Command Center 5.0

2015-05-15 13:29:23 UTC

Contents

Command Center 5.0

Citrix Command Center is a management and monitoring solution for Citrix application networking products that include Citrix NetScaler, Citrix Access Gateway Enterprise Edition, Citrix Branch Repeater, and Citrix Repeater. Use Command Center to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

What's New in Command Center 5.0

Command Center 5.0 provides operating system support for Windows Server 2008 R2 and CentOS 5.5. In this release, Command Center provides support for Branch Repeater 6.0 release features such as 11 new built-in custom reports for Repeater devices, three new counter groups, and 18 new SNMP traps.

Command Center provides support for NetScaler SDX devices and you can view the device properties, provision or de-provision NetScaler instances on NetScaler SDX, and monitor the device from the Command Center console.

In this release, there are significant enhancements in Command Center authentication and authorization capabilities can seamlessly change the authentication settings for a user between Local and External authentication types from the Command Center interface. Group Extraction capability has been added to the Active Directory authentication type. Also, you can add multiple Active Directory groups to Command Center.

For more information, see New in This Release.

In This Section

Getting Started with Command Center Appliance	Provides step-by-step instructions for installing, configuring, upgrading, performing backup and restore operations on Command Center hardware appliance.
Installing Command Center	Provides step-by-step instructions for installing Command Center server on Windows Server and Linux operating systems. Also included is information about certificates and using Command Center as a startup service. Also provides a list of the Citrix products that Command Center supports.
Upgrading Command Center	Provides step-by-step instructions for upgrading Command Center server on Windows Server and Linux operating systems.
Getting Started with Command Center	Provides instructions on how to log on to Command Center and begin monitoring and managing Citrix devices.

Monitoring the Citrix Network	Provides instructions on how to monitor the Citrix network using different views.
Monitoring Devices	Describes the operations you can perform on Citrix devices from the Citrix Network tab.
Monitoring Your Network by Using the Home Page	Describes the high-level view of the performance of your Citrix network.
Monitoring and Managing Events Generated on Citrix Devices	Provides a conceptual reference and instructions for monitoring and managing the SNMP and Syslog events generated on the Citrix devices.
Monitoring and Managing the Real-Time Status of Entities Configured on NetScaler Devices	Provides a conceptual reference and instructions for monitoring and managing the states of virtual servers, services, and service groups across the NetScaler infrastructure.
Using Tasks to Configure Managed Devices	Provides a conceptual reference and instructions for using built-in and custom tasks to make configuration changes across devices.
Monitoring and Managing SSL Certificates Configured on NetScaler Devices	Provides a conceptual reference and instructions for monitoring and managing SSL certificates installed across all managed NetScaler devices.
Auditing Configuration Changes Across NetScaler Devices	Provides a conceptual reference and instructions for monitoring and auditing configuration changes across managed NetScaler devices.
Using Performance Reports and Thresholds to Monitor Device Performance	Provides a conceptual reference and instructions for monitoring the performance of discovered Citrix devices by using performance reports and threshold functionality. Also provides instructions for monitoring Application Firewall syslog events.
Administering Command Center	Provides a conceptual reference and instructions for administering and securing the Command Center server.
NetScaler SNMP Counters Polled from Command Center	Describes the SNMP counters that Command Center polls from NetScaler devices to gather performance data.

Release Notes

The Citrix Command Center Release Notes describe the new features and enhancements, bug fixes, limitations, and known issues and workarounds in Citrix Command Center release 5.0.

In this section:

Release Notes

The Citrix Command Center Release Notes describe the new features and enhancements, bug fixes, limitations, and known issues and workarounds in Citrix Command Center release 5.0.

In this section:

New in This Release

The Citrix Command Center release 5.0 includes the following new features and enhancements.

Build 37.2

The Citrix Command Center release 5.0, build 37.2 includes the following new features and enhancements.

Command Center Appliance Setup Wizard

You can configure the initial settings by using the **Setup Wizard** available under **Administration > Settings** screen in Command Center graphical user interface. You can also change the existing network setting using this wizard.

Command Center Appliance High Availability Setup

You can initiate a high availability configuration from an appliance by using the **Setup High Availability** option under **Administration> Settings**. The appliance from which the configuration is initiated is designated as the primary node.

Build 35.2

The Citrix Command Center release 5.0, build 35.2 includes the following new features and enhancements.

Command Center Hardware Appliance

The Command Center appliance provides a hardware-based turnkey solution with a preloaded database. 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 Command Center appliance comprises the Citrix XenServer virtualization platform, 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.

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

Operating System Support

You can now install the Command Center server on Windows Server 2008 R2 and CentOS 5.5.

Changes in Database Requirements

With this release, the Oracle 11g database is supported.

Authentication and Authorization Enhancements

With this release, following are the significant enhancements to authentication and authorization capabilities in Command Center:

- **Local and External Authentication**

  You can seamlessly change the authentication settings for a user between Local and External authentication type, from Command Center interface. You can define the authentication type for the user when add the user to Command Center or edit the setting at a later point in time.

  When you modify the authentication type for a user from External to Local, the default password is same as the username. However, Citrix recommends that you change the password after modifying the authentication type to Local.

- **Active Directory Group Based Control**

  Group Extraction capability has been added to the Active Directory authentication type. Command Center can query Active Directory groups assigned for a user and authenticate the user in Command Center.

- **Add Groups by Browsing through Active Directory Groups**

  When you select the Group Extraction option under the Active Directory settings, and provide group attributes, you can directly browse the Active Directory groups in the Add Groups interface and add multiple groups in Command Center.

- **Add Multiple Groups**

  You can add multiple groups in Command Center in a single operation using comma as a delimiter.

- **Create Group Names with Special Characters**

  You can create group names with special characters. Note that comma is treated as a delimiter but not as a special character.

- **Authorize Users**

  For successful authorization in Command Center, user must belong to at least one group with privileges defined. If the authorization fails, the user is not authenticated in Command Center even if the user has provided correct login credentials.

- **Change Password upon Password Expiration**

  If the user's password expires, the user is automatically redirected to the Change Password page where the user can change the password and log into Command Center.

Audit Logs

You can view the details of security administration operations, such as operations on users or groups, which are audited by Command Center under the AuditedObjects column on the Audit Logs page. You can also export the audited information to a CSV file format by clicking the Export button on the Audit Logs page.

Support for Branch Repeater 6.0 Release

The Branch Repeater 6.0 release supports three major features – Traffic Shaping (QOS), Centralized License Server support, and HTTP Caching. To support these features following enhancements are added to Command Center:

- **Device Inventory**

  In addition to the previously existing device properties, the Device Properties page now displays the Branch Repeater appliance Serial Number and the QOS Status.

- **New Custom Reports**

  In this release, Command Center provides 11 new built-in custom reports for Repeater devices :

  - Repeater Plugin Usage
  - Repeater QOS
  - Repeater Service Class
  - Repeater Throughput
  - Repeater Application
  - Repeater Capacity Increase
  - Repeater CPU utilization
  - Repeater Data Reduction
  - Repeater Link Utilization
  - Repeater Packet Loss
  - Repeater Pass Through Connection

  To access custom reports on the Reporting tab, in the left pane, under Performance, click Custom Reports.

- **New Counter Groups**

  Command Center adds three new counter groups for Repeater devices:

- **Repeater App Traffic Group**

  This group reports acceleration statistics on all known applications. It includes the application name, per-poll-interval send rate (kbps), per-poll-interval receive rates (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **Repeater Link Stats Group**

  This group reports traffic on each Repeater logical link. It includes the link name, per-poll-interval send rate (kbps), per-poll-interval receive rate (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **Repeater QOS Stats Group**

  Reports traffic that the Repeater accelerates. It includes the QOS policy name, link name, per-poll-interval send rate (kbps), per-poll-interval receive rates (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **New SNMP Traps**

  Command Center has added eighteen new SNMP traps for Repeater devices.

NetScaler SDX Device Support in Command Center

Command Center provides support to NetScaler SDX devices. After the NetScaler SDX device is up and running, you can perform various tasks to manage and monitor the device from the Command Center console.

Note: Command Center supports the NetScaler SDX devices running NetScaler release 9.3, build 53.x or earlier.

Command Center provides the following enhancements to support NetScaler SDX devices:

Command Center provides the following enhancements to support NetScaler SDX devices:

- **Add NetScaler SDX Device Profile**

  You can add device profiles to specify the user credentials that are used by Command Center to communicate with the NetScaler SDX device and retrieve configuration data.

- **Add NetScaler SDX Device**

  The SDX device is represented as NS SDX in the right pane of the Citrix Network page. You can add devices by specifying the host names of the devices or the IP addresses of each SDX device. You can also add devices by importing the device names from a file.

- **View Device Properties**

  You can view the properties of the NetScaler SDX devices in Command Center. The properties displayed are Name, NetScaler SDX IP address, Node State, Maximum NetScaler instances, CPU and memory usage details, Monitoring details, and the

NetScaler instances provisioned and their provisioning status.

- **Provision NetScaler Instances on SDX**

  You can now provision NetScaler instances on NetScaler SDX and consequently manage and monitor the NetScaler instances. First, you need to add a NetScaler SDX device and set it for discovery. After the NetScaler SDX is discovered, you can provision the NetScaler instances on the NetScaler SDX from Command Center client. Command Center then deploys NetScaler instances on the NetScaler SDX and then discovers the NetScaler instances for monitoring and management.

  If you have NetScaler instances already installed on a NetScaler SDX, discovering the NetScaler SDX implicitly discovers all the NetScaler instances.

- **De-Provision NetScaler Instances**

  You can de-provision the discovered NetScaler instances on NetScaler SDX from Command Center console. The De-Provision icon is available on the Device Properties page of the NetScaler SDX device.

Application Template Group Deployment

You can now import an application template to multiple NetScaler devices simultaneously by using the Command Center built-in configuration task ImportApplicationTemplate. Before executing the built-in task, you need to download the application template either to your local system or to the Command Center server. Then, run the ImportApplicationTemplate task, and follow the prompts in the wizard to import the template and the deployment files to multiple NetScaler devices at the same time.

Note: This feature works only with NetScaler release 9.3 application templates.

Command Center Agent Setup

You can unassign the devices managed by the Command Center Agent and assign them back to the Command Center server when the Agent server is not active. The Unassign link for the Command Center Agent, which is not active is available on Agent Setup page on the Administration tab.

User Details in Task Execution Log

After executing a task, you can view the execution details of that task immediately or at a later time. When the task is executed, the details of the Command Center users who started the task are also displayed under CC User column on the Execution Log page.

Syslog Search

You can use the Search or Advanced Search functionality to search for specific AppFirewall log messages. You can either enter the entire log message or a substring of the message to search, or use the listed criteria. The enhancements in Syslog search are:

- You can search for Syslog messages generated within a range of time by selecting the ‘is between’ sub-criterion of date criteria on the Advanced Search page.

- You can specify multiple comma-delimited search strings to search Syslog messages generated for selected criteria on the Advanced Search page.

New in This Release

The Citrix Command Center release 5.0 includes the following new features and enhancements.

Build 37.2

The Citrix Command Center release 5.0, build 37.2 includes the following new features and enhancements.

Command Center Appliance Setup Wizard

You can configure the initial settings by using the **Setup Wizard** available under **Administration > Settings** screen in Command Center graphical user interface. You can also change the existing network setting using this wizard.

Command Center Appliance High Availability Setup

You can initiate a high availability configuration from an appliance by using the **Setup High Availability** option under **Administration> Settings**. The appliance from which the configuration is initiated is designated as the primary node.

Build 35.2

The Citrix Command Center release 5.0, build 35.2 includes the following new features and enhancements.

Command Center Hardware Appliance

The Command Center appliance provides a hardware-based turnkey solution with a preloaded database. 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 Command Center appliance comprises the Citrix XenServer virtualization platform, 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.

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

Operating System Support

You can now install the Command Center server on Windows Server 2008 R2 and CentOS 5.5.

Changes in Database Requirements

With this release, the Oracle 11g database is supported.

Authentication and Authorization Enhancements

With this release, following are the significant enhancements to authentication and authorization capabilities in Command Center:

- **Local and External Authentication**

  You can seamlessly change the authentication settings for a user between Local and External authentication type, from Command Center interface. You can define the authentication type for the user when add the user to Command Center or edit the setting at a later point in time.

  When you modify the authentication type for a user from External to Local, the default password is same as the username. However, Citrix recommends that you change the password after modifying the authentication type to Local.

- **Active Directory Group Based Control**

  Group Extraction capability has been added to the Active Directory authentication type. Command Center can query Active Directory groups assigned for a user and authenticate the user in Command Center.

- **Add Groups by Browsing through Active Directory Groups**

  When you select the Group Extraction option under the Active Directory settings, and provide group attributes, you can directly browse the Active Directory groups in the Add Groups interface and add multiple groups in Command Center.

- **Add Multiple Groups**

  You can add multiple groups in Command Center in a single operation using comma as a delimiter.

- **Create Group Names with Special Characters**

  You can create group names with special characters. Note that comma is treated as a delimiter but not as a special character.

- **Authorize Users**

  For successful authorization in Command Center, user must belong to at least one group with privileges defined. If the authorization fails, the user is not authenticated in Command Center even if the user has provided correct login credentials.

- **Change Password upon Password Expiration**

  If the user's password expires, the user is automatically redirected to the Change Password page where the user can change the password and log into Command Center.

Audit Logs

You can view the details of security administration operations, such as operations on users or groups, which are audited by Command Center under the AuditedObjects column on the Audit Logs page. You can also export the audited information to a CSV file format by clicking the Export button on the Audit Logs page.

Support for Branch Repeater 6.0 Release

The Branch Repeater 6.0 release supports three major features – Traffic Shaping (QOS), Centralized License Server support, and HTTP Caching. To support these features following enhancements are added to Command Center:

- **Device Inventory**

  In addition to the previously existing device properties, the Device Properties page now displays the Branch Repeater appliance Serial Number and the QOS Status.

- **New Custom Reports**

  In this release, Command Center provides 11 new built-in custom reports for Repeater devices :

  - Repeater Plugin Usage
  - Repeater QOS
  - Repeater Service Class
  - Repeater Throughput
  - Repeater Application
  - Repeater Capacity Increase
  - Repeater CPU utilization
  - Repeater Data Reduction
  - Repeater Link Utilization
  - Repeater Packet Loss
  - Repeater Pass Through Connection

  To access custom reports on the Reporting tab, in the left pane, under Performance, click Custom Reports.

- **New Counter Groups**

  Command Center adds three new counter groups for Repeater devices:

- **Repeater App Traffic Group**

  This group reports acceleration statistics on all known applications. It includes the application name, per-poll-interval send rate (kbps), per-poll-interval receive rates (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **Repeater Link Stats Group**

  This group reports traffic on each Repeater logical link. It includes the link name, per-poll-interval send rate (kbps), per-poll-interval receive rate (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **Repeater QOS Stats Group**

  Reports traffic that the Repeater accelerates. It includes the QOS policy name, link name, per-poll-interval send rate (kbps), per-poll-interval receive rates (bps), per-poll-interval dropped send bytes (due to exceeding QOS limits), and per-poll-interval dropped receive bytes.

- **New SNMP Traps**

  Command Center has added eighteen new SNMP traps for Repeater devices.

NetScaler SDX Device Support in Command Center

Command Center provides support to NetScaler SDX devices. After the NetScaler SDX device is up and running, you can perform various tasks to manage and monitor the device from the Command Center console.

Note: Command Center supports the NetScaler SDX devices running NetScaler release 9.3, build 53.x or earlier.

Command Center provides the following enhancements to support NetScaler SDX devices:

Command Center provides the following enhancements to support NetScaler SDX devices:

- **Add NetScaler SDX Device Profile**

  You can add device profiles to specify the user credentials that are used by Command Center to communicate with the NetScaler SDX device and retrieve configuration data.

- **Add NetScaler SDX Device**

  The SDX device is represented as NS SDX in the right pane of the Citrix Network page. You can add devices by specifying the host names of the devices or the IP addresses of each SDX device. You can also add devices by importing the device names from a file.

- **View Device Properties**

  You can view the properties of the NetScaler SDX devices in Command Center. The properties displayed are Name, NetScaler SDX IP address, Node State, Maximum NetScaler instances, CPU and memory usage details, Monitoring details, and the

NetScaler instances provisioned and their provisioning status.

- **Provision NetScaler Instances on SDX**

  You can now provision NetScaler instances on NetScaler SDX and consequently manage and monitor the NetScaler instances. First, you need to add a NetScaler SDX device and set it for discovery. After the NetScaler SDX is discovered, you can provision the NetScaler instances on the NetScaler SDX from Command Center client. Command Center then deploys NetScaler instances on the NetScaler SDX and then discovers the NetScaler instances for monitoring and management.

  If you have NetScaler instances already installed on a NetScaler SDX, discovering the NetScaler SDX implicitly discovers all the NetScaler instances.

- **De-Provision NetScaler Instances**

  You can de-provision the discovered NetScaler instances on NetScaler SDX from Command Center console. The De-Provision icon is available on the Device Properties page of the NetScaler SDX device.

Application Template Group Deployment

You can now import an application template to multiple NetScaler devices simultaneously by using the Command Center built-in configuration task ImportApplicationTemplate. Before executing the built-in task, you need to download the application template either to your local system or to the Command Center server. Then, run the ImportApplicationTemplate task, and follow the prompts in the wizard to import the template and the deployment files to multiple NetScaler devices at the same time.

Note: This feature works only with NetScaler release 9.3 application templates.

Command Center Agent Setup

You can unassign the devices managed by the Command Center Agent and assign them back to the Command Center server when the Agent server is not active. The Unassign link for the Command Center Agent, which is not active is available on Agent Setup page on the Administration tab.

User Details in Task Execution Log

After executing a task, you can view the execution details of that task immediately or at a later time. When the task is executed, the details of the Command Center users who started the task are also displayed under CC User column on the Execution Log page.

Syslog Search

You can use the Search or Advanced Search functionality to search for specific AppFirewall log messages. You can either enter the entire log message or a substring of the message to search, or use the listed criteria. The enhancements in Syslog search are:

- You can search for Syslog messages generated within a range of time by selecting the ‘is between’ sub-criterion of date criteria on the Advanced Search page.

- You can specify multiple comma-delimited search strings to search Syslog messages generated for selected criteria on the Advanced Search page.

Bug Fixes in Release 5.0

The following table lists the bug fixed in Command Center release 5.0.

Bug Fixes in Release 5.0 Build 37.2

Issue ID	Issue Description
0346650	Configuration of Command Center appliances in High Availability mode fails in Command Center release 5.0, build 35.11.
0351737	The Command Center software version displayed in the Add/Remove Programs >Support information window is incorrect.
0353659	You cannot select a group from the Active Directory groups list in Command Center if any of the Active Directory group names includes backslash (\) character.
0361321	The Active Directory users present under sub domain are not authenticated in Command Center.
0361473	The configuration of the Syslog Purge Interval doesn't work.
0363434	The resource check for port "8009" is removed as this port is no longer used by Command Center.
0356432	The discovery of Citrix Branch Repeater with Windows Server (CBRwWS), running release 6.2.0 or later, fails because the Command Center server does not automatically add the Command Center IP address as an SNMP manager on CBRwWS during the discovery process.
0303315	When you add a group in Command Center by browsing the Active Directory groups, not all the groups in Active Directory are displayed.

Bug Fixes in Release 5.0 Build 36.3

Issue ID	Issue Description
0292026	Even when the Mail server authentication is enabled, emails are not getting generated for alarm triggers.
0314359	The configuration change history is not displayed in device properties or on Change management page.

0319757	Config Change History audit policy report was empty when executed after 24 hours period even there are ns config change events.
0332374	When you discover a device and the profile has a special character in the community string, for every rediscovery process on the device, Command Center receives the "netscalerConfigchange" trap.
0332754	Authentication fails if the User password have special characters percentage(%) and ampersand(&) in it.
0346003	When the refresh interval is less than the time taken by CC to poll the entities, the Entity Monitoring tab in the UI does not display all the entities till the polling gets completed.
0346650	HA will not be formed for Command Center Installation for CC5.0 Builds 35.11
0347643	CC is not able to generate CSR for certs which were added in NS using FIPS key. CC uses openssl binary to generate CSR, but it doesn't understand FIPS, hence generating CSR will be failed.
0348611	Occasionally, the Certificate Monitoring tab was not showing all the polled SSL certificates. This issue is fixed.
0351712	Command Center installation is not successfully completed because some of the installation files are missing.

Bug Fixes in Release 5.0 Build 35.11

Issue ID	Issue Description
0289417	During installation of Command Center release 5.0 on a Linux machine, connection to an MSSQL 2008 database fails even if the database parameters are defined correctly.

Bug Fixes in Release 5.0 Build 35.6

Issue ID	Issue Description
0306513	If you are trying to discover SDX devices running NetScaler releases 9.3, build 55.x or higher, an error occurs, and the device inventory details are not displayed.

Bug Fixes in Release 5.0 Build 35.2

Issue ID	Issue Description

0273425	All the service groups bound to a load balancing server are not displayed. **Note:** This issue was identified in Command Center 4.1 release and has been fixed in this release.

Limitations

The following table describes the limitations and known issues in Command Center 5.0 release.

Issue ID	Issue Description
0355090	If you are using the pre-packaged PostgreSQL database with Command Center, an error occurs when you execute a custom task with the backslash (\) character.
0268327	If you are using Internet Explorer 9 on Windows 7 to access Command Center client, you may observe that the brows freezes or stops responding. You may be experiencing this behavior for one of the reasons mentioned in the links bel http://www.fixie9.com/fixie9/ie9freezes-windows7.php, http://windows.microsoft.com/en-US/windows-vista/tips-for-solving-problems-with-internet-explorer, and http://support.microsoft.com/kb/968136.
0246561	Command Center does not support MySQL database version 5.5 and later.
0238993	If you open the options under Security, Operations, or Settings on the Administration page in multiple tabs, the navigation path displayed for the current option includes the previously displayed options. For example, if, under Security, you open Authentication Settings in a new tab, and then open Users in another tab, the navigation path on Users page incorrectly displays Administration > Authentication Settings > Users instead of just Administration > User
0230431	If you want to use the pre-packaged Postgre SQL database with Command Center 4.1, you must have the .NET frame 3.5 installed on your system.
0234676	You cannot modify or delete NetScaler Pool maps.
0234377	The built-in task SoftwareUpgrade fails on Branch Repeater devices running on Windows platform.
0235683	If you have created custom view scopes in Command Center release 3.3 and have now upgraded to release 4.1, and t custom view scopes will no longer be available. This is because of the enhancements in the authorization mode.
0247421	If you have defined privileges in Command Center release 3.3 and have now upgraded to release 4.1, the privileges defined will no longer be available. This is because of the enhancements in the authorization mode.
0235498	If you are running Command Center as a virtual machine (VM), when Live Update process of Symantec Endpoint Protection runs, the Command Center server may lose connection to the database or may shut down.
0203098	Event Severity configuration changes roll back to their default configurations after a service pack installation.
0233920	If you are using Internet Explorer version 8, when you try to execute the built-in task InstallSSLCert, in the Preview p the actual file path is replaced with a fakepath, for example, c:\fakepath*filename*. This is due to a security feature Internet Explorer version 8. For more information, see http://www.telerik.com/community/forums/aspnet-ajax/upload/ie8-upload-control-shows-quot-c-fakepath-quot.as
0225713	If the hostname of the Command Center server contains an underscore ('_'), you may encounter a java exception.
0203033	Command Center displays only the latest 1000 events in the client. If an alarm is in the Clear state and a new event correlating to this alarm is not generated within 24 hours, the alarm is removed from display.

Known Issues and Workarounds

The following table describes the known issues with their workarounds in Command Center Release 5.0.

Issue ID	Issue Description	Workaround
0332765	The Command Center HA setup stops working when JVM fails on the Command Center secondary server.	Restart the Command Center secondary server.
0328324	If you upgrade Command Center from 4.x release to 5.0 release, two instances of Command Center are displayed in the Add/Remove programs window. An error occurs when you uninstall Command Center software.	If you want to uninstall Command Center software, you have to uninstall Command Center 5.0 version first and then uninstall the Command Center 4.x version from the Add/Remove programs.
0268067	When a user downloads the Command Center installer on Windows and uses the FTPS utility to transfer the same installer to a Linux system, the binary file retains the control characters in the installer. This results in the installer being corrupted. If you use the FTP utility in the text mode, then the chances of file getting corrupted is more. As a result of the control characters, the JVM displays error messages when the Command Center service starts.	Execute the following commands to convert the installer into the UNIX format: cd <CC_HOME>/jre/lib/i386 dos2unix -q -o jvm.cfg
0257635	A Branch Repeater device connected to Command Center becomes inaccessible from Command Center, and the following error message appears: "Exception while doing inventory collection :No such SNMP MIB exists" is displayed.	Provide a higher value for SNMP retry count and timeout value and then rediscover the Branch Repeater device.

0250905	On a HA failover, alarm triggers configured in the primary appliance within the file synchronization interval will be lost. As a result, the alarm triggers created are not displayed in the Command Center UI after the failover . Note: Configuration files synchronization happen between primary and secondary appliance every 2 minutes by default.	You can re-create the alarm triggers in Command Center.
0228281	Show Running Configuration and Difference between Running and Saved Configuration fails if the SSH password contains single quote (') or double quote (") characters.	Do not use single quote (') or double quote (") characters in your password.
0221240	If you have McAfee On-Demand scan running, and if you are using external MySQL database, a few device operations, such as Invoke NS CLI and Rediscover may not work, and you may encounter an error message, such as “java.sql.SQLException: General error message from server: “Can't create/write to file 'c:\windows\temp\#sql_5ac_0.MYI' (Errcode: 13)””	Configure the McAfee On-Demand scan such that it does not protect write operations on the following directory: c:\windows\temp For more information, see http://forums.mysql.com/read.php?34,33544,233949#msg-233949

Command Center Appliance

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

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.

External Software Components

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

Hardware Components

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.

Ports

RS232 Serial Port

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.

Copper Ethernet Ports

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

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, and MPX 22040/22060/22080/22100/22120 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.
			Blinking green	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

For appliances containing two power supplies, the second power supply acts as a backup. The MPX 22040/22060/22080/22100/22120 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 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 1. 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.
	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 2. 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.
	RED	Power supply failure.

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

Electrical Safety Precautions for Power Supply Replacement

- 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.

Replacing an AC Power Supply

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 platform 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 platform which needs 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.

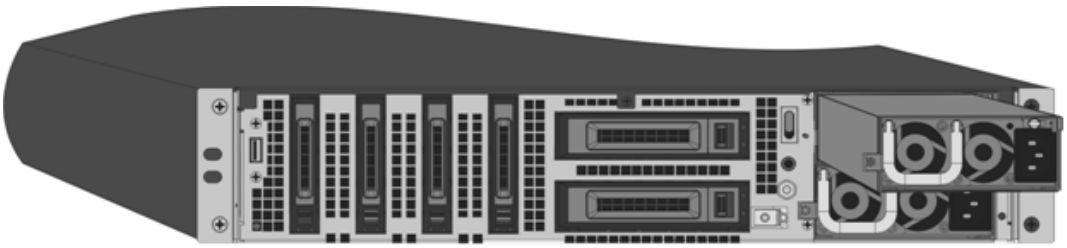


Figure 2. Inserting the Replacement AC Power Supply

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.

Replacing a DC Power Supply

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 platform 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 platform which needs 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.

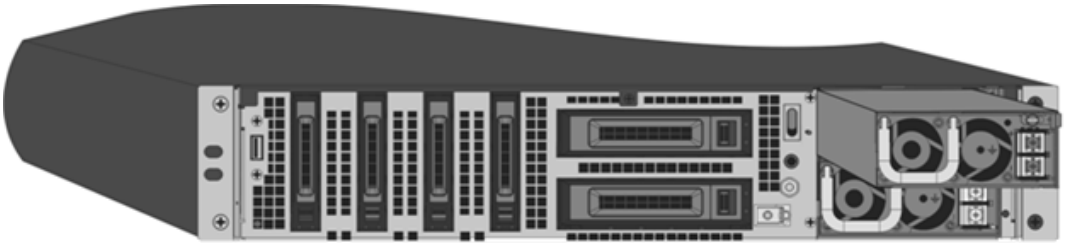


Figure 4. Inserting the Replacement DC Power Supply

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

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

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

Replacing a Hard Disk Drive

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.

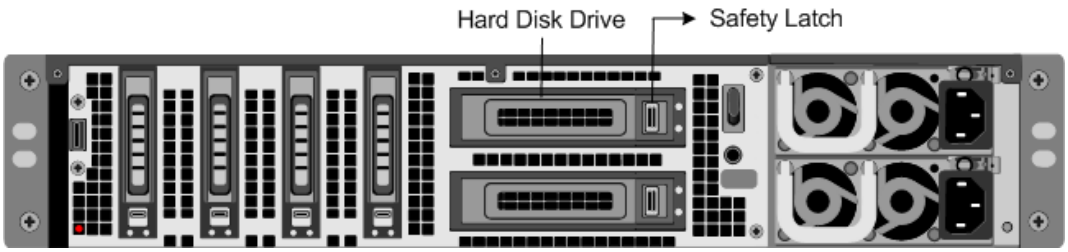


Figure 1. Removing the Existing Hard Disk Drive

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 2. 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.

Hardware Platform

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.

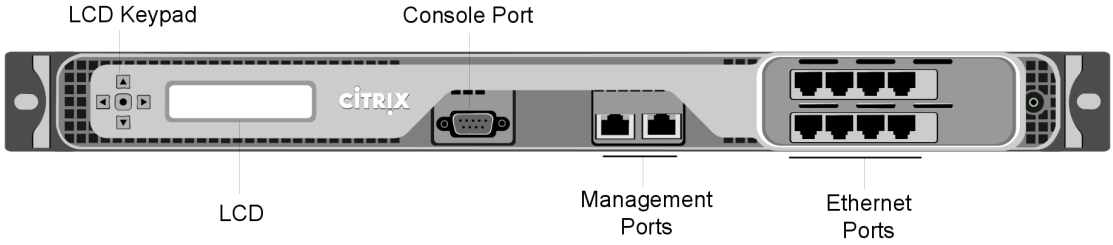


Figure 1. Citrix Command Center MPX 7500(8x10/100/1000Base-T copper Ethernet ports), front panel

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.

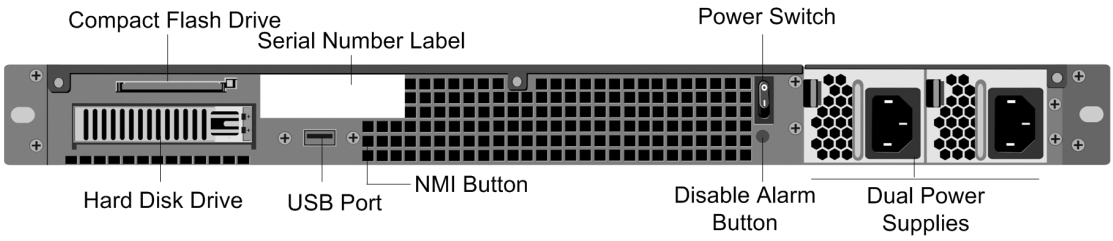


Figure 2. Citrix Command Center MPX 7500, back panel

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

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.

Unpacking the Appliance

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, and MPX 17500/19500/21500, 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 appliance

    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

Preparing the Site and Rack

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 21 degrees C/70 degrees F at altitudes of up to 2100 m/7000 ft, or 15 degrees C/60 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.

Cautions and Warnings

Electrical Safety Precautions

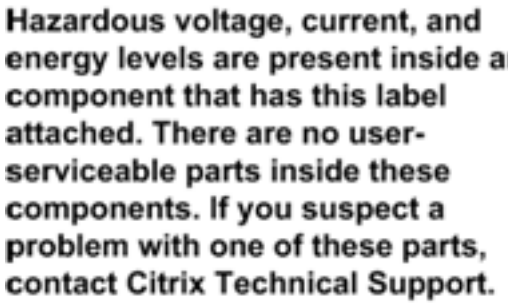
Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

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:



Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- 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

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.

Rack Mounting the Appliance

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.

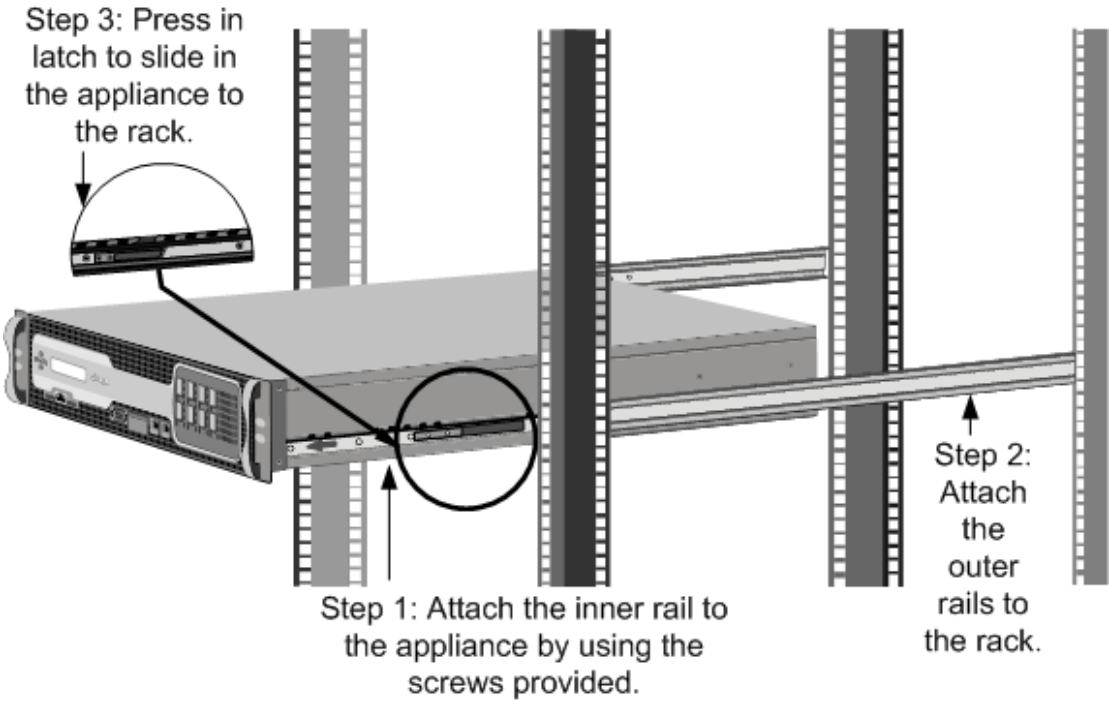


Figure 1. Rack Mounting the Appliance

Connecting the Cables

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.

To connect an Ethernet cable to 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.

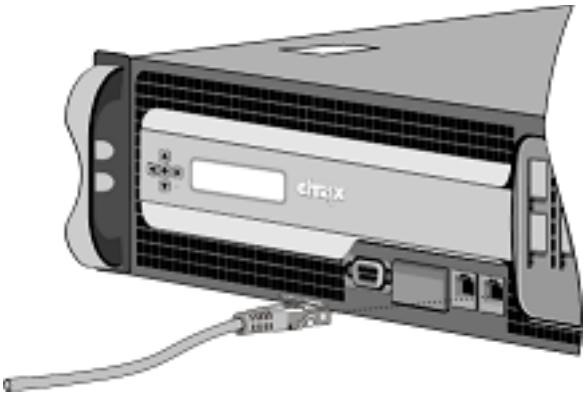


Figure 1. Inserting an Ethernet cable

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

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.

   Figure 2. Inserting a console cable

   Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

The MPX 7500 appliances ship with two power cables. A separate ground cable is not required, because the three-prong plug provides grounding.

The CloudBridge appliances can have either one or two power supplies. A separate ground cable is not required, because the three-prong plug provides grounding. Power up the appliance by installing one or both power cords.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.

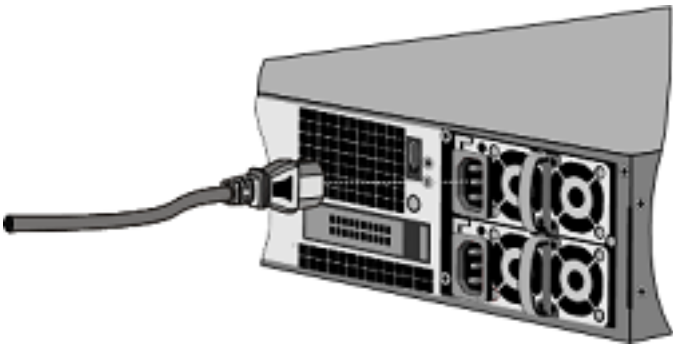


Figure 3. Inserting a power cable

2. Connect the other end of the power cable to a standard 110V/220V power outlet.

3. Repeat steps 1 and 2 to connect the second power supply.

Note: The appliance emits a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.

Switching on the Appliance

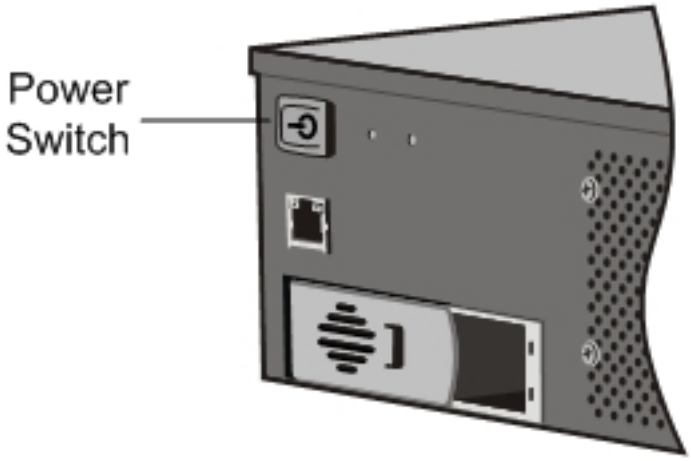
After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you 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 1. 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.

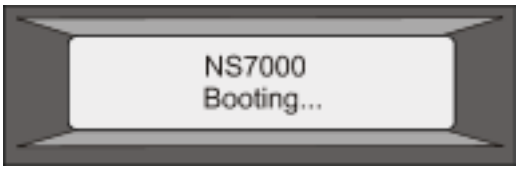


Figure 2. LCD startup screen

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

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.

Configuring Initial Settings by using the Serial Console

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. For more information about configuring the appliance, see http://support.citrix.com/proddocs/topic/netscaler/cc-gen-command-center50-wrapper-con.html.

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 :
```

Configuring Initial Settings without using the Serial Console

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 > Settings, 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. For more information about configuring the appliance, see http://support.citrix.com/proddocs/topic/netscaler/cc-gen-command-center50-wrapper-con.html.

Changing the Network Settings by using the Serial Console

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. For more information about configuring the appliance, see http://support.citrix.com/proddocs/topic/netscaler/cc-gen-command-center50-wrapper-con.html.

Changing the Default Password of the 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. Click the Change Password link.
4. Type the Current Password.
5. Type and re-type the new password.
6. Click OK.

Command Center Appliances in a High Availability Pair

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.

Prerequisites

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.

Configuring High Availability

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 > Settings**.
2. Under **Settings**, 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.)

Removing Command Center Appliances from an HA Setup

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.)

Performing a Force Failover in a High Availability Setup

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 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

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.

Obtaining Appliance Licenses

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.

Upgrading Appliance Licenses

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 appliance license from an Evaluation license to a Retail license

Follow this procedure to upgrade the 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

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.

Upgrading a Standalone 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.

Parameters for Upgrading Command Center

SP_FILE

Complete path to the service pack file.

USER_NAME

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

Upgrading Command Center Appliances in a High Availability Setup

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>
   ```

4. When prompted, type the password.

Performing Backup and Restore Operations

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.

Database Backup

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 Operations, 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

Restoring the Data

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

Restoring the Data on an External Appliance

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
…
…
…
```

You can now generate reports from this external database. For more information about running a quick report, see http://support.citrix.com/proddocs/topic/command-center-50/cc-perf-report-quick-tsk.htmlthe Command Center User's Guide at . For more information about creating a c report, see http://support.citrix.com/proddocs/topic/command-center-50/cc-perf-report-conf-custom-tsk.htmlthe Command Center User's Guide at .

Installing Command Center Software

Command Center 5.0 offers new features and improved functionality of existing features. For more information, see New in This Release.

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

Licensing

The following Citrix products and editions are supported by Command Center. A Citrix license is required for each edition you want to use on Command Center.

- NetScaler Enterprise and Platinum editions
- Access Gateway Enterprise edition
- Repeater and Branch Repeater, all editions

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

Citrix Products Supported

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

Before You Begin

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.

In this section:

Hardware Requirements

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

Disk Space for Performance Management

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
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

Operating System Requirements

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

Operating System	Version
Windows	· Windows 2008 · Windows 2008 R2 · Windows 2003 Service Pack 2 · Windows 2003 Server R2 Standard x64 Edition
Linux	· Red Hat Enterprise Linux AS 4.0 · Red Hat Enterprise Linux ES 4.0 and 5.1 · CentOS 5.5 version

Database Requirements

Command Center supports the following databases and their versions.

Database Type	Version
MySQL	5.1.x with InnoDB storage engine
Oracle	10g/11g
Microsoft SQL Server	2005 and 2008 2005, 2008, and 2008 R2

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.

Additional Linux Requirements

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*

Client Requirements

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

Client type	Platform	Software
HTML	Windows	· Microsoft Internet Explorer 5.0 or later · Mozilla Firefox 1.0 or later · Netscape 7.1 or later · Google Chrome 7.0 or later
	Linux	Mozilla Firefox 1.0 or later

Port Settings

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 Branch Repeater.

Purpose	Port
SNMP communication between the Citrix Command Center server and the Citrix NetScaler system and Citrix Branch Repeater.	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 Branch Repeater.	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

Database Settings

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

  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.
- Oracle 10g and 11g. For instructions on installation, see http://www.oracle.com/technology/documentation/database10gr2.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.
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 *'DatabaseUserPassword'*; GRANT SELECT, UPDATE on 'mysql'.'user' TO *'DatabaseUserName'@'CommandCenterIPAddress';* GRANT RELOAD, PROCESS ON *.* TO *DatabaseUserName@CommandCenterIPAddress;*

Installing the Command Center Server on Windows

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:

CC_Setup_5.0_20_0.exe

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:

   a. 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.

   b. Under Security Settings, select either HTTP or HTTPS.

   c. 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

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, monitoring entities and syslog messages, and configuration using tasks. The agents are used 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 server and the agents are connected to the same database.

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 executable file with the following naming convention:

CC_Setup_*ReleaseNumber_BuildNumber*.exe

Example:

CC_Setup_5.0_20_0.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. For information on installing the server on Windows, see Installing the Command Center server on Windows.

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

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

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:

CC_Setup_5.0_20_0.bin

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:
   ./CC_Setup_*ReleaseNumber_BuildNumber*.bin

   Example:

   ./CC_Setup_5.0_20_0.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:

   a. 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.

   b. Under Security Settings, select either HTTP or HTTPS.

   c. 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:

   ./CC_Setup_5.0_20_0.bin -i console

   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:

   a. Enter one of the following database options - 1 for MYSQL, 2 for Oracle, or 3 for MS SQL.

   b. 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."

   c. Enter the communication mode you want to use. Type 1 for HTTP or 2 for HTTPS.

   d. 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.

In this section:

- 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.*Citrix Command Center 5.0 Administrator's Guide*.

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:

CC_Setup_5.0_20_0.bin

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. For information on installing the server on Linux, see Installing the Command Center server on Linux.

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

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 a 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

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

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

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.

It is assumed that you already have the certificate you want to install. If you do not have a certificate, see the section "Generating a New Certificate and Key" in the *Citrix NetScaler Traffic Management Guide* at: http://support.citrix.com/article/CTX128670.

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 Settings, 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

Command Center 5.0 offers new features and improved functionality of existing features. For more information, see

Upgrading the Command Center server to release 5.0 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.

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 5.0, 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 5.0.

Upgrade Scenarios and Steps

The following table summarizes three scenarios and the upgrade steps you must follow to upgrade your Command Center under each scenario.

Scenario	Upgrade Steps

Upgrading from Command Center release 3.x with one of the following databases: · MS SQL database · Oracle database · External MySQL 5.1.x with InnoDB storage engine	1. Upgrade to Command Center 4.0 by installing the service CC_SP4.exe (for Windows) or, CC_SP4.bin (for Linux) For information about the installation steps, see Installin Service Pack. 2. Upgrade to Command Center 4.1 by installing the latest v of the service pack with file naming convention: CC_SP_*ReleaseNumber_BuildNumber*.exe (for Windows) o CC_SP_*ReleaseNumber_BuildNumber*.bin (for Linux) 3. Upgrade to Command Center 5.x by installing the latest v of the service pack with file naming convention: CC_SP_*ReleaseNumber_BuildNumber*.exe (for Windows) o CC_SP_*ReleaseNumber_BuildNumber*.bin (for Linux) For information about the installation steps, see Installing th Service Pack.
Upgrading from Command Center release 3.x with one of the following MySQL database versions: · Internal MySQL · External MySQL running a version earlier than 5.1.x · External MySQL running version 5.1.x and with MyISAM storage engine.	1. Migrate to an external MySQL database running version 5. with InnoDB storage engine. For information about the migration executable and the migration steps, see Migrating MySQL Database. 2. Upgrade to Command Center 4.0 by installing the service CC_SP4.exe (for Windows) or, CC_SP4.bin (for Linux). For information about the installation steps, see Installin Service Pack. 3. Upgrade to Command Center 4.1 by installing the latest v of the service pack with file naming convention: CC_SP_*ReleaseNumber_BuildNumber*.exe (for Windows) o CC_SP_*ReleaseNumber_BuildNumber*.bin (for Linux) 4. Upgrade to Command Center 5.x by installing the latest v of the service pack with file naming convention: CC_SP_*ReleaseNumber_BuildNumber*.exe (for Windows) o CC_SP_*ReleaseNumber_BuildNumber*.bin (for Linux) For information about the installation steps, see Installing th Service Pack.
Upgrading within Command Center release 4.x	Install only the latest version of the 4.1 5.1 service pack with naming convention: CC_SP_*ReleaseNumber_BuildNumber*.exe Windows) or, CC_SP_*ReleaseNumber_BuildNumber*.bin (for L For information on the installation steps, see Installing the Se Pack.

In this section:

Migrating MySQL Database

For Command Center release 5.0, 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

You need to install the Command Center service pack to upgrade the Command Center server to release 5.0. 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 5.0 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 5.0, 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

Citrix Command Center is a management and monitoring solution for Citrix application networking products that include Citrix NetScaler, Citrix NetScaler VPX, Citrix Access Gateway Enterprise Edition, Citrix Branch Repeater, Citrix Branch Repeater VPX, NetScaler SDX and Citrix Repeater. 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.

In this section:

- Adding Devices
- Understanding the Discovery Process
- Provisioning NetScaler VPX Devices on XenServers
- Provisioning NetScaler Instances on NetScaler SDX
- Viewing the Discovery Status of Devices
- Viewing Inaccessible Devices

Logging on to Command Center

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

Devices are Citrix appliances or virtual appliances that you want to discover and manage.

The devices are represented as icons in the right pane of the Command Center interface. Different icons depict the different types of devices. **NS** depicts NetScaler, **AG** depicts Access Gateway, **NS VPX** depicts NetScaler VPX, **NS SDX** depicts NetScaler SDX, **R** depicts Repeaters, **BR** depicts Branch Repeaters, **BR** also depicts Branch Repeaters VPX, and **X** depicts XenServer devices. Different notations, such as green, red, and yellow arrows depict the state of the device. **HA** (high availability), **P** (primary), and **S** (secondary) depict the mode of the device.

The Command Center server supports two 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.

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. 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, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click Add Device.
3. Under Add Device, do one of the following:
   - In the Devices text box, type the host names, IP addresses, range of IP addresses of devices, and IP addresses of NAT devices you want to discover.
   - Click the Import from file check box, and then click the Browse button to select a file containing the host names and/or IP addresses of the devices you want to discover.
4. Under Select device profile, click a profile you want to use. To add a new profile, click Add Profile, and follow the steps described in Add Device Profiles.

Understanding the Discovery Process

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 >>> icon next to the device, and select 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. To check the cause of failure, on the Citrix Network tab, click the >>> icon next to the device, and select Status. You can also view the cause of failure on the Device Status page.

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. To check the cause of failure, on the Citrix Network tab, click the >>> icon next to the device, and select Status. You can also view the cause of failure on the Device Status page.

   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. To check the cause of failure, on the Citrix Network tab, click the >>> icon next to the device, and select 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 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 Repeater 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 >>> icon next to the device, and select 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

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 Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to the XenServer device on which you want to provision the NetScaler VPX devices, and then click Provision VPX.
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

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 the number of NetScaler instances already provisioned, to ensure that you do not exceed the maximum number of NetScaler instances that can be provisioned for that NetScaler SDX device.

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.
- Image: The .xva image file that you need to provision.
- 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.
- NSVLAN ID: An integer that uniquely identifies the NSVLAN. Minimum value: 2. Maximum value: 4095.
- 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

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.
2. In the right pane, click the >>> icon next to the NetScaler SDX device on which you want to provision the NetScaler instances, and then click Provision NetScaler Instance.
3. In the Provision NetScaler Instance dialog box, specify values for the following parameters.
   - Name*
   - IP Address*
   - Netmask*
   - Gateway*
   - #SSL Cores*
   - Image*
   - Feature License*
   - Admin Profile*
   - Description
4. Under Instance Admin, specify values for the following parameters.
   - User Name*
   - Password*
   - Confirm Password*
   - Shell/Sftp/Scp Access*
5. Under Resource Allocation, specify values for the following parameters.
   - Total Memory (GB)*
   - Throughput (Mbps)*
   - Packets per second*
6. Under Interfaces, 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.
7. Under NSVLAN, specify the NSVLAN ID. Optionally, select Tagged to tag packets with the specified NSVLAN ID. 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.

Viewing the Discovery Status of Devices

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, click Discovery Status.
2. On the Discovery Status page, you can view the following details:
   - Settings: Set the refresh interval for the page. Click Settings, and then in the Refresh Interval text box, type the time interval in seconds at which you want Command Center to update the discovery status, and then click Submit. By default, the refresh interval is set to 10 seconds.
   - Refresh: Refresh the discovery status at the current time.
   - Time: Time when the step in the discovery process started.
   - Device: Device that is being discovered.
   - Step: 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.
   - Message: Message that describes the reason of the discovery process failure or the details of when the discovery process started on a particular device.

Viewing Inaccessible Devices

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, under Citrix Network, click Inaccessible Systems.

2. You can perform a set of tasks on inaccessible devices, such as viewing the device properties and status, invoking the configuration utility and CLI, and rediscovering the device. For more information, see Monitoring Devices.

Monitoring the Citrix Network

Citrix network comprises devices or Citrix systems that you want to discover and manage. To begin monitoring and managing devices, you need to add the devices to your Command Center, which sets them for discovery.

After devices are discovered, you can group them under logical containers called maps, or you can create NetScaler pools that represent a group of devices considered as a single logical unit. The devices are further grouped based on their location values and you can monitor the devices using the Datacenter pane.

You can also monitor applications configured on NetScaler devices set up in a two-tier architecture.

In this section:

Configuring Maps

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.

In this section:

Adding Maps

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. You can either add a map and group devices under it logically, such as based on features configured on your devices.

Or, you can add a NetScaler pool and add devices to it. The devices added in maps configured as NetScaler pools are considered one logical unit. All configuration changes are done on all the devices in a pool. After adding a NetScaler pool, you need to configure VIPs on the pool.(See Configuring NetScaler Pool) Note that if you have a NetScaler pool already configured on your network, you only need to add the devices that are part of the pool.

Note: For more information on how NetScaler pools work, see the *Citrix NetScaler Networking Guide*

To add maps

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Maps.
2. In the right pane, click Add Map.
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. To create a NetScaler pool, select the NetScaler pool check box.
6. Under Select Devices, select the check boxes next to the devices you want to add to the map or the NetScaler pool, and then click OK.

Adding Submaps

You can add submaps within existing maps. Submaps let you logically group the devices discovered on a map. For example, you may want to configure a submap based on the geographical location of your devices. By default, when a submap is created under a map, it inherits the properties of the parent map.

To add a submap

1. On the Citrix Network tab, in the left pane, under Maps, click a map name.
2. In the right pane, click Add SubMap.
3. Under Add SubMap, enter the details as described in Adding Maps, and then click OK.

   Note: The device profile details of the NetScaler or Repeater devices are populated based on your map details.

Modifying Maps

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, under Citrix Network, expand Maps.
2. Under Maps, click the map name you want to modify.
3. In the right pane, click the map name, and then click Modify Map.
4. Under Modify Map, make the required changes, and then click OK.

Deleting Maps

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, click the map you want to delete.
2. Click Delete Map, and in the confirmation dialog box, click OK. The map is deleted.

Performing Operations on Maps

After you have grouped devices by adding maps or NetScaler pools (see Adding Maps), you can perform a set of operations on all the devices grouped under a specific map or pool, such as run reports and execute tasks.

To perform operations on maps

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Maps, and then click the map or pool name on which you want to perform an operation.
2. In the right pane, click a map on which you want to perform an operation.
    - Add SubMap: Add submaps within existing maps. You cannot create a submap within a pool.
    - Modify: Modify the map to add or remove devices, or if the device login credentials and SNMP version details have changed. You cannot modify a pool.
    - 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 or a pool.
    - Delete: Delete all the devices from the map or pool.

Configuring NetScaler Pool

A map configured as a NetScaler pool consists of devices that are considered as one logical unit. All configuration changes are done on all the devices in a pool.

You may have a NetScaler pool already configured on your network; in which case, you need to add the devices that are part of the pool when adding the map. (See Adding Maps).

Or, you may configure a NetScaler pool from Command Center. In this case, add the devices that you want to be part of the pool when adding the map. These devices are displayed as a single unit in the Maps pane. After you have added a NetScaler pool and added devices to it (see Adding Maps), you need to configure the NetScaler pool by adding VIPs to it. After you have added the VIP addresses, Command Center implicitly configures these VIPs across all the NetScaler devices added to the pool. Command Center further assigns priorities to these VIPs to set up a distributed VIP configuration.

Note: For more information on how NetScaler pools work, see the *Citrix NetScaler Networking Guide*.

To configure NetScaler pool

1. On the Citrix Network tab, in the left pane, click Maps.
2. In the right pane, under Maps, click the >>> icon next to the NetScaler pool, and then click Configure NS Pool.
3. Follow the prompts in the wizard to set up a basic distributed VIP configuration. After you have configured the NetScaler pool, you can view the configured VIP status on the NS Pool Dashboard. (see Viewing NetScaler Pool Dashboard.)

Viewing the NetScaler Pool Dashboard

After Command Center configures the VIPs across all the NetScaler devices added to a pool, you can view the configured VIP status across all the NetScaler devices in that pool. The NS Pool Dashboard provides a tabular view of the VIPs assigned to the NetScaler devices based on the priorities assigned to the VIPs. The active VIPs are depicted by a green icon.

To view NetScaler pool dashboard

1. On the Citrix Network tab, in the left pane, click Maps.
2. In the right pane, under Maps, click the >>> icon next to the NetScaler pool, and then click NS Pool Dashboard.
3. On the NS Pool Dashboard, you can view the name of the VIP and the IP addresses of the devices in that pool on which the VIPs are configured.

Performing Operations on NetScaler Pool

You can also perform various operations on a NetScaler pool, such as run a report and execute a task. When you perform an operation on a pool, the operation is performed on all the devices in the pool. If an operation, such as executing a configuration, fails on one of the devices in the pool, the configuration is rolled back on all the other devices where it has been successfully executed.

To perform operations on a NetScaler pool

1. On the Citrix Network tab, in the left pane, click Maps.
2. In the right pane, under Maps, click the >>> icon next to the NetScaler pool, and then click the operation you want to perform.

Monitoring Two-Tier Application View

You can view and monitor applications configured on NetScaler devices set up in a two-tier architecture.

Consider that you have configured a load balancing virtual on a NetScaler device in tier-1, which is the Flex tier. And you have three NetScaler VPX devices with load balancing virtual servers configured in tier-2, which is the application tier. Now, on the NetScaler in tier-1 (Flex tier), configure and bind services that represent the virtual servers on your NetScaler VPX devices in tier-2 (App tier).

Using Command Center you can view and monitor the devices and the entities configured in this topology.

To view and monitor the application view

1. On the Citrix Network tab, in the left pane, under Views, click Application.
2. In the right pane, under Application, you can view the applications configured on your NetScaler devices:
   - Application Name: Specifies the name of the application that you have configured in the two-tier topology. Clicking the application name displays the IP addresses of the devices and the endpoints configured in your setup.
   - Flex Tier: Specifies the number of devices configured in the Flex tier (tier-1). Clicking this number displays the details of the devices configured in this tier.
   - App Tier: Specifies the number of devices configured in the App tier (tier-2). Clicking this number displays the details of the devices configured in this tier.
   - Refresh: Retrieves latest data from the devices configured in the two-tier topology.
3. To view the application details, click the application name. Under Application > Details, you can view the following:
   - Under Flex Tier, view the IP address of the device configured in this tier. Also, view the endpoint configured. This is the public endpoint and specifies how users access an application. It receives all of the traffic from a client that pertains to a particular application. The endpoint is represented as IP:Port combination, for example, 6.6.6.13:443.
   - Under App Tier, view the IP address of the devices configured in this tier. Also, view the endpoints configured. These endpoints are accessed by the services configured on the NetScaler device in Flex tier. The endpoint is represented as IP:Port combination, for example, 1.1.1.132:80.

Monitoring Datacenter View

The Datacenter pane groups the discovered Citrix devices based on the location configured on these devices. For example, if you configure the Location value of a set of devices as Santa Clara, Command Center groups these devices within the Santa Clara group. Further if you change the Location value of a device, Command Center regroups the device on subsequent rediscovery of the device.

To monitor the datacenter view

1. On the Citrix Network tab, in the left pane, under Views , click Datacenter.
2. In the right pane, under Datacenter, you can view the location-based groups.

You can perform the following operations on the devices in these groups:

- Run Report: Run a custom report of any polled counters to troubleshoot or analyze the behavior of a device.
- Execute Task: Execute built-in and custom tasks to make configuration changes across devices.
- Config Audit : Run configuration audits on the devices to monitor configuration changes across managed devices and troubleshoot configuration errors.

To perform these operations, click the >>> icon next to a group, and then click the operation you want to run.

cc-citrix-network-mon-devices-con

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/command-center-50/cc-citrix-network-mon-devices-con.html

cc-citrix-network-view-dvc-props-tsk

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/command-center-50/cc-citrix-network-view-dvc-props-tsk.html

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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, select the devices on which you want to run a report, 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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, click >>> next to a device, and then click Events or Alarms.

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, under Citrix Network, click Complete View.
2. In the right pane, under Complete View, select the devices on which you want to execute a task, and then click Execute Task.

   Note: You can also execute a task on all devices in a map or pool. For more information, see Performing Operations on a Map.
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.

   Note: To execute a task on a single device, under **Complete View**, click >>> icon next to a device, and then click **Execute Task**.

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, under **Citrix Network**, click Device Inventory .
2. In the right pane, under Device Inventory, select the devices on which you want to run configuration audits, and then click Config Audit.

   Note: You can also run configuration audits on all devices in a map or pool. For more information, see Performing Operations on a Map.
3. Under Config Audit, in Audit Policy Name, click the name of the audit policy you want to execute to generate the audit report.

   Note: To add an audit policy, click the + (plus) sign next to the Audit Policy Name list.
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, under **Citrix Network**, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to a NetScaler device, select Utilities, 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 Access Gateway and NetScaler VPX devices).

To invoke the user interface of NetScaler devices

1. On the Citrix Network tab, in the left pane, under **Citrix Network**, click **Device Inventory**.

2. In the right pane, under Device Inventory, click the >>> icon next to a device, select Utilities, and then click **Invoke Configuration Utility**. The NetScaler user interface appears from where you can launch configuration utility, dashboard, monitoring, and reporting.

   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 Repeater Devices

You can launch the Citrix Repeater CLI for a selected Repeater device by using Command Center. From the CLI, you can configure and manage various features of the Citrix Repeater device.

To invoke the CLI of Repeater devices

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to the device whose CLI you want to launch, select Utilities, 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 Repeater device by using Command Center.

To invoke the user interface of Repeater devices

1. On the Citrix Network tab, in the left pane, under **Citrix Network**, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to the device whose configuration utility you want to launch, select Utilities, and then click Invoke 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, under **Citrix Network**, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to a device, select Utilities, 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 Repeater Device's Configuration to Other Repeater Devices

You can use Command Center to replicate the configuration of a Repeater device to multiple Repeater 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 Repeater devices. Command Center does not propagate node- or device-specific details, such as IP addresses.

To replicate configuration of a Repeater device

1. On the Citrix Network tab, in the left pane, under **Citrix Network**, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the Repeater 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. 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 >>> icon next to the device and click Show Configuration from the menu.

Viewing the Replication Status of Repeater Devices

You can view the status of a configuration that has been replicated from a Repeater device to one or more Repeater 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, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the Repeater 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 Repeater 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 Repeater Devices

You can view the running configuration of standalone and high availability (HA) primary Repeater devices.

To view the device configuration of Repeater devices

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, click >>> next to a device, and then click Show Configuration.

   Note: For an HA pair, click >>> next to the primary device, and then click Show Configuration.

Searching Devices from Device Inventory

You can search for any discovered NetScaler, NetScaler VPX, Access Gateway, Branch Repeater, Repeater, Branch Repeater VPX, NetScaler SDX, or Xen Server device on your Citrix network.

To search devices from Device Inventory

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.

2. Under Advanced Search, do one of the following:

   - To find devices that match any one of the search criteria that you specify, click Match any of the Following .

   - To find devices that match the full search criteria that you specify, click Match all of the Following.

3. Specify the criteria based on which you want to search the devices, and then click Search . The search results are displayed. You can select and save a group of devices from the search results as a map by clicking Save as Map icon.

Configuring the Location

The Citrix devices are configured with the location value during installation. However, you can use Command Center to modify the location of a device. The devices are grouped based on the location in the Datacenter view.

To configure location of devices

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the device for which you want to set the location, and then click Configure Location.
3. Under Configure Location, in Location, type the name of the location you want to specify.

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, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the device you want to restart, and then click Reboot.

   Note: For an HA pair, click >>> next to 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, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to the device you want to ping, select Utilities, and then click Ping.
3. Under Ping Response, 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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, click >>> next to a 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 Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the device for which you want to view the discovery status, and then click Status.

   Note: For an HA pair, click >>> next to the primary or secondary device, and then click 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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, select the devices that you want to set for rediscovery, and then click Rediscover.

   Note: To rediscover a single device, under Device Inventory, click >>> next to a device, and then click Rediscover.

Moving Devices to Another Map

You can move a discovered device from one map to another.

To move devices to a map

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the device you want to move, and then click Move To

   Note: For an HA pair, click >>> next to the HA pair, and then click Move To.
3. Under Move Device, in Destination Map, click the map to which you want to move the device to, and then click OK.

De-Provisioning NetScaler VPX on NetScaler SDX

Using Command Center you can de-provision the NetScaler VPX instances that are provisioned on NetScaler SDX.

To de-provision NetScaler VPX devices on a NetScaler SDX

1. On the Citrix Network tab, in the left pane, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click the >>> icon next to the NetScaler SDX device on which you want to de-provision the NetScaler VPX devices, 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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, select the devices that you want to delete, and then click Delete.

   Note: To delete a single device, under Device Inventory, click >>> next to the device you want to delete, 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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, select the devices that you want to unmanage, and then click Unmanage.

   Note: To unmanage a single device, under Device Inventory, click >>> next to the device you want to unmanage, 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.

In this section:

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, under Citrix Network, click Device Inventory.

2. In the right pane, under Device Inventory, click >>> next to the HA pair, and then click Force Failover.

3. Under Force Failover, click OK 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, under Citrix Network, click Device Inventory.
2. In the right pane, under Device Inventory, click >>> next to the secondary device, and then click Stay as Secondary.

Monitoring Your Network by Using the Home Page

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.
- **Device Inventory:** Summary of alarm status for each device category, such as NetScaler or Access 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.
- **Recent Alarms:** A list of the five most recent alarms with details, such as date or time, severity, category, source of alarm (system IP address), and description.

In this section:

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

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 (NS), NetScaler VPX (NS VPX), Access Gateway (AG), Repeater (R), and Branch Repeater (BR), NetScaler SDX (NS SDX), and XenServer (X). 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 Standalone or Primary.

- **Build Version:** Specifies the release version, build version, and date and time of the build.

- **Map Name:** Specifies the user-defined name of the map that contains 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.

Finding Devices

You can search for any discovered NetScaler or Repeater device on your Citrix network.

To find devices

1. On the Home tab, in Find Device, type the IP address of the device that you want to find, and then click GO.
2. If Command Center does not find the device that you are searching for, you can search for that device using specific criteria.

To find devices based on specific criteria

1. On the Home tab, click Advanced Search.
2. Under Advanced Search, do one of the following:
   - To find devices that match any one of the search criteria that you specify, click Match any of the Following.
   - To find devices that match the full search criteria that you specify, click Match all of the Following.
3. Specify the criteria based on which you want to search the devices, and then click Search.

Monitoring and Managing Events Generated on Citrix Devices

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:

For information about NetScaler SNMP OIDs, traps, and system health counters, see the Citrix NetScaler SNMP OID Reference at: http://support.citrix.com/article/CTX128676.

For information about NetScaler Syslog messages, see the Citrix NetScaler Log Message Reference at: http://support.citrix.com/article/CTX128679.

Monitoring SNMP Events and Alarms

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.

In this section:

For information about NetScaler SNMP OIDs, traps, and system health counters, see NetScaler SNMP OID Reference.

Viewing Events

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.
   - Message: 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 of the device that failed authentication.
   - Device Type: Specifies the type of the device, such as NetScaler or Repeater.

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, under 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, under SNMP, click Events.
2. In the right pane, under Events, select the check box next to the event for which you want to view the alarm, and then click View 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. In the right pane, under Events or Alarms, click Add View.
3. Under Add 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, Repeater, NetScaler VPX, and Branch Repeater 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 Repeater 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.

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 View.
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 View.

Searching Events and Alarms

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 .
3. Under Advanced Search, select the required options, and then click Search.

Managing SNMP Events and Alarms

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.

In this section:

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.
3. Under Alarm Properties - Assign Alarm, in Assign To, click 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.

Setting the Auto Refresh Interval for Events and Alarms

You can change the default interval for automatically refreshing the list of events in Command Center. By default, the events are polled every 10 seconds.

To set the auto refresh interval 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 Settings.
3. Under Settings, in Refresh Interval, type the number of seconds you want to set as the time interval for which Command Center must poll the events status, and then click OK.

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

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 right pane, under Events, click Event Severity.
3. Under Event Severity, click any of the tabs, and then under the Severity column, click the Configure Event Severity icon.
4. In Configure Event Severity, click the severity you want to assign, and then click OK.

Clearing and Deleting Alarms

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

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.

Monitoring Syslog Events

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 (M

   Example
   add audit syslogAction CC_action 10.102.29.70 -serverPort 514 -logLevel ALL -dateFormat MMDDYYYY -lo

   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

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.").

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 Complete View.
2. In the right pane, under Complete View, click Add View.
3. Under Add 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 the view name you want to modify.
2. In the right pane, click Modify View.
3. Under Modify 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 the view name you want to delete.
2. In the right pane, click Delete View.

Configuring Event and Alarm Triggers

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.

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 Event Triggers or Alarm Triggers.
3. Under Add Filter, in Name, type a filter name. The filter name is unique and user-defined.
4. In Status, select either Enable or Disable.
5. In Device Type, select the type of device, such as NetScaler and Repeater.
6. In Severity, select the severity level of the events for which you want to add the filter.
7. 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.
8. In Categories, click the icon next to the text box to select the categories of events generated by the managed devices.
9. In Failure Objects, either type the entity instances or counters for which an event 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 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 Alarm Age, type the time length (in seconds) after which you want to trigger the alarm action for an event. For example, an alarm action, such as sending an email notification, is performed only after an entity has been continuously down for the specified length of time.
12. Under Filter Action Details, 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, and Send Trap 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.

Monitoring and Managing the Real-Time Status of Entities Configured on NetScaler Devices

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.

In this section:

Monitoring Virtual Servers, Services, Servers, and Service Groups

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.

In this section:

Viewing the Status of Virtual Servers

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, 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 Services and Service Groups Bound to a Virtual Server

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, click Virtual Servers.
2. In the right pane, under Virtual Servers, in the Name column, click the name of the virtual server for which you want to view the bound services and service groups.
3. Under Virtual Servers > Details, do the following:
   - On the Services tab, view the status of the services bound to the virtual server. For more information about the status of services, see Viewing the Status of Services.
   - On the Service Groups tab, view the status of the service groups bound to the virtual server. For more information about the status of service groups, see Viewing the Status of Service Groups.

Viewing the Status of Services

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, 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

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, click Services.
2. In the right pane, under Services, in the Name column, click the name of the service for which you want to view the bound virtual servers.
3. On the Details page, view the status of the virtual servers to which the service is bound. For more information about the status of virtual servers, see Viewing the Status of Virtual Servers.

Viewing the Status of Service Groups

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, 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

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, click Service Groups.
2. In the right pane, under Service Groups, in the Name column, click the name of the service group for which you want to view the bound virtual servers.
3. Under Service Groups > Details page, view the status of the virtual servers to which the service group is bound. For more information about the status of the virtual server, see Viewing the Status of Virtual Servers.

Configuring Views

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.

In this section:

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, click Virtual Servers.
2. In the right pane, under Virtual Servers, click Add View.
3. Under Add 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 Device Names, select the device(s) and click the right arrow
6. In States, select the state(s) of the virtual server and click the right arrow.
7. In Protocols, select the protocols and click the right arrow.
8. In Health, choose the operator, and in the text box, type the health percentage, and then click OK.

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, click Services.
2. In the right pane, under Services, click Add View.
3. Under Add 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 Device Names, select the device(s) and click the right arrow.
6. In Protocols, select the protocol type(s) and click the right arrow.
7. In States, select the state(s) of the service(s) and click the right arrow.
8. In Last State Change, choose the operator, type the time period, and choose the time interval, and then click OK.

   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.

To add views for services

1. On the Monitoring tab, in the left pane, 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 Devices, click **+ Add** and select the device(s) from the list.
6. In Protocols, select the protocol type(s).
7. In States, select the state(s) of the service(s).
8. 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, click Service Groups.
2. In the right pane, under Service Groups, click Add View.
3. Under Add 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 Device Names, select the device(s) and click the right arrow.
6. In Protocols, select the protocol type(s) and click the right arrow.
7. In States, select the state(s) of the service and click the right arrow, and then click OK.

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, expand Virtual Servers, Services, or Service Groups, and click a view name.
2. In the right pane, click Modify View.
3. 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 views

1. On the Monitoring tab, in the left pane, expand Virtual Servers, Services, or Service Groups, and click a view name.
2. In the right pane, click Delete View, and then click OK on the confirmation message.

Managing the Real-Time Status of Entities

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).

In this section:

Configuring the Polling Interval

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, 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, and then 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.

Enabling or Disabling Virtual Servers

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, click Virtual Servers.
2. In the right pane, under Virtual Servers, select the check box for the virtual server(s) you want to enable or disable, and then 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

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.

To enable or disable services

1. On the Monitoring tab, in the left pane, 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 Services, in Annotation, type a message describing the reason why you are enabling or disabling the service.
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 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

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.

To enable or disable service groups

1. On the Monitoring tab, in the left pane, click Service Groups.
2. In the right pane, under Service Groups, select the check box for the service group(s) you want to enable or disable, and then click Enable or Disable.
3. Under Enable or Disable Services, in Annotation, type a message describing the reason why you are enabling or disabling the service group.
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 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

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, navigate to Virtual Servers, Services, Servers, or Service Groups >Audit Trails.
2. In the right pane, click Audit Trail.
3. Under Audit Trail, you can view the following:
   - Settings: Opens the Settings box for specifying how often you want Command Center to update the audit trail in seconds. By default, the refresh interval is set to 10 seconds.
   - Refresh: Refreshes the audit trail at the current time.
   - 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

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, click Virtual Servers, Services, or Service Groups.
2. In the right pane, under Virtual Servers, Services, or Service Groups, click Search.
3. Under Advanced Search, select the required options, and then click Search.

Polling the Status of Virtual Servers, Services, and Service Groups

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, click Virtual Servers, Services, or Service Groups.
2. In the right pane, under Virtual Servers, Services, or Service Groups, click Poll.

Customizing Columns

You can customize the columns displayed on the virtual server, service, and service group pages to display only those columns that you want to view. You can also customize columns in a custom view.

To customize columns

1. On the Monitoring tab, in the left pane, click Virtual Servers, Services, or Service Groups.
2. In the right pane, under Virtual Servers, Services, or Service Groups, click Customize Columns.
3. Under Customize Columns, in Available Columns, select the columns you want to monitor, click the right arrow, and then click OK.

Using Tasks to Configure Managed Devices

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 Repeater managed devices, Command Center uses the NetScaler and Repeater command-line interface (CLI) and the Secure Shell (SSH) and Secure File Transfer Protocol (SFTP) protocols. To view the status of the tasks executed, see the execution log that Command Center provides.

In this section:

cc-tasks-mng-builtin-con-sh

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/command-center-50/cc-tasks-mng-builtin-con-sh.html

Upgrading NetScaler with Built-in Tasks

The built-in upgrade tasks that you can execute on NetScaler devices are:

- **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.

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.

Upgrading Repeater with Built-in Tasks

The built-in upgrade task that you can execute on a Repeater device is:

- **Software Upgrade**: Use this task to upgrade one or more Repeater devices to a newer release of the Repeater software by specifying the path to the installation file of the software version to which you want to upgrade.

Configuring Repeater with Built-in Tasks

The built-in configuration tasks that you can execute on Repeater devices are:

- EnableRepeater: Enable traffic through Repeater devices.
- DisableRepeater: Disable traffic through Repeater devices.
- Configure Alert: Configure an alert (alert name and level) on Repeater devices.
- Configure Sys Log Server: Configure a new system log server for Repeater devices.
- Add User: Set up a new user account on selected devices and assign privileges.
- ConfigureBandwidth-5.xandearlier: Configure the bandwidth parameters of Repeater devices of version 5.x and earlier.
- ConfigureBandwidth-6.xandlater: Configure the bandwidth parameters of Repeater devices of version 6.x and later.
- RestoreConfig: Restore the configuration on a Repeater device from any configuration file.
- ConfigureRemoteLicenseServer: Configure multiple Branch Repeater 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 Branch Repeater VPX devices to use local licensing server.
- RestartRepeater: Restart the Repeater devices.
- SoftwareUpgrade: Software Upgrade for CloudBridge devices.
- AddUser: Add a new user and assign the privileges.

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 Access 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, do one or both of the following:
   - In Device Family, select the device type, such as All, NetScaler, and Repeater.
   - In Category, select the category, such as All, Software Upgrade, and General.

Executing Built-in Tasks

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 Execute next to the task you want to execute, and follow the wizard instructions.

Viewing the Execution Log for Specific Built-in Tasks

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 Execution Log next to the task whose execution details you want to view, 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.
   - Executed By: Specifies the NetScaler or Repeater 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

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, click Schedule next to the task you want to execute, and follow the wizard instructions.

Note: To view scheduled built-in tasks, in the right pane, under Built-in Tasks, on the top bar, click Scheduled Tasks. You can stop, resume, or remove a scheduled built-in task.

Exporting Built-in Tasks

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.

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 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

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
- Exporting Custom Tasks
- Modifying Custom Tasks
- Deleting Custom Tasks

Adding Custom Tasks

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: Executes a custom task on a set of devices sequentially. However, if a task execution fails on any device, it does not continue to the next device.

Execute on Inaccessible System(s): Executes a custom task on inaccessible devices in the following scenarios:

- If you configure a task to execute on inaccessible devices, and if the device list consists of both managed and inaccessible devices, the task is executed on all the devices in the device list.
- If you configure a task not to execute on inaccessible devices, and if the device list consists of both managed and inaccessible devices, the task is executed only on the managed devices.

Enable Role-Based Authorization (RBA): Ensures that only authorized users execute the tasks. 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.

Enable Automated Rollback (auto rollback): Generates rollback commands at runtime by fetching these commands based on the version of the operating system of the device. The auto rollback feature is supported only on Citrix NetScaler versions 8.1 and later. It is not supported on Repeater devices. This feature ensures that task execution behaves as a transaction such that if even one command execution within a task fails, the entire task is

rolled back. Auto rollback is an enhancement over the existing manual rollback mechanism where you need to manually type the rollback commands. This feature identifies the NetScaler version (both major and minor) and accordingly determines the appropriate command that must be used to reverse the configuration, if required.

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

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 Custom Task.
3. Under Custom Task Add Options, click Define new commands, and then click Next.
4. Under Add custom task, in Task Name, type the name of the task, and in Description, type the description of the task you want to create.
5. In Category, select the category of the task, or click + (plus) to add a new category.
6. In Device Family, select the type of device on which you want to execute the task. The NetScaler device family also includes Access Gateway Enterprise and NetScaler VPX device types. The Repeater device family includes both Repeater and Branch Repeater devices.
7. Specify the 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.
   - **Save configuration on success**: Specifies whether the custom task is saved implicitly by Command Center on the NetScaler and Repeater devices. If you select this option, you do not have to explicitly add the save config command when creating a custom task.
8. Click Add Command.
9. 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.
10. In Protocol, select the protocol you want to associate with the command.
11. 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.

12. Click OK.

13. In the Add custom task pane, click Add Task Variable.

14. In the Variable dialog box, specify the variable information, and then click OK.

Adding Custom Tasks from Command Files

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 Custom Task.
3. Under Custom Task Add Options, click Create Task from command file, and then click Browse.
4. In the Choose File dialog box, select the command file you want to use, click Open, and then click Next.
5. 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 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.
6. In the Add custom task pane, click Add Task Variable.
7. In the Variable dialog box, specify the variable information, and then click OK.

Adding Custom Tasks by Importing from Task Files

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 Custom Task.
3. Under Custom Task Add Options, click Import from task file, and then click Browse.
4. In the Choose File dialog box, select the task file you want to use, click Open, and then click Next.
5. 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.
6. In the Add custom task pane, click Add Task Variable.
7. In the Variable dialog box, specify the variable information, and then click OK.

Executing Custom Tasks

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, click Execute next to the custom task you want to execute, and follow the wizard instructions.

Viewing the Execution Log for Specific Custom Tasks

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, click Execution Log next to the custom task whose execution details you want to view, 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 Repeater 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

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, click Schedule next to the custom task you want to execute, and follow the prompts in the wizard.

Note: To view scheduled custom tasks, in the right pane, under Custom Tasks, on the top bar, click Scheduled Tasks. You can stop, resume, or remove a scheduled custom task.

Exporting Custom Tasks

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 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.

Modifying Custom Tasks

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 then in the Action column, click the Modify Task icon.
3. Under Modify custom task, make changes to the fields you want to modify, and then click OK.

Deleting Custom Tasks

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 in the Action column, click the Delete Task icon click **Delete**. Alternately, right-click the task, and click **Delete**..
3. In the confirmation message box, click **OK**.

Customizing Built-in and Custom Tasks

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.

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 then click Customize.
3. Under Customize Task, in 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 Repeater 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 $policyr
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.

Viewing the Execution Log for all Tasks

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 Name: Specifies the IP address of the device on which the task is performed.
   - Start Time: Specifies the time at which the task started.
   - Finish Time: Specifies the time at which the task completed.
   - Status: Specifies the status of the task execution - success or failure.
   - Settings: 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).
   - Refresh: To immediately refresh the execution log information displayed in this pane, click Refresh.

Monitoring and Managing SSL Certificates Configured on NetScaler Devices

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.

In this section:

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, under 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, Poll Now.

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, 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 Certificate Management, click 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, in the Generate CSR column, click Generate next to the certificate for which you want to generate the CSR.
3. Under CSR Output, 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 Certificate Management, in the Update column, click 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 Browse to select the path.
4. In Key File, either type the path of the key file or click Browse 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 Certificate Management, 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 Certificate Management, select the certificate you want to download, and then click Download.

3. Under Download, select Download key file also if you want to download the corresponding key file, and then click OK.

Auditing Configuration Changes Across NetScaler Devices

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.

In this section:

- Configuring Audit Templates
- Configuring Audit Policies
- Generating Audit Reports

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. For more information about audit policies, see Configuring Audit Policies.

After adding the audit templates, you can also modify and delete the audit templates.

In this section:

- Adding Audit Templates
- Modifying Audit Templates
- Deleting Audit Templates

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 Audit Template.
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, in the Action column, click the Modify Audit Template icon next to the audit template you want to modify.

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.

In this section:

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 Audit Policy .
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 Execute next to the audit policy you want to execute.
3. Under Execute Policy, select one of the following:
   - Devices: Select a device from Available Devices and click the right arrow.
   - Device Lists: Select a device list name from Device Lists. If you do not have a device list, click Add Device List 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, and click Schedule next to the audit policy you want to schedule.

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 Lists: Select a device list name. If you do not have a device list, click Add Device List 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.

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, in the Actions column, click Modify Audit Policy next to the audit policy you want to modify.
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 check boxes corresponding to 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.

In this section:

- Viewing Audit Reports

- Exporting Audit Reports

- Setting Auto Refresh Interval for 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 Reports.
2. Under 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).

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 Reports.
2. Under Reports, click the report name for which you want to monitor the configuration mismatches.
3. Under Device Level, click the IP address of the device for which you want to view the report.
4. On the report that appears, click Export, and in the File Save dialog box, click Save.

Setting Auto Refresh Interval for Audit Reports

You can set an interval for automatically updating the audit reports that you monitor. The default refresh interval for audit reports is 10 seconds.

To set the auto refresh interval for audit reports

1. On the Configuration tab, in the left pane, under Change Management, click Reports.
2. Under Reports, click Settings.
3. Under Settings, in Refresh Interval, type how often you want this information refreshed (in seconds), and then click OK.

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 Reports.
2. Under 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

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

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 Access Gateway) devices and more than 20 counters for Repeater and Branch Repeater 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 Repeater. 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 either Quick Report or Custom Reports.
2. In the right pane, click Configure Polled Counters.
3. In the Polled Counter Configuration window, select the NetScaler or **Repeater** 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 Access 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

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, 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 Access Gateway and NetScaler VPX device types. The Repeater device family includes both Repeater and Branch Repeater devices.

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 View, select the type of graph you want to view.

6. 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.

7. 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

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.

Repeater 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 Repeater devices. This number includes the number of TCP connections passing through the Repeater 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

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, click Custom Reports.
2. In the right pane, under Custom Reports, click Add Custom Report.
3. Follow the steps in the wizard, and then click Finish. The custom report is listed under Custom Reports.

Viewing Custom Reports

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, click Custom Reports.
2. In the right pane, under Custom Reports, click View Graph next to the report you want to view.
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 Schedule Report next to the report you want to 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.
7. Click **OK**.

Modifying Custom Reports

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, click Custom Reports.
2. In the right pane, under Custom Reports, in the Actions column, click the Modify Custom Report icon next to the custom report you want to modify.
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, click Custom Reports.
2. In the right pane, under Custom Reports, in the Actions column, click the Delete Custom Report icon next to the custom report you want to delete.

Configuring Thresholds to Monitor Devices

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, click Thresholds.
2. In the right pane, under Thresholds, click Add Threshold.
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 Access Gateway and NetScaler VPX device types. The Repeater device family includes both Repeater and Branch Repeater devices.

     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

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, click Thresholds.
2. In the right pane, under Thresholds, in the Threshold Name column, click the threshold name that you want to modify.
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, click Thresholds.
2. In the right pane, under Thresholds, in the Actions column, click the Delete Threshold icon for the threshold that you want to delete.

Monitoring AppFirewall Syslog Events

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.

In this section:

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 View Graph next to each built-in report 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 Schedule Report next to each built-in 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.

In this Section:

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, click Recent Logs.
2. In the right pane, under Recent Logs, click Add View.
3. Under Add View, fill the following details.
   - Name: The user-defined view name. Type a name for the AppFirewall log view.
   - Source: 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.
2. Under Recent Logs, click the view name you want to modify.
3. In the right pane, click Modify View.
4. Under Modify View, modify the values you want to change, and then click OK.

Searching Recent AppFirewall Log Messages

Use the Search and Advanced 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 based on message string

1. On the Reporting tab, in the left pane, under AppFirewall, click Recent Logs.
2. In the right pane, under Recent Logs, 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.

To search for log messages based on specific criteria

1. On the Reporting tab, in the left pane, under AppFirewall, click Recent Logs.
2. In the right pane, under Recent Logs, click Advanced Search.
3. Under Advanced Search, specify the criteria based on which you want to search the devices. You can specify multiple comma-delimited search strings to search Syslog messages generated for selected criteria.
4. Click Search.

Administering Command Center

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:

- CloudBridge Registration

Configuring Discovery Settings

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 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

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, Repeater, NetScaler SDX and XenServer. These device profiles are used by Command Center to discover the Citrix devices.

In this section:

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 Administration tab, under Settings, click Device Profiles.
2. Under Device Profiles, click Add Profile.
3. Under Add 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, Repeater, NetScaler SDX, and XenServer.
5. Do one of the following:
   - For the NetScaler device family, perform the following steps.

     Note: NetScaler device family also includes NetScaler VPX virtual devices, and Access Gateway devices.

     a. Under User Credentials, 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.

     b. 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.

     c. 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 , perform the following steps.
  a. Create a NetScaler profile by following the procedure described above for adding device profile for NetScaler device family.
  b. 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`.
  c. In Select 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 the **Repeater** device family, perform the following steps.

  Note: The Repeater device family includes both Repeater and Branch Repeater devices.

  a. 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 Repeater 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.
  b. 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 Repeater 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.

  a. Create a NetScaler profile by following the procedure described above for adding device profile for NetScaler device family. .

  b. 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.

  c. 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 Administration tab, in the right pane, under Settings, 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, Repeater, and XenServer.
   - Description: Specifies the description of the profile you have created.
   - Add Profile: Click Add Profile to add new device profiles. For more information, see Adding Device Profiles.
   - Delete: Click Delete to delete a device profile. For more information, see Deleting Device Profiles.

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 Administrationtab, in the right pane, under Settings, click Device Profiles.
2. Under Device Profiles, click the profile name you want to modify, and then click Modify....
3. Under Modify 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 Administration tab, in the right pane, under Settings, click Device Profiles.
2. Under Device Profiles, select the check boxes next to the profile names you want to delete, and then click Delete.

Configuring Server Settings

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.

To configure server settings

1. On the Administration tab, in the right pane, under Settings, click Server Settings.
2. Under 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.
   - Under Performance Data Configuration, 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.

Configuring Inventory Settings

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 every rediscovery.
- During specific intervals set by the user.

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. Under Inventory Settings, in What to archive, select SSL Certificates if you want to archive the SSL certificates in addition to the configuration and license files.
3. Under When to archive configuration files, select one or more of the following options for archiving.
    - On every rediscovery: Clear this check box if you do not want the files to be downloaded during rediscovery. By default, all files are downloaded and stored during every rediscovery.
    - On receiving "save config" SNMP trap from managed devices: Select this check box if you want the server to archive files when the "save config" trap is received.
    - At regular interval: Select this if you want the server to archive files at specific intervals.
    - Archive Interval (in minutes): Specify the archive interval in minutes.
4. In Number of previous archive files to retain, type the number of files that you want to retain after download.
5. Click OK.

Configuring High Availability Settings

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

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 Mail Server Settings.
2. Under Mail Server Settings, in Server Name / IP Address, 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.

Configuring Access Settings

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 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 *Citrix Command Center 5.0 User's Guide*.

   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

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 the "Installing Command Center" chapter in the *Citrix Command Center 5.0 Installation Guide*. 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, under Settings, click Agent Setup.
2. Under Agent Details, you can view and do the following.
   - Agent: 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 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.

Installing Certificates for Secure Communication

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.

It is assumed that you already have the certificate you want to install. If you do not have a certificate, see the section "Generating a New Certificate and Key" in the *Citrix NetScaler Traffic Management Guide* at: http://support.citrix.com/article/CTX128670.

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 Settings, 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.

Configuring SNMP Trap Forwarding

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:

    a. Trap Destination: Specify the IP address of the device that receives the forwarded SNMP trap.

    b. Destination Port: Specify the port number of the device that receives the forwarded SNMP trap.

    c. Trap Community: Specify the group to which the device belongs.
3. Click OK.

Configuring Security Settings

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:

Configuring Authentication Settings

Command Center supports authentication policies for external authentication of users.

When users, who are not configured in Command Center, log on for the first time, those users are assigned to the default Users group. Administrators must assign those users to appropriate groups, depending on the privilege levels that they want to grant those users.

The administrator must configure authentication servers to authenticate the users who are not configured in Command Center.

Command Center supports the following authentication servers:

- Local
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)
- Active Directory

  If you are using Active Directory server for authentication, groups in the Command Center 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 group in the Command Center.

To configure authentication settings

1. On the Administration tab, under Security, click Authentication Settings.
2. Under Authentication Settings, in Authentication Server, select the type of authentication server you want to use: Local, Active Directory, RADIUS, or TACACS+.
3. Depending on the authentication server you have selected, type or select the details. If you selected Active Directory, you can, in addition, use the Enable Group Extraction option to apply Active Directory authorization settings to groups configured in Command Center. Under Enable Group Extraction, type or select the Active Directory Server settings. User authorization is then is then based on the groups with which the users are associated in Command Center.

   Note: After you specify Active Directory Admin username and password, you can click the Retrieve Attributes icon to retrieve additional group attribute details automatically.
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 Group.
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. Under Delegated Administration, 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 **Assign To**.
3. Under Modify Group profile, under Members, click Assign User.
4. Under Assign Users, in Available Users, click the user(s) that you want to include in the group, and then click the right arrow.

Note: To remove a selected user, click the user you want to remove in Enrolled Users, and then click the left arrow.

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, under Modify Group profile, under Members, click Assign User.
4. To change the permissions assigned to a group, under Delegated Administration, 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.

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+.

In this section:

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 User.
3. In User name, type a user name for the new user and in Password and Re-type Password, type a password for the user name.
4. In Available group names, select the groups to which you want to add the new user.

   Note: To add the new user account to a new group, select the Add this user to a new group check box and type the name of the group.
5. Select the Password expires in check box and 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. Select the Account expires in check box and type the number of days after which you want the account to expire.
7. Set the authentication type for the user. For local authentication, select Local Authentication User check box. For external authentication, make sure that the check box is not selected.

   Note: The external authentication type is supported only when you set up one of the authentication servers: Radius, Active Directory or TACACS+.
8. Click OK. 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 **Assign To**.
3. Under Modify User profile, expand Associated Groups, and then click Configure Group.
4. Under Modify profile, in Available groups, click the groups that you want to associate with the user, and then click the right arrow.

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 **Assign To**.
3. Under Modify User profile, expand Permitted Operations to view the list of operations.

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 Edit User icon next to the user name you want to modify.
3. Under Modify User profile, make changes as required. To modify the authentication type of the user, select or clear the Local Authentication User check box. Clearing the check box specifies external authentication.

   Note: Alternately, you can modify the authentication type for a user from the User page under Administration tab. Select one or more users by selecting the check box next to the user, and then select the authentication type from the Authentication Type menu. Additionally 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.

To change the root user password

1. On the Administration tab, under Security, click Users.
2. Under Users, click the Edit User icon next to the root user name.
3. Under Modify User profile - root, 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 Delete User icon next to the user name you want to delete.

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 Name: 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.
    - Audit 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.
    - Clear Audit: Select the check box next to the audit log you want to clear, and then click Clear Audit if you want to clear the audit logs of a user.
    - Search: Click Search if you want to search for a specific audit log based on one of the following criteria: Audit Time, Category, User Name, Operation, AuditedObject, and Status.
    - Export: Click Export if you want to export all the audited information to a CSV file.

Configuring Logs

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.

In this section:

Generating Support Logs

Command Center lets you generate support archive logs for analysis.

To generate support logs

1. On the Administration tab, in the right pane, under Operations, click Generate support logs.
2. Under Generate support logs, 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: Specifies the name of the log file. Click a file name to view the log details.
   - Last modified: Specifies the date and time when the log file was last modified.
   - Size: Specifies the size of a log file.

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.

Viewing Server Details, Logged-in User Information, and License Details

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 right 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.
3. Under Port Details, you can view information, such as the TCP and SNMP ports.

To view logged-in user information

1. On the Administration tab, in the right 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 right 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

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 Operations, 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.

Shutting Down the Command Center Server

You can shut down the Command Center server from the client.

To shut down the Command Center server

1. On the Administration tab, in the right pane, under Operations, click Shutdown.
2. Under Shutdown, click OK to shut down the server.

NetScaler SNMP Counters Polled from Command Center

Command Center polls SNMP counters in Citrix NetScaler devices to gather performance data. You can use Command Center to generate graphs or charts of counters that have values in count, number, bytes, kilobytes, and megabits. However, you cannot generate graphs or charts of counters with enum and string values.

In this section:

- Simple ACL Counters
- SSL Counters
- Service Groups Counters
- Services Counters
- Sure Connect Counters
- System Disk Counters
- TCP Counters
- UDP Counters
- VLAN Counters
- Virtual Servers Counters
- Virtual Services Counters
- VPN Counters

For information about NetScaler SNMP OIDs, traps, and system health counters, see NetScaler SNMP OID Reference.

AAA Counters

The following table gives you a basic overview of the Authentication, Authorization, and Accounting (AAA) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
AAA sessions	AAA sessions established on the appliance.	N	Count	Y	Y	Y	Y	Y
Authentication failures	Unsuccessful authentication requests, for all authentication methods.	N	Count	Y	Y	Y	Y	Y
Authentication success ratio	Ratio of successful authentication requests to total requests, for all authentication methods.	N	Number	Y	Y	Y	Y	Y
Authentication successes	Successful authentication requests, for all authentication methods.	N	Count	Y	Y	Y	Y	Y
Current AAA sessions	AAA sessions currently active on the appliance.	N	Count	Y	Y	Y	Y	Y
HTTP authorization success ratio	Ratio of successful HTTP authorization requests to total HTTP requests.	N	Number	Y	Y	Y	Y	Y

HTTP authorization failures	Unsuccessful authorization requests for HTTP resources, such as web servers. When a user tries to access any resource through the VPN, the appliance checks to verify that the user is authorized to access that resource.	N	Count	Y	Y	Y	Y	Y
HTTP authorization successes	Successful authorization requests for HTTP resources, such as Web servers. When a user tries to access any resource through the VPN, the appliance checks to verify that the user is authorized to access that resource.	N	Count	Y	Y	Y	Y	Y
Non HTTP authorization failures	Unsuccessful authorization requests for non-HTTP resources, such as telnet or SSH. When a user tries to access any resource over the VPN, the appliance checks to verify that the user is authorized to access the resource.	N	Count	Y	Y	Y	Y	Y

Non HTTP authorization successes	Successful authorization requests for non-HTTP resources, such as telnet or SSH. When a user tries to access any resource over the VPN, the appliance checks to verify that the user is authorized to access the resource.	N	Count	Y	Y	Y	Y	Y
Non HTTP authorization success ratio	Ratio of successful non HTTP authorization requests to total non HTTP requests.	N	Number	Y	Y	Y	Y	Y
Timed out AAA sessions	AAA sessions that were timed out on the appliance.	N	Count	Y	Y	Y	Y	Y

ACL Counters

The following table gives you a basic overview of the Access Control List (ACL) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Allow ACL Hits	Packets matching ACLs with processing mode set to ALLOW. NetScaler processes these packets.	Y	Count	Y	Y	Y	Y	Y
Deny ACL Hits	Packets dropped because they match ACLs with processing mode set to DENY.	Y	Count	Y	Y	Y	Y	Y
Bridge ACL Hits	Packets matching a bridge ACL, which in transparent mode bypasses service processing.	Y	Count	Y	Y	Y	Y	Y

ACL Table Counters

The following table gives you a basic overview of the ACL Table counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter Name	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
ACL Hits	Number of times the ACL was hit.	N	Count	Y	Y	Y	Y	Y
ACL Priority	The priority of the ACL.	N	Enum	Y	Y	Y	Y	Y

ACL6 Counters

The following table gives you a basic overview of the ACL6 counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
ACL6 Hits	Packets matching an IPv6 ACL	N	Count	Y	Y	Y	Y	Y
ACL6 Misses	Packets not matching any IPv6 ACL.	N	Count	Y	Y	Y	Y	Y
Allow ACL6 hits	Packets matching IPv6 ACLs with processing mode set to ALLOW. NetScaler processes these packets.	N	Count	Y	Y	Y	Y	Y
Bridge ACL6 hits	Packets matching a bridge IPv6 ACL, which in transparent mode bypasses service processing.	N	Count	Y	Y	Y	Y	Y
Deny ACL6 hits	Packets dropped because they match IPv6 ACLs with processing mode set to DENY.	N	Count	Y	Y	Y	Y	Y
NAT ACL6 hits	Packets matching a NAT ACL6, resulting in a NAT session.	N	Count	Y	Y	Y	Y	Y

ACL6 Table Counters

The following table gives you a basic overview of the ACL6 Table counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter Name	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
ACL6 Hits	Number of times an ACL6 counter was hit.	N	Count	Y	Y	Y	Y	Y
ACL6 Priority	Priority of the ACL6.	N	Enum	Y	Y	Y	Y	Y

Application Firewall Counters

The following table gives you a basic overview of the App Firewall counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.2	9.3
Buffer Overflow Violations	Number of buffer overflow violations seen by the Application Firewall. When an inappropriate amount or type of data in the URL or designated HTTP headers is sent, a violation occurs.	N	Count	Y	Y	Y	Y	Y	Y
Cookie Violations	Number of cookie consistency violations seen by the Application Firewall. When cookies set by the server are modified on the client, a violation occurs.	N	Count	Y	Y	Y	Y	Y	Y
Credit Card Violations	The number of credit card violations seen by the Application Firewall.	N	Count	Y	Y	Y	Y	Y	Y
Cross-site Scripting Violations	Number of HTML cross-site scripting (XSS) violations seen by the Application Firewall.	N	Count	Y	Y	Y	Y	Y	Y

Deny URL Violations	Number of deny URL violations seen by the Application Firewall. When an attempt is made to access any URL on the Deny URL list, a violation occurs.	N	Count	Y	Y	Y	Y	Y	Y
Field Consistency Violations	The number of field consistency violations seen by the Application Firewall.	N	Count	Y	Y	Y	Y	Y	Y
Requests Aborted	Number of requests aborted by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y
Requests Received	Number of requests received by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y
Requests Redirected (HTTP 302)	Number of requests redirected by the application firewall (HTTP 302).	N	Count	Y	Y	Y	Y	Y	Y
Responses Handled	Number of responses handled by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y
SQL Violations	Number of HTML SQL injection violations seen by the Application Firewall.	N	Count	Y	Y	Y	Y	Y	Y
Safe Object Violations	Number of safe object violations seen by the Application Firewall.	N	Count	Y	Y	Y	Y	Y	Y

Start URL Violations	Number of start URL violations seen by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y
Total Number of Violations	Number of violations seen by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y
Field Format Violations	Number of field format violations seen by the application firewall.	N	Count	Y	Y	Y	Y	Y	Y

Cache Redirection Policies Counters

The following table gives you a basic overview of the Cache Redirection Policies counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Policy Hits	This represents the name of the policy bound to cache redirection vserver.	N	Count	Y	Y	Y	Y	Y
Policy Name	This represents the hits on the cache redirection policy.	N	String	Y	Y	Y	Y	Y

Compression Counters

The following table gives you a basic overview of the Compression counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Compressed packets transmitted	Number of HTTP packets that the Citrix NetScaler system sends to the client after compressing the response from the server.	Y	Count	Y	Y	Y	Y	Y
Compressible bytes received	Number of bytes that can be compressed, which the Citrix NetScaler system receives from the server. This gives the content length of the response that the system receives from server.	Y	Count	Y	Y	Y	Y	Y
Compressible packets received	Number of HTTP packets that can be compressed, which the Citrix NetScaler system receives from the server.	Y	Count	Y	Y	Y	Y	Y
HTTP bytes compressed	Total HTTP bytes compressed by NetScaler.	Y	Bytes	Y	Y	Y	Y	Y
HTTP compression ratio	HTTP compression ratio expressed as percentage.	Y	Count	Y	Y	Y	Y	Y

HTTP compression requests	Number of HTTP compression requests the Citrix NetScaler system receives for which the response is successfully compressed. For example, after you enable compression and configure services, if you send requests to the system with the following header information: “Accept-Encoding: gzip, deflate”, and NetScaler compresses the corresponding response, this counter is incremented.	Y	Count	Y	Y	Y	Y	Y
HTTP compression success ratio	Ratio of the compressible data received from the server to the compressed data sent to the client. This is expressed as a percentage value.	Y	Count	Y	Y	Y	Y	Y

Content Filters Counters

The following table gives you a basic overview of the Content Filters+ counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Hits	Total number of hits on the content filter policy.	N	Count	N	N	N	N	N

Content Switch Policies Counters

The following table gives you a basic overview of the Content Switch Policies counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Content switch policy hits	Total number of hits on the content switch policy.	N	Count	Y	Y	Y	Y	Y
Destination VServer Name	This represents the name of the destination vserver to which the request has to be directed to if the content switching policy evaluates to true.	N	String	Y	Y	Y	Y	Y
Policy Name	This represents the name of the policy bound to content switching vserver.	N	String	Y	Y	Y	Y	Y

CPU Usage Counters

The following table gives you a basic overview of the CPU usage counter including details such as its description, the default poll status on Command Center, interpretation of counter values, and its availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
CPU Usage (Percentage)	The CPU utilization calculated as the percentage of the total CPU capacity. This counter is used for multi-processor systems. If there are dual CPUs on a system, the counter is polled for two instances of the CPU: CPU0 and CPU1.	Y	Number	Y	Y	Y	Y	Y

DNS Counters

The following table gives you a basic overview of the Domain Name Server (DNS) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Address record query	Total number of A queries received.	Y	Count	Y	Y	Y	Y	Y
CNAME record query	Total number of CNAME queries received.	Y	Count	Y	Y	Y	Y	Y
DNS queries	Total number of DNS queries received.	Y	Count	Y	Y	Y	Y	Y
DNS requests refused	Number of DNS requests refused.	Y	Count	Y	Y	Y	Y	Y
DNS responses	Total number of DNS responses received.	Y	Count	Y	Y	Y	Y	Y
Mail Exchanger Record	Total number of MX records.	Y	Count	Y	Y	Y	Y	Y
NS record query	Total number of NS records.	Y	Count	Y	Y	Y	Y	Y
Other errors	Total number of other errors.	Y	Count	Y	Y	Y	Y	Y
Queries authoritatively answered	Number of queries, which were authoritatively answered.	Y	Count	Y	Y	Y	Y	Y
Queries which were authoritatively answered with no data	Number of queries, which were authoritatively answered with no data.	Y	Count	Y	Y	Y	Y	Y
Queries which were non-authoritatively answered	Number of queries that were non-authoritatively answered.	Y	Count	Y	Y	Y	Y	Y
Queries which were non-authoritatively answered with no data	Number of queries that were non-authoritatively answered with no data.	Y	Count	Y	Y	Y	Y	Y

SOA record query	Total number of SOA record queries received.	Y	Count	Y	Y	Y	Y	Y
Unparseable requests received	Total number of requests for which query type requested was unsupported.	Y	Count	Y	Y	Y	Y	Y
Unsupported record type	Total number of responses for which response type requested was unsupported.	Y	Count	Y	Y	Y		
`authoritative no such name' responses	Number of queries for which no record was found.	Y	Count	Y	Y	Y		

GSLB Counters

The following table gives you a basic overview of the Global Server Load Balancing (GSLB) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Custom Entries	Number of custom locations.	N	Count	Y	Y	Y	Y	Y
Static Entries	Number of static locations.	N	Count	Y	Y	Y	Y	Y

HTTP Counters

The following table gives you a basic overview of the HTTP counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

nter	Description	Default Poll	Values	8.1	9.0	9.1
nked uests	HTTP requests in which the Transfer-Encoding field of the HTTP header has been set to chunked.	Y	Count	Y	Y	Y
nked onses	HTTP responses sent in which the Transfer-Encoding field of the HTTP header has been set to chunked. This setting is used when the server wants to start sending the response before knowing its total length. The server breaks the response into chunks and sends them in sequence, inserting the length of each chunk before the actual data. The message ends with a chunk of size zero.	Y	Count	Y	Y	Y
tent length uests	HTTP requests in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.	Y	Count	Y	Y	Y
tent length onses	HTTP responses sent in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.	Y	Count	Y	Y	Y
P GET uests eived	HTTP requests received using the GET method.	Y	Count	Y	Y	Y
P POST uests eived	HTTP requests received using the POST method.	Y	Count	Y	Y	Y
P request es received	Bytes of HTTP data received.	Y	Bytes	Y	Y	Y
P response es received	Bytes received as response data.	Y	Bytes	Y	Y	Y
P responses eived	Number of HTTP responses received from servers.	Y	Count	Y	Y	Y
P/1.0 uests eived	Number of HTTP/1.0 requests received from servers.	Y	Count	Y	Y	Y
P/1.0 onses eived	Number of HTTP/1.0 responses received from servers.	Y	Count	Y	Y	Y
P/1.1 eline requests	Number of HTTP/1.1 pipeline requests received.	Y	Count	Y	Y	Y
mplete HTTP ders	HTTP requests and responses received in which the HTTP header spans more than one packet.	Y	Count	Y	Y	Y

omplete uest headers	HTTP requests received in which the header spans more than one packet.	Y	Count	Y	Y	Y
omplete ponse headers	HTTP responses received in which the header spans more than one packet.	Y	Count	Y	Y	Y
ge/invalid nk requests	Large or invalid requests received in which the Transfer-Encoding field of the HTTP header has been set to chunked.	Y	Count	Y	Y	Y
ge/invalid uests	Large or invalid requests and responses received.	Y	Count	Y	Y	Y
e than tent length a	Number of large/invalid content-length requests/responses received.	Y	Count	Y	Y	Y
-GET/POST hods eived	Number of non-GET/POST HTTP methods received.	Y	Count	Y	Y	Y
uest bytes nsmitted	Bytes of HTTP data transmitted.	Y	Bytes	Y	Y	Y
ponse bytes nsmitted	Bytes transmitted as response data.	Y	Bytes	Y	Y	Y
ver BUSY ponses (500)	Error responses received. Some of the error responses are: · 500 Internal Server Error · 501 Not Implemented · 502 Bad Gateway · 503 Service Unavailable · 504 Gateway Timeout · 505 HTTP Version Not Supported	Y	Count	Y	Y	Y

ICMP Counters

The following table gives you a basic overview of the Internet Control Message Protocol (ICMP) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
ICMP bytes received	Bytes of ICMP data received.	Y	Bytes	Y	Y	Y	Y	Y
ICMP bytes transmitted	Total number of ICMP bytes transmitted by NetScaler.	Y	Bytes	Y	Y	Y	Y	Y
ICMP echo replies received	ICMP Ping echo replies received.	Y	Count	Y	Y	Y	Y	Y
ICMP echo replies transmitted	ICMP Ping echo replies transmitted.	Y	Count	Y	Y	Y	Y	Y
ICMP echos received	ICMP Ping Echo Request and Echo Reply packets received.	Y	Count	Y	Y	Y	Y	Y
ICMP packets dropped	ICMP packets dropped because the rate threshold has been exceeded.	Y	Count	Y	Y	Y	Y	Y
ICMP packets received	Total number of ICMP packets received by NetScaler.	Y	Count	Y	Y	Y	Y	Y
ICMP packets transmitted	Total number of ICMP packets transmitted by NetScaler.	Y	Count	Y	Y	Y	Y	Y
ICMP rate threshold	The value set for the ICMP rate threshold.	Y	Number	Y	Y	Y	Y	Y

ICMP rate threshold exceeded	Times the ICMP rate threshold is exceeded. If this counter continuously increases, first make sure the ICMP packets received are genuine. If they are, increase the current rate threshold.	Y	Count	Y	Y	Y	Y	Y

Integrated Cache Counters

The following table gives you a basic overview of the Integrated Cache counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.1
304 hit ratio (Percentage)	304 responses as a percentage of all responses that the NetScaler served.	Y	Number	Y	Y	Y	Y	Y
304 hits	Total number of 304 Not Modified responses served from the cache.	Y	Count	Y	Y	Y	Y	Y
Byte hit ratio (Percentage)	Bytes served from the cache divided by total bytes served to the client. If compression is On in the NetScaler, this ratio may not reflect the bytes served by the compression module. If the compression is Off this ratio is the same as cachePercentOriginBandwidthSaved.	Y	Number	Y	Y	Y	Y	Y
Bytes served by NetScaler	Total bytes served from cache.	Y	Bytes	Y	Y	Y	Y	Y
Bytes served by cache	Bytes served from cache.	Y	Bytes	Y	Y	Y	Y	Y
Cached objects	Responses currently stored in integrated cache. Includes responses fully downloaded, in the process of being downloaded, and expired or flushed but not yet removed.	Y	Count	Y	Y	Y	Y	Y
Compressed bytes from cache	Bytes of compressed data served from the cache.	Y	Bytes	Y	Y	Y	Y	Y
Conversions to conditional req	Number of user-agent requests for a cached Poll Every Time (PET) response that were sent to the origin server as conditional requests.	Y	Count	Y	Y	Y	Y	Y
Expire at last byte	Instances of content expiring immediately after receiving the last body byte due to the Expire at Last Byte setting for the content group.	Y	Count	Y	Y	Y	Y	Y
Flashcache hits	Instances of requests to a content group with flash cache enabled where the response was found and served.	Y	Count	Y	Y	Y	Y	Y

Flashcache misses	Number of requests to a content group with flash cache enabled that were cache misses. Flash cache distributes a response to all clients in a queue.	Y	Count	Y	Y	Y	Y	Y
Full inval requests	Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.	Y	Count	Y	Y	Y	Y	Y
Hit ratio(Percentage)	Cache hits as percentage of the total number of requests.	Y	Number	Y	Y	Y	Y	Y
Hits	Responses served from the integrated cache. These responses match a policy with a CACHE action.	Y	Count	Y	Y	Y	Y	Y
Hits being served	This number should be close to the number of hits being served currently.	Y	Count	Y	Y	Y	Y	Y
Inval requests	Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.	Y	Count	Y	Y	Y	Y	Y
Largest response so far (B)	Size, in bytes, of largest response sent to client from the cache or the origin server.	Y	Size in bytes	Y	Y	Y	Y	Y
Maximum memory (KB)	Largest amount of memory the NetScaler can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.	Y	Size in kilobytes	Y	Y	Y	Y	Y
Memory allocation failures	Total number of times the cache failed to allocate memory to store responses.	Y	Count	Y	Y	Y	Y	Y
Misses	Total number of misses to the server.	Y	Count	Y	Y	Y	Y	Y
Misses being handled	Cache misses processed.	Y	Count	Y	Y	Y	Y	Y
Non-304 hits	Full (non-304) responses served from the cache.	Y	Count	Y	Y	Y	Y	Y
Non-storable misses	Cache misses for which the fetched response is not stored in the cache. These responses match policies with a NOCACHE action or are affected by Poll Every Time.	Y	Count	Y	Y	Y	Y	Y
Origin bandwidth saved (Percentage)	Bytes served from cache divided by total bytes served to client.	Y	Number	Y	Y	Y	Y	Y
Parameterized 304 hit ratio (Percentage)	Parameterized 304 hits as a percentage of all cache hits.	Y	Number	Y	Y	Y	Y	Y
Parameterized 304 hits	Parameterized requests resulting in an object not updated (status code 304) response.	Y	Count	Y	Y	Y	Y	Y

Parameterized inval requests	Total number of requests which performed parameterized invalidation. Parameterized invalidation happens when the INVAL policy has the invalObjects parameter specified.	Y	Count	Y	Y	Y	Y	Y
Parameterized non-304 hits	Parameterized requests resulting in a full response (not status code 304: Object Not Updated) served from the cache.	Y	Count	Y	Y	Y	Y	Y
Parameterized requests	Parameterized requests received.	Y	Count	Y	Y	Y	Y	Y
Poll every time hit ratio(Percentage)	Percentage of cache hits in content groups that have Poll Every Time enabled, relative to all searches of content groups with Poll Every Time enabled.	Y	Number	Y	Y	Y	Y	Y
Poll every time hits	Number of times a cache hit was found during a search of a content group that has Poll Every Time enabled.	Y	Count	Y	Y	Y	Y	Y
Poll every time requests	Requests that triggered a search of a content group that has Poll Every Time (PET) enabled (always consult the origin server before serving cached data).	Y	Count	Y	Y	Y	Y	Y
Recent 304 hit ratio (Percentage)	Recently recorded ratio of 304 hits to all hits expressed as percentage.	Y	Number	Y	Y	Y	Y	Y
Recent byte hit ratio (Percentage)	Cache byte hit ratio expressed as percentage. Byte hit ratio is defined as (number of bytes served from the cache)/(total number of bytes served to the client). If compression (CMP) is turned ON in NetScaler, this ratio is not meaningful. This ratio might underestimate or overestimate the origin-to-cache bandwidth saving (depending upon whether bytes served by CMP in NetScaler are more or less than compressed bytes served from the cache). If CMP is turned OFF in NetScaler, this ratio is the same as cachePercentOriginBandwidthSaved.	Y	Number	Y	Y	Y	Y	Y

Recent hit ratio (Percentage)	Cache byte hit ratio expressed as percentage. Byte hit ratio is defined as (number of bytes served from the cache)/(total number of bytes served to the client). If compression (CMP) is turned ON in NetScaler, this ratio is not meaningful. This ratio might underestimate or overestimate the origin-to-cache bandwidth saving (depending upon whether bytes served by CMP in NetScaler are more or less than compressed bytes served from the cache). If CMP is turned OFF in NetScaler, this ratio is the same as cachePercentOriginBandwidthSaved.	Y	Number	Y	Y	Y	Y	Y
Recent origin bandwidth saved (Percentage)	Recently recorded cache byte hit ratio expressed as percentage. Byte hit ratio is defined as (number of extra bytes that would have been served by the origin)/(total number of bytes served to the client). This definition shows the benefits of integrated compression. The byte hit ratio can be greater than 1 because of integrated compression. The assumption is that all the compression has been done in NetScaler.	Y	Number	Y	Y	Y	Y	Y
Recent parameterized 304 hit ratio (Percentage)	Recently recorded ratio of parameterized 304 hits to all parameterized hits expressed as a percentage.	Y	Number	Y	Y	Y	Y	Y
Recent storable miss ratio (Percentage)	Recent recorded ratio of misses where the response was considered cacheable expressed as a percentage.	Y	Number	Y	Y	Y	Y	Y
Recent successful reval ratio (Percentage)	Percentage of times stored content was successfully revalidated by a 304 response rather than by a full response.	Y	Number	Y	Y	Y	Y	Y
Requests	Total requests. (= Total hits + Total misses).	Y	Count	Y	Y	Y	Y	Y
Revalidations	Responses that an intervening cache revalidated with the integrated cache before serving, as determined by a Cache-Control: Max-Age header configurable in the integrated cache.	Y	Count	Y	Y	Y	Y	Y
Storable miss ratio (Percentage)	Responses that were fetched from the origin and stored in the cache, as a percentage of all cache misses.	Y	Number	Y	Y	Y	Y	Y

Storable misses	Responses that were fetched from the origin, stored in the cache, and then served to the client, as a percentage of all cache misses.	Y	Count	Y	Y	Y	Y	Y
Successful reval ratio (Percentage)	Successful revalidations as a percentage of all revalidation attempts.	Y	Number	Y	Y	Y	Y	Y
Successful revalidations	Number of revalidations that have been performed. For more information, see Revalidations (Reval).	Y	Count	Y	Y	Y		
Total parameterized hits	Parameterized requests resulting in either a 304 or non-304 hit.	Y	Count	Y	Y	Y		
Utilized memory(KB)	Amount of memory the integrated cache is currently using.	Y	Size in kilobytes	Y	Y	Y		

IP Counters

The following table gives you a basic overview of the IP counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
IP bytes received	Total number of IP bytes received by NetScaler.	Y	Count	Y	Y	Y	Y	Y
IP bytes transmitted	Total number of IP bytes transmitted by NetScaler.	Y	Count	Y	Y	Y	Y	Y
IP fragments received	Total number of IP fragments received by NetScaler.	Y	Count	Y	Y	Y	Y	Y
IP packets received	Total number of IP packets received by NetScaler	Y	Count	Y	Y	Y	Y	Y
IP packets transmitted	Total number of IP packets transmitted by NetScaler.	Y	Count	Y	Y	Y	Y	Y
Megabits received	Megabits of IP data received.	Y	Count in Megabits	Y	Y	Y	Y	Y
Megabits transmitted	Megabits of IP data transmitted.	Y	Count in Megabits	Y	Y	Y	Y	Y
Packets with bad MAC sent	IP packets transmitted with a bad MAC address.	Y	Count	Y	Y	Y	Y	Y

Packets with len > 1514 rcvd	Packets received with a length greater than the normal maximum transmission unit of 1514 bytes.	Y	Count	Y	Y	Y	Y	Y
Unknown services	Packets received on a port or service that is not configured.	Y	Count	Y	Y	Y	Y	Y
land-attacks	Land-attack packets received. The source and destination addresses are the same.	Y	Count	Y	Y	Y	Y	Y
max non-TCP clients	Attempts to open a new connection to a service for which the maximum limit has been exceeded. Default value, 0, applies no limit.	Y	Count	N	N	N		

Interface Counters

The following table gives you a basic overview of the Interface counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Media type	The media type of the interface.	Y	String	Y	Y	Y	Y	Y
Rx Average bandwidth(bits/sec)	The average rx bandwidth on interface in bits per second.	Y	Count in bits/second	Y	Y	Y	Y	Y
Rx Average packet rate	The average rate of incoming packets on the interface since the system start.	Y	Count	Y	Y	Y	Y	Y
Rx CRC errors	Number of received packets with CRC errors (alignment or FCS).	Y	Count	Y	Y	Y	Y	Y
Rx Frame errors	Number of packets received on the interface that are too long.	Y	Count	Y	Y	Y	Y	Y
Rx alignment errors	The number of alignment errors received on the interface.	Y	Count	Y	Y	Y	Y	Y
Tx Average bandwidth(bits/sec)	The average tx bandwidth on interface in bits per second (bps).	Y	Count in bps	Y	Y	Y	Y	Y

Tx Average packet rate	The average rate of outgoing packets on the interface since the system start.	Y	Count	Y	Y	Y	Y	Y
Tx Carrier errors	Number of carrier errors during transmission.	Y	Count	Y	Y	Y	Y	Y
Tx collisions	Number of collisions in transmission (half-duplex only).	Y	Count	Y	Y	Y	Y	Y
Tx excess collisions	Number of excess collisions in transmission (half-duplex only).	Y	Count	Y	Y	Y	Y	Y
Tx late collisions	Number of late collisions in transmission (half-duplex only).	Y	Count	N	N	N	N	N
Tx multiple collision errors	Number of multiple collisions during transmission (half-duplex only).	Y	Count	Y	Y	Y	Y	Y

Policy Engine Counters

The following table gives you a basic overview of the Policy Engine counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Policy bytes in	Input traffic of a compression policy.	N	Count	Y	Y	Y	Y	Y
Policy bytes out	Output traffic of a compression policy.	N	Count	Y	Y	Y	Y	Y
Policy hits	Total policy hits count.	N	Count	Y	Y	Y	Y	Y

Resources Counters

The following table gives you a basic overview of the Resources counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
CPU Usage(Percentage)	CPU utilization percentage.	Y	Number	Y	Y	Y	Y	Y
Memory Usage(Percentage)	This represents the percentage of memory utilization on NetScaler.	Y	Number	Y	Y	Y	Y	Y

Simple ACL Counters

The following table gives you a basic overview of the simpleACL counters including details, such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Allow Simple ACL hits	Total packets that matched a SimpleACL with action ALLOW and got consumed by NetScaler.	N	Count	Y	Y	Y	Y	Y
Bridge Simple ACL hits	Total packets that matched a SimpleACL with action BRIDGE and got bridged by NetScaler.	N	Count	Y	Y	Y	Y	Y
Deny Simple ACL hits	Total packets that matched a SimpleACL with action DENY and got dropped by NetScaler.	N	Count	Y	Y	Y	Y	Y
Simple ACL hits	Total packets that matched any SimpleACL.	N	Count	Y	Y	Y	Y	Y
Simple ACL misses	Total packets that did not match any SimpleACL.	N	Count	Y	Y	Y	Y	Y

SSL Counters

The following table gives you a basic overview of the SSL counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Backend 3DES 168-bit encryptions	Number of Backend 3DES 168-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend DES 40-bit encryptions	Number of Backend DES 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend DES 56-bit encryptions	Number of Backend DES 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend DH 1024-bit key exchanges	Number of Backend DH 1024-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend DH 2048-bit key exchanges	Number of Backend DH 2048-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend DH 512-bit key exchanges	Number of Backend DH 512-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend DH authentications	Number of Backend DH authentications.	Y	Count	Y	Y	Y	Y	Y
Backend DSS authentications	Number of Backend DSS authentications.	Y	Count	Y	Y	Y	Y	Y
Backend IDEA 128-bit encryptions	Number of Backend IDEA 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend MD5 hashes	Number of Backend MD5 hashes.	Y	Count	Y	Y	Y	Y	Y
Backend RC2 128-bit encryptions	Number of Backend RC2 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RC2 40-bit encryptions	Number of Backend RC2 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y

Backend RC2 56-bit encryptions	Number of Backend RC2 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RC4 128-bit encryptions	Number of Backend RC2 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RC4 40-bit encryptions	Number of Backend RC4 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RC4 56-bit encryptions	Number of Backend RC4 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RC4 64-bit encryptions	Number of Backend RC4 64-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend RSA 1024-bit key exchanges	Number of Backend RSA 1024-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend RSA 2048-bit key exchanges	Number of Backend RSA 2048-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend RSA 512-bit key exchanges	Number of Backend RSA 512-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
Backend RSA authentications	Number of Backend RSA authentications.	Y	Count	Y	Y	Y	Y	Y
Backend SHA hashes	Number of Backend SHA hashes.	Y	Count	Y	Y	Y	Y	Y
Backend SSL multiplex failures	Number of Backend SSL session multiplex failures.	Y	Count	Y	Y	Y	Y	Y
Backend SSL sessions	Number of Backend SSL sessions.	Y	Count	Y	Y	Y	Y	Y
Backend SSL sessions reused	Number of Backend SSL sessions reused.	Y	Count	Y	Y	Y	Y	Y
Backend SSLv3 client authentications	Number of Backend SSLv3 client authentications.	Y	Count	Y	Y	Y	Y	Y
Backend SSLv3 handshakes	Number of Backend SSLv3 handshakes.	Y	Count	Y	Y	Y	Y	Y
Backend SSLv3 sessions	Number of Backend SSLv3 sessions.	Y	Count	Y	Y	Y	Y	Y
Backend TLSv1 client authentications	Number of Backend TLSv1 client authentications.	Y	Count	Y	Y	Y	Y	Y

Backend TLSv1 handshakes	Number of Backend TLSv1 handshakes.	Y	Count	Y	Y	Y	Y	Y
Backend TLSv1 sessions	Number of Backend TLSv1 sessions.	Y	Count	Y	Y	Y	Y	Y
Backend export sessions	Number of Backend export sessions.	Y	Count	Y	Y	Y	Y	Y
Backend null authentications	Number of Backend null authentications.	Y	Count	Y	Y	Y	Y	Y
Backend null encryptions	Number of Backend null cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
Backend session multiplex attempts	Number of Backend SSL session multiplex attempts.	Y	Count	Y	Y	Y	Y	Y
Backend session multiplex successes	Number of Backend SSL session multiplex successes.	Y	Count	Y	Y	Y	Y	Y
Current SSL sessions	Number of active SSL sessions.	Y	Count	Y	Y	Y	Y	Y
DES 168-bit encryptions	Number of Backend 3DES 168-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
DES 40-bit encryptions	Number of Backend DES 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
DES 56-bit encryptions	Number of Backend DES 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
DES encryptions offloaded	Number of DES encryptions offloaded to crypto card.	Y	Count	Y	Y	Y	Y	Y
DH 1024-bit key exchanges	Number of Backend DH 1024-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
DH 2048-bit key exchanges	Number of Backend DH 2048-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
DH 512-bit key exchanges	Number of Backend DH 512-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
DH authentications	Number of Backend DH authentications.	Y	Count	Y	Y	Y	Y	Y

DH key exchanges offloaded	Number of DH key exchanges offloaded to crypto card.	Y	Count	Y	Y	Y	Y	Y
DSS (DSA) authentications	Total number of times DSS authorization used.	Y	Count	Y	Y	Y	Y	Y
Export sessions (40-bit)	Number of Backend export sessions.	Y	Count	Y	Y	Y	Y	Y
IDEA 128-bit encryptions	Number of Backend IDEA 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
MD5 hashes	Number of MD5 hashes.	Y	Count	Y	Y	Y	Y	Y
New SSL sessions	Number of new SSL sessions created.	Y	Count	Y	Y	Y	Y	Y
Null authentications	Number of Null authentications.	Y	Count	Y	Y	Y	Y	Y
Null cipher encryptions	Number of Null cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC2 128-bit encryptions	Number of Backend RC2 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC2 40-bit encryptions	Number of Backend RC2 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC2 56-bit encryptions	Number of Backend RC2 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC4 128-bit encryptions	Number of Backend RC4 128-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC4 40-bit encryptions	Number of Backend RC4 40-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC4 56-bit encryptions	Number of Backend RC4 56-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RC4 64-bit encryptions	Number of Backend RC4 64-bit cipher encryptions.	Y	Count	Y	Y	Y	Y	Y
RSA 1024-bit key exchanges	Number of Backend RSA 1024-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
RSA 2048-bit key exchanges	Number of Backend RSA 2048-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y

RSA 512-bit key exchanges	Number of Backend RSA 512-bit key exchanges.	Y	Count	Y	Y	Y	Y	Y
RSA authentications	Number of RSA authentications.	Y	Count	Y	Y	Y	Y	Y
RSA key exchanges offloaded	Number of RSA key exchanges offloaded to crypto card.	Y	Count	Y	Y	Y	Y	Y
RSA sign operations offloaded	Number of RSA key exchanges offloaded to crypto card.	Y	Count	Y	Y	Y	Y	Y
SHA hashes	Number of Backend SHA hashes.	Y	Count	Y	Y	Y	Y	Y
SSL Crypto card status	Status of the SSL card (1=UP, 0=DOWN).	Y	Count	Y	Y	Y	Y	Y
SSL Engine status	Status of the SSL Engine (1=UP/0=DOWN). This state is decided based on SSL Feature/License status and minimum number of cards UP.	Y	Count	Y	Y	Y	Y	Y
SSL session hits	Number of SSL session reuse hits.	Y	Count	Y	Y	Y	Y	Y
SSL session misses	Number of SSL session reuse misses.	Y	Count	Y	Y	Y	Y	Y
SSL sessions	Number of SSL sessions.	Y	Count	Y	Y	Y	Y	Y
SSL sessions per second	Number of new SSL sessions created.	Y	Count	Y	Y	Y	Y	Y
SSL transactions	Number of SSL transactions.	Y	Count	Y	Y	Y	Y	Y
SSLv2 SSL handshakes	Number of handshakes on SSLv2.	Y	Count	Y	Y	Y	Y	Y
SSLv2 client authentications	Number of client authentications done on SSLv2.	Y	Count	Y	Y	Y	Y	Y
SSLv2 sessions	Number of SSLv2 sessions.	Y	Count	Y	Y	Y	Y	Y

SSLv2 transactions	Number of SSLv2 transactions.	Y	Count	Y	Y	Y	Y	Y
SSLv3 SSL handshakes	Number of handshakes on SSLv3.	Y	Count	Y	Y	Y	Y	Y
SSLv3 client authentications	Number of client authentications done on SSLv3.	Y	Count	Y	Y	Y	Y	Y
SSLv3 session renegotiations	Number of session renegotiations done on SSLv3.	Y	Count	Y	Y	Y	Y	Y
SSLv3 sessions	Number of SSLv3 sessions.	Y	Count	Y	Y	Y	Y	Y
SSLv3 transactions	Total number of SSLv3 Transactions.	Y	Count	Y	Y	Y	Y	Y
TLSv1 SSL handshakes	Number of SSL handshakes on TLSv1.	Y	Count	Y	Y	Y	Y	Y
TLSv1 client authentications	Number of client authentications done on TLSv1.	Y	Count	Y	Y	Y	Y	Y
TLSv1 session renegotiations	Number of SSL session renegotiations done on TLSv1.	Y	Count	Y	Y	Y	Y	Y
TLSv1 sessions	Number of TLSv1 sessions.	Y	Count	Y	Y	Y	Y	Y
TLSv1 transactions	Number of TLSv1 transactions.	Y	Count	Y	Y	Y	Y	Y
Total SSL Session Renegotiations	Number of SSL session renegotiations.	Y	Count	Y	Y	Y	Y	Y

Service Groups Counters

The following table gives you a basic overview of the Service Group counters including details, such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Average TTFB	Average time required for the server to receive the first byte of data from the NetScaler. This average is calculated repeatedly every 14 seconds.	N	Count	Y	Y	Y	Y	Y
Average transaction time	Average transaction time between NetScaler and the service behind it.	N	Count	Y	Y	Y	Y	Y
Current client connections	Client connections that are currently open to the selected service, including both established connections and those in the surge queue.	N	Count	Y	Y	Y	Y	Y
Established active connections	The number of established connections that are currently active.	N	Count	Y	Y	Y	Y	Y
Established connections	The number of established connections.	N	Count	Y	Y	Y	Y	Y
Genuine clients on this service	The number of genuine client on a service.	N	Count	Y	Y	Y	Y	Y
JavaScript sent to genuine clients	Total number of JavaScripts sent to genuine clients.	N	Count	Y	Y	Y	Y	Y

Request bytes	The total number of request bytes received on a service or vserver.	N	Count	Y	Y	Y	Y	Y
Request rate	This represents the request rate in requests per second for a service or vserver.	N	Count	Y	Y	Y	Y	Y
Request rate bytes	This represents the request rate in bytes per second for a service or vserver.	N	Count	Y	Y	Y	Y	Y
Response bytes	Number of response bytes received on a service or vserver.	N	Count	Y	Y	Y	Y	Y
Response rate bytes	This represents the response rate in bytes per second for a service or vserver.	N	Count	Y	Y	Y	Y	Y
Service Group FullName	The name of the service group.	N	String	Y	Y	Y	Y	Y
Service Group Member FullName	The name of the service group member.	N	String	Y	Y	Y	Y	Y
Service Group Name	The name of the service group.	N	String	Y	Y	Y	Y	Y
State	Current state of the server.	N	Enum	Y	Y	Y	Y	Y
Surge queue requests	The number of requests in the surge queue.	N	Count	Y	Y	Y		
Type	The protocol type of the service.	N	Enum	Y	Y	Y		
Unacknowledged SYNs rate	This represents the rate of unacknowledged SYNs for a service or vserver.	N	Count	Y	Y	Y		

Services Counters

The following table gives you a basic overview of the Services counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Active connections	The number of established connections that are currently active.	N	Count	Y	Y	Y	Y	Y
Average transaction time	Average transaction time between NetScaler and the service behind it.	N	Number	Y	Y	Y	Y	Y
Established connections	The number of established connections.	N	Count	Y	Y	Y	Y	Y
GSLB site name	The name of the GSLB site on which this service is defined.	N	String	Y	Y	Y	Y	Y
Genuine clients on this service	The number of genuine client on this service.	N	Count	Y	Y	Y	Y	Y
JavaScripts sent to genuine clients	Total number of JavaScripts sent to genuine clients.	N	Count	Y	Y	Y	Y	Y
Maximum requests per connection	The maximum requests per connection allowed on this service.	N	Count	Y	Y	Y	Y	Y
Packets received	The total number of packets received on this service/vserver.	N	Count	Y	Y	Y	Y	Y
Packets sent	The total number of packets sent.	N	Count	Y	Y	Y	Y	Y

Request bytes	The total number of request bytes received on this service/vserver.	N	Bytes	Y	Y	Y	Y	Y
Requests	The total number of requests received on this service/vserver. (This is applicable for HTTP/SSL servicetype.)	N	Count	Y	Y	Y	Y	Y
Response Bytes	Number of response bytes received on this service/vserver.	N	Bytes	Y	Y	Y	Y	Y
Responses	Number of responses received on this service/vserver. (This is applicable for HTTP/SSL servicetype.)	N	Count	Y	Y	Y	Y	Y
State	Current state of the server.	N	Enum	Y	Y	Y	Y	Y
Surge count	The number requests in the surge queue.	N	Count	Y	Y	Y	Y	Y
Syns received	The total number of syns received from clients on this service/vserver.	N	Count	Y	Y	Y		
Type	The protocol type of the service.	N	Enum	Y	Y	Y		

Sure Connect Counters

The following table gives you a basic overview of the Sure Connect counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Alternate content hits	Number of requests that are required to load the alternate content in the pop-up window.	N	Count	Y	Y	Y	Y	Y
Corrupted SureConnect cookies	Number of times NetScaler encountered corrupted SureConnect Cookies.	N	Count	Y	Y	Y	Y	Y
Delay stats reset	Number of times SureConnect statistics were reset.	N	Count	Y	Y	Y	Y	Y
In-memory pop-up screen hits	Number of times NetScaler served the in-memory java script, which displays the pop-up window.	N	Count	Y	Y	Y	Y	Y
POST requests	Number of times a POST request triggered SureConnect.	N	Count	Y	Y	Y	Y	Y
Requests from unsupported browsers	Number of times requests came from unsupported browsers.	N	Count	Y	Y	Y	Y	Y

Requests in SureConnect session	Number of requests that came in a SureConnect session.	N	Count	Y	Y	Y	Y	Y
SureConnect URL hits	Number of times NetScaler matched an incoming request with a Configured SureConnect policy.	N	Count	Y	Y	Y	Y	Y
Threshold conditions failed	This counter gives the number of times NetScaler did not serve the in-memory response because the thresholds conditions had failed.	N	Count	Y	Y	Y	Y	Y

System Disk Counters

The following table gives you a basic overview of the System Disk counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Available disk space (MB)	Available space in the /flash or /var partition of the disk.	Y	Count	Y	Y	Y	Y	Y
Percentage of disk space used (%)	Used space in the /var or /flash partition of the disk, as a percentage. You can configure /var Used (%) or /flash Used (%) by using the "Set snmp alarm DISK-USAGE-HIGH" command.	Y	Integer	Y	Y	Y	Y	Y
Total disk space (MB)	Total disk space of the /var or /flash partition of the disk.	Y	Count	Y	Y	Y	Y	Y
Used disk space (MB)	Used space in /flash or /var partition of the disk.	Y	Count	Y	Y	Y	Y	Y

TCP Counters

The following table gives you a basic overview of the TCP counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
All client connections	Client connections, including connections in the Opening, Established, and Closing state.	Y	Count	Y	Y	Y	Y	Y
All server connections	Server connections, including connections in the Opening, Established, and Closing state.	Y	Count	Y	Y	Y	Y	Y
Closing client connections	Client connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.	Y	Count	Y	Y	Y	Y	Y
Closing server connections	Server connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.	Y	Count	Y	Y	Y	Y	Y

Current Physical servers with open conns	The number of physical servers that NetScaler has open connections with.	Y	Count	Y	Y	Y	Y	Y
Established client connections	Current client connections in the Established state, which indicates that data transfer can occur between the NetScaler and the client.	Y	Count	Y	Y	Y	Y	Y
Established server connections	Current server connections in the Established state, which indicates that data transfer can occur between the NetScaler and the server.	Y	Count	Y	Y	Y	Y	Y
Max Requests per Connection	Maximum number of requests per connection.	Y	Count	Y	Y	Y	Y	Y
Max Server Connections	Maximum number of server connections.	Y	Count	Y	Y	Y	Y	Y
Opening client connections	Client connections in the Opening state, which indicates that the handshakes are not yet complete.	Y	Count	Y	Y	Y	Y	Y
Opening server connections	Server connections in the Opening state, which indicates that the handshakes are not yet complete.	Y	Count	Y	Y	Y	Y	Y

Rejected TCP SYN cookie packets (Bad Seq No)	Number of TCP SYN cookie packets rejected due to incorrect sequence number.	Y	Count	Y	Y	Y	Y	Y
Rejected TCP SYN cookie packets (Bad Signature)	Number of TCP SYN cookie packets rejected due to incorrect signature.	Y	Count	Y	Y	Y	Y	Y
Server Conn Reuse-pool hits	Number of client transactions that found the server connection in the reuse-pool.	Y	Count	Y	Y	Y	Y	Y
Server active connections	Number of connections currently serving requests.	Y	Count	Y	Y	Y	Y	Y
Spare connections	Spare connections available. To save time and resources in establishing another connection for a new client, the connection on the server is not closed after completing the request from the first client and is available for serving future requests.	Y	Count	Y	Y	Y	Y	Y

Surge queue	Connections in the surge queue. When the NetScaler cannot open a connection to the server, for example when maximum connections have been reached, the NetScaler queues these requests.	Y	Count	Y	Y	Y	Y	Y
TCP current pending connections	Number of current pending TCP connections.	Y	Count	Y	Y	Y		

UDP Counters

The following table gives you a basic overview of the User Datagram Protocol (UDP) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
UDP bytes received	Bytes of UDP data received.	Y	Bytes	Y	Y	Y	Y	Y
UDP bytes transmitted	Bytes of UDP data transmitted. **Note:** Total represents a cumulative aggregate since the NetScaler became operational. This value is reset to 0 when the NetScaler is restarted. Rate is computed as the number of times the Total statistic is incremented per second, averaged across seven-second intervals. The rate remains 0 if the NetScaler is not handling any UDP traffic.	Y	Bytes	Y	Y	Y	Y	Y

UDP packet rate threshold	Value set for 10ms rate threshold for UDP packets. This implies that within 10 milliseconds (ms) range, NetScaler can allow (receive or pass through) the set number of UDP packets.	Y	Number	Y	Y	Y	Y	Y
UDP packets received	UDP packets received.	Y	Count	Y	Y	Y	Y	Y
UDP packets transmitted	UDP packets transmitted.	Y	Count	Y	Y	Y	Y	Y
UDP rate threshold	Number of time UDP rate threshold was exceeded.	Y	Count	Y	Y	Y	Y	Y
UDP unknown service errors	Total number of UDP packets received by NetScaler to unconfigured services.	Y	Count	Y	Y	Y		

VLAN Counters

The following table gives you a basic overview of the VLAN counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Broadcast packets sent and received	Broadcast packets sent and received on the VLAN. **Note:** Total represents a cumulative aggregate since the VLAN became operational. This value is reset to 0 when a NetScaler is restarted or the VLAN configuration is updated. Rate is computed as the number of times the Total statistic is incremented per second, averaged across seven-second intervals. The rate remains 0 if the VLAN is not handling any traffic.	Y	Count	Y	Y	Y	Y	Y
Bytes received	Bytes of data received on the VLAN.	Y	Bytes	Y	Y	Y	Y	Y

Bytes sent	Bytes of data transmitted on the VLAN.	Y	Bytes	Y	Y	Y	Y	Y
Member Interfaces	List of interfaces on the NetScaler that are members of the VLAN.	Y	Count	Y	Y	Y	Y	Y
Packets dropped	Inbound packets dropped by the VLAN upon reception.	Y	Count	Y	Y	Y		
Packets received	Packets received on the VLAN.	Y	Count	Y	Y	Y		
Packets sent	Packets transmitted on the VLAN.	Y	Count	Y	Y	Y		
Tagged Interfaces	List of interfaces on the NetScaler that are members of the VLAN that carry tagged packets.	Y	Count	Y	Y	Y		

Virtual Servers Counters

The following table gives you a basic overview of the Virtual Server (vserver) counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Current Configured VServers	Number of vservers configured on the NetScaler.	Y	Count	Y	Y	Y	Y	Y
Current Services Down	Number of services that are bound to this vserver and are in the state 'down'.	Y	Count	Y	Y	Y	Y	Y
Current Services UnKnown	Number of services that are bound to this vserver and are in the state 'unKnown'.	Y	Count	Y	Y	Y	Y	Y
Current Services Up	Number of services that are bound to this vserver and are in the state 'up'.	N	Count	Y	Y	Y	Y	Y
Current client connections	Number of current client connections.	N	Count	Y	Y	Y	Y	Y
Current server connections	Number of current connections to the real servers behind the vserver.	N	Count	Y	Y	Y	Y	Y
Number of services	Number of services bound to the vserver.	N	Count	N	Y	Y	Y	Y
Number of spill overs	Number of times vserver experienced spill over.	N	Count	N	Y	Y	Y	Y
Number of SSL users	Current number of SSL users accessing this vserver.	N	Count	N	Y	Y	Y	Y
Maximum requests per connection	Maximum number of requests per connection allowed on this vserver.	N	Number	N	N	N	N	N
Packets received	Number of packets received on this service/vserver.	N	Count	Y	Y	Y	Y	Y
Packets sent	Number of packets sent.	N	Count	Y	Y	Y	Y	Y
Requests	Number of requests received on this service/vserver. (This is applicable for HTTP/SSL servicetype.)	N	Count	Y	Y	Y	Y	Y
Requests bytes	Number of request bytes received on this service/vserver.	N	Bytes	Y	Y	Y	Y	Y

Response Bytes	Number of response bytes received on this service/vserver.	N	Bytes	Y	Y	Y	Y	Y
Responses	Number of responses received on this service/vserver (This is applicable for HTTP/SSL servicetype).	N	Count	Y	Y	Y	Y	Y
Services Out of Svc	Number of services which are bound to this vserver and are in the state 'outOfService'.	N	Count	Y	Y	Y	Y	Y
Services Transition to Out of Svc	Number of services which are bound to this vserver and are in the state 'transitionToOutOfService'.	N	Count	Y	Y	Y	Y	Y
State	State of the server.	N	Enum	Y	Y	Y	Y	Y
Syns received	Number of syns received from clients on this service/vserver.	N	Count	Y	Y	Y	Y	Y
Time since last state change	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.	N	Date/ Time	N	Y	Y	Y	Y
Total Vserver Hits	Number of times this vserver has been provided.	N	Count	N	Y	Y	Y	Y
Total Vserver Misses	Total vserver misses.	N	Count	Y	Y	Y	Y	Y
Type	Protocol associated with the vserver.	N	Enum	Y	Y	Y		
UP services (%)	Percentage of UP services bound to this vserver.	N	Number	N	Y	Y		

Virtual Services Counters

The following table gives you a basic overview of the Virtual Services counters including details such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Service Hits	This represents the number of times that the service has been provided.	Y	Count	Y	Y	Y	Y	Y
Service Persistent Hits	The total number of persistent hits.	Y	Count	Y	Y	Y	Y	Y
Service Weight	The weight of the service tied to the vserver.	Y	Number	Y	Y	Y	Y	Y

VPN Counters

The following table gives you a basic overview of the Virtual Private Network (VPN) counters including details, such as their descriptions, the default poll status on Command Center, interpretation of counter values, and their availability on various NetScaler versions.

Counter	Description	Default Poll	Values	8.1	9.0	9.1	9.2	9.3
Backend HTTP server probes	Number of probes from NetScaler to backend HTTP server. The backend servers are those servers that have been accessed by a VPN client. This is an application debug counter.	N	Count	Y	Y	Y	Y	Y
Backend non-HTTP server probes	Number of probes from NetScaler to backend non-HTTP servers. The backend servers are those servers that have been accessed by a VPN client. This is an application debug counter.	N	Count	Y	Y	Y	Y	Y
Backend servers probe successes	Number of successful probes to backend servers (both HTTP and non- HTTP). This is an application debug counter.	N	Count	Y	Y	Y	Y	Y
CPS connection failure	Number of CPS connection failure.	N	Count	Y	Y	Y	Y	Y

CPS connection success	Number of CPS connection success.	N	Count	Y	Y	Y	Y	Y
Client configuration requests	Number of SSLVPN-client configuration requests received by the SSLVPN server. In response to these requests, the SSLVPN server returns information to configure the SSLVPN client.	N	Count	Y	Y	Y	Y	Y
DNS queries received	Number of DNS queries received by SSLVPN server.	N	Count	Y	Y	Y	Y	Y
File-system requests received	Number of file-system request received by the SSLVPN server.	N	Count	Y	Y	Y	Y	Y
ICA license failure	Number of ICA license failures.	N	Count	Y	Y	Y	Y	Y
IIP disabled and MIP disabled	Number of times IIP and MIP are disabled.	N	Count	Y	Y	Y	Y	Y
IIP disabled and MIP used	Number of times MIP is used and IIP is disabled.	N	Count	Y	Y	Y	Y	Y
IIP failed and MIP disabled	Number of times IIP assignment failed and MIP is disabled.	N	Count	Y	Y	Y	Y	Y
IIP failed and MIP used	Number of times MIP is used and IIP assignment failed.	N	Count	Y	Y	Y	Y	Y
Login-page delivery failures	Number of times the login page has not been delivered by SSLVPN server.	N	Count	Y	Y	Y	Y	Y

Login-page requests received	Number of login page requests received by SSLVPN server.	N	Count	Y	Y	Y	Y	Y
SOCKS client error	Number of SOCKS client error.	N	Count	Y	Y	Y	Y	Y
SOCKS connect request received	Number of received SOCKS connect request.	N	Count	Y	Y	Y	Y	Y
SOCKS connect request sent	Number of sent SOCKS connect request.	N	Count	Y	Y	Y	Y	Y
SOCKS connect response received	Number of received SOCKS connect response.	N	Count	Y	Y	Y	Y	Y
SOCKS connect response sent	Number of sent SOCKS connect response.	N	Count	Y	Y	Y	Y	Y
SOCKS method request received	Number of received SOCKS method request.	N	Count	Y	Y	Y	Y	Y
SOCKS method request sent	Number of sent SOCKS method request.	N	Count	Y	Y	Y	Y	Y
SOCKS method response received	Number of received SOCKS method response.	N	Count	Y	Y	Y	Y	Y
SOCKS method response sent	Number of sent SOCKS method response.	N	Count	Y	Y	Y	Y	Y
SOCKS server error	Number of SOCKS server error.	N	Count	Y	Y	Y	Y	Y
SSLVPN tunnels	Total number of SSLVPN tunnels created between SSLVPN client and server.	N	Count	Y	Y	Y	Y	Y
STA connection failure	Number of STA connection failure.	N	Count	Y	Y	Y	Y	Y

STA connection success	Number of STA connection success.	N	Count	Y	Y	Y	Y	Y
STA request sent	Number of STA request sent.	N	Count	Y	Y	Y	Y	Y
STA response received	Number of STA response received.	N	Count	Y	Y	Y	Y	Y
WINS queries received	Total number of WINS query(s) received by SSLVPN server.	N	Count	Y	Y	Y	Y	Y

FAQs

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

General

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: 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://support.citrix.com/proddocs/topic/command-center-51/cc-install-plan-installation-con.html.

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.

Installation & Setup

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.SQLServer Driver</property>

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

Administration

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.

Citrix Network

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.

Configuration

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.

Fault

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:

- 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.
- Traps are being dropped for this device.
- 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)`

Reporting

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.

Command Center Appliance

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.