



Configuring Local and Regional Administrators

This chapter explains how to set up network administrators at the local and regional clusters through Cisco CNS Network Registrar's Web-based user interface (Web UI) and command line interface (CLI). The chapter also includes local and regional cluster tutorials for many of the administration features.

Administrators, Roles, and Groups

The types of functions that network administrators can perform in Network Registrar are based on the roles that they are assigned. The Web UI administrators can define these roles, which lends granularity to the network administration functions. Network Registrar differentiates between base roles and constrained roles:

- Base—General, unconstrained roles for administrative functions
- Constrained—Roles (derived from base roles) that are limited by a set of constraints

How Administrators Relate to Groups and Roles

There are three administrator concepts in Network Registrar—administrators, groups, and roles:

- Administrator—An account that logs in and that, through its association with one or more groups or roles, can perform certain functions. At the local cluster, these functions include host, zone, address space, and DHCP administration. At the regional cluster, these functions include regional administration, central configuration administration, and regional address space administration.
- Group—A grouping of roles that takes the place of associating a role directly with an administrator.
- Role—Defines the functions that the administrator can perform and possible additional constraints. An administrator or group must be assigned at least one role to be usable.

Base and Constrained Roles

You can limit administrator roles by applying constraints on a base role. The base roles on which you apply constrained roles for the local and regional clusters are described in [Table 4-1](#) and [Table 4-2](#), respectively. Creating, and associating administrators with, roles is available in the Web UI only.

For example, a base role might be host-admin, and the constrained role based on it (that limits operation to a specific subnet) might be named 192.168.50.0-host-admin. The administrator assigned this role then logs in with these constraints in effect.

Roles can be further limited to read-only mode. An administrator can be allowed to read any of the data for that role, but not modify it. When a read-only constraint is applied to a role, it supersedes all other constraints, making the role entirely read-only.

Table 4-1 Local Cluster Administrator Base Roles

Base Role	Function
ccm-admin	Global administrator—Administers the Central Configuration Management (CCM) database. A constrained role derived from this base role can have the following subroles (they all apply by default): <i>authentication</i> —Can create and modify administrators and groups <i>authorization</i> —Can create and modify roles <i>owner-region</i> —Can create and modify owners and regions <i>server-management</i> —Can manage the servers of the cluster <i>database</i> —Can view the CCM and MCD database change logs and tasks
host-admin	Host administrator—Usually focused only on the Address (A) resource records in a zone and managing host IP addresses, rather than the full zone data. This role can be constrained by zone and IP address range, and by host name in a set of zones.
zone-admin	Zone administrator—Usually focused on managing zone data such as Start of Authority (SOA) resource record and nameserver attributes, and other resource records, rather than hosts in the zone. This role can be constrained by zones and their owners.
dhcp-admin	DHCP administrator—Manages dynamic host configuration, such as scopes, policies, and failover configurations. This role cannot be further constrained.
addrblock-admin	Address block administrator—Manages address space at a higher level than specific subnets or static address allocations, using hierarchical representation of address blocks to organize the address space. This role cannot be further constrained.

Table 4-2 Regional Cluster Administrator Base Roles and Subroles

Base Role	Function and Subroles
regional-admin	Regional administration—Creates regional cluster administrators, groups, role instances, manages licenses, views change sets and tasks. A constrained role derived from this base role can have the following subroles (they all apply by default): <i>authentication</i> —Can create and modify administrators and groups <i>authorization</i> —Can create and modify roles <i>owner-region</i> —Can create and modify owners and regions <i>server-management</i> —Can manage servers of the regional cluster <i>database</i> —Can view the CCM database change logs and tasks, and perform trimming of the subnet utilization and lease history databases

Table 4-2 Regional Cluster Administrator Base Roles and Subroles (continued)

Base Role	Function and Subroles
central-cfg-admin	<p>Central configuration administration—Manages clusters, routers and interfaces (physical and virtual), VPNs, policies, client-classes, and scope templates, including pulling them from or pushing them to the local cluster. A constrained role derived from this base role can have the following subroles (they all apply by default):</p> <p><i>dhcp-management</i>—Can push DHCP objects and manage failover server pairs</p> <p><i>ric-management</i>—Can manage router interfaces (requires a router license)</p> <p><i>dns-management</i>—Can manage DNS zone distributions</p>
regional-addr-admin	<p>Regional address space role—Manages and delegates address blocks and subnets, manages address destinations, and collects subnet utilization and lease history data. A constrained role derived from this base role can have the following subroles (they all apply by default):</p> <p><i>subnet-utilization</i>—Can view subnet utilization reports</p> <p><i>lease-history</i>—Can view subnet lease history reports</p> <p><i>ric-management</i>—Can push and de-allocate subnets to router interfaces (requires a router license)</p> <p><i>dhcp-management</i>—Can add and remove subnets from failover server pairs</p>

Subroles

The local and regional clusters provide further subrole constraints for certain roles. For example, the Central Configuration Management (CCM) or regional administrator might be constrained further by the owner-region subrole to manage owners and regions only. By default, all the possible subroles apply when you create a constrained role. These subroles were previously described in [Table 4-1](#) and [Table 4-2](#).

Groups

An administrator group is a grouping of roles that you can assign to administrators. This provides some flexibility and convenience, and is especially useful when adding new users. Groups assignment is available only in the Web UI.

The local cluster Web UI is predefined with two groups (see [Table 4-3](#)). You can create additional groups in the local and regional cluster Web UIs.

Table 4-3 Predefined Local Cluster Administrator Groups

Group	Description
address-mgt-group	Combined DHCP, address block, and Central Configuration Management (CCM) administrator.
dns-mgt-group	Combined host, zone, and CCM administrator.

Adding Administrators

The Web UIs have only one predefined administrator, the admin account. This superuser can exercise all the functions of the Web UI and usually adds the other key administrators (some of whom can be set up with user administration functions themselves). Adding an administrator requires:

- Adding an administrator name.
- Adding a password.
- Determining if the administrator should have full or limited access to the CLI.
- Determining if the administrator should have superuser privileges—Usually assigned on an extremely limited basis.
- Determining if the administrator should belong to a group.
- Associating the administrator with a role (and possible subrole).

In the local and regional Web UIs, click **Administration** on the Primary Navigation bar, then **Administrators** on the Secondary Navigation bar. This opens the List/Add Administrators page (see [Figure 4-1 on page 4-6](#)), where you can create administrators.

In the CLI, use the **admin name create** command (see the **admin** command in the *Network Registrar CLI Reference* for syntax and attribute descriptions). You must have full **nrcmd** or superuser privileges to use this command.

Adding Passwords Without Exposing Them

In the Web UI, adding a password never exposes it on the page. Logging in always hides the password.

In the CLI, prevent exposing the password by creating an administrator, omitting the password, then using the **admin name enterPassword** command, where the prompt displays the password as asterisks.

Changing Administrator Passwords

If you have CCM administrator or superuser privileges, you can change any administrator's password. You should do this for security reasons. (If you lack full administrator privileges and try to change a password, an error message appears.)

In the Web UI, the CCM administrator and superuser can change administrator passwords at any time.

In the CLI, change an existing password by using the **admin name set password** command. Note, however, that this takes a plain text value so that if you do not want to expose it, see the [“Adding Passwords Without Exposing Them”](#) section.

Listing and Deleting Administrators

If you have full administrator privileges, you can list the administrators and delete specific ones, if necessary. (If you lack full administrator privileges, an error message appears.)

In the Web UI, the superuser, CCM administrator, and regional administrator can list and delete administrators at any time.

In the CLI, list the administrators by using the **admin list** or **admin listnames** command, and delete an administrator by using the **admin name delete** command.

Licensing

There is a single license required for the local cluster. The regional cluster can require as many as three:

- central-cluster—Regional management of multiple local clusters
- addrspace—Regional management of subnets and address blocks
- router—Regional management of routers through the Router Interface Configuration (RIC) server

The local and regional clusters also provide a node-count license so that you can manage a certain number of address nodes.

Centrally Configuring Administrators

Pulling local administrators, groups, roles, role instances, owners, and regions to the central cluster. Also, pushing these objects to the local clusters.

TBD

Local Cluster Management Tutorial

This tutorial describes a basic scenario on two local clusters of the Example Company that are in Boston and Chicago. Administrators at each cluster are responsible for users, zone data, DHCP data, address space data, and the servers in general. The task is to set up three zones (example.com, boston.example.com, and chicago.example.com), hosts in the zones, and a subnet. The two local clusters must also create a special administrator account so that the regional cluster in San Jose can perform the central configuration described in the [“Regional Cluster Management Tutorial”](#) section on page 4-15.

Administrator Responsibilities and Tasks

The local cluster administrators have the following responsibilities and tasks:

- example-cluster-admin (created by the superuser at the Boston and Chicago clusters):
 - At the Boston cluster, sets up the other local administrators and their access constraints—example-host-admin, example-zone-admin, and example-central-admin. (At the Chicago cluster, the example-cluster-admin handles all of these functions).
 - Creates the basic network infrastructure for the local clusters.
 - Creates the example-host-role for assignment to the example-host-admin at the Boston cluster
 - Creates the example.com and chicago.example.com zones at the Chicago cluster.
- example-zone-admin (Boston cluster only):
 - Assigns the constrained example-host-role to the example-host-admin in Boston
 - Creates the example.com and boston.example.com zones, and maintains the latter zone.
- example-host-admin (Boston cluster only):
 - Assures that hosts can access the network at the Boston cluster
 - Maintains local host lists and IP address assignments
- The example-central-admin account is created purely for read-only access from the regional cluster.

Create the Administrators

For this example, the superuser in Boston creates the local cluster, zone, host, address, and DHCP administrators; and the superuser in Chicago creates the cluster administrator, with the responsibilities described in the “[Administrator Responsibilities and Tasks](#)” section on page 4-5. The superusers also create the example-central-admin account for access from the regional cluster.

-
- Step 1** At the Boston cluster, log in as superuser (usually **admin**).
- Step 2** Click **Administration** on the Primary Navigation bar, then **Administrators** on the Secondary Navigation bar.
- Step 3** Add the Boston cluster administrator—On the List/Add Administrators page, enter **example-cluster-admin** in the Name field and **exampleadmin** in the Password field.
- Step 4** Make the example-cluster-admin a superuser with full CLI access (superuser authorization is required to synchronize the local with the regional cluster, which is part of this administrator’s role):
- Click a check mark in the Superuser box.
 - Select **full** in the NRCMD drop-down list.
 - Click **Add Administrator** (see [Figure 4-1](#)).

Figure 4-1 Adding a Local Cluster Administrator

Name*	Password	Superuser	NRCMD	Groups	Roles
		<input type="checkbox"/>		address-mgt-group dns-mgt-group	addrblock-admin addrblock-admin-readonly ccm-admin

Add Administrator

Name	Password	Superuser	NRCMD	Groups	Roles
admin	*****	<input checked="" type="checkbox"/>	full		

- Step 5** Add the Boston zone administrator:
- Enter **example-zone-admin** in the Name field, then **examplezone** in the Password field.
 - Click **dns-mgt-group** in the Groups drop-down list—Because example-zone-admin should manage the DNS server, the dns-mgt-group is a perfect group in which to include the administrator. This group automatically has the ccm-admin, host-admin, and zone-admin unconstrained roles assigned to it. (Only unconstrained zone administrators can view and edit DNS server properties, and start, stop, and reload the DNS server.)
 - Click **Add Administrator**.
- Step 6** Add the Boston host administrator:
- Enter **example-host-admin** in the Name field, then **examplehost** in the Password field.
 - Do not select any more items—The example-zone-admin will define a constrained role for the example-host-admin.
 - Click **Add Administrator**.
- Step 7** Add a read-only central configuration administrator account for the benefit of regional access:
- Enter **example-central-admin** in the Name field, then **centraladmin** in the Password field.

- b. Multiselect all the roles ending with “-readonly” in the Roles field.
- c. Click **Add Administrator**.

The names of the four new administrators should appear on the List/Add Administrators page of the Boston cluster and should have the following attributes:

- example-central-admin—Read-only roles in the Roles column
- example-cluster-admin—Superuser flag checked and “full” in the NRCMD column
- example-host-admin—No groups or roles
- example-zone-admin—The dns-mgt-group in the Groups column

- Step 8** Go to the Chicago cluster and create the same **example-cluster-admin** and **example-central-admin**, using the same passwords and settings as in the previous steps. (You do not need to create the other two administrators at the Chicago cluster.)
-

Create the Address Infrastructure

A condition 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 scenario assumes that you are starting with a clean slate.

The example-cluster-admin in Boston next creates the allowable address ranges for the hosts in the boston.example.com zone that will be assigned static IP addresses. The example-cluster-admin in Chicago must do the same for the chicago.example.com zone. Both create a range of fixed IP addresses to include the managed hosts:

- boston.example.com—192.168.50.0/24 subnet
- chicago.example.com—192.168.60.0/24 subnet

The host address ranges at both sites should be 101 through 200 in each subnet.

- Step 1** At the Boston cluster, log out as superuser, then log in as **example-cluster-admin** with password **exampleadmin**.
- Step 2** Click the **Address Space** link, then click **Subnets** on the Secondary Navigation bar.
- Step 3** On the List/Add Subnets page, enter the subnet address:
- a. In the Address/Mask field, enter **192.168.50.0**.
 - b. Select **24** in the mask drop-down list.
 - c. Leave the Owner, Region, and Address Type fields as **[none]** (see [Figure 4-2](#)).

Figure 4-2 Adding a Subnet to the Local Cluster

Address/Mask*	Owner	Region	Address Type	Description
192.168.50.0 / 24	[none]	[none]	[none]	

Add Subnet

Address/Mask	Owner	Region	Address Type	Description
[Address/Mask]				

10 Change Page Size

d. Click **Add Subnet** to return to the List/Add Subnets page.

Step 4 Click the **192.168.50.0/24** link to open the Edit Subnet page.

Step 5 Enter the address range:

- a. Enter **101** in the Start field.
- b. Enter **200** in the End field.
- c. Click **Add IP Range** (see Figure 4-3).

Figure 4-3 Adding an Address Range to a Subnet

Parent Block	Owner	Region	Address Type	Description
192.168.50.0/24	[none]	[none]	[none]	

Modify Subnet Cancel

Start	End	Type
		static

Add IP Range

192.168.50.101	192.168.50.200	static
----------------	----------------	--------

Step 6 Click **Modify Subnet**.

Step 7 Click **Address Space** on the Secondary Navigation bar 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 (🔄).

Step 8 At the Chicago cluster, as in the previous steps:

- a. Log out as superuser, then log in as **example-cluster-admin** with password **exampleadmin**.
- b. Go to the List/Add Subnets page, enter **192.168.60.0/24** as the subnet, then click **Add Subnet**.
- c. Go to the Edit Subnet page, enter **101** through **200** as the address range, then click **Add Range**.
- d. Click **Modify Subnet**.
- e. Confirm your settings as in Step 7.

Create the Zone Infrastructure

For this scenario, example-cluster-admin in Boston and Chicago must create the Example Company zones locally, including the example.com zone and its individual subzones. The example-cluster-admin in Boston also adds some initial host records to the boston.example.com zone.

Create the Zones

First, create the example.com, boston.example.com, and chicago.example.com zones.

- Step 1** At the Boston cluster, log out as example-cluster admin, then log in as **example-zone-admin** with password **examplezone**. Note that the Address Space and DHCP menu items do not appear, because this administrator is limited to CCM, zone, and host administrator.
- Step 2** Click the **Zone** link to open the List/Add Zones page.
- Step 3** Create the zone name:
- Enter **example.com** in the Name field.
 - Leave the Owner and Template as **[none]** (see [Figure 4-4](#)).

Figure 4-4 Creating a Zone

Name*	Owner	Template
example.com	[none]	[none]

Add Zone

Name	Owner	Configuration RRs	Active Server RRs
[Name]	[Name]		10

- Click **Add Zone**.
- Step 4** On the Add Zone page, enter the minimum data to create the zone, which is the Start of Authority (SOA) serial number, primary DNS server name, hostmaster's contact E-mail address, and zone's authoritative nameserver. In each of these fields:
- Serial Number—Enter **1**
 - Nameserver—Enter **ns1**
 - Contact E-Mail—Enter **hostmaster**
 - In the second field of Nameservers—Enter **ns1**, then click **Add Nameserver** (see [Figure 4-5](#)).

Figure 4-5 Adding Zone Information

Home | Administration | **Zone** | Host

Forward Zones | Forward Zones Tree | Reverse Zones | Reverse Zones Tree | Secondary Zones | Zone Templates | Zone Distribution | DNS Server

Add Zone

Attribute	Value
Name*	example.com.
Owner	[none] ▼
Distribution	Default ▼
Zone Default TTL	24h
SOA Attributes	
Serial Number*	1
SOA TTL	
Nameserver*	ns1.example.com.
Contact E-Mail*	hostmaster.example.com.
Secondary Refresh	3h
Secondary Retry	60m
Secondary Expire	1w
Minimum TTL	10m
Nameservers	
NS TTL	
	ns1.example.com.
	<input type="text"/> <input type="button" value="Add Nameserver"/>

84331

- Step 5** Click **Add Zone** at the bottom of the page to return to the List/Add Zones page.
- Step 6** Create the **boston.example.com** zone in the same way, using the same values as in the previous steps. The page should now list example.com and boston.example.com (see Figure 4-6).

Figure 4-6 Viewing the Zones

Home | Administration | **Zone** | Host

Forward Zones | Forward Zones Tree | Reverse Zones | Reverse Zones Tree | Secondary Zones | Zone Templates | Zone Distribution | DNS Server

List/Add Zones

Name*	Owner	Template		
<input type="text"/>	[none] ▼	[none] ▼		
<input type="button" value="Add Zone"/>				
Name	Owner	Configuration RRs	Active	Server RRs
boston.example.com.	[none]	🔗		🔗
example.com.	[none]	🔗		🔗

🔍 [Name] 10 Change Page Size

84332

- Step 7** Click **Forward Zones Tree** on the Secondary Navigation bar to show the hierarchy of the zones on the View Forward Zones Tree page.
- Step 8** At the Chicago cluster, the example-cluster-admin creates the zones:
- Click the **Zone** link to open the List/Add Zones page.
 - Enter the **example.com** and **chicago.example.com** zones using the sequence in the previous steps, with the same values.

The List/Add Zones page should now list example.com and chicago.example.com, and the View Forward Zones Tree page should show the proper relationship of the two zones.

Create the Initial Hosts

As a confirmation that hosts can be created at the Boston cluster, the example-zone-admin in Boston creates two hosts in the example.com zone.

- Step 1** At the Boston cluster, log out as example-cluster-admin, log in as **example-zone-admin**, then click **Host** on the Primary Navigation bar to open the List Zones page.
- Step 2** Click **example.com** in the list of zones. This opens the List/Add Hosts for Zone page.
- Step 3** Add the first host:
- Enter **userhost1** in the Name field.
 - Enter **192.168.50.101** in the IP Address field.
 - Leave the check mark in the Create PTR Records? box.
 - Click **Add Host**.
- Step 4** Add the second host:
- Enter **userhost2** in the Name field.
 - Enter **192.168.50.102** in the IP Address field.
 - Leave the check mark in the Create PTR Records? box.
 - Click **Add Host**.

The two hosts should now appear on the List/Add Hosts for Zone page (see [Figure 4-7](#)).

Figure 4-7 Adding a Host and Address to a Zone

Home | Administration | Zone | **Host**
Zones | Hosts

List/Add Hosts for Zone *example.com*.

Name	IP Address	Create PTR Records?	Valid IP Ranges
<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	[unconstrained]
<input type="button" value="Add Host"/>			
Name	IP Address(es)	Create PTR Records?	
userhost1	192.168.50.101	<input checked="" type="checkbox"/>	
userhost2	192.168.50.102	<input checked="" type="checkbox"/>	
<input type="button" value="Return to Zone List"/>			
<input type="text" value=""/>		<input type="text" value="10"/>	<input type="button" value="Change Page Size"/>

Create and Assign the Constrained Host Role

The example-cluster-admin at the Boston cluster next creates the example-host-role so that the example-zone-admin can assign it to the example-host-admin. This role will be constrained to managing a certain address range in the boston.example.com zone.

- Step 1** At the Boston cluster, log out as example-zone-admin, then log in as **example-cluster-admin**.
- Step 2** Click **Administration** on the Primary Navigation bar, then **Roles** on the Secondary Navigation bar.
- Step 3** Add the role:
- On the List/Add Administrator Roles page, enter **example-host-role** in the Name field.
 - Click **host-admin** in the Base Role drop-down list (see [Figure 4-8](#)).

Figure 4-8 Creating a Constrained Administrator Role

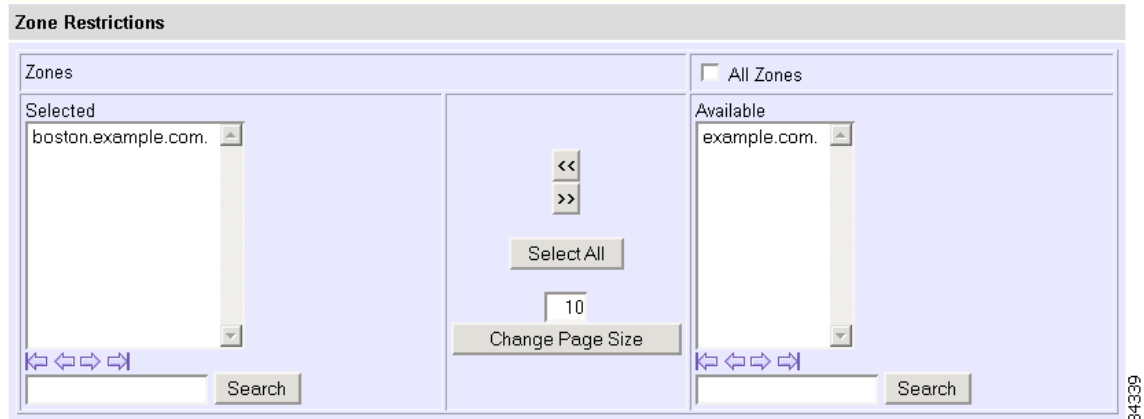
Name*	Base Role
example-host-role	host-admin

Add Role

Name	Base Role
addrblock-admin	addrblock-admin
addrblock-admin-readonly	addrblock-admin
ccm-admin	ccm-admin
ccm-admin-readonly	ccm-admin
dhcp-admin	dhcp-admin
dhcp-admin-readonly	dhcp-admin
host-admin	host-admin
host-admin-readonly	host-admin
zone-admin	zone-admin
zone-admin-readonly	zone-admin

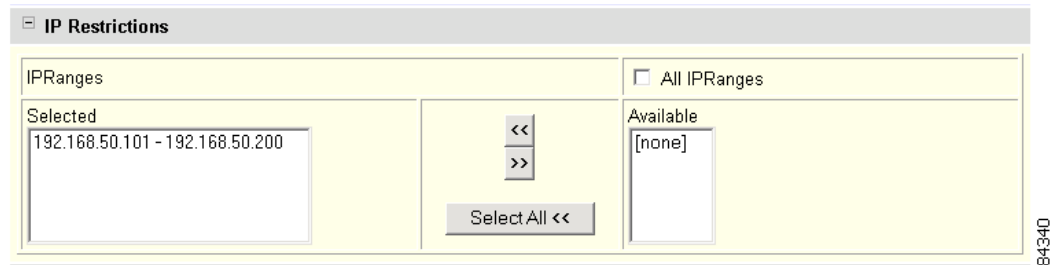
- Click **Add Role** to open the Add Host Administrator Role page.
- Step 4** Constrain the role:
- Under Zone Restrictions, select **boston.example.com** in the Available list.
 - Click << to move it to the Selected list (see [Figure 4-9](#) for this section of the page).

Figure 4-9 Setting Zone Restrictions for a Role



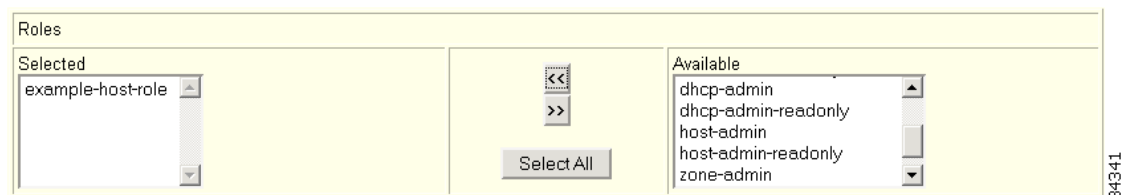
- c. Under IP Restrictions, select **192.168.50.101 – 192.168.50.200** in the Available list.
- d. Click << to move this range to the Selected list (see Figure 4-10 for this section of the page).

Figure 4-10 Setting IP Address Restrictions for a Role



- Step 5** Click **Add Role** at the bottom of the page. The role appears on the List/Add Administrator Roles page.
- Step 6** Log out as example-cluster-admin, then log in as **example-zone-admin**.
- Step 7** Assign the constrained role to the example-host-admin:
 - a. Click **Administration** on the Primary Navigation bar, then **Administrators** on the Secondary Navigation bar.
 - b. On the List/Add Administrators page, click **example-host-admin** to edit the administrator.
 - c. On the Edit Administrator page, in the Roles section, click **example-host-role** in the Available list.
 - d. Click << to move it to the Selected list (see Figure 4-11 for this section of the page).

Figure 4-11 Assigning a Role to an Administrator



- e. Click **Modify Administrator** at the bottom of the page. The example-host-admin should now show example-host-role in the Roles 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.

-
- Step 1** At the Boston cluster, log out as example-zone-admin, then log in as **example-host-admin** with password **examplehost**. Note that only the Host selection appears, because this administrator is limited to host administration.
 - Step 2** Click the **Host** link. This goes directly to the List/Add Hosts for Zone page for boston.example.com, because this administrator's view is limited to a single zone.
 - Step 3** Try to enter an out-of-range address:
 - a. Enter **userhost3** in the Name field.
 - b. Look in the Valid IP Ranges field for the valid range, then deliberately enter an out-of-range address (**192.168.50.5**) in the IP Address field.
 - c. Click **Add Host**. You should get an error message and the fields are cleared.
 - Step 4** Enter a valid address:
 - a. Enter **userhost3** again.
 - b. Enter **192.168.50.103** in the IP Address field.
 - c. Click **Add Host**. The host should now appear with that address in the list.
-

Create a DHCP Policy

The example-cluster-admin at the Boston cluster next creates a DHCP policy that will later be pulled from the regional cluster in San Jose so that it can be distributed to all the clusters.

-
- Step 1** At the Boston cluster, log out as example-host-admin, then log in as **example-cluster-admin**.
 - Step 2** Click **DHCP** on the Primary Navigation bar, then **Policies** on the Secondary Navigation bar. This opens the List DHCP Policies page, where the default and system_default_policy policies are already listed.
 - Step 3** Click **Add Policy** to open the Add DHCP Policy page.
 - Step 4** Enter **examplepolicy** in the Name field. Leave the Offer Timeout and Grace Period values as they are.
 - Step 5** Assign the policy a 24-hour lease period:
 - a. Under Options, select the **[51] dhcp-lease-time** option from the drop-down list.
 - b. Enter **24h** in the Value field.
 - c. Click **Add Option** (see [Figure 4-12](#) for the relevant section of the page).

Figure 4-12 Adding a DHCP Policy

Attribute	Value
Name*	examplepolicy
Offer timeout	2m
Grace period	5m

Options	Number	Value

Add Option

[51]	dhcp-lease-time	(unsigned time)	24h
------	-----------------	-----------------	-----

Step 6 Click **Add Policy** at the bottom of the page. The policy should appear on the List DHCP Policies page.

Regional Cluster Management Tutorial

This tutorial is an extension of the scenario described in the [“Local Cluster Management Tutorial” section on page 4-5](#). In the regional cluster tutorial, San Jose has three administrators—a regional, central configuration, and address space administrator. Their goal is to coordinate activities with the local clusters in Boston and Chicago so as to create a DNS zone distribution, router configuration, and DHCP failover configuration 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 San Jose
- One DHCP relay agent machine in Boston

Administrator Responsibilities and Tasks

The regional administrators have the following responsibilities and tasks:

- superuser (as regional administrator):
 - Adds the licenses required for the administrative functions.
 - Creates the example-central-admin and example-address-admin accounts at the regional cluster.
- example-central-admin (regional central configuration administrator):
 - Adds a router and modifies a router interface. (This is done first to prevent overlapping subnets and router synchronization problems later on.)
 - Adds the existing local server clusters for Boston and Chicago to the regional cluster.
 - Pulls zone data from the local clusters and creates a zone distribution. (The zones were previously set up in the [“Create the Zone Infrastructure” section on page 4-9](#).)
 - Pulls a DHCP policy from the Boston cluster. (The policy was previously set up in the [“Create a DHCP Policy” section on page 4-14](#).)

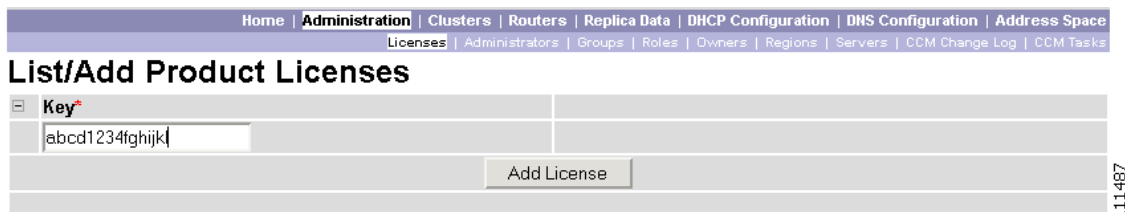
- Creates another regional DHCP policy and pushes it to the local clusters.
- Adds a DHCP scope template for server failover purposes.
- Creates and synchronizes the DHCP failover server pair between the two local clusters.
- Checks the failover configuration at the local clusters. (Single sign-on to the local clusters was previously set up in the “[Create the Administrators](#)” section on page 4-6.)
- example-address-admin (regional address space administrator)—Creates address blocks, subnets, address types, and address destinations, and delegates address space to the local clusters.

Add the Licenses

The superuser first adds the licenses for the required address space and router management functions.

-
- Step 1** Enter the central-cluster license key as part of the Network Registrar regional cluster installation.
- Step 2** Open the Web UI and log in as the default superuser (such as **admin**).
- Step 3** Click **Administration** on the Primary Navigation bar, then **Licenses** on the Secondary Navigation bar.
- Step 4** Register the address space license on the List/Add Product Licenses page:
- a. Enter the key for the address space license as given with the product (see [Figure 4-13](#)).

Figure 4-13 Adding a Product License



- b. Click **Add License**.
- Step 5** Register the router license:
- a. Enter the key for the router license as given with the product.
 - b. Click **Add License**. The central-cluster, address space, and router licenses should appear on the page.
-

Create the Regional Administrators

The superuser next creates the regional, central configuration, and address administrators.

-
- Step 1** As superuser, click **Administrators** on the Secondary Navigation bar.
- Step 2** On the List/Add Administrators page, create the central configuration administrator:
- a. Enter **example-central-admin** in the Name field.
 - b. Enter **centraladmin** in the Password field.

- c. Click **central-cfg-admin** role in the Roles drop-down list (see [Figure 4-14](#)).

Figure 4-14 Adding a Regional Administrator

Name*	Password	Superuser	Groups	Roles
example-central-e	*****	<input type="checkbox"/>	[none]	central-cfg-admin central-cfg-admin-readonly regional-addr-admin
Add Administrator				
Name	Password	Superuser	Groups	Roles
admin	*****	<input checked="" type="checkbox"/>		

- d. Click **Add Administrator**.

Step 3 Create the regional address administrator:

- Enter **example-address-admin** in the Name field.
- Enter **addressadmin** in the Password field.
- Click the **regional-addr-admin** role in the Roles drop-down list.
- Click **Add Administrator**. Both administrators should appear on the page in addition to the admin administrator. The example-address-admin should have the regional-addr-admin role, and the example-central-admin should have the central-cfg-admin role.

Add a Router and Modify an Interface

The example-central-admin next adds a router and modifies one of its interfaces to add a DHCP relay agent. The administrator can do this because it is part of the role definition, and because the address space and router licenses are entered. Adding the router pulls in subnets. It is done at this point to prevent overlapping subnets and router synchronization errors, once other address space is added later on.

- Step 1** Log out as superuser, then log in as **example-central-admin** with password **centraladmin**. (Notice that Administration no longer appears on the Primary Navigation bar.)
- Step 2** Click **Routers** on the Primary Navigation bar, then **Router List** on the Secondary Navigation bar, to open the List Routers page (see [Figure 5-5 on page 5-8](#)).
- Step 3** Click **Add Router** to open the Add Router page (see [Figure 4-15](#)).

Figure 4-15 Adding a Router

Home | Clusters | **Routers** | Replica Data | DHCP Configuration | DNS Configuration
Router Tree | Router List

Add Router

Attribute	Value
name*	<input type="text"/>
Router Type*	[none] ▾

Attribute	Value	Data Type	Default
address*	<input type="text"/>	IP address	
username	<input type="text"/>	string	
password	<input type="text"/>	password	
enable	<input type="text"/>	password	
description	<input type="text"/>	string	
owner	[none] ▾	owner	
region	[none] ▾	region	

± Reserved

Add Router Cancel

111477

Step 4 Add the router:

- a. Give the router a distinguishing name in the name field. For this example, enter **router-1**.
- b. Because this router is a Cisco uBR7200 router, click **Ubr72xx** in the Router Type drop-down list.
- c. Enter the router's IP address in the address field.
- a. Enter the router administrator's username in the username field.
- b. Enter the router administrator's password in the password field.
- c. Enter the router administrator's enable password in the enable field.
- d. Click **Add Router**. Adding the router synchronizes it with the Web UI, and it should now appear on the List Routers page.

Step 5 Confirm that the router is created—Click **Router Tree** on the Secondary Navigation bar to view the hierarchy of router interfaces for router-1 on the View Tree of Routers page.**Step 6** Configure a DHCP relay agent for the router:

- a. Click one of the interface names on the View Tree of Routers page to open the Edit Router Interface page. (You can also get there from the List Routers page by clicking the Interfaces icon (🔌) associated with router, then clicking the interface name on the List Router Interfaces for Router page.)
- b. Enter the IP address of the DHCP server in the ip-helper field (see Figure 4-16).

Figure 4-16 Editing a Router Interface

Attribute	Value	Data Type	Default	Unset?
name	Cable3/0	string		
description		string		<input type="checkbox"/>
primary-subnet		IP address/mask		<input type="checkbox"/>
secondary-subnets		IP address/mask list		<input type="checkbox"/>
ip-helper	192.168.132.55	IP address list		<input type="checkbox"/>
cable-helper		IP address list		<input type="checkbox"/>

c. Click **Modify Router Interface** at the bottom of the page.

Step 7 Confirm with the router administrator that the DHCP relay agent was successfully added.

Create a Subnet

The example-address-admin next logs in to create a subnet at the regional cluster. This subnet will later serve to create the DHCP failover server configuration between the two local clusters.

- Step 1** Log out as example-central-admin, then log in as **example-address-admin** with password **addressadmin**. (Notice that only Home and Address Space are available on the Primary Navigation bar.)
- Step 2** Click **Address Space** on the Primary Navigation bar, then **Subnets** on the Secondary Navigation bar, to open the List/Add Subnets page. You should see the subnets created by adding the router.
- Step 3** Create an additional subnet:
- Enter **192.168.50** (the abbreviated form) as the subnet's network address in the Address/Mask field.
 - Leave the **24** (255.255.255.0) selected as the network mask (see Figure 4-17).

Figure 4-17 Adding a Regional Subnet

Address/Mask	Owner	Region	Address Type	Description
192.168.50 / 24	[none]	[none]	[none]	

Add Subnet

c. Click **Add Subnet**.

Step 4 Click **Address Space** on the Secondary Navigation bar to confirm the subnet you created.

Add the Local Clusters



The example-central-admin next logs in to add the local clusters to the regional cluster.

- Step 1** Log out as example-address-admin, then log in as **example-central-admin** with password **centraladmin**.
- Step 2** Click **Clusters** on the Primary Navigation bar, then **Cluster List** on the Secondary Navigation bar to open the List Server Clusters page.
- Step 3** Click **Add Cluster** to open the Add Server Cluster page.
- Step 4** Create the Boston cluster based on data provided by the administrator at the cluster:
 - a. Enter **Boston-cluster** in the name field.
 - b. Enter the IP address of the Web UI machine in Boston in the ipaddr field.
 - c. Enter **example-cluster-admin** in the admin field. (A superuser account is required.)
 - d. Enter **exampleadmin** in the password field.
 - e. Enter the SCP port number to access the cluster machine in the scp-port field (usually **1234**).
 - f. Enter the HTTP port number to access the cluster machine in the http-port field (usually **8080**) (see [Figure 4-18](#)).

Figure 4-18 Adding a Server Cluster

Attribute	Value	Data Type	Default
name*	Boston-cluster	string	
fqdn		DNS name	
ipaddr*	192.168.40.123	IP address	
admin	example-cluster-admin	string	
password	password	password	
scp-port	1234	unsigned 32-bit	
Webserver Settings			
Attribute	Value	Data Type	Default
http-port	8080	unsigned 32-bit	
https-port		unsigned 32-bit	

- g. Click **Add Cluster** at the bottom of the page.

- 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 Server Clusters page.
- Step 6** Confirm the cluster connectivity—Click **Cluster Tree** on the Secondary Navigation bar. The created server clusters should appear with their servers listed on the View Tree of Server Clusters page.
- Step 7** Connect to the Boston cluster—Click the Go Local icon () next to Boston-cluster. If this opens the local cluster's Manage Servers page, this confirms the administrator's connectivity to the cluster. To return to the regional cluster Web UI, click the Go Regional icon (.

Step 8 Connect to the Chicago cluster in the same way.

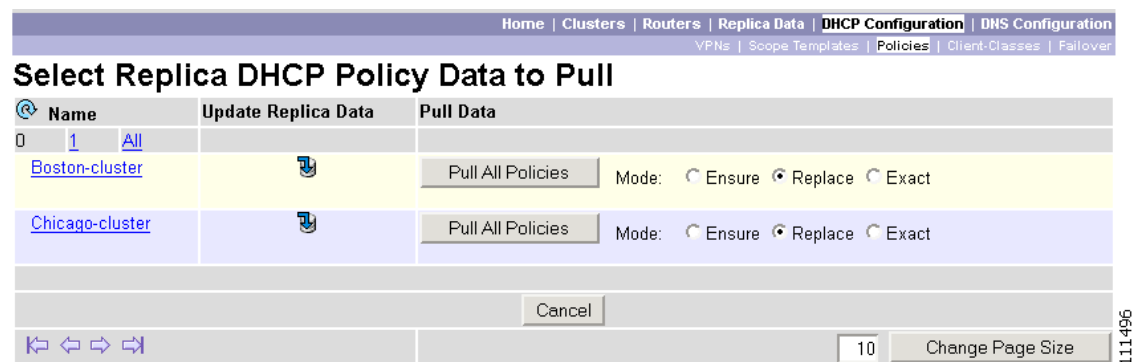
Pull a Policy from a Local Cluster


The example-central-admin next pulls a DHCP policy from the Boston cluster so that it can be replicated at the regional cluster.

Step 1 As example-central-admin, click **DHCP Configuration** on the Primary Navigation bar, then **Policies** on the Secondary Navigation bar to open the List DHCP Policies page.

Step 2 Click **Pull Replica Policies** at the bottom of the page. This opens the Select Replica DHCP Policy Data to Pull page (see [Figure 4-19](#)).

Figure 4-19 Pulling DHCP Policies from a Local Cluster



Step 3 Replicate the policy data at the regional cluster—Click the Replica icon () next to Boston-cluster. The cluster now shows a plus sign (+) next to it name. Click it to show the existing policies at the cluster.

Step 4 Pull the policy data from the replica database:

- Leave the **Replace** mode selected next to Boston-cluster—This replaces the data for any policy that may already exist with that name at the regional cluster).
- Click **Pull All Policies**.
- Click **Run** on the Report Pull Replica DHCP Policies page.
- Click **OK** on the Run Pull Replica DHCP Policies page. The List DHCP Policies page now shows the additional policies pulled from the Boston cluster.

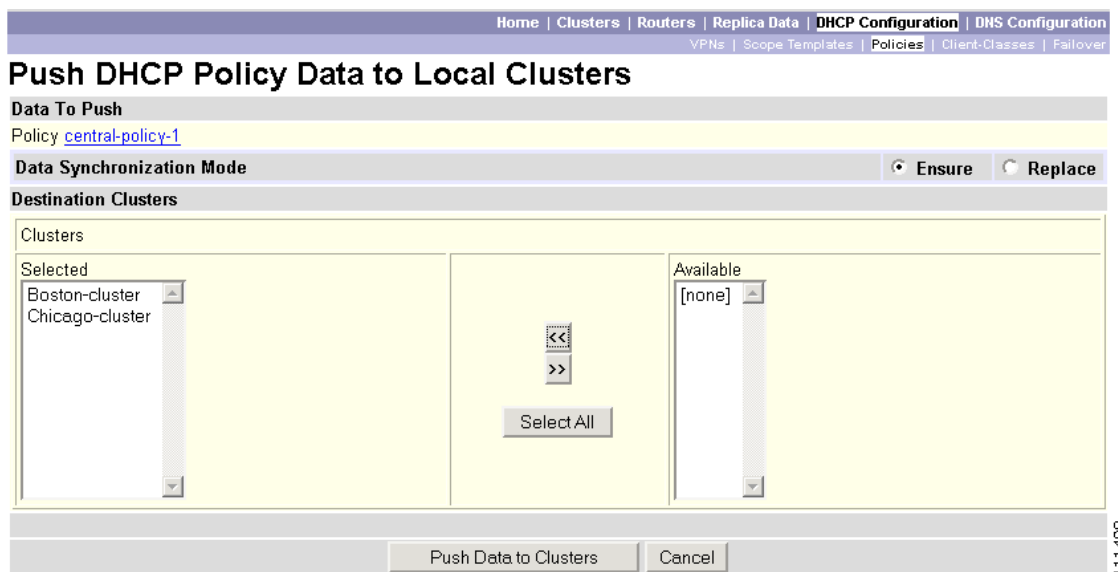
Create a Regional DHCP Policy and Push It to the Local Clusters

The example-central-admin next creates another DHCP a policy, with different attributes, at the regional cluster, and then pushes it to the local clusters.


Step 1 As example-central-admin, click **Add Policy** on the List DHCP Policies page to open the Add DHCP Policy page (which is almost identical to the local cluster page shown in [Figure 4-12 on page 4-15](#)).

- Step 2** Create a central policy for all the local clusters:
- Enter **central-policy-1** in the Name field.
 - Enter a lease period for the policy—Select **[51]dhcp-lease-time** in the Options drop-down list, then enter **2w** (for two weeks) for the lease period in the Value field.
 - Click **Add Option**.
 - Click **Add Policy** at the bottom of the page to return to the List DHCP Policies page. The central-policy-1 should appear.
- Step 3** Push the policy to the local clusters:
- Click **Push Policy** next to central-policy-1 to open 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.
 - Click **Select All** in the Destination Clusters section of the page.
 - Click << to move both clusters to the Selected field (see [Figure 4-20](#)).

Figure 4-20 Pushing a DHCP Policy to Local Clusters



- Click **Push Data to Clusters**.
- Step 4** View the push operation results on the View Push DHCP Policy Data Report page, then click **OK**.
- Step 5** Confirm that the policy now exists at the local cluster:
- Click **Clusters** on the Primary Navigation bar to open the View Tree of Server Clusters page.
 - Next to Boston-cluster, click the Go Local icon (🖥️➡️) in the Connect column.
 - In the Boston cluster Web UI, click **DHCP** on the Primary Navigation bar, then **Policies** on the Secondary Navigation bar to open the List DHCP Policies page. The central-policy-1 should appear.
 - Click the policy name to confirm the attributes set for it.

- e. Click the Go Regional icon () at the top right corner of the page to return to the regional cluster.
-

Create a Scope Template

The example-central-admin next creates a DHCP scope template to handle failover server pair creation.

- Step 1** As example-central-admin, click **DHCP Configuration** on the Primary Navigation bar, then **Scope Templates** on the Secondary Navigation bar to open the List DHCP Scope Templates page.
- Step 2** Click **Add Scope Template** to open the Add DHCP Scope Template page.
- Step 3** Set the basic properties for the scope template—Enter or select the following values in the fields:
 - a. Name—Enter **scopetemplate-1**.
 - b. Scope Name Expression—Concatenate the example-scope string with the subnet defined for the scope: Enter (**concat "example-scope-" subnet**).
 - c. Policy—Select the policy that defines the lease time: Click **central-policy-1** in the drop-down list.
 - d. Embedded Policy Option Expression—Define the router for the scope in its embedded policy and assign it the first address in the subnet: Enter (**create-option "routers" (create-ipaddr subnet 1)**).
 - e. Range Expression—Create an address range based on the remainder of the subnet (the second through last address): Enter (**create-range 2 100**).
- Step 4** Set the failover properties for the scope template—Expand the Failover attributes further down the page, then enter or select the following values:
 - a. Failover Setting—Click **scope-enabled**.
 - b. Main Server—Enter the IP address of the Boston-cluster host.
 - c. Backup Server—Enter the IP address of the Chicago-cluster host (see [Figure 4-21](#)).

Figure 4-21 Adding a Regional Scope Template

Attribute	Value				
Name*	scopetemplate-1				
Scope Name Expression	(concat "example-scope-" subnet)				
Policy	central-policy-1				
Range Expression	(create-range 2 100)				
Embedded Policy Option Expression	(create-option "routers" (create-ipaddr subnet 1))				
<input type="checkbox"/> Scope Selection Tags <table border="1"> <thead> <tr> <th>Tag</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table> <input type="button" value="Add Selection Tag"/>		Tag	Value	<input type="text"/>	<input type="text"/>
Tag	Value				
<input type="text"/>	<input type="text"/>				
<input type="checkbox"/> Dynamic DNS Settings <input type="checkbox"/> Failover Settings					
Attribute	Value	Data Type	Default		
Failover Setting <small>(failover)</small>	scope-enabled	enum			
Main Server <small>(failover-main-server)</small>	192.168.50.3	string			
Backup Server <small>(failover-backup-server)</small>	192.168.60.12	string			

111478

- Step 5** Click **Add Scope Template** at the bottom of the page. The scopetemplate-1 should appear on the List DHCP Scope Templates page.

Create and Synchronize the Failover Pair

The example-central-admin next creates the DHCP failover server pair relationship and synchronizes the failover pair. The DHCP server at the Boston-cluster will become the main, and the server at the Chicago-cluster the backup.

- Step 1** As example-central-admin, click **Failover** on the Secondary Navigation bar to open the List Failover Pairs page.
- Step 2** Click **Add Failover Pair** to open the Add Failover Pair page.
- Step 3** Add the failover pair—Enter or select the following values in the relevant fields:
- Failover Pair Name—Enter **central-fo-pair**.
 - Main DHCP Server—Click **Boston-cluster**.
 - Backup DHCP Server—Click **Chicago-cluster**.
 - Scope Template—Click **scopetemplate-1**.
 - Subnets—Move **192.168.50.0/24** from the Available field to the Selected field (see [Figure 4-22](#)).

Figure 4-22 Adding a Regional Failover Pair

The screenshot shows the 'Add Failover Pair' configuration page. At the top, there is a navigation bar with links: Home, Clusters, Routers, Replica Data, DHCP Configuration (highlighted), DNS Configuration, VPNs, Scope Templates, Policies, Client-Classes, and Failover. Below the navigation bar, the page title is 'Add Failover Pair'. The configuration fields are as follows:

- Failover Pair Name*: central-fo-pair
- Main DHCP Server*: Boston-cluster
- Backup DHCP Server*: Chicago-cluster
- Scope Template: scopetemplate-1

Below the fields is a 'Subnets' section. It contains two lists of subnets: 'Selected' and 'Available'. The 'Selected' list contains '192.168.50.0/24'. The 'Available' list contains '2.2.2.0/24', '3.3.0.0/16', '10.86.144.128/26', and '192.168.70.0/24'. Between the lists are navigation arrows: '<<', '>>', and a 'Select All' button. At the bottom of each list are search boxes and search buttons. The page number '111475' is visible on the right side.

- f. Click **Add Failover Pair** at the bottom of the page. The central-fo-pair should be listed on the List Failover Pairs page.

Step 4 Synchronize the failover pair with the local clusters:

- a. Click the Report icon (📄) to open the Report Synchronize Failover Pair page.
- b. Accept the default **Use Regional Subnets** setting.
- c. Accept the default **Main to Backup** synchronization direction setting.
- d. Accept the default **Update** operation setting (see Figure 4-23).

Figure 4-23 Setting Up Failover Synchronization



Home Clusters Routers Replica Data DHCP Configuration DNS Configuration				
VPNs Scope Templates Policies Client-Classes Failover				
Report Synchronize Failover Pair <i>central-fo-pair</i>				
Subnets	<input checked="" type="radio"/> Use Regional Subnets	<input type="radio"/> Use Local DHCP Scopes		
Direction of Synchronization	<input checked="" type="radio"/> Main to Backup	<input type="radio"/> Backup to Main		
Operation	<input checked="" type="radio"/> Update	<input type="radio"/> Complete	<input type="radio"/> Exact	
DHCP Server (server level failover pair)		replace		replace
Client Class Properties		replace		
Failover Properties		replace		
Failover Tuning Properties		replace		
Dynamic DNS Security Properties		replace		
All other Properties		no change		
LDAP Event Service		replace		replace
Policy		replace		exact
Option-list Property		ensure		
All other Properties		replace		
Client		replace	replace	exact
ClientClass		replace	replace	exact
Scopes (related to this failover pair)		exact	exact	exact
VPN		replace	replace	exact
Key		replace	replace	exact
Extensions		ensure	replace	exact
Extension Point		replace	replace	replace
Option Information		ensure	exact	exact
Custom options list				
Vendor options list				
Option-Data-types list				
Report Cancel				

111505

- e. Click **Report** at the bottom of the page.
- f. Click **Run Update** on the View Failover Pair Sync Report page.

The View Failover Pair Sync Report page now shows the details of the synchronization. If there are obsolete scopes at one of the clusters, you can delete them, or click **Return to Failover Pair List**. In either case, you return to the List Failover Pairs page.

Step 5 Confirm the failover configuration at the Boston cluster:

- a. Click the Go Local icon () next to Boston-cluster for single sign-on.
- b. On the Manage DHCP Server page of the local cluster, click the **Local DHCP Server** link.
- c. On the Edit DHCP Server page, check the failover attribute settings to ensure that they match those of the regional cluster configuration.
- d. Click the Go Regional icon () at the top of the page to return to the regional cluster.

Step 6 Confirm the failover configuration at the Chicago cluster in the same way.

Step 7 If sure that the data is correct, have the local cluster DHCP administrators reload their DHCP servers.

Delegate an Address Block

The example-address-admin next logs in to add an address type and address destination, add an address block, and delegate the address block to the address destination. When you delegate an address block, responsibility for creating subnets and allocating these to the DHCP server or static address ranges is handled by the local cluster administrator. For this example, an administrator at a second local cluster intentionally creates a scope with an address range in the address block delegated to the first local cluster. The regional administrator then replicates the data, pulls the data to the authoritative database, and does a consistency check, only to find that the address range is double-booked (overlaps).

-
- Step 1** Log out as example-central-admin, then log in as **example-address-admin**.
- Step 2** Click **Address Space** on the Primary Navigation bar, then **Address Types** on the Secondary Navigation bar to open the List Address Types page.
- Step 3** Create an address type:
- Click **Add Address Type** to open the Add Address Type page.
 - Enter **example-address-type** in the Name field.
 - Click **scopetemplate-1** in the Scope Template drop-down list.
 - Click **Add Address Type**. The example-address-type appears on the List Address Types page.
- Step 4** Create an address destination:
- Click **Address Destinations** on the Secondary Navigation bar.
 - Enter **destserver-1** in the Name field on the List/Add Address Destinations page.
 - Click **Boston-cluster** in the Server drop-down list.
 - Click **Add Address Destination** (see [Figure 18-4 on page 18-8](#)).
- Step 5** Create an address block:
- Click **Address Blocks** on the Secondary Navigation bar to open the List/Add Address Blocks page.
 - Enter **192.168.60** in the Address/Mask field.
 - Click **example-address-type** in the Address Type drop-down list.
 - Click **Add Address Block**.
- Step 6** Delegate the address block:
- Click the address block name to open the Edit Address Block page.
 - Click **destserver-1** in the Delegate To drop-down list in the middle of the page.
 - Click **Delegate Block**. On the Edit Address Block page, the text “Block is delegated to destserver-1” should appear under the Description field.
 - Click **Modify Address Block**. The address block now appears with a **D** (for delegated) next to it on the List/Add Address Blocks page.
- Step 7** At the Boston cluster, the local address administrator creates a static subnet for part of this delegated address block to use for new host address assignments. For example, create the 192.168.60.0/26 subnet with a range of 1 through 63.
- Step 8** At the Chicago cluster, the local address administrator creates a scope for network 192.168.60.0/26, with an address range of 1 through 63. This creates an IP address range and subnet overlapping condition at the regional cluster when the address space is replicated and pulled to the authoritative database.
- Step 9** At the regional cluster, replicate the data from Boston-cluster and Chicago-cluster.

- Step 10** Pull the replica address space data into the central authoritative database at the regional cluster.
- Step 11** Check the address range consistency:
- a. Click **Address Space** on the Primary Navigation bar, then **Consistency Rules** on the Secondary Navigation bar to open the List Consistency Rules page.
 - b. Click a check mark in the IP Range Consistency Rule box.
 - c. Click **Run Rules**. An IP range inconsistency violation should be returned.
-

Additional Regional Cluster Configuration

In addition to these configuration steps, the regional address administrator can also generate subnet utilization and lease history reports. For details on these functions, see the [“Polling Subnet Utilization and Lease History Data”](#) section on page 5-5.