
5. In Server IPs, type the IP address of the server(s).
6. In Devices, click + Add and select the devices from the available list.
7. In States, select the state(s) of the server and then click Create.

After creating views, you can modify the filter criteria of the views or delete it if you do not want to use it again.

Modifying Views

After creating views, you can modify the filter criteria of the views.

To modify views

1. On the Monitoring tab, in the left pane, under NetScaler, expand Virtual Servers, Services, or Service Groups, and click **Views**.
2. In the right pane, click the view you want to modify, and click **Modify**. Alternately, right-click the view and click **Modify**.
3. Make changes to the values as required, and then click OK.

To modify views

1. On the Monitoring tab, in the left pane, under NetScaler, expand Virtual Servers, Services, Service Groups, or Servers and click **Views**.
2. In the right pane, click the view you want to modify, and click **Modify**. Alternately, right-click the view and click **Modify**.
3. Make changes to the values as required, and then click OK.

Deleting Views

You can delete a view if you do not want to use it again.

To delete views

1. On the Monitoring tab, in the left pane, under Netscaler, expand Virtual Servers, Services, or Service Groups, and click **Views**.
2. In the right pane, click the view, and then click Delete. Click Yes on the confirmation message.

To delete views

1. On the Monitoring tab, in the left pane, under Netscaler, expand Virtual Servers, Services, Service Groups, or Servers and click **Views**.
2. In the right pane, click the view, and then click Delete. Click Yes on the confirmation message.

Assigning Views

After you create a view, the view is visible only to you. If you want the same view to be visible to others, you must assign administrator privileges to the view. The administrator can then assign the view to the required group of users. Only the administrator can assign the view to other groups. After you specify administrator privileges, you no longer have permission to modify or delete the view.

If a view is modified by an administrator, the modified data is applicable to all users in the assigned groups.

You can specify administrator privileges to a view when you create the view, or you can assign them by modifying an existing view.

Example

Sam, in the engineering group, creates a view displaying all the NetScaler virtual servers that are in the unknown state. He wants the analytics group to be able to use this view to analyze the reason for the unknown state. The analytics team

could create a similar view, but it might not use the same filters, and Sam's filters are uniquely effective. Sam therefore assigns administrator privileges to the view, and the administrator assigns the view to the analytics group. Both Sam and the analytics group can now access the view. Only the administrator can modify it.

To assign administrator privileges to an existing view

1. On the Monitoring tab, navigate to NetScaler, and then to Virtual Servers, Services, Service Groups, or Servers, and then click Views.
2. In the right pane, select the view and click Edit.
3. On the page for modifying views, click Administrator View.

To assign views to different groups

Note: This task is applicable to administrators only.

1. On the Monitoring tab, navigate to NetScaler, and then to Virtual Servers, Services, Service Groups, or Servers, and then click Views.
2. In the right pane, select the view and click **Assign View**.

Managing the Real-Time Status of Entities

May 27, 2015

You can manage the virtual servers, services, and service groups configured across all your NetScaler devices from the Command Center console. You can set a time interval for which you want Command Center to poll the values of the entities. You can manage the states of the entities by enabling or disabling them and view the details of command execution using the Audit Trail.

You can poll the latest status of the entities at any given point of time, for example, after you have made a configuration change. You can also conduct a search for the entities based on different parameters, such as health, name, state and Type (CSVserver and LB).

This topic includes the following details:

Configuring the Polling Interval

Updated: 2014-04-18

You can set the time interval for which you want Command Center to poll the real-time values of the virtual servers, services, and service groups. By default, Command Center polls the values every 300 seconds (5 minutes).

Setting the polling interval on any one of the entity nodes (Virtual Servers, Services, or Service Groups) sets it across all the entity nodes.

To configure the polling interval for virtual servers, services, and service groups

1. On the Monitoring tab, click the Virtual Servers, Services, or Service Groups, and in the right pane, click Configure Polling Interval.
2. In Configure Polling Interval, type the number of seconds you want to set as the time interval for which Command Center must poll the entity value. Minimum value of the polling interval is 300 seconds (5 minutes). Click OK
   Note: Setting the polling interval on any one of the entity nodes (Virtual Servers, Services, or Service Groups) sets it across all the entity nodes.

To configure the polling interval for virtual servers, services, and service groups

1. On the Monitoring tab, under NetScaler click the Virtual Servers, Services, or Service Groups, and in the right pane, select the Virtual Server, Service, or Service Group and from the Action drop-down list, select Configure Polling Interval.
2. In Configure Polling Interval, type the number of seconds you want to set as the time interval for which Command Center must poll the entity value. Minimum value of the polling interval is 300 seconds (5 minutes).
   Note: Setting the polling interval on any one of the entity nodes (Virtual Servers, Services, or Service Groups) sets it

across all the entity nodes.
3. Click OK

Enabling or Disabling Virtual Servers

Updated: 2014-04-15

You can also change the state of a virtual server by enabling or disabling it.

When you enable a virtual server with a state of DOWN or OUT OF SERVICE, its state changes to either UP or DOWN, depending on whether the actual server is UP or DOWN. If the state of the virtual server does not change to UP, log on to the NetScaler to identify the cause and make appropriate changes to the virtual server configuration.

When you disable a virtual server with a state of UP, its state changes to OUT OF SERVICE.

To enable or disable virtual servers

1. On the Monitoring tab, in the left pane, under NetScaler, click Virtual Servers.
2. In the right pane, under Virtual Servers, select the virtual server(s) you want to enable or disable, and then click Enable or Disable. Alternately, you can right-click the virtual server, and click Enable or Disable.
3. Under Enable or Disable Virtual Servers, in Annotation, type a message describing the reason why you are enabling or disabling the virtual server.
4. Select Save configuration on success if you want to save the configuration, and then click OK.
5. Under Operation Status, view the status of the task and the following details:
   - Command: Specifies the name of the command executed on the device. Clicking this displays the details of command execution, such as the time when the command was executed and the result of the command execution.
   - Device Name: Specifies the IP address of the device on which the virtual server is configured.
   - Start Time: Specifies the time when the command execution started.
   - Finish Time: Specifies the time when the command execution ended.
   - Status: Specifies the status of command execution (for example, Success and Failed).

Enabling or Disabling Services

Updated: 2014-04-15

You can also change the state of a service by enabling or disabling it.

When you enable a service with a state of DOWN or OUT OF SERVICE, its state changes to either UP or DOWN, depending on whether the actual backend server is UP or DOWN. If the state of the service does not change to UP, log on to the NetScaler to identify the cause and make appropriate changes to the service configuration.

When you disable a service with a state of UP, its state changes to OUT OF SERVICE.

During scheduled network outages such as system upgrades or hardware maintenance, you may have to close or disable some services. To avoid disrupting sessions that have already been established, you can specify a wait time, which places a service in the transition out of service (TROFS) state until the specified wait time expires. The service then enters the OUT OF SERVICE (OFS) state.

Often, however, you cannot estimate the amount of time needed for all the connections to a service to complete the existing transactions. If a transaction is unfinished when the wait time expires, shutting down the service may result in data loss. In this case, you can specify graceful shutdown for the service, so that the service is disabled only when all the

established connections are closed by either the server or the client.

Persistence is maintained according to the specified method even if you enable graceful shutdown. The system continues to serve all the persistent clients, including new connections from the clients, unless the service is marked DOWN during the graceful shutdown state as a result of the checks made by a monitor.

The following table describes graceful shutdown options.

Table 1. Graceful Shutdown Options

State	Results
Graceful shutdown is enabled and a wait time is specified.	Service is shut down after the last of the previously established connections is served, even if the wait time has not expired. The device checks the status of the connections once every second. If the wait time expires, any open sessions are closed.
Graceful shutdown is disabled and a wait time is specified.	Service is shut down only after the wait time expires, even if all established connections are served before expiration.
Graceful shutdown is enabled and no wait time is specified.	Service is shut down only after the last of the previously established connections is served, regardless of the time taken to serve the last connection.
Graceful shutdown is disabled and no wait time is specified.	No graceful shutdown. Service is shut down immediately after the disable option is chosen or the disable command is issued. (The default wait time is zero seconds.)

To enable or disable services

1. On the Monitoring tab, in the left pane, under NetScaler, click Services.
2. In the right pane, under Services, select the check box for the service(s) you want to enable or disable, and then click Enable or Disable.
3. Under Enable or Disable, in Annotation, type a message describing the reason why you are enabling or disabling the service.
4. In **Disable Services**, you can specify a wait time and the graceful shutdown time to ensure services are not shut down abruptly.
5. Select Save configuration on success if you want to save the configuration, and then click OK.
6. Under Operation Status, view the status of the task and the following details:
   - Command: Specifies the name of the command executed on the device. Clicking this displays the details of command execution, such as the time when the command was executed and the result of the command execution.
   - Device Name: Specifies the IP address of the device on which the service is configured.
   - Start Time: Specifies the time when the command execution started.
   - Finish Time: Specifies the time when the command execution ended.
   - Status: Specifies the status of command execution (for example, Success and Failed).

Enabling or Disabling Service Groups

Updated: 2014-04-15

You can also change the state of a service group by enabling or disabling it.

When you enable a service group member with a state of DOWN or OUT OF SERVICE, the state of the service group to which it belongs changes to either UP or DOWN, depending on whether the actual backend server is UP or DOWN. If the state of the service group does not change to UP, log on to the NetScaler to identify the cause and make appropriate changes to the configuration of the service group.

When you disable a service group member with a state of UP, the state of the service group to which it belongs changes to OUT OF SERVICE.

During scheduled network outages such as system upgrades or hardware maintenance, you may have to close or disable some services. To avoid disrupting sessions that have already been established, you can specify a wait time, which places a service in the transition out of service (TROFS) state until the specified wait time expires. The service then enters the OUT OF SERVICE (OFS) state.

Often, however, you cannot estimate the amount of time needed for all the connections to a service to complete the existing transactions. If a transaction is unfinished when the wait time expires, shutting down the service may result in data loss. In this case, you can specify graceful shutdown for the service, so that the service is disabled only when all the established connections are closed by either the server or the client.

Persistence is maintained according to the specified method even if you enable graceful shutdown. The system continues to serve all the persistent clients, including new connections from the clients, unless the service is marked DOWN during the graceful shutdown state as a result of the checks made by a monitor.

The following table describes graceful shutdown options.

Table 2. Graceful Shutdown Options

State	Results
Graceful shutdown is enabled and a wait time is specified.	Service group is shut down after the last of the previously established connections is served, even if the wait time has not expired. The device checks the status of the connections once every second. If the wait time expires, any open sessions are closed.
Graceful shutdown is disabled and a wait time is specified.	Service group is shut down only after the wait time expires, even if all established connections are served before expiration.
Graceful shutdown is enabled and no wait time is specified.	Service group is shut down only after the last of the previously established connections is served, regardless of the time taken to serve the last connection.
Graceful shutdown is disabled and no wait time is specified.	No graceful shutdown. Service group is shut down immediately after the disable option is chosen or the disable command is issued. (The default wait time is zero seconds.)

To enable or disable service groups

1. On the Monitoring tab, in the left pane, under NetScaler, click Service Groups.
2. In the right pane, under Service Groups, select the service group(s) you want to enable or disable, and then click Enable or Disable.
3. Under Enable or Disable, in Annotation, type a message describing the reason why you are enabling or disabling the service group.
4. In **Disable Services**, you can specify a wait time and the graceful shutdown time to ensure services are not shut down abruptly.
5. Select Save configuration on success if you want to save the configuration, and then click OK.
6. Under Operation Status, view the status of the task and the following details:
   - Command: Specifies the name of the command executed on the device. Clicking this displays the details of command execution, such as the time when the command was executed and the result of the command execution.
   - Device Name: Specifies the IP address of the device on which the service group is configured.
   - Start Time: Specifies the time when the command execution started.
   - Finish Time: Specifies the time when the command execution ended.
   - Status: Specifies the status of command execution (for example, Success and Failed).

Viewing the Audit Trail

Updated: 2014-04-17

You can view the audit trail to identify enabled and disabled operations on virtual servers, services, servers, and service group members.

To view the audit trail

1. On the Monitoring tab, in the left pane, under NetScaler, navigate to Virtual Servers, Services, Servers, or Service Groups >Audit Trails.
2. Under Audit Trails, you can view the following:
   - Device: Specifies the IP address of the device on which the operation is performed.
   - Operation: Specifies the operation performed on the virtual server, service, or service group member.
   - Name: Specifies the name of the virtual server, service, or service group member on which you have performed the operation.
   - Executed By: Specifies the username of the NetScaler user who performed the operation.
   - Time: Specifies the time when the operation was performed.
   - Status: Specifies the status of the operation performed, which can be Success or Failed.
   - Annotation: Specifies the message describing the reason why the enable or disable operation was performed. This message was entered when performing the operation.

Searching Virtual Servers, Services, and Service Groups

Updated: 2014-04-15

You can use the search option of the Monitoring feature to search for virtual servers, services, or service groups.

To search for a virtual server, service, or service group

1. On the Monitoring tab, in the left pane, under NetScaler, click Virtual Servers, Services, or Service Groups.
2. In the right pane, under Virtual Servers, Services, or Service Groups, click Search.
3. Select the options, and then click Refine Search.

Polling the Status of Virtual Servers, Services, and Service Groups

Updated: 2014-04-15

You can poll the status of specific virtual servers, services, or service groups at any given point of time.

To poll the status of a virtual server, service, or service group

1. On the Monitoring tab, in the left pane, under Network, click Virtual Servers, Services, or Service Groups.
2. In the right pane, under Virtual Servers, Services, or Service Groups, select the virtual server, services, or service groups, and then click Poll.

Using Tasks to Configure Managed Devices

Nov 04, 2016

You can simplify device management and minimize configuration errors by using built-in and custom tasks to make configuration changes across devices, upgrade firmware, and replicate a device's configuration to other devices on your network.

To make configuration changes on NetScaler and CloudBridge managed devices, Command Center uses the NetScaler and CloudBridge command-line interface (CLI) and the Secure Shell (SSH), Secure File Transfer Protocol (SFTP), and Secure Copy Protocol (SCP) protocols. To view the status of the tasks executed, see the execution log that Command Center provides.

In this section:

Managing Built-in Tasks

May 27, 2015

Built-in tasks are a set of predefined configuration tasks that you can execute on one or more managed devices. These tasks help you address the most commonly used configuration changes of the discovered devices. Command Center supports built-in tasks for both NetScaler and CloudBridge devices.

You can execute the built-in tasks instantly or schedule them for execution at a later time. You can view the execution log to check the task status and view the list of tasks scheduled for execution. You can also export a built-in task as an XML file. Note that you cannot modify or delete built-in tasks.

Use the following procedures for managing built-in tasks:

- Upgrading NetScaler with Built-in Tasks
- Configuring NetScaler with Built-in Tasks
- Importing Application Templates with Built-in Tasks
- Configuring Parameter Values Across NetScaler Devices with Built-In Tasks
- Upgrading CloudBridge with Built-in Tasks
- Configuring CloudBridge with Built-in Tasks
- Configuring CloudBridge Advanced Platform with Built-in Tasks
- Uploading Upgrade Files to NetScaler SDX with Built-In Tasks
- Viewing Built-in Tasks
- Executing Built-in Tasks
- Viewing the Execution Log for Built-in Tasks
- Scheduling Built-in Tasks
- Exporting Built-in Tasks

Upgrading NetScaler with Built-in Tasks

The built-in upgrade tasks that you can execute on NetScaler devices are:

- **SoftwareUpgrade-9.xto10.x**: Upgrade one or more devices from the 9.x release to any version of the 10.x release of NetScaler.
- **SoftwareUpgrade-Within10.x**: Upgrade one or more devices from the 10.x release to a newer 10.x version.
- **SoftwareUpgrade-Within9.x**: Upgrade one or more devices from the 9.0 release to 9.1 or 9.2 releases of NetScaler, or from any version of 9.1 or 9.2 release to a newer version of 9.1 or 9.2. release. To execute this task, you must have the upgrade file present on the Command Center server or your local system, and you must specify the correct image file.
- **SoftwareUpgrade-8.xto9.x**: Upgrade one or more devices from the 8.x release to any version of the 9.1 or 9.2 release of NetScaler . You must specify the upgrade file and/or the 9.x license file, and you must have these files present on the Command Center server or your local system. Note that image and license files are not prepackaged with Command Center, and you must copy these files from an appropriate location. When the user input screen prompts you, select the correct image and license files for the upgrade.
- **SoftwareUpgrade-8.xto9.0**: Upgrade one or more devices from the 8.x release to any version of the 9.0 release of NetScaler, or from the 9.0 release to a newer version of 9.0.
- **SoftwareUpgrade-Within8.x**: Upgrade one or more devices from the 8.0 release to a newer 8.x version. To execute this task, you must have the upgrade file present on the Command Center server or your local system, and you must specify the correct image file.

Configuring NetScaler with Built-in Tasks

The built-in configuration tasks that you can execute on NetScaler devices are:

- **ConfigureCompression Policy**: Configure compression policies on NetScaler devices.
- **InstallSSLCert**: Upload and install SSL certificates from the Command Center server to the discovered NetScaler devices.
- **ConfigureFilterPolicy**: Configure filter policies on NetScaler devices.
- **NSConfigureSyslogServer**: Configure syslog server settings on NetScaler devices.

Importing Application Templates with Built-in Tasks

You can import an application template to multiple NetScaler appliances using the Command Center built-in configuration task ImportApplicationTemplate.

Consider that you have an application template with configuration for optimizing traffic for an application. You want to import this template to ten other NetScaler devices that require a similar AppExpert application configuration. You can import the application template to the ten NetScaler devices simultaneously using the ImportApplicationTemplate built-in task.

Note: This feature works only with NetScaler release 9.3 application templates.

Configuring Parameter Values Across NetScaler Devices with Built-In Tasks

Updated: 2015-04-02

You can now configure parameter values across different NetScaler devices by applying a global configuration template and an input file. Specify the parameter names in the global configuration template, specify the parameter values in the input file, and then execute the task on multiple devices.
Note: The task is executed sequentially on all the devices.
The following code is an example for an input file:

```
<?xml version="1.0" encoding="UTF-8" ?>
<properties>
<global>
   <param name="CC_Trap_Dest" value="100.10.10.1"/>
   <param name="HostName" value="NS433"/>
</global>
<device name="10.102.43.3">
   <param name="NSIP" value="10.102.43.3"/>
   <param name="HostName" value="NS433"/>
   <param name="LBSERVER1" value="server43http"/>
</device>
<device name="10.102.40.20">
   <param name="NSIP" value="10.102.40.20"/>
   <param name="LBSERVER1" value="server20http"/>
   <param name="CC_Trap_Dest" value="15.3.4.6"/>
</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="LBSERVER1" value="haserver43http"/>
```



```
    <param name="CC_Trap_Dest" value="15.3.4.5"/>
</device>
</properties>
```

The following code is an example for a command in the template file:

```
add snmp trap specific <CC_Trap_Dest> -communityName public
set ns config -IPAddress <NSIP> -netmask 255.255.255.0
set ns hostName <HostName>
add lb vserver <LBSERVER1> HTTP
```

Note: Click the Downloads button on the Command Center server to download the following sample files:

- Sample NetScaler Global Configuration Template File
- Sample NetScaler Global Configuration Input File

Points to Note

- In the template file, a parameter name must be enclosed in angle brackets-< >. Example: <NSIP>, <CC_Trap_Dest>
- Parameter names specified in template file must be defined in the input file.
- In the input file:
  - The global parameters must be defined within the global tag.
  - All parameter values for specific devices must be defined within the device tag.
  - If the parameter names and their values are available in both the global tag and device tag, the values in the device tag takes precedence.
  - An HA pair is specified by adding a hyphen. Example: 1.1.1.1-2.2.2.2.

Limitation

In the input file, within the device tag, you can only specify the device IP address and not the hostname of the device.

To execute the built-in task

1. On the Configuration tab, navigate to Configuration > Built-in Tasks, and in the right-pane, click NetScaler tab.
2. Select DeployMasterConfig and click Execute.

Upgrading CloudBridge with Built-in Tasks

Updated: 2014-08-12

The built-in upgrade task that you can execute on a CloudBridge device is:

- **Software Upgrade**: Use this task to upgrade one or more CloudBridge devices to a newer release of the CloudBridge software by specifying the path to the installation file of the software version to which you want to upgrade.

Note: This task is supported only on CloudBridge VPX, CloudBridge 600, Repeater 8500 and Repeater 8800 appliances.

Configuring CloudBridge with Built-in Tasks

Updated: 2014-10-17

The built-in configuration tasks that you can execute on CloudBridge devices are:

- EnableCloudBridge: Enable traffic through CloudBridge devices.
- DisableCloudBridge: Disable traffic through CloudBridge devices.
- Configure Alert: Configure an alert (alert name and level) on CloudBridge devices.
- Configure Sys Log Server: Configure a new system log server for CloudBridge devices.

- Add User: Set up a new user account on selected devices and assign privileges.
- ConfigureBandwidth-5.xandearlier: Configure the bandwidth parameters of CloudBridge devices of version 5.x and earlier.
- ConfigureBandwidth-6.xandlater: Configure the bandwidth parameters of CloudBridge devices of version 6.x and later.
- RestoreConfig: Restore the configuration on a CloudBridge device from any configuration file.
- ConfigureRemoteLicenseServer: Configure multiple CloudBridge VPX devices to use a centralized licensing server. You can configure parameters, such as IP address, port of the licensing server, and the license model.
- ConfigureLocalLicenseServer: Configure multiple CloudBridge VPX devices to use local licensing server.
- RestartCloudBridge: Restart the CloudBridge devices.
- InstallCACert : Install CA certificates for CloudBridge devices.
- InstallCombinedCertKey: Install combined certificate key for CloudBridge devices.
- InstallSeparateCertKey: Install separate certificate key for CloudBridge devices.
- AddWCCPServiceGroup: Add a new WCCP service-group definition for one or more CloudBridge devices
- EnableWCCP: Enable the WCCP deployment mode on one or more CloudBridge devices
- DisableWCCP: Disable the WCCP deployment mode on one or more CloudBridge devices
- SetApplication: Create or modify an application on a CloudBridge device
- SetTrafficShapingPolicy: Modify the traffic shaping policy for one or more CloudBridge devices
- AddTrafficShappingPolicy: Add a traffic shaping policy for one or more CloudBridge devices.
- AddService: Create a service class for CloudBridge devices with one or more service class filters and enable the service class.
- AddLink: Creates a link for regulation and reporting for CloudBridge devices.
- SoftwareUpgrade: Software Upgrade for CloudBridge devices.
- AddUser: Add a new user and assign the privileges.
- AddVideoCachingSource: Add the IP address or domain name of the video source, and enable, disable, or exclude video caching from that source.
- AddorRemoveVideoCachingPorts: Add or remove port numbers at which the video source can receive or send data. Default port is 80.
- SetVideoCaching: Update the DNS suffix, maximum object size, policy file, or X-Forwarded-For configuration for video caching.
  - DNS Suffix: Convert the host name of the video caching source to a domain name.
  - Object Size: Maximum size for cached objects. An object larger than this limit is not cached.
  - Policy File: Policy rules for video caching.
  - X-Forwarded-For: Identify the client IP address for all HTTP requests that the appliance proxies.
- RemoveVideoCachingSource: Remove one or more video caching sources.
- RemoveAllVideoCaching: Remove all video caching sources.
- ClearVideoCaching: Clear the video cache, or clear video caching statistics.
- VideoCachingState: Enable or disable the video caching feature on one or more CloudBridge appliances.
- AddVideoPrePopulationNow: Configure video prepopulation to specify how you want to download and cache videos from the URL(s).
- AddorUpdateVideoPrePopulation: Add or modify a video prepolution entry to schedule it for a specified time period.
- VideoPrePulationState: Start or disable video prepopulation.

Note: The export option and customize option are not available for the following built-in tasks:

- AddWCCPServiceGroup
- EnableWCCP
- DisableWCCP
- SetApplication
- SetTrafficShapingPolicy

- AddTrafficShappingPolicy
- AddService

To execute the built-in tasks

On the Configuration tab, navigate to Configuration > Built-in Tasks, and in the right-pane, click CloudBridge tab.

Upgrading CloudBridge Advanced Platform with Built-in Tasks

Updated: 2015-04-02

The built-in upgrade tasks that you can execute on CloudBridge Advanced Platforms are:

- **UpgradeSoftware**: Use the uploaded upgrade file to upgrade the CloudBridge Advanced Platform and all its components.
  Note: While executing the task, Command Center displays the Management Service IP address.

Uploading Upgrade Files to NetScaler SDX with Built-in Tasks

Updated: 2015-03-18

You can upload the NetScaler upgrade files to multiple NetScaler SDX appliances at the same time.

- **UploadNetScalerImage**: Upload the NetScaler image to one or more NetScaler SDX appliances.
- **UpgradeXVA**: Upload the XenServer Virtual Appliance (XVA) image to one or more NetScaler SDX appliances.

Viewing Built-in Tasks

You can view the built-in tasks by device family and category. The NetScaler device family also includes NetScaler VPX and NetScaler Gateway Enterprise devices.

To view built-in tasks by device family and category

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks.
2. In the right pane, under **Built-in Tasks**, you can view the built-in tasks.

Executing Built-in Tasks

Updated: 2014-04-15

You can execute a built-in task on multiple devices at the same time. You can either select devices individually or select a device list for the tasks. You can execute the same task several times on different devices or device lists. You can also preview a task (the commands and rollback commands) before executing it.

To execute built-in tasks

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks.
2. In the right pane, under **Built-in Tasks**, click the task you want to execute, and from the Action drop-down list, click **Execute**, and then follow the wizard instructions. Alternately, right-click the task, click **Execute**, and then follow the wizard instructions.

Viewing the Execution Log for Specific Built-in Tasks

Updated: 2014-04-15

After executing a task, you can view the execution details of that task instantly or at a later time.

To view the execution log for built-in tasks

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks.
2. In the right pane, under **Built-in Tasks**, click either the NetScaler tab or CloudBridge tab.
3. Select the task whose execution details you want to view, and from the Action drop-down list, select **Execution Log**, and then follow the wizard instructions. Alternately, right-click the task, click **Execution Log**, and then follow the wizard instructions.
4. Under Execution Log, you can view the following:
   - Task Name: Specifies the task name.
   - Device Name: Specifies the IP address of the device on which the task is executed.
   - Start Time: Specifies the time when the task started.
   - End Time: Specifies the time when the task ended.
   - Executed By: Specifies the NetScaler or CloudBridge user who started the task.
   - Status: Specifies the completion status of the task, such as Success, Failed, and Queued.
   - Annotation: Specifies a message that is annotated when executing the task.

Note: You can also view an execution log for all executed tasks, including custom tasks, by clicking Execution Log under Configuration in the left pane.

Scheduling Built-in Tasks

Updated: 2014-04-16

You can schedule built-in tasks to execute at a later period or recur at regular intervals. For example, you can schedule tasks to be executed at specific hours daily, at specific hours on specific days of the week, and at specific hours on specific days of the month.

You can also view the details of all the built-in tasks that you have scheduled.

To schedule built-in tasks

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks.
2. In the right pane, under **Built-in Tasks**, select the task you want to execute, click **Schedule**, and then follow the wizard instructions. Alternately, right-click the task and click **Schedule**, and then follow the wizard instructions.

Note: To view scheduled built-in tasks, in the right pane, under Built-in Tasks, on the bottom bar, click Scheduled Tasks. You can stop, resume, or remove a scheduled built-in task.

Exporting Built-in Tasks

Updated: 2014-04-16

You can save the built-in tasks in XML format on the Command Center server. This XML file, also known as task file, can be used to create a new custom task in the existing server or can be copied to another Command Center server.

Note: The location of the exported file is CC_Home\provisioningtemplates\exportedtemplates.

Note: The export option is not available for the following built-in tasks:

- AddWCCPServiceGroup
- EnableWCCP
- DisableWCCP
- SetApplication
- SetTrafficShapingPolicy
- AddTrafficShappingPolicy
- AddService

To export built-in tasks

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks.
2. In the right pane, under Built-in Tasks, select the task you want to export, and from the Action drop-down list, click Export. Alternately, right-click the task, and then click **Export**.
3. Under Export Task, in Name, type a name for the task file, and then click OK. A message appears confirming that the selected task is successfully exported.

Configuring Custom Tasks

Nov 04, 2016

Custom tasks are user-defined configuration tasks that you can add in Command Center to perform a defined set of operations on the managed devices. These tasks may contain a heterogeneous set of commands, such as CLI commands, SHELL, or Secure File Transfer Protocol (SFTP), that you can execute on a single device or a set of devices grouped together in a device list.

Use the following procedures for configuring custom tasks:

- Adding Custom Tasks
- Executing Custom Tasks
- Viewing the Execution Log for Specific Custom Tasks
- Scheduling Custom Tasks
- Rescheduling Custom Tasks
- Exporting Custom Tasks
- Modifying Custom Tasks
- Deleting Custom Tasks

Adding Custom Tasks

Updated: 2015-05-26

You can add custom tasks using one of the following methods:

- Define new commands: Create a new task by defining task variables and commands. For more information see Adding New Custom Tasks.
- Import from command file: Create a task from a command file. A command file is a text file containing a list of commands that constitute a task; the content could be a snippet of the ns.conf file. Each command may be a NetScaler CLI, Shell, or FTP command. You must have the command file present on the Command Center server or on the local file system. For more information see Adding Custom Tasks from Command Files.
- Import from task file: Create a task from an existing task file. Use this option to enhance or modify an existing task. For example, you can create a new task from a built-in task or import a task already created on another Command Center server. You must have the task file present on the Command Center server or on the local file system. For more information see Adding Custom Tasks by Importing from Task Files.

With custom tasks, you have the option to configure task operations in the following ways:

Execute Sequentially: Execute a task on a set of devices, one device at a time. If task execution fails on any device, it does not continue on the remaining devices . By default, if you do not select this option, the task will be executed in parallel.

Execute on Inaccessible System(s): If the selected devices or the device list include any inaccessible devices (discovery failed devices), the task is executed on these devices as well as on the others.
Enable Role-Based Authorization (RBA): Allow task execution by authorized users only. Specify the user names and passwords of the authorized users. RBA works in the following scenarios:

- If you enable RBA globally on the Admin tab, regardless of the task-level setting, a custom task is executed only after you provide RBA credentials.
- If you do not enable RBA globally, task execution prompts for RBA credentials based on the task-level settings.
- Save Configuration on Success: After successful execution, the configuration is saved on the device.

If at any point of time, the task witnesses a command failure you can choose to perform any of the following actions:

- Stop Further Execution:
  If a command fails, Command Center stops executing the remaining commands. If you have selected the **Execute Sequentially** option and the command fails on one of the devices, execution does not proceed on the remaining devices.

  If you have not selected the **Execute Sequentially** option , task execution continues on the remaining devices even if the command fails on one of the devices.

- Ignore and Continue:
  If a command fails, Command Center ignores the failed command and continues executing the remaining commands on the device . However, if you have selected the **Execute Sequentially** option and the command fails and continues executing the remaining commands, execution does not proceed on the remaining devices.

  If you have not selected the **Execute Sequentially** option , and the command fails and continues executing the remaining commands, task execution does not proceed on the remaining devices.

- Rollback Successful Commands:
  Generate rollback commands at run time by fetching these commands based on the version of the device. If command execution within a task fails, the entire task is rolled back.

  Device specific rollback commands have precedence over the user defined rollback commands.

  When executing tasks, click **Preview** to display the system-generated rollback commands .

Note: Rollback Successful Commands is applicable only for NetScaler ADCs.
If you configure a task to support the auto rollback feature, the preview screen displays the actual executable commands and the corresponding rollback commands in a tabular format for devices selected in the device list. However, if you configure a task to not support the auto rollback feature, the preview screen displays the actual commands sequentially.

You may encounter errors in the following scenarios:

- When the auto rollback feature is not supported for a particular device version.
- When there are no CLI commands in a task.

Adding New Custom Tasks

Updated: 2014-04-15

You can create a custom task form start by defining commands and task variables.
To add new custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, click Add.
3. Under Custom Task Add Options, click Define new commands, and then click Next.
4. Under Add custom task, click either of the following:
   - Define new commands— Create a new task by defining task variables and commands.
   - Import from command file— In the Choose File dialog box, select the command file you want to use, click Open, and then click Next.
   - Import from task file— n the Choose File dialog box, select the task file you want to use, click Open, and then click Next.
5. Specify the Task Name, Description, Category, Device Family, and then select one or more of the following check boxes:

- **Execute Sequentially**: Specifies whether to execute the task on the devices in a sequential manner.
- **Execute on Inaccessible system(s) also**: Specifies whether to execute the task on inaccessible devices.
- **Enable RBA**: Specifies whether the user should provide user credentials before task execution.
- **Enable Auto Rollback**: Specifies whether rollback commands are generated implicitly during runtime. When you select this check box, you do not need to manually type rollback commands when adding actual commands in step 8.
-

6. Click Add Command.
7. In the Command dialog box, in Command, type the command you want to execute. This must be the actual command that you need to execute on the managed device. The commands you define here may use the task variables. The following is a sample command for creating and binding a filter policy:
   ```
   add filter policy $policyname$ -rule $expression$
    -$actionType$ $actionname$ bind filter global $policyname$
   ```
   Note: You must enclose task variables between the $ symbols.
8. In Protocol, select the protocol you want to associate with the command.
9. In Rollback, type the rollback command to use if the actual command fails.
   Note: If you have selected the Enable Auto Rollback option in step 7, you do not need to type the rollback command here.
10. Click OK.
11. In the Add custom task, click Add Task Variable.
12. In the Variable dialog box, specify the variable information, and then click OK.

Adding Custom Tasks from Command Files

Updated: 2014-04-15

You can add a custom task from a command file that contains the commands to be executed on the devices.

A command file is a text file containing a list of commands that constitute a task; the content could be a snippet of the ns.conf file. Each command may be a NetScaler CLI, Shell, or FTP command. You must have the command file present on the Command Center server or on your local system.

To add custom tasks from command files

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, click Add.
3. Under Custom Task Add Options, select either of the following click Next:
   - Define new commands— Create a new task by defining task variables and commands.
   - Import from command file— In the Choose File dialog box, select the command file you want to use, click Open, and then click Next.
   - Import from task file— n the Choose File dialog box, select the task file you want to use, click Open, and then click Next.
4. Under Add Custom Task, specify the task name and description, category, device family, and then select one or more of the following check boxes:
   - **Execute Sequentially**: Specifies whether to execute the task on the devices in a sequential manner.
   - **Execute on Inaccessible system(s) also**: Specifies whether to execute the task on inaccessible devices also.
   - **Enable RBA**: Specifies whether the user should provide user credentials before task execution.
   - **Enable Auto Rollback**: Specifies whether rollback commands are generated implicitly during runtime.
5. In the Add custom task, click Add Task Variable.

6. In the Variable dialog box, specify the variable information, and then click OK.

Adding Custom Tasks by Importing from Task Files

Updated: 2014-04-15

You can add a custom task from an existing task file. You can also enhance or modify an existing task to create a new task. For example, you can create a new task from a built-in task, or import a task already created on another Command Center server. You must have the task file present on the Command Center server or on your local system.

To add custom tasks by importing from task files

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, click Add.
3. Under Custom Task Add Options, select either of the following and click Next:
   - Define new commands— Create a new task by defining task variables and commands.
   - Import from command file— In the Choose File dialog box, select the command file you want to use, click Open, and then click Next.
   - Import from task file— n the Choose File dialog box, select the task file you want to use, click Open, and then click Next.
4. Under Add Custom Task, select one or more of the following check boxes:
   - **Execute Sequentially**: Specifies whether to execute the task on the devices in a sequential manner.
   - **Execute on Inaccessible system(s) also**: Specifies whether to execute the task on inaccessible devices.
   - Enable RBA: Specifies whether the user should provide user credentials before task execution.
   - Enable Auto Rollback: Specifies whether rollback commands are generated implicitly during runtime.
5. In the Add custom task, click Add Task Variable.
6. In the Variable dialog box, specify the variable information, and then click OK.

Executing Custom Tasks

Updated: 2014-04-15

You can execute a custom task on multiple devices at the same time. You can either select devices individually or select a device list for the tasks. You can execute the same task several times on different devices or device lists. You can also preview a task (the commands and rollback commands) before executing it.

To execute custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under **Custom Tasks**, select the custom task you want to execute, and from the Action drop-down list, click **Execute**

Viewing the Execution Log for Specific Custom Tasks

Updated: 2014-04-15

After executing a task, you can view the following execution details of that task instantly or at a later time.

To view the execution log for specific custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.

2. In the right pane, under **Custom Tasks**, select the custom task whose execution details you want to view, and from the Action drop-down list, select **Execution Log**, and follow the wizard instructions.
3. Under Execution Log, you can view the following:
   - Task Name: Specifies the task name.
   - Device Name: Specifies the IP address of the device on which the task is executed.
   - Start Time: Specifies the time when the task started.
   - End Time: Specifies the time when the task ended.
   - CC User: Specifies the Command Center user who initiated the task.
   - Device User: Specifies the NetScaler or CloudBridge user who initiated the task.
   - Status: Specifies the completion status of the task, such as Success, Failed, and Queued.
   - Annotation: Specifies a message that is annotated when executing the task.

> **Note**
>
> You can also view an execution log for all executed custom tasks by clicking **Execution Log** under **Configuration** in the left pane.

Scheduling Custom Tasks

Updated: 2014-04-16

You can schedule custom tasks to execute at a later period or recur at regular intervals. For example, you can schedule tasks to be executed at specific hours daily, at specific hours on specific days of the week, and at specific hours on specific days of the month.

To schedule custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under **Custom Tasks**, select the custom task you want to execute, and from the Action drop-down list click **Schedule**, and follow the prompts in the wizard. Alternately, right-click the custom task, click **Schedule**, and then follow the prompts in the wizard.

> **Note**
>
> To view scheduled custom tasks, in the right pane, under **Custom Tasks**, on the bottom bar, click **Scheduled Tasks**. You can stop, resume, or remove a scheduled custom task.

Rescheduling Custom Tasks

You can now reschedule already scheduled tasks in the Configuration tab.

To reschedule custom tasks

1. Navigate to the **Configuration** tab. In the left pane, under **Configuration**, click **Scheduled Tasks**.
2. Select the task you want to reschedule, and click **Reschedule**.
3. Enter the new schedule in the Schedule Details window.
4. Click **OK**.

Exporting Custom Tasks

Updated: 2014-04-16

You can save the custom tasks in XML format on the Command Center server. This XML file, also known as task file, can be used to create a new custom task in the existing server, or can be copied to another Command Center server.

Note: The location of the exported file is CC_Home\provisioningtemplates\exportedtemplates.

To export custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, select the task you want to export, and from the Action drop-down list select Export.
3. Under Export Task, in Name, type a name for the task file, and then click OK. A message appears confirming that the selected task is successfully exported.

Modifying Custom Tasks

Updated: 2014-04-18

You can modify the values of the fields in a custom task.

To modify custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, select the task you want to export, and from the Action drop-down list, click Edit.
3. Under Modify custom task, make changes to the fields you want to modify, and then click OK.

Deleting Custom Tasks

Updated: 2014-04-15

If you do not want to use a custom task again, you can delete it.

To delete custom tasks

1. On the Configuration tab, in the left pane, under Configuration, click Custom Tasks.
2. In the right pane, under Custom Tasks, select the task you want to export, and then click Delete.
3. In the confirmation message box, click **OK**.

Customizing Built-in and Custom Tasks

Apr 15, 2014

You can customize built-in tasks to create custom tasks from them. When you customize a built-in task, the commands and variables are imported and you can define the name, category, and description of the task according to your requirements. You can also customize custom tasks to create new custom tasks.

Note: The customize option is not available for the following built-in tasks:

- AddWCCPServiceGroup
- EnableWCCP
- DisableWCCP
- SetApplication
- SetTrafficShapingPolicy
- AddTrafficShappingPolicy
- AddService

To customize tasks

1. On the Configuration tab, in the left pane, under Configuration, click Built-in Tasks or Custom Tasks.
2. In the right pane, under Built-in Tasks or Custom Tasks, select the task you want to customize, and from the Action drop-down list, click Customize.
3. Under Customize Task, in Task Name, type a name for the task, and in Description, type a description for the task.
4. In Category, select the type of task you want to create. The available values are: General and Software Upgrade. Click the + (plus) sign to type a new category name.
5. In **Device Family**, select the device family.
6. Select one or more of the following check boxes:
   - Execute Sequentially : Specifies whether to execute the task on the devices in a sequential manner.
   - Execute on Inaccessible system(s) also : Specifies whether to execute the task on inaccessible devices also.
   - Enable RBA : Specifies whether the user should provide user credentials before task execution.
   - Enable Auto Rollback : Specifies whether rollback commands are generated implicitly during runtime. When you enable this check box, you do not need to manually type rollback commands when adding actual commands in step 8.
   - Save configuration on success : Specifies whether the custom task is saved implicitly by Command Center on the NetScaler and CloudBridge devices. If you select this option, you do not have to explicitly add the "save config" command when creating a custom task.
7. To add more commands, click Add Command.
8. In the Command dialog box, in Command, type the command you want to execute. This must be the actual command that you need to execute on the managed device. The commands you define here may use the task variables. For example, to run the command, `add filter policy <name> -rule <expression> (-reqAction <string> | -resAction <string>)`, enclose the task variables within the $ symbol as shown in the following example:
   The following is a sample command for creating and binding a filter policy:

   ```
   add filter policy $policyname$ -rule $expression$ -$actionType$ $actionname$ bind filter global $policyname$
   ```
9. In the Protocol list, select the protocol you want to associate with the command.
10. In the Rollback text box, type the rollback command to use if the actual command fails, and then click OK.
    Note: If you have selected the Enable Auto Rollback option in step 6, you do not need to type the rollback command here.
11. To add variables, click Add Task Variable.
12. Under Variable, specify the variable information, and then click OK.

Customizing the DeployMasterConfig Built-In Task

Oct 13, 2015

If you want to replicate the complete existing state of a NetScaler appliance on another NetScaler appliance, you must replicate the configuration, license, and certificate files. By executing the DeployMasterConfig built-in task without customizing it, you can replicate only the configuration file.

You can customize the DeployMasterConfig built-in task to add additional commands, so that you can replicate license and certificate files to other NetScaler devices, and execute any other commands required for your configuration.

You can customize the DeployMasterConfig built-in task to do the following:

- Add additional commands
- Modify existing commands
- Add variables to commands
- Delete commands
- Change the order of commands

Caution: Be careful when changing the order of commands in the DeployMasterConfig built-in task.

When you customize the DeployMasterConfig built-in task, the commands and variables are imported and you can define the name, category, and description of the task.

To customize the DeployMasterConfig Built-In Task

1. On the **Configuration** tab, navigate to **Configuration** > **Built-in Tasks** > **NetScaler**.
2. Select **DeployMasterConfig**, and then click **Save As**.
3. Under **Customize Task**, in **Task Name**, type a name for the task, and in **Description**, type a description for the task.
4. Follow the prompts to complete the configuration.

Viewing the Execution Log for all Tasks

Apr 16, 2014

View the status of commands in a task being executed, with the state (Failed, Success, or In-Progress) of the task. You can also set the interval for automatically refreshing the execution log.

To view the execution log for all tasks

1. On the Configuration tab, in the left pane, under Configuration, click Execution Logs.
2. The Execution Log pane displays the following details:
   - Task Name: Specifies the name of the executed task. Click the task name to view details about the commands that are executed.
   - Device: Specifies the IP address of the device on which the task is performed.
   - Start Time: Specifies the time at which the task started.
   - End Time: Specifies the time at which the task completed.
   - Status: Specifies the status of the task execution - success or failure.

Executing Commands using Configuration Profiles

May 27, 2015

Configuration Management module in Command Center enables you to execute various configuration commands over multiple devices at the same time. You can create configuration profiles, which are templates that you can use to execute configuration tasks. The configuration profiles allow you to import configuration from existing devices or existing configuration profiles. After the commands are imported, they are displayed in the Commands section in "Add Configuration" page. You can now choose to add or modify or delete the configuration commands to create a new configuration profile.

The configuration profiles created can be applied to a device or a set of discovered devices. When you choose to apply the configuration on multiple devices, the configuration profiles will be executed in parallel over the set of devices.

This topic includes the following details:

Adding Configuration Profiles

Updated: 2014-02-14

You can add a configuration profile to execute various configuration commands over multiple devices.

To add configuration profiles

1. On the Configuration tab, in the left pane, under Configuration, click Configuration Profiles.
2. In the right pane, do one of the following:
   - Click the NetScaler tab, and click Add.
   - Click the CloudBridge tab, and click Add.
3. Specify the following details in the Add Configuration Profile
   - Name— Name of the configuration profile
   - Description— Description of the configuration profile
   - Device Family— Select the type of device for which you want to create the configuration profile

   Select either of the following to choose the profile source:
   - Select Create New and specify the configuration details.
   - Select Load from device and then choose the device IP from the Devices drop-down list.
     The configuration commands for the selected device is displayed in the Commands box.
   - Select Load from the profile and then choose the profile from the Profile list.
     The configuration for the selected profile is displayed in the Commands box.
4. Click OK The configuration profile will be displayed under Configuration > Configuration Profiles.

Executing Configuration Profiles

Updated: 2014-02-13

You can execute a configuration profile on a single device or on multiple devices at the same time. You can either select

devices individually or select a device list. You can execute the same task several times on different devices or device lists.

To execute configuration profiles

1. On the Configuration tab, in the left pane, under Configuration, click Configuration Profiles.
2. In the right pane, do one of the following:
   - Click the NetScaler tab.
   - Click the CloudBridge tab.
3. Select a profile name and from the Action drop-down list, select Execute.
4. In the Execute Configuration profile, provide the following details:
   - Name—Provide a name for executing the configuration profile
   - Device— Do either of the following:
     - Select Device and then choose the device(s) over which you want to execute the configuration.
     - Select Device Groups and choose the device list(s) over which you want to execute the configuration.
5. Click OK The status of the execution task will be displayed under Configuration > Execution log.

Execution Log

Updated: 2014-02-05

The Execution Log page displays the following details:

- **Device**: IP address of the device on which the configuration profile has been executed. Clicking the IP address displays the commands that are executed on the Citrix device.
- **Start Time**: Time when the task execution started.
- **End Time**: Time when the task execution completed.
- **Executed By**: Username of the Command Center user who executed the task.
- **Status**: Status of the task execution, which can be Success or Failed.
- **Annotation**: Message describing the reason for task execution. This message was entered when executing the task.

Using Deployment Automation to Migrate Configurations

Apr 14, 2014

The Deployment Automation feature provides easy automation for deployment management when deployments are going through rapid changes.

This module provides smooth migration of configurations across different deployments and exposes RESTful NITRO APIs with which you can automate the entire process.

You can migrate the configurations from one NetScaler appliance to multiple NetScaler appliances by choosing and editing the configurations that you want to migrate. This process enables you to configure and validate the NetScaler configurations in a staging environment, and then apply them to a production environment.

To migrate the configurations

1. On the Configuration tab, in the details pane, under Deployment Automation, click Configuration Migration.
2. Under Source Configuration, do either of the following:
   - Click Device, and then choose the device IP from the Select Device drop-down list. Also, under Configuration Change Period, choose the configuration history duration.
   - Click Configuration Profile, and then choose the profile from the Select Profile drop-down list.
3. Click Get.
   The Source Configuration Summary section provides a summary of the configuration migration details.

   The Source Configuration Commands lists the commands selected for performing migration.

   Note: To edit the commands click the > icon. After editing, click Save.
4. Click Next.
5. Under Target Devices for Configuration Migration, click the > icon to add the target devices. On the Configuration Migration Target page, do either of the following:
   - Click Devices, select the target devices, and then click Insert.
   - Click Device Groups, select the target device groups, and then click Insert.
     Click Add to add a new device group. Provide the required details, and click Create.
6. Click Next.
7. Under Actions, choose either or all of the following:
   - Auto Rollback on failure
   - Save configuration after execution
8. Click Execute. The Configuration Migration Summary page displays the configuration migration logs. Expand either or all of the following tabs to view the summary:
   - Migration Status— Select the device, and then Command Log to view the command details, or right-click the device row and click Command Log. Optionally, select the command and click Details to view the details for a specific command.
   - NetScaler Statistics— Lists the statistics of the selected NetScaler devices for performing the migration.
   - Virtual Server Status— Shows the status of the virtual servers that belong to the NetScaler device(s).
   - Notification Settings— Select the notifications you want to receive in the configuration migration reports:
     - Enable alarm settings

- Receive execution report through email
  Note: If you have not configured any mail server settings, then click the > icon and configure them.

9. Click Done. The Configuration Migration Logs page displays the log details.
   Click Download Report to download the details to your local machine.

To display the migration details

You can view the configuration migration logs after performing the task.

1. On the Configuration tab, in the right pane, under Deployment Automation, click Configuration Migration Logs.
2. The Configuration Migration Logs page displays the following details:
   - Source— Source IP address of the selected NetScaler device or configuration profile from which the configurations were migrated.
   - Host Name— The host name of the source device.
     Note: The field is empty if you selected a configuration profile as the source device.
   - Start Time—Time when task execution started.
   - End Time—Time when task execution completed.
   - Executed By—User name of the Command Center user who executed the task.
   - Target devices—The target NetScaler appliances to which you applied the configurations.
   - Report Name—Name of the report.

   Additionally, you can export a report as a CSV file to your local computer. To download the report, select and click Download Report.

Email Notifications for Executed Tasks

Nov 04, 2016

Email notifications are now sent every time a built-in or custom task is executed. The notification will cover details such as the success or failure of the task along with the relevant details. For example, if you have scheduled a custom task in Command Center to perform specific configuration changes on NetScaler and you want to know if the scheduled task has succeeded or failed. Previously, you had to re-login to Command Center to know if your task succeeded or failed. You can now avoid such a scenario by sending a report of the success or failure of the tasks executed and, if further probing was required via an email notification.

To send email notification for a task

1. Navigate to the **Configuration** tab. In the left pane, under **Configuration**, click **Custom Tasks**.
2. Click **Add**.
3. After selecting the required custom task parameters such as the devices it must be run on, the schedule, and any comments you have, you will be directed to the **View Summary** page.
4. Select the **E-mail the report** checkbox to send an email notification when the task is executed by entering the following details:

- **From** - The address from which the email is sent.
- **To** - The addresses that you want to send the email report to.
- **User Name and Password** - Main server credentials.

> ### Note
>
> Click **Test Mail** to check if the mail server credentials provided are accurate and if the mail server is accessible from command center server. If the connection to the mail server is successful, a test mail is sent to the specified email and the settings are saved.

Monitoring and Managing SSL Certificates Configured on NetScaler Devices

May 28, 2015

Command Center provides a centralized view of Secure Socket Layer (SSL) certificates installed across all managed NetScaler devices. To manage SSL certificates, you need to ensure that certificate management is enabled. Then, you can view the current status of the certificates, and configure Command Center to update the status at regular intervals.

To prevent server downtime from expired SSL certificates, you can set severity levels, which will generate events when severity levels are met. You can configure these events to notify you when a certificate is about to expire. You can then generate Certificate Signing Requests (CSR) and update the certificates from Command Center.

Use the Audit Trail option to view the status of certificates that are updated. You can also download the certificates and the corresponding key pair to your local system.

You can link a NetScaler device's certificate(s) to a CA certificate. However, make sure that all of the certificate(s) that you link to the same CA certificate have the same source and the same issuer. After you have linked the certificate(s) to a CA certificate, you can unlink them.

Note: Command Center supports the certificate management feature for NetScaler releases 7.0.52 and later.
This topic includes the following details:

Enabling or Disabling Certificate Management

The certificate management option is enabled by default. If you do not want to manage certificates by using Command Center, you can disable the feature.

To enable or disable certificate management

1. On the Administration tab, in the right pane, under Global Settings, click Server Settings.
2. Under Server Settings, in SSL Certificate Management, select Enable or Disable.

Viewing the Current Status of SSL Certificates

You can refresh the certificate status to view the most recent state of all the certificates deployed on all the devices managed by Command Center.

To view the current status of SSL Certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificate Management, select the certificate name, and from the action drop-down list select Poll Now. Alternately, right click the certificate name and click **Poll Now** option.

Setting the Polling Interval for SSL Certificates

You can set the time interval for which you want Command Center to poll the real-time status of the SSL certificates. By default, Command Center polls the values every 24 hours.

To set the polling interval for SSL certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificate Management, and from the action drop-down list select Configure Polling Interval. Alternately, right-click the certificate name and click **Configure Polling Interval**.
3. In Configure Polling Interval, type the number of hours you want to set as the time interval for which Command Center must poll the SSL certificates status, and then click OK.

Setting the Expiry Criteria of SSL Certificates

You can set severity levels based on expiration values of certificates configured on managed devices. Command Center generates events when an assigned severity level is met. The default severity levels are as follows:

- Critical: Certificate has expired.
- Major: Certificate will expire within 7 days.
- Minor: Certificate will expire within 30 days.
- Warning: Certificate will expire within 90 days.

To set the expiration criteria for SSL certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificates, from the action drop-down list select Severity Levels.
3. Under Severity Levels, select the severity levels you want to use. For each severity level you want to use, define the number of days in which you want to be notified before a certificate expires.

Generating Certificate Signing Requests

You can generate Certificate Signing Requests (CSR) for the certificates you want to renew. Command Center generates the CSR with the user details and information about the public/private key pair of the existing certificates. After the CSR is generated, you can download it and email it to a Certificate Authority (CA). After the CA signs the CSR, it becomes a valid certificate.

To generate a CSR

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificate Management, select the certificate for which you want to generate CSR and from the Action drop-down list select Generate CSR.
3. In the right pane, click or right-click Download CSR, and save the file on your local system. The CSR file is saved on your local system as an MHT file.
4. To renew the certificate, email the generated CSR to your CA.

Updating SSL Certificates

After you receive the renewed certificate from the Certificate Authority (CA), you can update the certificates from Command Center without needing to log on to the NetScaler.

To update SSL certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificates, , click the certificate and from the action drop-down list select Update for the certificate you want to update.
3. Under Update Certificate, in Certificate File, either type the path of the certificate file or click Choose File to select the path.
4. In Key File, either type the path of the key file or click Choose File to select the path.
5. In Password, type the password for the certificate.
6. Select the Domain Check check box if you want to match the domain while updating the certificate.
7. In Annotation, type a message describing the reason why you are updating the certificate, and then click OK.

Note: Under Certificate Details, you can view the certificate name and file path and the IP address of the device on which the certificate is configured. You can also view the key file path.

Viewing the Audit Trail for SSL Certificates

You can view the update status of the certificate by using the Audit Trail option. The Audit Trail displays the details of the devices including the certificate update status (failed or success) for each device. You can also view the time a certificate was successfully updated.

To view the audit trail

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. In the right pane, under Certificates, click Audit Trails.
3. Under Audit Trail, you can do the following:
   - To set the refresh interval for the audit trail information displayed in this pane, click Settings, and then type how often you want this information refreshed (in seconds).
   - To immediately refresh the audit trail information displayed in this pane, click Refresh.

   You can also view the following:

- **Device Name:** Specifies the IP address of the device on which the certificate update task is performed. Clicking the IP address displays the commands associated with the Citrix device.
- **Start Time:** Specifies the time when the task started.
- **End Time:** Specifies the time when the task finished.
- **Executed By:** Specifies the NetScaler user who executed the task.
- **Status:** Specifies the status of the certificate update task, which can be Success or Failed.
- **Annotation:** Displays a message describing a reason for the tasks.

Downloading SSL Certificates

You can download the SSL certificates and corresponding key files to your local system. Before you download the certificates, you need to enable archiving of SSL certificates on the Administration tab.

To download SSL certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. Under Certificates, select the certificate you want to download, and from the action drop-down list select Download.
3. Under Download, select Download key file also if you want to download the corresponding key file, and then click OK.

Linking and Unlinking SSL Certificates

You can now link certificate (s) of a NetScaler device to a CA certificate. However, make sure that the certificate (s) have the same issuer.

To link SSL certificate(s) to CA certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. On the right pane, select the certificate(s) that belong to the same source.
3. From the Action drop-down list, click Link.
4. On the Link Servers Certificate(s) dialog box, choose a certificate from CA Certificate Name drop-down list and click OK. The certificates will be linked.

To unlink SSL certificates and CA certificates

If you have linked certificate (s) to a CA certificate, you can unlink them.

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. On the right pane, select the certificate(s) that are already linked.
3. From the Action drop-down list, click Unlink. The certificates will be unlinked.

Viewing SSL Certificate Links

You can view the SSL certificates that are linked to the CA certificates.

To view SSL certificates

1. On the Configuration tab, in the left pane, under Certificate Management, click Certificates.
2. On the right pane, select a certificate that you want to view and from the Action drop- down list, select Cert Links. The SSL certificate link details are displayed.

Auditing Configuration Changes Across NetScaler Devices

May 27, 2015

You can use the change management feature to monitor configuration changes across managed NetScaler devices, troubleshoot configuration errors, and recover unsaved configurations upon a sudden system shutdown.

The typical workflow for auditing configuration changes consists of the following tasks:

- Create audit templates with a set of valid NetScaler commands for auditing device configurations and detecting conflicts that result from configuration changes on a device.
- Add audit policies and map them to the corresponding audit templates.
- Generate audit reports from the policies to analyze and resolve configuration mismatches and conflicts.

This topic includes the following details:

Configuring Audit Templates

Audit templates contain a set of valid NetScaler commands for auditing device configurations and reporting conflicts that result from configuration changes. These configuration conflicts can be between the running and saved configurations of a device or among the devices in the device list or network.

You need to create audit policies to map the running configuration of the devices to the configuration specified in the audit templates, and then generate an audit report that compares the differences between the two configurations.

After adding the audit templates, you can also modify and delete the audit templates, as described in the following sections.

Adding Audit Templates

Audit templates contain a set of valid NetScaler commands for detecting configuration conflicts on a device.

To add audit templates

1. On the Configuration tab, in the left pane, under Change Management, click Audit Templates.
2. In the right pane, under Audit Templates, click Add.
3. Under Add Audit Template, in Name, type the name of the audit template that you want to create.
4. In Audit Template Commands, type the commands that you want to be part of the new template, and then click OK.

Modifying Audit Templates

You can modify audit templates to change the commands included in them.

To modify audit templates

1. On the Configuration tab, in the left pane, under Change Management, click Audit Templates.

2. In the right pane, under **Audit Templates**, select the audit template you want to modify, click **Add**.
3. Under Modify Audit Template, make the changes you want, and then click OK.

Deleting Audit Templates

You can delete one audit template or bulk delete multiple audit templates.

To delete audit templates

1. On the Configuration tab, in the left pane, under Change Management, click Audit Templates.
2. In the right pane, under Audit Templates, select the check boxes corresponding to the audit templates you want to delete, and then click Delete.
3. Click OK on the confirmation message box.

Configuring Audit Policies

Use Command Center Audit Policies to generate change management reports based on your requirements. You can either use built-in policies or add user-defined policies.

Reports are generated by the following two built-in audit policies:

- RunningVsSavedConfiguration: Results from this report compare the running and saved configuration on a device and highlights specific differences or mismatches between the configurations. If a system shuts down unexpectedly, you can use this report to recover and save configuration changes that were executed but not saved.
- ConfigurationChangeHistory: Results from this report track configuration changes that take place over a period of time. The default period is seven days.

You can add a user-defined audit policy and map it to corresponding audit templates. You must execute an audit policy on one or more devices or device lists to generate an audit report that compares the running configuration of a device with the selected audit templates. You can schedule both built-in and user-defined audit policies to run at any time. You can modify the existing audit policies and you can delete user-defined audit policies. However, you cannot delete the two built-in audit policies.

The following sections describe how to configure audit policies:

- Adding User-Defined Audit Policies
- Executing Built-in and User-Defined Audit Policies
- Scheduling Built-in and User-Defined Audit Policies
- Modifying User-Defined Audit Policies
- Deleting User-Defined Audit Policies

Adding User-Defined Audit Policies

You can create a user-defined audit policy that generates a report that compares the running configuration of a device with the selected audit templates. This type of report is called Running vs.Chosen audit templates report.

To add audit policies

1. On the Configuration tab, in the left pane, under Change Management, click Audit Policies.
2. In the right pane, under Audit Policies, click Add.
3. Under Add Audit Policy, in Name, type the name of the audit policy you want to create.

4. Under Choose report(s) to be generated, select one or more of the following:
   - Running vs. Chosen Audit templates: Results from this report compare the running configuration of a device with audit templates chosen. Select the audit templates that you want to use for the report from the Available Audit Templates list, and then click the right arrow.
   - Running vs. Saved Configuration: Results from this report compare the running and saved configuration on a device. After a system restarts, this option helps you recover and save the configuration changes that are executed but not saved.
5. Click OK.

Executing Built-in and User-Defined Audit Policies

You can execute an audit policy on one or more devices and device lists. Executing an audit policy generates a report.

To execute audit policies

1. On the Configuration tab, in the left pane, under Change Management, click Audit Policies.
2. In the right pane, under Audit Policies, click the audit policy you want to execute, and then click Action and click Execute
3. Under Execute Policy, select one of the following:
   - Devices: Select a device from Available Devices and click the right arrow.
   - Device Groups: Select a device list name from Device Groups. If you do not have a device list, click Add Device Group to add one.

Scheduling Built-in and User-Defined Audit Policies

You can schedule both built-in and user-defined audit policies to run at a later date and time. You can schedule the policies to run daily at specified hours or to run on specific days of a week or month at specified hours.

To schedule audit policies

1. On the Configuration tab, in the left pane, under Change Management, click Audit Policies.
2. In the right pane, under Audit Policies, click the audit policy, and and click and from the Action drop-down list, clickSchedule.
3. Under Schedule Policy, choose one of the following:
   - Devices: Select one or more devices from the Available Devices list, and then click the right arrow.
   - Device Groups: Select a device group name. If you do not have a device group, click Add Device Group to add one.
4. Under Schedule Details, choose one of the following:
   - Daily: Specifies that policies run daily. In Scheduled Hours, specify the hour(s) when you want the policy to run. For example, if you specify 2, the audit policy runs at 2 AM. Note that this follows the 24-hour clock.
   - Day(s) of week: Specifies that policies run on certain days of the week. In Day(s) of week, select the day(s) when you want to run the policy, and in Scheduled Hours, specify the hour(s) at which you want the policy to run. For example, if you specify Monday and 15, the audit policy runs every Monday at 3 PM.
   - Day(s) of month: Specifies that policies run monthly. In Day(s) of month, specify the dates when you want to run the policy, and in Scheduled Hours, specify the hour(s) at which you want the policy to run. For example, if you specify 4, 14, and 24 as the days of month and 15 as the scheduled hour, the audit policy runs at 3 PM on 4th, 14th, and 24th of every month.
5. Optionally, you can choose to send a report of the changed configuration by selecting the Email the report check box. Enter the **From**, **To**, and **Server Name** details. Select the **Attach the generated report(s)** check box if you wish to receive the configuration report as an attachment in CVS file format. If there are configuration changes, you will receive an email with the changes after the policy is executed at the scheduled time. Click **Test Mail** to check if the mail server

credentials provided are accurate and if the mail server is accessible from command center server. If the connection to the mail server is successful, a test mail is sent to the specified email and the settings are saved.

Modifying User-Defined Audit Policies

After creating audit policies, you can modify them to change the settings of the type of reports to be generated.

Note: You cannot modify built-in audit policies.
To modify audit policies

1. On the Configuration tab, in the left pane, under Change Management, click Audit Policies.
2. In the right pane, under Audit Policies, click the audit policy you want to modify, and then click Edit.
3. Under Modify Audit Policy, make the changes you want to, and then click OK.

Deleting User-Defined Audit Policies

You can delete a single user-defined audit policy or bulk delete multiple user-defined audit policies.

Note: You cannot delete the two built-in audit policies RunningVsSavedConfiguration and ConfigurationChangeHistory.
To delete audit policies

1. On the Configuration tab, in the left pane, under Change Management, click Audit Policies.
2. In the right pane, under Audit Policies, select the audit policies you want to delete, and then click Delete.
3. Click OK.

Generating Audit Reports

Audit reports are generated when you execute audit policies. Using these reports, you can monitor the configuration change events for each device on which an audit policy is executed. You can also resolve configuration mismatches and conflicts. You can monitor the following types of audit reports:

- Running vs. Saved Configuration: Generated when you execute the RunningVsSavedConfiguration audit policy. Specifies specific instances of difference or mismatch between the running configuration and the saved configuration of the device.
- Running vs. Audit Templates: Generated when a user-defined audit policy, which maps running configuration to audit templates is executed. Specifies specific instances of syntactical differences or mismatches between the commands in a running configuration and the assigned templates. Displays these differences or mismatches and the corrective commands that must be executed to resolve the conflicts. You can create a custom task to resolve this conflict. If there are no conflicts, the following message appears: "The audited configurations are in sync."
- Configuration change events: Generated when you execute the ConfigurationChangeHistory audit policy. Specifies configuration change events generated for a given device for the specified period (age). This facilitates troubleshooting of configuration errors by enabling the administrator to view all the commands executed over a period of time and also the exact date and time when a command was run.

You can view a list of all the reports generated. You can export a report as a CSV file to your local system or to the Command Center server. You can also set an interval for automatically updating the audit reports that you monitor. If you do not want to use a report, you can delete it. Those tasks are described in the following sections:

- Viewing Audit Reports
- Exporting Audit Reports
- Deleting Audit Reports

Viewing Audit Reports

You can view a list of all the generated reports. You can also monitor the configuration change events or configuration conflicts for each device on which an audit policy is executed.

To view audit reports

1. On the Configuration tab, in the left pane, under Change Management, click Audit Reports.
2. Under Audit Reports, you can view the following:
   - Name: Specifies the name of the audit report. Click the report name to display the IP address of the device(s) for which the report is generated, the start and end times of report generation for each device, and the status of the report.
   - Start Time: Specifies the time when the report generation started.
   - End Time: Specifies the time when the report generation ended.
   - Audit By: Specifies the user who executed the policy that generated the audit report.
   - Status: Specifies the status of the report (for example, changes exist, no changes, in progress, and failed).
   - Description: Specifies the report description.

Exporting Audit Reports

You can export a report as a CSV file to your local system or to the Command Center server.

To export audit reports

1. On the Configuration tab, in the left pane, under Change Management, click Audit Reports.
2. Under Audit Reports, click the report name for which you want to monitor the configuration mismatches.
3. Click Devices, and click the IP address of the device for which you want to view the report, and click Details.
4. On the report that appears, click Export.

Deleting Audit Reports

You can delete one audit report or bulk delete multiple audit reports.

To delete audit reports

1. On the Configuration tab, in the left pane, under Change Management, click Audit Reports.
2. Under Audit Reports, select the reports you want to delete, and then click Delete.
3. Click OK on the confirmation message box.

Using Performance Reports and Thresholds to Monitor Device Performance

May 28, 2015

Command Center provides the ability to monitor the performance of discovered Citrix devices by using performance reports and threshold functionality.

Before you run the reports, you must ensure that the performance counters are enabled for polling. Command Center monitors the health of a device by polling the performance counters supported by the device.

You can then generate quick reports about the performance of a specific device and custom reports showing performance data across a set of multiple devices or for multiple counters from one or more devices. You can, therefore, monitor the performance of the entire application delivery infrastructure (for example, you can view statistics of the total number of requests handled by a user-defined service that is receiving application traffic).

Each quick or custom report consists of three charts, each of which plots a different time interval. The top chart plots data in 5-minute intervals, the middle chart plots hourly average data for three months, and the bottom chart plots daily average data for one year. You can also export the performance graph report to a file in CSV or XML format.

You can set thresholds for monitoring the state of a discovered Citrix device. You can set a threshold for a specific counter to monitor devices or instances of entities of managed devices.

You can use built-in reports and log messages to monitor security violations encountered on the NetScaler devices by the Application Firewall module.

In this section:

Configuring Polled Counters

Jun 05, 2013

Command Center monitors the health of a device by polling the performance counters supported by the device. Command Center supports more than 300 counters for NetScaler (including NetScaler VPX and NetScaler Gateway) devices and more than 20 counters for CloudBridge devices. There are two types of counters: scalar and vector. The scalar counters (for example, TCP and UDP) are device-level, and they are enabled for polling by default.

The vector counters, which are identified by plus (+) signs following the counter names, are entity-level counters that display statistics for entities, such as interfaces, vservers, services, and service groups. You have to enable the vector counters explicitly. They are not enabled for polling by default because they may impact the Command Center server performance if there is a large number of entities configured on the devices. Enable polling on vector counters only when you need to monitor them.

If you run reports on counters that are not enabled for polling, the following error appears: "The selected counter is not enabled for polling. Enable the counter using the Polled Counters option and try again." If you run a report on a counter that the device does not support, the following error appears: "The managed device(s) may not support the selected counter(s). Modify your selection of the counter(s) and try again."

Note: Command Center provides a consolidated list of possible counters that can be enabled or disabled for polling. The counters are displayed at the time you want to run reports. Not all the counters are available on all releases of NetScaler or CloudBridge. For example, a counter that was available on NetScaler release 6.0 may be deprecated on NetScaler release 8.0. If you run a custom report looking for this counter, and if the device list contains NetScaler devices running both 6.0 and 8.0 releases, the data is displayed for the device with the release that supports the counter.
The default polling interval value set by Command Center is 300 seconds. If you do not change the default polling interval, Command Center polls data from the devices every 5 minutes (300 seconds) and stores this data in its database. You can view the last polled data using quick reports, custom reports, or trend reports. The different types of reports are explained in the following sections. Note that if you have a higher number of counters enabled, it is advisable to set a higher polling interval to prevent performance overload on the network. However, if you want more detail, you may enable only a few counters and decrease the polling interval value. The minimum polling interval value Command Center supports is 30 seconds.

To configure polled counters

1. On the **Reporting** tab, in the left pane, click **Performance**.
2. In the right pane, click Configure Polled Counters.
3. In the Polled Counter Configuration window, select the NetScaler or **CloudBridge** tab based on the type of device for which you want to enable polling, and select the counters you want to poll. NetScaler devices include NetScaler Gateway and NetScaler VPX device types.
4. In Polling Interval, type the time interval (in seconds) at which you want Command Center to poll the counters.

Running Quick Reports

Jun 05, 2013

Run quick reports to quickly view performance data for a single device. Performance data is displayed in a graphical format and the data is used to troubleshoot or analyze the behavior of a device. You can view the data for only one scalar counter and one or more instances of a vector counter on a selected device over a specified time interval. For more information about scalar and vector counters, see Configuring Polled Counters.

You can also export the performance graph report to a file in CSV or XML format. This file can be saved locally.

Each quick report generates three charts and each chart plots a different time interval: the top chart plots data in 5-minute intervals, the middle chart plots hourly average data for three months, and the bottom chart plots daily average data for one year. However, you can customize the number of days for which you want to collect and maintain performance data.

To run quick reports

1. On the Reporting tab, in the left pane, expand **Performance**, and then click Quick Report.
2. Under Quick Report, in Device Family, select the type of device for which you want to generate a quick report. The NetScaler device family includes NetScaler Gateway and NetScaler VPX device types.
3. In Device Name, select the IP address of the device for which you want to generate a quick report.
4. In Group, select the counter group. Depending on the type of group you select, the options in Counter change, and the availability of the Type and Instance fields may vary. Provide the appropriate information as needed.
   Note: If you want to view only those counters with non-zero values, select the Exclude zero values check box.
5. In Period, select the time interval for which you want to view the specified counter. If you select Custom, select the Start Date and End Date.
   Note: The values specified in Period are displayed only in the top chart. By default, two other charts are plotted for hourly and daily average data for the counters selected in the previous steps. These two other charts are plotted for a time duration of three months and one year, respectively. You can change the duration using the Settings option on the View Graph page.
6. Click View Graph. On the View Graph page, you can perform additional tasks, such as customizing graph series, changing the scale, modifying the report settings, exporting data to your local system, and refreshing the report. For more information, click Help on the View Graph page.

Configuring Custom Reports

May 24, 2012

Use custom reports to view performance data across a set of multiple devices and to view performance data for multiple counters from one or more devices. You can add your own custom reports and save them with user-defined descriptive names for reuse. The custom reports can be viewed in a graphical format.

Each custom report consists of three charts and each chart plots a different time interval: the top chart plots data in 5-minute intervals, the middle chart plots hourly average data, and the bottom chart plots daily average data. You can also export the performance graph report to a file in CSV or XML format. This file can be saved locally.

You can schedule custom reports to run at a specified time and send the report as an email notification in CSV, XML, or graph formats when the report is run. You can also modify and delete the custom reports.

You can do the following with custom reports:

- Using Built-in Custom Reports
- Adding Custom Reports
- Viewing Custom Reports
- Scheduling Custom Reports
- Modifying Custom Reports
- Deleting Custom Reports

Using Built-in Custom Reports

Command Center provides sixteen built-in custom reports. You can view these built-in reports and also save them to your local system. You can also schedule these reports to run at a specified time. However, you cannot modify or delete the built-in custom reports.

The sixteen built-in custom reports are:

ResourceUtilization

Use this report to analyze the CPU and memory utilization by different devices at specific time periods. This report provides information about the average resource load across multiple devices in your network.

HTTP requests – TCP connections

Use this report to analyze the number of HTTP requests received and the number of TCP connections on different devices at specific time periods. Use this information to analyze the resource load across multiple devices in your network.

TCPMultiplexing

Use this report to view the number of client and server connections for each vserver on each device across multiple devices in your network.

VirtualServerThroughputDistribution

Use this report to view the number of request and response bytes on the vservers and the services bound to each vserver across multiple devices in your network. With this report, you can learn how the resource load on a particular virtual server is being redistributed to the individual bound services based on the current load balancing algorithm and/or also how the load is distributed among the virtual servers across devices.

CloudBridge acceleration

Use this report to analyze the pattern of accelerated traffic (KBPS by service class) and the number of accelerated TCP

connections passing through the CloudBridge devices. This number includes the number of TCP connections passing through the CloudBridge device that undergo acceleration, the number of open and half-closed connections that have been selected for acceleration, and the number of half-open connections that are candidates for acceleration.

Repeater Application

Use this report to view the sent and received data volume in bits-per-second for the applications running on the Repeater devices.

Repeater Capacity Increase

Use this report to view the cumulative send compression ratio for the Repeater device.

Repeater CPU Utilization

Use this report to view the CPU utilization of the Repeater device as a percentage.

Repeater Data Reduction

Use this report to view the transmit and receive bandwidth savings as a percentage. You can also analyze the transmit bandwidth and receive bandwidth saving values separately for the Repeater device.

Repeater Link Utilization

Use this report to view the transmit link utilization and receive link utilization for the Repeater device as a percentage.

Repeater Packet Loss

Use this report to view the link dropped sent packets and link dropped received packets for the links defined in the Repeater device.

Repeater Pass Through Connection

Use this report to view the non-accelerated connections for the Repeater device.

Repeater Plugin Usage

Use this report to view the number of plugins connected to Repeater device.

Repeater Traffic Shaping

You can view the Repeater QOS Sent and Repeater QOS Receive volume in bits-per-sec for the Repeater device.

Repeater Service Class

You can view the sent and receive bandwidth savings based on the service class type defined for the Repeater device.

Repeater Throughput

You can view the link sent volume and link received volume in bits-per- second for the Repeater device.

Adding Custom Reports

Updated: 2013-07-22

You can add your own custom reports and save them with user-defined descriptive names for reuse.

When adding a custom report, you can assign an aggregate function to the desired counters. The aggregate functions supported are Sum, Average, Minimum, and Maximum. The aggregate function is applied to the selected counters for all the selected devices.

To add custom reports

1. On the Reporting tab, in the left pane, expand **Performance**, and then click Custom Reports.
2. In the right pane, under Custom Reports, click Add.
3. Follow the steps in the wizard, and then click Finish. The custom report is listed under Custom Reports.

Viewing Custom Reports

Updated: 2014-04-15

The custom reports are displayed in a graphical format. Each custom report consists of three charts and each chart plots a different time intervals:

- Top chart. Plots data in 5-minute intervals and displays performance data for the time period you selected when creating the custom report.
- Middle chart. Plots hourly average data for the specified time period. By default, displays data for the last three months.
- Bottom chart. Plots daily average data for the specified time period. By default, displays data for the last year.

Options for displaying each chart are Line, Area, Bar, Stacked Area, and Stacked Bar views. You can use the Zoom In function to zoom in to each data point in a plotted series. Use the Zoom Out function to zoom out of it.

To view custom reports

1. On the Reporting tab, in the left pane, expand **Performance**, and then click Custom Reports.
2. In the right pane, under **Custom Reports**, click the report you want to view, and from the action drop-down list click **View Graph**.
3. Under Graph Options, in Devices, select the IP addresses of the device(s) for which you want to run the report.
   Note: If the device contains vector counters, you have the option to choose instances. In Choose Instances, select the instances for which you want to run the report.
4. In Period, select the time interval for which you want to view the specified counter. If you select Custom, select the Start Date and End Date. The values specified in Period are displayed only in the top chart. By default, two other charts are plotted for hourly and daily average data for the counters selected in the previous steps.
   Note: If you want to view only those counters with non-zero values, select the Exclude zero values check box.
5. Click View Graph.
   Note: On the View Graph page, you can perform additional tasks, such as customizing graph series, changing the scale, modifying the report settings, exporting data to your local system, and refreshing the report. For more information, click Help on the View Graph page.

Scheduling Custom Reports

You can schedule custom reports to run at a specified time and send the report as an email notification in CSV, XML, or graph formats when the report is run. However, note that you may not want to attach a report that contains a large amount of data.

To schedule custom reports

1. On the Reporting tab, in the left pane, expand **Performance**, click Custom Reports.
2. In the right pane, under **Custom Reports**, click the report you want to schedule, then click **Schedule**.
3. Under Schedule, in Devices, select the IP addresses of the device(s) on which you want to run the report.
   Note: If the device contains vector counters, you have the option to choose instances. In Select Instances, select the instances for which you want to run the report.
4. In Period, select the time interval for which you want to view the specified counter. The values specified in Period are displayed only in the top chart. By default, two other charts are plotted for hourly and daily average data for the counters selected in the previous steps.
   Note: If you want to view only those counters with non-zero values, select the Exclude zero values check box.
5. Under Schedule Details, select one of the following:
   - Daily: Specifies that reports run daily. In Scheduled Hours, specify the hour(s) when you want the report run.

- Day(s) of week: Specifies that reports run on certain days of the week. In Day(s) of week, select the day(s) when you want to run the report, and in Scheduled Hours, specify the hour(s) at which you want the report run.
- Day(s) of month: Specifies that reports run monthly. In Day(s) of month, specify the dates when you want to run the report, and in Scheduled Hours, specify the hour(s) at which you want the report run.

6. Under Choose Report format, select one or more formats for the report output. If you want to send the report as an email attachment, select the E-mail the report check box and fill out the required fields.
   Note: Click **Test Mail** to check if the mail server credentials provided are accurate and if the mail server is accessible from command center server. If the connection to the mail server is successful, a test mail is sent to the specified email and the settings are saved.
7. Click **OK**.

Modifying Custom Reports

Updated: 2014-04-15

You can modify the custom reports you have added. You cannot modify built-in custom reports.

To modify custom reports

1. On the Reporting tab, in the left pane, expand **Performance**, click Custom Reports.
2. In the right pane, under **Custom Reports**, click the custom report you want to modify, and then click Edit.
3. Follow the steps in the wizard, and then click Finish.

Deleting Custom Reports

You can delete the custom reports you have added. You cannot delete built-in custom reports.

To delete custom reports

1. On the Reporting tab, in the left pane, expand **Performance**, click Custom Reports.
2. In the right pane, under **Custom Reports**, click the custom report you want to delete, then click **Delete**. Alternately, right-click the custom report, and then click **Delete**.

Configuring Thresholds to Monitor Devices

May 24, 2012

Thresholds are used to monitor the state of a discovered Citrix device. You can set a threshold for a specific counter to monitor devices or instances of entities configured on managed devices as follows:

- All devices. Thresholds are applied to all devices by default.
- Specific instances of entities on managed devices. You can select specific instances of entities, such as virtual servers and services configured on managed devices, for which you want to set the threshold.
- Specific devices. You can select specific devices on which you want to set the threshold.
- Specific instances of specific entities of managed devices. You can select specific devices and then select instances of entities, such as virtual servers and services, for which you want to apply the threshold.

When monitored values (values collected during polling) for the counters are collected for each device instance, the Command Center server checks the monitored values against the corresponding threshold values. If the monitored value exceeds the threshold, Command Center generates an event to signify a performance-related issue on the device or the device instance.

When the threshold is breached, events are generated and displayed on the Fault tab. You can resolve these events from the Fault tab. For information about resolving the events, see Monitoring and Managing Events Generated on Citrix Devices. When the selected 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 perform the following tasks with thresholds:

- Adding Threshold Limits
- Modifying Thresholds
- Deleting Thresholds

Adding Threshold Limits

When adding threshold limits, you need to specify threshold values and clear values. When the monitored value of a counter exceeds the threshold value, Command Center generates an event to signify a performance-related issue on the device or the device instance. When the selected 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 define an action associated with the threshold. When the threshold is breached, the action you define is taken automatically.

Note: Command Center 3.3 and later versions support only sending email notifications action.

To add a threshold and associated action

1. On the Reporting tab, in the left pane, expand Performance, click Thresholds.
2. In the right pane, under Thresholds, click Add.
3. Under Add Threshold, do the following:
   - In Threshold Name, type a unique threshold name.
   - In Device Family, select the type of device on which you want to set the threshold limit.
     Note:
     The NetScaler device family includes NetScaler Gateway and NetScaler VPX device types.

By default, the threshold applies to all devices. If you want to specify specific devices or specific entities of managed devices, clear the Apply to all devices check box, and then, in Devices, specify the devices or entities.

- In Group, select the counter group. Depending on the type of group you select, the options in the Counter field change and the availability of the Type and Instance fields may vary. Provide the appropriate information as needed.

4. Click Criteria and do the following:
   - Specify whether the monitored value is greater than or equal to or less than or equal to the threshold value.
   - In Threshold Value, type the value for which the event severity is calculated. For example, you may want to generate an event with critical severity if the monitored value for CPU usage reaches 80 percent. In this case, type 80 as the threshold value.
   - In Clear Value, type the value that indicates when to clear the value. For example, you may want to clear the CPU usage threshold when the monitored value reaches 50 percent. In this case, type 50 as the clear value.
   - In Event Severity, select the security level that you want to set for the threshold value.
   - In Event Message, type a message that you want to appear when the threshold is met. Command Center appends the monitored value and the threshold value to this message.
5. Under Action, do the following:
   - In Action Type, select the action you want to specify (for example, Send e-mail Action).
     Note: Command Center 3.3 and later versions support only sending email notifications.
   - In From, To, and Server Name/IP Address, type the respective email address of the sender, the email address(es) of the recipients separated by commas, and the IP address of the mail server that you want to use to send the email notification.
     Note: If you have configured the mail server settings on the Admin tab, the From, To, and Server Name / IP Address fields are updated automatically.
   - Select the Mail server requires authentication check box, and type the user name and password if your mail server is configured to authenticate the email addresses.
6. Click OK.

Modifying Thresholds

Updated: 2014-04-15

You can modify the devices or instances of a device associated to a particular threshold. You can also modify the threshold value you have set.

You can unset the action associated with the threshold when modifying the threshold.

To modify thresholds

1. On the Reporting tab, in the left pane, expand Performance, click Thresholds.
2. In the right pane, under Thresholds, click the threshold name that you want to modify, and then click Edit. Alternately, right-click the threshold name and click Edit. .
3. Under Modify Threshold, edit the parameters you want to modify, and then click OK.
   Note: You can modify only the Devices and Instances fields and information on the Criteria and Action tabs.

Deleting Thresholds

You can delete a threshold if you do not want to use it anymore. When you delete a threshold, the action associated with that threshold is also deleted.

To delete thresholds

1. On the Reporting tab, in the left pane, expand Performance, click Thresholds.
2. In the right pane, under Thresholds, select the threshold that you want to delete and then click **Delete**.

Monitoring the Status of CloudBridge Devices

May 26, 2015

You can use the CloudBridge Dashboard to view the status of all the CloudBridge Devices being managed by Command Center. You can view the Name, Operation State, System Load, Data Reduction, WAN Sent, WAN Received, LAN Sent, and LAN Received data for each of the discovered device. The dashboard data is refreshed after each polling interval. The default interval is 5 minutes.

Note: The Dashboard does not display the data of CloudBridge Devices whose state is Failed, or Unmanaged. Also, if you have disabled a counter, the corresponding Dashboard value is not displayed.

Using the Dashboard

Updated: 2015-03-31

Use the CloudBridge Dashboard to view the operational status of the CloudBridge devices. By default, the Dashboard data is refreshed every 5 minutes, you can change it by setting the polling interval value in Command Center.

To use the Dashboard

1. On the **Monitoring** tab, in the left pane, under **CloudBridge**, click **Dashboard**.
2. In the right pane, under **Dashboard**, you can view the following:
   - Name - The name or IP address of the device.
     Note: If you discover a CloudBridge appliance by using both IPv4 and IPv6 addresses, the screen displays both the IP addresses in different rows.
   - Operation State - Status of the device.
   - System Load(%) - The percentage of CPU utilization on the device.
   - Data Reduction(%) - The percentage of bandwidth reduction.
   - WAN Sent (Mbps) - Current WAN bandwidth usage in the sending direction.
   - WAN Received(Mbps) - Current WAN bandwidth usage in the receiving direction.
   - LAN Sent(Mbps) - Current LAN bandwidth usage in the sending direction.
   - LAN Received(Mbps) - Current LAN bandwidth usage in the receiving direction.
3. Click the arrow next to the name of a device to view the connection details for that device.
   - Accelerated Connections - Current number of accelerated connections.
   - Unaccelerated Connections - Current number of unaccelerated connections.

Monitoring AppFirewall Syslog Events

May 27, 2015

Use Command Center to monitor security violations encountered on the NetScaler devices by the Application Firewall module. Run built-in reports to monitor the top security violations encountered by the application firewall feature. Also, view the details of the AppFirewall log messages when a message is generated on a security violation. Further configure views to monitor specific violations, and use the Search functionality to search for specific log messages.

This topic includes the following details:

Using the Dashboard

Use the Application Firewall dashboard to monitor security violations encountered on the NetScaler devices by the Application Firewall module. By default, you can view the security violations encountered in the last one week during the day.

To monitor the AppFirewall syslog events dashboard

1. On the Reporting tab, in the left pane, under AppFirewall, click Dashboard.
2. In the right pane, under Dashboard, you can view the following:
   - Violations by type: Specifies the number of violations for each type of threat, such as Deny URL, SQL Injection, and Cross-site Script.
   - Number of violations: Specifies the total number of violations that are blocked, not blocked, and transformed.
   - Signature violations by category: Specifies the number of violations encountered by types of application firewall signatures, such as web-cgi, web-client, and so on. The application firewall signatures function provides specific rules (or signatures), and specific SQL injection and cross-site scripting patterns, that protect your Web sites against known attacks. For more information about signatures, see the "Signatures" chapter in the *Citrix Application Firewall Guide*.
   - Top 5 clients by violations: Specifies the top five clients that have encountered security violations.
   - Top 5 NetScalers by violations: Specifies the top five devices that have encountered security violations.
   - Top 5 profiles by violations: Specifies the top five profiles that have encountered security violations.
   - Recent 5 violations: Specifies the recent five security violations.
3. To view violations in the last 24 hours, or last 2 weeks, or for a custom period of time, under Dashboard, click Settings.

Using Reports

Command Center provides four built-in reports to monitor the top security violations encountered by the application firewall feature. These reports let you monitor violations encountered by clients, devices, and profiles, and also the different types of violations.

The four reports are:

- Top violations by client
- Top violations by profile

- Top violations by device
- Top violations by type
- Top signature violations by category

To monitor the AppFirewall syslog events using reports

1. On the Reporting tab, in the left pane, under AppFirewall, click Reports.
2. In the right pane, under Reports, you can do the following:
   - View Graphs: Click the built-in report and click View Graph to view the graphical report of the top 5, 10, 15, or 20 violations encountered during the last 24 hours, one week, two weeks, or a period of time.
   - Schedule Reports: Click the built-in report, and click Schedule Report to run the violations reports at a later date and time.
   - View Scheduled Reports: Click Scheduled Reports to view the details of the date and time when the reports are scheduled to be run.

Viewing Recent Log Messages

You can view the details of the AppFirewall log messages when a message is generated on a security violation. You can also search for specific log messages based on the entire message text or a substring of the message.

To view the recent AppFirewall Log Messages

1. On the Reporting tab, in the left pane, under AppFirewall, click Recent Logs.
2. In the right pane, under Recent Logs, you can view the following details for each security violation:
   - Date/Time: Specifies the date and time when the violation was encountered.
   - Source: Specifies the IP address, the system name, or the host name of the NetScaler device on which the violation was noticed., based on the device label configuration. For more information about configuring the device label, see Configuring Server Settings.
   - Event ID: Specifies the unique identification number of every NetScaler syslog.
   - Transaction ID: Specifies the unique identification number of every AppFirewall syslog message from the NetScaler appliance.
   - Message: Specifies the message that is generated on the device when the violation occurs. The message describes the type of violation.
3. To search for log messages based on message string, in Search type the message text or a substring of the message, and then click GO. For example, if you want to view the log messages for a specific session, such as 232173, type 232173. And, if you want to view all log messages for the profile pr_html, type pr_html.

Configuring Views

You can add views to monitor specific types of AppFirewall log messages based on the source, violation type, message generated, and date range. Views make it easier to monitor a large number of violations encountered by the AppFirewall module. For example, you can create a view to monitor all violations of type Deny URL.

The views you create are associated with your Command Center user account.

Adding Views

You can create different views for various types of AppFirewall log messages that are generated on the devices monitored in the Citrix network when a security violation is encountered.

To add views to monitor AppFirewall logs

1. On the Reporting tab, in the left pane, under AppFirewall, expand Recent Logs, and then click **Views**.
2. In the right pane, under Views, click **Add**.
3. Under Create Recent Logs View, fill the following details.
   - Name: The user-defined view name. Type a name for the AppFirewall log view.
   - Devices: The IP address of the device on which the log is generated when the violation occurs. Select the IP addresses of the devices for which you want to create the view.
   - Violation Type: The type of violation encountered by AppFirewall, such as SQL Injection and Deny URL. Select the violation types for which you want to create the view.
   - Profile: The profile containing the security checks that you want the Application Firewall to use when filtering a particular request or response, and how to handle a request or response that fails a security check. Type the name of the profile for which you want to create the view.
   - Client IP: The client IP that the client used to connect to your protected Web server. Type the IP address of the client based on which you want to create the view.
   - URL: The URL to which requests are directed.
   - Message: The log message that is generated. Select the operator, such as equals, not equals, and then type the message for which you want to create the view. Note that the message should be exactly the same as it is generated on the NetScaler device.
   - From Date and To Date: The date range when the syslogs are generated. Select the range for which you want to create the view.

Modifying Views

Use the Modify View option to modify the AppFirewall views you have created.
To modify views to monitor AppFirewall logs

1. On the Reporting tab, in the left pane, under AppFirewall, expand Recent Logs, and click **Views**.
2. In the right pane, under Views, click the view name you want to modify.
3. In the right pane, click Modify View.
4. Under Configure Recent Log View, modify the values you want to change, and then click OK.

Searching Recent AppFirewall Log Messages

Use the Search functionality to search for specific AppFirewall log messages.

Use either the entire log message or a substring of the message to search, or use one of the following criteria to search:

- Client IP: The IP address that the client used to connect to your protected Web server.
- Date : The date range when the syslogs are generated. Select the date and time for which you want to search the syslog messages. You can search for Syslog messages generated within a range of time by selecting the ‘is between’ sub-criterion of date criteria.
- Message: The syslog message that is generated. Select Message and then type the message based on which you want to search the syslog messages. Note that the message should be exactly the same as it is generated on the NetScaler device.
- Profile: The profile containing the security checks that you want the Application Firewall to use when filtering a particular request or response, and how to handle a request or response that fails a security check. The IP addresses of the devices for which you want to search the syslog messages.
- URL: The URL to which requests are directed.

- Violation Type: The type of violation encountered by AppFirewall, such as SQL Injection and Deny URL.

To search for log messages

1. On the Reporting tab, in the left pane, under AppFirewall, click Recent Logs.
2. In the right pane, under Recent Logs, click Search icon.
3. In the search pane, use the drop down list to select the filter criteria. Enter the search keyword in the text box. You can also use the logical operators to define the search keyword.
4. Click **+** icon or press the Enter key to add the criteria, and then click Refine Search. The search results are displayed.

Monitoring NetScaler Gateway Syslog Events

May 27, 2015

You can use the Command Center dashboard to view graphical reports of NetScaler Gateway user sessions. The reports are based on parameters such as session access, ICA applications accessed, bandwidth usage, client type usage, EPA scan failures, and log in failures. NetScaler Gateway log messages also provide information about these parameters.

This topic includes the following details:

- Using the Dashboard
- Viewing Recent Log Messages
- Configuring Views
- Discarding NetScaler Gateway Syslogs

Using the Dashboard

Use the dashboard to monitor usage reports of the NetScaler Gateway devices. By default, you can view daily usage reports on the basis of various parameters.

To monitor the NetScaler Gateway syslog events dashboard

1. On the Reporting tab, in the navigation pane, expand NetScaler Gateway, and then click Dashboard or, in the details pane, click the Dashboard icon.
2. In the details pane, under **Dashboard**, you can view the following graphical reports:
   - **Top 10 users by session**: Displays the top ten users accessing applications through NetScaler Gateway. The report is based on the number of sessions for each user.
   - **Top 10 ICA applications by user access.** Displays the top ten ICA applications accessed by the users.
   - **Top 10 users by bandwidth** . Displays the top ten users in terms of bandwidth consumption across NetScaler Gateway sessions.
   - **Client type usage.** Displays the distribution of the NetScaler Gateway usage by client type (for example, e.g. Clientless VPN, Java, ICA, Agent.)
   - **Top 10 users by EPA scan failures.** Displays the top ten users whose devices failed to comply with the Citrix End Point Analysis (EPA) policy configured on NetScaler Gateway.
     Citrix Endpoint Analysis scans a user device and detects information such as the presence and version level of operating system, antivirus, firewall, or browser software. Use Citrix Endpoint Analysis to verify that the user device meets your requirements before you allow it to connect to your network. You can monitor files, processes, and registry entries on the user device throughout the user session to ensure that the device continues to meet requirements.
   - **Top 10 users by failed attempts.** Displays the top ten users experiencing failed login attempts. This report can help identify a breach to the VPN access.
3. To view usage reports in the last 24 hours, or last one week, or last two weeks, select the required time period from the drop-down menu in the Dashboard.
4. Click the graph to drill down and view the details on the Reports page.

Viewing Recent Log Messages

Updated: 2014-04-16

You can view the details of the NetScaler Gateway log messages when a message is generated on usage parameter.

To view the recent NetScaler Gateway Log Messages

1. On the Reporting tab, expand NetScaler Gateway in the navigation pane and then click Recent Logs. Alternately, click Recent Logs icon in the right pane.
2. In the right pane, under Recent Logs, you can view the following details for each of the message:
   - **Date** : Specifies the date and time when the event occurred.
   - **Source** : Specifies the IP address, the system name, or the host name of the NetScaler Gateway device for which the message was generated.
   - **Event ID** : Specifies the unique identification number of every NetScaler Gateway syslog.
   - **Description** : Specifies the message that is generated on the device when the event occurs. The message describes the type of event.

Configuring Views

You can add views to monitor specific types of NetScaler Gateway log messages based on parameters such as session access, ICA applications accessed, bandwidth usage, client type usage, EPA scan failures, and logon failures. Views make it easier to monitor data on NetScaler Gateway user sessions.

The views you create are associated with your Command Center user account.

Adding Views

You can create different views for various types of NetScaler Gateway log messages that are generated on the devices monitored in the Citrix network.
To add views to monitor NetScaler Gateway logs

1. On the Reporting tab, in the left pane, under **NetScaler Gateway**, expand Recent Logs, and then click **Views**.
2. In the right pane, under Views, click **Add**.
3. Under Create Recent Logs View, fill the following details.
   - Name: The user-defined view name. Type a name for the NetScaler Gateway log view.
   - Devices: The IP address of the device on which the log is generated. Select the IP addresses of the devices for which you want to create the view.
   - Type: The type of NetScaler Gateway log types generated on the devices, such as LOGIN,LOGOUT,ICASTART,TCPCONNSTAT, HTTPREQUEST and others. Select the types for which you want to create the view.
   - User Name: Type the name of the profile for which you want to create the view.
   - Client IP: The client IP that the client used to connect to your Web server. Type the IP address of the client based on which you want to create the view.
   - Vserver: Type the virtual server details.
   - Client Type: Select the client type, such as Java, Agent, Clientless, ICA, or Mac.
   - Message: The log message that is generated. Select the operator, such as equals, not equals, and then type the message for which you want to create the view. Note that the message should be exactly the same as it is generated on the NetScaler device.
   - ICA Application Name: Type the ICA application that you want to access.
   - From Date and To Date: The date range when the syslogs are generated. Select the range for which you want to create the view.

Modifying Views

Updated: 2014-04-16

Use the Modify View option to modify the NetScaler Gateway views you have created.
To modify views to monitor AppFirewall logs

1. On the Reporting tab, in the left pane, under **NetScaler Gateway**, expand Recent Logs, and click **Views**.
2. In the right pane, under Views, click the view name you want to modify.
3. In the right pane, click Edit.
4. Under Configure Recent Log View, modify the values you want to change, and then click OK.

Discarding NetScaler Gateway Syslogs

Updated: 2015-03-18

A large number of syslog records can occupy an excessive amount of the Command Center server space. If you do not want the Command Center server to store obsolete syslog records generated by NetScaler Gateway devices, you can create a NetScaler Gateway filter that discards those records.

After you create the filter, the Command Center server discards the syslogs that meet the criteria you specified.

To create a NetScaler Gateway Syslog

On the Reporting tab, in the left pane, expand NetScaler Gateway, click Filters, then click Add, and specify the filter criteria.

Administering Command Center

Nov 04, 2016

After logging on to Command Center, you can modify the default settings and configure various parameters for reporting and security.

You can configure the discovery settings and device profiles that are used when discovering or rediscovering a device. You can configure global settings for fault, certificate management, and monitoring using the server settings option. You can configure the inventory settings to specify the time when you want to download the configuration and license files, and the number of downloaded files you want to store in the database.

You can also configure the high availability (HA) parameters if your Command Center is set in an HA mode. Further, you can configure your mail server settings.

If you have installed Command Center agents, you can configure the agent settings and assign devices to each agent. You can also generate support logs and view the server logs, and change the database password or shut down the Command Center server.

In this section:

Configuring Discovery Settings

Apr 15, 2014

You can set default values for discovery configuration settings, including SNMP time-out, the number of SNMP retries, rediscovery intervals, and status polling intervals.

- SNMP Timeout: Specifies the maximum amount of time, in seconds, that the Command Center server will wait for the Citrix device to return a response for an SNMP request. If the time to receive the response exceeds the specified time-out value, the server gives up. By default, the time-out value is 5 seconds.
- SNMP Retries: Specifies the number of times the Command Center server attempts to connect to the device before giving up. By default, the Command Center server attempts to connect to the device three times before giving up.
- Rediscovery Interval: Specifies the duration for which Command Center waits until the next rediscovery. The default value is 60 minutes. You can specify the rediscovery interval only in terms of minutes (integer values).
- Status Poll Interval: Specifies the duration for which Command Center waits to poll the status of all discovered devices. The default value is 1800 seconds (30 minutes). You can specify the status polling interval only in terms of seconds (integer values). For example, to specify an interval of 1 hour, type 3600.

To configure discovery settings

1. On the Administration tab, in the right pane, under Settings, click Discovery Settings.
2. Under Configure Discovery Settings, in SNMP Timeout, choose a value to specify the number of seconds after which SNMP discovery must time out.
3. In SNMP Retries, choose a value to specify the number of retries that Command Center must perform when discovering a device using SNMP.
4. In Re-Discovery Interval, type the number of minutes after which Command Center must rediscover managed devices. By default, Command Center discovers devices every 60 minutes.
5. In Status Poll Interval, type the number of seconds after which Command Center must poll the status of all discovered devices.
6. Click OK.

Configuring Device Profiles

May 26, 2015

Device profiles specify the user credentials and SNMP details that are used by Command Center to communicate with the Citrix devices and retrieve configuration data and SNMP traps. You can create device profiles for the four device families: NetScaler, CloudBridge, NetScaler SDX and XenServer. These device profiles are used by Command Center to discover the Citrix devices.

This topic includes the following details:

Adding Device Profiles

You need to add device profiles to specify the user credentials and SNMP details that are used by Command Center to communicate with the Citrix devices and retrieve configuration data and SNMP traps.

To add device profiles

1. On the Citrix Network tab, under Device Inventory, click Device Profiles.
2. Under Device Profiles, click Add.
3. Under Create Device Profile, in Name, type a name for the profile and in Description, type a description for the profile.
4. In Device Family, select the device family for which you want to create the profile. The possible values are: NetScaler, CloudBridge, NetScaler SDX Platform, CloudBridge Advanced Platform, and XenServer.
5. Do one of the following:
   - For the NetScaler device family, perform the following steps.
     Note: NetScaler device family also includes NetScaler MPX, CloudBridge Connector, NetScaler VPX virtual devices, and CloudBridge devices.
     1. Specify the following user credentials for Device Login and File Transfer:
        - User Name: The user name for accessing the device. The default user name for a Citrix NetScaler device is nsroot.
        - Password: The password for the accessing device. The default password for a Citrix NetScaler device for the user name nsroot is nsroot.
        - Timeout (sec): The time-out period, in seconds, after which the Citrix Command Center server stops waiting for a connection to be established. The default time-out value is 5.
     2. To use the same user credentials for both Device Login and File Transfer, select the Use Device Login credentials for both Device Login and File Transfer protocols check box.
     3. Under SNMP, enter the following details:
        - In the Version list, select the version number of the SNMP protocol for Citrix Command Center to use. SNMP versions 1, 2, and 3 are supported.
          Citrix recommends that the NetScaler devices running release 8.0 and above use SNMP versions 2 or 3.
        - In Port, type the SNMP port number. The default port number is 161.
        - For versions 1 and 2, in Community, type the SNMP community string. The community string enables the

NetScaler device to respond to SNMP queries after a successful match.
For version 3, specify the following details:

- User Name: The user name of the SNMP user.
- Security Level: The security level of the group to which the user is assigned. The possible values are: Without Authentication and Privacy, With Authentication and without Privacy, and With Authentication and Privacy.
- Authentication Type: The authentication type assigned to the user. The possible values are MD5 and SHA.
- Privacy Type: The encryption type. The possible values are DES and AES . You can select AES as the privacy type only if the SNMP version is v3 and the security level is set to With Authentication and Privacy.
- Privacy Password: The encryption password.

- For NetScaler SDX NetScaler SDX Platform, perform the following steps.
  1. Create a NetScaler profile by following the procedure described above for adding device profile for NetScaler device family.
  2. Under User Credentials, specify the following user credentials for Device Login.
     - User Name: The user name for the device.
     - Password: Type the password for the device. The default password for a Citrix NetScaler device with the user name nsroot is nsroot.
     - Community: Type the SNMP community string. The community string enables the NetScaler SDX device to respond to SNMP queries after a successful match.
  3. In NetScaler Profile *: Select the NetScaler profile that you want to use to discover the NetScaler instances installed on the NetScaler SDX. Command Center implicitly discovers NetScaler instances installed on the NetScaler SDX device.
- For CloudBridge Advanced Platform, perform the following steps.
  1. Create a NetScaler profile by following the procedure described above for adding device profile for NetScaler device family.
  2. Under User Credentials, specify the following user credentials.
     - User Name: The user name for the device.
     - Password: Type the password for the device. The default password for a Citrix NetScaler device with the user name nsroot is nsroot.
     - NetScaler Profile : Select the NetScaler profile that you want to use to discover the CloudBridge Connector installed on the CloudBridge Advanced Platform. Command Center implicitly discovers CloudBridge Connector installed on the CloudBridge Advanced Platform .
       Note: You do not have to select a NetScaler profile for CloudBridge 2000 and 3000 models.
     - Community: Type the SNMP community string. The community string enables the CloudBridge Advanced Platform to respond to SNMP queries after a successful match.
- For the **CloudBridge** device family, perform the following steps.
  1. Under User Credentials, specify the following user credentials for Device Login and File Transfer:
     - User Name: The user name for accessing the device.
     - Password: The password for accessing the device.
       Note: By default, the user name and password for Device Login are the same as those specified for the CloudBridge user interface. The user name for File Transfer is transfer (this is populated by default), and the password is set by Command Center during the first-time discovery of the device
     - Timeout (sec): The time out period in seconds, after which the Citrix Command Center server stops waiting for a connection to be established. The default time out value is 15s.
  2. Under SNMP, specify the following details:
     - In the Version list, select the version number of the SNMP protocol for Citrix Command Center to use.
     - In Community, type the SNMP community string. The community string enables the CloudBridge device to

respond to SNMP queries after a successful match.
    - In Port, type the SNMP port number. The default SNMP port is 161.
- For XenServer, perform the following steps.
  1. Create a NetScaler profile by following the procedure described above for adding device profile for NetScaler device family. .
  2. Under User Credentials, specify the following user credentials for Device Login.
     - User Name: The user name for accessing the device.
     - Password: The password for accessing the device.
     - Port: The port at which the XenServer device listens for incoming traffic. The default port is 443.
  3. In Select NetScaler Profile: Select the NetScaler profile that you want to use to discover the NetScaler VPX devices installed on the XenServer. Command Center implicitly discovers NetScaler VPX devices installed on the XenServer.

Viewing Device Profiles

After you have configured device profiles with the user credentials and SNMP details, you can view the profiles from the Command Center client.

To view device profiles

1. On the **Citrix Network** tab, in the left pane, expand **Device Inventory**, click **Device Profiles**
2. Under Device Profiles, you can view and do the following.
   - Name: Specifies the name of the device profile you have created.
   - Device Family: Specifies the device family for which the profile is created. The possible values are: NetScaler, NetScaler SDX, CloudBridge, and XenServer.
   - Description: Specifies the description of the profile you have created.
   - Add: Click Add to add new device profiles. For more information, see Adding Device Profiles.
   - Delete: Select the profile you want to delete, and then click Delete to delete a device profile. For more information, see Deleting Device Profiles.
   - Edit: Select the profile you want to modify, and then click Modify to modify a device profile.

Modifying Device Profiles

After you have added a device profile, you can modify the values of the user credentials and SNMP details that are used by Command Center to communicate with the Citrix devices and retrieve configuration data and SNMP traps.

To modify device profiles

1. On the Citrix Networktab, in the left pane, under Device Inventory, click Device Profiles.
2. Under Device Profiles, click the profile name you want to modify, and then click Edit.
3. Under Configure Device Profile, make the required changes, and then click OK.

Deleting Device Profiles

If you do not want to use a device profile, you can delete it from your server.

To delete device profiles

1. On the Citrix Network tab, in the left pane, under Device Inventory, click Device Profiles.
2. Under Device Profiles, select the profile you want to delete, and then click Delete.

Configuring Server Settings

Nov 04, 2016

You can set the default values for the following Command Center server settings:

- SNMP Trap Destination: A Simple Network Management Protocol (SNMP) trap is a notification event issued by a managed device to the network management station when a significant event (not necessarily an outage, a fault, or a security violation) occurs. The SNMP trap destination in the Command Center context is the IP address to be used on managed devices to send SNMP traps when the Command Center server is multihomed or if there is a Network Address Translation (NAT) device between the server and the managed devices.
- SNMP Trap Port: You can specify either a single port number or multiple port numbers (separated by commas) to receive the traps. The default SNMP trap port number is 162. However, if you specify a different port number, you must configure the SNMP agent of the managed device to send the trap on the new port.
- Device Label: A device label is used when the discovered devices are displayed on a map. The default device label is the IP address of the managed device. If you choose System Name as the device label, the SNMP system names configured on the devices are shown. If you choose Host Name the devices are labeled by their DNS host names. Note that the host names are displayed only when the devices are discovered using host names. The devices located on the Citrix Network tab reflect the change.
  Note: By default, NetScaler devices have the sysname NetScaler.
- SSL Certificate Management: You can centrally manage the Secure Sockets Layer (SSL) certificates installed on the managed devices. You can poll all the managed devices for certificate status, install SSL certificates, update existing certificates, generate new certificate signing requests (CSRs), and set up polling intervals and severity levels. This feature is enabled by default. So, if you do not want to use the SSL Certificate Management feature to centrally manage the SSL certificates on all the managed devices, you must disable this feature.
  Note: Command Center supports this feature on NetScaler 7.0 and later.
- Task Execution User Credentials: You can set up authentication using the user credentials of the device for executing tasks on managed devices. You can execute tasks on the managed devices from Command Center using the same credentials used for discovering devices. However, the role-based access capabilities of Command Center allow you to override the credentials for task execution and prompt users to input their user credentials. This provides administrators the ability to control users to execute only those commands that are configured on the device using the device role-based access privileges for those user IDs.
- Performance Data Configuration: You can access the collected performance data using quick report, custom report, and trend report generators. Note that trend reports are available only in the HTML client.
  By default, for quick and custom reports, you can view performance data for the last 14 days in 5-minute granularity. In trend reports, you can view consolidated hourly data for the last 30 days and daily data for the last 365 days. However, you can customize the number of days for which you want to collect and maintain performance data.
- Monitoring: You can centrally manage the Monitoring feature for monitoring the real-time status of virtual servers, services, and service group members configured on all discovered NetScaler devices. This feature is enabled by default. In an environment with multiple NetScaler devices and many vservers, services, and service groups configured on the devices, the regular monitoring of these entities may add to the network load. If you find that this network load is too high in your environment and results in other issues, you can disable the monitoring feature for that environment.

- Syslog Clean Interval: To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. A purge job is enabled by default, and is scheduled to run at 1:00 AM daily. By default, Command Center stores syslog messages for the last 90 days. To customize the purge interval, you can specify the number of days in the Syslog Clean interval (in days) field. Only the records older than the number of days that you specify are purged. For example, if you specify as 45 days, Command Center purges syslog messages that are older than 45 days.

To configure server settings

1. On the Administration tab, in the right pane, under Settings, click Server Settings.
2. Under Configure Server Settings, do one or more of the following:
   - In SNMP Trap Destination, type the IP address of the destination system to which the SNMP traps must be sent.
   - In SNMP Trap Port, type either a single port number or multiple port numbers (separated by commas) to receive the traps.
   - In Device Label, select one of the following device labels that you want Command Center to use: System IP, System Name, or Host Name.
   - In SSL Certificate Management, click Enable or Disable.
   - In Task Execution User Credentials, click Enable or Disable.
   - Configure the following parameters:
     - Duration of performance data collected at configured interval (default: 5 minutes): Specifies the number of days for which you want Command Center to maintain performance data at the specified duration interval. The default duration is 14 days.
     - Duration of performance data consolidated at hourly interval: Specifies the number of days for which you want to maintain hourly performance data. The default duration is 30 days.
     - Duration of performance data consolidated at daily interval: Specifies the number of days for which you want to maintain the daily performance data. The default duration is 365 days.
       Note: You must restart the Command Center server to complete the performance data configuration.
   - In Monitoring, click Enable or Disable.
   - In Syslog Clean interval (in days), specify the number of days you want to retain syslog data.

To configure event purge settings

You can now specify the number of days after which event data will be deleted from the Command Center server.

1. Navigate to **Administration** > **Database Management**.
2. In the right pane, select **Event Purge Settings** under **Database Management** and enter the purge interval in days.
3. Click **OK**.

Configuring Purge Settings

Nov 04, 2016

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the NetScaler 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 purge syslog data. You can specify the number of days after which the following syslog data will be deleted from the Command Center server:

- Generic Syslog Data
- AppFirewall Data
- NetScaler Gateway Data

You can also configure the NetScaler Gateway purge interval by syslog type. This purge interval takes precedence over the purge interval configured to retain NetScaler Gateway data.

To configure purge settings

1. Navigate to **Administration** > **Database Management**, and then click **Syslog Purge Settings**.
2. In the **Configure Syslog Purge Settings** page, enter the following details:
   - **Retain Syslog Generic Data** - Specify the number of days after which the Command Center server deletes generic syslog messages.
   - **Retain AppFirewall Data** – Specify the number of days after which the Command Center server deletes AppFirewall syslog messages.
   - **Retain NetScaler Gateway Data** – Specify the number of days after which the Command Center server deletes NetScaler Gateway syslog messages.
3. Select the **Configure NetScaler Gateway Purge Interval by Syslog Type** checkbox if you want this to take precedence over the purge settings interval configured to retain the NetScaler Gateway data.
4. Select one or more of the following options to edit:
   - **Type** - The type of NetScaler Gateway syslog types generated on the devices, such as Login, Logout, Login failed, ICA proxy session start, and others. Select the type for which you want syslog data deleted from the Command Center server.
   - **Purge Interval (Days)** - The time interval between two successive purge operations performed on syslog data. Click on the number to make the field editable.
5. Under **Configure Syslog Purge Time**, specify the syslog purge scheduling time (in hours). Use the 24 hour format.
6. Click **OK**

CloudBridge Registration

Aug 11, 2014

The CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800) can initiate discovery by Command Center, by configuring the IP address, port, and password of the Command Center server on the CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800). The appliances then use NITRO APIs to send registration requests to Command Center. Command Center server then automatically starts the discovery process.

With this feature, you can also choose to apply configuration profiles on multiple devices at the same time. On Command Center, you must first specify the CloudBridge serial number or IP address of the CloudBridge device and also specify the configuration profiles that you want to apply on the CloudBridge device(s). For more details, see Automatically Configuring CloudBridge Devices..

By default, the CloudBridge registration feature is enabled on Command Center.

Note: CloudBridge registration is supported only on the CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800). .
Command Center uses the following default profiles for discovery of CloudBridge Advanced Platform and the instances:

- REGISTRATION_NS
- REGISTRATION_CB_ADVANCED_PLATFORM
- REGISTRATION_CB

You can view the discovery status on the Command Center server when you navigate to the Citrix Network > Dsicoverystatus tab. You can also view the status of the registration request on the CloudBridge Advanced Platform.

To register a CloudBridge Advanced Platform (CloudBridge 400 and CloudBridge 800)

1. Enter the Command Center parameters on the CloudBridge Advanced Platform.
   1. On the appliance, navigate to Configuration > Appliance settings > Logging/Monitoring and click Command Center.
   2. Provide the following details:
      - IP Address-IP address of the Command Center server
      - Port-Port number of Command Center
      - Registration password-Registration password to register Command Center
   3. To apply configuration profiles on multiple devices, choose AutoConfiguration By Citrix Command Center.
   4. Click Update.
      The CloudBridge Advanced Platform initiates the discovery process on Command Center, which uses the default profiles
2. On the Command Center server, you can view the discovery status of the CloudBridge Advanced Platform and the associated instances.
   - On the Citrix Network tab of the Command Center interface, navigate to Device Inventory > Devices > Discovery Status.
   - View the discovery status of the CloudBridge Advanced Platform and the associated instances.

To modify the registration settings

Optionally, you can modify the registration details on the Command Center server. To modify the details, navigate to Administration > Settings > CloudBridge Registration Settings . In the Configure CloudBridgeRegistration Settings, you can specify the following details:

- Status— You can enable or disable the registration feature on Command Center. Default value: Enable.
- Default Profile— Choose the profile that you want to use for the registration process. Default Value: AUTO_REGISTRATION_CB_ADVANCED_PLATFORM. Possible Values: The device profiles created for CloudBridge Advanced Platform in Command Center.
- Registration Requests Threshold Limit— Maximum number of registration requests process per minute. Default: 5; Minimum: 5; Maximum:10
- You can also modify the default registration password by providing the current and the new password in their respective fields.

Configuring Inventory Settings

Apr 17, 2014

With inventory management, Command Center downloads the configuration and license files and SSL certificate files from each discovered device and stores these files in the database. By default, Command Center downloads the files during every discovery or rediscovery of a device. However, you can configure the inventory settings feature to download the configuration and license files in the following scenarios:

- When Command Center receives the "save config" trap.
- During specific intervals set by the user.
- During a backup operation initiated by the user from the Device Properties page.

You can also configure inventory settings to specify the number of copies of the downloaded files you want Command Center to store in the database. For example, you can choose to store only one copy each of the configuration and license files that are older than one week. In this case, Command Center stores the last downloaded file set.

Note: By default, every file that is downloaded is stored in the database, and Command Center maintains the last 10 copies of the files.

To configure inventory settings

1. On the Administration tab, in the right pane, under Settings, click Inventory Settings.
2. Select one or more of the following options for archiving.
   - Archive "Save Config" Trap: Select this check box if you want the server to archive files when the "save config" trap is received.
   - Archive Interval (in hours): Specify the archive interval in hours.
3. In Number of previous archive files to retain, type the number of files that you want to retain after download.
4. Click OK.

Configuring High Availability Settings

Apr 17, 2014

You can configure two Command Center servers to work as a high availability (HA) pair by configuring one server as primary and the other server as secondary. For more information, see Installing Command Center in High Availability Mode.

Use the HA pair mode of operation to ensure uninterrupted management of network devices by allowing the secondary Command Center server to take over in case the primary server fails, terminates, or shuts down.

To configure high availability settings

1. On the Administration tab, in the right pane, under Settings, click High Availability Settings.
2. Under High Availability Details, click Edit and configure the following HA parameters:
   - Heart beat interval: Heartbeats periodically check the availability of an HA node. Specify the interval at which the primary Command Center server must update its health in a database table. The default is 60 seconds.
   - Failover interval: Failover refers to the process of the secondary node taking over when the primary server goes down. Specify the interval at which the secondary Command Center server must check the status of the primary Command Center server in the database. The default is 75 seconds.
   - Retry count: The secondary Command Center server checks the status of the primary Command Center server for failure. Specify the number of times the secondary Command Center server must check the status of the primary Command Center Server before assuming that the primary Command Center server has failed. The default is 1.
   - Backup interval: Specify the interval at which the secondary Command Center server backs up the configuration files from the primary Command Center server.
3. Click OK.

Configuring Mail Server Settings

Nov 04, 2014

Command Center uses Simple Mail Transfer Protocol (SMTP) to send email messages. You can configure the mail server settings globally from the Admin tab. Then, when you add an event or alarm trigger and associate an email action with it, the mail server settings are updated automatically for that email action. However, mail server settings specified at the event or alarm level will override global settings.

To configure mail server settings

1. On the Administration tab, in the right pane, under Settings, click Email Server Settings.
2. Under Configure Mail Server, in Mail Server, type the IP address of the SMTP mail server that you want to use to send email notifications.
3. In From and To, type the email addresses of the sender and the recipients. Note that you can enter multiple email addresses in the To field.
4. Select Mail server requires authentication and type the user name and password if your mail server is configured to authenticate email addresses.
5. Click OK. If the connection to the mail server is successful, a test mail is sent to the specified email and the settings are saved.

Configuring Access Settings

Apr 17, 2014

You can configure the security settings by changing the default communication mode (HTTP or HTTPS) and the port used between the Command Center server and the client.

To configure the security settings

1. On the Administration tab, in the right pane, under Settings, click Access Settings.
2. Under Configure Access Settings, in Server Protocol, click the communication mode you want to use.
   Note: By default, HTTPS communication mode is used.
3. In Server Port, type the port number you want to use.
4. In Session Timeout, type the length of time (in minutes) for which the session can be inactive before you must log in again. You must restart Command Center for the timeout settings to take effect. The timeout duration that you specify here is applicable to all users. However, you can specify specific timeout duration for your device on the Login page. For more information, see the "Logging on to Command Center" section in the .
   Note: You must minimize the Alarm Summary table for the session timeout to work. If the Alarm Summary table is expanded, the session is considered to be active.
5. Click OK.

Setting Up Command Center Agents

Apr 18, 2014

Command Center provides a distributed multi-tier architecture by letting you configure agents that manage and monitor the Citrix devices. This architecture reduces the load on the Command Center server by distributing the load across the different agents. Note that, for now, the agents are used only for monitoring entities and syslog messages, for polling and collecting data used for performance monitoring, such as CPU usage, resource utilization, and IP bytes transmitted, and for certificate management.

The Command Center agents are installed using the Command Center installer. For more information, see After the agents are installed and connected to the Command Center server, you can view the agent details on the Administration tab of the Command Center client. You can activate the agents from the client, and then assign devices to the agent to manage.

To set up Command Center agents

1. On the Administration tab, on the right pane, under Tools, click Agent Setup.
2. Under Agent Details, you can view and do the following.
   - Name: Specifies the IP address of the Command Center agent.
   - Status: Specifies whether the agent is active, inactive, or has been stopped.
   - Action: Based on the Status of an agent, you can take actions. If an agent is in an inactive state and is not managing devices, you need to activate the agent and assign devices to it to manage. If you want to stop an agent from managing devices, you need to deactivate it. You can activate or deactivate an agent by selecting the agent and then clicking Activate or Deactivate. To assign devices to an agent to manage, click Assign. If a Command Center agent is in an inactive state or has been stopped, you can unassign the devices managed by this device. These devices get assigned to the Command Center server. To unassign the devices managed by a Command Center agent, click Unassign for the inactive or stopped agent.

Configuring SNMP Trap Forwarding

Apr 02, 2015

You can configure Command Center to receive traps on an available port and forward them to any device. You can set the default values for the destination that receives the trap, the port number of the destination device, and the community to which the device belongs.

To configure SNMP trap forwarding

1. On the Administration tab, in the right pane, under Settings, click Trap Forward Settings.
2. Configure the following:
    1. Trap Destination: Specify the IP address of the device that receives the forwarded SNMP trap.
    2. Destination Port: Specify the port number of the device that receives the forwarded SNMP trap.
    3. Trap Community: Specify the community string of the trap receiver.
3. Click OK.

Configuring Security Settings

Nov 04, 2016

You can configure various parameters to ensure that only authenticated users log on to Command Center. You can also create users and groups and assign specific operations to the groups.

In this section:

Cascading External Authentication Servers

The Command Center server supports a unified system of authentication, authorization, and accounting (AAA) protocols, including RADIUS, LDAP, and TACACS, in addition to supporting local servers for authenticating local users and groups. The unified support provides a common interface to authenticate and authorize all of the local and external AAA clients who are accessing the system. Command Center can authenticate users regardless of the actual protocols they use to communicate with the system.

Cascading external authentication servers provides a continuous non-failing process for authenticating external users. If authentication fails on the first authentication server, the Command Center server attempts to authenticate the user by using the second external authentication server, and so on. If you **Enable fallback local authentication**, then the authentication will fallback to local Command Center authentication server if all external authentication fails.

To enable cascading authentication, you need to add the external authentication servers to Command Center. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS). For example, if you want to add four external authentication servers for cascading authentication, you can add two RADIUS servers, one LDAP server, and one TACACS server, or all servers can be of RADIUS type. You can configure up to 32 external authentication servers in Command Center.

You can add any number of external authentication profiles in Command Center by navigating to **Authentication** > **LDAP/RADIUS/TACACS**.

To configure cascading external authentication servers

1. In Command Center, navigate to **Administration**> **Authentication**. In the right pane, click **Authentication Settings**.
2. On the **Configure Authentication Settings** page, select **EXTERNAL** from the **Authentication Server** drop-down list (only external servers can be cascaded).
3. Move the available external servers from the **Available** table to the **Configured** table to add them to your instance group. You can specify the order of authentication by using the arrow keys icon in the configured table to move the server up or down the configured list.
4. You can choose to use local authentication server in case external authentication fails by selecting the **Enable fallback local authentication** checkbox.
5. Click **OK**.

Configuring Authentication Settings

Command Center supports authentication policies for external authentication of users.

When a user for whom no configuration has been created in Command Center logs on for the first time, the user is assigned to the default Users group. The administrator must assign the new user to the appropriate group or groups, depending on the privileges the user needs.

Command Center supports the following authentication servers:

- Local
- LDAP (Lightweight Directory Access Protocol)
  - Active Directory
  - OpenLDAP (Open source implementation of LDAP)
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)

Note: If you use Active Directory, OpenLDAP, or RADIUS servers for authentication, groups in Command Center are configured to match groups configured on the authentication servers. When a user logs on and is authenticated, if a group name in an authentication server matches a group name in Command Center, the user inherits the settings of the Command Center group.

Command Center supports deployment of RADIUS authentication with an Active Directory server (realm deployment). For a realm deployment, you must enable group extraction and specify the group vendor identifier and the type of group attribute.

By default, Command Center uses the local authentication.

In this section:

- Configuring the LDAP Authentication Server
- Configuring the RADIUS Authentication Server
- Configuring the TACACS Authentication Server

Configuring the LDAP Authentication Server

You can configure either an Active Directory or an OpenLDAP authentication server in Command Center. You can enable group extraction to apply Active Directory or OpenLDAP authorization settings to groups configured in Command Center.

To configure an Active Directory or OpenLDAP authentication server

1. In Command Center, on the **Administration** tab, in the right pane, under **Security**, click **Authentication Settings**.
2. Under **Configure Authentication Settings**, in **Authentication Server**, select **LDAP**.
3. In the **Server Type on which the LDAP is configured*** list, select **Active Directory** or **OpenLDAP**.
4. Set the following parameters:

- **Server Name/IP Address***. Server Name or IP address of the Active Directory or the OpenLDAP server.
- **Server Port***. Port number of the Active Directory or the OpenLDAP server.
- **Base DN***. Fully qualified domain name. For example, 'DC=company,DC=net'.
- **Administrator Bind DN***. User name of the Active Directory or OpenLDAP server. For example, admin@company.net or

CN=admin,CN=Users,DC=company,DC=net

- **Administrator Password***. Password for the Active Directory or OpenLDAP server.

5. Select the **Enable Group Extraction** option to apply the Active Directory or OpenLDAP authorization settings to groups configured in Command Center.

6. Set the following parameters:

- **Logon Name Attribute***. Name attribute used by Command Center to query the external Active Directory or OpenLDAP server. For example, sAMAccountName or uid.
- **Search Filter**. Search string to extract groups from the Active Directory or OpenLDAP server.
- **Group Attribute***. Attribute name of group extraction from the Active Directory or OpenLDAP server. For example, memberOf.
- **Group Sub Attribute***. Sub-attribute name of group extraction from the Active Directory or OpenLDAP server. For example, cn.

7. Click **OK**.

Configuring the RADIUS Authentication Server

RADIUS authentication uses a secret key, an IP address, and the port number.

If Command Center servers are configured in an HA mode, you must provide the identification code assigned to the secondary server.

To configure a RADIUS authentication server

1. In Command Center, on the **Administration tab**, in the right pane, under **Security**, click **Authentication Settings**.
2. Under **Configure Authentication Settings**, in **Authentication Server**, select **RADIUS**.
3. Set the following parameters:

- **Server Name/IP Address***. Server Name or IP address of the RADIUS server.
- **Server Port***. Port number of the RADIUS server.
- **Secret Key***. Key shared between Command Center and the RADIUS server for communication.
- **Password Encoding***. Type of encoding of passwords for packets travelling from Command Center to the RADIUS server.
- **NAS IP Address**. IP address of Command Center. The Command Center IP address is sent to the RADIUS server as the Network Access Server (NAS) IP Address.
- **NAS Identifier**. String sent to the RADIUS server as the Network Access Server ID (NASID).

4. In **Secondary Server NAS Identifier**, you must specify the NAS identifier assigned to the secondary server if Command Center servers are configured in HA mode.
5. Select the **Enable Group Extraction** option to apply the RADIUS authorization settings to groups configured in Command Center.
6. Set the following parameters:

- **Group Vendor Identifier**. RADIUS vendor ID attribute, used for RADIUS group extraction.
- **Group Attribute Type**. RADIUS attribute type, used for RADIUS group extraction.

7. Click **OK**.

Configuring the TACACS Authentication Server

Similar to RADIUS authentication, TACACS+ uses a secret key, an IP address, and the port number. The default port number is 49.

To configure a TACACS authentication server

1. In Command Center, on the **Administration** tab, in the right pane, under **Security**, click **Authentication Settings**.
2. Under **Configure Authentication Settings**, in **Authentication Server**, select **TACACS+**.
3. Set the following parameters:
- **Server Name/IP Address***. Server Name or IP address of the TACACS server.
- **Server Port***. Port number of the TACACS server.
- **Secret Key***. Key shared between Command Center and the TACACS server for communication.
- **Password Encoding***. Type of encoding of passwords for packets travelling from Command Center to the TACACS server.
4. Click **OK**.

Configuring Groups

Groups are logical sets of users that need to access common information or perform similar kinds of tasks. You can organize users into groups defined by a set of common operations. By providing specific permissions to groups rather than individual users, you can save time when creating new users.

If you are using an Active Directory server for authentication, groups in the Command Center can be configured to match groups configured on Active Directory servers. When a user belonging to a group whose name matches a group on an authentication server, logs on and is authenticated, the user inherits the settings for the group in the Command Center.

In this section:

Adding Groups

You can add groups and assign permissions to the groups.

To add groups

1. On the Administration tab, under Security, click Groups.
2. Under Groups, click Add.
3. Under Add Group, in Group Name, type the name of the new group or multiple comma-delimited groups that you want to create. In case you have enabled group extraction from Active Directory, you can browse and add groups extracted from the Active Directory server after you have configured Active Directory settings under Authentication settings. Click on the Browse button to select the group name from the retrieved Active Directory group names.
   Note: The Browse button is available only if you have enabled group extraction and provided the Active Directory group attributes.
   Important: When creating groups in the Command Center for group extraction from Active Directory, group names must be the same as those defined in Active Directory. Group names are also case-sensitive and must match those in

Active Directory. Special characters are supported in group names.

4. Select the check boxes against the permissions you want to assign for each feature. Note that selecting Grant administrative privileges assigns permission to perform all operations on only the Administration tab.

Assigning Users to Groups

You can assign Command Center users to a group depending on the permissions that you want to grant them.

To assign user to groups

1. On the Administration tab, under Security, click Groups.
2. Under Groups, click the group to which you want to assign users and from the action drop-down list select, and then click **Assign To**.
3. Under Configure Group, in Available Users, click the user(s) that you want to include in the group, and then click the + icon.

Note: To remove a selected user, click the user you want to remove in Configured Users, and then click the**-** icon.

Modifying Groups

After you have added a group, you can modify the permissions assigned to that group. You can also add or remove users assigned to a group.

You can also modify a group to provide fine-grained authorization support. You can ensure that the user performs operations only on those devices or data defined by the authorization settings assigned to his or her account or group. For example, if you want to restrict any operations that the user performs to a specific set of devices (for example, NetScaler VPX), then you must set the authorization criteria with the relevant property values as described in the following procedure.

To modify groups

1. On the Administration tab, under Security, click Groups.
2. Under Groups, click the group you want to modify.
3. To add or remove a user, and select **Assign To** from the action drop-down list, and make the modifications as required.
4. To change the permissions assigned to a group, click Edit, make changes to the permissions you want to assign for each feature.
5. To configure authorization settings, click Advanced Settings.
6. Under Advanced Settings, in Property Name, select the property for which you want to add the authorization settings (for example, Device Type), and in Property Value, enter the value of the property (for example, NetScaler VPX), and then click OK.
   Note: You can enter the property value along with the wildcard character %. For example, you can if you enter the server name as webin%, or %storfron%, then Command Center looks for server names beginning with 'webin' or server names containing the term 'storfron', then adds the authorization settings.

Deleting Groups

You can delete groups that you no longer want to use from the database. Ensure that all the users assigned to the group are removed from the group before deleting the group.

To delete groups

1. On the Administration tab, under Security, click Groups.
2. Under Groups, select the groups that you want to remove, and then click Delete.

Configuring Users

A user is an individual entity that logs on to Command Center to perform a set of device management tasks. To allow someone access to Command Center, you must create a user account for that user. After you create a user account, you can associate the user with groups and set permissions according to the group requirements.

From the Command Center interface, you can seamlessly specify local or external as the authentication type for a user. You can specify the authentication type when adding the user to Command Center, or you can edit the user's settings later.

Important: The external authentication type is supported only when you set up one of the authentication servers: Radius, Active Directory or TACACS+.
This topic includes the following details:

Adding Users

You can add new users whenever you need to provide a user access to Command Center. By default, a new user has only log on permission. You can provide access to various modules by making the user a member of pre-configured groups that contain those modules.

To add users

1. On the Administration tab, under Security, click Users.
2. Under Users, click Add.
3. In User name, type a user name for the new user and in Password and Confirm Password, type a password for the user name.
4. In **Groups**, click **Available**, and then, select the groups to which you want to add the new user.
   Note: To add the new user account to a new group, type the name of the group, and click Add.
5. In Password Expires In, type the number of days after which you want the password to expire.
   Note: If the user logs on after the password expires, the user is directed to the Change Password page to reset the password. The user can change the password only if the authentication type of the user is Local.
6. In Account Expires In, type the number of days after which you want the account to expire.
7. Set the authentication type for the user. Select Local Authentication User value as True for local authentication. For external authentication, select False.
   Note: The external authentication type is supported only when you set up one of the authentication servers: Radius, Active Directory or TACACS+.
8. Click Create. The user is added to Command Center, with the selected authorization type. You can view the details on the Users page.

Assigning Groups to a User

You must associate a user to a minimum of one group.

To assign groups to a user

1. On the Administration tab, under Security, click Users.
2. Under Users, click a user name to which you want to associate a group and from the action drop-down list select, and then click **Assign To**.
3. In Configure User, click **+ Add**, click the groups that you want to associate with the user, and then click **OK**.

Viewing Permissions Assigned to Users

You can view the permissions that are assigned to a user.

To view permitted operations assigned to users

1. On the Administration tab, under Security, click Users.
2. Under Users, click the user name for which you want to view the permitted operations and from the action drop-down list select **Assign To**.
3. In Groups page, for the groups associated, view the permitted operations by clicking Edit.

Modifying User Profiles

You can modify the user profiles you have created. You can make changes to various parameters, such as the state of a user, password to log on, password expiration, account expiration, authentication type, assigned groups, and permitted operations.

To modify user profiles

1. On the Administration tab, under Security, click Users.
2. Under Users, click the user profile you want to modify, click Edit.
3. Under Configure User, make changes as required. To modify the authentication type of the user, select the options in Local Authentication User.
   Note: If you modify the authentication type for a user from external to local, the default password is same as the username.
4. Click OK.

Changing the Root User Password

The root user account is the super user account in Command Center. The default password for the root account is public. Citrix recommends that you change the password after you install the Command Center server.

If you specify the password expiry value for the user account, the password expires after the number of days specified. When the password is about to expire, a notification is displayed when you log on to Command Center server, and you are prompted to navigate to the Change Password screen to modify the password.

In Command Center appliance, when you modify the root user credentials on the primary, the password for the root user in Command Center, SSH root user of the CentOS, SSH root user of the XenServer, and the database password in both primary and secondary devices are modified.
To change the root user password

1. On the Administration tab, under Security, click Users.
2. Under Users, select the root user name, and then click Edit.
3. Under Configure User, in New password and Re-type password, type and retype the new password you want to use, and then click OK.

Deleting Users

You can remove user accounts you do not want to use.

To delete users

1. On the Administration tab, under Security, click Users.
2. Under Users, click the user name(s) you want to delete, and then click Delete.

Configuring Password Policy

Updated: 2014-07-31

Command Center applies a password policy to provide security against hackers and password-cracking software.

The password policy specifies the minimum length and complexity of a password.

To set the password policy

On the Administration tab, click Security, and in the right pane, select Password Policy.

Viewing Audit Logs for All Users

Use audit logs to view the operations that a Command Center user has performed. The audit log identifies all operations that a user performs, the date and time of each operation, and the success or failure status of the operation. Citrix recommends that you periodically clear audit logs after reviewing them.

You can perform the following operations on audit logs:

- View the audit log details of all users or a single user.
- Sort the details by user, operation, audit time, category, AuditedObject, and status by clicking the appropriate column heading.
- Clear the audit logs when you no longer need to manage them.

To view audit logs for all users

1. On the Administration tab, in the right pane, under Security, click Audit Logs.
2. Under Audit Logs, you can view and do the following:
   - User: Specifies the user name of the user for which you can view the audit logs. Click the user name to view the audit details of that user.
   - Operation: Specifies the operation the user has performed for which the audit log is available.
   - Time: Specifies the time when the audit log was generated.
   - Status: Specifies the status of the audit, such as Success or Failed.
   - Category: Specifies the category of the operation that is audited, such as Authentication.
   - Audited Object: Specifies the security administration operations, such as operations on users or groups, that are audited by Command Center.
   - Export: Click Export if you want to export all the audited information to a CSV file.

Configuring a Command Center Appliance as an SNMP Agent

You can configure a Command Center appliance as an SNMP agent, therefore any external SNMP manager can monitor the appliance and query any of its Management Information Base (MIB) objects. To query the Command Center MIB

objects, you must specify the community string, the IP address of the SNMP Manager, and the SNMP access level.

To configure an SNMP agent

1. On the Administration tab, under Security, click SNMP Agent Configuration.
2. Click Add, and configure the SNMP agent to communicate with the SNMP manager.

Configuring Logs

May 26, 2015

The Command Center server implicitly generates server logs that you can use to analyze the server activity and debug any issues. You can configure the log settings to specify the number of lines each log file should contain and the log level for which you want to use the log file. You can also generate support logs for analysis.

This topic includes the following details:

Generating Technical Support File

Command Center lets you generate support archive logs for analysis.

To generate support logs

1. On the Administration tab, in the right pane, under Tools, click Generate Technical Support File.
2. Under Generate Technical Support File, click OK.

Viewing Server Logs

The Command Center server implicitly generates server logs that you can use to analyze the server activity and debug any issues.

To view server logs

1. On the Administration tab, in the right pane, under Logging, click View Logs.
2. Under View Logs, you can view the following:
   - Name—Name of the log file. Click a file name to view the log details.
   - Last modified—Date and time when the log file was last modified.
   - Size—Size of a log file.

   Note:
   To display additional details, right-click the name of the log and select Open Link in New Tab.

   To display the logs on a Command Center server, use editor tools such as notepad or text pad for Windows, and vi editor or vim editor for Linux and Command Center appliances.

Configuring Server Log Settings

The Command Center server implicitly generates server logs that you can use to analyze the server activity and debug any issues. You can configure the log settings to specify the number of lines each log file should contain and the log level for which you want to use the log file.

To configure log settings

1. On the Administration tab, in the right pane, under Logging, click Log Settings.

2. Under Log Settings, you can view and do the following.
   - Logger: Type of log file.
   - Max Lines / File: Specifies the maximum number of lines in a log file. Select the number of lines you want a file to contain. The possible values are: 5000, 10000, and 20000.
   - Level: Level of log you want to generate. Select the log level for a file.
   - Appender: A link to set the file appender details.
     When you click on file name in the Appender column, you can modify the following settings:
     - File Name: Name of the log file with which the appender is associated.
     - Max Backup: Maximum number of files to be backed up when storing the logs. When this limit is reached, the log file is rolled back.
     - File Size: Maximum size of the log file.

Monitoring Syslog Events

You can designate a syslog server to monitor the syslog events generated by the Command Center. Command Center then redirects all syslog messages to the syslog server. After you configure the syslog server, it displays the details of the events.

You can click the System Logs Parameters and specify the date and time format, and select the types of messages to be displayed by the syslog server.

Designating a Syslog Server

1. On the Administration tab, on the right-pane, under Security, click Syslog Server.
2. Click Add, specify the date and time format, and select the type of events to be displayed in the logs.

Viewing Server Details, Logged-in User Information, and License Details

Apr 18, 2014

You can view the server and port information, such as the host name and IP address of the server and the TCP port. You can view the details of the users that are connected to the Command Center server at the current time. You can also view the Command Center appliance license details.

To view server information

1. On the Administration tab, in the left pane, under Information, click Server.
2. Under Server Details, you can view information, such as the host name and address, operating system on which the server is running, database to which the Command Center server is connected, and the total and free memory.

To view logged-in user information

1. On the Administration tab, in the left pane, under Information, click Logged-in Users.
2. Under Logged-in Users, you can view information, such as the user name of the Command Center user that is connected to the server, the IP address of the user that is connected to the server, and the time since when the user is logged on.

To view License information

You can view the Command Center appliance license details.

Note: The license information is displayed only for Command Center appliances.

1. On the Administration tab, in the left pane Information, click License Details.
2. Under License Details, you can view information, such as the license type of the Command Center appliances, IP Addresses, and the Company Name.

Changing the Database Password

Apr 17, 2014

You can change the password that the Command Center server uses to connect to the database.

To change the database password

1. On the Administration tab, in the right pane, under Tools, click Change Database Password.
2. Under Change Database Password, in Current Password, type the current password that the Command Center server uses to connect to the database.
3. In New password and in Re-type password, type the new password you want to the Command Center server to use to connect to the database, and then click OK.

Support for Applying XenServer Hotfixes on Command Center Appliance

Apr 28, 2014

You can apply XenServer hotfixes on the Command Center hardware appliance. To apply the XenServer hotfixes, you must first download the files.

To apply XenServer hotfixes

1. Upload the latest XenServer hotfix to the Command Center.
   1. On the Administration tab, in the right pane, under Operations, select XenServer Hotfixes.
   2. From the Action drop-down list, click Upload.
   3. On the Upload XenServer Hotfix page, click Browse and navigate to the folder that contains the build file, and then double-click the build file .
   4. Click OK.

   The hotfix will be available on the XenServer Hotfixes page and the Applied status is set to No.
2. Apply XenServer to a new version.
   1. On the Administration tab, in the right pane, under Operations, select XenServer Hotfixes.
   2. Select the hotfix that you want to apply and from the **Action** drop-down list, click **Apply**.

   After the XenServer is applied successfully, the Applied Status is set to Yes. The hotfixes patch is only applied on the primary Command Center server. To apply the files on the secondary server, you must perform a force failover.

Configuring Database Settings

Nov 04, 2016

You can now configure database reconnection parameters such as the number of retry attempts and the retry delay taken to restore database connection from the Command Center GUI.

To configure database retry settings

1. Navigate to the **Administration** tab. In the left pane, under **Database Management**, click **Database Retry Settings**.

2. In the **Configure Database Retry Settings** page, enter the following details:

- **Retry Attempts** - Specifies the number of database connection retry attempts. By default, the number of attempts is set at 2.
- **Retry Delay (in seconds)** - Specifies the database connection timeout in seconds. By default, the number of seconds is set at 15.

3. Click **OK**.

NITRO API

May 27, 2015

The Citrix® Command Center NITRO protocol allows you to configure the Command Center server programmatically.

NITRO exposes its functionality through Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET, NITRO APIs are exposed through Java and .NET libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of the Command Center server before using the NITRO protocol.
To use the NITRO protocol, the client application needs only the following:

- Access to a Command Center server, version 5.1 build 30.x or later.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the Command Center server. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from http://www.microsoft.com/downloads/en/default.aspx.

This topic includes the following details:

Obtaining the NITRO Package

The NITRO package is available as a tar file on the Downloads page of the Command Center server GUI. You must download and un-tar the file to a folder on your local system. This folder is referred to as <NITRO_SDK_HOME> in this documentation.

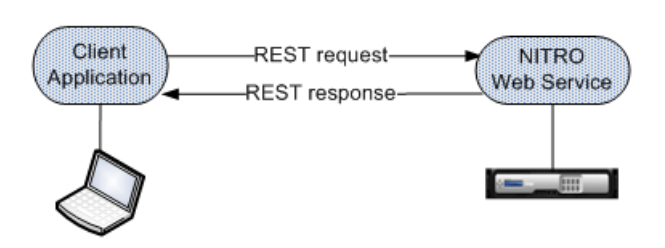
The folder contains the NITRO libraries (JARs for Java and DLLs for .NET) in the lib subfolder. The libraries must be added to the client application's classpath to access NITRO functionality. The <NITRO_SDK_HOME> folder also provides samples and documentation that can help you understand the NITRO SDK.

Note: The REST package contains only documentation for using the REST interfaces.

How NITRO Works

The NITRO infrastructure consists of a client application and the NITRO Web service running on a Command Center server. The communication between the client application and the NITRO web service is based on REST architecture using HTTP or HTTPS.

Figure 1. NITRO execution flow



As shown in the above figure, a NITRO request is executed as follows:

1. The client application sends REST request message to the NITRO web service. When using Java or .NET SDKs, an API call is translated into the appropriate REST request message.
2. The web service processes the REST request message.
3. The NITRO web service returns the corresponding REST response message to the client application. When using Java or .NET SDKs, the REST response message is translated into the appropriate response for the API call.

To minimize network traffic, you retrieve the whole state of a resource from the server, make modifications to the state of the resource locally, and then upload it back to the server in one network transaction.

Note: Local operations on a resource (changing its properties) do not affect its state on the server until the state of the object is explicitly uploaded.
NITRO APIs are synchronous in nature. This means that the client application waits for a response from the NITRO web service before executing another NITRO API.

Java SDK

May 27, 2015

Command Center NITRO APIs are categorized based on the actions that can be performed on the Command Center server. Each category is grouped into different packages which consists of classes that provide the APIs to perform the operations.

For example, APIs to discover devices are available in the com.citrix.cmdctr.nitro.resource.discovery package. Similarly, APIs to configure the Command Center are available in the com.citrix.cmdctr.nitro.resource.configuration package.

For detailed information on the APIs, refer to the API reference available in the <NITRO_SDK_HOME>/doc/api_reference folder.

This topic includes the following details:

Logging on to the Command Center Server

The first step towards using NITRO API is to establish a session with the server and then authenticate the session by using the administrator's credentials.

You must create an object of the com.citrix.cmdctr.nitro.service.nitro_service class by specifying the IP address of the Command Center server, the protocol to be used to connect to the server (HTTP or HTTPS), and the port number. You then use this object to log on to the server.

Note: You must have a user account on that server. The configuration operations that you perform are limited by the administrative roles assigned to your account.
The following sample code establishes a session with a Command Center server with IP address 10.102.29.9 and port 8443, by using HTTPS protocol:

```
//Specify the Command Center server IP address, protocol, and port
nitro_service c = new nitro_service ("10.102.29.9",8443,"https");

//Specify the login credentials
c.login ("admin","verysecret");
```

Note: You must use the nitro_service object in all further NITRO operations on the server.
Note: The default port for HTTP is 9090 and for HTTPS is 8443. You can modify the ports of the Command Center server by using the com.citrix.cmdctr.nitro.resource.admin.access_setting class.
Note: By default, the connection to the server expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the login method. For example, to modify the timeout period to 60 minutes:

```
c.login("admin","verysecret",3600);
```

Adding Device Profiles

To discover devices on a Command Center server you must first configure a device profile that specifies the credentials and SNMP details of the device you want to discover. The APIs are provided by the com.citrix.cmdctr.nitro.resource.discovery.device_profile class.

Example: To add a device profile named "my_profile1" for a NetScaler appliance with username as "user1" and password as "secret".

```
device_profile dpTO = new device_profile();
device_profile_details details = new device_profile_details();

dpTO.set_name("my_profile1");
dpTO.set_device_family("NS");
dpTO.set_desc("NetScaler profile using NITRO API");

details.set_ssh_user_name("user1");
details.set_ssh_password("secret");
details.set_ssh_port("22");
details.set_ssh_retry_count("3");
details.set_ssh_timeout("5");

details.set_sftp_user_name("nsroot");
details.set_sftp_password("nsroot");
details.set_sftp_port("22");
```

```
details.set_sftp_timeout("5");
details.set_sftp_retry_count("5");
details.set_snmp_community("public");
details.set_snmp_port("161");
details.set_snmp_version("v2");

dpTO.set_prof_details(details);
device_profile.add(c,dpTO);
```

Adding Devices

To add a device to a Command Center server you must specify the details of the device (IP address or hostname) and associate the device profile. The server automatically discovers the device by using the specified details.

The APIs to add a device are provided by the com.citrix.cmdctr.nitro.resource.discovery.device_discovery_data class.

Example: To add a NetScaler appliance with IP address 10.102.43.4 by using a profile named "my_profile1".

```
device_discovery_data discoveryData = new device_discovery_data();
discoveryData.set_devices("10.102.43.4");
discoveryData.set_profile_name("my_profile1");
device_discovery_data.discover(c,discoveryData);
```

Monitoring Services and Virtual Servers

You can monitor the services, service groups, and virtual servers across the Netscaler devices that are configured on the Command Center server by using APIs that are provided by the com.citrix.cmdctr.nitro.resource.monitoring package.

Example: To get the virtual servers available on configured NetScaler appliances.

```
//Get virtual servers
options opts = new options();
opts.set_pagesize(20);
opts.set_pageno(1);
opts.set_ascending((new Boolean("true")).booleanValue());
opts.set_orderby("vsvr_name");

vserver vsvr[] = vserver.get(c,opts);

//Get criteria-based virtual servers
filtervalue[] filterval= {new filtervalue("ns_ip","10.102.43.4")};
vserver vsvr1[] = vserver.get_filtered(c,filterval,opts);
```

Creating Performance Reports

The Command Center server stores performance data of the discovered devices. You can use this data to create reports that can help you analyze the performance of the devices.

You can create quick reports by using the APIs provided by the com.citrix.cmdctr.nitro.resource.reporting.quick_report_execdata class.

Example: To get a quick report of a device with IP address 10.102.43.4 for the current day.

```
quick_report_execdata qrExecData = new quick_report_execdata();
qrExecData.set_device_name("10.102.43.4");
qrExecData.set_group_name("nsIfStatsTable");
qrExecData.set_counter_name("rxRawBandwidthUsage");
qrExecData.set_counter_complete_name("nsIfStatsTable_rxRawBandwidthUsage");

qrExecData.set_exclude_zero(false);
qrExecData.set_graph_type("LineGraph");
qrExecData.set_period("Today");

qrExecData = quick_report_execdata.execute(c,qrExecData);
graph_details details = qrExecData.get_graph_details();
System.out.println("Report URL: " +details.get_image_url());
```

You can create custom reports by using the APIs provided by the com.citrix.cmdctr.nitro.resource.reporting.custom_report_execdata class.

Example: To get a custom report of CPU-memory utilization for the current day.

```
custom_report_execdata crExecData = new custom_report_execdata();
crExecData.set_custom_report_name("CPU-MemoryUtilization");
crExecData.set_custom_report_display_name("ResourceUtilization");
crExecData.set_device_names("10.102.43.4");
crExecData.set_exclude_zero(false);
crExecData.set_graph_type("LineGraph");
```



```
crExecData.set_period("Today");

crExecData = custom_report_execdata.execute(c,crExecData);
graph_details details = crExecData.get_graph_details();
System.out.println("Custom Report URL: " +details.get_image_url());
```

Managing Device Certificates

You can manage the certificates of the devices discovered on the Command Center server by using the APIs provided by the com.citrix.cmdctr.nitro.resource.certificate package.

Example: To retrieve details of the certificates of discovered devices.

```
certificate[] cer = certificate.get(service);
long certcount = certificate.count(service);

System.out.println("Total Number of Certificates displayed : " +certcount);

for (int i=0; i< certcount;i++)
{
   System.out.println("Agent: " +cer[i].get_agent());
   System.out.println("Cert Name : " +cer[i].get_cert_name());
   System.out.println("Certificate path : " +cer[i].get_cert_path());
   System.out.println("Key path : " +cer[i].get_key_path());
   System.out.println("Days to Expire: " +cer[i].get_days_to_expire());
   System.out.println("Device Label: " +cer[i].get_label());
}
```

Monitoring Configuration Changes

You can monitor configuration changes across devices by using audit policies on the Command Center server. The APIs for this are provided in the com.citrix.cmdctr.nitro.resource.changemgmt package.

Example: To execute an audit policy.

```
audit_policy_execdata apExecData = new audit_policy_execdata();
apExecData.set_device_selected(true);
apExecData.set_policy_name("RunningVsSavedConfiguration");
apExecData.set_selected_devices(new String[] {"10.102.43.4"});
apExecData.set_operation("execute");
apExecData = audit_policy_execdata.execute(c,apExecData);

//Audit report
System.out.println("id:"+apExecData.get_auditreport_id());
ns_audit_report auditReport = ns_audit_report.get(c,apExecData.get_auditreport_id());
System.out.println("name:"+auditReport.get_report_id());
System.out.println("name:"+auditReport.get_instance_name());
System.out.println("Audit By:"+auditReport.get_exec_by());
System.out.println("Status:"+auditReport.get_status());

//Device-specific report
ns_audit_report_device_details_info deviceDetails = ns_audit_report_device_details_info.get(c,apExecData.get_auditreport_id(),"10.102.43.4");
System.out.println("device details id:"+deviceDetails.get_report_id());
System.out.println("device:"+deviceDetails.get_device_name());
System.out.println("status:"+deviceDetails.get_status());
```

Example: To schedule an audit policy.

```
audit_policy_execdata apExecData = new audit_policy_execdata();
apExecData.set_device_selected(true);
apExecData.set_policy_name("ConfigurationChangeHistory");
apExecData.set_selected_devices(new String[] {"10.102.43.4"});
apExecData.set_operation("schedule");
apExecData.set_ccevent_duration("10");
apExecData.set_ccevent_duration_condition("<=");
apExecData.set_ccevent_duration_type(com.citrix.cmdctr.nitro.resource.AttributeNames.TIME_OPTION_IN_DAYS);

//Set Scheduling details
apExecData.set_scheduler_type(TaskConstants.SCHEDULER_TYPE_DAYBASED);
apExecData.set_scheduled_days(new String[]{"5", "6"});
apExecData.set_scheduled_hours("11,12,20");
```

```
audit_policy_execdata.schedule(c,apExecData);
```

Using Tasks to Configure Managed Devices

You can configure the devices available on the Command Center server by using built-in tasks or by defining custom tasks. The APIs are available in the com.citrix.cmdctr.nitro.resource.configuration package.

Example: To add a custom task and to execute it.

```
ns_task nsTask = ns_task.get(c,"newtask");
System.out.println("nsTask="+nsTask);
ns_task_execution_data nsExecData = new ns_task_execution_data();
nsExecData.set_task_name("newtask");
nsExecData.set_device_list(new String[]{"10.102.43.4"});
scheduler_data schedData = new scheduler_data();
schedData.set_recurr_type(TaskConstants.NO_RECURRING);
nsExecData.set_scheduler_data(schedData);
nsExecData.set_executed_by("root");
nsExecData.set_annotation("executing task using NITRO APIs");

Properties userInputProps = new Properties();
ns_task_variables nsTaskVariables[] = nsTask.get_task_variable_list();

if (nsTaskVariables != null)
{
   for (int i=0;i<nsTaskVariables.length;i++)
   {
      userInputProps.setProperty("$UserInput$" + nsTaskVariables[i].get_name(),"xyz");
   }
   nsExecData.set_user_input_props(userInputProps);
}

nsExecData = ns_task_execution_data.execute(c,nsExecData);

int ids[] = nsExecData.get_execution_ids();
System.out.println("ids="+ids.length);
Thread.sleep(5000);
ns_task_status taskStatus = ns_task_status.get(c,ids[0]);
System.out.println("taskStatus deviceId = "+taskStatus.get_device_id());
System.out.println("taskStatus status = "+taskStatus.get_status());
System.out.println("taskStatus annotation = "+taskStatus.get_annotation());

filtervalue[]  value= {new filtervalue("id",String.valueOf(taskStatus.get_taskexecution_id()))};
command_log cmdlog[] = command_log.get_filtered(c,value);
for(int i=0;i<cmdlog.length;i++)
{
 System.out.println("command = "+cmdlog[i].get_identifier());
 System.out.println("status = "+cmdlog[i].get_status());
}
```

Example: To schedule a custom task.

```
ns_task_execution_data nsExecData = new ns_task_execution_data();
nsExecData.set_task_name("newtask");
nsExecData.set_device_list(new String[]{"10.102.43.4"});
scheduler_data schedData = new scheduler_data();
schedData.set_recurr_type(TaskConstants.NO_RECURRING);
long scheduleTime = new Date().getTime() + (24*60*60*1000);
schedData.set_schedule_date_time(new Date(scheduleTime));
nsExecData.set_scheduler_data(schedData);
nsExecData.set_executed_by("root");
nsExecData.set_annotation("Scheduling task using NITRO APIs");

ns_task_execution_data.execute(c,nsExecData);
```

Migrating NetScaler Configurations

You can port the configurations from a source NetScaler appliance to target NetScaler appliances using one of the following approaches, described in this section:

- Directly from Source to Target
- After Editing the Configurations

The APIs to migrate configurations are provided by the com.citrix.cmdctr.nitro.resource.configuration.configuration_template class.

Directly from Source to Target

In this approach, you specify the source NetScaler details and the details of the NetScaler to which you want to migrate the configurations.

Example: To migrate the configurations of NetScaler appliance with IP address "10.102.5.6" to NetScaler appliances with IP addresses "10.102.40.60" and "10.102.40.17".

```
configuration_template config = new configuration_template();
config.set_action("execute");
config.set_source_device("10.102.5.6");
config.set_configuration_period("LastOneWeek");
config.set_name("config_rest");
config.set_device_family("NS");
config.set_devices(["10.102.40.60","10.102.40.17"]);
configuration_template.execute(c,config);
```

After Editing the Configurations

You must retrieve the NetScaler configurations. These configurations are saved as a text file in the <Command_Center_Home>\temp directory. Then, you can edit the configurations as required and port them to the target NetScaler appliances.

1. Retrieve the NetScaler configurations.
   Example: To save the configurations of NetScaler appliance with IP address "10.102.5.6".

   ```
   configuration_template config = new configuration_template();
   config.set_action("save");
   config.set_source_device("10.102.5.6");
   config.set_configuration_period("LastOneWeek");
   config.set_name("Rest_Save_1 ");
   config.set_device_family("NS");
   config.set_config_as_file (true);
   configuration_template.execute(c,config);
   ```
2. Edit the configurations as required.
3. Migrate the updated configurations to the target NetScaler appliance.
   Example: To migrate the configurations to NetScaler appliances with IP addresses "10.102.40.60" and "10.102.40.17".

   ```
   configuration_template config = new configuration_template();
   config.set_action("load_execute");
   config.set_name("Rest_load_execute_1");
   config.set_profile_file_name("Rest_Save_1");
   config.set_device_family("NS");
   config.set_devices(["10.102.40.60","10.102.40.17"]);
   configuration_template.execute(c,config);
   ```

Exception Handling

The status of a NITRO request is captured in the com.citrix.cmdctr.nitro.exception.nitro_exception class. This class provides the following details of the exception:

- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** Provides a brief description of the exception.

.NET SDK

May 27, 2015

Command Center NITRO APIs are categorized based on the actions that can be performed on the Command Center server. Each category is grouped into different packages which consists of classes that provide the APIs to perform the operations.

For example, APIs to discover devices are available in the com.citrix.cmdctr.nitro.resource.discovery namespace. Similarly, APIs to configure the Command Center are available in the com.citrix.cmdctr.nitro.resource.configuration namespace.

For detailed information on the APIs, refer to the API reference available in the <NITRO_SDK_HOME>/doc/api_reference folder.

This topic includes the following details:

Logging on to the Command Center Server

The first step towards using NITRO API is to establish a session with the server and then authenticate the session by using the administrator's credentials.

You must create an object of the com.citrix.cmdctr.nitro.service.nitro_service class by specifying the IP address of the Command Center server, the protocol to be used to connect to the server (HTTP or HTTPS), and the port number. You then use this object to log on to the server.

Note: You must have a user account on that server. The configuration operations that you perform are limited by the administrative roles assigned to your account.
The following sample code establishes a session with a Command Center server with IP address 10.102.29.9 and port 8443, by using HTTPS protocol:

```
//Specify the Command Center server IP address, protocol, and port
nitro_service c = new nitro_service ("10.102.29.9",8443,"https");

//Specify the login credentials
c.login ("admin","verysecret");
```

Note: You must use the nitro_service object in all further NITRO operations on the server.
Note: The default port for HTTP is 9090 and for HTTPS is 8443. You can modify the ports of the Command Center server by using the com.citrix.cmdctr.nitro.resource.admin.access_setting class.
Note: By default, the connection to the server expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the login method. For example, to modify the timeout period to 60 minutes:

```
c.login("admin","verysecret",3600);
```

Adding Device Profiles

To discover devices on a Command Center server you must first configure a device profile that specifies the credentials and SNMP details of the device you want to discover. The APIs are provided by the com.citrix.cmdctr.nitro.resource.discovery.device_profile class.

Example: To add a device profile named "my_profile2" for a NetScaler appliance with username as "user1" and password as "secret".

```
device_profile dpTO = new device_profile();
device_profile_details details = new device_profile_details();

dpTO.name = "my_profile2";
dpTO.device_family ="NS";
dpTO.desc = "NetScaler profile using NITRO API";

details.ssh_user_name = "user1";
details.ssh_password ="secret";
details.ssh_port="22";
details.ssh_retry_count="3";
details.ssh_timeout="5";
```

```
details.sftp_user_name="nsroot";
details.sftp_password="nsroot";
details.sftp_port="22";
details.sftp_timeout="5";
details.sftp_retry_count="5";
details.snmp_community="public";
details.snmp_port="161";
details.snmp_version="v2";

dpTO.prof_details = details;
device_profile.add(c,dpTO);
```

Adding Devices

To add a device to a Command Center server you must specify the details of the device (IP address or hostname) and associate the device profile. The server automatically discovers the device by using the specified details.

The APIs to add a device are provided by the com.citrix.cmdctr.nitro.resource.discovery.device_discovery_data class.

Example: To add a NetScaler appliance with IP address 10.102.43.4 by using a profile named "my_profile2".

```
device_discovery_data discoveryData = new device_discovery_data();
discoveryData.devices = "10.102.43.4";
discoveryData.profile_name = "my_profile2";
device_discovery_data.discover(c,discoveryData);
Console.WriteLine("Discovery started for 10.102.43.4");
```

Monitoring Services and Virtual Servers

You can monitor the services, service groups, and virtual servers across the Netscaler devices that are configured on the Command Center server by using APIs that are provided by the com.citrix.cmdctr.nitro.resource.monitoring namespace.

Example: To get the virtual servers available on configured NetScaler appliances.

```
options opts = new options();
opts.pagesize = 20;
opts.pageno = 1;
opts.isAscendingOrder = true;
opts.orderBy = "vsvr_name";

//Get virtual servers
vserver[] vsvr = vserver.get(c,opts);

//Get criteria-based virtual servers
filtervalue filterval =new filtervalue();
filterval.properties.Add("ns_ip", "10.102.43.4");
vserver[] vservr = vserver.get_filtered(c,filterval,opts);
```

Creating Performance Reports

The Command Center server stores performance data of the discovered devices. You can use this data to create reports that can help you analyze the performance of the devices.

You can create quick reports by using the APIs provided by the com.citrix.cmdctr.nitro.resource.reporting.quick_report_execdata class.

Example: To get a quick report of a device with IP address 10.102.43.4 for the current day.

```
quick_report_execdata qrExecData = new quick_report_execdata();
qrExecData.device_name = "10.102.43.4";
qrExecData.group_name = "nsIfStatsTable";
qrExecData.counter_name = "rxRawBandwidthUsage";
qrExecData.counter_complete_name = "nsIfStatsTable_rxRawBandwidthUsage";

qrExecData.exclude_zero = false;
qrExecData.graph_type = "LineGraph";
qrExecData.period = "Today";

qrExecData = quick_report_execdata.execute(c,qrExecData);
graph_details details = qrExecData.graph_details;
Console.WriteLine("Report URL: " +details.image_url);
```

You can create custom reports by using the APIs provided by the com.citrix.cmdctr.nitro.resource.reporting.custom_report_execdata class.

Example: To get a custom report of CPU-memory utilization for the current day.

```
custom_report_execdata crExecData = new custom_report_execdata();
crExecData.custom_report_name = "CPU-MemoryUtilization";
crExecData.custom_report_display_name = "ResourceUtilization";
crExecData.device_names = "10.102.43.4";
crExecData.exclude_zero = false;
crExecData.graph_type = "LineGraph";
crExecData.period = "Today";

crExecData = custom_report_execdata.execute(c,crExecData);
graph_details details = crExecData.graph_details;
Console.WriteLine("Custom Report URL: " +details.image_url);
```

Managing Device Certificates

You can manage the certificates of the devices discovered on the Command Center server by using the APIs provided by the com.citrix.cmdctr.nitro.resource.certificate namespace.

Example: To retrieve details of the certificates of discovered devices.

```
certificate[] cer = certificate.get(service);
long certcount = certificate.count(service);

Console.WriteLine("Total Number of Certificates displayed : " +certcount);

for (int i=0; i< certcount;i++)
{
   Console.WriteLine("Agent: " +cer[i].agent);
   Console.WriteLine("Cert Name : " +cer[i].cert_name);
   Console.WriteLine("Certificate path : " +cer[i].cert_path);
   Console.WriteLine("Key path : " +cer[i].key_path);
   Console.WriteLine("Days to Expire: " +cer[i].days_to_expire);
   Console.WriteLine("Device Label: " +cer[i].label);
}
```

Monitoring Configuration Changes

You can monitor configuration changes across devices by using audit policies on the Command Center server. The APIs for this are provided in the com.citrix.cmdctr.nitro.resource.changemgmt namespace.

Example: To execute an audit policy.

```
audit_policy_execdata apExecData = new audit_policy_execdata();
apExecData.device_selected = true ;
apExecData.policy_name = "RunningVsSavedConfiguration";
String[] str = new String[] {"10.102.43.4"};
apExecData.selected_devices = str;
apExecData.operation = "execute";
apExecData = audit_policy_execdata.execute(c,apExecData);
Console.WriteLine("id:"+apExecData.auditreport_id);

//Audit report
ns_audit_report auditReport = ns_audit_report.get(c,apExecData.auditreport_id);
Console.WriteLine("name:"+auditReport.report_id);
Console.WriteLine("name:"+auditReport.instance_name);
Console.WriteLine("Audit By:"+auditReport.exec_by);
Console.WriteLine("Status:"+auditReport.status);

//Device-specific report
ns_audit_report_device_details_info deviceDetails = ns_audit_report_device_details_info.get(c,apExecData.auditreport_id,"10.102.43.4");
Console.WriteLine("device details id:"+deviceDetails.report_id);
Console.WriteLine("device:"+deviceDetails.device_name);
Console.WriteLine("status:"+deviceDetails.status);
```

Example: To schedule an audit policy.

```
audit_policy_execdata apExecData = new audit_policy_execdata();
apExecData.device_selected = true ;
```



```
apExecData.policy_name = "ConfigurationChangeHistory";
apExecData.selected_devices = new String[] { "10.102.43.4" };
apExecData.operation = "schedule";
apExecData.ccevent_duration = "10";
apExecData.ccevent_duration_condition = "<=";
apExecData.ccevent_duration_type = com.citrix.cmdctr.nitro.resource.AttributeNames.TIME_OPTION_IN_DAYS;

//Set Scheduling details
apExecData.scheduler_type = "dayBased";
apExecData.scheduled_days = new String[]{"4", "5"};
apExecData.scheduled_hours = "12,13,20";

audit_policy_execdata.schedule(c,apExecData);
```

Using Tasks to Configure Managed Devices

You can configure the devices available on the Command Center server by using built-in tasks or by defining custom tasks. The APIs are available in the com.citrix.cmdctr.nitro.resource.configuration namespace.

Example: To add a custom task and to execute it.

```
ns_task nsTask = ns_task.get(c,"newtask");
Console.WriteLine("nsTask="+nsTask);

ns_task_execution_data nsExecData = new ns_task_execution_data();
nsExecData.task_name = "newtask";
nsExecData.device_list = new String[]{"10.102.43.4"};
scheduler_data schedData = new scheduler_data();
schedData.recurr_type = "no_reccur";
nsExecData.scheduler_data = schedData;
nsExecData.executed_by = "root";
nsExecData.annotation = "executing task using NITRO APIs" ;

Dictionary<string, string> userInputProps = new Dictionary<string, string>();
ns_task_variables[] nsTaskVariables = nsTask.task_variable_list;

if (nsTaskVariables != null)
{
   for (int i=0;i<nsTaskVariables.Length;i++)
   {
      userInputProps["$UserInput$" + nsTaskVariables[i].name] = "xyz";
   }
   nsExecData.user_input_props = userInputProps;
}

nsExecData = ns_task_execution_data.execute(c,nsExecData);
int[] ids = nsExecData.execution_ids;
Console.WriteLine("ids="+ids.Length);
System.Threading.Thread.Sleep(5000);
ns_task_status taskStatus = ns_task_status.get(c,ids[0]);
Console.WriteLine("taskStatus deviceId = "+taskStatus.device_id);
Console.WriteLine("taskStatus status = "+taskStatus.status);
Console.WriteLine("taskStatus annotation = "+taskStatus.annotation);

filtervalue  value = new filtervalue();
value.properties.Add("id",taskStatus.taskexecution_id+"");
command_log[] cmdlog = command_log.get_filtered(c,value);
for(int i=0;i<cmdlog.Length;i++)
{
 Console.WriteLine("command = "+cmdlog[i].identifier);
 Console.WriteLine("status = "+cmdlog[i].status);
}
```

Example: To schedule a custom task.

```
ns_task_execution_data nsExecData = new ns_task_execution_data();
nsExecData.task_name = "newtask" ;
nsExecData.device_list = new String[]{"10.102.43.4"};
```

```
scheduler_data schedData = new scheduler_data();
schedData.recurr_type = "daily";
schedData.recurr_hours="2";
nsExecData.scheduler_data = schedData;
nsExecData.executed_by = "root";
nsExecData.annotation = "Scheduling task using NITRO APIs";

ns_task_execution_data.execute(c,nsExecData);
```

Migrating NetScaler Configurations

Updated: 2014-04-23

You can port the configurations from a source NetScaler appliance to target NetScaler appliances using one of the following approaches, described in this section:

- Directly from Source to Target
- After Editing the Configurations

The APIs to migrate configurations are provided by the com.citrix.cmdctr.nitro.resource.configuration.configuration_template class.

Directly from Source to Target

In this approach, you specify the source NetScaler details and the details of the NetScaler to which you want to migrate the configurations.

Example: To migrate the configurations of NetScaler appliance with IP address "10.102.5.6" to NetScaler appliances with IP addresses "10.102.40.60" and "10.102.40.17".

```
configuration_template config = new configuration_template();
config.action = "execute";
config.source_device = "10.102.5.6";
config.configuration_period = "LastOneWeek";
config.name = "config_rest";
config.device_family = "NS";
config.devices = ["10.102.40.60","10.102.40.17"];
configuration_template.execute(c,config);
```

After Editing the Configurations

You must retrieve the NetScaler configurations. These configurations are saved as a text file in the <Command_Center_Home>\temp directory. Then, you can edit the configurations as required and port them to the target NetScaler appliances.

1. Retrieve the NetScaler configurations.
   Example: To save the configurations of NetScaler appliance with IP address "10.102.5.6".

   ```
   configuration_template config = new configuration_template();
   config.action = "save";
   config.source_device = "10.102.5.6";
   config.configuration_period = "LastOneWeek";
   config.name = "Rest_Save_1";
   config.device_family = "NS";
   config.config_as_file = true;
   configuration_template.execute(c,config);
   ```
2. Edit the configurations as required.
3. Migrate the updated configurations to the target NetScaler appliance.
   Example: To migrate the configurations to NetScaler appliances with IP addresses "10.102.40.60" and "10.102.40.17".

   ```
   configuration_template config = new configuration_template();
   config.action = "load_execute";
   config.name = "Rest_load_execute_1";
   config.profile_file_name = "Rest_Save_1";
   config.device_family = "NS";
   config.devices = ["10.102.40.60","10.102.40.17"];
   configuration_template.execute(c,config);
   ```

Exception Handling

The status of a NITRO request is captured in the com.citrix.cmdctr.nitro.exception.nitro_exception class. This class provides the following details of the exception:

- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** Provides a brief description of the exception.

REST Web Service

May 27, 2015

REST (REpresentational State Transfer) is an architectural style based on simple HTTP requests and responses between the client and the server. REST is used to query or change the state of objects on the server side. In REST, the server side is modeled as a set of entities where each entity is identified by a unique URL.

Each resource also has a state on which the following operations can be performed:

- **Create.** Clients can create new server-side resources on a "container" resource. You can think of container resources as folders, and child resources as files or subfolders. The calling client provides the state for the resource to be created. The state can be specified in the request by using XML or JSON format. The client can also specify the unique URL that will identify the new object. Alternatively, the server can choose and return a unique URL identifying the created object. The HTTP method used for Create requests is POST.
- **Read.** Clients can retrieve the state of a resource by specifying its URL with the HTTP GET method. The response message contains the resource state, expressed in JSON format.
- **Update.** You can update the state of an existing resource by specifying the URL that identifies that object and its new state in JSON or XML, using the PUT HTTP method.
- **Delete.** You can destroy a resource that exists on the server-side by using the DELETE HTTP method and the URL identifying the resource to be removed.

In addition to these four CRUD operations (Create, Read, Update, and Delete), resources can support other operations or actions. These operations use the HTTP POST method, with the request body in JSON specifying the operation to be performed and parameters for that operation.

This topic includes the following details:

Logging on to the Command Center Server

The first step towards using NITRO API is to establish a session with the server and then authenticate the session by using the administrator's credentials. You must specify the username and password in the login object. The session ID that is created must be specified for all further operations in the session.

Note: You cannot log on to the Command Center server unless you have a user account on the appliance. The configuration operations that you can perform are limited by the administrative roles assigned to your account.
To establish a session with a Command Center server with IP address 10.144.9.22 and port 8443, by using HTTPS protocol:

- **URL.** https://10.144.9.22:8443/nitro/v1/login
- **HTTP Method.** POST

- **Request Payload.**

```
{
  "login":
  {
    "username":"user",
    "password":"secret",
    "session_timeout":3600
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "login" :
  {
    "password":"",
    "session_timeout":3600,
    "sessionid":"70795094%3A13d1a1dee5e%3A-7f37",
    "username":"user",
    "remarks":""
  }
}
```

Note: The default port for HTTP is 9090 and for HTTPS is 8443.
Note: By default, the connection to the server expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the login object.
To disconnect from the Command Center server, specify the session ID in the URL:

- **URL.** https://10.144.9.22:8443/nitro/v1/login/70795094%3A13d1a1dee5e%3A-7f37
- **HTTP Method.** DELETE
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done"
}
```

Adding Device Profiles

To discover devices on a Command Center server you must first configure a device profile that specifies the credentials and SNMP details of the device you want to discover.

To add a device profile named "my_profile1" for a NetScaler appliance.

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/device_profile
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  "device_profile":
```



```
    {
      "name":"my_profile1",
      "desc":"NetScaler profile using NITRO API",
      "device_family":"NS",
      "prof_details":
      {
        "ssh_user_name":"user1",
        ...
        ...
      }
    }
  }
```

- **Response Payload.**

```
  {
    "errorcode": 0,
    "message": "Done",
    "device_profile" :
    [
      {
        "id":7,
        "name":"my_profile1"
        ...
        ...
      }
    ]
  }
```

To retrieve, in a paginated manner, the details of all device profiles available on the server.

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/device_profile?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
  {
    "errorcode": 0,
    "message": "Done",
    "device_profile" :
    [
      {
        "id":10,
        "name":"ns6",
        "desc":"new profile"
        ...
        ...
      }
    ]
  }
```

Note: You can retrieve the details of a specific device profile by specifying the profile ID in the URL as follows: https://10.144.9.22:8443/nitro/v1/discovery/device_profile/3, where 3 is the ID of the profile.
Note: You can retrieve the count of device profiles available by using the following URL: https://10.144.9.22:8443/nitro/v1/discovery/device_profile?count=yes.
To update the details of a device profile named "my_profile1".

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/device_profile
- **HTTP Method.** PUT
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  "device_profile":
  {
    "id":"11",
    "name":"my_profile1",
    "desc":"Updated description",
    "device_family":"NS",
    "prof_details":
    {
      "ssh_user_name":"user1",
      ...
      ...
    }
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "device_profile" :
  [
    {
      "id":7,
      "name":"my_profile1"
      ...
      ...
    }
  ]
}
```

To delete a device profile named "my_profile1" and that has ID 11.

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/device_profile/11
- **HTTP Method.** DELETE
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
```

```
    "message": "Done"
  }
```

Adding Devices

To add a device to a Command Center server you must specify the details of the device (IP address or hostname) and associate the device profile. The server automatically discovers the device by using the specified details.

To add a NetScaler appliance with IP address 10.102.29.195 by using a profile named "my_profile1".

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/device_discovery_data
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
  {
    "device_discovery_data":
    {
      "import_from_file":"false",
      "ip_address_file":"",
      "devices":"10.102.29.195",
      "profile_name":"my_profile1"
    }
  }
```

- **Response Payload.**

```
  {
    "errorcode": 0,
    "message": "Done",
    "device_discovery_data" :
    {
      "devices":"10.102.29.195",
      "profile_id":0,
      "profile_name":"my_profile1",
      "import_from_file":"false",
      "ip_address_file":""
    }
  }
```

To retrieve, in a paginated manner, the details of all devices discovered on the server.

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/citrix_mo_device?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
  {
    "errorcode": 0,
    "message": "Done",
    "citrix_mo_device" :
    [
```

```
    {
      "name":"10.102.29.60",
      "display_name":"10.102.29.60",
      ...,
      ...
    }
  ]
}
```

Note: You can retrieve the count of devices discovered by using the following URL: https://10.144.9.22:8443/nitro/v1/discovery/citrix_mo_device?count=yes.
Note: You can get the status of device discovery by specifying the device in the URL as follows: https://10.144.9.22:8443/nitro/v1/discovery/discovery_status_log/10.102.29.60?pageno=1&pagesize=25, where 10.102.29.60 is the IP address of the device.
To delete a discovered device that has IP address 10.102.29.60.

- **URL.** https://10.144.9.22:8443/nitro/v1/discovery/citrix_mo_device/10.102.29.60
- **HTTP Method.** DELETE
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done"
}
```

Monitoring Services and Virtual Servers

You can monitor the services, service groups, and virtual servers across the Netscaler devices that are configured on the Command Center server.

To get the virtual servers available on discovered NetScaler appliances.

- **URL.** https://10.144.9.22:8443/nitro/v1/monitoring/vserver?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "vserver" :
  [
    {
      "view_id":-1,
      "annotation":"Update from Periodic Poll",
      "ns_ip":"10.102.29.60",
      "label":"10.102.29.60",
      "vsvr_name":"lb-vserver1",
      ...
      ...
```



```
        }
      ]
    }
```

To get the services available on discovered NetScaler appliances.

- **URL.** https://10.144.9.22:8443/nitro/v1/monitoring/services?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "services" :
  [
    {
      "view_id":-1,
      "annotation":"Update from Periodic Poll",
      "ns_ip":"10.102.29.65",
      "label":"10.102.29.65",
      "svc_name":"nsrpcs-::1l-3008",
      ...
      ...
    }
  ]
}
```

To get the service groups available on discovered NetScaler appliances.

- **URL.** https://10.144.9.22:8443/nitro/v1/monitoring/svcgrp?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "svcgrp" :
  [
    {
      ...
      ...
    }
  ]
}
```

Creating Performance Reports

The Command Center server stores performance data of the discovered devices. You can use this data to create reports that can help you analyze the performance of the devices.

To get a quick report.

- **URL.** https://10.144.9.22:8443/nitro/v1/reporting/quick_report_execdata
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  quick_report_execdata:
  {
    "multiple_polled_data":<Boolean_value>,
    "device_name":<String_value>,
    "instances":<String_value>,
    "group_name":<String_value>,
    "report_type":<String_value>,
    "counter_complete_name":<String_value>,
    "counter_name":<String_value>
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "quick_report_execdata":
  [
    {
      "multiple_polled_data":<Boolean_value>,
      ...
      ...
    }
  ]
}
```

To get a custom report.

- **URL.** https://10.144.9.22:8443/nitro/v1/reporting/custom_report_execdata
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  custom_report_execdata:
  {
    "report_type":<String_value>,
    "file_name_date":<String_value>,
    "aggregate_report":<Boolean_value>,
    "plot_bound_service":<Boolean_value>,
    "report_datatype":<String_value>,
    "device_names":<String_value>,
```

```
        "custom_report_display_name":<String_value>,
        "custom_report_name":<String_value>,
        "instance_map":<instance_map[]_value>,
        "graph_key":<String_value>
      }
    }
```

- **Response Payload.**

```
    {
      "errorcode": 0,
      "message": "Done",
      "custom_report_execdata":
      [
        {
          "report_type":<String_value>,
          ...
          ...
        }
      ]
    }
```

Managing Device Certificates

You can manage the certificates of the devices discovered on the Command Center server.

To retrieve the certificates available on all discovered devices.

- **URL.** https://10.144.9.22:8443/nitro/v1/certificate/certificate?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
    {
      "errorcode": 0,
      "message": "Done",
      "certificate" :
      [
        {
          "cert_name":"ns-server-certificate",
          "agent":"10.102.29.65",
          "device_type":"NetScalerVPX",
          ...
          ...
        }
      ]
    }
```

Note: You can view the details of a specific certificate by using a URL as follows: https://10.144.9.22:8443/nitro/v1/certificate/certificate?filter=cert_name:ns-server-certificate,agent:10.102.29.65.
To modify the certificate polling interval to 23 hours.

- **URL.** https://10.144.9.22:8443/nitro/v1/certificate/cert_polling_interval
- **HTTP Method.** PUT
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  "cert_polling_interval":
  {
    "polling_interval":"23"
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "cert_polling_interval" :
  {
    "polling_interval":23
  }
}
```

Monitoring Configuration Changes

You can monitor configuration changes across devices by using audit policies on the Command Center server. To create an audit policy you must first create an audit template.

To add an audit template.

- **URL.** https://10.144.9.22:8443/nitro/v1/changemgmt/ns_template_info
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  ns_template_info:
  {
    "owner":<String_value>,
    "template_name":<String_value>,
    "template_id":<Integer_value>,
    "last_modified":<String_value>,
    "template_commands":<ns_template_commands_info[]_value>
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "ns_template_info":
  [
    {
```



```
        "owner":<String_value>,
        ...
        ...
      }
    ]
  }
```

To retrieve the audit templates configured on the server.

- **URL.** https://10.144.9.22:8443/nitro/v1/changemgmt/ns_template_info?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "ns_template_info":
  [
    {
      "template_name":<String_value>,
      "owner":<String_value>,
      ...
      ...
    }
  ]
}
```

To add an audit policy.

- **URL.** https://10.144.9.22:8443/nitro/v1/changemgmt/audit_policy
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  audit_policy:
  {
    "selected_templates":<String_value>,
    "policy_name":<String_value>,
    "running_vs_saved":<Boolean_value>,
    "schedule_time":<String_value>,
    "running_vs_chosen_template":<Boolean_value>
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "audit_policy":
```



```
    [
      {
        "selected_templates":<String_value>,
        "policy_name":<String_value>,
        …
        …
      }
    ]
  }
```

To retrieve the audit policies configured on the server.

- **URL.** https://10.144.9.22:8443/nitro/v1/changemgmt/audit_policy?pageno=1&pagesize=25
- **HTTP Method.** GET
- **Cookie.** SESSID=70795094%3A1...
- **Response Payload.**

```
  {
    "errorcode": 0,
    "message": "Done",
    "audit_policy":
    [
      {
        "policy_name":<String_value>,
        …
        …
      }
    ]
  }
```

Using Tasks to Configure Managed Devices

You can configure the devices available on the Command Center server by using built-in tasks or by defining custom tasks.

To add a custom task.

- **URL.** https://10.144.9.22:8443/nitro/v1/configuration/ns_task
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
  {
    ns_task:
    {
      "secondary_first":<Boolean_value>,
      "enable_rba":<Boolean_value>,
      …
      …
    }
  }
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "ns_task":
  [
    {
      "secondary_first":<Boolean_value>,
      "enable_rba":<Boolean_value>,
      ...
      ...
    }
  ]
}
```

To schedule a custom task.

- **URL.** https://10.144.9.22:8443/nitro/v1/configuration/ns_task_execution_data
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  ns_task_execution_data:
  {
    "rba_password":<String_value>,
    "user_input_props":<Properties_value>,
    "device_list":<String[]_value>,
    "execute_on_secondary_first":<Boolean_value>,
    ...
    ...
  }
}
```

- **Response Payload.**

```
{
  "errorcode": 0,
  "message": "Done",
  "ns_task_execution_data":
  [
    {
      "rba_password":<String_value>,
      "user_input_props":<Properties_value>,
      "device_list":<String[]_value>,
      "execute_on_secondary_first":<Boolean_value>,
      ...
      ...
    }
  ]
}
```

You can port the configurations from a source NetScaler appliance to target NetScaler appliances using one of the following approaches, described in this section.

- Directly from Source to Target
- After Editing the Configurations

Directly from Source to Target

In this approach, you specify the source NetScaler details and the details of the NetScaler to which you want to migrate the configurations.

- **URL.** https://10.144.9.22:8443/nitro/v1/configuration/configuration_template
- **HTTP Method.** POST
- **Cookie.** SESSID=70795094%3A1...
- **Request Payload.**

```
{
  "params":
  {
    "action":"execute"
  },
  "configuration_template":
  {
    "name":"Rest_Execute_1",
    "device_family":"NS",
    "template_source":"device",
    "source_device":"10.102.40.66",
    "configuration_period":"Today",
    "devices":["10.102.40.60","10.102.40.61"],
    "config_as_file":false,
    "auto_rollback":false,
    "alarm_settings":true,
    "report_as_mail":true,
    "report_mail_id":"abc@xyz.com",
    "critical_severity":true,
    "major_severity":false,
    "minor_severity":false,
    "warning_severity":false
  }
}
```

After Editing the Configurations

You must retrieve the NetScaler configurations. These configurations are saved as a text file in the <Command_Center_Home>\temp directory. Then, you can edit the configurations as required and port them to the target NetScaler appliances.

1. Retrieve the NetScaler configurations.
   - **URL.** https://10.144.9.22:8443/nitro/v1/configuration/configuration_template
   - **HTTP Method.** POST
   - **Cookie.** SESSID=70795094%3A1...
   - **Request Payload.**

```
{
  "params":
  {
    "action":"save"
  },
  "configuration_template":
  {
    "name":"Rest_Save_1",
    "device_family":"NS",
    "template_source":"device",
    "source_device":"10.102.40.66",
    "configuration_period":"Today",
    "config_as_file":true,

  }
}
```

2. Edit the configurations as required.
3. Migrate the updated configurations to the target NetScaler appliance.
   - **URL.** https://10.144.9.22:8443/nitro/v1/configuration/configuration_template
   - **HTTP Method.** POST
   - **Cookie.** SESSID=70795094%3A1...
   - **Request Payload.**

```
{
  "params":
  {
    "action":"load_execute"
  },
  "configuration_template":
  {
    "name":"Rest_load_execute_1",
    "device_family":"NS",
    "template_source":"device",
    "profile_file_name":"Rest_Save_1",
    "devices":["10.102.40.60","10.102.40.61"],
    "config_as_file":false,
    "auto_rollback":false,
    "alarm_settings":true,
    "report_as_mail":true,
    "report_mail_id":"abc@xyz.com",
    "critical_severity":true,
    "major_severity":false,
```



```
        "minor_severity":false,
        "warning_severity":false
      }
    }
```