Cisco Prime IP Express 9.0 Administration Guide

First Published: 2016-12-22

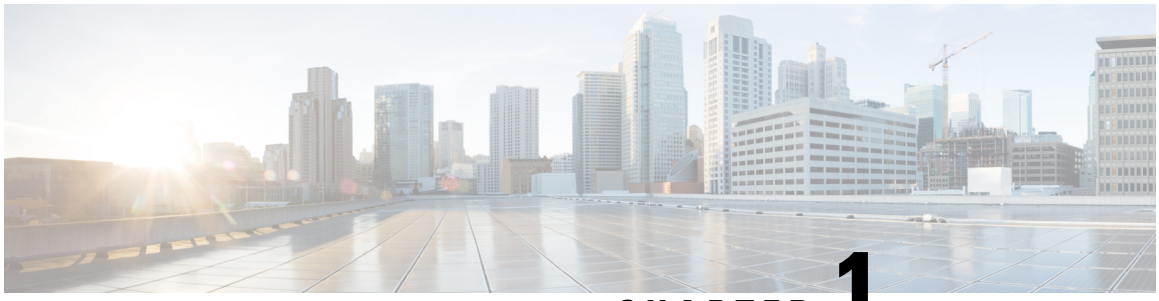
Last Modified: 2016-12-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Getting Started



CHAPTER 1

Introduction to Cisco Prime IP Express

Cisco Prime IP Express is a full featured, scalable Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) implementation for medium to large IP networks. It provides the key benefits of stabilizing the IP infrastructure and automating networking services, such as configuring clients and provisioning cable modems. This provides a foundation for policy-based networking.

Enterprise users can better manage their networks to integrate with other network infrastructure software and business applications.

Target Users

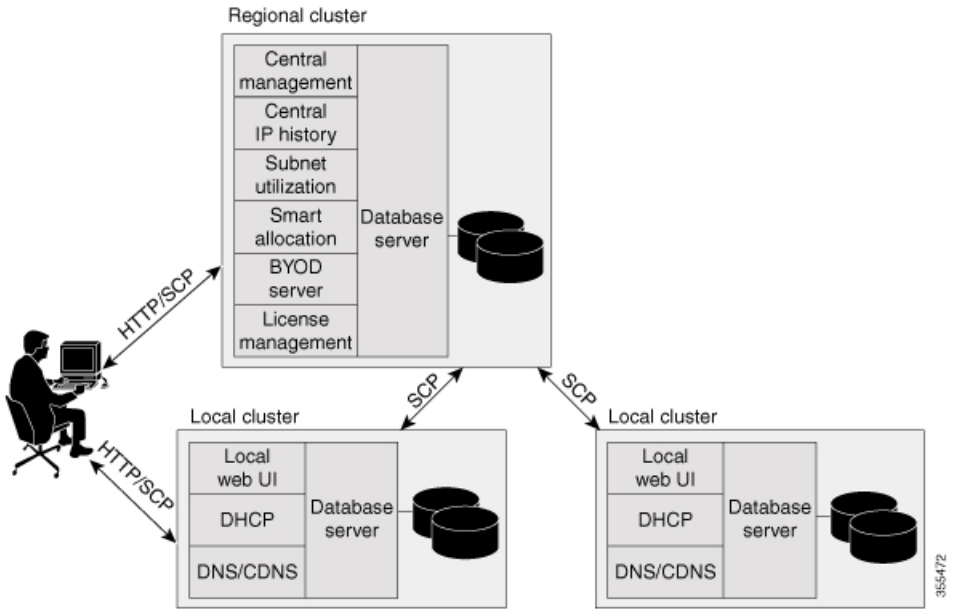
Cisco Prime IP Express is designed for these users:

- **Enterprises**—Helps meet the needs of single- and multisite enterprises (small-to-large businesses) to administer and control network functions. Cisco Prime IP Express automates the tasks of assigning IP addresses and configuring the Transport Control Protocol/Internet Protocol (TCP/IP) software for individual network devices. Forward-looking enterprise users can benefit from class-of-service and other features that help integrate with new or existing network management applications, such as user registration.

Regional and Local Clusters

The regional cluster acts as an aggregate management system for up to a hundred local clusters. Address and server administrators interact at the regional and local clusters through the regional and local web-based user interfaces (web UIs), and local cluster administrators can continue to use the command line interface (CLI) at the local cluster. The regional cluster consists of a Central Configuration Management (CCM) server, Tomcat web server, servlet engine, and server agent (see Management Components, on page 9). The license management is now done at the regional cluster and hence the local server has to be registered to a regional server to avail the necessary services. See the *"Overview" chapter in Cisco Prime IP Express Installation Guide* for more details.

Figure 1: Cisco Prime IP Express User Interfaces and Server Clusters



A typical deployment is one regional cluster at a customer network operation center (NOC), the central point of network operations for an organization. Each division of the organization includes a local address management server cluster responsible for managing a part of the network. The System Configuration Protocol (SCP) communicates the configuration changes between the servers.

Deployment Scenarios

The Cisco Prime IP Express regional cluster web UI provides a single point to manage any number of local clusters hosting DNS, CDNS, or DHCP servers. The regional and local clusters also provide administrator management so that you can assign administrative roles to users logged in to the application.

This section describes two basic administrative scenarios and the hardware and software deployments for two different types of installations—a small-to-medium local area network (LAN), and a large-enterprise or service-provider network with three geographic locations.

Related Topics

Small-to-Medium-Size LANs, on page 2

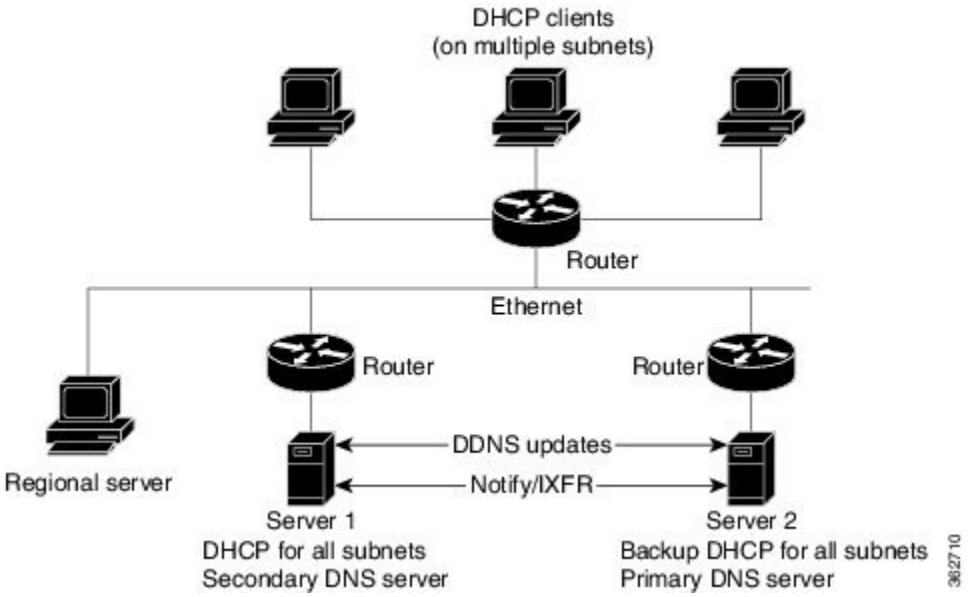
Large Enterprise Networks, on page 3

Small-to-Medium-Size LANs

In this scenario, low-end Windows or Linux servers are acceptable. The image below shows a configuration that would be adequate for this network.

Note Regional server is MUST in deployment for small and medium sized LANs.

Figure 2: Small-to-Medium LAN Configuration

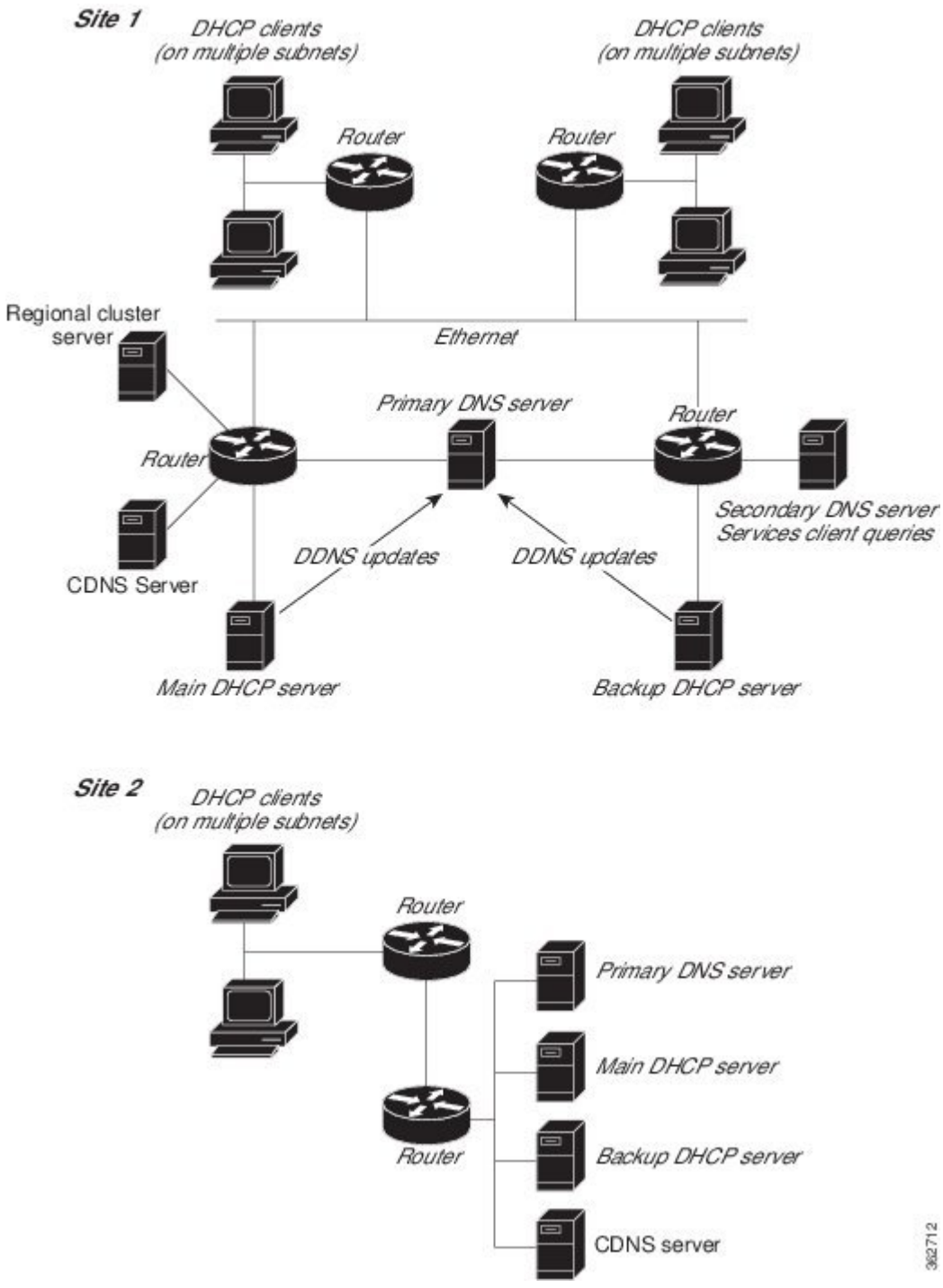


Large Enterprise Networks

In a large enterprise network serving over 500,000 DHCP clients, use mid-range Windows or Linux servers. Put DNS and DHCP servers on different systems. The image below shows the hardware that would be adequate for this network.

When supporting geographically dispersed clients, locate DHCP servers at remote locations to avoid disrupting local services if wide-area connections fail. Install the Cisco Prime IP Express regional cluster to centrally manage the distributed clusters.

Figure 3: Large Enterprise Network Configuration



Configuration and Performance Guidelines

Cisco Prime IP Express is an integrated DHCP and DNS server cluster capable of running on a Windows or Linux workstation or server.

Because of the wide range of network topologies for which you can deploy Cisco Prime IP Express, you should first consider the following guidelines. These guidelines are very general and cover most cases. Specific or challenging implementations could require additional hardware or servers.

Related Topics

General Configuration Guidelines, on page 5

Special Configuration Cases, on page 6

General Performance Guidelines, on page 6

General Configuration Guidelines

The following suggestions apply to most Cisco Prime IP Express deployments:

- Configure a separate DHCP server to run in remote segments of the wide area network (WAN).

  Ensure that the DHCP client can consistently send a packet to the server in under a second. The DHCP protocol dictates that the client receive a response to a DHCPDISCOVER or DHCPREQUEST packet within four seconds of transmission. Many clients (notably early releases of the Microsoft DHCP stack) actually implement a two-second timeout.

- In large deployments, separate the secondary DHCP server from the primary DNS server used for dynamic DNS updates.

  Because lease requests and dynamic DNS updates are persisted to disk, server performance is impacted when using a common disk system. So that the DNS server is not adversely affected, run it on a different cluster than the DHCP server.

- Include a time server in your configuration to deal with time differences between the local and regional clusters so that aggregated data at the regional server appears in a consistent way. See the Polling Lease History Data, on page 88.
- Set DHCP lease times in policies to four to ten days.

  To prevent leases from expiring when the DHCP client is turned off (overnight or over long weekends), set the DHCP lease time longer than the longest period of expected downtime, such as seven days. See *"Managing Leases" section in Cisco Prime IP Express 9.0 DHCP User Guide*.

- Locate backup DNS servers on separate network segments.

  DNS servers are redundant by nature. However, to minimize client impact during a network failure, ensure that primary and secondary DNS servers are on separate network segments.

- If there are high dynamic DNS update rates in the network, configure separate DNS servers for forward and reverse zones.
- Use NOTIFY/IXFR.

  Secondary DNS servers can receive their data from the primary DNS server in two ways: through a full zone transfer (AXFR) or an incremental zone transfer (NOTIFY/IXFR, as described in RFCs 1995 and

1996). Use NOTIFY/IXFR in environments where the name space is relatively dynamic. This reduces the number of records transferred from the primary to the secondary server. See the *"Enabling Incremental Zone Transfers (IXFR)" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.

Special Configuration Cases

The following suggestions apply to some special configurations:

- When using dynamic DNS updates for large deployments or very dynamic networks, divide primary and secondary DNS and DHCP servers across multiple clusters.

  Dynamic DNS updates generate an additional load on all Cisco Prime IP Express servers as new DHCP lease requests trigger dynamic DNS updates to primary servers that update secondary servers through zone transfers.

- During network reconfiguration, set DHCP lease renewal times to a small value.

  Do this several days before making changes in network infrastructure (such as to gateway router and DNS server addresses). A renewal time of eight hours ensures that all DHCP clients receive a changed DHCP option parameter within one working day. See the *"Managing Leases" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*

General Performance Guidelines

For Cisco Prime IP Express, the general guideline is to invest in the highest performance disk I/O subsystem available, then memory, and finally the processors. DHCP and Authoritative DNS (especially if using DNS updates) will be most impacted by disk latency, then memory and network performance, and finally CPU (these applications are not CPU intensive).

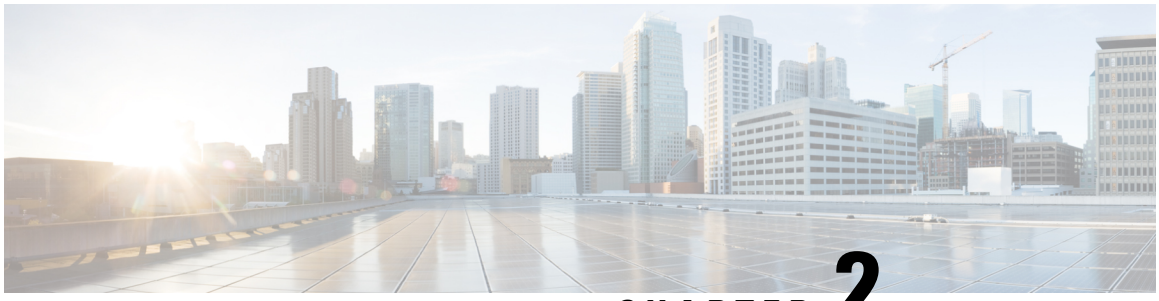
- The best way to reduce latency and improve performance is to provide high performance disks (SSD are recommended over traditional hard disks). High performance disk controllers are also recommended. This is especially important for DHCP and Authoritative DNS servers that handle Dynamic Updates.
- Providing lots of memory is also important as it reduces disk read requirements if the file system cache can be used. The recommendation here is to assure that a system has sufficient free memory that is twice the size of the CPIPEdatabases. It is difficult to give exact requirements here as it depends on many variables.
- Network performance is also an important consideration and 1 GB or better Ethernet controllers are recommended.
- As most Cisco Prime IP Express uses are not CPU intensive, the CPU performance tends to be least important.

Interoperability with Earlier Releases

The following table shows the interoperability of Cisco Prime Network Registrar / Cisco Prime IP Express features on the regional CCM server with versions of the local cluster.

Table 1: CCM Regional Feature Interoperability with Server Versions

Feature	Local Cluster Version			
	8.1 (CPNR)	8.2 (CPNR/CPIPE)	8.3 (CPNR/CPIPE)	9.0 (CPNR/CPIPE)
Push and pull:				
Address space	x	x	x	x
IPv6 address space	x	x	x	x
Scope templates, policies, client-classes	x	x	x	x
IPv6 prefix and link templates	x	x	x	x
Zone data and templates	x	x	x	x
Groups, owners, regions	x	x	x	x
Resource records (RRs)	x	x	x	x
Local cluster restoration	x	x	x	x
Host administration	x	x	x	x
Extended host administration	x	x	x	x
Administrators and roles	x	x	x	x
Zone Views		x	x	x
Administrator:				
Single sign-on	x	x	x	x
Password change	x	x	x	x
IP history reporting:				
Lease history	x	x	x	x
Detailed lease history	x	x	x	x
Utilization reporting:				
Subnet utilization history	x	x	x	x
Subnet and scope utilization	x	x	x	x
IPv6 prefix utilization	x	x	x	x



CHAPTER 2

Cisco Prime IP Express User Interfaces

Cisco Prime IP Express provides a regional and a local web UI and a regional and local CLI to manage the CDNS, DNS, DHCP, and CCM servers:

- **Web UI for the regional cluster to access local cluster servers**—See Regional Cluster Web UI, on page 19.
- **Web UI for the local cluster**—See Local Cluster Web UI, on page 16.
- **CLI for the local clusters**—Open the **CLIContent.html** file in the installation **/docs** directory (see Command Line Interface, on page 20).
- **CCM servers that provide the infrastructure to support these interfaces**— See Central Configuration Management Server, on page 75.

This chapter describes the Cisco Prime IP Express user interfaces and the services that the CCM servers provide. Read this chapter before starting to configure the Cisco Prime IP Express servers so that you become familiar with each user interface capability.

Management Components

Cisco Prime IP Express contains two management components:

- Regional component, consisting of:
  - Web UI
  - CLI
  - CCM Server
  - Bring your own device (BYOD)
  - Simple Network Management Protocol (SNMP) server
- Local component, consisting of:

- Web UI
- CLI
- CCM server
- Authoritative Domain Name System (DNS) server
- Caching / Recursive Domain Name System (CDNS) server
- Dynamic Host Configuration Protocol (DHCP) server
- SNMP server
- Management of local address space, zones, scopes, DHCPv6 prefixes and links, and users

Note Cisco Prime IP Express includes a Hybrid DNS feature that allows you to run both the Caching DNS and Authoritative DNS servers on the same operating system without two separate virtual or physical machines. However, Cisco recommends hybrid mode for smaller sized deployments only. For larger deployments, Cisco recommends separating Caching and Authoritative DNS on separate physical machines or VMs.

License management is done from the regional cluster when Cisco Prime IP Express is installed. You must install the regional server first and load all licenses in the regional server. When you install the local cluster, it registers with regional to obtain its license.

The regional CCM server provides central management of local clusters, with an aggregated view of DHCP address space and DNS zones. It provides management of the distributed address space, zones, scopes, DHCPv6 prefixes and links, and users.

The local CCM server provides management of the local address space, zones, scopes, DHCPv6 prefixes and links, and users.

The remainder of this chapter describes the SNMP protocol. The CCM server, web UIs, and CLI are described in Cisco Prime IP Express User Interfaces, on page 9. The DNS, CDNS, and DHCP servers are described in their respective sections.

Introduction to the Web-Based User Interfaces

The web UI provides granular access to configuration data through user roles and constraints. The UI provides quick access to common functions. The web UI granularity is described in the following sections.

Related Topics

Supported Web Browsers, on page 11

Access Security, on page 11

Logging In to the Web UIs, on page 11

Multiple Users, on page 12

Changing Passwords, on page 12

Navigating the Web UIs, on page 13

Waiting for Page Resolution Before Proceeding, on page 13

Committing Changes in the Web UIs, on page 14

Supported Web Browsers

The web UI has been tested on Microsoft Internet Explorer 9, Mozilla Firefox 21 and later, and Google Chrome 53. Internet Explorer 8 is not supported.

Access Security

At Cisco Prime IP Express installation, you can choose to configure HTTPS to support secure client access to the web UIs. You must specify the HTTPS port number and provide the keystore at that time. With HTTPS security in effect, the web UI Login page indicates that the "Page is SSL[1] Secure."

Note Do not use a dollar sign (**$**) symbol as part of a keystore password.

Logging In to the Web UIs

You can log into the Cisco Prime IP Express local or regional cluster web UIs either by HTTPS secure or HTTP nonsecure login. After installing Cisco Prime IP Express, open one of the supported web browsers and specify the login location URL in the browser address or netsite field. Login is convenient and provides some memory features to increase login speed.

You can log in using a nonsecure login in two ways:

- On Windows, from the Start menu, choose **Start** > **All Programs** > **IP Express 9.0** > **IP Express 9.0** {**local** | **regional**} **Web UI**. This opens the local or regional cluster web UI from your default web browser.

  Note Open the regional Web UI first and add the licenses for the required services.

- Open the web browser and go to the web site. For example, if default ports were used during the installation, the URLs would be **http://***hostname***:8080** for the local cluster web UI, and **http://***hostname***:8090** for the regional cluster web UI.

This opens the New Product Installation page if no valid license is added at the time of installation. You have to browse and add the valid license. If the license key is acceptable, the Cisco Prime IP Express login page is displayed.

[1] This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Note You can add the licenses only in the regional server. The local has to be registered to the regional at the time of installation to run the desired licensed services.

In the local server, confirm the regional server IP address and port number and also the services you want to run at the time of your first login. Click **Register** to confirm registration. If the regional server is configured with the required licenses, you will be displayed the login page.

Enter the superuser username and password created at the time of installation to log into the Web UI. The password is case-sensitive (See Managing Passwords, on page 47). If you already added the valid license and superuser and configured a password at the time of installation, then you can log into the web UI using that username and password.

Note There is no default username or password for login.

Note To prepare for an HTTPS-secured login, see *Cisco Prime IP Express Installation Guide.*

Depending on how your browser is set up, you might be able to abbreviate the account name or choose it from a drop-down list while setting the username.

To log in, click **Login**.

Multiple Users

The Cisco Prime IP Express user interfaces support multiple, concurrent users. If two users try to access the same object record or data, a **Modified object** error will occur for the second user. If you receive this error while editing user data, do the following:

- **In the web UI**—Cancel the edits and refresh the list. Changes made by the first user will be reflected in the list. Redo the edits, if necessary.
- **In the CLI**—Use the **session cache refresh** command to clear the current edits, before viewing the changes and making further edits. Make changes, if you feel that it is necessary even after the other user's changes.

Changing Passwords

Whenever you edit a password on a web UI page, it is displayed as a string of eight dots. The actual password value is never sent to the web browser. So, if you change the password, the field is automatically cleared. You must enter the new password value completely, exactly as you want it to be.

Note The password should not be more than 255 characters long.

For details on changing administrator passwords at the local and regional cluster, see Managing Passwords, on page 47.

Navigating the Web UIs

The web UI provides a hierarchy of pages based on the functionality you desire and the thread you are following as part of your administration tasks. The page hierarchy prevents you from getting lost easily.

Caution Do not use the Back button of the browser. Always use the navigation menu, or the **Cancel** button on the page to return to a previous page. Using the browser Back button can cause erratic behavior or can cause failures.

A single sign-on feature is available to connect between the regional and local cluster web UIs. The regional cluster web UI pages include the Connect button in the List/Add Remote clusters page, which you can click to connect to the local cluster associated with the icon. If you have single sign-on privileges to the local cluster, the connection takes you to the related local server management page (or a related page for related server configurations). If you do not have these privileges, the connection takes you to the login page for the local cluster. To return to the regional cluster, local cluster pages have the Return button on the main toolbar.

The Search bar in the navigation menu provides an easy way to search for menus. The Pin icon in the top right corner of the navigation menu helps to pin/unpin the menu.

Starting from release 9.0, Cisco Prime IP Express provides a facility to save the frequently used pages/menus as favorites, which helps in accessing them easily. To configure the page/menu as favorite, after navigating to the desired menu, click the Favorite icon (star icon ( ) next to the navigation path), provide the appropriate name, and then click **OK**. The pages/menus which are configured as favorites appear under the Favorites section of the global navigation. You can delete the menus from the favorites list by clicking the Delete icon next to them. Configuration Summary page is listed under the Favorites section by default.

Note Click the double arrow icon ( ) in any page to view the hidden options/functionalities.

Note Navigation menu items can vary based on if you have the role privileges for IPv4 or IPv6. For example, the **Design** menu can be **DHCPv4** and **DHCPv6** if you have the ipv6-management subrole of the addrblock-admin role assigned.

Waiting for Page Resolution Before Proceeding

Operations performed in the web UI, such as resynchronizing or replicating data from server clusters, are synchronous in that they do not return control to the browser until the operation is completed. These operations display confirmation messages in blue text. Also, both the Netscape and IE browsers display a wait cursor while the operation is in progress.

Tip Wait for each operation in the web UI to finish before you begin a new operation. If the browser becomes impaired, close the browser, reopen it, then log in again. Some operations like zone distributions can take significant amount of time, so you may have to wait till the operation completes.

Committing Changes in the Web UIs

You do not actually commit the page entries you make until you click **Save** on the page. You can delete items using the Delete icon. To prevent unwanted deletions, a Confirm Delete dialog box appears in many cases so that you have a chance to confirm or cancel the deletion.

Role and Attribute Visibility Settings

Click the **Settings** drop-down list on the top of the main page to modify user preferences, session settings, user permissions, or debug settings.

- To view the user groups and roles for the administrator, select the **User Preferences** option. Superuser is a special kind of administrator. (For details how to set up these administrator roles, see Create the Administrators, on page 100.)
- Select **Session Settings** to open the Session Settings dialog, select the mode from the **Session Web UI Mode** drop-down list, and click **Modify Session Settings**. You can also click the drop-down arrow of the Mode icon () to view the list of modes. Select the required mode from the list:
  - **Basic**—Basic user mode (the preset choice).
  - **Advanced**—Advanced user mode that exposes the normal attributes.
  - **Expert**—Expert user mode that exposes a set of attributes that are relevant for fine-tuning or troubleshooting the configuration. In most cases, you would accept the default values for these expert attributes and not change them without guidance from the Cisco Technical Assistance Center (TAC). Each Expert mode attribute is marked with a Warning icon on the configuration pages. Each page is clearly marked as being in Expert mode.

Displaying and Modifying Attributes

Many of the web UI pages, such as those for servers, zones, and scopes, include attribute settings that correspond to those you can set using the CLI. (The CLI name equivalents appear under the attribute name.) The attributes are categorized into groups by their function, with the more prominent attributes listed first and the ones less often configured nearer the bottom of the page.

Grouping and Sorting Attributes

On many Advanced mode web UI pages, you can toggle between showing attributes in groups and in alphabetical order. These pages generally open by default in group view so that you can see the attributes in their respective categories. However, in the case of large numbers of attributes, you might want to see the attributes alphabetized. Click **Show A-Z View** to change the page to show the attributes alphabetically. Click **Show Group View** to change the page to show the attributes in groups. You can also expand or collapse the attribute groups in group view by clicking **Expand All** or **Collapse All**. In Expert mode, the Expert mode attributes are alphabetized separately further down the page under the Visibility=3 heading and are all marked with the Warning icon.

Modifying Attributes

You can modify attribute values and unset those for optional attributes. In many cases, these attributes have preset values, which are listed under the Default column on the page. The explicit value overrides the default

one, but the default one is always the fallback. If there is no default value, unsetting the explicit value removes all values for that attribute.

Displaying Attribute Help

For contextual help for an attribute, click the name of the attribute to open a separate popup window.

Left Navigation Pane

The Web UI also provides a navigation pane on the left of the main pages. This navigation pane provides access to objects that are added as part of the various categories. The objects are listed in a tabular format and you can click the object to edit its properties in the main page.

Each object displayed under a category in the pane has a Quick View icon associated with it. The Quick View icon expands to open a dialog box that displays the main details about the object, and provides links (if any) to perform the main actions associated with the object.

By default, the list of objects is displayed in a single column format. However, you can add additional columns in the left pane. To add additional columns for objects, click the gear icon ( ) above the objects table in the left pane, select the desired column names, and then click **Close**. You can save the column format by clicking the **Save Column Format** button.

There are Quick Filter and Advanced Filter options available to filter the objects as needed. To do a quick search for the objects, you can use the Quick Filter option. Click the Filter icon ( ) or select **Quick Filter** from the **Show** drop-down list located above the objects table and then enter the search string in the search bar. The objects are listed as per your search criteria.

You can also use Advanced Filter to filter the objects. Select **Advanced Filter** from the **Show** drop-down list, set the appropriate filter and condition in the Advanced Filter dialog box, and then click **OK**. Once you click OK, the object list on the left pane is filtered as per the filter specified. To save the filter, click **Save As** in the Advanced Filter dialog box, enter the appropriate name in the Save Filter dialog box, and then click **Save**. The saved filter name appears in the Show drop-down list and you can use this filter on that particular object list at any time. You can also set this filter as the default filter by clicking the **Set Default Filter** button.

The user defined filters can be edited or removed. To do this, select **Manage User Defined Filters** from the **Show** drop-down list, select the required user defined filter from the filter list in the Manage User Defined Filters dialog box, and then click **Edit** or **Remove** as required.

Help Pages

The web UI provides a separate window that displays help text for each page. The Help pages provide:

- A context-sensitive help topic depending on which application page you have open.
- A clickable and hierarchical Contents and Index, and a Favorites setting, as tabs on a left-hand pane that you can show or hide.
- A Search facility that returns a list of topics containing the search string, ordered by frequency of appearance of the search string.
- Forward and backward navigation through the history of Help pages opened.
- A Print function.
- A Glossary.

Logging Out

Log out of the web UI by clicking **Log Out** link. You can find the **Log Out** under the gear icon at the top right corner of the application page.

Local Cluster Web UI

The local cluster web UI provides concurrent access to Cisco Prime IP Express user and protocol server administration and configuration. It provides granular administration across servers with permissions you can set on a per element or feature basis. The local cluster web UI is available in three user modes:

- **Basic Mode**— Provides a more simplified configuration for the more frequently configured objects, such as DHCP scopes and DNS zones (see Local Basic Main Menu Page, on page 16).
- **Advanced Mode**— Provides the more advanced configuration method familiar to past users of the Cisco Prime IP Express web UI, with some enhancements (see Local Advanced Main Menu Page, on page 17).
- **Expert Mode** (marked with the icon)-For details on Expert mode, see Role and Attribute Visibility Settings, on page 14.

Change to Basic, Advanced, or Expert mode by clicking the drop-down arrow of the Mode icon ( ) on the toolbar at the top right of the page (see Setting Local User Preferences, on page 18).

Note If you change the IP address of your local cluster machine, see the Note in Configuring Clusters in the Local Web UI, on page 19.

Related Topics

Introduction to the Web-Based User Interfaces, on page 10

Regional Cluster Web UI, on page 19

Local Basic Main Menu Page

The Basic tab activated on the toolbar at the top right corner of the page implies that you are in Basic user mode. Otherwise, click the drop-down arrow of the Mode icon ( ) to view the list of modes and select **Basic**.

You can see the submenu items under the navigation menu by clicking the global navigation icon on the top left corner of the page. To choose a submenu under a navigation menu, place the cursor over the navigation menu item. For example, place the cursor on **Operate** to choose the **Manage Servers**.

Also, you can select any submenu under the required navigation menu and then navigate to the required submenu page from the left pane. For example, place the cursor on **Operate**, choose **Schedule Tasks**. You can see List/Add Scheduled Tasks page along with a left pane that has links to Manage Servers, Manage Clusters, Schedule Tasks, and View Change Log. Click the **Manage Servers** link to view the Manage Servers page.

The Local Basic main menu page provides functions with which you can:

- **Open the dashboard to monitor system health**—Open **Operate** menu and click **Dashboard**. See the "Server Status Dashboard" chapter.

- **Set up a basic configuration by using the Setup interview pages**—Click the **Setup** icon at the top, and select the different tabs in the Setup page. See *Cisco Prime IP Express Quick Start Guide* for more details.
- **Administer users, encryption keys**—Place the cursor on **Administration** menu (for user access options) or **Design** menu (for Security > Keys option). See Managing Administrators, on page 37.
- **Manage the Cisco Prime IP Express protocol servers**—Place the cursor on **Operate** menu and select **Manage Servers** or **Schedule Tasks** option. See Maintaining Servers and Databases, on page 115.
- **Manage clusters**—Place the cursor on **Operate** menu and choose **Manage Clusters** option. See Configuring Server Clusters, on page 70.
- **Configure DHCP**—Place the cursor on **Design** menu and select the options under **DHCP Settings**, **DHCPv4** or **DHCPv6**. See the *"Configuring Scopes and Networks" section in Cisco Prime IP Express 9.0 DHCP User Guide*.
- **Configure DNS**—Place the cursor on **Design** menu and select the options under **Cache DNS** and **Auth DNS**. Place the cursor on **Deploy** menu and select the options under **DNS** and **DNS Updates**. See the *"Managing Zones" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.
- **Manage hosts in zones**—From the **Design** menu, choose **Hosts** under the **Auth DNS** submenu. See the *"Managing Hosts" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.
- **Go to Advanced mode**—Click **Advanced** in the top right corner of the page. See Local Advanced Main Menu Page, on page 17.

Local Advanced Main Menu Page

To switch to Advanced user mode from the Basic user Main Menu page, click the drop-down arrow of the Mode icon ( ) at the top right of the window to view the list of modes and select **Advanced**. Doing so opens another Main Menu page, except that it shows the Advanced user mode functions. To switch back to Basic mode at any time, click next to the Mode icon at the top right of the window and select **Basic**.

The local Advanced mode Main Menu page includes advanced Cisco Prime IP Express functions that are in addition to the ones in Basic mode:

- **Open the dashboard to monitor system health**—Open **Operate** menu and click **Dashboard**. See the "Server Status Dashboard" chapter.
- **Administer users, groups, roles, regions, access control lists (ACLs)**, and **view change logs**—Place the cursor on **Administration** menu (for user access options), **Design** menu (for ACLs) or **Operate** menu (for change logs). See Managing Administrators, on page 37.
- **Manage the Cisco Prime IP Express protocol servers**—Place the cursor on **Operate** menu and select **Manage Servers** or **Schedule Tasks** option. See Maintaining Servers and Databases, on page 115.
- **Manage clusters**—Place the cursor on **Operate** menu and choose **Manage Clusters** option. See Configuring Server Clusters, on page 70.
- **Configure DHCPv4**—Place the cursor on **Design** and select any option under **DHCPv4**. See the *"Configuring Scopes and Networks" section in Cisco Prime IP Express 9.0 DHCP User Guide*.
- **Configure DHCPv6**—Place the cursor on **Design** and select any option under **DHCPv6**. See the *"Managing DHCPv6 addresses" section in Cisco Prime IP Express 9.0 DHCP User Guide*.
- **Configure DNS**—Place the cursor on **Design** menu and select the options under **Cache DNS** and **Auth DNS**. Place the cursor on **Deploy** menu and select the options under **DNS** and **DNS Updates**. See the *"Managing Zones" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.

- **Manage hosts in zones**—From the **Design** menu, choose **Hosts** under the **Auth DNS** submenu. See the *"Managing Hosts" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.
- **Manage IPv4 address space**—Place the cursor on **Design** and select any option under **DHCPv4**. See the *"Managing Address Space" section in Cisco Prime IP Express 9.0 DHCP User Guide.*
- **Configure IPv6 address space**—Place the cursor on **Design** and select any option under **DHCPv6**. See the *"Managing DHCPv6 Addresses" section in Cisco Prime IP Express 9.0 DHCP User Guide*.
- **Go to Basic mode**— Click the drop-down arrow of the Mode icon () at the top right corner of the page and choose **Basic**. See Local Basic Main Menu Page, on page 16.

The Advanced user mode page provides additional functions:

- **View the user role and group data for the logged-in user**—See Role and Attribute Visibility Settings, on page 14.
- **Set your preferred session settings**—See Role and Attribute Visibility Settings, on page 14.
- **Set server debugging**—You can set debug flags for the protocol servers. Set these values only under diagnostic conditions when communicating with the Cisco Technical Assistance Center (TAC).
- **Change your login administrator password**—See Managing Passwords, on page 47.

Setting Local User Preferences

You can maintain a short list of web UI settings through subsequent user sessions. The only difference between the Basic and Advanced or Expert mode user preference pages is that Advanced and Expert modes have additional columns listing the data types and defaults.

You can edit the user preferences by going to **User Preferences** under the **Settings** drop-down list. The user preference attributes to set are:

- **Username**—Username string, with a preset value of **admin**. You cannot modify this field.
- **Web UI list page size**—Adjust the page size by the number of displayed lines in a list; the preset value is 10 lines.
- **Web UI mode**—User mode at startup: Basic, Advanced, or Expert (see Role and Attribute Visibility Settings, on page 14). If unset, the mode defaults to the one set in the CCM server configuration (see Managing Servers, on page 115).
- **Web UI tree page size**—Adjust the page size when displaying a tree view in the web UI.
- **Web UI log page size**—Adjust the page size on log pages.
- **Views**—Specify the DNS view setting at session startup in the web UI or CLI.
- **VPN**—Specify the VPN setting at session startup in the web UI or CLI.
- **Alarm poll interval**—Adjust the alarm poll interval; that is, how often IP Express polls the alarm data from server.
- **Homepage**—Set a page from favorites list as the homepage for the application. By default, Configuration Summary page is set as the homepage. Starting from release 9.0, you can set a page of your choice as the homepage for the application. To do this, add the desired page to the Favorites list (see Navigating the Web UIs, on page 13), select the page name from the Homepage drop-down list, and then click **Modify User Preferences**. You can click the Home icon () on the top left corner of the web UI to go to the homepage.

- **Date format**—Set the date-time format for date-time values in the web UI. A format can be selected from the default list or entered in text form as <date-pattern> <time-pattern>.

  Supported patterns are:

  - Year as "yy", "yyyy"
  - Month as "M", "MM", "MMM", "MMMM"
  - Day as "d", "dd"
  - Hour as "h", "hh", "H", "HH"
  - Minute as "mm"
  - Second as "s", "ss"
  - Delimiters as ":", "-", "/"

You can unset the page size and web UI mode values by checking the check box in the *Unset?* column, next to the attribute. After making the user preference settings, click **Modify User Preferences**.

Configuring Clusters in the Local Web UI

You can define other local Cisco Prime IP Express clusters in the local web UI. The local cluster on the current machine is called the **localhost** cluster. To set up other clusters, choose **Manage Clusters** from **Operate** menu to open the List/Add Clusters page. Note that the **localhost** cluster has the IP address and SCP port of the local machine.

Click the **Add Cluster** icon in the left pane to open the Add Cluster page. At a minimum, you must enter the name and address (IPv4 and/or IPv6) of the remote local cluster. You should also enter the admin name and password, along with possibly the SCP port (if not 1234) of the remote cluster. Click **Add Cluster**. To edit a cluster, click the cluster name in the Clusters pane on the left to open the Edit Cluster page. If you want to use secure access mode, select use-ssl as disabled, optional, or required (optional is the preset value; you need the security library installed if you choose required). Make the changes and then click **Save**.

Note If you change the IP address of your local cluster machine, you must modify the **localhost** cluster to change the address in the ipaddr field. Avoid setting the value to the loopback address (127.0.0.1); if you do, you must also set the actual IP addresses of main and backup servers for DHCP failover and High-Availability (HA) DNS configurations.

Regional Cluster Web UI

The regional cluster web UI provides concurrent access to regional and central administration tasks. It provides granular administration across servers with permissions you can set on a per element or feature basis. After you log into the application, the Home page appears. Regional cluster administration is described in Managing the Central Configuration, on page 65.

Related Topics

Introduction to the Web-Based User Interfaces, on page 10

Local Cluster Web UI, on page 16

Command Line Interface

Using the Cisco Prime IP Express CLI (the **nrcmd** program), you can control your local cluster server operations. You can set all configurable options, as well as start and stop the servers.

Note The CLI provides concurrent access, by at most 14 simultaneous users and processes per cluster.

Tip See the **CLIContents.html** file in the **/docs** subdirectory of your installation directory for details.

The **nrcmd** program for the CLI is located on:

- **Windows**—In the *install-path* \bin directory.
- **Linux**—In the *install-path* /usrbin directory.

On a local cluster, once you are in the appropriate directory, use the following command at the prompt:

```
nrcmd [-C cluster[:port]] [-N user] [-P password] [-h] [-r] [-v] [-b < script | command]
```

- **–C**—Cluster name, preset value **localhost**. Specify the port number with the cluster name while invoking nrcmd to connect to another cluster. See the preceding example.

  The port number is optional if the cluster uses the default SCP port—1234 for local and 1244 for regional. Ensure that you include the port number if the port used is not the default one.

- **–N**—Username. You have to enter the username that you created when first logged into the Web UI.
- **–P**—User password. You have to enter the password that you created for the username.
- The local cluster (**–L**) is implied; use **–R** to open the regional cluster CLI.
- -b < script Process script file of nrcmd commands.
- -h Print this help text.
- -r Login as a read-only user.
- -R Connect to regional.
- -v (or -vv) Report the program version and exit.
- -V Specify the session visibility

Note Cluster defaults to localhost if not specified.

Tip For additional command options, see the **CLIGuide.html** file in /docs.

Note If you change the IP address of your local cluster machine, you must modify the **localhost** cluster to change the address in the *ipaddress* attribute. Do not set the value to 127.0.0.1.

You can also send the output to a file using:

```
nrcmd> session log filename
```

For example:

To send the leases on the DHCP server to a file (leases.txt), use the following commands:

```
nrcmd> session log leases.txt
nrcmd> lease list
```

Note To close a previously opened file, use session log (no filename). This stops writing the output to any file.

To disconnect from the cluster, use **exit**:

```
nrcmd> exit
```

Tip The CLI operates on a coordinated basis with multiple user logins. If you receive a cluster lock message, determine who has the lock and discuss the issue with that person. (See Multiple Users, on page 12.)

Global Search in Prime IP Express

The Local and Regional Web UI in Prime IP Express also provides a global search functionality for the IP addresses or DNS names available in the local clusters. The search interface element is available at the top right corner of the main page.

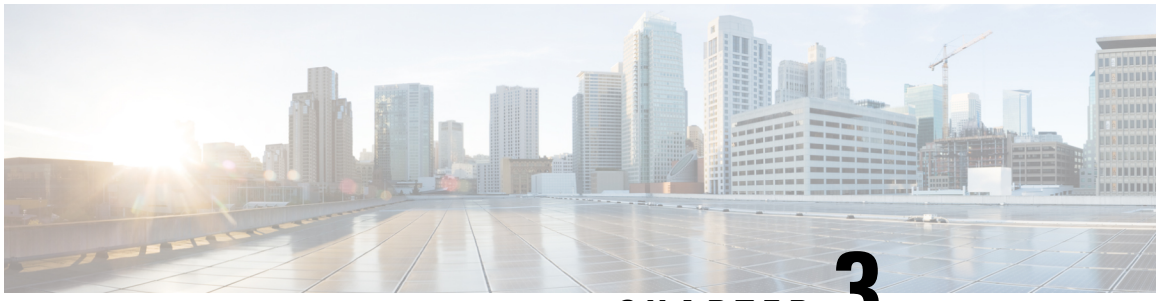
Note To view the search interface element and run the search for IP addresses and DNS names, Cisco Prime IP Express must be licensed with DHCP or DNS, and the DHCP or DNS services must be enabled for the local cluster (in the List/Add Remote Clusters page in Regional Web UI).

The following table shows the typical search results under different scenarios.

Table 2: Typical Search Results

You search for...	With active licenses and services for...	Search Results
An IPv4 address	Only DHCP	The closest matching scope, scope lease or scope reservation

You search for...	With active licenses and services for...	Search Results
An IPv4 address or a DNS FQDN	Only DNS	The related Zone or Resource Record
An IPv6 address	Only DHCP	The closest matching prefix, prefix lease or prefix reservation
An IPv6 address or a DNS FQDN	Only DNS	The related Zone or Resource Record
An IPv4 address, an IPv6 address or a DNS FQDN	Both DHCP and DNS	All of the above, based on the type of address



CHAPTER 3

Server Status Dashboard

The Cisco Prime IP Express server status dashboard in the web user interface (web UI) presents a graphical view of the system status, using graphs, charts, and tables, to help in tracking and diagnosis. These dashboard elements are designed to convey system information in an organized and consolidated way, and include:

- Significant protocol server and other metrics
- Alarms and alerts
- Database inventories
- Server health trends

The dashboard is best used in a troubleshooting desk context, where the system displaying the dashboard is dedicated for that purpose and might be distinct from the systems running the protocol servers. The dashboard system should point its browser to the system running the protocol servers.

You should interpret dashboard indicators in terms of deviations from your expected normal usage pattern. If you notice unusual spikes or drops in activity, there could be communication failures or power outages on the network that you need to investigate.

Opening the Dashboard

Starting from Cisco Prime IP Express 9.0, the Dashboard feature is available on the regional cluster also. It provides System Metrics chart by default. It allows you to display the server specific (DHCP, DNS, and CDNS) charts for various clusters. This can be configured in the Chart Selections page.

To open the dashboard in the web UI, from the **Operate** menu, choose **Dashboard**.

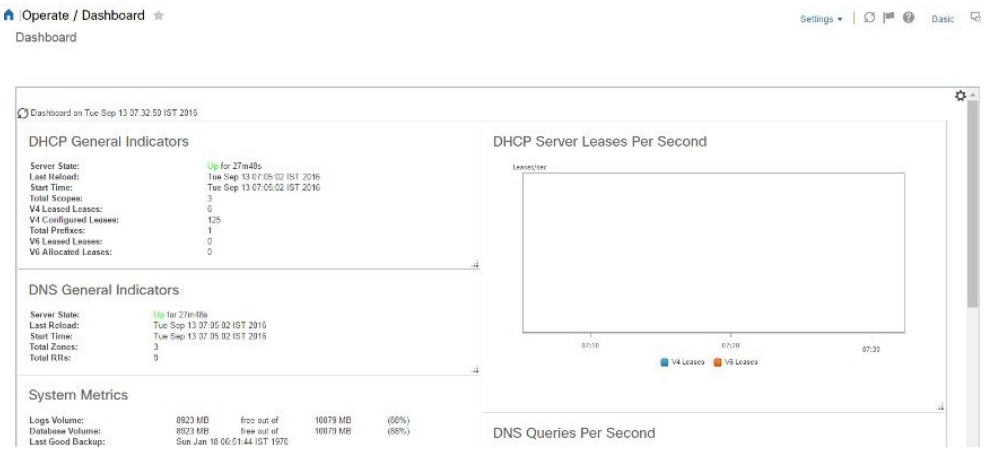
Display Types

Provided you have DHCP and DNS privileges through administrator roles assigned to you, the preset display of the dashboard consists of the following tables (See the table below for an example):

- **System Metrics**—See System Metrics, on page 32.
- **DHCP General Indicators**—See the *"DHCP General Indicators" section in Cisco Prime IP Express 9.0 DHCP User Guide*.
- **DNS General Indicators**—See the *"DNS General Indicators" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.

Tip These are just the preset selections. See Selecting Dashboard Elements to Include, on page 30 for other dashboard elements you can select. The dashboard retains your selections from session to session.

Figure 4: Preset Dashboard Elements



Each dashboard element initially appears as a table or a specific chart type, depending on the element:

- **Table**—See Tables, on page 25.
- **Line chart**—See Line Charts, on page 25.
- **Stacked area chart**—See Stacked Area Charts, on page 27.

General Status Indicators

Note the green box next to each dashboard element name in the above image. This box indicates that the server sourcing the information is functioning normally. A yellow box indicates that server operation is less than optimum. A red box indicates that the server is down. These indicators are the same as for the server health on the Manage Servers page in the regular web UI.

Graphic Indicators for Levels of Alert

Graphed lines and stacked areas in the charts follow a standard color and visual coding so that you can immediately determine key diagnostic indicators at a glance. The charts use the following color and textural indicators:

- **High alerts or warnings**—Lines or areas in red, with a hatched texture.
- **All other indicators**—Lines or areas in various other colors distinguish the data elements. The charts do not use green or yellow.

Magnifying and Converting Charts

If Magnified Chart is the selected Chart Link, you can magnify a chart in a separate window by clicking the chart. In magnified chart view, you can choose an alternative chart type from the one that comes up initially (see Other Chart Types, on page 27).

Note Automatic refresh is turned off for magnified charts. To get the most recent data, click the **Refresh** icon next to the word Dashboard at the top left of the page.

To convert a chart to a table, see the *Displaying Charts as Tables* section. You cannot convert tables to a graphic chart format.

Legends

Each chart initially includes a color-coded legend. Removing the legend renders the graphic chart size relatively larger, which can be helpful if you have many charts displayed. You cannot remove legends in magnified views.

Tables

Dashboard elements rendered as tables have data displayed in rows and columns. The following dashboard elements are preset to consist of (or include) tables:

- System Metrics
- DHCP DNS Updates
- DHCP Address Current Utilization
- DHCP General Indicators
- DNS General Indicators
- Caching DNS General Indicators

Note If you view a table in Expert mode, additional data might appear.

Line Charts

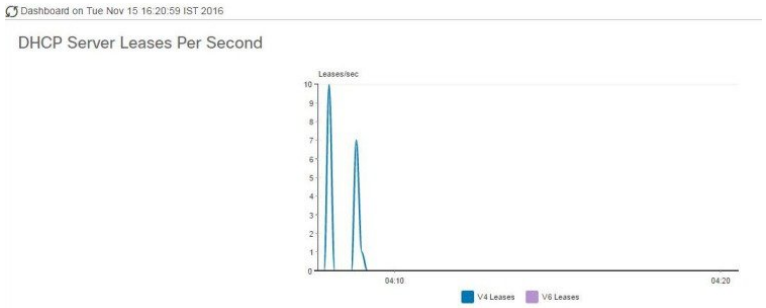
Dashboard elements rendered as line charts can include one or more lines plotted against the x and y axes. The three types of line charts are described in the following table.

Table 3: Line Chart Types

Type of Line Chart	Description	Dashboard Elements Rendered
Raw data line chart	Lines plotted against raw data.	• Java Virtual Machine (JVM) Memory Utilization (Expert mode only) • DHCP Buffer Capacity • DHCP Failover Status (two charts) • DNS Network Errors • DNS Related Servers Errors
Delta line chart	Lines plotted against the difference between two sequential raw data.	• DNS Inbound Zone Transfers • DNS Outbound Zone Transfer
Rate line chart	Lines plotted against the difference between two sequential raw data divided by the sample time between them.	• DHCP Server Request Activity (see the image below) • DHCP Server Response Activity • DHCP Response Latency • DNS Query Responses • DNS Forwarding Errors

Tip To get the raw data for a chart that shows delta or rate data, enter Expert mode, set the Chart Link to Data Table, then click the chart. The Raw Data table is below the Chart Data table.

Figure 5: Line Chart Example



Stacked Area Charts

Dashboard elements rendered as stacked area charts have multiple related metrics plotted as trend charts, but stacked one on top of the other, so that the highest point represents a cumulative value. The values are independently shaded in contrasting colors. (See the image below for an example of the DHCP Server Request Activity chart shown in Figure 5: Line Chart Example, on page 26 rendered as a stacked area chart.)

Figure 6: Stacked Area Chart Example

They are stacked in the order listed in the legend, the left-most legend item at the bottom of the stack and the right-most legend item at the top of the stack. The dashboard elements that are pre-set to stacked area charts are:

- DHCP Server Request Activity
- DHCP Server Response Activity
- DHCP Response Latency
- DNS Outbound Zone Transfers
- DNS Inbound Zone Transfers

Other Chart Types

The other chart types available for you to choose are:

- **Line**—One of the line charts described in Table 3: Line Chart Types, on page 26.
- **Stacked Area**—Charts described in the Stacked Area Charts, on page 27.
- **Pie**—Shows a single percentage pie chart of the data averaged over the time sampled.
- **Bar**—Multiple related current value metrics plotted side by side as groups of bars that show the actual data sampled.
- **Stacked Bar**—Addition total of the actual samples. This chart shows more distinct data points than the stacked area chart.

Tip Each chart type shows the data in distinct ways and in different interpretations. You can decide which type best suits your needs.

Getting Help for the Dashboard Elements

You can open a help window for each dashboard element by clicking the title of the element.

Customizing the Display

To customize the dashboard display, you can:

- Refresh the data and set an automatic refresh interval.
- Expand a chart and render it in a different format.
- Convert a graphic chart to a table.
- Download data to comma-separated value (CSV) output.
- Display or hide chart legends.
- Configure server chart types.
- Reset to default display

Each chart supports:

- Resizing
- Drag and drop to new cell position
- Minimizing
- Closing

Each chart has a help icon with a description of the chart and a detailed help if you click the chart title.

Note The changes made to the dashboard/chart will persist only if you click **Save** in the Dashboard window.

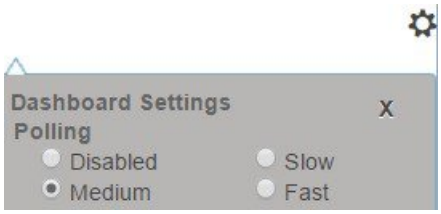
Refreshing Displays

Refresh each display so that it picks up the most recent polling by clicking the **Refresh** icon.

Setting the Polling Interval

You can set how often to poll for data. Click the **Dashboard Settings** icon in the upper-right corner of the dashboard display. There are four options to set the polling interval of the cached data, which polls the protocol servers for updates. (See the image below)

Figure 7: Setting the Chart Polling Interval



You can set the cached data polling (hence, automatic refresh) interval to:

- **Disabled**— Does not poll, therefore does not automatically refresh the data.
- **Slow**— Refreshes the data every 30 seconds.
- **Medium**— Refreshes the data every 20 seconds.
- **Fast** (the preset value)— Refreshes the data every 10 seconds.

Displaying Charts as Tables

You can choose to display a graphic chart as a table when you magnify the chart by clicking it. At the middle of the top of the dashboard display are the controls for the chart links (see the image below)

Figure 8: Specifying Chart Conversion to Table Format

Click the **Data Table** radio button. When you click the chart itself, it opens as a table. The preset display format is Magnified Chart. Displaying Charts as Tables

Exporting to CSV Format

You can dump the chart data to a comma-separated value (CSV) file (such as a spreadsheet) when you magnify the chart by clicking it. In the Chart Link controls at the top of the page (see the above image), click the **CSV Export** radio button, then click the chart. A Save As window appears, where you can specify the name and location of the CSV file.

Displaying or Hiding Chart Legends

You can include or exclude the color-coded legends for charts on the main dashboard page. You might want to remove the legends as you become more familiar with the data and track it on a slightly larger chart display. In the upper-right of the dashboard display are the controls for the legend display (see the image below). The preset value is Visible.

Figure 9: Displaying or Hiding Chart Legends and Selecting Chart

Selecting Dashboard Elements to Include

You can decide how many dashboard elements you want to display on the page. At times, you might want to focus on one server activity only, such as for the DHCP server, and exclude all other metrics for the other servers. In this way, the dashboard becomes less crowded, the elements are larger and more readable. At other times, you might want an overview of all server activities, with a resulting smaller element display.

You can select the dashboard elements to display from the main Dashboard page by clicking **Chart Selections** in the Dashboard Settings dialog. Clicking the link opens the Chart Selection page.

Configuring Server Chart Types

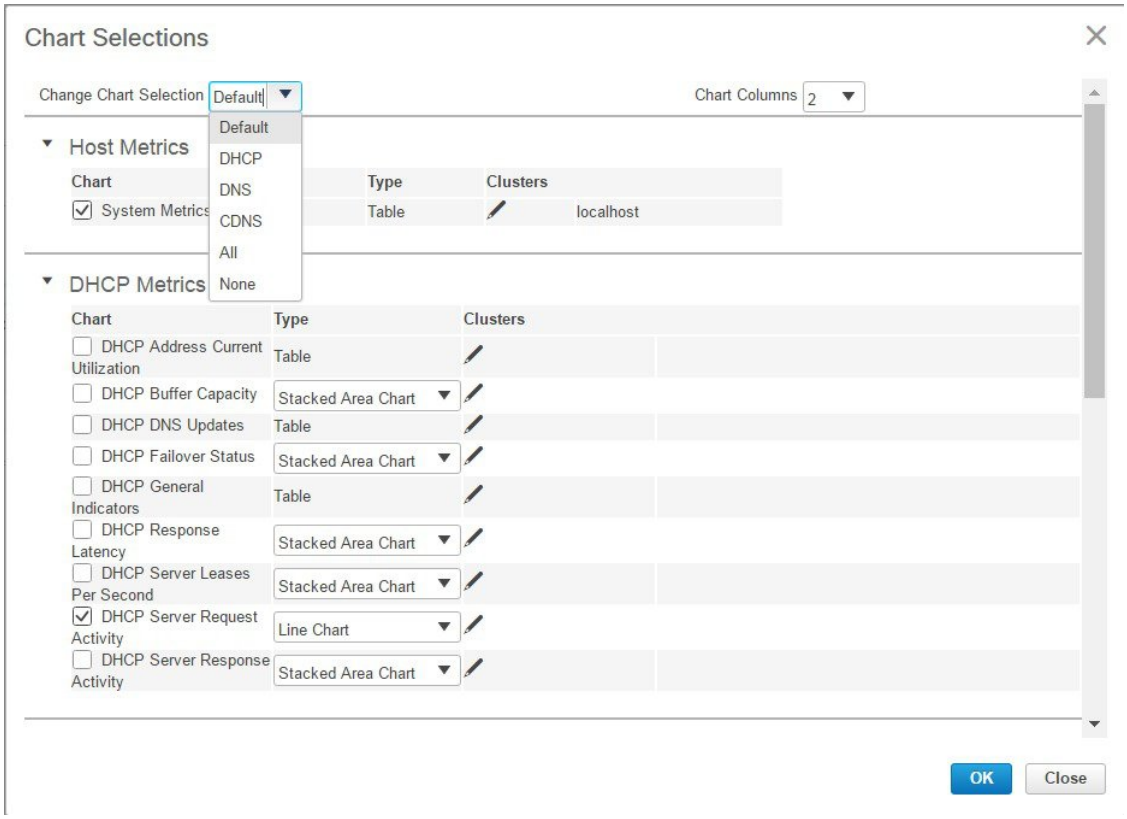
You can set the default chart types on the main dashboard view. You can customize the server charts in the dashboard to display only the specific chart types as default.

To set up default chart type, check the check box corresponding to the Metrics chart that you want to display and choose a chart type from the **Type** drop-down list. The default chart types are consistent and shared across different user sessions (see the image below).

Note You can see either the CDNS or DNS Metrics in the **Dashboard Settings** > **Chart Selection** page based on the service configured on the server.

Tip The order in which the dashboard elements appear in the Chart Selection list does not necessarily determine the order in which the elements will appear on the page. An algorithm that considers the available space determines the order and size in a grid layout. The layout might be different each time you submit the dashboard element selections. To change selections, check the check box next to the dashboard element that you want to display.

Figure 10: Selecting Dashboard Elements



The above image displays the Charts Selection table in the regional web UI. The Clusters column is available only in regional dashboard and it displays the list of local clusters configured. You can add the local cluster by clicking the Edit icon and then by selecting the local cluster name from the Local Cluster List dialog box.

To change selections, check the check box next to the dashboard element that you want to display.

Specific group controls are available in the drop-down list, **Change Chart Selection**, at the top of the page. To:

- Uncheck all check boxes, choose **None**.
- Revert to the preset selections, choose **Default**. The preset dashboard elements for administrator roles supporting DHCP and DNS are:
    - Host Metrics: System Metrics
    - DHCP Metrics: General Indicators
    - DNS Metrics: General Indicators
- Select the DHCP metrics only, choose **DHCP** (see the *"DHCP Metrics" section in Cisco Prime IP Express 9.0 DHCP User Guide*).
- Select the DNS metrics only, choose **DNS** (see the *"Dashboard and Authoritative DNS Metrics" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*).
- Select the DNS metrics only, choose **CDNS** (see the *"Caching DNS Metrics" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*)
- Select all the dashboard elements, choose **All**.

Click **OK** at the bottom of the page to save your choices, or **Cancel** to cancel the changes.

Host Metrics

Host metrics comprise two charts:

- **System Metrics**—See the System Metrics, on page 32.
- **JVM Memory Utilization** (available in Expert mode only).

System Metrics

The System Metrics dashboard element shows the free space on the disk volumes where the Cisco Prime IP Express logs and database directories are located, the date and time of the last server backup, and CPU and memory usage for the various servers. System metrics are available if you choose **Host Metrics**: **System Metrics** in the Chart Selection list.

The resulting table shows:

- **Logs Volume**—Current free space out of the total space on the disk drive where the logs directory is located, with the equivalent percentage of free space.
- **Database Volume**—Current free space out of the total space on the disk drive where the data directory is located, with the equivalent percentage of free space.
- **Last Good Backup**—Date and time when the last successful shadow database backup occurred (or Not Done if it did not yet occur) since the server agent was last started.
- **CPU Utilization** (in seconds), **Memory Utilization** (in kilobytes), and (in Expert mode only) the **VM Utilization** (in kilobytes) and Process ID (**PID**) for the:
  - Cisco Prime IP Express server agent
  - CCM server
  - DNS server
  - DHCP server
  - Web server
  - SNMP server
  - DNS caching server

How to Interpret the Data

The System Metrics data shows how full your disk volumes are getting based on the available free space for the Cisco Prime IP Express logs and data volumes. It also shows if you had a last successful backup of the data files and when that occurred. Finally, it shows how much of the available CPU and memory the Cisco Prime IP Express servers are using. The difference in the memory and VM utilization values is:

- **Memory Utilization**—Physical memory that a process uses, or roughly equivalent to the Resident Set Size (RSS) value in UNIX **ps** command output, or to the Task Manager Mem Usage value in Windows: the number of pages the process has in real memory minus administrative usage. This value includes only the pages that count toward text, data, or stack space, but not those demand-loaded in or swapped out.
- **VM Utilization**—Virtual memory that a process uses, or roughly equivalent to the SZ value in UNIX **ps** command output, or to the Task Manager VM Size value in Windows: the in-memory pages plus the page files and demand-zero pages, but not usually the memory-mapped files. This value is useful in diagnosing how large a process is and if it continues to grow.

Troubleshooting Based on the Results

If you notice the free disk space decreasing for the logs or data directory, you might want to consider increasing the disk capacity or look at the programs you are running concurrently with Cisco Prime IP Express.

JVM Memory Utilization

The Java Virtual Machine (JVM) Memory Utilization dashboard element is available only when you are in Expert mode. It is rendered as a line trend chart that traces the Unused Maximum, Free, and Used bytes of JVM memory. The chart is available if you choose **Host Metrics: JVM Memory Utilization** in the Chart Selection list when you are in Expert mode.

How to Interpret the Data

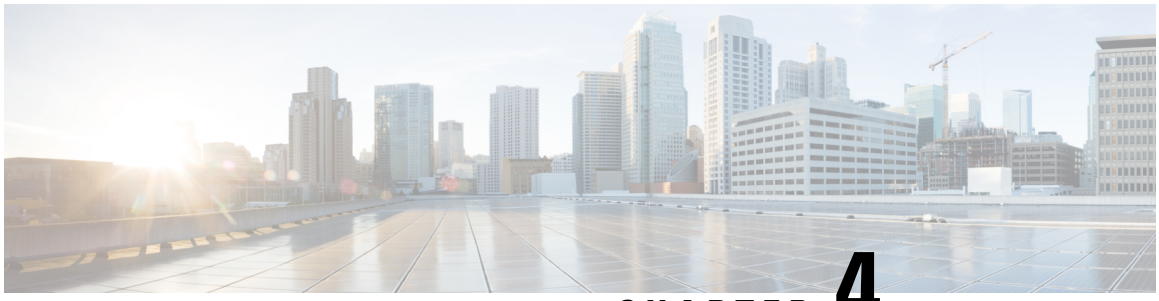
The JVM Memory Utilization data shows how much memory applies to running the dashboard in your browser. If you see the Used byte data spiking, dashboard elements might be using too much memory.

Troubleshooting Based on the Results

If you see spikes in Used memory data, check your browser settings or adjust the polling interval to poll for data less frequently.

PART II

Local and Regional Administration



CHAPTER 4

Managing Administrators

This chapter explains how to set up network administrators at the local and regional clusters. The chapter also includes local and regional cluster tutorials for many of the administration features.

Administrators, Groups, and Roles

The types of functions that network administrators can perform in Cisco Prime IP Express are based on the roles assigned to them. Local and regional administrators can define these roles to provide granularity for the network administration functions. Cisco Prime IP Express predefines a set of base roles that segment the administrative functions. From these base roles you can define further constrained roles that are limited to administering particular addresses, zones, and other network objects.

The mechanism to associate administrators with their roles is to place the administrators in groups that include these roles.

Related Topics

How Administrators Relate to Groups and Roles, on page 38

Administrator Types, on page 38

Roles, Subroles, and Constraints, on page 38

Groups, on page 42

Managing Administrators, on page 46

Managing Passwords, on page 47

Managing Groups, on page 47

Managing Roles, on page 48

How Administrators Relate to Groups and Roles

There are three administrator objects in Cisco Prime IP Express—administrator, group, and role:

- **Administrator**—An account that logs in and that, through its association with one or more administrator groups, can perform certain functions based on its assigned role or roles. At the local cluster, these functions are administering the local Central Configuration Management (CCM) server and databases, hosts, zones, address space, and DHCP. At the regional cluster, these functions administer the regional CCM server and databases, central configuration, and regional address space. An administrator must be assigned to at least one group to be effective.

  Adding administrators is described in Managing Administrators, on page 46.

- **Group**—A grouping of roles. You must associate one or more groups with an administrator, and a group must be assigned at least one role to be usable. The predefined groups that Cisco Prime IP Express provides map each role to a unique group.

  Adding groups is described in Managing Groups, on page 47.

- **Role**—Defines the network objects that an administrator can manage and the functions that an administrator can perform. A set of predefined roles are created at installation, and you can define additional constrained roles. Some of the roles include subroles that provide further functional constraints.

  Adding roles is described in Managing Roles, on page 48.

Administrator Types

There are two basic types of administrators: superusers and specialized administrators:

- **Superuser**—Administrator with unrestricted access to the web UI, CLI, and all features. This administrator type should be restricted to a few individuals. The superuser privileges of an administrator override all its other roles.

  Tip You have to create the superuser and password at installation, or when you first log into the web UI.

- **Specialized**—Administrator created by name to fulfill specialized functions, for example, to administer a specific DNS forward or reverse zone, based on the administrator assigned role (and subrole, if applicable). Specialized administrators, like the superuser, require a password, but must also be assigned at least one administrator group that defines the relevant roles. The CLI provides the **admin** command.

  For an example of creating a local zone or host administrator, see Create the Administrators, on page 100.

Roles, Subroles, and Constraints

A license type is associated with each role-subrole combination. A role-subrole is enabled only if that license is available in that cluster.

You can limit an administrator role by applying constraints. For example, you can use the host-admin base role to create a host administrator, named 192.168.50-host-admin, who is constrained to the 192.168.50.0

subnet. The administrator assigned a group that includes this role then logs in with this constraint in effect. Adding roles and subroles is described in Managing Roles, on page 48.

You can further limit the constraints on roles to read-only access. An administrator can be allowed to read any of the data for that role, but not modify it. However, if the constrained data is also associated with a read-write role, the read-write privilege supersedes the read-only constraints.

Tip An example of adding role constraints is in Create a Host Administrator Role with Constraints, on page 104.

The interplay between DNS and host administrator role assignments is such that you can combine an unconstrained dns-admin role with any host-admin role in a group. For example, combining the dns-admin-readonly role and a host-admin role in a group (and naming the group host-rw-dns-ro) provides full host access and read-only access to zones and RRs. However, if you assign a constrained dns-admin role along with a host-admin role to a group and then to an administrator, the constrained dns-admin role takes precedence, and the administrator privileges at login will preclude any host administration.

Certain roles provide subroles with which you can further limit the role functionality. For example, the local ccm-admin or regional-admin, with just the owner-region subrole applied, can manage only owners and regions. By default, all the possible subroles apply when you create a constrained role.

The predefined roles are described in Table 4: Local Cluster Administrator Predefined and Base Roles , on page 39 (local), and Table 5: Regional Cluster Administrator Predefined and Base Roles , on page 41 (regional).

Table 4: Local Cluster Administrator Predefined and Base Roles

Local Role	Subroles and Active Functionality
addrblock-admin	Core functionality: Manage address block, subnets, and reverse DNS zones (also requires dns-admin); and notify of scope activity. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations.
ccm-admin	Core functionality: Manage access control lists (ACLs), and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets.
cdns-admin	Core functionality: Manage in-memory cache (flush cache and flush cache name). • *security-management*: Manage ACLs and DNSSEC configuration. • *server-management*: Manage DNSSEC configuration, as well as forwarders, exceptions, DNS64, and scheduled tasks, and stop, start, or reload the server.

Local Role	Subroles and Active Functionality
cfg-admin	Core functionality: Manage clusters. • *ccm-management*: Manage the CCM server configuration. • *dhcp-management*: Manage the DHCP server configuration. • *dns-management*: Manage the DNS server configuration. • *cdns-management*: Manage Caching DNS server configuration. • *snmp-management*: Manage the SNMP server configuration.
dhcp-admin	Core functionality: Manage DHCP scopes and templates, policies, clients, client-classes, options, leases, and reservations. • *server-management*: Manage the DHCP server configuration, failover pairs, LDAP servers, extensions, and statistics. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations.
dns-admin	Core functionality: Manage DNS zones and templates, resource records, secondary servers, and hosts. • *security-management*: Manage DNS update policies, ACLs, and encryption keys. • *server-management*: Manage DNS server configurations and zone distributions, synchronize zones and HA server pairs, and push update maps. • *ipv6-management*: Manage IPv6 zones and hosts.
host-admin	Core functionality: Manage DNS hosts. (Note that if an administrator is also assigned a constrained dns-admin role that overrides the host-admin definition, the administrator is not assigned the host-admin role.)

Table 5: Regional Cluster Administrator Predefined and Base Roles

Regional Role	Subroles and Active Functionality
central-cfg-admin	Core functionality: Manage clusters and view replica data. • *dhcp-management*: Manage DHCP scope templates, policies, client-classes, failover pairs, virtual private networks (VPNs), and options; modify subnets; and replicate data. • *ccm-management*: Manage CCM Server configuration • *snmp-management*: Manage SNMP Server configuration. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations. • *cdns-management*: Manage CDNS Server configuration. • *byod-management*: Manage BYOD Server configuration.
central-dns-admin	Core functionality: Manage DNS zones and templates, hosts, resource records, and secondary servers; and create subzones and reverse zones. • *security-management*: Manage DNS update policies, ACLs, and encryption keys. • *server-management*: Synchronize DNS zones and HA server pairs, manage zone distributions, pull replica zone data, and push update maps. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations.
central-host-admin	Core functionality: Manage DNS hosts. (Note that if an administrator is also assigned a constrained central-dns-admin role that overrides the central-host-admin definition, the administrator is not assigned the central-host-admin role.)
regional-admin	Core functionality: Manage licenses and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets. • *security-management*: Manage ACLs and DNSSEC configuration.

Regional Role	Subroles and Active Functionality
regional-addr-admin	Core functionality: Manage address blocks, subnets, and address ranges; generate allocation reports; and pull replica address space data. • *dhcp-management*: Push and reclaim subnets; and add subnets to, and remove subnets from, DHCP failover pairs. • *lease-history*: Query, poll, and trim lease history data. • *subnet-utilization*: Query, poll, trim, and compact subnet utilization data. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations. • *byod-management*: Manage BYOD Server configuration.

Groups

Administrator groups are the mechanism used to assign roles to administrators. Hence, a group must consist of one or more administrator roles to be usable. When you first install Cisco Prime IP Express, a predefined group is created to correspond to each predefined role.

Roles with the same base role are combined. A group with an unconstrained dhcp-admin role and a constrained dns-admin role, does not change the privileges assigned to the dns-admin role. For example, if one of the roles is assigned unconstrained read-write privileges, the group is assigned unconstrained read-write privileges, even though other roles might be assigned read-only privileges. Therefore, to limit the read-write privileges of a user while allowing read-only access to all data, create a group that includes the unconstrained read-only role along with a constrained read-write role. (See Roles, Subroles, and Constraints, on page 38 for the implementation of host-admin and dns-admin roles combined in a group.)

External Authentication Servers

Cisco Prime IP Express includes a RADIUS client component and Active Directory (AD) client component, which are integrated with the authentication and authorization modules of the CCM server. To enable external authentication, you must configure a list of external RADIUS or an AD server at local and regional clusters, and ensure all authorized users are appropriately configured on the respective servers.

When external authentication is enabled, the CCM server handles attempts to log in via the web UI, SDK, or CLI, by issuing a RADIUS request to a RADIUS server or a LDAP request to a AD server that is selected from the configured list. If the corresponding server validates the login request, access is granted, and the CCM server creates an authorized session with the group assignments specified by the RADIUS or the AD server.

Note Any administrators defined in the CCM server's database are ignored when external authentication is enabled. Attempting to log in with these usernames and passwords will fail. To disable external authentication, you must remove or disable all the configured external servers or change the auth-type attribute value to Local.

Tip If all logins fail because the RADIUS servers are inaccessible or misconfigured, use the local.superusers file to create a temporary username and password. See Managing Administrators, on page 46 for more details.

Configuring an RADIUS External Authentication Server

Cisco Prime IP Express administrators must be assigned to one or more administrator groups to perform management functions. When using a RADIUS server for external authentication, these are set as a vendor specific attribute for each user. Using the Cisco vendor id (9), create the Cisco Prime IP Express groups attribute for each administrator, using the format **cnr:groups=**group1, group2, group3.

For example, to assign an administrator to the built-in groups **dhcp-admin-group** and **dns-admin-group**, enter:

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

To assign superuser access privileges, the reserved group name **superusers** is used. To provide superuser privileges to an administrator, enter:

```
cnr:groups=superusers
```

The superuser privileges override all other groups

Note You cannot add, delete, or modify external user names and their passwords or groups using Cisco Prime IP Express. You must use the RADIUS server to perform this configuration.

Adding an RADIUS External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional Web UI

Step 1 From the **Administration** menu, choose **Radius** under the External Authentication submenu. The List/Add Radius Server page is displayed.

Step 2 Click the **Add Radius** icon in the Radius pane, enter the name, IPv4 and/or IPv6 address of the server you want to configure as the external authentication server, and you can set the key attribute which will be used for communicating with this server in the Add External Authentication Server dialog box, and click **Add External Authentication Server**. The CCM server uses the key to set the key-secret attribute which is the secret key shared by client and the server.

Step 3 To enable the external authentication server, check **enabled** check box of the ext-auth attribute in the Edit Authentication Server page, and then click **Save**.

Step 4 Change the auth-type attribute to RADIUS in the Manage Server page, click **Save**, and then restart Cisco Prime IP Express.

CLI Commands

To create an external authentication server, use **auth-server** *name* **create** <*address* | *ip6address*> [*attribute=value ...*] (see the **auth-server** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Deleting an RADIUS External Authentication Server

Local Advanced and Regional Web UI

To delete an RADIUS external authentication server, select the server in the Radius pane, click the **Delete Radius** icon, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

Configuring an AD External Authentication Server

Cisco Prime IP Express administrators must be assigned to one or more administrator groups to perform management functions. When using an AD server for external authentication, these are set as a vendor specific attribute for each user. Using the Cisco vendor id (9), create the Cisco Prime IP Express groups attribute for each administrator, using the format **cnr:groups=***group1*, *group2*, *group3*.

For example, to assign an administrator to the built-in groups **dhcp-admin-group** and **dns-admin-group**, enter:

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

To assign superuser access privileges, the reserved group name **superusers** is used. To provide superuser privileges to an administrator, enter:

```
cnr:groups=superusers
```

The superuser privileges override all other groups.

A group needs to be created to access CPIPE and add the users to that group. Select an user attribute and provide the group information in the format **cnr:group1,group2,..**

To configure an Active Directory (AD) external authentication server:

Step 1 In AD server, create a new group, for example **CPIPE**, with the group scope *Domain Local*.

Step 2 Select a user and click **Add** to a group.

Step 3 In Enter the Object Names window, select **CPIPE** and click **OK**.

Step 4 In AD Server Object windows, select **CPIPE** for the *ad-group-name* attribute and **info** for the *ad-user-attr-map* attribute.

Note You cannot add, delete, or modify external user names and their passwords or groups using Cisco Prime IP Express. You must use the AD server to perform this configuration.

Configuring Kerbero's Realm and KDC

For the Cisco Prime IP Express to communicate with the AD server, the Kerbero's Realm and KDC servers are required. To configure the Kerbero's Realm and KDC servers in Windows and Linux platforms follow the below examples.

If the Cisco Prime IP Express is running on Windows platform (ksetup), define a KDC entry for a realm by running the following command:

ksetup /AddKdc *<RealmName> [KdcName]*

For example, `Ksetup /AddKdc ECNR.COM tm-chn-ecnr-ad.ecnr.com`

To verify, run the following command:

ksetup /dumpstate

The result should be similar to the message below:

```
default realm = partnet.cisco.com (NT Domain)
ECNR.COM:
 kdc = tm-chn-ecnr-ad.ecnr.com
 Realm Flags = 0x0No Realm Flags
No user mappings defined.
```

If the Prime IP Express is running on Linux platform, the changes need to be configured in **krb5.conf** *(/etc/krb5.conf)* file, as shown below:

```
default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 ticket_lifetime = 1d
 default_realm = ECNR.COM
 default_tkt_enctypes = rc4-hmac
 default_tgs_enctypes = rc4-hmac
 dns_lookup_realm = false
 dns_lookup_kdc = false
 forwardable = true
[realms]
 ECNR.COM = {
 kdc = <kdc server host name>
admin_server = <kdc server host name>
 }
[domain_realm]
 .ecnr.com = ECNR.COM
 ecnr.com = ECNR.COM
```

Adding an AD External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu. The List/Add Active Directory Server page is displayed.

Step 2 Click the **Add Active Directory Server** icon in the Active Directory pane, enter the name, hostname of the server, domain you want to configure as the external authentication server, and you can set the base domain, LDAP user attribute map, AD group name which will be used for communicating with this server in the Add Active Directory Server dialog box, and click **Add Active Directory Server**.

Step 3 Change the auth-type attribute to Active Directory in the Manage Server page, click **Save**, and then restart Cisco Prime IP Express.

CLI Commands

To create an external authentication server, use **auth-server** *name* **create** <*address* | *ip6address*> [*attribute=value* ...].

Deleting an AD External Authentication Server

Local Advanced and Regional Web UI

To delete an AD external authentication server, select the server in the Active Directory pane, click the **Delete Active Directory Server** icon, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

Managing Administrators

When you first log in, Cisco Prime IP Express will have one administrator—the superuser account. This superuser can exercise all the functions of the web UI and usually adds the other key administrators. However, ccm-admin and regional-admin administrators can also add, edit, and delete administrators. Creating an administrator requires:

- Adding its name.
- Adding a password.
- Specifying if the administrator should have superuser privileges (usually assigned on an extremely limited basis).
- If not creating a superuser, specifying the group or groups to which the administrator should belong. These groups should have the appropriate role (and possibly subrole) assignments, thereby setting the proper constraints.

Tip If you accidentally delete all the roles by which you can log into Cisco Prime IP Express (those having superuser, ccm-admin, or regional-admin privileges), you can recover by creating a username/password pair in the *install-path* /conf/priv/local.superusers file. You must create this file, have write access to it, and include a line in it with the format *username password*. Use this username and password for the next login session. Note, however, that using the local.superusers file causes reduced security. Therefore, use this file only in emergencies such as when temporarily losing all login access. After you log in, create a superuser account in the usual way, then delete the local.superusers file or its contents. You must create a new administrator account for each individual, to track administrative changes.

Adding Administrators

To add a administrator, do the following:

Local and Regional Web UI

Step 1 From the **Administration** menu, choose **Administrators** under the **User Access** submenu. This opens the List/Add Administrators page (see the Create the Administrators, on page 100 for an example).

Step 2 Click the **Add Administrators** icon in the **Administrators** pane, enter the name in the Name field, enter the password in the Password field, retype the password in the Confirm Password field in the Add Admin dialog box, and then click **Add Admin**.

Step 3 Choose one or more existing groups from the Groups Available list (or whether the administrator should be a superuser) and then click **Save**.

Editing Administrators

To edit an administrator, select the administrator in the Administrators pane, modify the name, password, superuser status, or group membership on the Edit Administrator page, and then click **Save**. The active group or groups should be in the Selected list.

Deleting Administrators

To delete an administrator, select the administrator in the Administrators pane, click the **Delete Administrators** icon, and then confirm or cancel the deletion.

Managing Passwords

Passwords are key to administrator access to the web UI and CLI. In the web UI, you enter the password on the Login page. In the CLI, you enter the password when you first invoke the **nrcmd** program. The local or regional CCM administrator or superuser can change any administrator password.

You can prevent exposing a password on entry. In the web UI, logging in or adding a password never exposes it on the page, except as asterisks. In the CLI, you can prevent exposing the password by creating an administrator, omitting the password, then using **admin** *name* **enterPassword**, where the prompt displays the password as asterisks. You can do this instead of the usual **admin** *name* **set password** command that exposes the password as plain text.

Administrators can change their own passwords on clusters. If you want the password change propagated from the regional server to all local clusters, log into the regional cluster. First ensure that your session admin-edit-mode is set to synchronous, and then update your password.

Note The password should not be more than 255 characters long.

Managing Groups

A superuser, ccm-admin, or regional-admin can create, edit, and delete administrator groups. Creating an administrator group involves:

- Adding its name.
- Adding an optional description.
- Choosing associated roles.

Adding Groups

To add a group, do the following:

Local Advanced and Regional Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu. This opens the List/Add Administrator Groups page (see the Create a Group to Assign to the Host Administrator, on page 105 for an example).

Step 2 Click the **Add Groups** icon in the Groups pane, enter a name and an optional description in the Add CCMAdminGroup dialog box, and then click **Add CCMAdminGroup**.

Step 3 Choose one or more existing roles from the **Roles Available** list and then click **Save**.

Editing Groups

To edit a group, click the name of the group that you want to edit in the Groups pane to open the Edit Administrator Group page. You can modify the name, description, or role membership in this page. You can view the active roles in the Selected list.

Deleting Groups

To delete a group, select the group in the Groups pane, click the **Delete Groups** icon, and then confirm the deletion. Click **Cancel** in the confirmation window to cancel the deletion.

Managing Roles

A superuser, ccm-admin, or regional-admin administrator can create, edit, and delete administrator roles. Creating an administrator role involves:

- Adding its name.
- Choosing a base role.
- Possibly specifying if the role should be unconstrained, or read-only.
- Possibly adding constraints.
- Possibly assigning groups.

Adding Roles

To add a role, do the following:

Local and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu. This opens the List/Add Administrator Roles page.

Step 2 Click the **Add Role** icon in the Roles pane and enter a name and a base role in the Add Roles dialog box, and then click **Add Role**.

Step 3 On the List/Add Administrator Roles page, specify any role constraints, subrole restrictions, or group selections, then click **Save**.

Editing Roles

To edit a role, select the role in the Roles pane, then modify the name or any constraints, subrole restrictions, or group selections on the Edit Administrator Role page. The active subroles or groups should be in the Selected list. Click **Save**.

Deleting Roles

To delete a role, select the role in the Roles pane, click the **Delete Role** icon, and then confirm the deletion.

Note You cannot delete the default roles.

CLI Commands

To add and edit administrator roles, use **role** *name* **create** *base-role* [*attribute=value*] (see the **role** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions). The base roles have default groups associated with them. To add other groups, set the *groups* attribute (a comma-separated string value).

Granular Administration

Granular administration prevents unauthorized users from accidentally making a change on zones, address blocks, subnets, and router interfaces. It also ensures that only authorized users view or modify specific scopes, prefixes, and links. Granular administration constraints administrators to specific set of scopes, prefixes, and links. A constrained administrator can view or make changes to authorized scope, prefix, and link objects only. The CCM server uses owner and region constraints to authorize and filter IPv4 address space objects, and DNS zone related objects (CCMZone, CCMReverseZone, CCMSecondaryZone, CCMRRSet, and CCMHost). The zones are constrained by owners and regions. Owner or region attributes on the CCMSubnet control access to scopes. Also, owner or region attributes on the Prefix and Link objects control access to prefixes and links.

Local Advanced and Regional Web UI

Step 1 From the **Administration** menu, choose **Roles** to open the List/Add Administrator Roles page.

Step 2 Click the **Add Role** icon in the Roles pane, enter a name for the custom role, for example, my-dhcp, and choose **dhcp-admin** from the Role drop-down list and click **Add Role**.

Step 3 Click **True** or **False** radio button as necessary, on the Add DHCP Administrator Role page.

Step 4 Choose the required sub roles in the Available field and move them to the Selected field.

Step 5 Click **Add Constraint**.

a) On the Add Role Constraint page, modify the fields as necessary.

b) Click **Add Constraint**. The constraint must have an index number of 1.

Step 6 Click **Save**.

The name of the custom role appears on the list of roles in the List/Add Administrator Roles page.

Related Topics

Scope-Level Constraints, on page 50
Prefix-Level Constraints, on page 51
Link-Level Constraints, on page 52

Scope-Level Constraints

A dhcp admin user can view or modify a scope if any of the following conditions is met:

- Owner of the subnet for the scope matches the dhcp-admin owner.
- Region of the subnet for the scope matches the region role constraints.
- Owner or region of the parent address block matches the dhcp-admin owner or region role constraints. Note that the most immediate parent address block that has owner or region defined takes precedence.

The following conditions are also valid:

- If the matching owner or region constraint is marked as read-only, you can only view the scope.
- If a scope has a primary network defined, the primary subnet and its parent address block owner or region constraints override secondary subnets.
- If no parent subnet or address block defines owner or region constraints, then you can access the scope.
- If you are an unconstrained dhcp-admin user, you can have access to all scopes.

Note These hierarchical authorization checks for dhcp-admin owner/region constraints are applicable to scopes, subnets, and parent address blocks. Identical hierarchical authorization checks for addrblock-admin owner/region constraints apply to address blocks and subnets. If you have dhcp-admin and the addrblock-admin privileges, you can access address blocks and subnets, if either of the roles allow access.

Examples of Scope-Level Constraints:

```
Parent CCMAddrBlock 10.0.0.0/8 has owner 'blue' set.
    Scope 'A' has subnet 10.0.0.0/24 has parent CCMSubnet with owner 'red'.
    Scope 'B' has subnet 10.0.1.0/24 has parent CCMSubnet with no owner set.
    Scope 'C' has subnet 10.10.0.0/24 has parent CCMSubnet with owner 'green' and
primary-subnet 10.0.0.0/24.
    Scope 'D' has subnet 100.10.0.0/24 has parent CCMSubnet with owner unset, and no parent
 block.

    Scope 'A' owner is 'red'.
    Scope 'B' owner is 'blue'.
```

```
    Scope 'C' owner is 'red'.
    Scope 'D' owner is unset. Only unconstrained users can access this scope.
```

Local Advanced Web UI

To add scopes, do the following:

Step 1 From the **Design** menu, choose **Scopes** under the **DHCPv4** submenu to open the List/Add DHCP Scopes.

Step 2 Click the **Add Scopes** icon in the Scopes pane, enter a name, subnet, primary subnet, choose policy, enter a selection-tag-list, and select the scope template in the Add DHCP Scope dialog box.

Step 3 Click **Add DHCP Scope**. The List/Add DHCP Scopes page appears.

Step 4 Enter values for the fields or attributes as necessary.

Step 5 To unset any attribute value, check the check box in the **Unset?** column, then click **Unset Fields** at the bottom of the page.

Step 6 Click **Save** to add scope or **Revert** to cancel the changes.

Tip If you add new scope values or edit existing ones, click **Save** to save the scope object.

Prefix-Level Constraints

You can view or modify a prefix, if you have either of the following:

- The ipv6-management subrole of the dhcp-admin, or addrblock-admin role on the local cluster.
- The central-cfg-admin, or regional-addr-admin role on the regional cluster.

You can view or modify a prefix if any of the following conditions is true:

- The owner or region of the parent link matches the owner or region role constraints defined for you.
- The owner or region of this prefix matches the owner or region role constraints defined for you.
- The owner or region of the parent prefix matches the owner or region role constraints defined for you.

You can view or modify a prefix if any of the following conditions is true:

- If the matching owner or region constraint for you is marked as read-only, then you can only view the prefix.
- If the prefix references a parent link, the link owner or region constraints is applicable if the link owner or region constraints set.
- If no parent link or prefix defines any owner or region constraints, then you can access this prefix only if owner or region role constraints are not defined for you.
- If you are an unconstrained user, then you have access to all.

Examples of Prefix-Level constraints:

```
Link 'BLUE' has owner 'blue' set.
    Parent Prefix 'GREEN' has owner 'green' set.
    Prefix 'A' has owner 'red' set, no parent prefix, and no parent link.
    Prefix 'B' has owner 'yellow' set, parent Prefix 'GREEN' and parent link 'BLUE'.
```

```
Prefix 'C' has no owner set, parent prefix 'GREEN', and no parent link.
Prefix 'C' has no owner set, no parent prefix, and no parent link.

Prefix 'A' owner is 'red'.
Prefix 'B' owner is 'blue'.
Prefix 'C' owner is 'green'.
Prefix 'D' owner is unset. Only unconstrained users can access this prefix.
```

Local Advanced and Regional Web UI

To view unified v6 address space, do the following:

Step 1 From the **Design** menu, choose **Address Tree** under the **DHCPv6** submenu to open the DHCP v6 Address Tree page.

Step 2 View a prefix by adding its name, address, and range, then choosing a DHCP type and possible template (see the *"Viewing IPv6 Address Space" section in Cisco Prime IP Express 9.0 DHCP User Guide*).

Step 3 Choose the owner from the owner drop-down list.

Step 4 Choose the region from the region drop-down list.

Step 5 Click **Add Prefix**. The newly added Prefix appears on the DHCP v6 Address Tree page.

Local Advanced and Regional Web UI

To list or add DHCP prefixes, do the following:

Step 1 From the **Design** menu, choose **Prefixes** under the **DHCPv6** submenu to open the List/Add DHCP v6 Prefixes page.

Step 2 Click the **Add Prefixes** icon in the Prefixes pane, enter a name, address, and range for the prefix, then choose the DHCP type and possible template.

Step 3 Choose the owner from the owner drop-down list.

Step 4 Choose the region from the region drop-down list.

Step 5 Click **Add IPv6 Prefix**. The newly added Prefix appears on the List Prefixes page.

Link-Level Constraints

You can view or modify a link if:

- You are authorized for the ipv6-management subrole of the dhcp-admin or addrblock-admin role on the local cluster, or the central-cfg-admin or regional-addr-admin role on the regional cluster.
- The owner or region of the link matches the owner or region role constraints defined for you.
- No owner or region is defined for the link, and only if no owner or region role constraints are defined for you.

If you are an unconstrained user, then you have access to all links.

The following is an example of Link Level Constraints:

```
Link 'BLUE' has owner 'blue' set.
Link 'ORANGE' has owner unset.
```

```
Link 'BLUE' owner is 'blue'.
Link 'ORANGE' owner is unset. Only unconstrained users can access this link.
```

Local Advanced and Regional Web UI

To add links, do the following:

Step 1 From the **Design** menu, choose **Links** under the **DHCPv6** submenu to open the List/Add DHCP v6 Links page.

Step 2 Click the **Add Links** icon in the Links pane, enter a name, then choose the link type, and enter a group.

Step 3 Click **Add Link**. The newly added DHCPv6 Link appears on the List/Add DHCP v6 Links page.

Centrally Managing Administrators

As a regional or local CCM administrator, you can:

- Create and modify local and regional cluster administrators, groups, and roles.
- Push administrators, groups, and roles to local clusters.
- Pull local cluster administrators, groups, and roles to the central cluster.

Each of these functions involves having at least one regional CCM administrator subrole defined. The following table describes the subroles required for these operations.

Table 6: Subroles Required for Central Administrator Management

Central Administrator Management Action	Required Regional Subroles
Create, modify, push, pull, or delete administrators	authentication
Create, modify, push, pull, or delete groups or roles	authorization
Create, modify, push, pull, or delete groups or roles with associated owners or regions	authorization owner-region
Create, modify, push, pull, or delete external authentication servers	authentication

Related Topics

Pushing and Pulling Administrators, on page 53

Pushing and Pulling Groups, on page 58

Pushing and Pulling Roles, on page 59

Pushing and Pulling Administrators

You can push administrators to, and pull administrators from local clusters on the List/Add Administrators page in the regional cluster web UI.

You can create administrators with both local and regional roles at the regional cluster. However, you can push or pull only associated local roles, because local clusters do not recognize regional roles.

Related Topics

Pushing Administrators to Local Clusters, on page 54
Pushing Administrators Automatically to Local Clusters , on page 54
Pulling Administrators from the Replica Database, on page 55

Pushing Administrators to Local Clusters

Pushing administrators to local clusters involves choosing one or more clusters and a push mode.

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Administrators**.

Step 2 On the List/Add Administrators Page, click the **Push All** icon in the **Administrators** pane to push all the administrators listed on the page. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode by clicking one of the Data Synchronization Mode radio buttons. If you are pushing all the administrators, you can choose Ensure, Replace, or Exact. If you are pushing a single administrator, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing administrator data at the local cluster. You would choose Exact only if you want to create an exact copy of the administrator database at the local cluster, thereby deleting all administrators that are not defined at the regional cluster.

Step 4 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 5 Click **Push Data to Clusters**.

Step 6 On the View Push Data Report dialog box, view the push details, then click **OK** to return to the List/Add Administrators page.

Pushing Administrators Automatically to Local Clusters

You can automatically push the new user name and password changes from the regional cluster to the local cluster. To do this, you must enable the synchronous edit mode in the regional cluster. The edit mode is set for the current Web UI session, or set as default for all users is set in the CCM Server configuration.

When synchronous mode is set, all the subsequent changes to user name and password are synchronized with local clusters. You can modify your password on the regional server, and this change is automatically propagated to local clusters.

If you are an admin user, you can make multiple changes to the user credentials on the regional cluster. All these changes are automatically pushed to local clusters.

Regional Basic and Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under Servers submenu to open the Manage Servers page.

Step 2 Click the **Local CCM Server** link on the Manage Servers pane to open the Edit CCM Server page.

Step 3 Choose the synchronous radio buttons for the regional edit mode values for admin, dhcp, and dns.

Step 4 Choose the webui mode value from the webui-mode drop-down list.

Step 5 Enter the idle-timeout value.

Step 6 To unset any attribute value, check the check box in the Unset? column, then click **Unset Fields** at the bottom of the page. To unset the attribute value or to change it, click **Save**, or **Cancel** to cancel the changes.

Note Enter values for the attributes marked with asterisks because they are required for CCM server operation. You can click the name of any attribute to open a description window for the attribute.

Connecting to CLI in Regional Mode

You must connect to the CLI in Regional Mode. The -R flag is required for regional mode. To set the synchronous edit mode:

```
nrcmd-R> session set admin-edit-mode=synchronous
```

Pulling Administrators from the Replica Database

Pulling administrators from the local clusters is mainly useful only in creating an initial list of administrators that can then be pushed to other local clusters. The local administrators are not effective at the regional cluster itself, because these administrators do not have regional roles assigned to them.

When you pull an administrator, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Administrators** under the **User Access** submenu.

Step 2 On the List/Add Administrators page, click **Pull Data** on the**Administrators** pane. This opens the Select Replica Admin Data to Pull dialog box.

Step 3 Click the **Replica** icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data, on page 73.)

Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing administrator properties already defined at the regional cluster by choosing Ensure, or create an exact copy of the administrator database at the local cluster by choosing Exact (not recommended).

Step 5 Click **Pull Core Administrators** next to the cluster, or expand the cluster name and click **Pull Administrator** to pull an individual administrator in the cluster.

Step 6 On the Select Replica Admin Data to Pull dialog box, view the change set data, then click **OK**. You return to the List/Add Administrators page with the pulled administrators added to the list.

Note If you do not have a regional cluster and would like to copy administrators, roles, or groups from one local cluster to another, you can export them and then reimport them at the target cluster by using the cnr_exim tool (see the Using the cnr_exim Data Import and Export Tool, on page 154). However, the tool does not preserve the administrator passwords, and you must manually reset them at the target cluster. It is implemented this way to maintain password security. The export command is:

cnr_exim -c admin -x -e *outputfile*.**txt**

Pushing and Pulling External Authentication Servers

You can push all external authentication servers to local cluster or pull the external authentication server data from the local cluster on the List/Add RADIUS Server page or List/Add Active Directory Server page in the regional web UI.

Pushing RADIUS External Authentication Servers

To push external authentication servers to the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Radius** under the **External Authentication** submenu to view the List/Add RADIUS Server page in the regional web UI.

Step 2 Click **Push All** icon in the Radius pane to push all the external authentication servers listed on the page, or **Push** to push an individual external authentication server. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the external authentication servers, you can choose Ensure, Replace, or Exact.
- If you are pushing a single external authentication server, you can choose Ensure or Replace.

In both the above cases, Ensure is the default mode.

Choose Replace only if you want to replace the existing external authentication server data at the local cluster. Choose Exact only if you want to create an exact copy of the external authentication server data at the local cluster, thereby deleting all external authentication servers that are not defined at the regional cluster.

Step 4 Click **Push Data to Clusters**.

Pulling RADIUS External Authentication Servers

To pull the external authentication server data from the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Radius** under the **External Authentication** submenu to view the List/Add Radius Server page in the regional web UI.

Step 2 On the List/Add Radius Server page, click **Pull Data** on the **Radius** pane. This opens the Select Replica External Authentication Server Data to Pull dialog box.

Step 3 Click the **Replica** icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data, on page 73.)

Step 4 Choose a replication mode using one of the Mode radio buttons.

Leave the default Replace mode enabled, unless you want to preserve any existing external authentication server properties at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the external authentication server data at the local cluster by choosing Exact.

Step 5 Click **Pull All External Authentication Servers** next to the cluster.

Step 6 On the Report Pull Replica Authentication servers page, view the pull details, then click **Run**.

On the Run Pull Replica Authentication servers page, view the change set data, then click **OK**. You return to the List/Add Authentication Server page with the pulled external authentication servers added to the list.

Pushing AD External Authentication Servers

To push external authentication servers to the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu to view the List/Add Active Directory Server page in the regional web UI.

Step 2 Click **Push All** on the **Active Directory** pane to push the external authentication server. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the external authentication servers, you can choose Ensure, Replace, or Exact.
- If you are pushing a single external authentication server, you can choose Ensure or Replace.

  In both the above cases, Ensure is the default mode.

Choose Replace only if you want to replace the existing external authentication server data at the local cluster. Choose Exact only if you want to create an exact copy of the external authentication server data at the local cluster, thereby deleting all external authentication servers that are not defined at the regional cluster.

Step 4 Click **Push Data to Clusters**.

Pulling AD External Authentication Servers

To pull the AD external authentication server data from the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu to view the List/Add Active Directory Server page in the regional web UI.

Step 2 On the List/Add Active Directory Server page, click **Pull Data** on the **Active Directory** pane. This opens the Select Replica External Authentication Server Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster (For the automatic replication interval, see the Replicating Local Cluster Data, on page 73).

Step 4 Choose a replication mode using one of the Mode radio buttons.

Leave the default Replace mode enabled, unless you want to preserve any existing external authentication server properties at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the external authentication server data at the local cluster by choosing Exact.

Step 5 Click **Pull All External Authentication Servers** next to the cluster.

Step 6 On the Report Pull Replica Authentication servers page, view the pull details, and then click **Run**.

On the Run Pull Replica Authentication servers page, view the change set data, and then click **OK**. You return to the List/Add Authentication Server page with the pulled external authentication servers added to the list.

Pushing and Pulling Groups

Pushing and pulling groups is vital in associating administrators with a consistent set of roles at the local clusters. You can push groups to, and pull groups from, local clusters on the List/Add Administrator Groups page in the regional cluster web UI.

Related Topics

Pushing Groups to Local Clusters, on page 58

Pulling Groups from the Replica Database, on page 58

Pushing Groups to Local Clusters

Pushing groups to local clusters involves choosing one or more clusters and a push mode.

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu.

Step 2 On the List/Add Administrator Groups page, click the **Push All** icon on Groups pane to push all the groups listed on the page, or **Push** to push an individual group. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the groups, you can choose Ensure, Replace, or Exact. If you are pushing a single group, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing group data at the local cluster. You would choose Exact only if you want to create an exact copy of the group data at the local cluster, thereby deleting all groups that are not defined at the regional cluster.

Step 4 By default, the associated roles and owners are pushed along with the group. Roles are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, uncheck the respective check box.

Step 5 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 6 Click **Push Data to Clusters**.

Step 7 On the View Push Group Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Groups page.

Pulling Groups from the Replica Database

Pulling administrator groups from the local clusters is mainly useful only in creating an initial list of groups that can then be pushed to other local clusters. The local groups are not useful at the regional cluster itself, because these groups do not have regional roles assigned to them.

When you pull a group, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However,

to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu.

Step 2 On the List/Add Administrator Groups page, click the **Pull Data** icon on the **Groups** pane. This opens the Select Replica CCMAdminGroup Data to Pull dialog box.

Step 3 Click the **Replica** icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data, on page 73.)

Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing group properties at the local cluster by choosing Ensure, or create an exact copy of the group data at the local cluster by choosing Exact (not recommended).

Step 5 Click **Pull Core Groups** next to the cluster, or expand the cluster name and click **Pull Group** to pull an individual group in the cluster.

Step 6 On the Report Pull Replica Groups page, view the pull details, then click **Run**.

Step 7 On the Run Pull Replica Groups page, view the change set data, then click **OK**. You return to the List/Add Administrator Groups page with the pulled groups added to the list.

Pushing and Pulling Roles

You can push roles to, and pull roles from, local clusters on the List/Add Administrator Roles page in the regional cluster web UI. You can also push associated groups and owners, and pull associated owners, depending on your subrole permissions (see Table 6: Subroles Required for Central Administrator Management , on page 53).

Related Topics

Pushing Roles to Local Clusters, on page 59

Pulling Roles from the Replica Database, on page 60

Pushing Roles to Local Clusters

Pushing administrator roles to local clusters involves choosing one or more clusters and a push mode.

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu.

Step 2 On the List/Add Administrator Roles page, click the **Push All** icon in the Roles pane to push all the roles listed on the page, or **Push** to push an individual role. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the roles, you can choose Ensure, Replace, or Exact. If you are pushing a single role, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing role data at the local cluster. You would choose Exact only if you want to create an exact copy of the role data at the local cluster, thereby deleting all roles that are not defined at the regional cluster.

Step 4 By default, the associated groups and owners are pushed along with the role. Groups are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, uncheck the respective check box:

- If you disable pushing associated groups and the group does not exist at the local cluster, a group based on the name of the role is created at the local cluster.
- If you disable pushing associated owners and the owner does not exist at the local cluster, the role will not be configured with its intended constraints. You must separately push the group to the local cluster, or ensure that the regional administrator assigned the owner-region subrole has pushed the group before pushing the role.

Step 5 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 6 Click **Push Data to Clusters**.

Step 7 On the View Push Role Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Roles page.

Pulling Roles from the Replica Database

Pulling administrator roles from the local clusters is mainly useful only in creating an initial list of roles that can then be pushed to other local clusters. The local roles are not useful at the regional cluster itself.

When you pull a role, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu.

Step 2 On the List/Add Administrator Roles page, click the **Pull Data** icon in the **Roles** pane. This opens the Select Replica Administrator Role Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data, on page 73.)

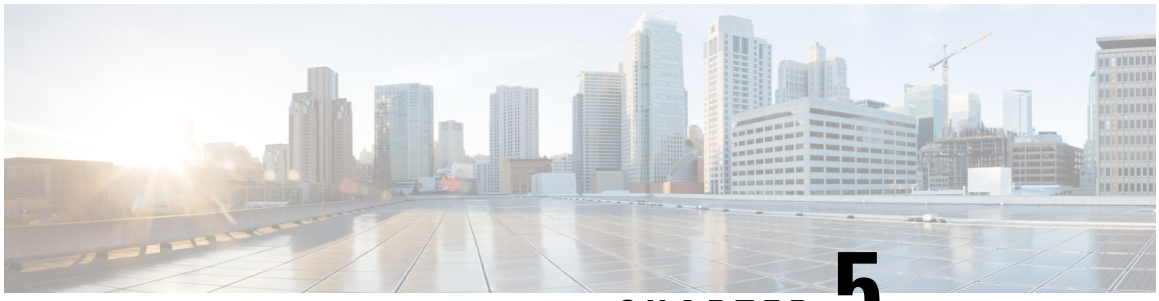
Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing role properties at the local cluster by choosing Ensure, or create an exact copy of the role data at the local cluster by choosing Exact (not recommended).

Step 5 If you have the owner-region subrole permission, you can decide if you want to pull all the associated owners with the role, which is always in Ensure mode. This choice is enabled by default.

Step 6 Click **Pull Core Roles** next to the cluster, or expand the cluster name and click **Pull Role** to pull an individual role in the cluster.

Step 7 On the Report Pull Replica Roles page, view the pull details, then click **Run**.

Step 8 On the Run Pull Replica Roles page, view the change set data, then click **OK**. You return to the List/Add Administrator Roles page with the pulled roles added to the list.



CHAPTER 5

Managing Owners and Regions

This chapter explains how to configure owners and regions that can be applied to DHCP address blocks, subnets, prefixes, links, and zones.

Managing Owners

You can create owners to associate with address blocks, subnets, prefixes, links, and zones. You can list and add owners on a single page. Creating an owner involves creating a tag name, full name, and contact name.

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Owners** under the **Settings** submenu to open the List/Add Owners page. The regional cluster includes pull and push functions also.

Step 2 Click the **Add Owners** icon in the Owners pane on the left. This opens the Add Owner page.

Step 3 Enter a unique owner tag.

Step 4 Enter an owner name.

Step 5 Enter an optional contact name.

Step 6 Click **Add Owner**.

Step 7 To edit an owner, click its name in the Owners pane on the left.

CLI Commands

Use **owner** *tag* **create** *name* [*attribute*=*value*] to create an owner. For example:

```
nrcmd> owner owner-1 create "First Owner" contact="Contact at owner-1"
```

Managing Regions

You can create regions to associate with address blocks, subnets, prefixes, links, and zones. You can list and add regions on a single page. Creating a region involves creating a tag name, full name, and contact name.

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Regions** under the **Settings** submenu to open the List/Add Regions page. The regional cluster includes pull and push functions also.

Step 2 Click the **Add Regions** icon in the Regions pane on the left.

Step 3 Enter a unique region tag.

Step 4 Enter a region name.

Step 5 Enter an optional contact name.

Step 6 Click **Add Region**.

Step 7 To edit a region, click its name in the Regions pane on the left.

CLI Commands

Use **region** *tag* **create** *name* [*attribute=value*]. For example:

```
nrcmd> region region-1 create "Boston Region" contact="Contact at region-1"
```

Centrally Managing Owners and Regions

As a regional or local CCM administrator, you can:

- Push owners and regions to local clusters.
- Pull local cluster owners and regions to the central cluster.

Each of these functions involves having at least one regional CCM administrator subrole defined (see Roles, Subroles, and Constraints, on page 38).

The following table describes the subroles required for these operations.

Table 7: Subroles Required for Central Administrator Management

Central Administrator Management Action	Required Regional Subroles
Create, modify, pull, push, or delete owners or regions	owner-region

Related Topics

Pushing and Pulling Owners or Regions, on page 63

Pushing and Pulling Owners or Regions

You can push owners or regions to, and pull them from, local clusters on the List/Add Owners page or List/Add Regions page, respectively, in the regional cluster web UI.

Related Topics

Pushing Owners or Regions to Local Clusters, on page 63

Pulling Owners and Regions from the Replica Database, on page 63

Pushing Owners or Regions to Local Clusters

Pushing owners or regions to local clusters involves choosing one or more clusters and a push mode.

Regional Web UI

Step 1 From the **Administration** menu, choose **Owners** or **Regions** under the **Settings** submenu.

Step 2 On the List/Add Owners or List/Add Regions page, click the **Push All** icon in the left pane, or click **Push** at the top of the Edit Owner page or Edit Region page, for a particular owner or region. This opens the Push Owner or Push Region page.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the owners or regions, you can choose Ensure, Replace, or Exact.
- If you are pushing a single owner or region, you can choose Ensure or Replace.

  In both the above cases, Ensure is the default mode.

  Choose Replace only if you want to replace the existing owner or region data at the local cluster. Choose Exact only if you want to create an exact copy of the owner or region data at the local cluster, thereby deleting all owners or regions that are not defined at the regional cluster.

Step 4 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 5 Click **Push Data to Clusters**.

Step 6 On the View Push Owner Data Report or View Push Region Data Report page, view the push details, then click **OK** to return to the List/Add Owners or List/Add Regions page.

Pulling Owners and Regions from the Replica Database

When you pull an owner or region, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is current with the local cluster, you can force an update before pulling the data.

Regional Web UI

Step 1 From the **Administration** menu in the regional cluster web UI, choose **Owners** or **Regions** under the **Settings** submenu.

Step 2 On the List/Add Owners or List/Add Regions page, click the **Pull Data** icon in the left pane. This opens the Select Replica Owner Data to Pull or Select Replica Region Data to Pull page.

Step 3 Click the **Replicate** icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see Replicating Local Cluster Data, on page 73.)

Step 4 Choose a replication mode using one of the Mode radio buttons.

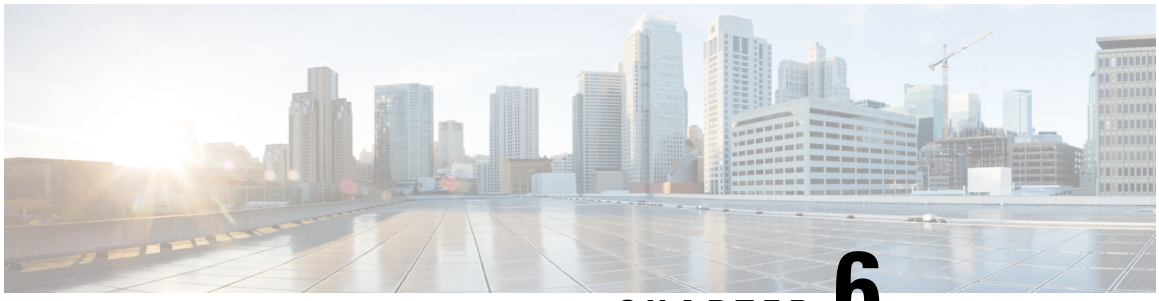
Leave the default Replace mode enabled, unless you want to preserve any existing owner or region properties at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the owner or region data at the local cluster by choosing Exact.

Step 5 Click **Pull All Owners** or **Pull All Regions** next to the cluster, or expand the cluster name and click **Pull Owner** or **Pull Region** to pull an individual owner or region in the cluster.

Step 6 On the Report Pull Replica Owners or Report Pull Replica Regions page, click **Run**.

Step 7 On the Run Pull Replica Owners or Run Pull Replica Region page, view the change set data, then click **OK**. You return to the List/Add Owners or List/Add Regions page with the pulled owners or regions added to the list.



CHAPTER 6

Managing the Central Configuration

This chapter explains how to manage the central configuration at the Cisco Prime IP Express regional cluster.

Central Configuration Tasks

Central configuration management at the regional cluster can involve:

- Setting up server clusters, replicating their data, and polling subnet utilization and lease history data from them.
- Setting up routers.
- Managing network objects such as DHCP scope templates, policies, client-classes, options, networks, and virtual private networks (VPNs).
- Managing DHCP failover server pairs.

These functions are available only to administrators assigned the central-cfg-admin role. (The full list of functions for the central-cfg-admin are listed in Table 5: Regional Cluster Administrator Predefined and Base Roles , on page 41.) Note that central configuration management does not involve setting up administrators

and checking the status of the regional servers. These functions are performed by the regional administrator, as described in Licensing, on page 67 and Managing Servers, on page 115.

Default Ports for Cisco Prime IP Express Services

The following table lists the default ports used for the Cisco Prime IP Express services.

Table 8: Default Ports for Cisco Prime IP Express Services

Port Number	Protocol	Service
53	TCP/UDP	DNS
53	TCP/UDP	Caching DNS
67	UDP	DHCP client to server
68	UDP	DHCP server to client
80	HTTP	BYOD web server client to server web UI
162	TCP	SNMP traps server to server
389	TCP	DHCP server to LDAP server
443	HTTPS	BYOD web server secure client to server web UI
546	UDP	DHCPv6 server to client
547	UDP	DHCPv6 client to server
647	TCP	DHCP failover server to server
653	TCP	High-Availability (HA) DNS server to server
1234	TCP	Local cluster CCM server to server
1244	TCP	Regional cluster CCM server to server
4444	TCP	SNMP client to server
5480	HTTPS	Virtual Appliance
8080	HTTP	Local cluster client to server web UI
8090	HTTP	Regional cluster client to server web UI

Port Number	Protocol	Service
8443	HTTPS	Local cluster secure client to server web UI
8453	HTTPS	Regional cluster secure client to server web UI

Firewall Considerations

When DNS (caching or authoritative) servers are deployed behind a stateful firewall (whether physical hardware or software, such as conntrack), it is recommended that:

- For at least UDP DNS traffic, stateful support be disabled if possible.
- If it is not possible to disable the stateful support, the number of allowed state table entries may need to be significantly increased.

DNS queries typically arrive from many different clients and requests from the same client may use different source ports. With thousands of queries per second, the number of these different sources can be large and if a firewall is using stateful tracking, it has to keep this state and does so for a period of time. Hence, you need to assure that the firewall can hold sufficient state - given the query traffic rates and the state time interval.

Licensing

Cisco Prime IP Express requires separate license for CCM, Authoritative DNS, Caching DNS, DHCP, and IPAM services or for combinations of these services. For more details on the Licensing, see the “License Files” section in the Overview chapter of the *Cisco Prime IP Express Installation Guide*.

You must have the Central Configuration Management (CCM) license to log into the UI. See Logging In to the Web UIs, on page 11 for entering license data the first time you try to log in. You can add the additional service based licenses in the regional server after you log in.

Whenever you log into a regional or local cluster, the overall licensing status of the system is checked. If there are any violations, you will be notified of the violation and the details. This notification is done only once for each user session. In addition, you will be able to see a message on each page indicating the violation.

Regional Web UI

Choose **Licenses** from **Administration > User Access** to open the List/Add Product Licenses page. Click **Browse** to locate the license file, click the file, then click **Open**. If the license ID in the file is valid, the license key appears in the list of licenses with the message “Successfully added license file “*filename*.” If the ID is not valid, the License field shows the contents of the file and the message “Object is invalid” appears.

The License Utilization section at the top of the page lists the type of license, the number of nodes allowed for the license, and the actual number of nodes used. Expand the section by clicking the plus (+) sign. The license utilization for each licensed service is listed separately in this section.

The Right To Use and the In Use counts are displayed for each licensed service. The Right To Use value will be the aggregation of the counts across all added licenses for that service. The ‘total in use’ value will be the aggregation of the latest utilization numbers obtained from all the local clusters. Only the services having a positive Right to use or In Use count will be listed in this section.

Licenses and usage count of earlier versions of Cisco IP Express will be listed under a separate section "ip-node".

The **Expert** mode attribute lets you specify how often license utilization is collected from all the local clusters. Changes to this setting require a server restart to take effect. You can set this attribute at the Edit CCM Server page. The default value is 4 hours.

Adding License

Cisco will e-mail you one or more license files after you register the Cisco Prime IP Express Product Authorization Key (PAK) on the web according to the Software License Claim Certificate shipped with the product. Cisco administers licenses through a FLEXlm system.

Note If a license file fails to load, check that the file is properly formatted text file without any extraneous characters in it. Extracting the file from email and moving it between systems can sometimes result in these problems.

Once you have the file or files:

Regional Web UI

Step 1 Locate the license file or files in a directory (or on the desktop) that is easy to find.

Step 2 On the List/Add Product Licenses page, browse for each file by clicking the **Choose File** button.

Note The List/Add Product Licenses option is only available at the Regional.

Step 3 In the Choose file window, find the location of the initial license file, then click **Open**.

Step 4 If the license key is acceptable, the Add Superuser Administrator page appears immediately.

Step 5 To add further licenses, from **Administration** menu, choose **Licenses** under the **User Access** submenu to open the List/Add Product Licenses page. Click **Choose File** to locate the additional license file, then click **Open**. If the key in the file is acceptable, the key, type, count, and expiration date appear, along with whether it is an evaluation key. If the key is not acceptable, the page shows the license text along with an error message. For the list of license types, see Licensing, on page 67.

Above the table of licenses is a License Utilization area that, when expanded, shows the license types along with the total nodes that you can use and those actually used.

If Cisco Prime IP Express is installed as a distributed system, the license management is done from the regional cluster. You will not have the option of adding licenses in local cluster.

CLI Commands

Use **license** *file* **create** to register licenses that are stored in file. The file referenced should include its absolute path or path relative to where you execute the commands. For example:

```
nrcmd-R> license "C:\licenses\product.licenses" create
```

Use **license list** to list the properties of all the created licenses (identified by key), and **license listnames** to list just the keys. Use **license** *key* **show** to show the properties of a specific license key.

Registering a Local Cluster that is Behind a NAT

License management is done from the regional cluster when Cisco Prime IP Express is installed. You must install the regional cluster first, and load all licenses in the regional cluster. A local cluster can register with a regional either by registering with the regional cluster during the installation process. However, if the local cluster is behind a NAT instance, then the registration may fail because the initial request does not reach the regional cluster.

In Cisco Prime IP Express 8.3 and later, you can register a local cluster that is behind a NAT instance by initiating the registration from the local cluster. To register a local cluster that is spanned by a NAT instance, you must ensure that Cisco Prime IP Express 8.3 or later is installed on both the regional and local clusters. You can also verify the license utilization for the local cluster.

Note To register a local cluster when the regional cluster is behind a NAT instance, you need to register the local cluster from the regional server by registering the local cluster from the regional server, selecting the services and resynchronizing the data.

To register a local cluster that is behind a NAT instance, do the following:

Local Web UI

Step 1 From **Administration** menu, choose **Licenses** under the **User Access** submenu to open the List Licenses page.

On the List Licenses page, add the details of the regional cluster.

a) Enter the IP address (IPv4 and/or IPv6) of the regional cluster.
b) Enter the SCP port of the regional cluster (1244 is the preset value).
c) Select the IP address (IPv4 and/or IPv6) of the local cluster that you want to register.
d) Select the component services that you want to register for the local cluster.

Step 2 Click **Register**.

Note The regional CCM server maintains the license utilization history for all the local clusters in the Cisco Prime IP Express system for all counted services (DHCP, DNS, and CDNS).

To view the license utilization for the local cluster, click **Check Poll Status**.

CLI Commands

Use the following commands to register or re-register a local cluster:

```
nrcmd> license register [cdns|dns|dhcp[,...]] [<regional-ip>|<regional-ipv6>]
[<regional-port>]

nrcmd> license register cdns|dns|dhcp[,...] <regional-ip> <regional-ipv6> [<regional-port>]
```

License History

The License History page allows you to view the licenses utilized in the specified time frame.

Regional Web UI

Step 1 Log into the regional cluster as superuser.

Step 2 From the **Administration** menu, choose **Administrators** to open the List/Add Administrators page for the local cluster version of this page, which is essentially identical.

Step 3 Click the **Add Administrators** icon in the Administrators pane, enter **example-regional-admin** in the Name field, then **examplereg** in the Password field in the Add Administrator dialog box, then click **Add Administrator**.

Step 4 Multiselect **central-cfg-admin-group** (for cluster administration) and **regional-admin-group** (for user administration) in the Groups drop-down list.

Step 5 Click **Save**.

CLI Command

Use **license showUtilHistory –full** view the number of utilized IP nodes against the RTUs (Right-to-Use) (see the **license** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Configuring Server Clusters

Server clusters are groupings of CCM, DNS, CDNS, and DHCP servers at local cluster locations. For example, an organization might have Boston and Chicago clusters of DNS and DHCP servers. A central administrator might want to affect how addresses are allocated at these clusters, or poll subnet utilization or lease history data from them. The central administrator might even want to connect to those local clusters, if the required permissions exist, to view changes there or restart the servers.

View the created clusters on the View Tree of Cluster Servers page. To get there, click **Clusters**. Once the page is populated with clusters, it shows some rich information and provides some useful functions. The Go Local icon allows single sign-on to a local cluster web UI, if an equivalent administrator account exists at the local cluster.

The View Tree of Clusters page might have been populated by manually adding clusters on the List/Add Remote Clusters page, or automatically when adding and synchronizing with routers, which also creates server clusters. The cluster names are links that you can click to edit the cluster information. The resynchronization, replication, and polling functions are described further on in this chapter.

The DHCP server may have the Related Servers icon next to the DHCP server for the cluster. Click this icon to open the List Related Servers for DHCP Server page. These servers can be DNS or DHCP failover servers.

Related Topics

Adding Local Clusters, on page 71

Editing Local Clusters, on page 72

Connecting to Local Clusters, on page 72

Synchronizing with Local Clusters, on page 72

Replicating Local Cluster Data, on page 73

Viewing Replica Data, on page 73

Purging Replica Data, on page 74

Deactivating, Reactivating, and Recovering Data for Clusters, on page 74

Polling Lease History Data, on page 88

Enabling Lease History Collection, on page 89

Adding Local Clusters

Adding local clusters to the regional cluster is the core functionality of the central-cfg-admin role.

To enable subnet utilization and lease history data collection, see Polling Lease History Data, on page 88.

The minimum required values to add a cluster are its name, IP address (IPv4 and/or IPv6) of the machine, administrator username, and password. The cluster name must be unique and its IP address must match that of the host where the CNRDB database is located. Obtain the SCP and HTTP ports, username, and password from the local cluster administrator. The preset value at Cisco Prime IP Express installation for the SCP port is 1234 and the HTTP port is 8080.

You can also set whether you want outbound connections to local servers to be secure by setting the *use-ssl* attribute to optional or required. It is set to optional by default, and it requires the Cisco Prime IP Express Communications Security Option installed to be effective.

Regional Web UI

From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu. This opens the Manage Servers page. View the local clusters on this page. You can also add server clusters on the List/Add Remote Clusters page. The List/Add Remote Clusters page provides the following functions:

- Connect to a local cluster web UI for local administration.
- Resynchronize with a local cluster to reconcile updates there.
- Pull data over to a regional cluster replica database.
- Purge replica to clear the bad replica data without deleting/re-adding the cluster. Whenever you perform purge replica, you must perform manual replication to the get the replica data again.

  Note This option appears only in Expert mode.

- Query subnet utilization data from a local cluster. This function appears only if you are assigned the regional-addr-admin role with at least the subnet-utilization subrole.
- Query lease history data from a local cluster. This function appears only if you are assigned the regional-addr-admin role with at least the lease-history subrole.

To add a cluster, click the **Add Cluster** icon in the **Manage Clusters** pane. This opens the Add Cluster dialog box. For an example of adding a local cluster, see Create the Local Clusters, on page 108. Click **Add Cluster** to return to the List/Add Remote Clusters page.

Local Web UI

You can also manage clusters in the local web UI. See Configuring Clusters in the Local Web UI, on page 19 for details.

CLI Commands

To add a cluster, use **cluster** *name* **create** <*address* | *ipv6-address*> [*attribute=value* ...] to give the cluster a name and address and set the important attributes. For example:

```
nrcmd> cluster example-cluster create 192.168.100.101 admin=admin password=changeme
```

Note that the administrator must be a superuser to fully synchronize at the local cluster.

Editing Local Clusters

Editing local clusters at the regional cluster is the core functionality of the central-cfg-admin role.

Regional Web UI

To edit a local cluster, click its name on the Manage Clusters pane to open the Edit Remote Cluster page. This page is essentially the same as the List/Add Remote Clusters page, except for an additional attribute unset function. You can choose the service (dhcp, dns, cdns, or none) that you want to run in the local by checking/unchecking the check boxes provided in the **Local Services** area. Make your changes, then click **Save**.

Local Web UI

You can also edit clusters in the local web UI. See Configuring Clusters in the Local Web UI, on page 19 for details.

CLI Commands

To edit a local cluster, use **cluster** *name* **set** *attribute=value* [*attribute=value* ...] to set or reset the attributes. For example:

```
nrcmd> cluster Example-cluster set poll-replica-interval=8h
```

Connecting to Local Clusters

In the web UI, if you have an equivalent administrator account at the local cluster, you can single sign-on to the local cluster Manage Servers page by clicking the **Connect** icon on the List/Add Remote Clusters page. To return to the regional cluster web UI, click the **Return** icon at the top right corner of the local cluster page. If you do not have an equivalent account at the local cluster, the Connect icon opens the local cluster login page.

Synchronizing with Local Clusters

Synchronization is configuring regional and local clusters so that they can work together in a unified fashion. When you synchronize:

1. The list of local servers are copied to the regional cluster.
2. A shared secret is established between the regional and local clusters for single sign-on.

Synchronization occurs once when you create a local cluster at the regional cluster. However, changes might occur at the local cluster periodically, requiring you to re synchronize with it. For example, you might change the username and password used to make local connections. Resynchronization does not happen

automatically—you must click the **Resynchronize** icon next to the cluster name on the List/Add Remote Clusters page. The result is a positive confirmation for success or an error message for a failure.

When you upgrade the local cluster, you should also resynchronize the cluster. For synchronization to be effective, the user account specified for the local cluster must be a superuser. If you get a synchronization error message, check the local cluster to ensure that it is running properly.

Note When you resynchronize clusters at the regional cluster, an automatic reinitialization of replica data occurs. The result is that for larger server configurations, resynchronization might take several minutes. The benefit, however, is that you do not need a separate action to update the replica data.

Replicating Local Cluster Data

Replication is copying the configuration data from a local server to the regional cluster replica database. Replication needs to occur before you can pull DHCP object data into the regional server database. During replication:

1. The current data from the local database is copied to the regional cluster. This usually occurs once.
2. Any changes made in the master database since the last replication are copied over.

Replication happens at a given time interval. You can also force an immediate replication by clicking the **Replicate** icon on the List/Add Remote Clusters page.

You can set the automatic replication interval on the Add Server Cluster page, or adjust it on the Edit Server Cluster page, using the *poll-replica-interval* attribute. This interval is preset at four hours. You can also set the fixed time of day to poll replica data by using the *poll-replica-offset* attribute; its default value is zero hours (no offset). The *poll-replica-rrs* attribute controls the replication of RR data without disabling other data replication. This attribute is present in Manage Servers and Manage Clusters page and has the values - none, all, and protected. If *poll-replica-rrs* is set to none, no RR data will be replicated for this cluster. If unset, the CCM server setting will apply.

Caution If the replica database is corrupted in any way, the regional CCM server will not start. If you encounter this problem, stop the regional service, remove (or move) the replica database files located in the *install-path* /regional/data/replica directory (and the log files in the /logs subdirectory), then restart the regional server. Doing so recreates the replica database without any data loss.

Viewing Replica Data

In the web UI, you can view the replica data cached in the replica database at the regional cluster by choosing **View Replica Data** from **Servers** submenu under the **Operate** menu. This opens the View Replica Class List page.

Regional Web UI

Select the:

1. Cluster in the Select Cluster list.
2. Object class in the Select Class list.

3. Replicate the data for the cluster and class chosen. Click the **Replicate Data for Cluster** button.
4. View the replica data. Click **View Replica Class List**, which opens a List Replica Data for Cluster page for the cluster and specific class of object you choose. On this page, you can:
   - Click the name of an object to open a View page at the regional cluster. Return to the List Replica page by clicking **Return to** *object* **List**.

     Note The List Replica Address Blocks and List Replica Subnets pages do not provide this function. To view the address blocks or subnets for the local cluster, use the **Go Local** icon.

   - Click the **Connect** icon to go to the List page for the object at the local cluster. Return to the List Replica *object* page by clicking the **Return** icon.

Click **Return** on the List Replica Data for Cluster page to return to the View Replica Class List page.

Purging Replica Data

In the regional web UI (only in Expert mode), you can clear the bad replica data without deleting/re-adding the clusters by clicking the **Purge Replica** icon on the List/Add Remote Clusters page. Whenever you perform purge replica, you must perform manual replication to get the replica data again.

Deactivating, Reactivating, and Recovering Data for Clusters

Deactivating a cluster might be necessary if you suspect that a hard disk error occurred where configuration data could have been lost. You can deactivate the cluster, remedy the problem, recover cluster data from the replica database, then reactivate the cluster. This saves you from having to delete and then recreate the cluster with all of its data lost in the process.

Deactivating, reactivating, and recovering the data for a cluster is available only in the web UI, and you must be an administrator assigned the central-config-admin role.

Data that is not recovered (and that you need to manually restore) includes:

- Contents of the **cnr.conf** file (see Modifying the cnr.conf File, on page 141)
- Web UI configuration files
- Unprotected DNS resource records
- Administrator accounts

Note If the local secret db is lost, the old references are no longer valid, even though they are restored. To recover your passwords, you have to use central management for your admins, and then push them to your local clusters. Routers, since they have their own secrets, also need to be centrally managed and then should be re-pushed. For the local cluster partner objects, running the sync from regional will create valid objects, but the old cluster objects may need to be deleted first.

- Lease history
- Extension scripts

Note Restoring the data to a different IP address requires some manual reconfiguration of such things as DHCP failover server pair and High-Availability (HA) DNS server pair addresses.

Regional Web UI

Deactivate a cluster by clicking the **Deactivate** button for the cluster. This immediately changes the button to Reactivate to show the status of the cluster. Deactivating a cluster disables deleting, synchronizing, replicating data, and polling subnet utilization and lease history. These operations are not available while the cluster is deactivated.

Deactivating the cluster also displays the Recover icon in the Recover Data column of the cluster. Click this icon to recover the replica data. This opens a separate "in process" status window that prevents any operations on the web UI pages while the recovery is in process. As soon as the recovery is successful, the disabled functions are again enabled and available.

To reactivate the cluster, click the **Reactivate** button to change back to the Deactivate button and show the status as active.

CLI Commands

The following cluster commands are only available when connected to a regional cluster:

Table 9: Cluster Commands

Action	Command
Activate	**cluster** *name* **activate**
Deactivate	**cluster** *name* **deactivate**
Resynchronize	**cluster** *name* **resynchronize**
Synchronize	**cluster** *name* **sync**
Update Replica Data	**cluster** *name* **updateReplicaData**
Remove Replica Data	**cluster** *name* **removeReplicaData**
Recover Data	**cluster** *name* **recoverData**
Poll Lease History	**cluster** *name* **pollLeaseHistory**
Get Lease History State	**cluster** *name* **getLeaseHistoryState**
Poll Subnet Utilization	**cluster** *name* **pollSubnetUtilization**

Central Configuration Management Server

The CCM servers at the local and regional clusters provide the infrastructure for Cisco Prime IP Express operation and user interfaces. The CCM Server reads, writes, and modifies the Cisco Prime IP Express database

(CCM DB). The main purpose of the CCM Server is to store and propagate data from the user to the protocol servers, and from the servers back to the user.

The change set is the fundamental unit of change to a data store. It sends incremental changes to a replicating server and provides an audit log for changes to the data store. Change sets consist of lists of change entries that are groups of one or more changes to a single network object. The web UI provides a view of the change sets for each data store.

Managing CCM Server

You can view logs and startup logs; edit the server attributes.

To view logs and startup logs, in the local cluster web UI, from the **Operate** menu, choose **Manage Servers** to open the Manage Servers page.

Editing CCM Server Properties

You can edit the CCM server properties using the Edit CCM Server page.

Local Basic or Advanced Web UI

Step 1 To access the CCM server properties, choose **Manage Servers** under **Operate** menu to open the Manage Servers page.

Step 2 Click **Local CCM Server** in the Manage Servers pane on the left. The Edit Local CCM Server page appears. This page displays all the CCM server attributes.

Step 3 Modify the settings as per your requirement.

Step 4 Click **Save** to save the CCM server attribute modifications.

Simple Network Management

The Cisco Prime IP Express Simple Network Management Protocol (SNMP) notification support allows you to query the DHCP and DNS counters, be warned of error conditions and possible problems with the DNS and DHCP servers, and monitor threshold conditions that can indicate failure or impending failure conditions.

Cisco Prime IP Express implements SNMP Trap Protocol Data Units (PDUs) according to the SNMPv2c standard. Each trap PDU contains:

- Generic-notification code, if enterprise-specific.
- A specific-notification field that contains a code indicating the event or threshold crossing that occurred.
- A variable-bindings field that contains additional information about certain events.

Refer to the Management Information Base (MIB) for the details. The SNMP server supports only reads of the MIB attributes. Writes to the attributes are not supported.

The following MIB files are required:

- **Traps**—CISCO-NETWORK-REGISTRAR-MIB.my and CISCO-EPM-NOTIFICATION-MIB.my
- **DNS server**—CISCO-DNS-SERVER-MIB.my

Note The Caching DNS server requires only a subset of the DNS MIB when it is operating. Caching DNS server only supports the *server-start* and *server-stop* notification events.

- **DHCPv4 server**—CISCO-IETF-DHCP-SERVER-MIB.my
- **DHCPv4 server capability**—CISCO-IETF-DHCP-SERVER-CAPABILITY.my
- **DHCPv4 server extensions**—CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- **DHCPv4 server extensions capability**—CISCO-IETF-DHCP-SERVER-EXT-CAPABILITY.my
- **DHCPv6 server**—CISCO-NETREG-DHCPV6-MIB.my (experimental)

Note The MIB, CISCO-NETREG-DHCPV6-MIB is defined to support query of new DHCP v6 related statistics and new DHCP v6 traps.

These MIB files are available in the /misc directory of the Cisco Prime IP Express installation path.

The following URL includes all files except the experimental CISCO-NETREG-DHCPV6-MIB.my file:

ftp://ftp.cisco.com/pub/mibs/supportlists/cnr/cnr-supportlist.html

The following dependency files are also required:

- **Dependency for DHCPv4 and DHCPv6**—CISCO-SMI.my
- **Additional dependencies for DHCPv6**—INET-ADDRESS-MIB.my

These dependency files are available along with all the MIB files at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/

To get the object identifiers (OIDs) for the MIB attributes, go to the equivalently named .oid file at:

ftp://ftp.cisco.com/pub/mibs/oid/

Related Topics

Setting Up the SNMP Server, on page 77
How Notification Works, on page 78
Handling SNMP Notification Events, on page 82
Handling SNMP Queries, on page 85

Setting Up the SNMP Server

To perform queries to the SNMP server, you need to set up the server properties.

Local Basic or Advanced and Regional Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page (see Managing Servers, on page 115).

Step 2 Click the **Local SNMP Server** link to open the Edit Local SNMP Server page.

Step 3 The *Community string* attribute is the password to access the server. (The community string is a read community string only.) The preset value is **public**.

Step 4 You can specify the Log Settings, Miscellaneous Options and Settings, and Advanced Options and Settings:

- **trap-source-addr**—Optional sender address to use for outgoing traps.
- **trap-source-ip6address**— Optional sender IPv6 address to use for outgoing traps.
- **server-active**—Determines whether the SNMP server is active for queries. The default value is true. If set to false, the server will run, but is not accessible for queries and does not send out traps.
- **cache-ttl**—Determines how long the SNMP caches responds to queries, default to 60 seconds.

Step 5 To manage the SNMP server interfaces in the Advanced mode, click the **Network Interfaces** tab. You can view the default configured network interfaces, and create and edit additional ones. To create and edit them, you must be assigned the server-management subrole of the ccm-admin role.

Step 6 To manage trap recipients for the server:

a) Click the **Trap Recipients** tab.
b) Enter the name of the trap recipient.
c) Enter the IPv4 and/or IPv6 address of a trap recipient.
d) Click **Add Trap Recipient**.
e) Repeat for each additional trap recipient.
f) To set the port, community string, and agent address for a trap recipient, click its name on the Trap Recipients tab to open the Edit Trap Recipient page, then set the values.

Step 7 Complete the SNMP server setup by clicking **Save**.

CLI Commands

To set the community string in the CLI so that you can access the SNMP server, use **snmp set community=***name*. Use **snmp set trap-source-addr** to set the trap source IPv4 address. Use **snmp set trap-source-ip6address** to set the trap source IPv6 address. Use **snmp disable server-active** to deactivate the SNMP server and **snmp set cache-ttl=***time* to set the cache time-to-live.

To set trap recipients, use **trap-recipient**, in the following syntax to include the IP address:

```
nrcmd> trap-recipient name create ip-addr=
nrcmd> trap-recipient name create ip6address=
```

You can also add the *agent-address*, *community*, and *port-number* values for the trap recipient.

Other SNMP-related commands include **snmp disable server-active** to prevent the server from running when started and the **snmp-interface** commands to configure the interfaces.

How Notification Works

Cisco Prime IP Express SNMP notification support allows a standard SNMP management station to receive notification messages from the DHCP and DNS servers. These messages contain the details of the event that triggered the SNMP trap.

Cisco Prime IP Express generates notifications in response to predetermined events that the application code detects and signals. Each event can also carry with it a particular set of parameters or current values. For example, the *free-address-low-threshold* event can occur in the scope with a value of 10% free. Other scopes and values are also possible for such an event, and each type of event can have different associated parameters.

The following table describes the events that can generate notifications.

Table 10: SNMP Notification Events

Event	Notification
Address conflict with another DHCP server detected (*address-conflict*)	An address conflicts with another DHCP server.
DNS queue becomes full (*dns-queue-size*)	The DHCP server DNS queue fills and the DHCP server stops processing requests. (This is usually a rare internal condition.)
Duplicate IP address detected (*duplicate-address* and *duplicate-address6*)	A duplicate IPv4 or IPv6 address occurs.
Duplicate IPv6 prefix detected (*duplicate-prefix6*)	A duplicate IPv6 prefix occurs.
Failover configuration mismatch (*failover-config-error*)	A DHCP failover configuration does not match between partners.
Free-address thresholds (*free-address-low* and *free-address-high*; or *free-address6-low* and *free-address6-high*)	The high trap when the number of free IPv4 or IPv6 addresses exceeds the high threshold; or a low trap when the number of free addresses falls below the low threshold after previously triggering the high trap.
High-availability (HA) DNS configuration mismatch (*ha-dns-config-error*)	An HA DNS configuration does not match between partners.
HA DNS partner not responding (*ha-dns-partner-down*)	An HA DNS partner stops responding to the DNS server.
HA DNS partner responding (*ha-dns-partner-up*)	An HA DNS partner responds after having been unresponsive.
DNS masters not responding (*masters-not-responding*)	Master DNS servers stop responding to the DNS server.
DNS masters responding (*masters-responding*)	Master DNS servers respond after having been unresponsive.
Other server not responding (*other-server-down*)	A DHCP failover partner, or a DNS or LDAP server, stops responding to the DHCP server.
Other server responding (*other-server-up*)	DHCP failover partner, or a DNS or LDAP server, responds after having been unresponsive.
DNS secondary zones expire (*secondary-zone-expired*)	A DNS secondary server can no longer claim authority for zone data when responding to queries during a zone transfer.

Event	Notification
Server start (*server-start*)	The DHCP or DNS server is started or reinitialized.
Server stop (*server-stop*)	The DHCP or DNS server is stopped.

Resource Monitoring SNMP Notifications

If SNMP traps are enabled for the resource limit alarms, Cisco Prime IP Express generates SNMP traps when the monitored resources exceed the critical or warning levels. SNMP traps are generated for resource limits:

- Whenever the resource's value exceeds the warning or critical limits (these are sent periodically while the value continues to exceed either threshold).
- Whenever the resource's value returns to a level below the warning limit.

The SNMP server generates a trap using the CISCO-EPM-NOTIFICATION-MIB. The mapping is as follows:

Trap Attribute Name	Object ID	Type	Value for Resource Events
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdminString (SIZE(1..16))	"1.2"
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Timestamp	Time of last resource event state change
cenAlarmUpdatedTimeStamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Timestamp	"current" time
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdminString (SIZE(1..20))	A unique id for the event - just hexadecimal digits
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32 (1..250)	1 (for Not acknowledged)
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdminString (SIZE(1..255))	"1,Not acknowledged"
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Integer	Not Used
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32 (1..250)	100 (for Raw alarm)
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdminString (SIZE(1..255))	"100,Raw alarm"
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddressType	Cluster server address type - IPv4(1) or IPv6(2)
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	Cluster address (based on local cluster's object)
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdminString (SIZE(1..255))	"Application"

Trap Attribute Name	Object ID	Type	Value for Resource Events
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddressType	Not used
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	Not used
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString (SIZE(1..1024))	Description formatted as " , "
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	0 for Clear, 2 for Warning, and 5 for Critical
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	SnmpAdminString (SIZE(1..255))	String alarm severity, one of "0,Clear", "2,Warning", or "5,Critical"
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32 (0..100)	Not used
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString (SIZE(1..1024))	Not used
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdminString (SIZE(1..255))	Name of monitored resource
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdminString (SIZE(1..255))	Server name (dhcp, dns, cdns, ...)
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdminString (SIZE(1..255))	"Network Registrar"
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Integer	3 (event)
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Guage (0..100)	Not used
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdminString (SIZE(1..255))	Not used
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdminString (SIZE(1..255))	Not used
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdminString (SIZE(1..255))	Not used
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdminString (SIZE(1..20))	Same as cenAlarmInstanceID

For more information on resource limit alarms, see Monitoring Resource Limit Alarms, on page 97.

Handling SNMP Notification Events

When Cisco Prime IP Express generates a notification, it transmits a single copy of the notification as an SNMP Trap PDU to each recipient. All events (and scopes or prefixes) share the list of recipients and other notification configuration data, and the server reads them when you initialize the notification.

You can set SNMP attributes in three ways:

- For the DHCP server, which includes the traps to enable and the default free-address trap configuration if you are not specifically configuring traps for scopes or prefixes (or their templates).
- On the scope or prefix (or its template) level by setting the *free-address-config* attribute.
- For the DNS server, which includes a *traps-enabled* setting.

To use SNMP notifications, you must specify trap recipients that indicate where trap notifications should go. By default, all notifications are enabled, but you must explicitly define the recipients, otherwise no notifications can go out. The IP address you use is often **localhost**.

The DHCP server provides special trap configurations so that it can send notifications, especially about free addresses for DHCPv4 and DHCPv6. You can set the trap configuration name, mode, and percentages for the low threshold and high threshold. The mode determines how scopes aggregate their free-address levels.

DHCP v4 Notification

The DHCP v4 modes and thresholds are (see also Handling Deactivated Scopes or Prefixes, on page 83):

- **scope mode**—Causes each scope to track its own free-address level independently (the default).
- **network mode**—Causes all scopes set with this trap configuration (through the scope or scope template *free-address-config* attribute) to aggregate their free-address levels if the scopes share the same *primary-subnet*.
- **selection-tags mode**—Causes scopes to aggregate their free-address levels if they share a primary subnet and have a matching list of selection tag values.
- **low-threshold**—Free-address percentage at which the DHCP server generates a low-threshold trap and re-enables the high threshold. The free-address level for scopes is the following calculation:

```
100 * available-nonreserved-leases
total-configured-leases
```

- **high-threshold**—Free-address percentage at which the DHCP server generates a high-threshold trap and re-enables the low threshold.

DHCP v6 Notification

The DHCP v6 modes and thresholds are (see also Handling Deactivated Scopes or Prefixes, on page 83):

- **prefix mode**—Causes each prefix to track its own free-address level independently.
- **link mode**—Causes all prefixes configured for the link to aggregate their own free-address levels if all prefixes share the same link.
- **v6-selection-tags mode**—Causes prefixes to aggregate their free-address levels if they share a link and have a matching list of selection tag values.

- **low-threshold**—Free-address percentage at which the DHCP server generates a low-threshold trap and re-enables the high threshold. The free-address level for prefixes is the following calculation:

```
100 * max-leases - dynamic-leases
max-leases
```

- **high-threshold**—Free-address percentage at which the DHCP server generates a high-threshold trap and re-enables the low threshold.

Handling Deactivated Scopes or Prefixes

A deactivated scope or prefix never aggregates its counters with other scopes or prefixes. For example, if you configure a prefix with **link** or **v6-selection-tags** trap mode, and then deactivate the prefix, its counters disappear from the total count on the aggregation. Any changes to the leases on the deactivated prefix do not apply to the aggregate totals.

Therefore, to detect clients for deactivated scopes or prefixes, you must set the event mode to **scope** or **prefix**, and not to any of the aggregate modes (**network**, **selection-tags**, **link**, or **v6-selection-tags**).

The use case for setting traps on deactivated prefixes, for example, is network renumbering. In this case, you might want to monitor both the new prefixes (as an aggregate, ensuring that you have enough space for all the clients) and old prefixes to ensure that their leases are freed up. You would probably also want to set the high threshold on an old prefix to 90% or 95%, so that you get a trap fired when most of its addresses are free.

Local Basic or Advanced Web UI

Access the SNMP attributes for the DHCP server by choosing **Manage Servers** from the **Operate** menu, then click **Local DHCP Server** in the left pane. You can view the SNMP attributes under SNMP (in Basic mode) or SNMP Settings (in Advanced mode) in the Edit DHCP Server page.

The four *lease-enabled* values (free-address6-low, free-address6-high, duplicate-address6, duplicate-prefix6) pertain to DHCPv6 only. Along with the traps to enable, you can specify the default free-address trap configuration by name, which affects all scopes and prefixes or links not explicitly configured.

To add a trap configuration, do the following:

Step 1 In Advanced mode, from the **Deploy** menu, choose **Traps** under the **DHCP** submenu to access the DHCP trap configurations. The List/Add Trap Configurations page appears.

Step 2 Click the **Add Traps** icon in the left pane to open the Add AddrTrapConfig page.

Step 3 Enter the name, mode, and threshold percentages, then click **Add AddrTrapConfig**.

Editing Trap Configuration

To edit a trap configuration, do the following:

Step 1 Click the desired trap name in the Traps pane to open the Edit Trap Configuration page

Step 2 Modify the name, mode, or threshold percentages.

Step 3 Click the **on** option for the *enabled* attribute to enable the trap configuration.

Step 4 Click **Save** for the changes to take effect.

Deleting Trap Configuration

To delete a trap configuration, select the trap in the Traps pane and click the **Delete** icon, then confirm or cancel the deletion.

Regional Basic or Advanced Web UI

In the regional web UI, you can add and edit trap configurations as in the local web UI. You can also pull replica trap configurations and push trap configurations to the local cluster on the List/Add Trap Configurations page.

Server Up/Down Traps

Every down trap must be followed by a corresponding up trap. However, this rule is not strictly applicable in the following scenarios:

1. If a failover partner or LDAP server or DNS server or HA DNS partner is down for a long time, down traps will be issued periodically. An up trap will be generated only when that server or partner returns to service.
2. If the DHCP or DNS server is reloaded or restarted, the prior state of the partner or related servers is not retained and duplicate down or up traps can result.

Note Other failover partner or LDAP server or DNS server or HA DNS partner up or down traps occur only to communicate with that partner or server, and therefore may not occur when the other partner or server goes down or returns to service.

CLI Commands

To set the trap values for the DHCP server at the local cluster, use **dhcp set traps-enabled**=*value*. You can also set the *default-free-address-config* attribute to the trap configuration. For example:

```
nrcmd> dhcp set traps-enabled=server-start,server-stop,free-address-low,free-address-high

nrcmd> dhcp set default-free-address-config=v4-trap-config
```

Note If you do not define a *default-free-address-config* (or *v6-default-free-address-config* for IPv6), Cisco Prime IP Express creates an internal, unlisted trap configuration named **default-aggregation-addr-trap-config**. Because of this, avoid using that name for a trap configuration you create.

To define trap configurations for DHCPv4 and DHCPv6, use **addr-trap** *name* **create** followed by the *attribute* =*value* pairs for the settings. For example:

```
nrcmd> addr-trap v4-trap-conf create mode=scope low-threshold=25% high-threshold=30%

nrcmd> addr-trap v6-trap-conf create mode=prefix low-threshold=20% high-threshold=25%
```

Handling SNMP Queries

You can use SNMP client applications to query the following MIBs:

- CISCO-DNS-SERVER-MIB.my
- CISCO-IETF-DHCP-SERVER-MIB.my
- CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- CISCO-NETREG-DHCPV6-MIB.my (experimental)

When the SNMP server receives a query for an attribute defined in one of these MIBs, it returns a response PDU containing that attribute value. For example, using the NET-SNMP client application (available over the Internet), you can use one of these commands to obtain a count of the DHCPDISCOVER packets for a certain address:

```
C:\net-snmp5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39:4444.iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.
ciscoIetfDhcpSrvMIB.ciscoIetfDhcpv4SrvMIBObjects.cDhcpv4Counters.cDhcpv4CountDiscovers

CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
C:\net-snmp5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39:4444
 1.3.6.1.4.1.9.10.102.1.3.1

CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
```

Both commands return the same results. The first one queries the full MIB attribute name, while the second one queries its OID equivalent (which can be less error prone). As previously described, the OID equivalents of the MIB attributes are located in the relevant files at the following URL:

ftp://ftp.cisco.com/pub/mibs/oid/

For example, the CISCO-IETF-DHCP-SERVER-MIB.oid file includes the following OID definition that corresponds to the previous query example:

```
"cDhcpv4CountDiscovers" "1.3.6.1.4.1.9.10.102.1.3.1"
```

Here are some possible SNMP query error conditions:

- The community string sent in the request PDU does not match what you configured.
- The version in the request PDU is not the same as the supported version (SNMPv2).
- If the object being queried does not have an instance in the server, the corresponding variable binding type field is set to SNMP_NOSUCHINSTANCE. With a GetNext, if there is no next attribute, the corresponding variable binding type field is set to SNMP_ENDOFMIBVIEW.
- If no match occurs for the OID, the corresponding variable binding type field is set to SNMP_NOSUCHOBJECT. With a GetNext, it is set to SNMP_ENDOFMIBVIEW.
- If there is a bad value returned by querying the attribute, the error status in the response PDU is set to SNMP_ERR_BAD_VALUE.

Integrating Cisco Prime IP Express SNMP into System SNMP

You can integrate the Cisco Prime IP Express SNMP server into the SNMP server for the system it runs on. The integration can be done in a way where the system will respond to queries for Cisco Prime IP Express MIB entries. On systems using NET-SNMP (and compatible servers) this is done by adding the following entries to the /etc/snmp/snmpd.conf configuration file

```
view systemview included .1.3.6.1.4.1.9.9
view systemview included .1.3.6.1.4.1.9.10

proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.9
proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.10
```

The community string **public** and the port number **4444** may have to be replaced if the Cisco Prime IP Express SNMP server has been configured with different values for those settings.

NET-SNMP is commonly available on Linux and other Unix-like systems. On other systems, similar mechanisms may also be available.

Bring Your Own Device Web Server

The BYOD web server at the regional cluster provides the infrastructure for Cisco Prime IP Express BYOD operation. The main purpose of the BYOD Web Server is to authenticate the user against AD and collect the device metadata by registering the user's own device in Cisco Prime IP Express.

Managing BYOD Web Server

You can view logs and startup logs; edit the server attributes.

To view logs and startup logs, in the regional cluster web UI, from the **Operate** menu, choose **Manage Servers** under the **Server** submenu to open the Manage Servers page.

Editing BYOD Web Server Properties

You can edit the BYOD web server properties using the Edit Local BYOD Web Server page.

Regional Basic or Advanced or Expert Web UI

Step 1 To access the BYOD web server properties, choose **Manage Servers** under **Operate** menu to open the Manage Servers page.

Step 2 Click Local **BYOD Web Server** in the Manage Servers pane on the left. The Edit Local BYOD Web Server page appears. This page displays the BYOD web server attributes.

- **KeyStore Settings:** Redirects the "http call" of the BYOD web server to secure "https" with a combination of key store file and key store password.
- **LDAP Settings:** Specifies the remote LDAP server used for client registration.
- **Additional Attributes (Auto- start)**: Indicates if the BYOD server should be started automatically after every server agent restart.

Step 3 Modify the settings as per your requirement.

Step 4 Click **Save** to save the BYOD web server attribute modifications.

Step 5 Click **Start Server** or **Restart Server** to apply the modifications to the BYOD web server.

Setting Up BYOD Theme and Content

You can create the content and multiple BYOD themes at the regional cluster which can be applied in BYOD web server interface.

Adding and Previewing BYOD Themes

You can create your own themes on the regional cluster using the BYOD Theme page and apply the created theme to the BYOD web server so that the logo, background, font, and other properties of the BYOD interface are displayed as per your customization. The created theme can be previewed prior to publishing it to the BYOD web server.

To add and preview a theme:

Regional Advanced or Expert Web UI

Step 1 From the **Deploy** menu, choose **Theme** under the **BYOD** submenu to open the List/Add Custom Theme page.

Step 2 Click the **Add Theme** icon in the Theme pane.
The **Add Custom Theme** window appears.

Step 3 Enter the Theme Name in the Add Custom Theme window.

Step 4 Click **Add Custom Theme** to create a new BYOD Theme.

Step 5 Update the Edit Custom Theme page with required theme attributes.

Step 6 Click the **Review Theme** icon in the top right corner of the List/Add Custom Theme page.
The Theme Preview window appears displaying the BYOD page with the newly added theme.

Note You can navigate between the BYOD pages with **Register** and **Reboot** to view how the theme is applied to the BYOD pages. By default, the **Theme preview** window loads the BYOD Device Registration page.

Step 7 Click **Reboot** to preview your theme in the Device Activation page.

Note You must close the Theme Preview window after preview to return to the List/Add Custom Theme page in the regional server.

Step 8 Click **Save** in the List/Add Custom Theme page in the regional server to apply the theme to the BYOD web server or click **Revert** to change the attribute values prior to saving the Custom Theme.

Note You can modify and preview the theme any number of times. Only the recently saved theme is applied to the BYOD web server.

Adding and Previewing BYOD Content

You can create the BYOD web server contents such as login page message, about, terms of services, contact details, and help message on the BYOD content page of the regional cluster, and preview it prior to publishing it to the BYOD web server. These contents can be published in the BYOD web server interface for the device registration and login pages.

To add and review content:

Regional Advanced or Expert Web UI

Step 1 From the **Deploy** menu, choose **Content** under the **BYOD** submenu to open the Edit BYOD content page.

Step 2 Upload the file or enter relevant text in the Edit BYOD content page.

Note You must upload only .html, .htm, or .txt files.

Step 3 Click **Review** to preview the content in the Edit BYOD content page before saving. A **Content Review** window containing the contents appears.

Step 4 Click on **About/Terms of Service/Contact/Help** in the content review page to preview the content added in the EDIT BYOD content page of the regional server.

Step 5 Click **Save** to publish the added BYOD content to the BYOD web server.

Polling Process

When the regional cluster polls the local cluster for subnet utilization or lease history, it first requests all available data up to the current time. This time is recorded in the history databases, and subsequent polls request only new data from this time forward. All times are stored relative to each local cluster time, adjusted for that cluster time zone.

If the times on each server are not synchronized, you might observe odd query results. For example, if the regional cluster time lags behind that of a local cluster, the collected history might be in the future relative to the time range queries at the regional cluster. If so, the result of the query would be an empty list. Data merged from the several clusters could also appear out of sequence, because of the different time skews between local clusters. This type of inconsistency would make it difficult to interpret trends. To avoid these issues, using a network time service for all clusters is strongly recommended.

Polling Lease History Data

Lease history data is automatically collected at any regional cluster where this feature is enabled for the DHCP server or failover pair. The default polling interval to update the regional databases is 4 hours. You can poll the servers by clicking the **Lease History** icon on the List/Add Remote Clusters page. For this manual polling, if the server is in a failover relationship, data is only retrieved for the subnets where the server is the main.

If you have address space privileges (you are assigned the regional-addr-admin role with at least the lease-history subrole), you can query the lease history data by choosing Current Utilization or Lease History from **Operate** menu (see the *"Running IP Lease Histories"* section in *Cisco Prime IP Express 9.0 DHCP User Guide*).

Related Topics

Polling Process, on page 88

Adjusting the Polling Intervals, on page 88

Adjusting the Polling Intervals

You can adjust the automatic polling interval for subnet utilization and lease history, along with other attributes. These attributes are set in three places at the regional cluster, with the following priority:

1. **Cluster**—These values override the server-wide settings, unless they are unset, in which case the server values are used. The cluster values are set when adding or editing the cluster. In the CLI, set the attributes listed in the table below, using the **cluster** command.
2. **Regional CCM server** (the preset polling interval is 4 hours)—This is set on the Edit CCM Server page, accessible by clicking **Servers**, then the Local CCM Server link. In the CLI, set the attributes listed in the table below using the **ccm** command.

Note If lease history collection is not explicitly turned on at the local cluster DHCP server (see Enabling Lease History Collection, on page 89), no data is collected, even though polling is on by default.

Table 11: Lease History Polling Regional Attributes

Attribute Type	Lease History
Polling interval—How often to poll data	*poll-lease-hist-interval* 0 (no polling) to 1 year, preset to 4 hours for the CCM server
Retry interval—How often to retry after an unsuccessful polling	*poll-lease-hist-retry* 0 to 4 retries
Offset—Hour of the day to guarantee polling	*poll-lease-hist-offset* 0 to 24h (0h=midnight)

The polling offset attribute ensures that polling occurs at a specific hour of the day, set as 24-hour time, in relation to the polling interval. For example, if you set the interval to 4h and the offset to 6h (6 A.M.), the polling occurs at 2 A.M., 6 A.M., 10 A.M., 2 P.M., 6 P.M., and 10 P.M. each day.

Enabling Lease History Collection

Step 1 Configure the local cluster DHCP server with scopes and address ranges so that clients have requested leases.

Step 2 Explicitly enable lease history data collection. The DHCP server attributes to set are:

- ***ip-history***—Enable or disable the lease history database for v4-only (DHCPv4), v6-only (DHCPv6), or both.
- ***ip-history-max-age***—Limit on the age of the history records (preset to 4 weeks).

In the CLI, set the attributes using the **dhcp set ip-history=<value> (v4-only, v6-only, both, or disable)** command.

Step 3 If in staged dhcp edit mode, reload the local cluster DHCP server.

Step 4 At the regional cluster, create the cluster that includes this DHCP server.

Step 5 In the regional web UI, go to the Lease History Settings section of the List/Add Remote Clusters page.

Step 6 Set the attributes in Table 11: Lease History Polling Regional Attributes, on page 89.

Step 7 Click **Save**.

Step 8 On the List/Add Remote Clusters page, click the **Replica** icon next to the cluster name.

Step 9 Click the **Lease History** icon for the cluster involved to obtain the initial set of lease history data. This data is refreshed automatically at each polling interval.

Managing DHCP Scope Templates

Scope templates apply certain common attributes to multiple scopes. These common attributes include a scope name based on an expression, policies, address ranges, and an embedded policy options based on an expression.

The scope templates you add or pull from the local clusters are visible on the List/Add DHCP Scope Templates page (choose **Scope Templates** from the **Design > DHCPv4** menu).

For details on creating and editing scope templates, and applying them to scopes, see the *"Creating and Applying Scope Templates" section in Cisco Prime IP Express 9.0 DHCP User Guide*. The regional cluster web UI has the added feature of pushing scope templates to local clusters and pulling them from local clusters.

Related Topics

Pushing Scope Templates to Local Clusters, on page 90

Pulling Scope Templates from Replica Data, on page 90

Pushing Scope Templates to Local Clusters

You can push the scope templates you create from the regional cluster to any of the local clusters. In the web UI, go to the List/Add DHCP Scope Templates page, and do any of the following:

- if you want to push a specific template to a cluster, select the scope template from the Scope Templates pane on the left, and click **Push** (at the top of the page). This opens the Push DHCP Scope Template page.
- If you want to push all of the available scope templates, click the **Push All** icon at the top of the Scope Templates pane. This opens the Push Data to Local Clusters page.

Regional Web UI

The Push DHCP Scope Template page and Push Data to Local Clusters page identify the data to push, how to synchronize it with the local cluster, and the cluster or clusters to which to push it. The data synchronization modes are:

- **Ensure** (preset value)—Ensures that the local cluster has new data without affecting any existing data.
- **Replace**—Replaces data without affecting other objects unique to the local cluster.
- **Exact**—Available for “push all” operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the local cluster.

Choose the destination cluster or clusters in the Available field and move it or them to the Selected field.

Tip The synchronization mode and cluster choice settings are persistent for the duration of the current login session, so that they are in effect each time you access this page, unless you change them.

After making these choices, click **Push Data to Clusters**. This opens the View Push Scope Template Data Report page.

Pulling Scope Templates from Replica Data

You may choose to pull scope templates from the replica data of the local clusters instead of explicitly creating them. (You may first want to update the policy replica data by clicking the **Replicate** icon next to the cluster name.) To pull the scope templates in the regional web UI, click the **Pull Data** icon at the top of the Scope Templates pane.

Regional Web UI

The Select Replica DHCP Scope Template Data to Pull page shows a tree view of the regional server replica data for the local clusters' scope templates. The tree has two levels, one for the local clusters and one for the scope templates in each cluster. You can pull individual scope templates from the clusters, or you can pull all of their scope templates. To pull individual scope templates, expand the tree for the cluster, then click **Pull Scope Template** next to its name. To pull all the scope templates from a cluster, click **Pull All Scope Templates**.

To pull the scope templates, you must also choose a synchronization mode:

- **Ensure**—Ensures that the regional cluster has new data without affecting any existing data.
- **Replace** (preset value)—Replaces data without affecting other objects unique to the regional cluster.
- **Exact**—Available for "pull all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the regional cluster.

Managing DHCP Policies

Every DHCP server must have one or more policies defined for it. Policies define lease duration, gateway routers, and other configuration parameters, in what are called DHCP options. Policies are especially useful if you have multiple scopes, because you need only define a policy once and apply it to the multiple scopes.

For details on creating and editing DHCP policies, and applying them to scopes, see the *"Configuring DHCP Policies" section in Cisco Prime IP Express 9.0 DHCP User Guide*. The regional cluster web UI has the added feature of pushing policies to, and pulling them from, the local clusters.

Related Topics

Pushing Policies to Local Clusters, on page 91

Pulling Policies from Replica Data, on page 92

Pushing Policies to Local Clusters

You can also push the policies you create from the regional cluster to any of the local clusters. In the regional web UI, go to List/Add DHCP Policies page, and do any of the following:

- If you want to push a specific policy to a cluster, select the policy from the Policies pane on the left, and click **Push** (at the top of the page).
- If you want to push all the policies, click the **Push All** icon at the top of the Policies pane.

Regional Web UI

The Push DHCP Policy Data to Local Clusters page identifies the data to push, how to synchronize it with the local cluster, and the cluster or clusters to which to push it. The data synchronization modes are:

- **Ensure** (preset value)—Ensures that the local cluster has new data without affecting any existing data.
- **Replace**—Replaces data without affecting other objects unique to the local cluster.
- **Exact**—Available for push-all operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the local cluster.

Choose the destination cluster or clusters in the Available field and move it or them to the Selected field. Then click **Push Data to Clusters** to open the View Push Policy Data Report page.

Tip The synchronization mode and cluster choice settings are persistent for the duration of the current login session, so that they are in effect each time you access this page, unless you change them.

Pulling Policies from Replica Data

You may choose to pull policies from the replica data of the local clusters instead of explicitly creating them. (In the regional web UI, you may first want to update the policy replica data by clicking the **Replicate** icon next to the cluster name). To pull the policies, click the **Pull Data** icon at the top of the Policies pane.

Regional Web UI

The Select Replica DHCP Policy Data to Pull page shows a tree view of the regional server replica data for the local clusters' policies. The tree has two levels, one for the local clusters and one for the policies in each cluster. You can pull individual policies from the clusters, or you can pull all of their policies. To pull individual policies, expand the tree for the cluster, then click **Pull Policy** next to its name. To pull all the policies from a cluster, click **Pull All Policies**.

To pull all the policies, you must also choose a synchronization mode:

- **Ensure**—Ensures that the regional cluster has new data without affecting any existing data.
- **Replace** (preset value)—Replaces data without affecting other objects unique to the regional cluster.
- **Exact**—Available for "pull all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the regional cluster.

Managing DHCP Client-Classes

Client-classes provide differentiated services to users that are connected to a common network. You can group your user community based on administrative criteria, and then ensure that each user receives the appropriate class of service. Although you can use the Cisco Prime IP Express client-class facility to control any configuration parameter, the most common uses are for:

- **Address leases**—How long a set of clients should keep its addresses.
- **IP address ranges**—From which lease pool to assign clients addresses.
- **DNS server addresses**—Where clients should direct their DNS queries.
- **DNS hostnames**—What name to assign clients.
- **Denial of service**—Whether unauthorized clients should be offered leases.

For details on creating and editing client-classes, see the *"Managing Client-Classes and Clients" chapter in Cisco Prime IP Express 9.0 DHCP User Guide*. The regional cluster web UI has the added feature of pushing client-classes to, and pulling them from, the local clusters.

Related Topics

Pushing Client-Classes to Local Clusters, on page 93

Pushing Client-Classes to Local Clusters, on page 93

Pushing Client-Classes to Local Clusters

You can also push the client-classes you create from the regional cluster to any of the local clusters. In the Regional web UI, go to the List/Add DHCP Client Classes page, and do any of the following:

- If you want to push a specific client-class to a cluster in the web UI, select the client-class from the Client Classes pane on the left, and click **Push** (at the top of the page). This opens the Push DHCP Client Class page.
- If you want to push all the client-classes, click the **Push All** icon at the top of the Client Classes pane. This opens the Push Data to Local Clusters page.

Regional Web UI

The Push DHCP Client Class page and Push Data to Local Clusters page identifies the data to push, how to synchronize it with the local cluster, and the cluster or clusters to which to push it. The data synchronization modes are:

- **Ensure** (preset value)—Ensures that the local cluster has new data without affecting any existing data.
- **Replace**—Replaces data without affecting other objects unique to the local cluster.
- **Exact**—Available for "push all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the local cluster.

Choose the destination cluster or clusters in the Available field and move it or them to the Selected field. Then click **Push Data to Clusters** to open the View Push Client-Class Data Report page.

Tip The synchronization mode and cluster choice settings are persistent for the duration of the current login session, so that they are in effect each time you access this page, unless you change them.

Pulling Client-Classes from Replica Data

You may choose to pull client-classes from the replica data of the local clusters instead of explicitly creating them. (In the web UI, you might first want to update the client-class replica data by clicking the **Replicate** icon next to the cluster name.) To pull the client-classes, click the **Pull Data** icon at the top of the Client Classes pane.

Regional Web UI

The Select Replica DHCP Client-Class Data to Pull page shows a tree view of the regional server replica data for the local clusters' client-classes. The tree has two levels, one for the local clusters and one for the client-classes in each cluster. You can pull individual client-classes from the clusters, or you can pull all of their client-classes. To pull individual client-classes, expand the tree for the cluster, then click **Pull Client-Class** next to its name. To pull all the client-classes from a cluster, click **Pull All Client-Classes**.

To pull the client-classes, you must also choose a synchronization mode:

- **Ensure**—Ensures that the regional cluster has new data without affecting any existing data.
- **Replace** (preset value)—Replaces data without affecting other objects unique to the regional cluster.
- **Exact**—Available for "pull all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the regional cluster.

Managing Virtual Private Networks

A virtual private network (VPN) is a specialized address space identified by a key. A VPN allows address overlap in a network, because the addresses are distinguished by separate keys. Most IP addresses exist in the global address space outside of a VPN. You can create regional VPNs only if you are an administrator assigned the dhcp-management subrole of the central-cfg-admin role.

For details on creating and editing VPNs, and applying them to various network objects, see the *"Configuring Virtual Private Networks Using DHCP" section in Cisco Prime IP Express 9.0 DHCP User Guide*. The regional web UI has the added feature of pushing VPNs to local clusters and pulling them from local clusters.

Related Topics

Pushing VPNs to Local Clusters, on page 94

Pulling VPNs from Replica Data, on page 94

Pushing VPNs to Local Clusters

You can push the VPNs you create from the regional cluster to any of the local clusters. In the Regional web UI, go to the List/Add VPNs page, and do any of the following:

- If you want to push a specific VPN to a cluster in the web UI, select the VPN from the VPNs pane on the left, and click **Push** (at the top of the page). This opens the Push VPN page.
- If you want to push all the VPNs, click the **Push All** icon at the top of the VPNs pane. This opens the Push Data to Local Clusters page.

Regional Web UI

The Push VPN page and Push Data to Local Clusters page identify the data to push, how to synchronize it with the local cluster, and the cluster or clusters to which to push it. The data synchronization modes are:

- **Ensure** (preset value)—Ensures that the local cluster has new data without affecting any existing data.
- **Replace**—Replaces data without affecting other objects unique to the local cluster.
- **Exact**—Available for “push all” operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the local cluster.

Choose the destination cluster or clusters in the Available field and move it or them to the Selected field. Then click **Push Data to Clusters** to open the View Push VPN Data Report page.

Tip The synchronization mode and cluster choice settings are persistent for the duration of the current login session, so that they are in effect each time you access this page, unless you change them.

Pulling VPNs from Replica Data

Instead of explicitly creating VPNs, you can pull them from the local clusters. (In the regional web UI, you may first want to update the VPN replica data by clicking the **Replica** icon next to the cluster name.) To pull the replica data, click the **Pull Data** icon at the top of the VPNs pane on the left, to open the Select Replica VPN Data to Pull page.

This page shows a tree view of the regional server replica data for the local clusters' VPNs. The tree has two levels, one for the local clusters and one for the VPNs in each cluster. You can pull individual VPNs or you can pull all of them. To pull individual VPNs, expand the tree for the cluster, then click **Pull VPN** next to its name. To pull all the VPNs, click **Pull All VPNs**.

To pull the VPNs, you must choose a synchronization mode:

- **Ensure**—Ensures that the regional cluster has new data without affecting any existing data.
- **Replace** (preset value)—Replaces data without affecting other objects unique to the regional cluster.
- **Exact**—Available for "pull all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the regional cluster.

Managing DHCP Failover Pairs

With DHCP failover, a backup DHCP server can take over for a main server if the latter comes off the network for any reason. You can use failover to configure two servers to operate as a redundant pair. If one server is down, the other server seamlessly takes over so that new DHCP clients can get, and existing clients can renew, their addresses. Clients requesting new leases need not know or care about which server responds to their lease request. These clients can obtain leases even if the main server is down.

In the regional web UI, you can view any created failover pairs on the List/Add DHCP Failover Pairs page. To access this page, click **DHCP**, then **Failover**. This functionality is available only to administrators who are assigned the dhcp-management subrole of the central-cfg-admin role.

For details on creating and editing failover pairs, see the *"Setting Up Failover Server Pairs" section in Cisco Prime IP Express 9.0 DHCP User Guide*. The regional cluster web UI has the added feature of pulling addresses from local clusters to create the failover pairs.

To pull the address space for a failover pair, you must have regional-addr-admin privileges.

Regional Web UI

Step 1 On the List/Add DHCP Failover Pairs page or View Unified Address Space page, click the **Pull v4 Data** or **Pull v6 Data** icon in the **Failover Pairs** pane.

Step 2 Choose the data synchronization mode (**Update**, **Complete**, or **Exact**) on the Select Pull Replica Address Space page. The results of choosing these modes are described in the table on the page.

Step 3 Click the **Report** button in the Synchronize Failover Pair tab and click **Return**.

Step 4 Click **Run** on the Report Pull Replica Address Space page.

Step 5 Click **OK** on the Run Pull Replica Address Space page.

Managing Lease Reservations

You can push lease reservations you create from the regional cluster to any of the local clusters. In the regional cluster web UI, go to the List/Add DHCPv4 Reservations page or List/Add DHCPv6 Reservations page, and click the **Push All** icon in the Reservations pane on the left. Note that you cannot push individual reservations. If the cluster pushed to is part of a DHCP failover configuration, pushing a reservation also pushes it to the partner server.

Related Topics

DHCPv4 Reservations, on page 96

DHCPv6 Reservations, on page 96

DHCPv4 Reservations

To create DHCPv4 reservations, the parent subnet object must exist on the regional server. If there are pending reservation edits at regional, these can be pushed to the subnet local cluster or failover pair. If the subnet has never been pushed, the parent scope is added to the local cluster or pair.

Once a subnet is pushed to a local cluster or pair, reservations are pushed to that cluster or pair. To move the scopes and subnet to another local cluster or failover pair, the subnet must first be reclaimed.

DHCPv6 Reservations

To create DHCPv6 reservations, the parent prefix must exist on the regional server. When there are pending reservation or prefix changes, you can push the updates to the local cluster.

Once a prefix is pushed to a local cluster, it can only update that local cluster. To move the prefix to another local cluster, it must first be reclaimed.

Regional Web UI

The ensuing page identifies the data to push, how to synchronize it with the local cluster, and the cluster or clusters to which to push it. The data synchronization modes are:

- **Ensure**—Ensures that the local cluster has new data without affecting any existing data.
- **Replace** (preset value)—Replaces data without affecting other objects unique to the local cluster.
- **Exact**—Available for "push all" operations only. Use this with caution, because it overwrites the data and deletes any other objects unique to the local cluster.

Choose the destination cluster or clusters in the Available field and move it or them to the Selected field.

Tip The synchronization mode and cluster choice settings are persistent for the duration of the current login session, so that they are in effect each time you access this page, unless you change them.

After making these choices, click **Push Data to Clusters**. This opens the View Push Reservations Data Report page. Click **OK** on this page.

You can also pull the replica address space on the List/Add DHCP v6 Reservations page, and opt whether to omit reservations when doing so. You should use this option only to reduce processing time when you are sure that there are no pending changes to reservations to merge. To omit reservations for the pull, check the *Omit Reservations?* check box, then click **Pull Data**.

See the *"Managing DHCPv6 Addresses" section in Cisco Prime IP Express 9.0 DHCP User Guide*.

Monitoring Resource Limit Alarms

Resource limit alarms enable you to monitor Cisco Prime IP Express system resources and provide an indication when one or more product resources has entered potentially dangerous level and requires attention. Resource limit alarms are designed to convey the resource limit information in an organized and consolidated way.

Note The log messages related to resource limits are logged to the ccm_monitor_log files. For more information on log files, see Log Files, on page 118.

You can reset the predefined threshold levels for both critical and warning levels for each monitored resource.

Cisco Prime IP Express reports the current status, the current value, and the peak value of the monitored resources in the web UI and CLI. The peak value is compared to the configured warning or critical limit for the resource limit alarm and the status of the resource limit alarm is displayed as OK, Warning, or Critical. Cisco Prime IP Express displays the alarms on the web UI and CLI until the resulting condition no longer occurs and the peak value is reset.

The resource limit alarms are updated at regular intervals based on the polling interval you configure. For more information on setting up the polling interval, see Setting Resource Limit Alarms Polling Interval, on page 98.

If SNMP traps are enabled for the resource limit alarms, Cisco Prime IP Express generates SNMP traps when the monitored resources exceed the critical or warning levels. SNMP traps are generated whenever the current value exceeds the configured warning or critical level.

The resource limit alarms can be configured both at the regional and in the local cluster. The resource limit alarms data is consolidated at the individual local cluster level. The resource limits alarms available on the regional cluster level pertain to only the regional cluster. The table below lists the types of resource limit alarms that are available on the regional or the local cluster.

Table 12: Resource Limit Alarms

	Regional Cluster	Local Cluster
Data Free Space in../Data Partition	□	□
Shadow Backup Time	□	□
CCM Memory	□	□
CNR Server Agent Memory	□	□
Tomcat Memory	□	□
DHCP Memory	x	□
CDNS Memory	x	□
DNS Memory	x	□
SNMP Memory	□	□

Lease Count	x	
Zone Count	x	
Resource Records Count	x	

Configuring Resource Limit Alarm Thresholds

You can configure the warning and critical limits for the resource limit alarms using the **Edit CCM Server** page.

Local and Regional Web UI

Step 1 To access the CCM server properties, choose **Manage Servers** under the **Operate** menu to open the Manage Servers page.

Step 2 Click **Local CCM Server** in the Manage Servers pane on the left. The Edit Local CCM Server page appears. This page displays all the CCM server attributes.

Step 3 Click the **Configure Resource Limits** tab.

Step 4 Modify the settings as per your requirement.

Note To enable the SNMP traps for the resource limit alarms, select the Enable Traps option in the Trap Configuration group.

Step 5 Click **Save** to save the CCM server attribute modifications.

CLI Commands

To set the resource limit alarms on the local or regional cluster, use **resource set** *attribute=value*. Use **resource show** to review the current setting and use **resource report** [**all** | **full** | **levels**] command to report on the resources.

To view the defined warning and critical levels, use **resource report levels** command.

A 109 status message is reported (if at least one resource is in the critical or warning state) under the following scenarios.

- Execute **resource report** command.
- Connect to a cluster via CLI.
- Exit from CLI.

Setting Resource Limit Alarms Polling Interval

You can set how often Cisco Prime IP Express polls for alarm data from the server and updates the web UI data. The *stats-history-sample-interval* controls the CCM server system polling rate.

Step 1 To edit the alarm poll interval, you need to edit the user preferences by going to **User Preferences** under the Settings drop-down list (at the top of the main page).

Step 2 After making the user preference settings, click **Modify User Preferences**.

Viewing Resource Limit Alarms

Resource limit alarms are displayed on the Alarms toolbar. To see a summary of the alarms, in the Cisco Prime IP Express web UI, click the **Alarms** toolbar on the bottom of the web UI. This opens the Alarms toolbar overlay which displays the status, resource values (current, configured warning, and critical value), and the peak value for each resource limit alarm. Based on the peak value for each resource limit, the status of resource limit is displayed as OK, Warning, or Critical on the web UI and CLI. The alarms are updated at regular intervals based on the polling interval you configure. For more information on setting up the polling interval, see Setting Resource Limit Alarms Polling Interval, on page 98.

Note When a resource is in a warning or critical state, the resource limit alarm is also displayed on the Configuration Summary page.

Resetting Resource Limit Alarms Peak Value

Cisco Prime IP Express maintains the peak values for each resource limit. The peak value is updated only when the current value exceeds the peak value. The peak value is compared to the configured warning or critical limit for the resource limit alarm and the status of the resource limit alarm is displayed as OK, Warning, or Critical.

When the peak value exceeds the configured warning or critical limit the status of the resource limit alarm is shown as Warning or Critical (on the web UI and CLI) respectively until the peak value is explicitly reset. To reset the peak value, perform the following steps:

Step 1 On the **Alarms** toolbar, select the Alarm for which you want to reset the peak value.

Step 2 Click **Reset Alarm** to clear the peak value.

CLI Commands

To reset the peak value on the local or regional cluster, use **resource reset** [*name* [,*name* [,...]]].

Note If no resource name is provided, all are reset.

Export Resource Limit Alarms Data

You can export the resource limit alarms data to a CSV file. To export the resource limit alarms:

Step 1 Select the alarm in the Alarms toolbar at the top of the web UI.

Step 2 Click **Export to CSV**.

Step 3 The File Download pop-up window displays. Click **Save**.

Step 4 In the Save As pop-up window, choose the location you want to save the file to and click **Save**.

Local Cluster Management Tutorial

This tutorial describes a basic scenario on a local cluster of the Example Company. Administrators at the cluster are responsible for users, zone data, DHCP data, address space data, and the servers in general. The task is to set up two zones (example.com and boston.example.com), hosts in the zones, and a subnet. The local cluster must also create a special administrator account so that the regional cluster in San Jose can perform the central configuration and replicate the local cluster administrators and address space at another cluster, as described in Regional Cluster Management Tutorial, on page 106.

Related Topics

Administrator Responsibilities and Tasks, on page 100

Create the Administrators, on page 100

Create the Address Infrastructure, on page 101

Create the Zone Infrastructure, on page 102

Create a Host Administrator Role with Constraints, on page 104

Create a Group to Assign to the Host Administrator, on page 105

Test the Host Address Range, on page 106

Administrator Responsibilities and Tasks

The local cluster administrators have the following responsibilities and tasks:

- **example-cluster-admin**—Created by the superuser:
  - At the Boston cluster, creates the other local administrators (example-zone-admin and example-host-admin).
  - Creates the basic network infrastructure for the local clusters.
  - Constrains the example-host-role to an address range in the boston.example.com zone.
  - Creates the example-host-group (defined with the example-host-role) that the example-zone-admin will assign to the example-host-admin.
- **example-zone-admin**:
  - Creates the example.com and boston.example.com zones, and maintains the latter zone.
  - Assigns the example-host-group to the example-host-admin.
- **example-host-admin**—Maintains local host lists and IP address assignments.

Create the Administrators

For this example, the superuser in Boston creates the local cluster, zone, and host administrators, as described in the Administrator Responsibilities and Tasks, on page 100.

Local Basic Web UI

Step 1 At the Boston local cluster, log in as superuser (usually **admin**).

Step 2 In Basic mode, from the **Administration** menu, choose **Administrators**.

Step 3 Add the local cluster administrator (with superuser access)—On the List/Add Administrators page:

a) Click the **Add Administrators** icon in the Administrators pane, enter **example-cluster-admin** in the Name field.
b) Enter **exampleadmin** in the Password and Confirm Password fields, then click **Add Admin**.
c) Check the Superuser check box.
d) Do not choose a group from the Groups list.
e) Click **Save**.

Step 4 Add the local zone administrator on the same page:

a) Click the **Add Administrators** icon in the Administrators pane, enter **example-zone-admin** in the Name field, and **examplezone** in the Password field, then click **Add Admin**.
b) Multiselect **ccm-admin-group**, **dns-admin-group**, and **host-admin-group** in the Groups drop-down list. The dns-admin-group is already predefined with the dns-admin role to administer DNS zones and servers. The ccm-admin-group guarantees that the example-zone-admin can set up the example-host-admin with a constrained role later on. The host-admin-group is mainly to test host creation in the zone.
c) Click **Save**.

Step 5 Add the local host administrator on the same page:

a) Click the **Add Administrators** icon in the Administrators pane, enter **example-host-admin** in the Name field, and **examplehost** in the Password field, then click **Add Admin**.
b) Do not choose a group at this point. (The example-zone-admin will later assign example-host-admin to a group with a constrained role.)
c) Click **Save**.

Note For a description on how to apply constraints to the administrator, see the Create a Host Administrator Role with Constraints, on page 104.

Create the Address Infrastructure

A prerequisite to managing the zones and hosts at the clusters is to create the underlying network infrastructure. The network configuration often already exists and was imported. However, this tutorial assumes that you are starting with a clean slate.

The local example-cluster-admin next creates the allowable address ranges for the hosts in the boston.example.com zone that will be assigned static IP addresses. These addresses are in the 192.168.50.0/24 subnet with a range of hosts from 100 through 200.

Local Advanced Web UI

Step 1 At the local cluster, log out as superuser, then log in as the **example-cluster-admin** user with password **exampleadmin**. Because the administrator is a superuser, all features are available.

Step 2 Click **Advanced** to go to Advanced mode.

Step 3 Click **Design**, then **Subnets** under DHCPv4 submenu.

Step 4 On the List/Add Subnets page, enter the boston.example.com subnet address:

a) Click the **Add Subnets** icon in the Subnets pane, enter **192.168.50** in the Address field.
b) Choose **24** in the mask drop-down list—This subnet will be a normal Class C network.
c) Leave the Owner, Region, and Address Type fields as is. Add description if desired.
d) Click **Add Subnet**.

Step 5 Click the 192.168.50.0/24 address to open the Edit Subnet page.

Step 6 In the IP Ranges fields, enter the static address range:

a) Enter **100** in the Start field. Tab to the next field.
b) Enter **200** in the End field.
c) Click **Add IP Range**. The address range appears under the fields.

Step 7 Click **Save**.

Step 8 Click **Address Space** to open the View Unified Address Space page. The 192.168.50.0/24 subnet should appear in the list. If not, click the **Refresh** icon.

Create the Zone Infrastructure

For this scenario, example-cluster-admin must create the Example Company zones locally, including the example.com zone and its subzones. The example-cluster-admin also adds some initial host records to the boston.example.com zone.

Related Topics

Create the Forward Zones, on page 102
Create the Reverse Zones, on page 103
Create the Initial Hosts, on page 103

Create the Forward Zones

First, create the example.com and boston.example.com forward zones.

Local Basic Web UI

Step 1 At the local cluster, log in as the **example-zone-admin** user with password **examplezone**.

Step 2 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu. This opens the List/Add Forward Zones page.

Step 3 Create the example.com zone (tab from field to field):

a) Click the **Add Forward Zone** icon in the Forward Zones pane, enter **example.com** in the Name field.
b) In the Nameserver FQDN field, enter **ns1**.
c) In the Contact E-Mail field, enter **hostmaster**.
d) In the Serial Number field, enter the serial number.
e) Click **Add Zone**.

Step 4 Create the **boston.example.com** zone in the same way, using the same values as in the previous steps:

a) Creating a zone with a prefix added to an existing zone opens the Create Subzone in Parent Zone page, because the zone can be a potential subzone. Because you do want to create this zone as a subzone to example.com, click **Create as Subzone** on the Create Subzone in Parent Zone page.
b) Because nameservers are different in each zone, you must create a glue Address (A) record to tie the zones together. Enter 192.168.50.1 in the A record field, then click **Specify Glue Records**. Then click **Report**, **Run**, and **Return**.
c) The List/Add Zones page should now list example.com and boston.example.com.

Step 5 Click **Advanced**, then **Show Forward Zone Tree** to show the hierarchy of the zones. Return to list mode by clicking **Show Forward Zone List**.

Create the Reverse Zones

Next, create the reverse zones for example.com and boston.example.com. This way you can add reverse address pointer (PTR) records for each added host. The reverse zone for example.com is based on the 192.168.50.0 subnet; the reverse zone for boston.example.com is based on the 192.168.60.0 subnet.

Local Basic Web UI

Step 1 At the local cluster, you should be logged in as the example-zone-admin user, as in the previous section.
Step 2 From the **Design** menu, choose **Reverse Zones** under the **Auth DNS** submenu.
Step 3 On the List/Add Reverse Zones page, click the **Add Reverse Zone** icon in the Reverse Zones pane, enter **50.168.192.in-addr.arpa** in the Name field. (There is already a reverse zone for the loopback address, 127.in-addr.arpa.)
Step 4 Enter the required fields to create the reverse zone, using the forward zone values:
a) **Nameserver**—Enter **ns1.example.com.** (be sure to include the trailing dot).
b) **Contact E-Mail**—Enter **hostmaster.example.com.** (be sure to include the trailing dot).
c) **Serial Number**—Enter the serial number.
Step 5 Click **Add Reverse Zone** to add the zone and return to the List/Add Reverse Zones page.
Step 6 Do the same for the boston.example.com zone, using **60.168.192.in-addr.arpa** as the zone name and the same nameserver and contact e-mail values as in **Step 4**. (You can cut and paste the values from the table.)

Create the Initial Hosts

As a confirmation that hosts can be created at the Boston cluster, the example-zone-admin tries to create two hosts in the example.com zone.

Local Advanced Web UI

Step 1 As the example-zone-admin user, click **Advanced** to enter Advanced mode.
Step 2 From the **Design** menu, choose **Hosts** under the **Auth DNS** submenu. This opens the List/Add Hosts for Zone page. You should see boston.example.com and example.com in the Select Zones box on the left side of the window.
Step 3 Click example.com in the list of zones.
Step 4 Add the first static host with address 192.168.50.101:
a) Enter **userhost101** in the Name field.

b) Enter the complete address **192.168.50.101** in the IP Address(es) field. Leave the IPv6 Address(es) and Alias(es) field blank.
c) Ensure that the Create PTR Records? check box is checked.
d) Click **Add Host**.

Step 5 Add the second host, **userhost102**, with address **192.168.50.102**, in the same way. The two hosts should now appear along with the nameserver host on the List/Add Hosts for Zone page.

Create a Host Administrator Role with Constraints

In this part of the tutorial, the Boston example-cluster-admin creates the example-host-role with address constraints in the boston.example.com zone.

Local Advanced Web UI

Step 1 Log out as the example-zone-admin user and log in as the **example-cluster-admin** user (with password **exampleadmin**).

Step 2 Click **Advanced** to enter Advanced mode.

Step 3 From the **Administration** menu, choose **Roles** under **User Access** submenu to open the List/Add Administrator Roles page.

Step 4 Add the example-host-role:
a) Click the **Add Role** icon in the Roles pan to open the Add Roles dialog box.
b) Enter **example-host-role** in the Name field.
c) Click **Add Role**. The example-host-role should now appear in the list of roles on the List/Add Administrator Roles page.

Step 5 Add the constraint for the role:
a) Click **Add Constraint**.
b) On the Add Role Constraint for Role page, scroll down to Host Restrictions.
c) For the *all-forward-zones* attribute, click the **false** radio button.
d) For the *zones* attribute, enter **boston.example.com**.
e) For the *ipranges* attribute, enter the range **192.168.50.101–192.168.50.200**.
f) The *zone-regexpr* and *host-regexpr* attribute fields are for entering regular expressions to match zones and hosts, respectively, in regex syntax. (See the following table for the commonly used regex values.)

Table 13: Common Regex Values

Value	Matches
. (dot)	Any character (a wildcard). Note that to match a literal dot character (such as in a domain name), you must escape it by using a backslash (\), such that **\.com** matches.com.
char	Literal character (*char*) that follows, or the *char* has special meaning. Used especially to escape metacharacters such as the dot (**.**) or another backslash. Special meanings include **\d** to match decimal digits, **\D** for nondigits, **\w** for alphanumerics, and **\s** for whitespace.

Value	Matches
*char***?**	Preceding *char* once or not at all, as if the character were optional. For example, **example\.?com** matches example.com or examplecom.
*char******	Preceding *char* zero or more times. For example, **ca*t** matches ct, cat, and caaat. This repetition metacharacter does iterative processing with character sets (see **[***charset***]**).
char+	Preceding *char* one or more times. For example, **ca+t** matches cat and caaat (but not ct).
[*charset***]**	Any of the characters enclosed in the brackets (a character set). You can include character ranges such as **[a–z]** (which matches any lowercase character). With the ***** repetition metacharacter applied, the search engine iterates through the set as many times as necessary to effect a match. For example, **a[bcd]*b** will find abcbd (by iterating through the set a second time). Note that many of the metacharacters (such as the dot) are inactive and considered literal inside a character set.
[^*charset***]**	Anything but the *charset*, such that **[^a-zA-Z0-9]** matches any nonalphanumeric character (which is equivalent to using **\W**). Note that the caret outside a character set has a different meaning.
^	Beginning of a line.
$	End of a line.

g) Click **Add Constraint**. The constraint should have an index number of 1.

Step 6 Click **Save**.

Create a Group to Assign to the Host Administrator

The Boston example-cluster-admin next creates an example-host-group that includes the example-host-role so that the example-zone-admin can assign this group to the example-host-admin.

Local Advanced Web UI

Step 1 As example-cluster-admin, still in Advanced mode, from the **Administration** menu, choose **Groups** submenu to open the List/Add Administrator Groups page.

Step 2 Create the example-host-group and assign the example-host-role to it:

a) Click the **Add Groups** icon in the Groups pane, enter **example-host-group** in the Name field.

b) From the Base Role drop-down list, choose **example-host-role**.

c) Click **Add Group**.
d) Add a description such as **Group for the example-host-role**, then click **Save**.

Step 3 Log out as example-cluster-admin, then log in as the **example-zone-admin** user (with password **examplezone**).

Step 4 As example-zone-admin, assign the example-host-group to the example-host-admin:

a) In Basic mode, from the **Administration** menu, choose **Administrators**.
b) On the List/Add Administrators page, click example-host-admin to edit the administrator.
c) On the Edit Administrator page, choose **example-host-group** in the Available list, then click << to move it to the Selected list.
d) Click **Save**. The example-host-admin should now show the example-host-group in the Groups column on the List/Add Administrators page.

Test the Host Address Range

The example-host-admin next tests an out-of-range address and then adds an acceptable one.

Local Advanced Web UI

Step 1 At the local cluster, log out as example-zone-admin, then log in as **example-host-admin** (with password **examplehost**).

Step 2 Click **Advanced** to enter Advanced mode.

Step 3 From the **Design** menu, choose **Hosts** from the **Auth DNS** submenu.

Step 4 On the List/Add Hosts for Zone page, try to enter an out-of-range address (note the range of valid addresses in the Valid IP Ranges field):

a) Enter **userhost3** in the Name field.
b) Deliberately enter an out-of-range address (**192.168.50.3**) in the IP Address(es) field.
c) Click **Add Host**. You should get an error message.

Step 5 Enter a valid address:

a) Enter **userhost103**.
b) Enter **192.168.50.103** in the IP Address(es) field.
c) Click **Add Host**. The host should now appear with that address in the list.

Regional Cluster Management Tutorial

This tutorial is an extension of the scenario described in the Local Cluster Management Tutorial, on page 100. In the regional cluster tutorial, San Jose has two administrators—a regional cluster administrator and a central configuration administrator. Their goal is to coordinate activities with the local clusters in Boston and Chicago so as to create DNS zone distributions, router configurations, and DHCP failover configurations using the servers at these clusters. The configuration consists of:

- One regional cluster machine in San Jose.
- Two local cluster machines, one in Boston and one in Chicago.
- One Cisco uBR7200 router in Chicago.

Related Topics

Administrator Responsibilities and Tasks, on page 107
Create the Regional Cluster Administrator, on page 107
Create the Central Configuration Administrator, on page 108
Create the Local Clusters, on page 108
Add Zone Management to the Configuration Administrator, on page 109
Create a Zone for the Local Cluster, on page 109
Pull Zone Data and Create a Zone Distribution, on page 110
Create a Subnet and Pull Address Space, on page 110
Push a DHCP Policy, on page 111
Create a Scope Template, on page 111
Create and Synchronize the Failover Pair, on page 112

Administrator Responsibilities and Tasks

The regional administrators have the following responsibilities and tasks:

- **example-regional-admin**—Created by the superuser at the San Jose regional cluster, who creates the example-cfg-admin.
- **example-cfg-admin**:
  - Defines the Boston and Chicago clusters and checks connectivity with them.
  - Adds a router and router interfaces.
  - Pulls zone data from the local clusters to create a zone distribution.
  - Creates a subnet and policy, and pulls address space, to configure DHCP failover pairs in Boston and Chicago.

Create the Regional Cluster Administrator

The regional superuser first creates the example-regional-administrator, defined with groups, to perform cluster and user administration.

Regional Web UI

Step 1 Log into the regional cluster as superuser.

Step 2 From the **Administration** menu, choose **Administrators** to open the List/Add Administrators page for the local cluster version of this page, which is essentially identical.

Step 3 Click the **Add Administrators** icon in the Administrators pane, enter **example-regional-admin** in the Name field, then **examplereg** in the Password field in the Add Administrator dialog box, then click **Add Administrator**.

Step 4 Multiselect **central-cfg-admin-group** (for cluster administration) and **regional-admin-group** (for user administration) in the Groups drop-down list.

Step 5 Click **Save**.

Create the Central Configuration Administrator

As part of this tutorial, the example-regional-admin next logs in to create the example-cfg-admin, who must have regional configuration and address management capabilities.

Regional Web UI

Step 1 Log out as superuser, then log in as **example-regional-admin** with password **examplereg**. Note that the administrator has all but host and address space administration privileges.

Step 2 From the **Administration** menu, choose **Administrators** to open the List/Add Administrators page.

Step 3 Click the **Add Administrators** icon in the Administrators pane, enter **example-cfg-admin** in the Name field, then **cfgadmin** in the Password field in the Add Administrator dialog box, then click **Add Administrator**.

Step 4 Multiselect **central-cfg-admin-group** and **regional-addr-admin-group** in the Groups drop-down list.

Step 5 Click **Save**. The example-cfg-admin now appears with the two groups assigned.

You can also add constraints for the administrator. Click **Add Constraint** and, on the Add Role Constraint for Role page, choose the read-only, owner, or region constraints, then click **Add Constraint**.

Create the Local Clusters

The example-cfg-admin next creates the two local clusters for Boston and Chicago.

Regional Web UI

Step 1 Log out as example-regional-admin, then log in as **example-cfg-admin** with password **cfg admin**.

Step 2 From the **Operate** menu, choose **Manage Clusters** from the **Servers** submenu to open the List/Add Remote Clusters page.

Step 3 Click the **Add Manage Clusters** icon in the**Manage Clusters** pane.

Step 4 On the Add Cluster dialog box, create the Boston cluster based on data provided by its administrator:

a) Enter **Boston-cluster** in the name field.
b) Enter the IPv4 address of the Boston server in the IPv4 Address field.
c) Enter the IPv6 address of the Boston server in the IPv6 Address field.
d) Enter **example-cluster-admin** in the admin field, then **exampleadmin** in the password field.
e) Enter in the SCPO-port field the SCP port to access the cluster as set at installation (**1234** is the preset value).
f) Click **Add Cluster**.

Step 5 Create the Chicago cluster in the same way, except use **Chicago-cluster** in the name field, enter the remaining values based on data provided by the Chicago administrator, then click **Add Cluster**. The two clusters should now appear on the List/Add Remote Clusters page.

Step 6 Connect to the Boston cluster. Click the **Go Local** icon next to Boston-cluster. If this opens the local cluster Manage Servers page, this confirms the administrator connectivity to the cluster. To return to the regional cluster web UI, click the **Go Regional** icon.

Step 7 Connect to the Chicago cluster to confirm the connectivity in the same way.

Step 8 Confirm that you can replicate data for the two forward zones from the Boston cluster synchronization:

a) From the **Operate** menu, choose **Replica Data** from the **Servers** submenu.
b) On the View Replica Class List page, click Boston-cluster in the Select Cluster list.
c) In the Select Class list, click **Forward Zones**.
d) Click the **Replicate** icon in the Replicate Data column.
e) Click **View Replica Class List**. On the List Replica Forward Zones for Cluster page, you should see the boston.example.com and example.com zones.

Add Zone Management to the Configuration Administrator

Because there are no zones set up at the Chicago cluster, the example-cfg-admin can create a zone at the regional cluster to make it part of the zone distribution. However, the example-regional-admin must first modify the example-cfg-admin to be able to create zones.

Regional Web UI

Step 1 Log out as example-cfg-admin, then log in as **example-regional-admin**.

Step 2 From the **Administration** menu, choose **Administrators** under the **User Access** submenu.

Step 3 On the List/Add Administrators page, click example-cfg-admin from the Administrators pane.

Step 4 On the Edit Administrator page, click central-dns-admin-group in the Groups Available list, then move it (using <<) to the Selected list. The Selected list should now have central-cfg-admin-group, regional-addr-admin-group, and central-dns-admin-group.

Step 5 Click **Save**. The change should be reflected on the List/Add Administrators page.

Create a Zone for the Local Cluster

The example-cfg-admin next creates the chicago.example.com zone for the zone distribution with the Boston and Chicago zones.

Regional Web UI

Step 1 Log out as example-regional-admin, then log in as **example-cfg-admin**.

Step 2 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu.

Step 3 Click the **Add Forward Zone** icon in the **Forward Zones** pane.

Step 4 On the Add DNS Zone dialog box, enter:

a) **Name—chicago.example.com**.
b) **Nameserver FQDN—ns1**.
c) **Contact E-mail—hostmaster**.

d) **Nameservers—ns1** (click **Add Nameserver**).
e) Click **Add DNS Zone**.

Step 5 Click the **Reverse Zones** submenu.

Step 6 On the List/Add Reverse Zones page, create the **60.168.192.in-addr.arpa** reverse zone for the Chicago zone, with the proper attributes set.

Pull Zone Data and Create a Zone Distribution

The example-cfg-admin next pulls zone data from Boston and Chicago and creates a zone distribution.

Regional Web UI

Step 1 As example-cfg-admin, from the **Design** menu, choose **Views** under the **Auth DNS** submenu to view the List/Add Zone Views page.

Step 2 On the List/Add Zone Views page, pull the zone from the replica database:
a) Click the **Pull Data** icon in the **Views** pane.
b) On the Select Replica DNS View Data to Pull dialog box, leave the Data Synchronization Mode defaulted as Update, then click **Report** to open the Report Pull Replica Zone Data page.
c) Notice the change sets of data to pull, then click **Run**.
d) On the Run Pull Replica Zone Data page, click **OK**.

Step 3 On the List/Add Zone Views page, notice that the Boston cluster zone distribution is assigned an index number (**1**) in the Name column. Click the number.

Step 4 On the Edit Zone Views page, in the Primary Server field, click Boston-cluster. (The IP address of the Boston-cluster becomes the first master server in the Master Servers list.)

Step 5 Because we want to make the Chicago-cluster DNS server a secondary server for the Boston-cluster:
a) Click **Add Server** in the Secondary Servers area.
b) On the Add Zone Distribution Secondary Server page, choose **Chicago-cluster** in the Secondary Server drop-down list.
c) Click **Add Secondary Server**.

Step 6 On the Edit Zone Distribution page, in the Forward Zones area, move **chicago.example.com** to the Selected list.

Step 7 In the Reverse Zones area, move **60.168.192.in-addr.arpa** to the Selected list.

Step 8 Click **Modify Zone Distribution**.

Create a Subnet and Pull Address Space

The example-cfg-admin next creates a subnet at the regional cluster. This subnet will be combined with the other two pulled subnets from the local clusters to create a DHCP failover server configuration.

Regional Web UI

Step 1 As example-cfg-admin, from the **Design** menu,choose **Subnets** under the **DHCPv4** submenu to open the List/Add Subnets page.

Step 2 Create an additional subnet, 192.168.70.0/24 by clicking the **Add Subnets** icon in the Subnets pane:
a) Enter **192.168.70** (the abbreviated form) as the subnet network address in the Address/Mask field.
b) Leave the **24** (255.255.255.0) selected as the network mask.
c) Click **Add Subnet**.

Step 3 Click **Address Space** to confirm the subnet you created.

Step 4 On the View Unified Address Space page, click **Pull Replica Address Space**.

Step 5 On the Select Pull Replica Address Space page, leave everything defaulted, then click **Report**.

Step 6 The Report Pull Replica Address Space page should show the change sets for the two subnets from the clusters. Click **Run**.

Step 7 Click **OK**. The two pulled subnets appear on the List/Add Subnets page.

Push a DHCP Policy

The example-cfg-admin next creates a DHCP policy, then pushes it to the local clusters.

Regional Web UI

Step 1 As example-cfg-admin, from the **Design** menu, choose **Policies** under the**DHCP Settings** submenu.

Step 2 On the List/Add DHCP Policies page, click the **Add Policies** icon in the**Policies** pane.

Step 3 On the Add DHCP Policy dialog box, create a central policy for all the local clusters:
a) Enter **central-policy-1** in the Name field. Leave the Offer Timeout and Grace Period values as is.
b) Enter a lease period. In the DHCP > DHCPv4 > Options drop-down list, choose **dhcp-lease-time [51] (unsigned time)**, then enter **2w** (two weeks) for the lease period in the Value field.
c) Click **Add Option**.
d) Click **Add Policy**. The central-policy-1 should appear on the List/Add DHCP Policies page.

Step 4 Push the policy to the local clusters:
a) Select the policy, central-policy-1 and click the **Push** button.
b) On the Push DHCP Policy Data to Local Clusters page, leave the Data Synchronization Mode as **Ensure**. This ensures that the policy is replicated at the local cluster, but does not replace its attributes if a policy by that name already exists.
c) Click **Select All** in the Destination Clusters section of the page.
d) Click **<<** to move both clusters to the Selected field.
e) Click **Push Data to Clusters**.
f) View the push operation results on the View Push DHCP Policy Data Report page, then click **OK**.

Create a Scope Template

The example-cfg-admin next creates a DHCP scope template to handle failover server pair creation.

Regional Web UI

Step 1 As the example-cfg-admin user, from the **Design** menu, choose **Scope Templates** under the **DHCPv4** submenu.

Step 2 On the List/Add DHCP Scope Templates page, click the **Add Scope Templates** icon in the **Scope Templates** pane. Enter **scope-template-1** in the Name field, then click **Add DHCP Scope Template**.

Step 3 The template should appear on the List/Add DHCP Scope Templates page. Set the basic properties for the scope template—Enter or choose the following values in the fields:

a) **Scope Name Expression**—To autogenerate names for the derivative scopes, concatenate the example-scope string with the subnet defined for the scope. To do this, enter **(concat "example-scope-" subnet)** in the field (including the parentheses).

b) **Policy**—Choose **central-policy-1** in the drop-down list.

c) **Range Expression**—Create an address range based on the remainder of the subnet (the second through last address) by entering **(create-range 2 100)**.

d) **Embedded Policy Option Expression**—Define the router for the scope in its embedded policy and assign it the first address in the subnet by entering **(create-option "routers" (create-ipaddr subnet 1))**.

Step 4 Click **Save**.

Create and Synchronize the Failover Pair

The example-cfg-admin next creates the failover server pair relationship and synchronizes the failover pair. The DHCP server at Boston becomes the main, and the server at Chicago becomes the backup.

Regional Web UI

Step 1 As the example-cfg-admin user, from the **Deploy** menu, choose **Failover Pairs** under the **DHCP** submenu.

Step 2 On the List/Add DHCP Failover Pairs page, click the **Add Failover Pair** icon in the **Failover Pairs** pane.

Step 3 On the Add DHCP Failover Pair dialog box, enter or choose the following values:

a) **Failover Pair Name**—Enter **central-fo-pair**.

b) **Main Server**—Click **Boston-cluster**.

c) **Backup Server**—Click **Chicago-cluster**.

d) **Scope Template**—Click **scopetemplate-1**

e) Click **Add Failover Pair**.

Step 4 Synchronize the failover pair with the local clusters:

a) On the List/Add DHCP Failover Pairs page, click the **Report** icon in the Synchronize column.

b) On the Report Synchronize Failover Pair page, accept **Local Server** as the source of network data.

c) Accept **Main to Backup** as the direction of synchronization.

d) Accept the operation **Update**.

e) Click **Report** at the bottom of the page.

f) On the View Failover Pair Sync Report page, click **Run Update**.

g) Click **Return**.

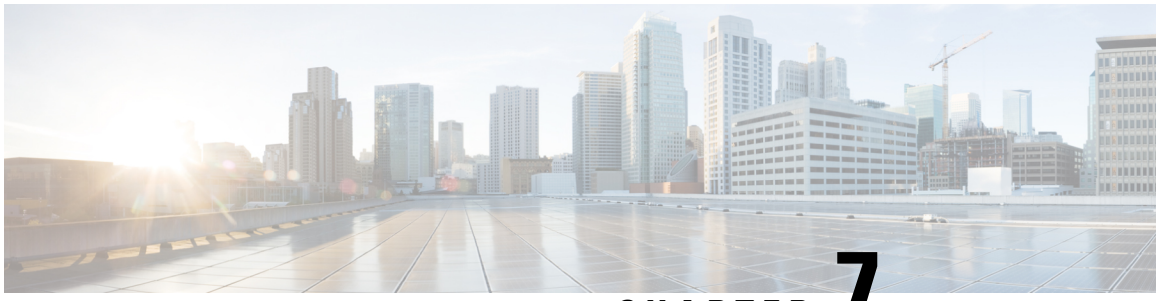
Step 5 Confirm the failover configuration and reload the server at the Boston cluster:

a) On the List/Add DHCP Failover Pairs page, click the **Go Local** icon next to Boston-cluster.

b) On the Manage DHCP Server page, click the **Reload** icon.

c) Click the **Go Regional** icon at the top of the page to return to the regional cluster.

Step 6 Confirm the failover configuration and reload the server at the Chicago cluster in the same way.



CHAPTER 7

Maintaining Servers and Databases

This chapter explains how to administer and control your local and regional server operations.

Managing Servers

If you are assigned the server-management subrole of the ccm-admin role, you can manage the Cisco Prime IP Express servers as follows:

- **Start**—Load the database and start the server.
- **Stop**—Stop the server.
- **Reload**—Stop and restart the server. (Note that you do not need to reload the server for all RR updates, even protected RR updates. For details, see *the "Managing DNS Update" chapter in Cisco Prime IP Express 9.0 DHCP User Guide*.)
- **Check statistics**—See the Displaying Statistics, on page 128.
- **View logs**—See the Searching the Logs, on page 121.
- **Manage interfaces**—See the specific protocol pages for how to manage server interfaces.

Starting and stopping a server is self-explanatory. When you reload the server, Cisco Prime IP Express performs three steps—stops the server, loads configuration data, and restarts the server. Only after you reload the server does it use your changes to the configuration.

Note The CDNS, DNS, DHCP, and SNMP servers are enabled by default to start on reboot. You can change this using [**server**] *type* **enable** or **disable start-on-reboot** in the CLI.

Note If **exit-on-stop** attribute of DHCP or DNS server is enabled, then the statistics and scope utilization data only from the last start (reload) is reported while if the attribute is disabled, information across reloads is displayed.

Local Basic or Advanced and Regional Web UI

You can manage the protocol servers in the following ways depending on if you are a:

- **Local or regional cluster administrator**—Choose **Manage Servers** from the **Operate** menu to open the Manage Servers page.

  The local and regional cluster web UI access to server administration is identical, even though the available functions are different. As a regional administrator, you can check the state and health of the regional CCM server and server agent. However, you cannot stop, start, reload, or view statistics, logs, or interfaces for them.

  At the local cluster, to manage the DHCP, DNS, CDNS, or SNMP servers, select the server in the Manage Servers pane and do any of the following:

  - Click the **Statistics** tab to view statistics for the server. (See the Displaying Statistics, on page 128.)
  - Click the **Logs** tab in the View Log column to view the log messages for the server. (See the Searching the Logs, on page 121.)
  - Click the **Start Server** button to start the server.
  - Click the **Stop Server** button stop the server.
  - Click the **Restart Server** button to reload the server.

- **Local cluster DNS administrator**—Choose **DNS Server** from the **Deploy** menu to open the Manage DNS Authoritative Server page.

  Along with the Statistics, Startup Logs, Logs, HA DNS Server Status, Start Server, Stop Server, and Restart Server functions, you can also perform other functions when you click the **Commands** button to open the DNS Commands dialog box.

  The server command functions are:

  - **Forcing all zone transfers** (see the *"Enabling Zone Transfers" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*)—Click the **Run** icon. This is the equivalent of **dns forceXfer secondary** in the CLI.
  - **Scavenging all zones** (see the *"Scavenging Dynamic Records" section in Cisco Prime IP Express 9.0 DHCP User Guide*)—Click the **Run** icon. This is the equivalent of **dns scavenge** in the CLI.

- **Local cluster Caching DNS server—**Choose **CDNS Server** from the **Deploy** menu to open the Manage DNS Caching Server page.

  Along with the Statistics, Startup Logs, Logs, Start Server, Stop Server, and Restart Server functions, you can also perform other functions when you click the **Commands** button to open the CDNS Commands dialog box.

  In Advanced and Expert modes, you can flush Caching CDNS cache and flush the resource records. Click the Commands button to execute the commands.

- **Local cluster DHCP administrator**—Click **DHCP Server** from the **Deploy** menu to open the Manage DHCP Server page.

Along with the Statistics, Startup Logs, Logs, Start Server, Stop Server, and Restart Server functions, you can also perform other functions when you click the **Commands** button to open the DHCP Server Commands dialog box.

This page provides the Get Leases with Limitation ID feature, to find clients that are associated through a common limitation identifier (see the *"Administering Option 82 Limitation" section in Cisco Prime IP Express 9.0 DHCP User Guide*). Enter at least the IP address of the currently active lease in the IP Address field, then click the **Run** icon. You can also enter the limitation ID itself in the form *nn***:***nn***:***nn* or as a string (**"***nnnn***"**), in which case the IP address becomes the network in which to search. This function is the equivalent of **dhcp limitationList** *ipaddress* [*limitation-id*] **show** in the CLI.

CLI Commands

In the CLI, the regional cluster allows CCM server management only:

- To start the server, use **server** *type* **start** (or simply *type* **start**; for example, **dhcp start**).
- To stop the server, use **server** *type* **stop** (or simply *type* **stop**; for example, **dhcp stop**). If stopping the server, it is advisable to save it first using the **save** command.
- To reload the server, use **server** *type* **reload** (or simply *type* **reload**; for example, **dhcp reload**). Cisco Prime IP Express stops the server you chose, loads the configuration data, and then restarts the server.
- To set or show attributes for the server, use [**server**] *type* **set** *attribute*=*value* or [**server**] *type* **show**. For example:

```
nrcmd> ccm set ipaddr=192.168.50.10
```

Scheduling Recurring Tasks

In Basic and Advanced user mode in the local cluster web UI, you can schedule a number of recurring tasks. These tasks are:

- Reloading the DHCP server.
- Reloading the DNS server.
- Synchronizing DHCP failover server pairs:
  - If in staged dhcp edit mode, reload the main DHCP server.
  - Synchronize the failover configuration to the backup DHCP server.
  - If in staged dhcp edit mode, reload the backup DHCP server.
- Synchronizing High-Availability (HA) DNS server pairs:
  - If in staged dhcp edit mode, reload the main DNS server.
  - Synchronize the HA DNS configuration to the backup DNS server.
  - If in staged dhcp edit mode, reload the backup DNS server.
- Synchronizing zone distribution maps:
  - If in staged dhcp edit mode, reload the main DNS server.
  - If in staged dhcp edit mode, reload the backup HA DNS server.
  - Synchronize the zone distribution maps.
  - If in staged dhcp edit mode, reload the secondary DNS server or servers.

Local Basic or Advanced Web UI

To set up one or more of these recurring server tasks:

Step 1 From the **Operate** menu, choose **Schedule Tasks** to open the List/Add Scheduled Tasks page.

Step 2 Click the **Add Scheduled Task** icon in the Scheduled Tasks pane on the left to open the Add Scheduled Task page.

Step 3 Enter values in the appropriate fields:

a) Name of the scheduled task. This can be any identifying text string.

b) Pull down from the available list of task types, which are:

- **dhcp-reload**—Reloads the DHCP server
- **dns-reload**—Reloads the DNS server
- **cdns-reload**—Reloads the Caching DNS server
- **sync-dhcp-pair**—Synchronizes the DHCP failover server pair
- **sync-dns-pair**—Synchronizes the HA DNS failover server pair
- **sync-zd-map**—Synchronizes zone distribution maps
- **sync-dns-update-map**—Synchronizes DNS update maps

c) Indicate the time interval for the scheduled task, such as 60m or 4w2d.

Step 4 Click **Add Scheduled Task**.

Step 5 If you click the name of the task on the List/Add Scheduled Tasks page, on the Edit Scheduled Task page you can view (in the Task Status section) the last status or the list of last errors (if any) that occurred during the task execution. Click **Run Now** to run the task immediately.

Note The DNS server startup and background loading slows down when HA is enabled before the HA DNS server communicates to its partner. You need to allow the HA DNS server to communicate with its partner before reloading or restarting the DNS server.

Logs

Log Files

The following table describes the Cisco Prime IP Express log files in the *install-path*/logs directory.

Table 14: Log Files in .../logs Directory

Component	File in /logs Directory	Local/Regional	Logs
Installation	install_cnr_log	Both	Installation process
Upgrade	ccm_upgrade_status_log	Both	Upgrade process
	dns_upgrade_status_log	Local	Upgrade process
Server agent	agent_server_1_log	Both	Server agent starts and stops

Component	File in /logs Directory	Local/Regional	Logs
Port check	checkports_log	Both	Network ports
DNS server	name_dns_1_log	Local	DNS activity
	dns_startup_log	Local	DNS startup activity
CDNS server	cdns_log	Local	CDNS activity
	cdns_startup_log	Local	CDNS startup activity
DHCP server	name_dhcp_1_log	Local	DHCP activity
	dhcp_startup_log	Local	DHCP startup activity
SNMP server	cnrsnmp_log	Both	SNMP activity
CCM database	config_ccm_1_log	Both	CCM configuration, starts, stops
	ccm_startup_log		CCM startup activity
Web UI	cnrwebui_log	Both	Web UI state
Tomcat/web UI (in cnrwebui subdirectory)	catalina.*date* .log.txt jsui_log.*date* .txt cnrwebui_access_log.*date* .txt	Both	CCM database for Tomcat server and web UI (Because new files are created daily, periodically archive old log files.)
Resource Limits	ccm_monitor_log	Both	Resource limit activity.

DNS, DHCP, CDNS, and CCM servers can generate a number of log files, each with a preconfigured maximum size of 10 MB. This preconfigured value applies to new installs only.

Note Upgrades from pre-9.0 versions will use the old preconfigured (or explicitly configured) value of 1,000,000 bytes for log files.

The first log file name has the _log suffix. When this file reaches its maximum size, it gets the .01 version extension appended to its name and a new log file is created without the version extension. Each version extension is incremented by one for each new file created. When the files reach their configured maximum number, the oldest file is deleted and the next oldest assumes its name. The usual maximum number is 10 for the DNS, DHCP, CDNS, and CCM servers.

Cisco Prime IP Express also has server_startup_log files. This applies to the CCM, DHCP, and DNS servers. These files log the start up and shut down phases of the server (the information is similar to the normal log file information). Server startup log files are useful in diagnosing problems that have been reported when the server was last started.

The number of these start-up logs is fixed at four for a server, and the size is fixed at 10 MB per server.

Note Some user commands can create *User authentication* entries in the Server Agent log because of separate connections to the cluster. Do not interpret these as a system security violation by another user.

Logging can also be directed to syslog. See Modifying the cnr.conf File, on page 141.

CLI Commands

You can check the configured maximums for the DNS and DHCP servers using [**server**] *type* **serverLogs show** in the CLI, which shows the maximum number (*nlogs*) and size (*logsize*) of these protocol server log files. You can adjust these parameters using [**server**] *type* **serverLogs set nlogs=***value* and [**server**] *type* **serverLogs set logsize=***value*. You cannot adjust these maximums for any of the other log files.

Note A change to the server logs will not take effect until you restart Cisco Prime IP Express.

Logging Server Events

When you start Cisco Prime IP Express, it automatically starts logging Cisco Prime IP Express system activity. Cisco Prime IP Express maintains all the logs by default on:

- **Windows**—*install-path*\logs
- **Linux**—*install-path*/logs (to view these logs, use the **tail -f** command)

Tip To avoid filling up the Windows Event Viewer and preventing Cisco Prime IP Express from running, in the Event Log Settings, check the **Overwrite Events as Needed** box. If the events do fill up, save them to a file, then clear them from the Event Log.

Local Basic or Advanced and Regional Web UI

Server logging is available in the web UI when you open the Manage Servers page for a server (see the Managing Servers, on page 115), then click the **Log** icon in the View Log column for the server. This opens the Log for Server page. The log is in chronological order with the page with the latest entries shown first. If you need to see earlier entries, click the left arrow at the top or bottom of the page.

Related Topics

Searching the Logs, on page 121

Logging Format and Settings, on page 120

Logging Format and Settings

The server log entries include the following categories:

- **Activity**—Logs the activity of your servers.
- **Info**—Logs standard operations of the servers, such as starting up and shutting down.

- **Warning**—Logs warnings, such as invalid packets, user miscommunication, or an error in a script while processing a request.
- **Error**—Logs events that prevent the server from operating properly, such as out of memory, unable to acquire resources, or errors in configuration.

Note Warnings and errors go to the Event Viewer on Windows (see the Tip in Logging Server Events, on page 120). For a description of the log messages for each server module, see the *install-path*/docs/msgid/MessageIdIndex.html file.

Local Basic or Advanced and Regional Web UI

You can affect which events to log. For example, to set the logging for the local cluster DNS and DHCP server:

- **DNS**—From the **Deploy** menu, choose **DNS Server** under the **DNS** submenu to open the Manage DNS Server page. Click the name of the server to open the Edit DNS Server page. Expand the Log Settings section to view the log settings. Make changes to the attributes as desired, click **Save**, and then reload the server. (See *Table 4 in the "Troubleshooting DNS Servers" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide* for the log settings to maximize DNS server performance.)
- **DHCP**—From the **Deploy** menu, choose **DHCP Server** under the **DHCP** submenu to open the Manage DHCP Server page. Click the name of the server to open the Edit DHCP Server page. Expand the Log Settings section to view the log settings. Make changes to the attributes as desired, click **Save**, and then reload the server. (See *Table 6 in the "Tuning the DHCP Server" section in Cisco Prime IP Express 9.0 DHCP User Guide* for the log settings to maximize DHCP server performance.)

CLI Commands

Use **dns set log-settings**=*value* and **dhcp set log-settings**=*value* for the respective servers.

Searching the Logs

The web UI provides a convenient way to search for entries in the activity and startup log files. You can locate specific message text, log message IDs, and message timestamps using a regular expression string entry. When you click the **Log** icon in the View Log or View Startup Log column on the Manage Servers page (or one of the specific server pages), this opens a Log for Server page. In the text field next to the Search icon at the top or bottom of the page, enter the search string in the regular expression syntax. (For example, entering **name?** searches for occurrences of the string *name* in the log file.) Click the **Search** icon to view the results of log search.

Click the name of the log message, which opens the Log for Server page with the full message text. To view the full message text, click the name of the log message. Change between Table and Text view by clicking the **Log** icon. Click **Close** on the Log Search Result page to close the browser window.

View Change Log

In the web UI, you can view the change logs and tasks associated with configurations you make.

Local Basic and Advanced Web UI

From the **Operate** menu, choose **Change Log**. To view the change log, you must be assigned the database subrole of the ccm-admin or regional-admin role:

- The View Change Log pageshows all the change logs, sorted by DBSN name. To get to the bottom of the list, click the right arrow at the bottom left of the page. Click the DBSN number of the change log entry to open a View Change Set page for it.

  On the View Change Log page, you can filter the list, manually trim it, and save it to a file. You can filter the list by:

- Start and end dates
- Administrator who initiated the changes
- Configuration object class
- Specific object
- Object identifier (ID), in the format OID-00:00:00:00:00:00:00:00
- Server
- Database

Click **Filter List** or **Clear Filter** (to clear the filter that persists through the session). You can initiate a trim of the change log by setting how many days old you want the record to get before trimming it, by setting a number of days value in the "older than" field and clicking the **Delete** icon.

To save the change log entries to a comma-separated values (CSV) file, click the **Save** icon.

If a task is associated with a change log, it appears on the View Change Set page. You can click the task name to open the View CCM Task page for it.

Dynamic Update on Server Log Settings

The DHCP and the DNS servers register the changes on the server logs only during the server configuration, which happens during a reload. Reloading the servers is time consuming. Cisco Prime IP Express allows the DHCP and DNS servers to register the changes to log settings, without a reload.

Local Basic or Advanced Web UI

To dynamically update DHCP server log settings, do the following:

Step 1 From the **Deploy** menu, choose **DHCP Server** under the **DHCP** submenu. The Manage DHCP Server page appears.

Step 2 Click the name of the DHCP server in the left pane to open the Edit DHCP Server page.

Step 3 Modify the log settings as desired.

Step 4 Click **Save** at the bottom of the page. The new log settings are applied to the DHCP server. The Manage DHCP Server page is displayed with an updated page refresh time.

Local Basic or Advanced Web UI

To dynamically update DNS server log settings, do the following:

Step 1 From the **Deploy** menu, choose **DNS Server** under the **DNS** submenu. This opens the Manage DNS Server page.

Step 2 Click the name of the DNS server in the left pane to open the Edit DNS Server page.

Step 3 Modify the log settings as desired.

Step 4 Click **Save** at the bottom of the page. The new log settings are applied to the DNS server. The Manage DNS Server page is displayed with an updated page refresh time.

Note If the dhcp-edit-mode or dns-edit-mode is set to synchronous, and if the server running, the change in server log settings is communicated to the server.

CLI Commands

To dynamically update the DHCP or DNS server log settings using the CLI, you must have the appropriate edit-mode set to synchronous. After changing the server log settings, use the save command to save the settings.

For example:

```
nrcmd> session set dhcp-edit-mode=synchronous
nrcmd> dhcp set log-settings=new-settings
nrcmd> save
```

Running Data Consistency Rules

Using consistency rules, you can check data inconsistencies such as overlapping address ranges and subnets. You can set data consistency rules at the regional and local clusters.

The table on the List Consistency Rules page explains these rules. Check the check box next to the rule that you want to run.

Note You must set the locale parameters on UNIX to en_US.UTF-8 when running Java tools that use Java SDK, such as cnr_rules.

The List Consistency Rules page includes functions to select all rules and clear selections. You can show the details for each of the rule violations as well as view the output. The rule selections you make are persistent during your user session.

Local Basic or Advanced and Regional Web UI

To run consistency rules, do the following:

Step 1 From the **Operate** menu, choose **Consistency Reports** under the **Reports** submenu.

The List Consistency Rules page appears.

Step 2 Check the check boxes for each of the listed consistency rules that you want to apply.

- To select all the rules, click the **Select All Rules** link.
- To clear all selections, click the **Clear Selection** link.

Step 3 Click **Run Rules**.

The Consistency Rules Violations page appears.The rules are categorized by violation type.

- To show details for the violations, click the **Show Details** link.
- To show the output, click the page icon.

Step 4 Click **Return to Consistency Rules** to return to the List Consistency Rules page.

CLI Tool

Use the **cnr_rules** consistency rules tool from the command line to check for database inconsistencies. You can also use this tool to capture the results of the rule in a text or XML file.

The cnr_rules tool is located at:

- **Windows**—...\bin\cnr_rules.bat
- **Linux**—.../usrbin/cnr_rules

To run the **cnr_rules** tool, enter:

```
> cnr_rules -N username -P password [options]
```

- **–N** *username* —Authenticates using the specified username.
- **–P** *password* —Authenticates using the specified password.
- *options* —Describes the qualifying options for the tool, as described in the following table. If you do not enter any options, the command usage appears.

Table 15: cnr_rules Options

Option	Description
Example	
–list	Lists the available consistency rules. **Note** The list of available commands is tailored to the permissions of the administrator specified in the value of the –**N** option.
	`> cnr_rules -N admin -P changeme -list`

Option	Description
–run [**rule-match**]	Run the available rules. Optionally, you can run a subset of the available rules by applying a case-insensitive rule-match string.

	• Runs all rules:
	`> cnr_rules -N admin -P changeme -run`
	• Runs only the rules whose names contain the string “dhcp”:
	`> cnr_rules -N admin -P changeme -run dhcp`
	Tip To match a string containing spaces, enclose the string using double-quotation marks ("). For example: > **cnr_rules -N admin -P changeme -run "router interface"**

–details	Includes details of the database objects that violate consistency rules in the results.
	Runs the DNS rules, and includes details of the database object in the results: `> cnr_rules -N admin -P changeme -run DNS -details`
–xml	Generates rule results in an XML file. **Note** When using the **–xml** option, the **–details** option is ignored because the XML file includes all the detailed information.
	`> cnr_rules -N admin -P changeme -run -xml`
–path *classpath*	Changes the Java classpath that is searched to locate the available consistency rules (optional). In order to run a new, custom consistency rule, you can use this option. You must get the support of a support engineer to do this.

Option	Description
–interactive	Runs the tool in an interactive session.

	`> cnr_rules -N admin -P changeme -run -interactive`
	`RuleEngine [type ? for help] > ?`
	`Commands:`
	`  load <class>  // load the specified rule class`
	`  run <rule-match> // run rules matching a string, or '*' for all`
	`  list  // list rules by name`
	`  xml  // toggle xml mode`
	`  detail  // toggle detail mode (non-xml only)`
	`  quit  // quit RuleEngine`

–both	Displays domain names in both Unicode and ASCII.

You can redirect the output of any of these preceding commands to another file. Use the following syntax to capture the rule results in a:

- Text file:

```
> cnr_rules -N username -P password -run -details > filename.txt
```

- XML file:

```
> cnr_rules -N username -P password -run -xml > filename.xml
```

Monitoring and Reporting Server Status

Monitoring the status of a server involves checking its:

- State
- Health
- Statistics
- Log messages
- Address usage
- Related servers (DNS and DHCP)
- Leases (DHCP)

Related Topics

Server States, on page 127

Displaying Health, on page 127

Displaying Statistics, on page 128

Displaying IP Address Usage, on page 137

Displaying Related Servers, on page 137

Displaying Leases, on page 140

Server States

All Cisco Prime IP Express protocol servers (DNS, DHCP, and SNMP) pass through a state machine consisting of the following states:

- **Loaded**—First step after the server agent starts the server (transitional).
- **Initialized**—Server was stopped or fails to configure.
- **Unconfigured**—Server is not operational because of a configuration failure (transitional).
- **Stopped**—Server was administratively stopped and is not running (transitional).
- **Running**—Server is running successfully.

The two essential states are initialized and running, because the server transitions through the states so quickly that the other states are essentially invisible. Normally, when the server agent starts the server, it tells the server to be up. The server process starts, sets its state to loaded, then moves up to running. If you stop the server, it walks down the states to initialized, and if you restart, it moves up to running again. If it fails to configure for some reason, it drops back to initialized, as if you had stopped it.

There is also an exiting state that the server is in very briefly when the process is exiting. The user interface can also consider the server to be disabled, but this rarely occurs and only when there is no server process at all (the server agent was told not to start one).

Displaying Health

You can display aspects of the health of a server, or how well it is running. The following items can decrement the server health, so you should monitor their status periodically. For the:

- Server agent (local and regional clusters)
- CCM server (local and regional clusters)
- DNS server (local cluster):
    - Configuration errors
    - Memory
    - Disk space usage
    - Inability to contact its root servers
- Caching DNS server (local cluster)
- DHCP server (local cluster):
    - Configuration errors
    - Memory
    - Disk space usage
    - Packet caching low
    - Options not fitting in the stated packet limit
    - No more leases available

Server Health Status

The server health status varies from the value 0 to 10. The value 0 means the server is not running and 10 means the server is running. Some of the servers report only 0 or 10, and not anything in between. When a server reports a value from 1 to 9, it means that it detected conditions that indicate possible problems. It has nothing to do with the actual performance of the server. So, if the health of the server is a value from 1 to 9, the server log files need to be reviewed to see what errors were logged.

Note Depending on the level of activity and the size and number of log files, the condition that reduced the server health might not be visible in the log files. It is important to review the log files, but the servers do not log all the conditions that reduce the server health.

The following conditions can reduce the DHCP server health:

- Configuration errors (occurs when the server is getting started or restarting)
- When the server detects out-of-memory conditions
- When packet receive failures occur
- When packets are dropped because the server is out of request or response buffers
- When the server is unable to construct a response packet

Tip Health values range from 0 (the server is not running) to 10 (the highest level of health). It is recommended that the health status can be ignored, with the understanding that zero means server is not running and greater than zero means server is running. On Linux, you can run the **cnr_status** command, in the *install-path* /usrbin/ directory, to see if your local cluster server is running. For more information on how to check whether the local cluster server is running, see the *Cisco Prime IP Express Installation Guide*.

Local Basic or Advanced and Regional Web UI

From the **Operate** menu, select **Manage Servers**. Check the Manage Servers page for the state and health of each server.

CLI Commands

Use [**server**] *type* **getHealth**. The number 10 indicates the highest level of health, 0 that the server is not running.

Displaying Statistics

To display server statistics, the server must be running.

Local Basic or Advanced and Regional Web UI

Go to the Manage Servers page, click the name of the server in the left pane, then click the **Statistics** tab, if available. On the Server Statistics page, click the name of the attribute to get popup help.

The DHCP, DNS, and CDNS statistics are each divided into two groups of statistics. The first group is for total statistics and the second group is for sample statistics. The total statistics are accumulated over time. The sample statistics occur during a configurable sample interval. The names of the two categories vary per server and per user interface, and are identified in the following table.

Table 16: Server Statistics Categories

Server	User Interface	Total Statistics (Command)	Sample Statistics (Command)
DHCP	Web UI	Total Statistics	Activity Summary
	CLI	Total Counters since the start of the last DHCP server process (**dhcp getStats**)	Sampled counters since the last sample interval (**dhcp getStats sample**)
DNS	Web UI	Total Statistics	Sample Statistics
	CLI	Total Counters since the start of the last server process (**dns getStats**)	Sampled counters since the last sample interval (**dns getStats sample**
CDNS	Web UI	Total Statistics	Sample Statistics
	CLI	Total Counters since the start of the last server process (**cdns getStats total)**	Sampled counters since the last sample interval (**cdns getStats sample**)

To set up the sample counters, you must activate either the *collect-sample-counters* attribute for the server or a *log-settings* attribute value called activity-summary. You can also set a *log-settings* value for the sample interval for each server, which is preset to 5 minutes. The *collect-sample-counters* attribute is preset to true for the DNS server, but is preset to false for the DHCP server. For example, to enable the sample counters and set the interval for DHCP, set the following attributes for the DHCP server:

- Enable *collect-sample-counters* (**dhcp enable collect-sample-counters**)
- Set *log-settings* for activity-summary (**dhcp set log-settings=activity-summary**)
- Set *activity-summary-interval* to 5m (**dhcp set activity-summary-interval=5m**)

CLI Commands

In the CLI, if you use [**server**] *type* **getStats**, the statistics are encoded in curly braces followed by sets of digits, as described in Table 17: DNS Statistics for DNS and Table 19: DHCP Statistics for DHCP. The **server** *type* **getStats all** command is more verbose and identifies each statistic on a line by itself. Using the additional **sample** keyword shows the sample statistics only.

Reset the counters and total statistic by using **dhcp resetStats**, **dns resetStats**, or **cdns resetStats**.

DNS Statistics

The DNS server statistics in the web UI appear on the DNS Server Statistics page, click on the statistic's name to read its description. You can refresh the DNS Server Statistics.

The DNS server statistics that you can view are:

- Attribute—Displays server statistics such as server identifier, recursive service, process uptime, time since reset, and so on.

Total Statistics

- Performance Statistics—Displays the total statistics of the DNS Server performance.
- Query Statistics—Displays the total statistics of the queries.
- HA Statistics—Displays the total statistics of the HA DNS Server.
- Push Notification Statistics—Displays the total statistics of DNS Push Notifications.
- Security Statistics—Displays the total statistics of the security.
- IPv6 Statistics—Displays the total statistics of the IPv6 packets received and sent.
- Error Statistics—Displays the total statistics of the errors.
- Max Counter Statistics—Displays the total statistics of the maximum number of concurrent threads, RRs, DNS update latency, concurrent packets, and so on.

Sample Statistics

- Performance Statistics—Displays the sample statistics about the DNS Server performance.
- Query Statistics—Displays the sample statistics about the queries.
- HA Statistics—Displays the sample statistics about the HA DNS Server.
- Push Notification Statistics—Displays the sample statistics of DNS Push Notifications.
- Security Statistics—Displays the sample statistics about the security.
- IPv6 Statistics—Displays the sample statistics about the IPv6 packets received and sent.
- Error Statistics—Displays the sample statistics about the errors.

Note To get the most recent data, click the **Refresh Server Statistics** icon at the top left of the Statistics page.

The **dns getStats** command has the following options:

```
dns getStats [performance | query | errors | security | maxcounters | ha | ipv6 | dns-pn |
 all] [total | sample]
```

The **dns getStats all** command is the most commonly used. The **dns getStats** command without **all** option returns the statistics in a single line of positional values in the following format (the table below shows how to read these values):

```
nrcmd> dns getStats

100 Ok
{1} 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
```

Table 17: DNS Statistics

Digit	Statistic	Description
{1}	id	Implementation ID (release and build information).
2	config-recurs	Recursion services—(1) available, (2) restricted, (3) unavailable.
3	config-up-time	Time (in seconds) elapsed since the last server startup.

Digit	Statistic	Description
4	config-reset-time	Time (in seconds) elapsed since the last server reset (restart).
5	config-reset	Status or action to reinitializes any name server state—If using the (2) reset action, reinitializes any persistent name server state; the following are read-only statuses: (1) other—server in some unknown state, (3) initializing, or (4) running.
6	counter-auth-ans	Number of queries answered authoritatively.
7	counter-auth-no-names	Number of queries returning authoritative no such name responses.
8	counter-auth-no-data-resps	Number of queries returning authoritative no such data (empty answer) responses. (Deprecated statistics)
9	counter-non-auth-datas	Number of queries answered nonauthoritatively (cached). (Deprecated statistics)
10	counter-non-auth-no-datas	Number of queries answered nonauthoritatively with no data.
11	counter-referrals	Number of queries forwarded to other servers.
12	counter-errors	Number of responses answered with errors (RCODE values other than 0 or 3).
13	counter-rel-names	Number of requests received for names of only one label (relative names).
14	counter-req-refusals	Number of refused queries.
15	counter-req-unparses	Number of unparsable requests.
16	counter-other-errors	Number of aborted requests due to other errors.
17	total-zones	Total number of configured zones.

CDNS Statistics

The CDNS server statistics in the web UI appear on the DNS Caching Server Statistics page, click on the name of the statistics to read its description. You can refresh the CDNS Server Statistics.

Table 18: CDNS Statistics

Digit	Statistic	Description
{1}	name	Name identifying the DNS Caching Server.
2	time-current	The current time given by the CDNS Server.
3	time-up	The amount of time the server has been up and running.
4	time-elapsed	The elapsed since last statistics poll.
5	queries-total	Total number of queries received by the CDNS Server.
6	queries-over-tcp	Total number of queries received over TCP by the CDNS Server.
7	queries-over-ipv6	Total number of queries received over TCP by the CDNS Server.
8	queries-with-edns	Number of queries with EDNS OPT RR present.
9	queries-with-edns-do	Number of queries with EDNS OPT RR with DO (DNSSEC OK) bit set.
10	queries-type-A	Number of A queries received.
11	queries-type-AAAA	Number of AAAA queries received.
12	queries-type-CNAME	Number of CNAME queries received.
13	queries-type-PTR	Number of PTR queries received.
14	queries-type-NS	Number of NS queries received.
15	queries-type-SOA	Number of SOA queries received.
16	queries-type-MX	Number of MX queries received.
17	queries-type-DS	Number of DS queries received.

Digit	Statistic	Description
18	queries-type-DNSKEY	Number of DNSKEY queries received.
19	queries-type-RRSIG	Number of RRSIG queries received.
21	queries-type-NSEC	Number of NSEC queries received.
22	queries-type-NSEC3	Number of NSEC3 queries received.
23	queries-type-other	Number of queries received of type 256+.
24	queries-with-flag-QR	Number of incoming queries with QR (query response) flag set. These queries are dropped.
25	queries-with-flag-AA	Number of incoming queries with AA (auth answer) flag set. These queries are dropped.
26	queries-with-flag-TC	Number of incoming queries with TC (truncation) flag set. These queries are dropped.
27	queries-with-flag-RD	Number of incoming queries with RD (recursion desired) flag set.
28	queries-with-flag-RA	Number of incoming queries with RA (recursion available) flag set.
29	queries-with-flag-Z	Number of incoming queries with Z flag set.
30	queries-with-flag-AD	Number of incoming queries with AD flag set.
31	queries-with-flag-CD	Number of incoming queries with CD flag set.
32	queries-failing-acl	Number of queries being dropped or refused due to ACL failures.
33	cache-hits	The total number of queries that were answered from cache.
34	cache-misses	The total number of queries that were not found in the cache.
35	cache-prefetches	Number of prefetches performed.

Digit	Statistic	Description
36	requestlist-total	The total number of queued requests waiting for recursive replies.
37	requestlist-total-user	The total number of queued user requests waiting for recursive replies.
38	requestlist-total-system	The total number of queued system requests waiting for recursive replies.
39	requestlist-total-average	The average number of requests on the request list.
40	requestlist-total-max	The maximum number of requests on the request list.
41	requestlist-total-overwritten	The number of requests on the request list that were overwritten by newer entries.
42	requestlist-total-exceeded	The number of requests dropped because the request list was full.
43	recursive-replies-total	The total number of recursive queries replies.
44	recursive-time-average	The average time to complete a recursive query.
45	recursive-time-median	The median time to complete a recursive query.
46	mem-process	An estimate of the memory in bytes of the CDNS process.
47	mem-cache	Memory in bytes of RRSet cache.
48	mem-query-cache	Memory in bytes of incoming query message cache.
49	mem-iterator	Memory in bytes used by the CDNS iterator module.
50	mem-validator	Memory in bytes used by the CDNS validator module.
51	answers-with-NOERROR	Number of answers from cache or recursion that result in rcode of NOERROR being returned to client.

Digit	Statistic	Description
52	answers-with- NXDOMAIN	Number of answers from cache or recursion that result in rcode of NXDOMAIN being returned to client.
53	answers-with-NODATA	Number of answers that result in pseudo rcode of NODATA being returned to client.
54	answers-with-other-errors	Number of answers that result in pseudo rcode of NODATA being returned to client.
55	answers-secure	Number of answers that correctly validated.
56	answers-unsecure	Number of answers that did not correctly validate.
57	answers-rrset-unsecure	Number of RRSets marked as bogus by the validator.
58	answers-unwanted	Number of replies that were unwanted or unsolicited. High values could indicate spoofing threat.
59	reset-time	Reports the most recent time the stats were reset (i.e. **cdns resetStats** in nrcmd).
60	sample-time	Reports the time the server collected the last set of sample statistics.
61	sample-interval	Reports the sample interval used by the server when collecting sample statistics.

DHCP Statistics

The DHCP server statistics in the web UI appear on the DHCP Server Statistics page, click on the statistic's name to read its description.

The DHCP server statistics details are available for:

- Attribute—Displays the server statistics such as server start time, server reload time, server up time, and statistics reset time.
- Total Statistics—Displays the total statistics of the scopes, request buffers, response buffers, packets and so on.

- Lease Counts (IPv4)—Displays the sample statistics of the IPv4 lease counts such as active leases, configured leases, reserved leases, and reserved active leases.
- Packets Received (IPv4)—Displays the sample statistics of the IPv4 packets received.
- Packets Sent (IPv4)—Displays the sample statistics of the IPv4 packets sent.
- Packets Failed (IPv4)—Displays the statistics of the failed IPv4 packets.

The Additional Attributes are:

- Failover Statistics—Displays the statistics of the DHCP failover server.
- IPv6 Statistics—Displays the statistics of the IPv6 prefixes configured, timed-out IPv6 offer packets and so on.
- Lease Counts (IPv6)—Displays the statistics of the IPv6 lease counts of active leases, configured leases, reserved leases, and reserved active leases.
- Packets Received (IPv6)—Displays the statistics of the IPv6 packets received.
- Packets Sent (IPv6)—Displays the statistics of the IPv6 packets sent.
- Packets Failed (IPv6)—Displays the statistics of the failed IPv6 packets.

Additional Attributes also includes Top Utilized Aggregations.

Note To get the most recent data, click the **Refresh Server Statistics** icon at the top left of the Statistics page.

The **dhcp getStats** command has the following options:

```
dhcp getStats [[all | server [,] failover [,] dhcpv6] [total | sample]
```

The **dhcp getStats all** command is the most commonly used. The **dhcp getStats** command without **all** option returns the statistics in a single line of positional values in the following format (the table below shows how to read these values):

```
nrcmd> dhcp getStats

100 Ok
{1} 2 3 4 5 6 7 8
```

Table 19: DHCP Statistics

Digit	Statistic	Description
{1}	start-time-str	Date and time of last server reload, as a text string.
2	total-discovers	Number of DISCOVER packets received.
3	total-requests	Number of REQUEST packets received.
4	total-releases	Number of RELEASED packets received.
5	total-offers	Number of OFFER packets sent.
6	total-acks	Number of acknowledgement (ACK) packets sent.

Digit	Statistic	Description
7	total-naks	Number of negative acknowledgement (NAK) packets sent.
8	total-declines	Number of DECLINE packets received.

Displaying IP Address Usage

Displaying IP address usage gives an overview of how clients are currently assigned addresses.

Local Advanced and Regional Web UI

You can look at the local or regional cluster address space, or generate a subnet utilization or lease history report at the regional cluster, to determine IP address usage. These functions are available in both web UIs in the **Design > DHCPv4** menu, if you have address space privileges at the local or regional cluster.

You can determine the current address space utilization by clicking the **View** icon in the Current Usage column for the unified address space, address block, and subnet (see the *"Viewing Address Utilization for Address Blocks, Subnets, and Scopes" section in Cisco Prime IP Express 9.0 DHCP User Guide*). You can also get the most current IP address utilization by querying the lease history (see the *"Querying Leases" section in Cisco Prime IP Express 9.0 DHCP User Guide*). In the latter case, the regional CCM server references the appropriate DHCP server directly. To ensure this subnet-to-server mapping, you must update the regional address space view so that it is consistent with the relevant local cluster. Do this by pulling the replica address space, or reclaiming the subnet to push to the DHCP server (see the *"Reclaiming Subnets" section in Cisco Prime IP Express 9.0 DHCP User Guide*). Also ensure that the particular DHCP server is running.

CLI Commands

You can generate an IP address usage report using the **report** command. The command has the following syntax:

```
report [column-separator=string]
       [dhcp-only]
       [dhcpv4]
       [dhcpv6]
       [file=outputfile]
       [vpn=name]
```

The column-separator specifies the character string that separates the report columns (the preset value is the space character). If you want to include more than one space, precede them with the backslash (\) escape character (enclosed in quotation marks). You can specify DHCPv4 or DHCPv6 addresses (**dhcp-only** is the same as **dhcpv4**). Not specifying the VPN returns the addresses in the current VPN only.

Displaying Related Servers

Cisco Prime IP Express displays the relationship among servers in a DNS zone distribution or a DHCP failover configuration. In the web UI, you can view a related servers page when you click the **Related Servers** icon on various pages. You can use the display of related servers to diagnose and monitor misconfigured or unreachable servers.

Related Topics

Monitoring Remote Servers Using Persistent Events, on page 138
DNS Zone Distribution Servers, on page 139
DHCP Failover Servers, on page 140

Monitoring Remote Servers Using Persistent Events

To service clients that require updates to DNS and LDAP related servers, the DHCP server uses a persistent event algorithm to ensure updates to related servers when a related server is temporarily unavailable. In addition, the algorithm prevents a misconfigured or offline DNS server from using up all the available update resources.

At startup, the DHCP server calculates the number of related servers in the configuration that require persistent events. A preconfigured Maximum Pending Events attribute (an Expert mode attribute that specifies the number of in-memory events that is preset to 40,000) is divided by the number of servers to obtain a limit on the number of events permitted for each remote server. This calculation covers related DNS and LDAP servers (DHCP failover does not use persistent storage for events). The DHCP server uses this calculation to issue log messages and take the action described in the following table. The table shows a hypothetical case of a DHCP server with four related DNS servers each having a limit of 10K events.

Table 20: Persistent Event Algorithm

Event Reached	DHCP Server Action
50% of the calculated per-server limit (Maximum Pending Events value divided by the number of total related servers); for example, 5K events on a related server out of a total of 40K maximum pending events	Issues an INFO log message every 2 minutes, as long as the limits are exceeded: `The queue of events for the name remote server at address has x events, and has reached the info limit of y/2 events out of an upper limit of y events per remote server. The remote server may be misconfigured, inoperative, or unreachable.`
100% of the calculated per-server limit and less than 50% of the Maximum Pending Events value; for example, 10K events on a related server, with fewer than 10K total maximum pending events	Issues a WARNING log message every 2 minutes, as long as the limits are exceeded: `The queue of events for the name remote server at address has x events, has exceeded the limit of y events per remote server, but is below the limit of z total events in memory. The remote server may be misconfigured, inoperative, or unreachable.`

Event Reached	DHCP Server Action
100% of the calculated per-server limit and 50% or more of the Maximum Pending Events value; for example, 10K events on a related server, with 20K total maximum pending events	Issues an ERROR log message every 2 minutes, as long as the limits are exceeded: `The queue of events for the name remote server at address has x events, and has grown so large that the server cannot continue to queue new events to the remote server. The limit of y events per remote server and z/2 total events in memory has been reached. This and future updates to this server will be dropped. The current eventID n is being dropped.` The server drops the current triggering event and all subsequent events with that server.
100% of the Maximum Pending Events value; for example, 40K events across all related servers	Issues an ERROR log message: `The queue of pending events has grown so large that the server cannot continue to queue new events. The queue's size is z, and the limit is z.` The server drops all subsequent events with all related servers.

SNMP traps and DHCP server log messages also provide notification that a related server is unreachable.

DNS Zone Distribution Servers

A DNS zone distribution simplifies creating multiple zones that share the same secondary server attributes. You can view and set the primary and secondary DNS servers in a zone distribution.

Local Basic or Advanced Web UI

From the **Deploy** menu, click **Zone Distribution** under the **DNS** submenu. This opens the List/Add Zone Distributions page. The local cluster allows only one zone distribution, the default. Click this zone distribution name to open the Edit Zone Distribution page, which shows the authoritative and secondary servers in the zone distribution.

Regional Web UI

From the **Deploy** menu, choose **Zone Distribution** under the **DNS** submenu. This opens the List/Add Zone Distributions page. The regional cluster allows creating more than one zone distribution. Click the zone distribution name to open the Edit Zone Distribution page, which shows the name of the zone distribution map, primary, authoritative, and secondary servers in the zone distribution.

Note Default zone distribution names are not editable. However, non-default zone distribution names are editable and can be saved.

CLI Commands

Create a zone distribution using **zone-dist** *name* **create** *primary-cluster* [*attribute=value*], then view it using **zone-dist list**. For example:

```
nrcmd> zone-dist distr-1 create Boston-cluster

nrcmd> zone-dist list
```

DHCP Failover Servers

Related servers in a DHCP failover pair relationship can show the following information:

- **Type**—Main or backup DHCP server.
- **Server name**—DNS name of the server.
- **IP address**—Server IP address in dotted octet format.
- **Requests**—Number of outstanding requests, or two dashes if not applicable.
- **Communication status**—OK or INTERRUPTED.
- **Cluster state**—Failover state of this DHCP server.
- **Partner state**—Failover state of its partner server.

For details on DHCP failover implementation, see the *"Managing DHCP Failover" section in Cisco Prime IP Express 9.0 DHCP User Guide*

Local Basic or Advanced Web UI

From the **Deploy** menu, choose **Failover Pairs** under the **DHCP** submenu. The List/Add DHCP Failover Pairs page shows the main and backup servers in the failover relationship.

CLI Commands

Use **dhcp getRelatedServers** to display the connection status between the main and partner DHCP servers. If there are no related servers, the output is simply 100 Ok.

Displaying Leases

After you create a scope, you can monitor lease activity and view lease attributes.

Local Basic or Advanced Web UI

From the **Design** menu, choose **Scopes** under the **DHCPv4** submenu; or from the **Design** menu, choose **Prefixes** under the **DHCPv6** submenu. On the List/Add DHCP Scopes or List/Add DHCPv6 Prefixes page, click the **View** icon in the Leases column to open the List DHCP Leases for Scope or List DHCP Leases for Prefix page.

Regional Advanced Web UI

From the **Operate** menu, choose **DHCPv4 Lease History** or **DHCPv6 Lease History** under the **Reports** submenu. Set the query parameters and then query the lease history. (See the *"Querying Leases" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*.)

Troubleshooting DHCP and DNS Servers

The following sections describe troubleshooting the configuration and the DNS and DHCP servers.

Related Topics

Immediate Troubleshooting Actions, on page 141

Immediate Troubleshooting Actions

When facing a problem, it is crucial not to cause further harm while isolating and fixing the initial problem. Here are things to do (or avoid doing) in particular:

- Have 512 MB or more of memory and 2.5 GB or more of a data partition.
- Do not reboot a cable modem termination system (CMTS).
- Enable DHCP failover.
- Do not reload, restart, or disrupt Cisco Prime IP Express with failover resynchronization in progress.

Modifying the cnr.conf File

Cisco Prime IP Express uses the **cnr.conf** file for basic configuration parameters. This file is normally located in the *install-path* /conf directory. Cisco Prime IP Express creates the file during installation and processes it line by line.

You can edit this file if configuration parameters change. Note that during normal operation, you would not want to change the values. However, certain conditions might require you to modify certain values, such as when you move the data files for disk space reasons.

The format of the **cnr.conf** file consists of parameter name-value pairs, one per line; for example, for a Windows local cluster installation:

```
cnr.rootdir=C:\\Program Files (x86)\\Cisco Prime IP Express\\Local
cnr.ccm-port=1234
cnr.cisco-gss-appliance-integration=n
cnr.datadir=C:\\CiscoPrimeIPExpress\\Local\\data
cnr.java-home=C:\\Program Files\\Java\\jre1.5.0_12
cnr.logdir=C:\\CiscoPrimeIPExpress\\Local\\logs
cnr.https-port=8443
cnr.tempdir=C:\\CiscoPrimeIPExpress\\Local\\temp
cnr.http-port=8080
cnr.ccm-mode=local
cnr.ccm-type=cnr
cnr.http-enabled=y
cnr.https-enabled=n
cnr.keystore-file=C:
cnr.keystore-password=unset
cnr.backup-time=23:45
```

Directory paths must be in the native syntax for the operating system. The format allows the use of colons (:) in directory paths, but not as name-value pair separators; it does not allow line continuation or embedded unicode characters. Other modifications to the file might include the location of the log directory (see Log Files, on page 118) or the time cnr_shadow_backup backups should occur (see Setting Automatic Backup Time, on page 149).

In rare cases, you might want to modify the file; for example, to exclude certain data from daily backups due to capacity issues. To do this, you need to add the appropriate settings manually.

Caution We recommend that you use the default settings in this file. If you must change these settings, do so only in consultation with the Cisco Technical Assistance Center (TAC) or the Cisco Prime IP Express development team.

The following settings are supported:

- cnr.backup-dest—Specify the destination to place backed up databases. Defaults to cnr.datadir if not specified.
- cnr.backup-dbs—Provide a comma-separated list of the databases you want to backup. For a local cluster the default is ccm,dhcp,dns,mcd. For a regional cluster it is ccm,lease6hist,leasehist,subnetutil,replica.
- cnr.backup-files—Provide a comma-separated list of files and the complete path to the files that you want copied as part of the backup. Files are copied to cnr.backup-dest.
- cnr.dbrecover-backup—Specify whether to run db recover and db verify on a backed up Oracle Berkeley database. The default is true. This setting is used for daily backups only. Manual backups ignore this setting. Disabling the automatic operation means that you must run the operation manually, preferably on a separate machine, or at a time when the Cisco Prime IP Express servers are relatively idle.
- cnr.daily-backup—Specify whether to run the daily back up. The default is true.

Modifying the cnr.conf File for Syslog Support

Cisco Prime IP Express supports logging to a Syslog server (on Linux). The Syslog support is not enabled by default. To configure which messages need to be logged, based on logging levels, the cnr.conf file must be updated.

In addition, on Windows, event logging for Warnings and Errors is enabled by default (for Windows Event log). In this release, you can log more (or less) to the event log by changing the log settings.

The following cnr.conf configuration parameters are supported:

- cnr.syslog.enable—Specifies whether logging to Syslog server or Windows Event log is enabled for Prime IP Express servers.
  - To disable all logging, the value can be 0, off, or disabled.
  - To enable all logging, the value can be 1, on, or enabled.
  - By default, this parameter is disabled for Linux and enabled for Windows.
- cnr.syslog.levels—Specifies the severity levels to be logged to Syslog or Windows Event log. If Syslog is enabled, this defaults to warning and error. The value can be a case-blind, comma separated, list of the following keywords: error, warning, info, activity, and debug. This parameter is ignored if Syslog is disabled.

Note While it is possible to enable all of the severity levels and thus all messages written to the server log files are also logged to Syslog, this is not recommended unless the server log settings are reviewed and minimized. The performance impact on Syslog and the servers may vary greatly depending on how logging is configured. Syslog may rate limit the messages, so useful messages may also be lost.

- cnr.syslog.facility-Specifies the facility under which Syslog logs (Linux OS). This parameter is ignored for Windows. The valid facility keywords are daemon (the default), local0, local1, local2, local3, local4, local5, local6, local7.

Note

- These parameters apply to all Cisco Prime IP Express servers (cnrservagt, ccm, cdns, cnrsnmp, dns, and dhcp).
- To apply any change to the cnr.conf parameters, Cisco Prime IP Express must be restarted.

The following cnr.conf configuration parameters allow server-specific overrides of the above parameters. server is one of cnrservagt, ccm, cdns, cnrsnmp, dns, and dhcp.

- cnr.syslog.server.enable—Specifies whether Syslog or Windows Event logging is enabled for the specified server (cnr.syslog.enable is ignored for that server).
- cnr.syslog.server.levels—Specifies the severity levels for the specified server (cnr.syslog.levels is ignored for that server).
- cnr.syslog.server.facility—Specifies the Syslog facility for the specified server (cnr.syslog.facility is ignored for that server).

The server specific configuration value is used, if specified. Otherwise, all parameters of the server are used. For example, to enable Syslog only for DHCP, add the following to the cnr.conf file:

```
cnr.syslog.dhcp.enable=1
```

To change the severity levels to include all non-debug logging (this assumes logging has been enabled for some or all servers), use:

```
cnr.syslog.enable=1
cnr.syslog.levels=error,warning,info,activity
```

To enable Syslog only for the DNS server:

```
cnr.syslog.dns.enable=1
cnr.syslog.dns.levels=error,warning,info,activity
```

Tip Syntax or other errors in the cnr.conf parameters are not reported and are ignored (that is, if a levels keyword is mistyped, that keyword is ignored). Therefore, if a configuration change does not work, check if the parameter(s) have been specified correctly.

Troubleshooting Server Failures

The server agent processes (nwreglocal and nwregregion) normally detect server failures and restart the server. You can usually recover from the failure and the server is not likely to fail again immediately after restarting. On rare occasions, the source of the server failure prevents the server from successfully restarting, and the server fails again as soon as it restarts. In such instances, perform the following steps:

Step 1 If the server takes a significantly long time to restart, stop and restart the server agent. On:

- Windows:

```
net stop nwreglocal or nwregregion
net start nwreglocal or nwregregion
```

- Linux:

```
/etc/rc.d/init.d/nwreglocal stop or nwregregion stop
/etc/rc.d/init.d/nwreglocal stop or nwregregion start
```

Step 2 Keep a copy of all the log files. Log files are located in the *install-path* /logs directory on Linux, and the *install-path* \logs folder on Windows. The log files often contain useful information that can help isolate the cause of a server failure.

Step 3 Use the TAC tool, as described in Using the TAC Tool, on page 145, or save the core or user.dmp file, if one exists, depending on the operating system:

- **Windows**—The user.dmp file is located in the system directory, which varies depending on the Windows system. Search for this file and save a renamed copy.
- **Linux**—The core file is located in the *install-path*. Save a renamed copy of this file that Cisco Prime IP Express does not overwrite.

Step 4 On Windows, use the native event logging application to save the System and Application event logs to files. You can do this from the Event Viewer. These event logs often contain data that helps debug Cisco Prime IP Express server problems. For a description of the log messages for each server module, see the *install-path* /docs/msgid/MessageIdIndex.html file.

Linux Troubleshooting Tools

You can also use the following commands on Linux systems to troubleshoot Cisco Prime IP Express. To:

- See all Cisco Prime IP Express processes:

```
ps -leaf | grep nwr
```

- Monitor system usage and performance:

```
top
vmstat
```

- View login or bootup errors:

```
grep /var/log/messages*
```

- View the configured interfaces and other network data:

```
ifconfig -a
```

Using the TAC Tool

There may be times when any amount of troubleshooting steps will not resolve your problem and you have to resort to contacting the Cisco Technical Assistance Center (TAC) for help. Cisco Prime IP Express provides a tool so that you can easily assemble the server or system error information, and package this data for TAC support engineers. This eliminates having to manually assemble this information with TAC assistance. The resulting package from this tool provides the engineers enough data so that they can more quickly and easily diagnose the problem and provide a solution.

The **cnr_tactool** utility is available in the bin directory of the Windows, and usrbin directory of the UNIX or Linux, installation directories. Execute the **cnr_tactool** utility:

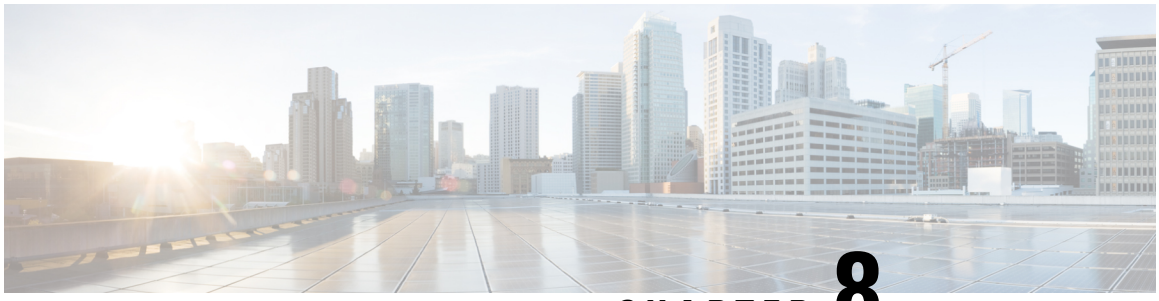
```
> cnr_tactool -N username -P password [-d output-directory] [-n]
```

The output directory is optional and normally is the temp directory of the installation directories (in the /var path on Linux). You may specify the **-n** option to indicate that when the cnr_exim tool is run, it is run without exporting any resource records (this specifies the -a none option to cnr_exim). If you do not supply the username and password on the command line, you are prompted for them:

```
> cnr_tactool

user:
password:
[processing messages....]
```

The tool generates a packaged tar file whose name includes the date and version. The tar file contains all the diagnostic files.



CHAPTER 8

Backup and Recovery

This chapter explains how to maintain the Cisco Prime IP Express databases.

Backing Up Databases

Because the Cisco Prime IP Express databases do a variety of memory caching and can be active at any time, you cannot rely on third-party system backups to protect the database. They can cause backup data inconsistency and an unusable replacement database.

For this purpose, Cisco Prime IP Express provides a shadow backup utility, cnr_shadow_backup. Once a day, at a configurable time, Cisco Prime IP Express takes a snapshot of the critical files. This snapshot is guaranteed to be a consistent view of the databases.

Related Topics

Syntax and Location, on page 148

Backup Strategy, on page 148

Database Recovery Strategy, on page 151

Backing Up CNRDB Data, on page 150

Backing Up All CNRDBs Using tar or Similar Tools, on page 150

Recovering CNRDB Data from Backups, on page 152

Recovering All CNRDBs Using tar or Similar Tools, on page 153

Recovering Single CNRDB from tar or Similar Tools, on page 153

Virus Scanning While Running Cisco Prime IP Express, on page 154

Syntax and Location

Be sure to understand that the notation ".../data/db" in the following sections refers to directories in the Cisco Prime IP Express product data location path, depending on the operating system:

- **Windows**—".../data" means the data directory, which by default is **C:\IPExpress\{Local | Regional}\data**.
- **Linux**—".../data" means the data directory, which by default is **/var/nwreg2/{local | regional}/data**.

Cisco Prime IP Express database utility programs mentioned in the following sections are located in the ".../bin" directory, which you run as its full path name:

- **Windows**—".../bin/*program* " means the program file in the bin directory, which by default is **C:\Program Files\IP Express\{Local | Regional}\bin***program* for a 32-bit OS and **C:\Program Files (x86)\IP Express\{Local | Regional}\bin***program* for a 64-bit OS.
- **Linux**—".../bin/*program*" means the program file in the bin directory, which by default is **/opt/nwreg2/local/usrbin/***program* or **/opt/nwreg2/regional/usrbin/***program*.

Note Use only the approved utilities for each type of database. In Windows, if you want to run the utility from outside the installed path, you must set the CNR_HOME environment variable.

Backup Strategy

The backup strategy involves either:

- Making CCM perform a nightly shadow backup for you (See the Setting Automatic Backup Time, on page 149) and using the shadow backups for permanent backup and then doing an explicit backup - either using the cnr_shadow_backup utility and backing up the backup files (*.bak DBs)

  or

Shutting down Cisco Prime IP Express and performing a backup using TAR or other similar tools.

Manual Backup (Using cnr_shadow_backup utility)

Use the cnr_shadow_backup utility to back up the following databases:

- **CNRDB databases**—...data/dhcp, ...data/dns/csetdb, ...data/dns/rrdb, ...data/cdns, ...data/leasehist, ...data/lease6hist, ...data/subnetutil, ...data/mcd, ...data/replica, and ...data/ccm/ndb

Note If you change the location of the data directory, you must edit the **cnr.conf** file, which is located in .../conf (see Modifying the cnr.conf File, on page 141). Change the **cnr.datadir** variable to the full path to the data directory. For example, the following is the default value on Windows:

```
cnr.datadir=C:\\IPExpress\\{Local|Regional}\\data
```

The most basic component of a backup strategy is the daily shadow backup. When problems occur with the operational database, you might need to try recovering based on the shadow backup of the previous day. Therefore, you must recognize and correct any problems that prevent a successful backup.

The most common problem is disk space exhaustion. To get a rough estimate of disk space requirements, take the size of the .../data directory and multiply by 10. System load, such as usage patterns, application mix, and the load on Cisco Prime IP Express itself, may dictate that a much larger reserve of space be available.

You should regularly archive existing shadow backups (such as to tape, other disks, or other systems) to preserve them for possible future recovery purposes.

Caution Using a utility on the wrong type of database other than the one recommended can cause database corruption. Use only the utilities indicated. Also, never use the database utilities on the operational database, only on a copy.

Related Topics

Setting Automatic Backup Time, on page 149

Performing Manual Backups, on page 149

Using Third-Party Backup Programs with cnr_shadow_backup, on page 149

Setting Automatic Backup Time

You can set the time at which an automatic backup should occur by editing the **cnr.conf** file (in .../conf). Change the **cnr.backup-time** variable to the hour and minute of the automatic shadow backup, in 24-hour *HH*:*MM* format, then restart the server agent. For example, the following is the preset value:

```
cnr.backup-time=23:45
```

Performing Manual Backups

You can also initiate a manual backup with the cnr_shadow_backup utility, which requires root privileges. Enter the cnr_shadow_backup command at the prompt to perform the backup.

Note To restore DHCP data from a failover partner that is more up to date than a backup, see Restoring DHCP Data from a Failover Server, on page 161.

Using Third-Party Backup Programs with cnr_shadow_backup

You should avoid scheduling third-party backup programs while cnr_shadow_backup is operating. Third-party backup programs should be run either an hour earlier or later than the cnr_shadow_backup operation. As described in Setting Automatic Backup Time, on page 149, the default shadow backup time is daily at 23:45.

Configure third-party backup programs to skip the Cisco Prime IP Express operational database directories and files, and to back up only their shadow copies.

The operational files are listed in Backup Strategy, on page 148. On Linux, Cisco Prime IP Express also maintains lock files in the following directories:

- Cisco Prime IP Express server processes—/var/nwreg2/local/temp/np_destiny_trampoline or /var/nwreg2/regional/temp/np_destiny_trampoline

The lock files are recreated during a reboot. These files are important while a system is running. Any maintenance process (such as virus scanning and archiving) should exclude the temporary directories, operational database directories, and files.

Windows does not maintain lock files, but uses named-pipes instead.

Backing Up CNRDB Data

In the case of the CNRDB databases, the cnr_shadow_backup utility copies the database and all log files to a secondary directory in the directory tree of the installed Cisco Prime IP Express product. For:

- **DHCP**—The operational database is in the .../data/dhcp/ndb and .../data/dhcp/clientdb directories, with the log files in the .../data/dhcp/ndb/logs directory. The shadow copies are in the .../data/dhcp.bak/ndb directory.
- **DNS**—The operational database is in the .../data/dns/rrdb directory. The important operational components are the High-Availability (HA) DNS is in the .../data/dns/hadb directory, with log files in the .../data/dns/hadb/logs directory.The shadow copies are in the .../data/dns.bak directory.
- **CDNS—**The operational database is in the .../data/cdns directory. The shadow copies are in the .../data/cdns.bak directory.
- **CCM**—The operational database and log files are in the .../data/ccm/ndb directory. The shadow copies are in the .../data/ccm.bak directory.
- **MCD change log**—The operational database and log files are in the .../data/mcd/ndb directory. The shadow copies are in the .../data/mcd.bak directory. MCD Change Log database may not exist if there are no change log entries. Also, the database is deleted when the MCD change log history is trimmed or when there is no MCD change log data to begin with.
- **Lease history**—The operational database and log files are in the .../data/leasehist and .../data/lease6hist directories. The shadow copies are in the .../data/leasehist.bak and .../data/lease6hist.bak directories.
- **Subnet utilization**—The operational database and log files are in the .../data/subnetutil directory. The shadow copies are in the .../data/subnetutil.bak directory.
- **Replica**—The operational database and log files are in the .../data/replica directory.

The actual file naming convention is:

- **Database**—dhcp.ndb and dns.ndb.
- **Log files**—log.0000000001 through log.9999999999. The number of files varies with the rate of change to the server. There are typically only a small number. The specific filename extensions at a site vary over time as the database is used. These log files are not humanly readable.

Backing Up All CNRDBs Using tar or Similar Tools

This section describes the procedure for backing up all Cisco Prime IP Express databases using tar or similar tools.

Step 1 Shut down Cisco Prime IP Express.

Backups cannot be done using tar or similar tools if Cisco Prime IP Express is running.

Step 2 Back up the entire data directory and subdirectories:

```
> /var/nwreg2/local/data or /var/nwreg2/regional/data
> /opt/nwreg2/*/conf
```

Step 3 Restart Cisco Prime IP Express when the backup is complete.

Note Technically the backups do not need to include the *.bak directories (and subdirectories of those directories) as those contain nightly shadow backups. However, unless your available storage space is severely limited, we recommend a full backup of the entire data directory (and subdirectories) including the shadow backups.

Database Recovery Strategy

Cisco Prime IP Express uses the CNRDB database. The following table lists the types of CNRDB database that must be backed up and recovered.

Table 21: Cisco Prime IP Express Databases for Recovery

Subdirectory	Cluster	Type	Description
ccm	local, regional	CNRDB	Central Configuration Management database. Stores local centrally managed cluster and the SNMP server data.
dns	local	CNRDB	DNS database. Stores zone state information, names of protected RRs, and zone configuration data for the DNS server.
cdns	local	CNRDB	Caching DNS database. Stores the initial DNSSEC root trust anchor and root hints.
dhcp	local	CNRDB	DHCP database. Stores lease state data for the DHCP server.
dhcpeventstore	local		Queue that Cisco Prime IP Express maintains to interact with external servers, such as for LDAP and DHCPv4 DNS Update interactions. Recovery is not necessary.

Subdirectory	Cluster	Type	Description
replica	regional	CNRDB	Stores replica data for the local clusters.
lease6hist	regional	CNRDB	DHCPv6 lease history database.
leasehist	regional	CNRDB	DHCPv4 lease history database.

The general approach to recovering a Cisco Prime IP Express installation is:

1. Stop the Cisco Prime IP Express server agent.
2. Restore or repair the data.
3. Restart the server agent.
4. Monitor the server for errors.

After you are certain that you executed a successful database recovery, always manually execute the cnr_shadow_backup utility to make a backup of the current configuration and state.

Recovering CNRDB Data from Backups

If there are any indications, such as server log messages or missing data, that database recovery was unsuccessful, you may need to base a recovery attempt on the current shadow backup (in the Cisco Prime IP Express installation tree). To do this:

Step 1 Stop the Cisco Prime IP Express server agent.

Step 2 Move the operational database files to a separate temporary location.

Step 3 Copy each .../data/*name* .bak directory to .../data/*name* ; for example, copy .../data/ccm.bak to .../data/ccm.

Note If you set the cnr.dbrecover variable to false in the cnr.conf file to disable recovery during the cnr_shadow_backup nightly backup, you must also do a recovery as part of these steps.

Step 4 Rename the files.

The CNRDB database maintains centrally managed configuration data that is synchronized with the server configuration databases.

Step 5 Create a new data directory and then untar or recover the backed up directory.

We recommend that you run the DB directory and recovery tools to ensure that the databases are good.

Note Ensure that the logs subdirectory is present in the same directory or the logs path is mentioned in the DB_CONFIG file.

Step 6 Restart the server agent.

Note If the recovery fails, perhaps because the current shadow backup is simply a copy of corrupted files, use the most recent previous shadow backup. This illustrates the need to regularly archive shadow backups. You cannot add operational log files to older shadow backup files. All data added to the database since the shadow backup was made will be lost.

After a successful database recovery, initiate an immediate backup and archive the files using the cnr_shadow_backup utility (see Performing Manual Backups, on page 149).

Recovering All CNRDBs Using tar or Similar Tools

This section describes the procedure for recovering all Cisco Prime IP Express databases using tar or similar tools.

Step 1 Shut down Cisco Prime IP Express. Run **/etc/init.d/nwreglocal stop** to ensure that Cisco Prime IP Express is down.

Step 2 Rename the active data directory (such as mv data old-data).

Note You must have sufficient disk space for twice the size of the data directory (and all the files in it and its subdirectories). If you do not have sufficient disk space, move the active data directory to another drive.

Step 3 Create a new data directory and then untar or recover the backed up directory.

We recommend that you run the CNRDB directory and recovery tools to ensure that the databases are good.

Step 4 Start Cisco Prime IP Express.

Note Technically the restores do not need to include the *.bak directories (and subdirectories of those directories) as those contain nightly shadow backups. However, unless your available storage space is severely limited, we recommend a full restore of the entire data directory (and subdirectories) including the shadow backups.

Recovering Single CNRDB from tar or Similar Tools

This section describes the procedure for recovering single database using tar or similar tools.

Step 1 Shut down Cisco Prime IP Express. Run **/etc/init.d/nwreglocal stop** to ensure that Cisco Prime IP Express is down.

Step 2 Rename the active data directory (such as mv data old-data).

Note You must have sufficient disk space for twice the size of the data directory (and all the files in it and its subdirectories). If you do not have sufficient disk space, move the active data directory to another drive.

Step 3 Create a new data directory and then untar or recover only the files in that directory (and its subdirectories) from the backup.

We recommend that you run the CNRDB integrity and recovery tools to ensure that the CNRDB are good.

Step 4 Repeat **Step 2** to **Step 3** for other DBs that have to be recovered.

Step 5 Start Cisco Prime IP Express.

Virus Scanning While Running Cisco Prime IP Express

If you have virus scanning enabled on your system, it is best to configure it to exclude certain Cisco Prime IP Express directories from being scanned. Including these directories might impede Cisco Prime IP Express operation. The ones you can exclude are the .../data, .../logs, and .../temp directories and their subdirectories.

Troubleshooting Databases

The following sections describe troubleshooting the Cisco Prime IP Express databases.

Related Topics

Using the cnr_exim Data Import and Export Tool, on page 154

Using the cnrdb_recover Utility, on page 156

Using the cnrdb_verify Utility, on page 157

Using the cnrdb_checkpoint Utility, on page 158

Using the cnrdb_util Utility , on page 158

Restoring DHCP Data from a Failover Server, on page 161

Using the cnr_exim Data Import and Export Tool

The cnr_exim data import and export tool now supports the following for a user:

- Exporting all the data
- Exporting and importing license related data
- Importing all of the data

The cnr_exim tool also serves to export unprotected resource record information. However, cnr_exim simply overwrites existing data and does not try to resolve conflicts.

Note You cannot use cnr_exim tool for import or export of data from one version of Cisco Prime IP Express to another. It can be used only for import or export of data from or to the same versions of Cisco Prime IP Express.

Before using the cnr_exim tool, exit from the CLI, then find the tool on:

- **Windows**—...\bin\cnr_exim.exe
- **Linux**—.../usrbin/cnr_exim

You must reload the server for the imported data to become active.

Note that text exports are for reading purposes only. You cannot reimport them.

The text export prompts for the username and password (the cluster defaults to the local cluster). The syntax is:

```
> cnr_exim -e exportfile [-N username -P password -C cluster]
```

To export (importable) raw data, use the **–x** option:

```
> cnr_exim –e exportfile -x
```

To export DNS server and zone components as binary data in raw format, use the **–x** and **–c** options:

```
> cnr_exim –e exportfile –x –c "dnsserver,zone"
```

The data import syntax is (the import file must be in raw format):

```
> cnr_exim –i importfile [–N username –P password –C cluster]
```

You can also overwrite existing data with the **–o** option:

```
> cnr_exim –i importfile –o
```

The following table describes all the qualifying options for the cnr_exim tool.

Table 22: cnr_exim Options

Option	Description
–a *value*	Allows exporting and importing of protected or unprotected RRs. Valid *values* are: **protectedRR**, **unprotectedRR**, and **none** **Export**: All RRs are exported by default, so you must explicitly specify the export of protected or unprotected RRs using the option "-a protectedRR", "-a unprotectedRR", or "-a none". If this option is not specified, all RRs are exported. **Import:** All RRs are imported by default, so you must explicitly specify the import of protected or unprotected RRs using the option "-a protectedRR" or " -a unprotectedRR". If this option is not specified, all RRs are imported.
–c "*components***"**	Imports or exports Cisco Prime IP Express components, as a quoted, comma-delimited string. Use **–c help** to view the supported components. User are not exported by default; you must explicitly export them using this option, and they are always grouped with their defined groups and roles. Secrets are never exported. **Note** After you import administrator names, you must set new passwords for them. If you export groups and roles separately from usernames (which are not exported by default), their relationship to usernames is lost.
–C *cluster*	Imports from or exports to the specified cluster. Preset to **localhost**.

Option	Description
–e *exportfile*	Exports the configuration to the specified file.
–h	Displays help text for the supported options.
–i *importfile*	Imports the configuration to the specified file. The import file must be in raw format.
–N *username*	Imports or exports using the specified username.
–o	When used with the **–i** (import) option, overwrites existing data.
–p *port*	Port used to connect to the SCP server.
–P *password*	Imports or exports using the specified password.
–t *exportfile*	Specifies a file name to export to, exports data in s-expression format.
–v	Displays version information
–x	When used with the **–e** (export) option, exports binary data in (importable) raw format.
–d	Specifies the directory path of cnr_exim log file.
–b	Specifies that the core (base) objects are to be included in the import/export.
–w	Specifies the view tag to export. This option allows the user to export zone and RRs data which has the same view tag as mentioned in "w" option. All other objects will not take this option into consideration and will be exported as earlier if it is used.

Using the cnrdb_recover Utility

The **cnrdb_recover** utility is useful in restoring the Cisco Prime IP Express databases to a consistent state after a system failure. You would typically use the **–c** and **–v** options with this command (The following table describes all of the qualifying options). The utility is located in the installation bin directory.

Table 23: cnrdb_recover Options

Option	Description
–c	Performs a catastrophic recovery instead of a normal recovery. It not only examines all the log files present, but also recreates the .ndb (or .db) file in the current or specified directory if the file is missing, or updates it if is present.

Option	Description
–e	Retains the environment after running recovery, rarely used unless there is a DB_CONFIG file in the home directory.
–h *dir*	Specifies a home directory for the database environment. By default, the current working directory is used.
–t	Recovers to the time specified rather than to the most current possible date. The time format is *[[CC]YY]MMDDhhmm[.ss]* (the brackets indicating optional entries, with the omitted year defaulting to the current year).
–v	Runs in verbose mode.
–V	Writes the library version number to the standard output, and exits.

In the case of a catastrophic failure, restore a snapshot of all database files, along with all log files written since the snapshot. If not catastrophic, all you need are the system files at the time of failure. If any log files are missing, **cnrdb_recover –c** identifies the missing ones and fails, in which case you need to restore them and perform the recovery again.

Use of the catastrophic recovery option is highly recommended. In this way, the recovery utility plays back all the available database log files in sequential order. If, for some reason, there are missing log files, the recovery utility will report errors. For example, the following gap in the log files listed:

```
log.0000000001
log.0000000053
```

results in the following error that might require you to open a TAC case:

```
db_recover: Finding last valid log LSN:file:1 offset 2411756
db_recover: log_get: log.0000000002: No such file or directory
db_recover: DBENV->open: No such for or directory
```

Using the cnrdb_verify Utility

The **cnrdb_verify** utility is useful for verifying the structure of the Cisco Prime IP Express databases. The command requires a file parameter. Use this utility only if you are certain that there are no programs running that are modifying the file. The following table describes all its qualifying options. The utility is located in the installation bin directory. The syntax is described in the usage information when you run the command:

```
C:\Program Files\IP Express\Local\bin>cnrdb_verify

usage: cnrdb_verify [-NoqV] [-h dir] [-P password] file
```

Table 24: cnrdb_verify Options

Option	Description
–h *dir*	Specifies a home directory for the database environment. By default, the current working directory is used.
–N	Prevents acquiring shared region locks while running, intended for debugging errors only, and should not be used under any other circumstances.
–o	Ignores database sort or hash ordering and allows **cnrdb_verify** to be used on nondefault comparison or hashing configurations.
–P *password*	User password, if the file is protected.
–q	Suppresses printing any error descriptions other than exit success or failure.
–V	Writes the library version number to the standard output, and exits.

Using the cnrdb_checkpoint Utility

The **cnrdb_checkpoint** utility is useful in setting a checkpoint for the database files so as to keep them current. The utility is located in the installation bin directory. The syntax is described in the usage information when you run the command:

```
C:\Program Files\IP Express\Local\bin>cnrdb_checkpoint ?

usage: cnrdb_checkpoint [-1Vv] [-h home] [-k kbytes] [-L file] [-P password][-p min]
```

Using the cnrdb_util Utility

The cnrdb_util utility is useful for dumping and loading CPIPE databases. In addition, you can use this utility to shadow backup and recover the CPIPE databases, to clear the log files, as well as to change the database page size.

The utility is located on the following directory:

- **Window** — *(installation directory)*\bin\cnrdb_util.bat
- **Linux** — *(installation directory)*/userbin/cnrdb_util

Important It is strongly recommended that a backup be done before performing any operation on the CPIPE databases. If existing backup files are to be retained, they must be backed up as well.

The cnrdb_util utility runs in two modes.

- **Interactive mode** - Prompts the user for operations and options.

- **Batch mode** - Requires information (both operation and options) as arguments while executing this utility.

The syntax is described in the usage information when you run the command:

```
./cnrdb_util -h
```

The following tables describe all of the qualifying operations and options.

Table 25: cnrdb_util Operations

Operation	Description
–d	Dump one or all CPIPE databases.
–l	Load one or all CPIPE databases.
–b	Create shadow backup of all CPIPE databases.
–r	Recover one or all CPIPE databases from shadow backup.
–c	Cleanup sleepycat log files in one or all CPIPE databases.
–h	Display help text for the supported options.

Important You can perform only one operation at a time.

Table 26: cnrdb_util Options

Option	Description
-m { local | regional }	Specifies the CPIPE installation mode. If not specified, this information is read from the cnr.conf file. If the file is not found, local mode is used by default.
-prog path	Specifies the path to the dump, load, or shadow backup executable. If not specified, this will be derived from the CPIPE installation path.
-db db-path	Specifies the source database path for the '-d' dump, '-l' load, or '-r' recover operation. If not specified, the datadir entry from the cnr.conf file, or the current directory is used. This option is not applicable for the '-b' backup operation.

Option	Description
-n { ccm | dhcp | dns | mcd | leasehist | lease6hist | replica | subnetutil | all }	Specifies the name of the source database for the '-d' dump, '-l' load, or '-r' recover operation. If not specified, the operation will be performed on all databases present in database path. This option is not applicable for the '-b' backup operation. • Valid database names for local mode are { ccm | dhcp | dns | mcd | all } • Valid database names for regional mode are { ccm | dns | leasehist | lease6hist | replica | subnetutil | all }
-s	Specifies that this program should attempt to stop the CPIPE Server Agent, if it is running.
-out path	Specifies the destination path for output files. If not specified, the source db path is used. This option is not applicable for the '-b' backup and '-c' cleanup operations.
-db_pagesize number	Specifies the size of database pages (in bytes) to be used when creating new databases. The minimum page size is 512 bytes and the maximum page size is 64K bytes, and must be a power of two. If no page size is specified, a page size is selected based on the underlying filesystem I/O block size. (A page size selected in this way has a lower limit of 512 bytes and an upper limit of 16K bytes.) Usually the default is appropriate. However, large page sizes may not have good performance. 4096 and 8192 are typically good sizes. You can determine the page size of the database by using the **cnrdb_stat** utility.

Important If the source and target directories are the same, the Dump and Load operations will delete the source files when the target files are created. This is done to minimize the disk space requirements when a dump/load operation is run to recapture the unused space in large database files.

Note The Dump operation will dump each database to a file in the specified location using the database file name appended by '.dbdump'. The Load operation will only load database files if a *.dbdump file is found; the name of the database file is the name without '.dbdump'.

Restoring DHCP Data from a Failover Server

You can restore DHCP data from a failover server that is more current than the result of a shadow backup. Be sure that the failover partner configurations are synchronized. Also, ensure that the following steps are run on the bad failover partner (i.e., the one whose database is bad) and that you want to restore to.

On Windows

1. Set the default path; for example:

   ```
   SET PATH=%PATH%;.;C:\PROGRA~1\NETWOR~1\LOCAL\BIN
   ```

2. Stop the server agent:

   ```
   net stop "IP Express Local Server Agent"
   ```

3. Delete the eventstore, ndb, and logs directories:

   ```
   del C:\IPExpress\Local\data\dhcpeventstore\*.*
   del C:\IPExpress\Local\data\dhcp\ndb\dhcp.ndb
   del C:\IPExpress\Local\data\dhcp\ndb\logs\*.*
   ```

4. Restart the server agent:

   ```
   net start "IP Express Local Server Agent"
   ```

On Linux

1. Stop the server agent:

   ```
   /etc/init.d/nwreglocal stop
   ```

2. Determine the processes running:

   ```
   /opt/nwreg2/local/usrbin/cnr_status
   ```

3. Kill the remaining processes:

   ```
   kill -9 pid
   ```

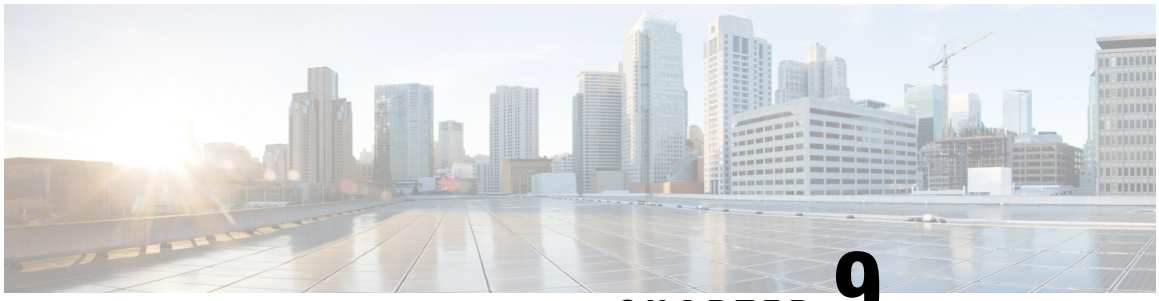
4. Delete the eventstore, ndb, and logs directories:

   ```
   rm /var/nwreg2/data/dhcpeventstore/*.*
   ```

   ```
   rm -r /var/nwreg2/data/dhcp/ndb/*
   ```

5. Restart the server agent:

   ```
   /etc/init.d/nwreglocal start
   ```



CHAPTER 9

Managing Reports

This chapter explains how to manage the Cisco Prime IP Express address space reporting tool, which is available from a regional cluster by using the web UI. Before you proceed with this chapter, become familiar with the concepts in the previous chapters of this part of the User's Guide.

ARIN Reports and Allocation Reports

Using the Cisco Prime IP Express web UI, you can generate:

- American Registry of Internet Numbers (ARIN) reports, including:
  - Organization and point of contact (POC) reports
  - IPv4 address space utilization reports
  - Shared WHOIS project (SWIP) allocation and assignment reports
- Allocation reports that show how addresses are deployed across the routers and router interfaces of your network, including:
  - Allocation by owner reports
  - Allocation by router interface or by network reports

Managing ARIN Reports

ARIN, which is one of the five Regional Internet Registries (RIRs), manages IP resources in Canada, the United States of America, and many Caribbean and North Atlantic islands.

ARIN allocates blocks of IP addresses to Internet Service Providers (ISPs), which, in turn, reassign blocks of address space to their customers. ARIN distinguishes between *allocating* IP address space and *assigning* IP address space. It allocates address space to smaller IRs for subsequent distribution to the IRs' members and

customers. It assigns address space to an ISP, or other organization, for use only within the network of that organization and only for the purposes documented in its requests and reports to ARIN.

Note ARIN manages IP address resources under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN). In other geographies, ICANN has delegated authority for IP resources to different regional Internet Registries. Cisco Prime IP Express does not currently support the reports that these registries might require, nor does it now support IPv6 reports or autonomous system (AS) numbers.

ARIN maintains detailed documentation about its policies and guidelines on its website.

`http://www.arin.net`

Be sure that you are familiar with these policies and guidelines before proceeding with ARIN reports.

The three options that you can specify for ARIN reports are:

- **New**—For a newly added POC or organization.
- **Modify**—Includes changed POC or organization data, such as phone numbers and addresses.
- **Remove**—Signals that you want to remove the POC or organization from the ARIN database.

Related Topics

Managing Point of Contact and Organization Reports, on page 164

Managing IPv4 Address Space Utilization Reports, on page 167

Managing Shared WHOIS Project Allocation and Assignment Reports, on page 168

Managing Point of Contact and Organization Reports

Cisco Prime IP Express provides reports that can submit Points of Contact (POC) and organizational information to ARIN. After you fill in these reports, you need to e-mail the information to ARIN. Submit the POC report (also called a template) to ARIN before preparing other reports.

Each POC is uniquely identified by a name called a POC handle and is associated with one or more Organization Identifiers (Org IDs) or resource delegations, such as an IP address space allocation or assignment. A POC handle, which ARIN assigns, can represent either an individual or a role.

The Organization report creates an Org ID and associates POC records with it. Create the Organization report after you create the POC report.

To manage POC and organization reports, log into the Cisco Prime IP Express regional web UI as a member of an administrator group assigned to the regional-addr-admin role.

Related Topics

Creating a Point of Contact Report, on page 165

Registering a Point of Contact, on page 165

Editing a Point of Contact Report, on page 165

Creating an Organization Report, on page 166

Registering an Organization, on page 166

Editing an Organization Report, on page 167

Creating a Point of Contact Report

You create POCs so that managers can interact with ARIN to request and administer IP resources and so that network professionals can manage network operation issues.

Regional Web UI

Step 1 From the **Administration** menu, choose **Contacts** under the **Settings** submenu to open the List/Add ARIN Points of Contact page.

Step 2 Click the **Add Contact** icon in the Contacts pane on the left, to open the Add Point of Contact page.

Step 3 Enter data in the fields on the page:

- **Name**—A unique identifier for the POC (required).
- **First Name**—The first name of the point of contact (required).
- **Last Name**—The last name of the point of contact (required).
- **Type**—From the drop-down list, choose Person or Role (optional, with preset value Person).

Step 4 Click **Add Point of Contact**.

Registering a Point of Contact

You must register the POC with ARIN to receive a POC handle.

Regional Web UI

Step 1 From the **Administration** menu, choose **Contacts** under the **Settings** submenu to open the List/Add ARIN Points of Contact page.

Step 2 Click the required contact in the Contacts pane on the left.

Step 3 Click the **Register Report** tab to view the ARIN template file.

Step 4 Copy and paste the template file into an e-mail and send the file to ARIN.

Editing a Point of Contact Report

Edit a POC report after ARIN returns a POC handle to your organization or if your POC has changed.

Regional Web UI

Step 1 From the **Administration** menu, choose **Contacts** under the **Settings** submenu to open the List/Add ARIN Points of Contact page.

Step 2 Click the required contact in the Contacts pane on the left**.** The Edit Point of Contact page opens.

Step 3 Enter values for Middle Name, Handle, and Description (optional)

Step 4 In the Poc Emails field:

a) Enter the e-mail address for the POC.

b) Click **Add Email Address** to add additional e-mail addresses.

Step 5 In the Poc Phones field:

a) Enter a phone number and extension, if applicable, then choose a type (Office, Mobile, Fax, or Pager) from the drop-down list,

b) Click **Add Phone** to add additional telephones.

Step 6 Miscellaneous Settings. Add these additional attributes as strings or lists of text.

Step 7 After making the changes, click **Save**.

Creating an Organization Report

Each organization is represented in the ARIN WHOIS database by a unique Org ID, consisting of an organization name, its postal address, and its POCs. While organizations may have more than one Org ID, ARIN recommends consolidating IP address resources under a single Org ID.

If you do not have an Org ID with ARIN, or you are establishing an additional Org ID, you must first create and submit a POC report. When ARIN confirms it has received your POC information, use Cisco Prime IP Express to complete an Organization form and submit that information.

Regional Web UI

Step 1 From the **Administration** menu, choose **Organizations** under the **Settings** submenu to open the List/Add ARIN Organizations page.

Step 2 Click the **Add Organization** icon in the Organizations pane on the left, to open the Add Organization page.

Step 3 Enter data in the fields on the page:

- **Organization Name**—Name of the organization that you want to register with ARIN.
- **Description**—A text description of the organization.
- **Organization Admin POC**—From the drop-down list, choose the POC who administers IP resources from the drop-down list.
- **Organization Technical Points Of Contact**—From the drop-down list, choose one or more POCs who manage network operations, or click **Add Point of Contact** to add new contact information.

Step 4 Click **Add Organization**. This opens the Edit Organization page where you can add more details.

Registering an Organization

You must register your Organization with ARIN to receive an Organization ID.

Regional Web UI

Step 1 From the **Administration** menu, choose **Organizations** under the **Settings** submenu to open the List/Add ARIN Organizations page.

Step 2 Click the required organization in the Organizations pane on the left.

Step 3 Click the **Register Report** tab to view the ARIN template file.

Step 4 Copy and paste the template file into an e-mail and send the file to ARIN.

Editing an Organization Report

You might need to change organizational information that you have registered with ARIN.

Regional Web UI

Step 1 From the **Administration** menu, choose **Organizations** under the **Settings** submenu to open the List/Add ARIN Organizations page.

Step 2 Click the required organization in the Organizations pane on the left.

Step 3 Enter or change data in the fields.

- **Miscellaneous Settings**—Add these additional attributes as strings or lists of text.
- **Organization Abuse Points of Contact**—From the drop-down list, choose one or more POCs who handle network abuse complaints, or click **Add Point of Contact** to add new contact information.
- **Organization NOC Points of Contact**—From the drop-down list, choose one or more POCs in network operations centers, or click **Add Point of Contact** to add new contact information.

Step 4 Click **Save**.

Step 5 Submit the updated report to ARIN as described in Registering an Organization, on page 166.

Managing IPv4 Address Space Utilization Reports

Address space utilization reports serve two purposes:

- To make an initial request for IPv4 address space after you receive a POC handle and an Org ID.
- To support a request for an additional allocation of IPv4 addresses when your business projections show that you are running out of IP addresses.

Note The ARIN website contains extensive information about how it initially allocates address space and its threshold criteria for requesting additional address space. In general, for a single-homed organization, the minimum allocation from ARIN is a /20 block of addresses. For a multihomed organization, the minimum allocation is a /22 block of addresses. ARIN recommends that an organization requiring a smaller block of addresses contact an upstream ISP to obtain addresses.

The Cisco Prime IP Express utilization report corresponds to the ARIN ISP Network Request template (ARIN-NET-ISP-3.2.2).

Regional Web UI

Step 1 From the **Operate** menu, choose **ARIN Address Space Usage** under the **Reports** submenu to open the Select Address Space Report page.

Step 2 In the Select the Report Type field, choose **Utilization** from the drop-down list. The Select the Filter Type field is updated with the value, *by-owner*. The browser redisplays the Select Address Space Report page with two new fields: Network Name and Network Prefix Length.

Step 3 In the Select Owner field, choose the owner of this address block from the drop-down list.

Step 4 Enter values for the Network Name and Network Prefix Length.

Step 5 Click **Generate Report**. The browser displays an ARIN template file (ARIN-NET-ISP-3.2.2).

Several sections of the report require that you manually enter data because the information is generated and maintained outside the Cisco Prime IP Express application.

Step 6 Click **Save Report**. The browser displays the Address Space Utilization Report as an unformatted text file.

Step 7 Copy the Address Space Utilization Report to a text editor to manually enter the data that Cisco Prime IP Express does not generate.

Step 8 Copy and paste the edited report into an e-mail and send the file to ARIN.

Managing Shared WHOIS Project Allocation and Assignment Reports

The ARIN shared WHOIS project (SWIP) provides a mechanism for finding contact and registration information for resources registered with ARIN. The ARIN database contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources, and related POCs.

The ARIN WHOIS does not locate any domain- or military-related information. Use whois.internic.net to locate domain information, and whois.nic.mil for military network information.

The regional web UI also provides two allocation and assignment report pages:

- View ARIN SWIP Reallocated Report
- View ARIN SWIP Reassigned Report

Managing BYOD Reports

There are two types of BYOD reports:

- Registered Devices
- Scopes/Prefix

Registered Devices

Registered Device report displays the list of devices that are registered through BYOD web server. The report can be exported in the csv format. Only an admin user is allowed to delete a device using the Registered Device Report page.

Registered Devices Report

To access the Registered Devices Report:

Regional Advanced or Expert Web UI

From the **Operate** menu, choose **BYOD Registered Devices** under the **Reports** submenu to access the report in the List BYOD Registered Devices page.

LDAP server(s) configured to the BYOD web server or local DHCP server(s) or failover pairs, associated with the regional server will be listed in the clusters pane. All the registered devices in the LDAP server or devices registered in the local DHCP servers or failover pairs through the BYOD web server will be displayed in the List BYOD Registered Devices page.

Note You must select the desired server from the cluster pane to view the corresponding registered devices report in the List BYOD Registered Devices page.

Scopes/Prefix

Scope/Prefix report displays the list of scopes and prefixes that are used for BYOD. The report can be exported in the csv format.

Scope/Prefix Report

To view the Scope/Prefix Report:

Regional Advanced or Expert Web UI

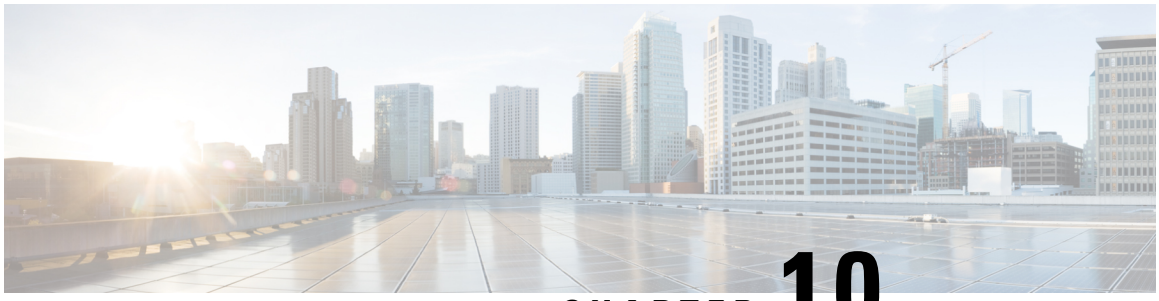
From the **Operate** menu, choose **BYOD Scopes/Prefix** under the **Reports** submenu to view the report in the List BYOD Scope/Prefix page.

Local DHCP server(s) or failover pairs associated with the regional server will be listed in the clusters pane. All the scopes and prefixes created in the local DHCP servers or failover pairs for the BYOD web server will be displayed in the List BYOD Scope/Prefix page.

Note You must select the desired server from the cluster pane to view the corresponding scopes and prefixes created during BYOD setup in the List BYOD Scope/Prefix page.

PART III

Virtual Appliance



CHAPTER 10

Introduction to Cisco Prime IP Express Virtual Appliance

The Cisco Prime IP Express virtual appliance aims at reducing the installation, configuration, and maintenance costs associated with running Cisco Prime IP Express on a local system. It also guarantees portability and thus reduces the risk in moving Cisco Prime IP Express from one machine to another.

You must get a license for Cisco Prime IP Express and download the virtual appliance from Cisco.com. Every Cisco Prime IP Express local cluster must be connected to a regional cluster which contains the licenses for the DHCP or DNS services provided by the local cluster. All licenses are loaded into the regional cluster, and local clusters are registered with the regional cluster at the time of their first installation. Cisco Prime IP Express will then be up and running, available to be configured.

This is different from just downloading a copy of Cisco Prime IP Express and installing it on a server or virtual machine provided by the customer, in that the operating system on which Cisco Prime IP Express runs is also provided in the virtual appliance.

The Cisco Prime IP Express virtual appliance is supported on VMware ESXi 5.5 or later platforms, CentOS/RHEL 7.2 Hypervisor, and an OpenStack installation running on CentOS/RHEL 7.2.

To know about the difference between vApp and a virtual appliance, see the *User's Guide to Deploying vApps and Virtual Appliances*.

How the Cisco Prime IP Express Virtual Appliance Works

The virtual appliance consists of a virtual machine, which contains a runnable guest OS (CentOS 7.2) and Cisco Prime IP Express installed on that OS. When the virtual appliance is installed, Cisco Prime IP Express is already installed and is started by the virtual machine power-up.

Invoking Cisco Prime IP Express on the Virtual Appliance

You can invoke the Cisco Prime IP Express application directly by using the URL **http://***hostname***:8080**. The secure **https** connection is also available via the URL **https://***hostname***:8443**.

Monitoring Disk Space Availability on VMware

To determine how much space is available to use for increasing the size of a virtual appliance's disk, do the following:

Step 1 In the vSphere Client window, select the host/server on which the virtual Cisco Prime IP Express appliance resides.

Step 2 Click **Storage Views** to see the list of the machines hosted by the server and the details about the space currently used by each machine.

Also, you can go to the Virtual Machines tab to view both the **Provisioned Space** and the **Used Space** by machine.

Step 3 Click **Summary**.

The **Resources** area of the Summary tab, displays the capacity of the disk and the CPU and memory used.

Step 4 Select the virtual machine and click the **Summary** tab.

The **Resources** area of the Summary tab displays the disk space details for the machine.

Monitoring Disk Space Availability in Use by the Virtual Appliance

To determine how much free space is left on the disk in use by the virtual appliance, as an aid to determine if you should increase the size of the virtual appliance's disk, do the following:

Step 1 Select the virtual machine in the vSphere Client window and either click the **Console** tab on the right pane or right-click the virtual machine name and choose **Open Console**.

Step 2 Log in as root and type df -k. The disk space details are displayed.

If the disk space on the disk mounted is not enough, then you should increase the size of the disk (see Increasing the Size of the Disk on VMware, on page 174).

Increasing the Size of the Disk on VMware

If you need a bigger disk, do the following:

Step 1 Stop the VM.

Step 2 Increase the size of the disk by changing the size in the Virtual Machine Properties window. To open the Virtual Machine Properties window, you have to select the VM using the VM name, right-click, and choose Edit Settings.

Step 3 Restart the VM.

During the boot process, the partition containing the filesystem will be extended to encompass the entire disk and the filesystem will be extended to fill the entire partition.

Increasing the Size of the Disk on a KVM Hypervisor

The initial disk size is 14 GB, with 6 GB allocated to a swap partition, leaving about 5.4 GB available in /dev/sda3, the partition in which Cisco Prime IP Express runs. This is certainly too small for all installations. Therefore, you may need to increase the size of the disk. There are two steps to this process.

- Make the disk backing file larger
- Repartition the disk and tell the filesystem to use all the available space in the partition

Increasing the size of the disk must be done when the VM is not running. You may do this before you install the VM, when the VM is certainly not running, or you may do this after you have brought up the VM and it has already run. If the VM is running, you must shut down the VM before you increase the size of the disk. Once the VM is not running, use the **truncate** and **virt-resize** commands to create a larger disk and copy the data onto the larger disk, as well as to change the partition table and resize the filesystem to use the additional space.

Following is an example of how you might use these commands to increase the size of the disk from the default size of 14 GB to 16 GB. In practice, you almost certainly would use a larger size than 16 GB. The new size of the disk is specified on the **truncate** command.

Example

```
root:tsegi$ truncate -s 16G @BUILDNAME-disk1.big.raw

root:tsegi$ virt-resize --expand /dev/sda3 @BUILDNAME-disk1.raw @BUILDNAME-disk1.big.raw

Examining @BUILDNAME-disk1.raw ...
 100%
[[▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒]] --:--

**********

Summary of changes:

/dev/sda1: This partition will be left alone.

/dev/sda2: This partition will be left alone.

/dev/sda3: This partition will be resized from 7.5G to 9.5G.

**********

Setting up initial partition table on @BUILDNAME-disk1.big.raw ...
```

```
Copying /dev/sda1 ...
 100%
[[▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒]] 00:00

Copying /dev/sda2 ...
 100%
[[▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒]] 00:00

Copying /dev/sda3 ...
 100%
[[▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒]] 00:00

Resize operation completed with no errors.  Before deleting the old disk, carefully check
that the resized disk boots and works correctly.
```

The operation in the above example took about 5 or 6 minutes on a moderately powerful machine. The time it will take on your machine will vary depending on a variety of factors.

The **truncate** command creates a new disk file of a specified size and the **virt-resize** command recreates the partitions of the input disk out the output disk, copies the data from the original disk file onto the new disk file, and enlarges the filesystem in the specified partition to encompass everything in the partition. After completing this operation, replace the disk of the VM with the new disk using the virtual machine manager.

Note Though once you have used the new disk, the data on the original disk is old and should not be used, it is still a working disk and could be saved as a backup. If you returned to using the original disk, all memory of the processing performed while the new, larger disk was operating will be lost, and serious conflicts between IP addresses granted to DHCP while the new disk was in use and the DHCP server's future activity when using the old disk will occur.

If you increase the size of the disk before the installation of the VM, you must rename the new disk file to be the same as the original disk file: @BUILDNAME-disk1.raw, as that is what the installonkvm script expects the name of the disk file to be.

Troubleshooting

If you experience any issues while working with the Cisco Prime IP Express virtual appliance, we recommend you to do the following:

Examine the log files in /var/nwreg2/{local | regional}/logs. Look particularly for errors in the log files as these signal exceptional conditions. If you are unable to resolve the problem and you have purchased Cisco support, then submit a case to Cisco Technical Assistance Center (TAC) regarding the problem.

Glossary

A	
A record	DNS Address resource record (RR). Maps a hostname to its address and specifies the Internet Protocol address (in dotted decimal form) of the host. There should be one A record for each host address.
access control list (ACL)	DHCP mechanism whereby the server can allow or disallow the request or action defined in a packet. *See also* transaction signature (TSIG).
address block	Block of IP addresses to use with DHCP subnet allocation that uses on-demand address pools.
admin	Default name of the superuser or global administrator.
administrator	User account to adopt certain functionality, be it defined by role, constrained role, or group.
alias	Pointer from one domain name to the official (canonical) domain name.
allocation priority	An alternate method of control over allocating addresses among scopes other than the default round-robin method.
ARIN	American Registry of Internet Numbers, one of several regional Internet Registries (IRs), manages IP resources in North America, parts of the Caribbean, and subequatorial Africa. Cisco Prime IP Express provides an address space report for this registry.
Asynchronous Transfer Mode (ATM)	International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells.
authoritative name server	DNS name server that possesses complete information about a zone.
AXFR	Full DNS zone transfer. *See also* zone transfer and IXFR.

B	
Berkeley Internet Name Domain (BIND)	Implementation of the Domain Name System (DNS) protocols. *See also* DNS.
binding	Collection of DHCP client options and lease information, managed by the main and backup DHCP servers. A binding database is a collection of configuration parameters associated with all DHCP clients. This database holds configuration information about all the datasets.
BOOTP	Bootstrap Protocol. Used by a network node to determine the IP address of its Ethernet interfaces, so that it can affect network booting.

C	

cable modem termination system (CMTS)	Cable modem termination system. Either a router or bridge, typically at the cable head end.
cache	Data stored in indexed disk files to reduce the amount of physical memory.
caching name server	Type of DNS server that caches information learned from other name servers so that it can answer requests quickly, without having to query other servers for each transaction.
canonical name	Another name for an alias DNS host, inherent in a CNAME resource record (RR).
case sensitivity	Values in Cisco Prime IP Express are not case-sensitive, with the exception of passwords.
Central Configuration Management (CCM) database	Main database for the Cisco Prime IP Express web-based user interface (web UI).
chaddr	DHCP client hardware (MAC) address. Sent in an RFC 2131 packet between the client and server.
change logs, changesets	A change log is a group of changesets made to the Cisco Prime IP Express databases due to additions, modifications or deletions in the web UI. A changeset is a set of changes made to a single object in the database.
ciaddr	DHCP client IP address. Sent in an RFC 2131 packet between the client and server.
class of address	Category of an IP address that determines the location of the boundary between network prefix and host suffix. Internet addresses can be A, B, C, D, or E level addresses. Class D addresses are used for multicasting and are not used on hosts. Class E addresses are for experimental use only.
client-class	Cisco Prime IP Express feature that provides differentiated services to users that are connected to a common network. You can thereby group your user community based on administrative criteria, and then ensure that each user receives the appropriate class of service.
cluster	In Cisco Prime IP Express, a group of DNS and DHCP servers that share the same database.
CNAME record	DNS Canonical Name resource record (RR). Used for nicknames or aliases. The name associated with the resource record is the nickname. The data portion is the official or canonical name.
CNRDB	Name of one of the Cisco Prime IP Express internal databases. The other is changeset database.
constraint	Assigned limitation on the role or allowable functionality of an administrator.

D	

Data Over Cable Service Interface Specification (DOCSIS)	Data Over Cable Service Interface Specification. Standard created by cable companies in 1995 to work toward an open cable system standard and that resulted in specifications for connection points, called interfaces.
delegation	Act of assigning responsibility for managing a DNS subzone to another server, or of assigning DHCP address blocks to local clusters.
DHCP	Dynamic Host Configuration Protocol. Designed by the Internet Engineering Task Force (IETF) to reduce the amount of configuration that is required when using TCP/IP. DHCP allocates IP addresses to hosts. It also provides all the parameters that hosts require to operate and exchange information on the Internet network to which they are attached.
Digital Subscriber Line (DSL)	Public network technology that delivers high bandwidth over conventional copper wiring at limited distances.
DNS	Domain Name System. Handles the growing number of Internet users. DNS translates names, such as www.cisco.com, into Internet Protocol (IP) addresses, such as 192.168.40.0, so that computers can communicate with each other.
DNS update	Protocol (RFC 2136) that integrates DNS with DHCP.
domain	Portion of the DNS naming hierarchy tree that refers to general groupings of networks based on organization type or geography. The hierarchy is root, top- or first-level, and second-level domain.
domain name	DNS name that can be either absolute or relative. An absolute name is the fully qualified domain name (FQDN) and is terminated with a period. A relative name is relative to the current domain and does not end with a period.
dotted decimal notation	Syntactic representation of a 32-bit integer that consists of four eight-bit numbers written in base 10 with dots separating them for a representation of IP addresses. Many TCP/IP application programs accept dotted decimal notation in place of destination machine names.

E	
expression	Construct commonly used in the Cisco Prime IP Express DHCP implementation to create client identities or look up clients. For example, an expression can be used to construct a scope from a template.
extension and extension point	In Cisco Prime IP Express, element of a script written in TCP, C, or C++ that customizes handling DHCP packets as the server processes them, and which supports additional levels of customizing DHCP clients.

F	

failover	Cisco Prime IP Express feature (as described in RFC 2131) that provides for multiple, redundant DHCP servers, whereby one server can take over in case of a failure. DHCP clients can continue to keep and renew their leases without needing to know or care which server is responding to their requests.
forwarder	DNS server designated to handle all offsite queries. Using forwarders relieves other DNS servers from having to send packets offsite.
forwarding, DHCP	Mechanism of forwarding DHCP packets to another DHCP server on a per-client basis. You can achieve this in Cisco Prime IP Express by using extension scripting.
FQDN	Fully qualified domain name. Absolute domain name that unambiguously specifies a host location in the DNS hierarchy.

G	
giaddr	DHCP gateway (relay agent) IP address. Sent in an RFC 2131 packet between the client and server.
glue record	DNS Address resource record that specifies the address of a subdomain authoritative name server. You only need glue records in the server delegating a domain, not in the domain itself.
group	Associative entity that combines administrators so that they can be assigned roles and constrained roles.

H	
High-Availability (HA) DNS	DNS configuration in which a second primary server can be made available as a hot standby that shadows the main primary server.
HINFO record	DNS Host Information resource record (RR). Provides information about the hardware and software of the host machine.
hint server	*See* root hint server.
host	Any network device with a TCP/IP network address.

I	
IEEE	Institute of Electrical and Electronics Engineers. Professional organization whose activities include developing communications and network standards.
in-addr.arpa	DNS address mapping domain with which you can index host addresses and names. The Internet can thereby convert IP addresses back to hostnames. See also reverse zone.
IP address	Internet Protocol address. For example, 192.168.40.123.

IP history	Cisco Prime IP Express tool that records the lease history of IP addresses in a database.
IPv6	New IP standard involving 128-bit addresses. Cisco Prime IP Express provides a DHCPv6 implementation.
ISP	Internet Service Provider. Company that provides leased line, dialup, and DSL (Point-to-Point over Ethernet and DHCP) access to customers.
iterative query	Type of DNS query whereby the name server returns the closest answer to the querying server.
IXFR	Incremental zone transfer. Standard that allows Cisco Prime IP Express to update a slave (secondary) server by transferring only the changed data from the primary server.

L	
lame delegation	Condition when DNS servers listed in a zone are not configured to be authoritative for the zone.
LDAP	Lightweight Directory Access Protocol. Method that provides directory services to integrate Cisco Prime IP Express client and lease information.
lease	IP address assignment to a DHCP client that also specifies how long the client can use the address. When the lease expires, the client must negotiate a new one with the DHCP server.
lease grace period	Length of time the lease is retained in the DHCP server database after it expires. This protects a client lease in case the client and server are in different time zones, their clocks are not synchronized, or the client is not on the network when the lease expires.
link group	Groups the links to accommodate CMTS Prefix Stability. The *group-name* attribute is used to specify the name of the group to which the link should belong.
lease history	A report that can be generated to provide a historical view of when a client was issued a lease, for how long, when the client or server released the lease before it expired, and if and when the server renewed the lease and for how long.
lease query	Process by which a relay agent can request lease (and reservation) data directly from a DHCP server in addition to gleaning it from client/server transactions.

link type	There are three different link types: topological, location-independent, and universal. Topological links means a client is allocated leases based on the network segment it is connected to. While the location-independent link type lets a subscriber, that is moved from one CMTS to another within a central office, to retain a delegated prefix, the universal link type lets the subscriber moving from one central office to another to retain the delegated prefix.
local cluster	Location of the local Cisco Prime IP Express servers. *See also* regional cluster.
localhost	Distinguished name referring to the name of the current machine. Localhost is useful for applications requiring a hostname.
loopback zone	DNS zone that enables the server to direct traffic to itself. The host number is almost always 127.0.0.1.

M	
MAC address	Standardized data link layer address. Required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports on the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as a hardware address, MAC layer address, and physical address. A typical MAC address is 1,6,00:d0:ba:d3:bd:3b.
mail exchanger	Host that accepts electronic mail, some of which act as mail forwarders. *See also* MX record.
master name server	Authoritative DNS name server that transfers zone data to secondary servers through zone transfers.
maximum client lead time (MCLT)	In DHCP failover, a type of lease insurance that controls how much ahead of the backup server lease expiration the client lease expiration should be.
multinetting	State of having multiple DHCP scopes on one subnet or several LAN segments.
Multiple Service Operator (MSO)	Provides subscribers Internet access using cable or wireless technologies.
multithreading	Process of performing multiple server tasks.
MX record	DNS Mail Exchanger resource record (RR). Specifies where mail for a domain name should be delivered. You can have multiple MX records for a single domain name, ranked in preference order.

N	
nameserver	DNS host that stores data and RRs for a domain.

NAPTR	DNS Naming Authority Pointer resource record (RR). Helps with name resolution in a particular namespace and is processed to get to a resolution service. Based on proposed standard RFC 2915.
negative cache time	Memory cache the DNS server maintains for a quick response to repeated requests for negative information, such as "no such name" or "no such data." Cisco Prime IP Express discards this information at intervals.
network ID	Portion of the 32-bit IP address that identifies which network a particular system is on, determined by performing an AND operation of the subnet mask and the IP address.
NOTIFY	Standard (RFC 1996) whereby DNS master servers can inform their slaves that changes were made to their zones, and which initiates a zone transfer.
nrcmd	Cisco Prime IP Express command line interface (CLI).

O	
on-demand address pool	Wholesale IP address pool issued to a client (usually a VPN router or other provisioning device), from which it can draw for lease assignments. Also known as DHCP subnet allocation.
option, DHCP	DHCP configuration parameter and other control information stored in the options field of a DHCP message. DHCP clients determine what options get requested and sent in a DHCP packet. Cisco Prime IP Express allows for creating option definitions as well as the option sets to which they belong.
Organization report	One of the reports to be submitted to ARIN, POC being the other report. *See also* ARIN and POC report.
Organizationally Unique Identifier (OUI)	Assigned by the IEEE to identify the owner or ISP of a VPN. *See also* IEEE and virtual private network (VPN).
owner	Owners can be created as distinguishing factors for address blocks, subnets, and zones. In the context or DNS RRs, an owner is the name of the RR.

P	
ping	Packet Internetwork Groper. A common method for troubleshooting device accessibility that uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine if a remote host is active or inactive, and the round-trip delay in communicating with the host.
POC report	Point of Contact report. One of the reports to be submitted to ARIN, Organization being the other report. *See also* ARIN and Organization report.

policy	Group of DHCP attributes or options applied to a single scope or group of scopes. Embedded policies can be created for scopes and other DHCP objects.
polling	Collection of subnet utilization or lease history data over a certain regular period.
prefix allocation groups	Groups prefixes in order to facilitate the prioritization of prefix allocation.
prefix stability	Clients can retain the delegated prefix when they change their location, that is even when they move from one CMTS to another (CMTS Prefix Stability) or move within an address space (Universal Prefix Stability).
primary master	DNS server from which a secondary server receive data through a zone transfer request.
provisional address	Address allocated by the DHCP server to unknown clients for a short time, one-shot basis.
PTR record	DNS Pointer resource record. Used to enable special names to point to some other location in the domain tree. Should refer to official (canonical) names and not aliases. *See also* in-addr.arpa.
pulling and pushing objects	The Cisco Prime IP Express regional cluster provides functions to pull network objects from the replica database of local cluster data, and push objects directly to the local clusters.

R	
recursive query	DNS query where the name server asks other DNS server for any nonauthoritative data not in its own cache. Recursive queries continue to query all name servers until receiving an answer or an error.
refresh interval	Time interval in which a secondary DNS server checks the accuracy of its data by sending an AXFR packet to the primary server.
region	Regions can be created as distinguishing factors for address blocks, subnets, and zones. A region is distinct from the regional cluster.
regional cluster	Location of the regional Cisco Prime IP Express CCM server. *See also* local cluster.
relay agent	Device that connects two or more networks or network systems. In DHCP, a router on a virtual private network that is the IP helper for the DHCP server.
replica database	CCM database that captures copies of local cluster configurations at the regional cluster. These configurations can be pulled to the regional cluster so that they can be pushed to other local clusters.

Request for Comments (RFC)	TCP/IP set of standards.
reservation	IP address or lease that is reserved for a specific DHCP client.
resolution exception	Selectively forwarding DNS queries for specified domains to internal servers rather than recursively querying Internet root name and external servers.
resolver	Client part of the DNS client/server mechanism. A resolver creates queries sent across a network to a name server, interprets responses, and returns information to the requesting programs.
resource record (RR)	DNS configuration record, such as SOA, NS, A, CNAME, HINFO, WKS, MX, and PTR that comprises the data within a DNS zone. Mostly abbreviated as RR. *See the "Resource Records" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*
reverse zone	DNS zone that uses names as addresses to support address queries. *See also* in-addr.arpa.
role, constrained role	Administrators can be assigned one or more roles to determine what functionality they have in the application. A constrained role is a role constrained by further limitations. There are general roles for DNS, host, address block, DHCP, and CCM database administration. You can further constrain roles for specific hosts and zones. Some roles have distinguishing subroles, such as the database subrole.
root hint server	DNS name server at the top of the hierarchy for all root name queries. A root name server knows the addresses of the authoritative name servers for all the top-level domains. Resolution of nonauthoritative or uncached data must start at the root servers. Sometimes called a hint server.
round-robin	Action when a DNS server rearranges the order of its multiple same-type records each time it is queried.
routed bridge encapsulation (RBE)	Process by which a stub-bridged segment is terminated on a point-to-point routed interface. Specifically, the router is routing on an IEEE 802.3 or Ethernet header carried over a point-to-point protocol, such as PPP, RFC 1483 ATM, or RFC 1490 Frame Relay.

S	
scavenging	Action of periodically scanning dynamic updates to the DNS server for stale resource records and purging these records.
scope	Administrative grouping of TCP/IP addresses on a DHCP server. Required for lease assignments.

secondary master	DNS name server that gets it zone data from another name server authoritative for the zone. When a secondary master server starts up, it contacts the primary master, from which it receives updates.
secondary subnet	A single LAN might have more than one subnet number applicable to the same LAN or network segment in a router. Typically, one subnet is designated as primary, the others as secondary. A site might support addresses on more than one subnet number associated with a single interface. You must configure the DHCP server with the necessary information about your secondary subnets.
selection tags	Mechanisms that help select DHCPv4 scopes and DHCPv6 prefixes for clients and client-classes.
siaddr	IP address of the server to use in the next step of the DHCP boot process. Sent in an RFC 2131 packet between the client and server.
slave forwarder	DNS server that behaves like a stub resolver and passes most queries on to another name server for resolution. *See also* stub resolver.
slave servers	DNS server that always forwards queries it cannot answer from its cache to a fixed list of forwarding servers instead of querying the root name servers for answers.
SNMP notification	Simple Network Management Protocol messages that warn of server error conditions and problems. *See also* trap.
SOA record	DNS Start of Authority resource record (RR). Designates the start of a zone.
SRV record	Type of DNS resource record (RR) that allows administrators to use several servers for a single host domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups.
staged edit mode	dhcp or dns edit mode in which the data is stored on the CCM server, but not live on the protocol server. *See also* synchronous edit mode.
stub resolver	DNS server that hands off queries to another server instead of performing the full resolution itself.
subnet allocation, DHCP	Cisco Prime IP Express use of on-demand address pools for entire subnet allocation of IP addresses to provisioning devices.
subnet mask	Separate IP address, or part of a host IP address, that determines the host address subnet. For example, 192.168.40.0 255.255.255.0 (or 192.168.40.0/24) indicates that the first 24 bits of the IP address are its subnet, 192.168.40. In this way, addresses do not need to be divided strictly along network class lines.
subnet pool	Set of IP addresses associated with a network number and subnet mask, including secondary subnets.

subnet sorting	Attribute of the Cisco Prime IP Express DNS server. By enabling it, the server checks the network address of the client before responding to a query.
subnet utilization	A report that can be generated to determine how many addresses in the subnet were allocated and what the free address space is.
subnetting	Action of dividing any network class into multiple subnetworks.
subscriber limitation	Limitation to the number of addresses service providers can determine for the DHCP server to give out to devices on customer premises, handled in Cisco Prime IP Express by DHCP option 82 definitions.
subzones	Partition of a delegated domain, represented as a child of the parent node. A subzone always ends with the name of its parent. For example, boston.example.com. can be a subzone of example.com.
subzone delegation	Dividing a zone into subzones. You can delegate administrative authority for these subzones, and have them managed by people within those zones or served by separate servers.
supernet	Aggregation of IP network addresses advertised as a single classless network address.
synchronization	Synchronization can occur between the regional cluster and local clusters, the CCM and other protocol servers, failover servers, HA DNS servers, and routers.
synchronous edit mode	dhcp or dns edit mode in which the data is live on the protocol server. *See also* staged edit mode.

T	
TAC	Cisco Technical Assistance Center. Cisco Prime IP Express provide a **cnr_tactool** utility to use in reporting issues to the TAC.
TCP/IP	Suite of data communication protocols. Its name comes from two of the more important protocols in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). It forms the basis of Internet traffic.
template	DNS zones and DHCP scopes can have templates to create multiple objects with similar properties.
transaction signature (TSIG)	DHCP mechanism that ensures that DNS messages come from a trusted source and are not tampered with. *See also* access control list (ACL).
trap	Criteria set to detect certain SNMP events, such as to determine free addresses on the network. *See also* SNMP notification.

trimming and compacting	Trimming is periodic elimination of old historical data to regulate the size of log and other files. Compacting is reducing data older than a certain age to subsets of the records.

U	
Universal Time (UT)	International standard time reference that was formerly called Greenwich Mean Time (GMT), also called Universal Coordinated Time (UCT).
update configuration, DNS	Defines the relationship of a zone with its main and backup DNS servers for DNS update purposes.
update map, DNS	Defines an update relationship between a DHCP policy and a list of DNS zones.
update policy, DNS	Provide a mechanism in DHCP for managing update authorization at the DNS RR level.
User Datagram Protocol (UDP)	Connectionless TCP/IP transport layer protocol.

V	
virtual channel identifier (VCI) and virtual path identifier (VPI)	16-bit field in the header of an ATM cell. The VCI, together with the VPI, identifies the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transit on its way to its final destination. The function of the VCI is similar to that of the DLCI in Frame Relay.
virtual private network (VPN)	Protocol over which IP traffic of private address space can travel securely over a public TCP/IP network. A VPN uses tunneling to encrypt all information at the IP level. *See also* VRF.
VRF	VPN Routing and Forwarding instance. Routing table and forwarding information base table, populated by routing protocol contexts. *See also* virtual private network (VPN).

W	
well-known port	Any set of IP protocol port numbers preassigned for specific uses by transport level protocols, for example, TCP and UDP. Each server listens at a well-known port so clients can locate it.
WKS record	DNS Well Known Service resource record (RR). Used to list the services provided by the hosts in a zone. Common protocols are TCP and UDP.

Y	
yiaddr	"Your" client IP address, or address that the DHCP server offers (and ultimately assigns) the client. Sent in an RFC 2131 packet between the client and server.

Z	
zone	Delegation point in the DNS tree hierarchy that contains all the names from a certain point downward, except for those names that were delegated to other zones. A zone defines the contents of a contiguous section of the domain space, usually bounded by administrative boundaries. Each zone has configuration data composed of entries called resource records. A zone can map exactly to a single domain, but can also include only part of a domain, with the remainder delegated to another subzone.
zone distribution	Configuration that simplifies creating multiple zones that share the same secondary zone attributes. The zone distribution requires adding one or more predefined secondary servers.
zone of authority	Group of DNS domains for which a given name server is an authority.
zone transfer	Action that occurs when a secondary DNS server starts up and updates itself from the primary server. A secondary DNS server queries a primary name server with a specific packet type called AXFR (transfer all) or IXFR (incrementally transfer) and initiates a transfer of a copy of the database.

Glossary