# Managing the Central Configuration

This chapter explains how to manage the central configuration at the Cisco Prime Network Registrar regional cluster.



# Central Configuration Tasks

Central configuration management at the regional cluster can involve:

- Setting up server clusters, replicating their data, and polling DHCP utilization and lease history data from them.
- Setting up routers (see Managing Routers and Router Interfaces).
- 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 2.) 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 Use Traditional Licensing, on page 15 and Managing Servers.

# Default Ports for Cisco Prime Network Registrar Services

The following table lists the default ports used for the Cisco Prime Network Registrar services.

***Table 1: Default Ports for Cisco Prime Network Registrar 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 |
| 69 | UDP | TFTP (optional) client to server |
| 162 | TCP | SNMP traps server to server |
| 389 | TCP | DHCP server to LDAP server |
| 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 |
| 853 | TCP | DNS over TLS |
| 1234 | TCP | Local cluster CCM server to server |
| 1244 | TCP | Regional cluster CCM server to server |
| 4444 | TCP | SNMP client to server |
| 8080 | HTTP | Local cluster client to server web UI |
| 8090 | HTTP | Regional cluster client to server web UI |
| 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.

If you are using a firewall, you may have to open it for some of the ports (listed in Default Ports for Cisco Prime Network Registrar Services, on page 2) depending on which services are in use.

## DNS Performance and Firewall Connection Tracking

**Note** Many distributions of Red Hat and CentOS Linux come with a firewall and connection tracking installed and enabled by default.

The Cisco Prime Network Registrar Caching and Authoritative DNS servers are designed and often deployed to process a very large volume of queries per second (QPS). Typically the majority of the queries are UDP based with rapid resolution times from many different clients with varying source port. When firewall connection tracking of DNS traffic is in use, the firewall will treat these requests as new connections for tracking. Since UDP is a connectionless protocol, the firewall must rely on a configuration timeout to stop monitoring the connection. The firewall connection monitoring timeout is typically very large relative to the DNS resolution time, meaning that the firewall will continue to use resources to monitor completed requests. This leads to the firewall to quickly hit its configuration limits and causes a huge drop in DNS performance as up to 90% of requests are dropped and never reach the DNS server.

Cisco strongly recommends NOT to use a firewall on the DNS server's operating system. The firewall should be run on a separate appliance outside of the DNS server's OS. If disabling the firewall is not possible, then connection tracking of DNS traffic MUST be disabled. Be aware that even with DNS connection tracking disabled, a co-located firewall can introduce a 25-30% performance impact on the system and DNS performance.

**Note** Cisco does NOT support deployments with firewall connection tracking of DNS traffic.

### Disabling the Firewall

Following is the example of stopping and disabling firewall. CentOS 7/Red Hat 7 and 8 use **firewalld**. Note that the commands must be run as root.

**firewalld**

```
# systemctl stop firewalld
# systemctl disable firewalld
```

## Disabling Connection Tracking for DNS Traffic

Following are the examples of disabling DNS from firewall connection tracking. CentOS 7/Red Hat 7 and 8 use **firewalld**/**firewall-cmd**. Note that the commands must be run as root and there are separate configuration for IPv4 and IPv6.

### firewall-cmd (IPv4)

```
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --dport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --sport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --sport 53 -j
ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --dport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --sport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --sport 53 -j
ACCEPT
```

### firewall-cmd (IPv6)

```
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --dport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --sport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --sport 53 -j
ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --dport 53 -j CT
--notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --sport 53 -j CT
```

```
--notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --sport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --dport 53 -j
ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --sport 53 -j
ACCEPT
```

## Configuring Caching DNS to Use Umbrella

Cisco Umbrella provides the first line of defense against threats on the internet, such as phishing and malware. By setting up the Caching DNS to use Umbrella for resolution, you can allow the Cisco cloud service of Umbrella to provide the latest responses for the requested domain/host. For more information, see the *"Configuring Caching DNS to Use Umbrella" section in Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide*.

**Note** To get full benefits of using the Umbrella service, you need to have a business relationship with Cisco Umbrella.

# Licensing

Cisco Prime Network Registrar requires separate license for CCM, Authoritative DNS, Caching DNS, and DHCP services or for combinations of these services. Cisco Prime Network Registrar 11.1 license file contains two sets of licenses which cover the permanent and subscription parts of the license. You must purchase subscription license for future upgrades. The initial subscription is always three years and one year extension for renewals. For more details on the Licensing, see the *"License Files" section in Cisco Prime Network Registrar 11.1 Installation Guide*.

You can add the additional service based licenses in the regional server after you log in. You should not delete any of the individual licenses loaded from the file. You may delete older version DNS and DHCP licenses after upgrade. Older version CDNS licenses must be retained if the servers are not upgraded.

Cisco Prime Network Registrar 11.1 supports both Smart Licensing and traditional licensing. However, it does not support the hybrid model, that is, you can use any one of the license types at a time. Previous versions (10.x or earlier) of Cisco Prime Network Registrar supported only FLEXlm licenses, in which you purchase a perpetual license for a version and use it until Cisco Prime Network Registrar servers are upgraded to a newer major version. At that time, you must purchase new licenses, and then the cycle repeats itself. One drawback with this approach is that every time Cisco Prime Network Registrar server is upgraded or purchased, license file is delivered to you via e-mail. This file is loaded into the regional server to enable the application.

Smart Licensing is not another traditional licensing system; it is more comparable to a software asset management system in which the licenses are not installed on the individual Cisco products. It is significantly more flexible than traditional software models, and it simplifies the way you activate and manage licenses. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

How to use Cisco Smart Licensing and traditional licensing in Cisco Prime Network Registrar is explained in the following topics:

# Use Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation**: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management**: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility**: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

In case of Smart Licensing, all the licenses purchased by you are kept in a centralized system called Cisco Smart Software Manager (CSSM) or CSSM On-Prem (Satellite), in customer specific Smart accounts. Cisco Prime Network Registrar server (regional) periodically sends the license usage information to the CSSM or Satellite. You can login to your Smart account and get the license utilization information.

In Cisco Prime Network Registrar, Smart Licensing is enabled by default. If you have disabled it for any reason, then enable it and then register Cisco Prime Network Registrar with the CSSM (or Satellite) using web UI or CLI. You will remain in evaluation mode (which is maximum 90 days) until this registration is successful. While in evaluation mode, you will be licensed for the selected features until the evaluation period expires. After the evaluation period of 90 days, if the product is not registered with the CSSM (or Satellite) or reservation is also not installed, all features will be marked as Out of Compliance (OOC). Smart License will still remain enabled and you can still register Cisco Prime Network Registrar with the CSSM (or Satellite) or install reservation. After the registration is successful, all Cisco Prime Network Registrar license types are available to you in the CSSM (or Satellite).

Following topics explain how to set up and manage Cisco Prime Network Registrar licenses using Cisco Smart Licensing.

## Setting Up Smart Licensing in Cisco Prime Network Registrar

To set up Cisco Smart Licensing so you can use it to manage your licenses, do the following:

**Step 1** Smart Licensing is enabled by default in Cisco Prime Network Registrar. If you have disabled it for any reason, then enable it. See Enabling Smart Licensing, on page 7.

**Step 2** Create a Smart Account with Cisco Systems. To do this, go to Smart Account Request and follow the instructions on the website.

**Step 3** Set up communication between Cisco Prime Network Registrar and the CSSM (or Satellite). See Setting Up the Transport Mode Between Cisco Prime Network Registrar and the CSSM, on page 7.

**Step 4** Register Cisco Prime Network Registrar with the CSSM (or Satellite) using web UI or CLI. See Registering Cisco Prime Network Registrar with the CSSM (or Satellite), on page 8.

**Step 5** Monitor your Smart License usage. See Viewing Smart License Usage, on page 9.

## Enabling Smart Licensing

In Cisco Prime Network Registrar, Smart Licensing is enabled by default for both new installations and upgrade from previous versions. If you have disabled Smart Licensing for any reason, then to enable it, do the following:

### *Regional Advanced Web UI*

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

**Step 2** Click the **Use Smart Software Licensing** button in the Smart Software Licensing page.

#### What to do next

Set up the transport mode between Cisco Prime Network Registrar and the CSSM (or Satellite) as described in Setting Up the Transport Mode Between Cisco Prime Network Registrar and the CSSM, on page 7.

### *CLI Commands*

Enable the Smart License configuration mode using the **smart** command and then use the **license smart enable** command to enable Smart Licensing:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart enable
```

## Setting Up the Transport Mode Between Cisco Prime Network Registrar and the CSSM

Cisco Prime Network Registrar regional server communicates with the CSSM using Call Home or Smart Transport, based on the transport configuration. Call Home is the default transport setting. Communication is established between the Smart Agent of Cisco Prime Network Registrar and the CSSM.

**Note** When using Smart Transport for communication, you must explicitly set the CSSM server URL to default or custom URL. To do this, use the **license smart url [default |** *url***]** command.

**Note** Smart Transport has a dependency on libcurl (built with OpenSSL). If libcurl present in the system is not built with OpenSSL, then communication with the CSSM will not be successful. In this situation, either you should use Call Home as the transport setting or install libcurl (built with OpenSSL) on the system.

To set up the transport mode between Cisco Prime Network Registrar and the CSSM, do the following:

### *Regional Advanced Web UI*

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

**Step 2** Click the **View / Edit** link next to **Transport Settings** to open the Transport Settings page. Select a communication mode (under Call Home Settings or Smart Transport Settings):

- Direct mode—Cisco Prime Network Registrar sends usage information directly over the internet. No additional components are required.
- Transport Gateway—Cisco Prime Network Registrar sends usage information to a locally installed satellite. Periodically, exchanges information with Cisco to keep satellite sync. This synchronization can occur automatically in connected environments or manually in disconnected environments.
- HTTP/HTTPS Proxy—Cisco Prime Network Registrar sends usage information over the internet via a proxy server. Any off-the-shelf proxy will work.

**Step 3** Click **Save** to save the transport settings.

#### What to do next

If you have not yet registered Cisco Prime Network Registrar with the CSSM (or Satellite), Cisco Prime Network Registrar will run in evaluation mode (which has a limit of 90 days). Register the product as described in Registering Cisco Prime Network Registrar with the CSSM (or Satellite), on page 8.

### *CLI Commands*

Enable the Smart License configuration mode using the **smart** command and then use the **license smart transport [callhome | smart]** command to set the transport type for Smart Licensing:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart transport [callhome | smart]
```

Then,

- If you use **callhome** transport setting, specify the URL using the following command:

  ```
  nrcmd-R [smartlic]> call-home destination address http url
  ```

- If you use **smart** transport setting, specify the URL using the following command:

  ```
  nrcmd-R [smartlic]> license smart url [default|url]
  ```

## Registering Cisco Prime Network Registrar with the CSSM (or Satellite)

To register Cisco Prime Network Registrar with the CSSM (or Satellite), you must obtain a token from the CSSM (or Satellite) and enter it in the Cisco Prime Network Registrar web UI or CLI. This is a one-time requirement.

#### Before you begin

Ensure that you have a Smart Account with Cisco Systems. If you do not have a Smart Account, then go to Smart Account Request and follow the instructions on the website. Also, ensure that you have connectivity

to the URL specified in the Transport Settings (available in the Smart Software Licensing page of Cisco Prime Network Registrar).

**Step 1** Log in to your Smart Account in the CSSM or Smart Software Manager satellite.

**Step 2** Navigate to the virtual account containing the licenses to be used by this product instance.

**Step 3** Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

**Regional Advanced Web UI**

**Step 4** From the **Administration** menu, choose **Smart Licenses** under the **User Access** submenu to open the Smart Software Licensing page.

**Step 5** Click the **Register** button to open the Smart Software Licensing Product Registration page.

**Step 6** Paste the Product Instance Registration Token you generated from the CSSM or Smart Software Manager satellite.

**Step 7** Click **Register**.

#### *CLI Commands*

Enable the Smart License configuration mode using the **smart** command and then use the **license smart register idtoken** *token* command to register Cisco Prime Network Registrar with the CSSM (or Satellite), where *token* is the Product Instance Registration Token generated from the CSSM (or Satellite):

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart register idtoken token
```

## Viewing Smart License Usage

When Smart Licensing is enabled, Cisco Prime Network Registrar will not display the information about the licensed number of leases (for DHCP), number of RRs (for Authoritative DNS), and number of Caching DNS servers. You must refer the CSSM (or Satellite) for the actual license count. However, you can use Cisco Prime Network Registrar web UI or CLI to view the license counts that are currently in use.

### Regional Advanced Web UI

To view the current license usage in web UI, from the **Administration** menu, choose **Smart Licenses** under the **User Access** submenu. The Smart License usage details are available in the **Smart License Usage** section at the bottom of the page.

### CLI Commands

Enable the Smart License configuration mode using the **smart** command and then use the **show license summary** command to display the license authorization state and the licenses that are currently used in the system:

```
nrcmd-R> smart

nrcmd-R [smartlic]> show license summary
```

# Renewing License Authorization and ID Certificate

### Renew License Authorization

After registration, when the Smart Agent receives a successful response to an Entitlement Authorization Request sent to the CSSM (or Satellite), it enters the Authorized or Out of Compliance state. Authorization periods are renewed by the Smart Licensing system every 30 days automatically. As long as the license is in Authorized or Out of Compliance state, the authorization period is renewed.

To manually renew the authorization to avoid waiting 30 days for the next renewal cycle, do the following:

*Regional Advanced Web UI*

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

**Step 2** Click the **Actions** button and then click **Renew Authorization Now**.

The Authorization Expired state starts when the authorization period expires (after 90 days).

*CLI Commands*

Enable the Smart License configuration mode using the **smart** command and then use the **license smart renew auth** command to manually renew the authorization:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart renew auth
```

### Renew ID Certificate

The ID certificate expires at the end of one year. After 6 months, the agent will try to renew the certificate. If the agent cannot communicate with the CSSM, it will continue to try and renew the ID certificate until the expiration date (one year). At the end of one year, the agent will go back to the Un-Identified state and will try to enable the Evaluation period. The CSSM will remove the product instance from its database.

To manually renew the ID certificate, do the following:

*Regional Advanced Web UI*

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

**Step 2** Click the **Actions** button and then click **Renew Registration Now**.

*CLI Commands*

Enable the Smart License configuration mode using the **smart** command and then use the **license smart renew ID** command to manually renew the ID certificate:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart renew ID
```

# Re-registering Cisco Prime Network Register with the CSSM (or Satellite)

If the registration fails due to communication failure between Cisco Prime Network Register and the CSSM (or Satellite), you may attempt to register the product again. To re-register Cisco Prime Network Register with the CSSM (or Satellite), do the following:

### Before you begin

Ensure that you have obtained the Product Instance Registration Token from the CSSM (or Satellite). For more information, see Registering Cisco Prime Network Registrar with the CSSM (or Satellite), on page 8.

### Regional Advanced Web UI

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

**Step 2** Click the **Actions** button and then click **ReRegister**.

### CLI Commands

Enable the Smart License configuration mode using the **smart** command and then use the **license smart register idtoken** *token* [**force**] command to re-register Cisco Prime Network Register with the CSSM (or Satellite), where *token* is the Product Instance Registration Token generated from the CSSM (or Satellite):

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart register idtoken token force
```

# Deregistering Cisco Prime Network Register

To cancel the registration of the Cisco Prime Network Register regional server, do the following:

### Regional Advanced Web UI

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

**Step 2** Click the **Actions** button and then click **DeRegister**.

After deregistering, the product will be moved to Evaluation mode and the product instance will be removed from the CSSM.

### CLI Commands

Enable the Smart License configuration mode using the **smart** command and then use the **license smart deregister** command to cancel the registration of the Cisco Prime Network Register regional server:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart deregister
```

# Disabling Smart Licensing

In Cisco Prime Network Registrar, Smart Licensing is enabled by default. To disable Smart Licensing for any reason (for example, in case you want to use traditional licensing), do the following:

### Regional Advanced Web UI

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

**Step 2** Click the **Actions** button and then click **Disable Smart Software Licensing**.

### CLI Commands

Enable the smart license configuration mode using the **smart** command and then use the **no license smart enable** command to disable Smart Licensing:

```
nrcmd-R> smart

nrcmd-R [smartlic]> no license smart enable
```

# Using Smart License Reservation

Cisco Prime Network Registrar supports Smart License Reservation mode wherein you can reserve a pool of licenses against a regional server. You can reserve Smart Software Licenses by providing a Reservation Request Code in the CSSM. In this method, you can deploy a software license on a product instance without communicating the usage information to the CSSM. It is useful in highly secure networks.

There are two types of Smart License Reservation:

- **Permanent License Reservation** (**PLR**)—PLR is a set of capabilities that is designed for highly secure environments, where communication with outside environment is impossible. Permanent licenses do not require periodic access to the License Authority. Like PAK licenses, you can purchase a license and install the license key for Cisco Prime Network Registrar.
- **Specific License Reservation** (**SLR**)—SLR is an enforced licensing model that is similar to node locked licensing. The main difference between PLR and SLR is, SLR allows you to select only the required licenses, whereas with PLR it is a single license that activates all the functionalities of the product. Anyone with a Smart Account can use the SLR feature if they have the product instances that support it.

### Enabling PLR/SLR

Note that in Cisco Prime Network Registrar, the configuration of Smart License Reservation is possible only via CLI.

To enable PLR/SLR in Cisco Prime Network Registrar, do the following:

**Step 1** Enable Smart License Reservation in the Cisco Prime Network Registrar regional server using the following commands:

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart reservation
```

**Step 2** Generate the Request Code using the following command. Copy this Request Code or save it as a file.

```
nrcmd-R [smartlic]> license smart reservation request [local | all]
```

**Note** It is recommended to use the **local** option to generate the code in Cisco Prime Network Registrar.

**Step 3** Enter the Reservation Request Code in the CSSM.

a) Log in to your Smart Account in the CSSM.
b) Click the **License Reservation** button to open the Smart License Reservation page.
c) Paste the Request Code in the **Reservation Request Code** text area or use the **Browse** option to add it as a file.
d) Click **Next**.

**Step 4** Select the type of license (**PNR-PLR** or **Reserve a specific license**) that you want to reserve. If you select specific license, then select the required number of licenses from the list. Click **Next**.

**Step 5** Review and confirm the information that you entered in the previous step, and click **Generate Authorization Code**. Either copy this Authorization Code to a clipboard, or download it as a file and save it in the Cisco Prime Network Registrar server.

**Step 6** Install the Authorization Code in Cisco Prime Network Registrar using either of the following commands:

- If you have copied the Authorization Code in the previous step, then use the following command. Ensure that you enclose the Authorization Code in double quotes.

  ```
  nrcmd-R [smartlic]> license smart reservation install auth-code
  ```

- If you have downloaded the Authorization Code as a file in the previous step, then use the following command:

  ```
  nrcmd-R [smartlic]> license smart reservation install file file-path
  ```

**Note** Since Authorization Code can be a long string, the install file option is recommended while installing SLR. Else, enclose the Authorization Code in double quotes.

### Updating Reserved Licenses

You can update the reservation counts in the CSSM. To update the reserved licenses, do the following:

**Step 1** Log in to your Smart Account in the CSSM.

**Step 2** Navigate to the required product instance in the Product Instance tab and click **Actions** > **Update Reserved Licenses**. The Update License Reservation page opens.

**Step 3** Select the **Reserve a specific license** radio button and then, update the reservation counts as required. Click **Next**.

**Step 4** Click **Generate Authorization Code**. Either copy this Authorization Code to a clipboard, or download it as a file and save it in the Cisco Prime Network Registrar server.

**Step 5** Install the Authorization Code in Cisco Prime Network Registrar using either of the following commands. This command generates a Confirmation Code.

- If you have copied the Authorization Code in the previous step, then use the following command. Ensure that you enclose the Authorization Code in double quotes.

  ```
  nrcmd-R [smartlic]> license smart reservation install auth-code
  ```

- If you have downloaded the Authorization Code as a file in the previous step, then use the following command:

  ```
  nrcmd-R [smartlic]> license smart reservation install file file-path
  ```

**Note** Since Authorization Code can be a long string, the install file option is recommended while installing SLR. Else, enclose the Authorization Code in double quotes.

**Step 6** Enter the Confirmation Code in the CSSM.

a) Go to the Update License Reservation page in the CSSM and click **Enter Confirmation Code**.
b) Paste the Confirmation Code in the **Reservation Confirmation Code** text area or use the **Browse** option to add it as a file.
c) Click **Ok**.

### Removing Product Instance

To remove the product instance from the License Reservation, do the following:

**Step 1** Generate the Return Code using the following commands. Copy this Request Code.

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart reservation return [local | all]
```

**Note** It is recommended to use the **local** option to generate the code in Cisco Prime Network Registrar.

**Step 2** Log in to your Smart Account in the CSSM.

**Step 3** Navigate to the required product instance in the Product Instance tab and click **Actions** > **Remove**. The Remove Product Instance page opens.

**Step 4** Paste the Return Code in the **Reservation Return Code** text area.

**Step 5** Click **Remove Product Instance**.

**Step 6** Disable the Smart License Reservation using the following commands:

```
nrcmd-R> smart

nrcmd-R [smartlic]> no license smart reservation
```

## Smart Product Registration and License Authorization Statuses

### Product Registration Status

The License Registration Status reflects whether the product is properly registered with Cisco Smart Software Licensing on Cisco.com.

| License Registration Status | Description |
|---|---|
| Unconfigured/Onboarding | Smart Licensing is initialized but not enabled yet. Cisco Prime Network Registrar server will move into this state if Smart Licensing is disabled. |
| Unregistered/Unidentified | Smart Licensing is enabled in Cisco Prime Network Registrar but Cisco Prime Network Registrar is not registered with the CSSM (or Satellite) yet. In this state, licensed features may be used freely during a 90-day evaluation period. |

| License Registration Status | Description |
|---|---|
| Registered | Cisco Prime Network Registrar is registered with the CSSM (or Satellite). Cisco Prime Network Registrar has received an ID certificate that will be used for future communication with the Cisco licensing authority. The certificate is valid for one year and will be renewed automatically after six months to ensure continuous operation. |
| Registration Expired | Cisco Prime Network Registrar did not successfully renew its registration prior to the expiration date and has been removed from the CSSM (or Satellite). After registration expires, registration to the CSSM (or Satellite) using a new registration ID token is required. |

### License Authorization Status

The License Authorization status reflects license usage against purchased licenses, and whether you are in compliance with Cisco Smart Licensing. If you exceed the number of purchased licenses, the product's status will be **Out of Compliance**.

| License Authorization Status | Description |
|---|---|
| Evaluation Mode | Cisco Prime Network Registrar is running in evaluation mode (expires in 90 days). |
| Authorized (In Compliance) | Cisco Prime Network Registrar has a valid Smart Account and is registered. All licenses requested by the product are authorized for use. |
| Out of Compliance | Cisco Prime Network Registrar has exceeded the number of licenses that were purchased. (Specifically, the virtual account for the product instance has a shortage of one or more licenses types.) |
| Evaluation Expired | The evaluation period has expired and Cisco Prime Network Registrar is in the unlicensed state. |
| Authorization Expired | Cisco Prime Network Registrar did not successfully renew its license authorization prior to the authorization expiration date. The CSSM (or Satellite) returns all in-use licenses for this server back to the pool since it has not had any communication for 90 days. |

# Use Traditional Licensing

To use traditional licensing, you must disable Smart Licensing first (see Disabling Smart Licensing, on page 12). Then, for entering the license data the first time, see Logging in to the Web UI.

Whenever you log in to a regional or local cluster, the overall licensing status of the system is checked. If there is no valid system license, the login will be rejected. 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 **Choose File** 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. If the In Use count exceeds the Right To Use count, the "License exceed count" error message appears.

Licenses and usage count of earlier versions of Cisco Prime Network Registrar are 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 Traditional License

Cisco will e-mail you one or more license files after you register the Cisco Prime Network Registrar Product Authorization Key (PAK) on the web according to the Software License Claim Certificate shipped with the product. Cisco administers traditional 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 e-mail 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 Use Traditional Licensing, on page 15.

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 Network Registrar 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.

# License History

The License History page allows you to view the licenses utilized in the specified time frame. You can view the license history in the form of chart, wherein you can see the license utilization history for various services over a period of time in one view. Also, the data is displayed in reverse chronological order, so that the most recent data is displayed on top. Based on usage and services configured, the chart's Y-axis may vary.

To view the license history, do the following:

## Regional Web UI

**Step 1** From the **Administration** menu, choose **License History** under the **User Access** submenu to open the View License Utilization History page.

**Step 2** Specify the filter settings in the **Set License History Filter** attribute. Enable the **Down-sample results** checkbox to down-sample the data set that matches the filter options to fit within the specified number of time buckets.

**Step 3** Click **Apply Filter** to view the license history for the specified time frame.

- The details appear in the form of chart under the **License History Charts** tab. You can change the chart type by clicking the **Chart Type** icon present below the chart. The different types of chart available are: Column Chart, Line Chart, Area Chart, and Scatter Chart. Click the **Table View** icon below the chart to view the chart data in the form of table.
- Click the **License Table** tab to view the license history details in the form of table.

## CLI Command

Use the **license showUtilHistory** [**-start** *start-time*] [**-end** *end-time*] [**-service cdns** | **dns** | **dhcp** |...| **all**] command to display the license usage history for all or selected services over time.

# License Utilization

The regional CCM server periodically collects license utilization information from the local clusters and updates the local clusters about whether licensing is in compliance or not based on the collected usage and registered licenses.

The regional server collects the following metrics from the local clusters to determine the license counts:

- **DHCP services**—The count of active leases is obtained by summing the DHCPv4 and DHCPv6 lease counts.

  Starting from Cisco Prime Network Registrar 11.0, the DHCPv4 count is calculated from the DHCP server's **server** category *active-leases* + *reserved-leases* – *reserved-active-leases* statistics. DHCPv6 count is calculated from the DHCP server's **dhcpv6** category *active-leases* + *reserved-leases* – *reserved-active-leases* statistics.

- **Auth DNS services**—The count is from the DNS server's **server** category *total-rrs* statistic.
- **Caching DNS services**—The count is 1 if CDNS has been licensed on the cluster.

**Note**

- For failover-pairs and HA-DNS pairs, only one of the clusters is contacted; usually the main if it is reachable. If the regional does not have valid failover-pair and HA-DNS information, it may calculate incorrect license utilization for DHCP or DNS.
- Ensure that the replica data is up to date for the clusters (see Synchronizing with Local Clusters, on page 21), and then pull the address space and/or zone data.

## CLI Command

Use the **license showUtilization** [**-rescan**] command to view the number of utilized IP nodes against the RTUs (Right-to-Use). If the **-rescan** option is specified on the regional, a licensing scan of the local clusters is initiated to update the licensing usage.

# Registering a Local Cluster that is Behind a NAT

License management is done from the regional cluster when Cisco Prime Network Registrar 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 Network Registrar, 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 Network Registrar 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 the **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 Network Registrar system for all counted services (DHCP, DNS, and CDNS).

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

## Generating a New UUID

To generate a new UUID and register, do the following:

### Local Web UI

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

**Step 2** Add the details of the regional cluster.

**Step 3** Check the **Generate new host identifier** check box.

**Step 4** Click **Register**.

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

# Configuring Server Clusters

Server clusters are groupings of CCM, DNS, CDNS, DHCP, and TFTP 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 DHCP 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, TFTP, or DHCP failover servers.

# Adding Local Clusters

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

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 Network Registrar 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 Network Registrar 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 DHCP 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 67. 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 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 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 **Resync** icon 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 primary 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 /var/nwreg2/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 the **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**. This 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. You must restart the cluster after recovery of the data is completed.

Deactivating, reactivating, and recovering the data for a cluster requires 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).
- 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. 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.

Sometimes the restore operation may return "Requested key/data pair not found" error or create duplicate entries for some objects on the local cluster. This issue is observed if the local cluster had some objects with corrupt/incorrect indexes before performing the restore operation. To resolve this, take either of the below mentioned actions. The first option is recommended, but it may not work always. Only in such situation, take the second action:

- Stop Cisco Prime Network Registrar on the local cluster and run rebuild_indexes for databases on the local cluster. Then, start the Cisco Prime Network Registrar local cluster and try the restore operation again.
- Stop Cisco Prime Network Registrar on the local cluster and move the existing content of the data directory to the backup location. Start the Cisco Prime Network Registrar local cluster again to create the fresh databases (two stop-start sequence is required to create all the databases). Register the local cluster with regional and perform the restore operation from the regional cluster.

## 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 DHCP 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 2: 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** |
| View Replica Data | **cluster** *name* **viewReplicaData** < *class-name* \| *cli-command* > [**-listbrief** \| **-listcsv**] |

# Viewing Cluster Report

The Cluster Report page on the regional web UI displays the relevant information for the selected cluster in a graphical/chart based manner, so that the cluster specific data can be easily monitored and visualized from the regional cluster. This report page displays the status of the cluster connection (connected, not connected, etc). It also displays the status of the services licensed on the cluster (DHCP is up, DNS is down, etc.), server summary, system metrics, DNS/CDNS top names, and resource summary.

To view the cluster report, do the following:

## Regional Web UI

**Step 1** From the **Operate** menu, choose **Manage Clusters** under the **Servers** submenu to open the List/Add Remote Clusters page.

**Step 2** Click the cluster name on the left pane.

**Step 3** Click the **Cluster Report** tab on the Edit Remote Cluster page. The relevant information for the selected cluster is displayed. The current system and resource metrics for the cluster are displayed in the form of chart/table. Use the **Show** icon (

) present below the chart to display the data in the form of chart or table and use the **Chart Type** icon (  ) to change the type of chart. The different types of chart available are: Column Chart, Line Chart, Area Chart, and Scatter Chart.

# Central Configuration Management Server

The CCM servers at the local and regional clusters provide the infrastructure for Cisco Prime Network Registrar operation and user interfaces. The CCM Server reads, writes, and modifies the Cisco Prime Network Registrar 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** under the **Servers** submenu to open the Manage Servers page. Use the CCM server *log-settings* attribute to enable or disable the required log categories, as described in the table below. Log categories apply only to informational messages. Error and warning level log messages are always written to log files.

***Table 3: CCM Log Settings***

| Log Setting (Numeric Equivalent) | Description |
|---|---|
| all (0) | Causes the server to log messages for all categories. This setting is enabled by default. |
| authentication (2) | Causes the server to log messages during user or token session authentication. |
| database (1) | Causes the server to log messages for database operations such as shadow backup. |
| dnssec (9) | Causes the server to log messages related to DNSSEC processing. Messages will be logged when a DNSSEC key is created, deleted, enabled, disabled or rolled over by the CCM Server. It also causes the server to log messages when DNSSEC is disabled on zone or when a task is scheduled to sign or resign a zone. |
| lease-history (10) | Causes the server to log messages when lease history polling is started or finished. |
| licensing (5) | Causes the server to log messages for local cluster registration, or when regional and local cluster license utilization reports are collected or reported. |
| replica (7) | Causes the server to log messages when replica polling is initiated or a local cluster is successfully restored. |
| scheduled-tasks (4) | Causes the server to log messages when the CCM server schedules a task or when a scheduled task is completed. |

| Log Setting (Numeric Equivalent) | Description |
|---|---|
| scp-details (3) | Causes the server to log SCP message responses and internal SCP communication between CCM and other servers. External SCP requests such as communication from the CLI or web UI are always logged. |
| server-events (6) | Causes the server to log all server-events sent from protocol servers to CCM server, including events for SNMP traps. |
| utilization (8) | Causes the server to log messages when utilization polling is started or finished. |

# Editing CCM Server Properties

You can edit the CCM server properties 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 **CCM** 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.

# Trivial File Transfer

The Trivial File Transfer Protocol (TFTP) is a way of transferring files across the network using the User Datagram Protocol (UDP), a connectionless transport layer protocol. Cisco Prime Network Registrar maintains a TFTP server so that systems can provide device provisioning files to cable modems that comply with the Data Over Cable Service Interface Specification (DOCSIS) standard. The TFTP server buffers the DOCSIS file in its local memory as it sends the file to the modem. After a TFTP transfer, the server flushes the file from local memory. TFTP also supports non-DOCSIS configuration files.

Here are some of the features of the Cisco Prime Network Registrar TFTP server:

- Complies with RFCs 1123, 1350, 1782, and 1783.
- Includes a high performance multithreaded architecture.
- Supports IPv6.
- Caches data for performance enhancements.
- Is configurable and controllable in the web UI and using the **tftp** command in the CLI.
- Includes flexible path and file access controls.
- Includes audit logging of TFTP connections and file transfers

- Has a default root directory in Cisco Prime Network Registrar /var/nwreg2/{local | regional}/data/tftp.

# Viewing and Editing the TFTP Server

At the local cluster, you can edit the TFTP server to modify its attributes. You must be assigned the server-management subrole of the ccm-admin role.

## Local Web UI

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

**Step 2** Click **TFTP** in the Manage Servers pane to open the Edit Local TFTP Server page.

You can click the name of any attribute to open a description window for the attribute.

**Step 3** To unset any attribute value, check the check box in the **Unset?** column.

**Step 4** Click **Save** to save the changes or **Revert** to cancel the changes.

## CLI Commands

Use **tftp show** to show the attribute values. Use **tftp set** *attribute=value* [*attribute=value* ...] or **tftp enable** *attribute* to set or enable attributes. You can also use **tftp serverLogs show**, and **tftp serverLogs nlogs**=*number* **logsize**=*size*.

# Managing the TFTP Server Network Interfaces

You can manage the network interfaces for the TFTP server.

## Local Advanced Web UI

Manage the network interfaces associated with the TFTP server by clicking the **Network Interfaces** tab for the selected Local TFTP Server in the Manage Servers page. 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.

The columns in the Network Interfaces page are:

- **Name**—Name of the network interface, such as the LAN adapter, loopback, and Fast Ethernet interfaces. If the name is under the **Configured Interfaces** column, you can edit and delete the interface. Clicking the name opens the Edit TFTP Server Network Interface page so that you can edit the interface name and addresses. Make the changes and then click **Save** on this page.
- **IP Address**—IP address of the network interface.
- **IPv6 Address**—IPv6 address, if applicable, of the network interface.
- **Flags**—Flags for whether the interface should be zero-broadcast, virtual, v4, v6, no-multicast, or receive-only.

- **Configure**—To configure a new network interface, click the **Configure** icon next to the interface name. This creates another interface based on the one selected, but with a more general IP address, and adds this interface to the Configured Interfaces for this TFTP Server.
- **List of available interfaces for this TFTP server**—User-configured network interfaces, showing each name and associated address. Click the interface name to edit it or click the **Delete** icon to delete it.

To return to managing the server, click **Revert**.

## CLI Commands

Use the **tftp-interface** commands.

# Simple Network Management

The Cisco Prime Network Registrar 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 Network Registrar implements SNMP Trap Protocol Data Units (PDUs) according to the SNMPv2c and SNMPv3 standards. 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.
- When sending SNMPv3 traps, there may be optional credentials included, depending on the recipient's configured requirements.

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 Network Registrar 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/

# Setting Up the SNMP Server

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

## Local 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).

**Step 2** Click **SNMP** in the Manage Servers pane 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. The interface properties are similar to those for the TFTP server (see Managing the TFTP Server Network Interfaces, on page 28).

**Step 6** To add 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.

**Step 7** To edit the trap recipients:

**SNMPv2c:**

a) Click the name of the trap recipient in the Trap Recipients tab to open the Edit Trap Recipient page.
b) Set the following attributes in the **Settings** section:

- *ip-addr*—Specifies the IP address of this trap recipient.
- *port-number*—The optional IP port number of this trap recipient.
- *community*—The SNMP community string of this trap recipient.
- *agent-addr*—An IP address to use as the source agent address in traps sent to this recipient.
- *tenant-id*—Identifies the tenant owner of this object.
- *ip6address*—Specifies the IPv6 address of this trap recipient.
- *v6-port-number*—The optional IPv6 port number of this trap recipient.

**SNMPv3:**

a) On the Edit Local SNMP Server page, select the **enabled** option for *local-proxy-only*. This attribute defines whether the server accepts queries only from local and proxied sources, or from any source. When using SNMPv3, enabling this is recommended. Enabling this setting overrides any SNMP interface configuration.
b) Click the name of the trap recipient in the Trap Recipients tab to open the Edit Trap Recipient page.
c) You can set the following attributes in the **SNMPv3 Settings** section in addition to those listed in the SNMPv2c section. Note that in most cases, the *Community string* attribute is optional (it is dependent on the recipient configuration).

- *snmp-user*—SNMP user name of this trap recipient.
- *snmp-trap-msg*—Defines if this client wants a TRAP or INFORM message.
- *snmp-security*—Specifies which security level to use.
  - no-auth—No authentication or privacy.
  - auth-nopriv—Use SHA for account authentication. Requires an authentication password.
  - auth-priv—Use SHA for account authentication and AES for communication privacy. Requires both authentication and privacy passwords.
- *snmp-auth-password*—Specifies the password for account authentication.
- *snmp-priv-password*—Specifies the password for communication privacy.
- *snmp-v3-protocol*—Specifies if this recipient should be sent messages over UDP or TCP.
- *snmp-engine-id*—Specifies the engine ID of the recipient, if required.

**Step 8** 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=***value* to set the trap source IPv4 address. Use **snmp set trap-source-ip6address=***value* 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** *name* **set** *attribute=value* [*attribute=value* ...]. For example:

```
nrcmd> trap-recipient example-recipient set ip-addr=192.168.0.34
nrcmd> trap-recipient example-recipient set ip6address=2001:4f8:ffff:0:8125:ef1b:bdcb:4b4e
```

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. The **addr-trap** command is described in Managing the TFTP Server Network Interfaces, on page 28.

# How Notification Works

Cisco Prime Network Registrar 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 Network Registrar 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 4: 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. |

| Event | Notification |
|---|---|
| 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 primary servers not responding (*primary-not-responding*) | Primary DNS servers stop responding to the DNS server. |
| DNS primary servers responding (*primary-responding*) | Primary 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. |
| 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 Network Registrar 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:

*Table 5: CISCO-EPM-NOTIFICATION-MIB Trap Attribute Mappings*

| 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" |
| 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" |

| Trap Attribute Name | Object ID | Type | Value for Resource Events |
|---|---|---|---|
| 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 49.

# Handling SNMP Notification Events

When Cisco Prime Network Registrar 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 36):

- **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 36):

- **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 Web UI

Access the SNMP attributes for the DHCP server by choosing **Manage Servers** from the **Operate** menu, then click **DHCP** 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 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 Network Registrar 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%
```

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified.

- **addr-trap** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **addr-trap** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]
- **addr-trap** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

# 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.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 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 Network Registrar SNMP into System SNMP

Starting from Cisco Prime Network Registrar 11.1, the Cisco Prime Network Registrar SNMP server automatically integrates into the system SNMP server via the proxy mechanism. When using SNMPv3 on the system SNMP server, you must manage the credentials using the appropriate system tools.

# Polling Process

When the regional cluster polls the local cluster for DHCP 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 Utilization and Lease History Data

When local is registered with regional or on default poll (every 1 hour) or on manual poll, the DHCP utilization data is collected. All available scope and prefix information will be collected by the regional server. The default polling interval to update the regional databases is 1 hour. 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 subnet-utilization and lease-history subroles), you can query the DHCP utilization or lease history data by choosing the Utilization or Lease History options from **Operate** menu (see the *"Generating Utilization History Reports" section in Cisco Prime Network Registrar 11.1 DHCP User Guide*, or the *"Running IP Lease Histories" section in Cisco Prime Network Registrar 11.1 DHCP User Guide*).

# Adjusting the Polling Intervals

You can adjust the automatic polling interval for DHCP 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 1 hour)—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 41), no data is collected, even though polling is on by default. DHCP utilization collection at the DHCP server is distinct from polling at the regional cluster, and polling does not automatically trigger collection. DHCP utilization collection must occur before new polling picks up any new data. Because this collection is preset to every 15 minutes, the polling interval should be set higher than this interval (the automatic polling interval is preset to every 1 hour).

*Table 6: DHCP Utilization and Lease History Polling Regional Attributes*

| Attribute Type | DHCP Utilization | Lease History |
|---|---|---|
| Polling interval—How often to poll data | *addrutil-poll-interval* 0 (no polling) to 1 year, preset to 1 hour for the CCM server | *lease-hist-poll-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 | *addrutil-poll-retry* 0 to 4 retries | *lease-hist-poll-retry* 0 to 4 retries |
| Offset—Hour of the day to guarantee polling | *addrutil-poll-offset* 0 to 24h (0h= midnight) | *lease-hist-poll-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 6: DHCP Utilization and Lease History Polling Regional Attributes, on page 41.

**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 Network Registrar 11.1 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.

# 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.

## CLI Command

When connected to a regional cluster, you can use the **scope-template** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

# 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.

### CLI Command

When connected to a regional cluster, you can use the **scope-template** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

# 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 Network Registrar 11.1 DHCP User Guide*. The regional cluster web UI has the added feature of pushing policies to, and pulling them from, the local clusters. It also provides the feature to reclaim policies.

## 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.

### CLI Command

When connected to a regional cluster, you can use the **policy** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

## 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.

### CLI Command

When connected to a regional cluster, you can use the **policy** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

# 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 Network Registrar 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 Network Registrar 11.1 DHCP User Guide*. The regional cluster web UI has the added feature of pushing client-classes to, and pulling them from, the local clusters. It also provides the feature to reclaim client-classes.

# 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.

## CLI Command

When connected to a regional cluster, you can use the **client-class** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

# 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.

## CLI Command

When connected to a regional cluster, you can use the **client-class** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

# 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 Network Registrar 11.1 DHCP User Guide*. The regional web UI has the added feature of pushing VPNs to local clusters and pulling them from local clusters. It also provides feature to reclaim VPNs.

# 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.

## CLI Command

When connected to a regional cluster, you can use the **vpn** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

# 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.

## CLI Command

When connected to a regional cluster, you can use the **vpn** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

# 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 Network Registrar 11.1 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.

## CLI Commands

When connected to a regional cluster, you can use the following commands to pull the address space (and reservations):

- **ccm pullAddressSpace** < **update** | **complete** | **exact** > [**-omitreservations**] [**-report-only** | **-report**]
- **ccm pullIPv6AddressSpace** < **update** | **complete** | **exact** > [**-report-only** | **-report**]

# 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.

# 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 *"DHCPv6 Addresses” section in Cisco Prime Network Registrar 11.1 DHCP User Guide*.

# Monitoring Resource Limit Alarms

Resource limit alarms enable you to monitor Cisco Prime Network Registrar 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.

You can reset the predefined threshold levels for both critical and warning levels for each monitored resource.

Cisco Prime Network Registrar 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 Network Registrar 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 52.

If SNMP traps are enabled for the resource limit alarms, Cisco Prime Network Registrar 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.

Starting from Cisco Prime Network Registrar 11.1, the resource monitoring will monitor the *queued-binding-updates* and trigger the standard resource monitoring notifications if the value is above the configured *queued-binding-updates-warning-level* and *queued-binding-updates-critical-level* (defaults are 10% and 25% of the resource monitoring *lease-count* value; with a minimum value of 1,000 binding updates).

Starting from Cisco Prime Network Registrar 11.1, you can also configure the the warning and critical levels for the number of DNS security events in the Authoritative and Caching DNS servers.

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 7: Resource Limit Alarms***

| | **Regional Cluster** | **Local Cluster** |
|---|---|---|
| **Data Free Space in../Data Partition** | ✓ | ✓ |
| **Shadow Backup Time** | ✓ | ✓ |
| **Memory Defaults** (available in Advanced mode) | ✓ | ✓ |
| **CCM Memory** | ✓ | ✓ |
| **CNR Server Agent Memory** | ✓ | ✓ |
| **DHCP Memory** | x | ✓ |
| **CDNS Memory** | x | ✓ |
| **DNS Memory** | x | ✓ |
| **SNMP Memory** | ✓ | ✓ |

| | | |
|---|---|---|
| **Tomcat Memory** | ✓ | ✓ |
| **TFTP Memory** | x | ✓ |
| **Lease Count** | x | ✓ |
| **Zone Count** | x | ✓ |
| **Resource Records Count** | x | ✓ |
| **Trap Configuration** | ✓ | ✓ |
| **Certificate Expiration** (available in Advanced mode) | ✓ | ✓ |
| **DNS Security Events** (available in Advanced mode) | ✓ | ✓ |
| **Queued Binding Updates** | 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 **CCM** 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* [*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 Network Registrar 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 page. To see a summary of the alarms, in the Cisco Prime Network Registrar web UI, click the **Alarms** icon at the top of the web UI. This opens the Alarms page which displays the resource, type, status, resource utilization, and the current 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 52.

**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 Network Registrar 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** Click the Alarms icon at the top of the web UI to open the Alarms page.

**Step 2** Select the Alarm for which you want to reset the peak value.

**Step 3** Click the **Reset Alarm** button 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** Click the Alarms icon at the top of the web UI to open the Alarms page.

**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**.

# Certificate Management

Cisco Prime Network Registrar uses SSL/TLS certificate in various parts of the product (web UI, Caching DNS, and Authoritative DNS). Cisco Prime Network Registrar allows you to input certificate files and have them stored in the appropriate location based on the Cisco Prime Network Registrar component. It also allows to keep track of the certificate expiration and warns when the certificate is about to expire.

You cannot create SSL/TLS keys or certificates in Cisco Prime Network Registrar. You must create them separately using tools like openssl or keytool. For example:

To create a self-signed certificate (cert.pem) using openssl, use the following command:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

To make the Certificate Authority (CA) requests using keytool, see the *"Installing Your Own Certificate for Web UI Access" section in Cisco Prime Network Registrar 11.1 Installation Guide*.

Once you have the certificate, you can add it to Cisco Prime Network Registrar via web UI, CLI, or REST API. The certificate contents are added to the *certificate-contents* attribute of the object being added. CCM validates the certificate file contents and auto-populates the certificate object attributes based on *certificate-contents*. It creates a certificate object and adds it to the CCM database.

For web UI certificates, CCM also stores the certificate file contents as a file (<cnr.datadir>/conf/cert/cnrcert_*certificate-name*.pem). For Authoritative DNS certificates, the server reads *certificate-contents* and uses them directly. For Caching DNS' TLS and HTTPS certificates, the Caching DNS server generates a certificate file based on *certificate-contents*, and stores it in <cnr.datadir>/cdns/tls/*certificate-name*. This certificate file is overwritten on every reload.

On the local clusters, if there are multiple Authoritative and Caching DNS certificates, the Authoritative and Caching DNS servers only pick up the first one for their appropriate component from the list of objects.

**Note** For web UI certificates, deleting the certificate object, deletes the associated web UI certificate file (<cnr.datadir>/conf/cert/cnrcert_*certificate-name*.pem). For Caching DNS certificates, you must delete the certificate file (<cnr.datadir>/cdns/tls/*certificate-name*) manually.

***Table 8: SSL/TLS Certificates Attributes***

| Attribute | Description |
|---|---|
| Name | The name of the certificate being managed. |
| Description | A description of the certificate being managed. |
| Type | Specifies the Cisco Network Registrar component that uses the certificate. |
| Version | Specifies the SSL version for the certificate. This field is automatically populated from the certificate contents. |
| Serial Number (*serial-number*) | Specifies the serial number of the certificate. This field is automatically populated from the certificate contents. |
| Validity Not Before (*validity-not-before*) | Specifies the date and time marking the start of the certificate validity period. This field is automatically populated from the certificate contents. |
| Validity Not After (*validity-not-after*) | Specifies the date and time marking the end of the certificate validity period. This field is automatically populated from the certificate contents. |
| Issuer | Specifies information about the entity that issued the certificate. This field is automatically populated from the certificate contents. |
| Subject | Specifies information about the entity receiving the certificate. This field is automatically populated from the certificate contents. |
| Public Key Algorithm (*public-key-algorithm*) | Specifies the algorithm and size of the public key. This field is automatically populated from the certificate contents. |
| Signature Algorithm (*signature-algorithm*) | Specifies the algorithm and size of the signature. This field is automatically populated from the certificate contents. |

### DNS TLS and Managed Certificates

When enabling TLS, you have to set various TLS settings on the Authoritative DNS and Caching DNS servers. The certificate attribute is *tls-service-pem*. However, if using managed certificates, the server uses the certificate object and the *tls-service-pem* attribute is ignored. The service configuration steps are as follows:

1. The server checks if TLS is enabled and reads the *tls-service-key* attribute.
2. The server looks for managed certificates for its component type (that is, certificates of type=cdns are for the Caching DNS server).

3. If the server finds managed certificates, it picks the first one and ignores the rest (if any). The TLS configuration log message lists tls-service-pem=*certificate-name* (managed) to denote that the managed certificates are used.
4. The server ignores the *tls-service-pem* attribute and uses the certificate object instead. If managed certificates are not used, the server reads the *tls-service-pem* attribute and the TLS configuration log message lists tls-service-pem=*filename*.

For more information on TLS settings in Authoritative and Caching DNS servers, see the *"Specifying TLS Settings" sections under the "Managing Caching DNS Server" and "Managing Authoritative DNS Server" chapters of Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide*.

# Adding SSL/TLS Certificates

To add SSL/TLS certificates to Cisco Prime Network Registrar, do the following:

### Before you begin

Create the SSL/TLS keys or certificates (cert.pem), or public certificate requests using tools such as openssl or keytool.

## Local Advanced and Regional Advanced Web UI

**Step 1** From the **Design** menu, choose **SSL/TLS Certificates** under the **Security** submenu to open the List/Add SSL/TLS Certificates page.

**Step 2** Click the **Add SSL/TLS Certificates** icon in the SSL/TLS Certificates pane. This opens the Add SSL/TLS Certificates page.

**Step 3** Enter the name of the certificate being managed and select the type of the Cisco Network Registrar component that uses the certificate.

**Step 4** Browse for the certificate file by clicking the **Choose File** button. Select the **cert.pem** file (public key) and click **Open** to add it.

**Step 5** Click **Add SSL/TLS Certificates**.

## CLI Commands

Use **certificate** *name* **create** *type* **file**=*file* [*attribute=value...*] to add SSL/TLS Certificates.

Use **certificate** *name* **delete** to delete SSL/TLS certificates.

Use **certificate** *name* **set** *attribute=value* to modify the certificate attribute values.

**Note** Many of the attributes of the certificate object are based on the contents of the certificate and cannot be changed. Currently you can only change the value of the *description* attribute.

# Pulling and Pushing SSL/TLS Certificates

You can push SSL/TLS certificates to and pull SSL/TLS certificates from local clusters on the List/Add SSL/TLS Certificates page in the regional cluster web UI.

## Pushing SSL/TLS Certificates to Local Clusters

To push SSL/TLS certificates to the local cluster, do the following:

### Regional Advanced Web UI

**Step 1** From the **Design** menu, choose **SSL/TLS Certificates** under the **Security** submenu to view the List/Add SSL/TLS Certificates page in the regional web UI.

**Step 2** Click the **Push All** icon in the SSL/TLS Certificates pane to push all the SSL/TLS certificates listed on the page, or select the SSL/TLS certificate on the SSL/TLS Certificates pane and click the **Push** icon to open the Push SSL/TLS Certificate page.

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

- If you are pushing all the SSL/TLS certificates, you can choose Ensure, Replace, or Exact.
- If you are pushing an SSL/TLS certificate, you can choose Ensure or Replace.

In both cases, Ensure is the default mode.

Choose Replace only if you want to replace the SSL/TLS certificate data at the local cluster. Choose Exact only if you want to create an exact copy of the SSL/TLS certificate data at the local cluster, thereby deleting all SSL/TLS certificate data that is not defined at the regional cluster.

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

**Step 5** On the View Push SSL/TLS Certificate Data Report page, view the push details, then click **OK** to return to the List/Add SSL/TLS Certificates page.

## Pulling SSL/TLS Certificates from the Replica Database

To pull SSL/TLS certificates from the replica database, do the following:

### Regional Advanced Web UI

**Step 1** From the **Design** menu, choose **SSL/TLS Certificates** under the **Security** submenu to open the List/Add SSL/TLS Certificates page.

**Step 2** Click the **Pull Data** icon in the SSL/TLS Certificates pane. This opens the Select Replica SSL/TLS Certificates Data to Pull page.

**Step 3** Click the **Replica** icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see Replicating Local Cluster Data, on page 22.)

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

**Step 5** Leave the default Replace mode enabled, unless you want to preserve any existing SSL/TLS Certificates data at the local cluster by choosing Ensure.

**Step 6** Click the **Pull all SSL/TLS Certificates** button to view the pull details, and then click **Run**.

## CLI Commands

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified.

- **certificate** <*name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**].
- **certificate** <*name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**].
- **certificate** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

# Cisco Prime Network Registrar Use of Certificates

CPNR uses Certificates for various services, most of which are managed through certificate management.

## Web UI

Cisco Prime Network Registrar will generate a self signed certificate as part of the product install for the Cisco Prime Network Registrar Web UI, but the user can also use their own certificate. See the *"Installing Your Own Certificate for Web UI Access" section in Cisco Prime Network Registrar 11.1 Installation Guide*. The certificate can be added to certificate management for monitoring and alarming. Expired or invalid certificates will cause the user to not be able to access the Web UI, but this can be remedied by using the CLI and system commands.

Web UI Certificates are used by all supported versions of Cisco Prime Network Registrar.

## Configuration Management Server

Cisco Prime Network Registrar will generate a self signed certificate as part of the product install for the Cisco Prime Network Registrar Configuration Management Server to be used for communication from the Web UI/CLI to the Cisco Prime Network Registrar Configuration Management Server (ccm), but the user can also use their own certificate. See the *"Installing Your Own Certificate for Web UI Access" section in Cisco Prime Network Registrar 11.1 Installation Guide*.

The initial certificates are generated as part of the install process. After which time the user can update them manually.

The certificate can be added to certificate management for monitoring and alarming. Expired or invalid certificates will cause the user to not be able to access the Web UI, but this can be remedied by using system commands.

Cisco Prime Network Registrar Configuration Management Certificates are used by all supported versions of Cisco Prime Network Registrar.

## Authoritative DNS Server

The Authoritative DNS server uses certificates when providing support for DNS over TLS/HTTPS (DoT/DoH). If enabled, the user will specify Certificates which can be added to Certificate Management or manually entered. See *"Specifying TLS Settings" section in Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide*.

Authoritative DNS TLS Certificates were introduced in Cisco Prime Network Registrar 11.0 and were not used prior to that release.

## Caching DNS Server

The Caching DNS server uses certificates when enabled to provide Caching/Recursive DNS service over TLS/HTTPS (DoT/DoH). If enabled, the user will specify Certificates which can be added to Certificate Management or manually entered. See *"Specifying TLS Settings" section in Cisco Prime Network Registrar Authoritative and Caching DNS User Gudie*.

The Caching DNS Server may also use a certificate bundle that includes certificates that come as part of the operating system.

Caching DNS TLS Certificates were introduced in Cisco Prime Network Registrar 11.0 and were not used prior to that release.

# Certificate Expiration Notification

CCM creates a resource management object based on the certificate's validity dates. It monitors and alerts you of the certificate expiration based on the resource configuration.

The *certificate-expiration-warning-level* attribute specifies the warning level for the certificate's expiration. If the current time exceeds this value, a warning notification is triggered. The default value is 25%. The *certificate-expiration-critical-level* attribute specifies the critical level for the certificate's expiration. If the current time exceeds this value, a critical notification is triggered. The default value is 10%.

To set these thresholds for certificate expiration, do the following:

## Local Advanced and Regional Advanced Web UI

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

**Step 2** Click **CCM** in the Manage Servers pane on the left. The Edit Local CCM Server page appears.

**Step 3** Click the **Configure Resource Limits** tab.

**Step 4** Find the *certificate-expiration-warning-level* and *certificate-expiration-critical-level* attributes under the **Certificate Expiration** section. Set the values for these attributes as per your requirement.

**Step 5** Click **Save** to save the settings.

## CLI Commands

Use **resource set certificate-expiration-warning-level**=*value* to set the warning level for the certificate's expiration.

Use **resource set certificate-expiration-critical-level**=*value* to set the critical level for the certificate's expiration.

# 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 65.

## Related Topics

Administrator Responsibilities and Tasks, on page 59

Create the Administrators, on page 59

Create the Address Infrastructure, on page 60

Create the Zone Infrastructure, on page 61

Create a Host Administrator Role with Constraints, on page 63

Create a Group to Assign to the Host Administrator, on page 64

Test the Host Address Range, on page 65

## 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 59.

## 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 and Confirm Password fields, then click **Add Admin**.
b) Click **Add** in the Groups section of the Edit Administrator page to open the Groups window. Select **ccm-admin-group**, **dns-admin-group**, and **host-admin-group** and click **Select**. The selected groups appear under the Groups section of the Edit Administrator page. 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 63.

# 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 enter Advanced mode.

**Step 3** From the **Design** menu, choose **Subnets** under the **DHCPv4** submenu to open the List/Add Subnets page.

**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.

## 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 **hostadmin**.
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 **hostadmin.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 the **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 9: 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. |
| *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). |

| Value | Matches |
|---|---|
| **[***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 59. 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.

## 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 in to the regional cluster as superuser.

**Step 2** From the **Administration** menu, choose **Administrators** under the **User Access** submenu 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 and Confirm Password fields in the Add Admin dialog box, then click **Add Admin**.

**Step 4** Click **Add** in the Groups section of the Edit Administrator page to open the Groups window. Select **central-cfg-admin-group** (for cluster administration) and **regional-admin-group** (for user administration) and click **Select**. The selected groups appear under the Groups section of the Edit Administrator page.

**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** under the **User Access** submenu 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 and Confirm Password fields in the Add Admin dialog box, then click **Add Admin**.

**Step 4** Click **Add** in the Groups section of the Edit Administrator page to open the Groups window. Select **central-cfg-admin-group** and **regional-addr-admin-group** and click **Select**. The selected groups appear under the Groups section of the Edit Administrator page.

**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 **cfgadmin**.

**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 Name field, then **exampleadmin** in the Admin Password field.
e) Enter in the SCP 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 **View Replica Data** under 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 **Replicate Data**.
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 a Router and Modify an Interface

The example-cfg-admin next takes over at the regional cluster to add a router and modify one of its interfaces to configure the DHCP relay agent. Add the subnets manually.

## Regional Advanced Web UI

**Step 1** As example-cfg-admin, from the **Deploy** menu, choose **Router List** under the **Router Configuration** submenu.

**Step 2** On the List/Add Routers page, click the **Add Router** icon in the Router List pane.

**Step 3** On the Add Router dialog box, add the router based on data from its administrator:

a) Give the router a distinguishing name in the name field. For this example, enter **router-1**.
b) Enter the router description in the description field.
c) Enter the management interface address for the router in the address field.
d) Enter the IPv6 management interface address for the router in the ip6address field.
e) Choose a owner and a region.
f) Click **Add Router**. The router should now appear on the List/Add Routers page.

**Step 4** Confirm that the router is created. Click **Router Tree** to view the hierarchy of router interfaces for router-1 on the View Tree of Routers page.

**Step 5** Configure a DHCP relay agent for the router:

a) Create a new interface for the router.
b) Click the interface names on the View Tree of Routers page to open the Edit Router Interface page. (Alternatively, from the List/Add Routers page, click the **Interfaces** icon associated with the router, then click the interface name on the List Router Interfaces for Router page.)
c) On the Edit Router Interface page, enter the IP address of the DHCP server in the ip-helper field.
d) Click **Save** at the bottom of the page.

**Step 6** Confirm with the router administrator that the DHCP relay agent was successfully added.

# 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 Zone dialog box, enter:

a) **Name**—**chicago.example.com**.
b) **Nameserver FQDN**—**ns1**.
c) **Contact E-mail**—**hostadmin**.
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 primary server in the Primary Servers list (that is, primary servers' list on the secondaries).

**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 Advanced 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. You should see the subnets created by adding the router (in the Add a Router and Modify an Interface, on page 67).

**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) Click **Add DHCP Policy**.
c) On the Edit DHCP Policy page, under the DHCPv4 Options section, choose **dhcp-lease-time [51] (unsigned time)** from the Name drop-down list, and then enter **2w** (two weeks) for the lease period in the Value field.
d) Click **Add Option**.
e) Click **Save**.

**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.

# 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.

## CLI Commands

Use **failover-pair** *name* **create** *main-cluster*/*address backup-cluster*/*address* [*attribute=value ...*] to create a failover pair. For example:

```
nrcmd> failover-pair example-fo-pair create Example-cluster Boston-cluster
```

Use **failover-pair** *name* **sync** {**update** | **complete** | **exact**} [{**main-to-backup** | **backup-to-main**}] [**-report-only** | **-report**] to synchronize the failover pair configuration. For example:

```
nrcmd> failover-pair example-fo-pair sync exact main-to-backup -report
```