



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, Groups, and Roles

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

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

How Administrators Relate to Groups and Roles

There are three administrator objects in Network Registrar—administrator, group, and role:

- **Administrator**—An account that logs in and that, through its association with one or more administrator groups, can perform certain functions based on its assigned role or roles. At the local cluster, these functions are administering the local Central Configuration Management (CCM) server and databases, hosts, zones, address space, and DHCP. At the regional cluster, these functions are administering the regional CCM server and databases, central configuration, and regional address space. An administrator must be assigned to at least one group to be effective.
- **Group**—A grouping of roles. You must associate one or more groups with an administrator, and a group must be assigned at least one role to be usable. The predefined groups that Network Registrar provides map each role to a unique group.
- **Role**—Defines the network objects that an administrator can manage and the functions that an administrator can perform. A set of predefined roles are created at installation, and you can define additional constrained roles. Some of the roles include subroles that provide further functional constraints.

Roles and Subroles

You can limit an administrator role by applying constraints. For example, you can use the `host-admin` base role to create a host administrator, named `192.168.50.0-host-admin`, who is constrained to the `192.168.50.0` subnet. The administrator assigned a group that includes this role then logs in with this constraint in effect.

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.

Certain roles provide subroles with which you can further limit the role functionality. For example, the local `ccm-admin` or `regional-admin`, with just the `owner-region` subrole applied, can manage only owners and regions. By default, all the possible subroles apply when you create a constrained role. (See [Table 4-4 on page 4-6](#) for how subroles affect which administrator objects you can push and pull.)

The predefined roles (and their possible subroles), and whether you can use them as base roles to define constrained roles, are described in [Table 4-1](#) for the local cluster, and [Table 4-2](#) for the regional cluster.

Table 4-1 Local Cluster Administrator Predefined and Base Roles

Predefined Role	Base Role?	Function (and Subroles)
<code>addrblock-admin</code> <code>addrblock-admin-readonly</code>		Address block administration—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.
<code>ccm-admin</code> <code>ccm-admin-readonly</code>	Yes	Local administration—Administers the local CCM server and databases. 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 local administrators. <i>authorization</i> —Can create and modify local groups and roles. <i>owner-region</i> —Can create and modify local owners and regions. <i>server-management</i> —Can manage the servers at the local cluster. <i>database</i> —Can view the CCM and MCD database change logs and tasks.
<code>dhcp-admin</code> <code>dhcp-admin-readonly</code>		DHCP administration—Manages dynamic host configuration, such as scopes, policies, and failover configurations. This role cannot be further constrained.
<code>host-admin</code> <code>host-admin-readonly</code>	Yes	Host administration—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 hostname in a set of zones.
<code>zone-admin</code> <code>zone-admin-readonly</code>	Yes	Zone administration—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.

Table 4-2 Regional Cluster Administrator Predefined and Base Roles

Predefined Role	Base Role?	Function (and Subroles)
addrblock-admin addrblock-admin-readonly		Local address block administration, only to be used at the local clusters—See Table 4-1 .
ccm-admin\ ccm-admin-readonly	Yes	Local administration—Administers the local CCM server and databases. 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 local administrators. <i>authorization</i> —Can create and modify local groups and roles. <i>owner-region</i> —Can create and modify local owners and regions. <i>server-management</i> —Can manage the servers at the local cluster. <i>database</i> —Can view the CCM and MCD database change logs and tasks.
central-cfg-admin central-cfg-admin-readonly	Yes	Central configuration administration—Manages clusters, routers and their interfaces (physical and virtual), VPNs, policies, client-classes, and scope templates, including pushing them to, or pulling them from, the local clusters. A constrained role derived from this base role can have the following subroles (they all apply by default): <i>dhcp-management</i> —Push and pull DHCP objects, and manage failover server pairs. <i>ric-management</i> —Manage router interfaces (requires a router license). <i>dns-management</i> —Manage DNS zone distributions.
dhcp-admin dhcp-admin-readonly		Local DHCP administration, only to be used at the local clusters—See Table 4-1 .
host-admin host-admin-readonly	Yes	Host administration, only to be used at the local clusters—See Table 4-1 .
zone-admin zone-admin-readonly	Yes	Zone administration, only to be used at the local clusters—See Table 4-1 .

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

Predefined Role	Base Role?	Function (and Subroles)
regional-admin regional-admin- readonly	Yes	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> —Create, modify, push, and pull administrators and groups. <i>authorization</i> —Create, modify, push, and pull roles and groups. <i>owner-region</i> —Create, modify, push, and pull owners and regions. <i>server-management</i> —Manage servers at the regional cluster. <i>database</i> —View the CCM database change logs and tasks, and perform trimming of the subnet utilization and lease history databases.
regional-addr-admin regional-addr- admin-readonly	Yes	Regional address administration—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): <i>subnet-utilization</i> —View subnet utilization reports. <i>lease-history</i> —View subnet lease history reports. <i>ric-management</i> —Push and de-allocate subnets to router interfaces (requires a router license). <i>dhcp-management</i> —Add and remove subnets from failover server pairs.

Groups

Administrator groups are the mechanism used to assign roles to administrators. Hence, a group must consist of one or more administrator roles to be usable. When you first install Network Registrar, a group is created for each predefined role. The local cluster Web UI is also predefined with two aggregate groups that are assigned multiple roles (see [Table 4-3](#)).



Note

When you upgrade from Network Registrar 6.0 or 6.1, this does not create groups for each predefined role. Groups are created for administrators that had direct role assignments in the earlier release. These group names are the original role names appended with *-group* (and a number if there happens to be an existing group by that name).

Table 4-3 Predefined Local Cluster Administrator Groups

Predefined Group	Associated Roles
address-mgt-group	addrblock-admin, ccm-admin, dhcp-admin
dns-mgt-group	ccm-admin, host-admin, zone-admin

Adding Administrators

The Network Registrar 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. 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 the group or groups to which the administrator should belong. These groups should have the appropriate role (and possibly subrole) assignments, thereby setting the proper constraints.

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 4-3 on page 4-14](#)).

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.

**Tip**

If you accidentally delete all the roles by which you can log in to Network Registrar (those having superuser, ccm-admin, or regional-admin privileges), you can recover by creating a username/password pair in the *install-path/conf/priv/local.superusers* file. You must create this file, have write access to it, and include a line in it with the format *username password*. After creating the file, stop and restart the Network Registrar server agent. Use this username and password for the next login session. Note, however, that using the local.superusers file causes reduced security. Therefore, use this file only in emergencies such as when temporarily losing all login access. Once logged in, create a superuser account in the usual way, then delete the local.superusers file or its contents.

Managing Passwords

Passwords are key to administrator access to the Web UI and CLI. In the Web UI, you enter the password on the Login page. In the CLI, you enter the password when you first invoke the **nrcmd** program. The local or regional CCM administrator or superuser can change any administrator's password. You can prevent exposing a password on entry:

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

Any administrator can change their own password on a given cluster. If you want the password change propagated to the regional cluster or other clusters, you must change the password at the regional cluster, then use the regional administrator push function to push the administrator to the other clusters (see the [“Pushing and Pulling Administrators” section on page 4-6](#)). You must have regional CCM administrator or superuser privileges; otherwise, you must have the regional administrator do it for you.

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, and local and regional CCM administrators 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 Managing Administrators

As a regional CCM administrator, you can:

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

Each of these functions involves having at least one regional CCM administrator subrole defined. [Table 4-4](#) describes the subroles required for these operations.

Table 4-4 Subroles Required for Central Administrator Management

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

Pushing and Pulling Administrators

You can push administrators to, and pull administrators from, local clusters on the List/Add Administrators page in the regional cluster Web UI (see [Figure 4-1](#)).


Figure 4-1 List/Add Administrators Page

Name*	Password	Superuser	NRCMD	Groups	
example-admin	*****	<input type="checkbox"/>	limited	address-admin-group central-admin-group example-group	
<input type="button" value="Add Administrator"/> <input type="button" value="Pull Replica Administrators"/> <input type="button" value="Push All Administrators"/>					
Name	Password	Superuser	NRCMD	Groups	Push Data
admin	*****	✓			<input type="button" value="Push Admin"/>

You can create both local and regional administrators at the regional cluster. However, you can push or pull only local administrators, because the local clusters cannot recognize regional administrators.

Pushing Administrators to Local Clusters

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

- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Administrators** on the Secondary Navigation bar.
- Step 2** On the List/Add Administrators Page, click **Push All Administrators** to push all the administrators listed on the page, or **Push Admin** next to an individual administrator. This opens the Push Administrator Data to Local Clusters page.
- Step 3** Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the administrators, you can choose Ensure, Replace, or Exact. If you are pushing a single administrator, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing administrator data at the local cluster. You would choose Exact only if you want to create an exact copy of the administrator database on the local cluster, thereby deleting all administrators that are not defined at the regional cluster.
- Step 4** Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.
- Step 5** Click **Push Data to Clusters**.
- Step 6** On the View Push Administrator Data Report page, view the push details, then click **OK** to return to the List/Add Administrators page.
- Step 7** To confirm that administrators are pushed successfully, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page. Click the Go Local icon () next to the cluster name to open the Web UI for the local cluster, then verify that the administrator or administrators are added to the cluster.

Pulling Administrators from the Replica Database

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

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

-
- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Administrators** on the Secondary Navigation bar.
 - Step 2** On the List/Add Administrators Page, click **Pull Replica Administrators**. This opens the Select Replica Administrator Data to Pull page.
 - Step 3** Click the Replicate icon (🔄) in the Update Replica Data column for the cluster. (For the automatic replication interval, see the [“Replicating Local Cluster Data”](#) section on page 5-6.)
 - Step 4** Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing administrator properties already defined at the regional cluster by choosing Ensure, or create an exact copy of the administrator database at the local cluster by choosing Exact (not recommended).
 - Step 5** Click **Pull All Administrators** next to the cluster, or expand the cluster name and click **Pull Administrator** to pull an individual administrator in the cluster.
 - Step 6** On the Report Pull Replica Administrators page, view the pull details, then click **Run**.
 - Step 7** On the Run Pull Replica Administrators page, view the change set data, then click **OK**. You return to the List/Add Administrators page with the pulled administrators added to the list.
-


Pushing and Pulling Groups

Pushing and pulling groups is vital in associating administrators with a consistent set of roles at the local clusters. You can push groups to, and pull groups from, local clusters on the List/Add Administrator Groups page in the regional cluster Web UI (see [Figure 4-13 on page 4-21](#)).

Pushing Groups to Local Clusters

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


-
- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Groups** on the Secondary Navigation bar.
 - Step 2** On the List/Add Administrator Groups page, click **Push All Groups** to push all the groups listed on the page, or **Push Group** next to an individual group. This opens the Push Group Data to Local Clusters page.
 - Step 3** Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the groups, you can choose Ensure, Replace, or Exact. If you are pushing a single group, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing group data at the local cluster. You would choose Exact only if you want to create an exact copy of the group data at the local cluster, thereby deleting all groups that are not defined at the regional cluster.
 - Step 4** By default, the associated roles and owners are pushed along with the group. Roles are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, remove the respective check mark.

- Step 5** Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.
 - Step 6** Click **Push Data to Clusters**.
 - Step 7** On the View Push Group Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Groups page.
 - Step 8** To confirm that groups are pushed successfully, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page. Click the Go Local icon () next to the cluster name to open the Web UI for the local cluster, then verify that the group or groups are added to the cluster.
-

Pulling Groups from the Replica Database

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

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

- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Groups** on the Secondary Navigation bar.
 - Step 2** On the List/Add Administrator Groups page, click **Pull Replica Groups**. This opens the Select Replica Group 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 the [“Replicating Local Cluster Data”](#) section on page 5-6.)
 - Step 4** Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing group properties at the local cluster by choosing Ensure, or create an exact copy of the group data at the local cluster by choosing Exact (not recommended).
 - Step 5** Click **Pull All Groups** next to the cluster, or expand the cluster name and click **Pull Group** to pull an individual group in the cluster.
 - Step 6** On the Report Pull Replica Groups page, view the pull details, then click **Run**.
 - Step 7** On the Run Pull Replica Groups page, view the change set data, then click **OK**. You return to the List/Add Administrator Groups page with the pulled groups added to the list.
-

Pushing and Pulling Roles

You can push roles to, and pull roles from, local clusters on the List/Add Administrator Roles page in the regional cluster Web UI (see [Figure 4-2](#)). You can also push associated groups and owners, and pull associated owners, depending on your subrole permissions (see [Table 4-4](#) on page 4-6).

Figure 4-2 List/Add Administrator Roles Page

Pushing Roles to Local Clusters


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

- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Roles** on the Secondary Navigation bar.
- Step 2** On the List/Add Administrator Roles page, click **Push All Groups** to push all the roles listed on the page, or **Push Role** next to an individual role. This opens the Push Role Data to Local Clusters page.
- Step 3** Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the roles, you can choose Ensure, Replace, or Exact. If you are pushing a single role, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing role data at the local cluster. You would choose Exact only if you want to create an exact copy of the role data at the local cluster, thereby deleting all roles that are not defined at the regional cluster.
- Step 4** By default, the associated groups and owners are pushed along with the role. Groups are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, remove the respective check mark:
 - If you disable pushing associated groups and the group does not exist at the local cluster, a group based on the name of the role is created at the local cluster.
 - If you disable pushing associated owners and the owner does not exist at the local cluster, the role will not be configured with its intended constraints. You must separately push the group to the local cluster, or ensure that the regional administrator assigned the owner-region subrole has pushed the group before pushing the role.
- Step 5** Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.
- Step 6** Click **Push Data to Clusters**.
- Step 7** On the View Push Role Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Roles page.
- Step 8** To confirm that roles are pushed successfully, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page. Click the Go Local icon (🏠➡) next to the cluster name to open the Web UI for the local cluster, then verify that the role or roles are added to the cluster.

Pulling Roles from the Replica Database

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

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

-
- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Roles** on the Secondary Navigation bar.
 - Step 2** On the List/Add Administrator Roles page, click **Pull Replica Roles**. This opens the Select Replica Role Data to Pull page.
 - Step 3** Click the Replicate icon () in the Update Replica Data column for the cluster. (For the automatic replication interval, see the [“Replicating Local Cluster Data”](#) section on page 5-6.)
 - Step 4** Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing role properties at the local cluster by choosing Ensure, or create an exact copy of the role data at the local cluster by choosing Exact (not recommended).
 - Step 5** If you have the owner-region subrole permission, you can decide if you want to pull all the associated owners with the role, which is always in Ensure mode. This choice is enabled by default.
 - Step 6** Click **Pull All Roles** next to the cluster, or expand the cluster name and click **Pull Role** to pull an individual role in the cluster.
 - Step 7** On the Report Pull Replica Roles page, view the pull details, then click **Run**.
 - Step 8** On the Run Pull Replica Roles page, view the change set data, then click **OK**. You return to the List/Add Administrator Roles page with the pulled roles added to the list.
-

Pushing and Pulling Owners or Regions


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

Pushing Owners or Regions to Local Clusters

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


-
- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Owners** or **Regions** on the Secondary Navigation bar.
 - Step 2** On the List/Add Owners or List/Add Regions page, click **Push All Owners** or **Push All Regions** to push all the owners or regions listed on the page, or **Push Owner** or **Push Region** next to an individual owner or region. This opens the Push Owner Data to Local Clusters or Push Owner Data to Local Clusters page.
 - Step 3** Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the owners or regions, you can choose Ensure, Replace, or Exact. If you are pushing a single owner or region, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose

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

- Step 4** Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.
 - Step 5** Click **Push Data to Clusters**.
 - Step 6** On the View Push Owner Data Report or View Push Region Data Report page, view the push details, then click **OK** to return to the List/Add Owners or List/Add Regions page.
 - Step 7** To confirm that owners or regions are pushed successfully, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page. Click the Go Local icon () next to the cluster name to open the Web UI for the local cluster, then verify that the owners or regions are added to the cluster.
-

Pulling Owners or Regions from the Replica Database

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

- Step 1** Click **Administration** on the Primary Navigation bar in the regional cluster Web UI, then **Owners** or **Regions** on the Secondary Navigation bar.
 - Step 2** On the List/Add Owners or List/Add Regions page, click **Pull Replica Owners** or **Pull Replica Regions**. This opens the Select Replica Owner Data to Pull or Select Replica Region Data to Pull page.
 - Step 3** Click the Replicate icon () in the Update Replica Data column for the cluster. (For the automatic replication interval, see the [“Replicating Local Cluster Data”](#) section on page 5-6.)
 - Step 4** Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing owner properties at the local cluster by choosing Ensure, or create an exact copy of the owner data at the local cluster by choosing Exact (not recommended).
 - Step 5** Click **Pull All Owners** or **Pull All Regions** next to the cluster, or expand the cluster name and click **Pull Owner** or **Pull Region** to pull an individual owner or region in the cluster.
 - Step 6** On the Report Pull Replica Owners or Report Pull Replica Regions page, view the pull details, then click **Run**.
 - Step 7** On the Run Pull Replica Owners or Run Pull Replica Region page, view the change set data, then click **OK**. You return to the List/Add Owners or List/Add Regions page with the pulled owners or regions added to the list.
-

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 4-22.

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 and example-zone-admin. (At the Chicago cluster, the example-cluster-admin acts as these two administrators.)
 - Creates the basic network infrastructure for the local clusters.
 - Creates the example-host-role to constrain host administration 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 at the Boston cluster.
 - Creates the chicago.example.com zone and its reverse zone at the Chicago cluster.
- example-zone-admin (Boston cluster only):
 - Assigns the example-host-admin the example-host-group in Boston.
 - Creates the example.com and boston.example.com zones, and maintains the latter zone.
- example-host-admin (Boston cluster only)—Maintains local host lists and IP address assignments.

Create the Administrators

For this example, the superuser in Boston creates the local cluster, zone, host, address, and DHCP administrators. Also, the superuser in Chicago creates the cluster administrator, with the responsibilities described in the [“Administrator Responsibilities and Tasks”](#) section on page 4-13.

-
- 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 (see [Figure 4-3](#)).

Figure 4-3 Adding a Local Cluster Administrator

Name	Password	Superuser	NRCMD	Groups
example-cluster-admin	*****	<input checked="" type="checkbox"/>	full	addrblock-admin-group addrblock-admin-readonly-group address-mgt-group
Add Administrator				
Name	Password	Superuser	NRCMD	Groups
admin	*****	<input checked="" type="checkbox"/>	full	

Step 4 Make the example-cluster-admin a superuser with full CLI access:

- a. Click a check mark in the Superuser box.
- b. Choose **full** in the NRCMD drop-down list.
- c. Click **Add Administrator**.

Step 5 Add the Boston zone administrator:

- a. Enter **example-zone-admin** in the Name field, then **examplezone** in the Password field.
- b. 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.)
- c. Click **Add Administrator**.

Step 6 Add the Boston host administrator:

- a. Enter **example-host-admin** in the Name field, then **examplehost** in the Password field.
- b. Do not choose any more items—The example-zone-admin will later assign a group with a constrained role to example-host-admin.
- c. Click **Add Administrator**.

The names of the three new administrators should appear on the List/Add Administrators page of the Boston cluster (see Figure 4-4) and should have the following properties:

- example-cluster-admin—Superuser flag checked and “full” in the NRCMD column.
- example-host-admin—No choices.
- example-zone-admin—The dns-mgt-group assigned.

Figure 4-4 Listing the Local Administrators

Name*	Password	Superuser	NRCMD	Groups
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	addrblock-admin-group addrblock-admin-readonly-group address-mgt-group
Add Administrator				
Name	Password	Superuser	NRCMD	Groups
admin	*****	✓	full	
example-cluster-admin	*****	✓	full	
example-host-admin	*****			
example-zone-admin	*****			dns-mgt-group

- Step 7** Go to the Chicago cluster and create the same **example-cluster-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 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 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:
- In the Address/Mask field, enter **192.168.50.0**.
 - Choose **24** in the mask drop-down list—This subnet will be a normal Class C network.
 - Leave the Owner, Region, and Address Type fields as **[none]**.
 - Click **Add Subnet** to show the subnet added to the list.
- Step 4** Click the **192.168.50.0/24** link to open the Edit Subnet page (see [Figure 4-5](#)).

Figure 4-5 Adding an Address Range to a Subnet

Home | Administration | Zone | Host | **Address Space** | DHCP
Address Space | Address Blocks | **Subnets** | Address Types | Consistency Rules

Edit Subnet 192.168.50.0/24

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

Modify Subnet Cancel

IP Ranges		
Start	End	Type
		static

Add IP Range

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

84336

- Step 5** Enter the address range:
- Enter **101** in the Start field.
 - Enter **200** in the End field.
 - Click **Add IP Range**.
- 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:
- Log out as superuser, then log in as **example-cluster-admin** with password **exampleadmin**.
 - Go to the List/Add Subnets page, enter **192.168.60.0/24** as the subnet, then click **Add Subnet**.
 - Go to the Edit Subnet page, enter **101** through **200** as the address range, then click **Add Range**.
 - Click **Modify Subnet**.
 - 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 and their subzones. The example-cluster-admin in Boston also adds some initial host records to the boston.example.com zone.

Create the Forward Zones

First, create the example.com, boston.example.com, and chicago.example.com forward 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 administration.
- 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 4-6](#)).

Figure 4-6 Creating a Zone

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
example.com.	[none]	[none]

Add Zone

⌂ Name Owner Configuration RRs Active Server RRs

⏪ ⏩ 🔍 [Name] 10 Change Page Size

- Click **Add Zone** to open the Add Zone page (see [Figure 4-7](#)).

Figure 4-7 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

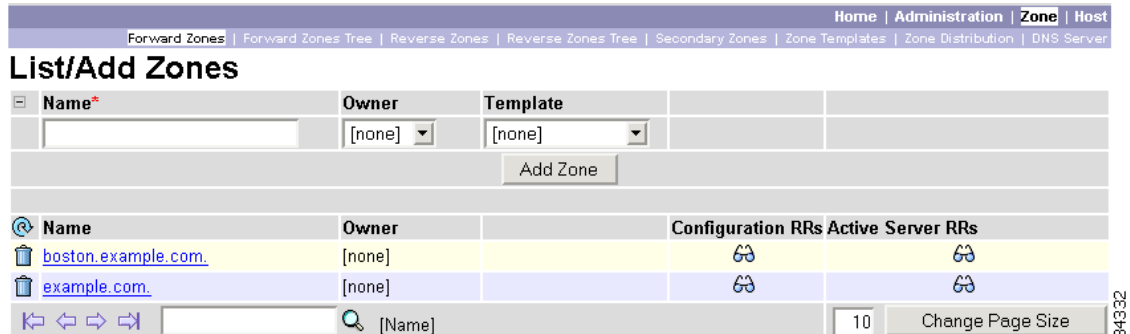
Add Zone

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.
	Add Nameserver

- Step 4** Enter the minimum data to create the zone—the Start of Authority (SOA) serial number, primary DNS server name, hostmaster’s contact 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 bottom field of Nameservers—Enter **ns1**, then click **Add Nameserver**.

- Step 5** Click **Add Zone** at the bottom of the page to add the zone and return to the List/Add Zones page (see Figure 4-8).

Figure 4-8 Viewing the Zones



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

Create the Reverse Zones

Next, create the reverse zones for example.com, boston.example.com, and chicago.example.com in Boston and Chicago. This enables adding reverse address pointer (PTR) records for each host added to the subnet. The reverse zone in Boston will be based on the 192.168.50.0 subnet, and the reverse zone in Chicago will be based on the 192.168.60.0 subnet.

- Step 1** At the Boston cluster, log back in as **example-zone-admin**.
- Step 2** Click **Zone** on the Primary Navigation bar, then **Reverse Zones** on the Secondary Navigation bar.
- Step 3** On the List/Add Reverse Zones page, enter **50.168.192.in-addr.arpa** in the Name field.
- Step 4** Click **Add Zone** to open the Add Zone page, as in the previous section.
- Step 5** Enter the minimum data to create the reverse zone, using the forward zone values. In each of these fields:
- Serial Number—Enter **1**.
 - Nameserver—Enter **ns1.boston.example.com**.
 - Contact E-Mail—Enter **hostmaster.boston.example.com**.
 - In the bottom field of Nameservers—Enter **ns1.boston.example.com.**, then click **Add Nameserver**.
- Step 6** Click **Add Zone** to add the zone and return to the List/Add Reverse Zones page. The page should now show the loopback zone **127.in-addr.arpa** and the reverse zone for Boston, **50.168.192.in-addr.arpa**.

- Step 7** At the Chicago-cluster, have the example-cluster-admin create the reverse zone for the chicago.example.com zone, naming it **60.168.192.in-addr.arpa.**, and setting the appropriate values based on the forward zone.

Create the Initial Hosts

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

- Step 1** At the Boston cluster, as example-zone-admin, 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 (see [Figure 4-9](#)).

Figure 4-9 Adding a Host and Address to a Zone

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?	Valid IP Ranges
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"/>			

Navigation: [Previous] [Next] [Search] [Name] [Page Size: 10] [Change Page Size]

- 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, **userhost2**, with address **192.168.50.102** in the same way. The two hosts should now appear on the List/Add Hosts for Zone page.

Assign a Constrained Group to the Administrator

The example-cluster-admin at the Boston cluster next creates the example-host-role with zone and address range constraints. The administrator also creates an example-host-group to include this role so that the example-zone-admin can assign this group to the example-host-admin. The example-host-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 to open the List/Add Administrator Roles page (see [Figure 4-10](#)),.

Figure 4-10 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

- Step 3** Add the role:
- Enter **example-host-role** in the Name field.
 - Click **host-admin** in the Base Role drop-down list.
 - Click **Add Role** to open the Add Host Administrator Role page.

- Step 4** Constrain the role:
- Under Zone Restrictions, (see [Figure 4-11](#)), choose **boston.example.com** in the Available list.
 - Click << to move it to the Selected list.

Figure 4-11 Setting Zone Restrictions for a Role

Zone Restrictions

Zones

Selected

boston.example.com

Available

example.com

<< >>

Select All

Deselect All

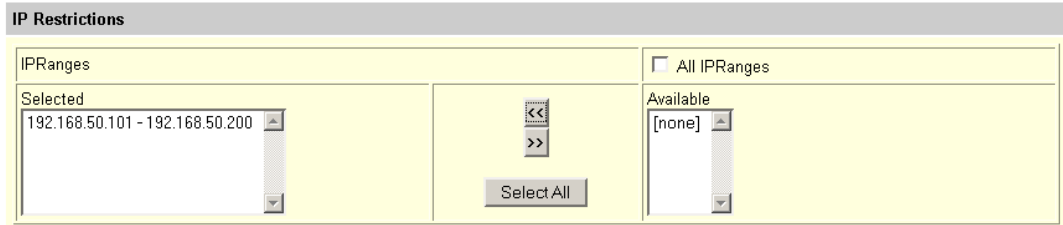
10

Change Page Size

Search

- Under IP Restrictions, (see [Figure 4-12](#)), choose **192.168.50.101 – 192.168.50.200** in the Available list.
- Click << to move this range to the Selected list.

Figure 4-12 Setting IP Address Restrictions for a Role

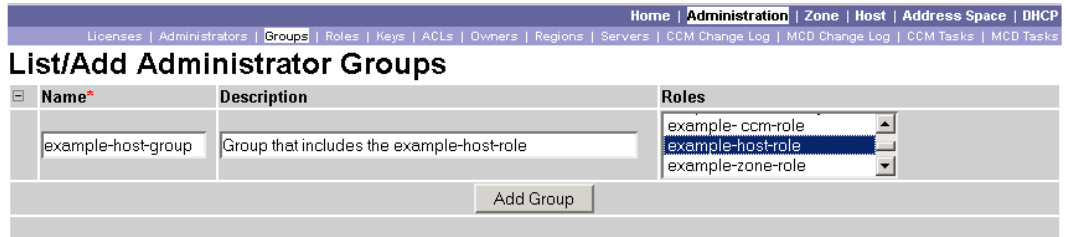


116761

Step 5 Click **Add Role** at the bottom of the page. The role appears on the List/Add Administrator Roles page.

Step 6 Click **Groups** on the Secondary Navigation bar to open the List/Add Administrator Groups page (Figure 4-13).

Figure 4-13 Creating a Group to Assign a Role to an Administrator



116762

Step 7 Create the example-host-group, assigning the example-host-role to it:

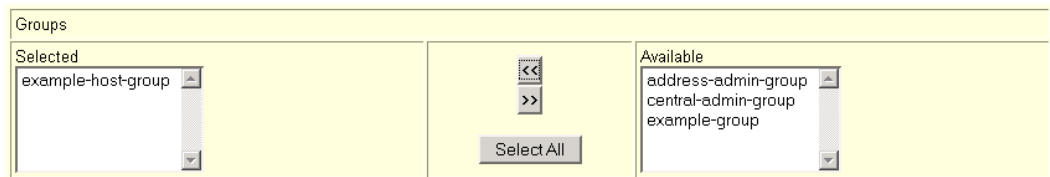
- a. Enter **example-host-group** in the Name field.
- b. Add a description such as “Group that includes the example-host-role.”
- c. Choose **example-host-role** in the Roles drop down list.
- d. Click **Add Group**.

Step 8 Log out as example-cluster-admin, then log in as **example-zone-admin**.

Step 9 As example-zone-admin, assign the example-host-group 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. In the Groups area of the Edit Administrator page (see Figure 4-14), click **example-host-group** in the Available list.

Figure 4-14 Assigning a Group to an Administrator



116763

- d. Click << to move the group to the Selected list.

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

- 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 choice 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.
-

Regional Cluster Management Tutorial

This tutorial is an extension of the scenario described in the [“Local Cluster Management Tutorial” section on page 4-12](#). In the regional cluster tutorial, San Jose has two administrators—a regional CCM administrator (who will have both regional and local administration functions), and a central configuration 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 Chicago.

Administrator Responsibilities and Tasks

The regional administrators have the following responsibilities and tasks:

- example-ccm-admin (created by the superuser at the San Jose cluster):
 - Creates the example-admin-group at the regional cluster.

- Creates the example-central-admin at the regional cluster.
- Creates the Boston and Chicago clusters.
- Modifies the example-central-admin to include local cluster administration.
- Pushes the example-central-admin to the clusters.
- example-central-admin:
 - Adds a router and modifies a router interface. (This occurs first to prevent overlapping subnets and router synchronization problems later on.)



Note Skip this step if a router is not available or the router license is not installed.

- Pulls zone data from the local clusters and creates a zone distribution.
- Creates a subnet and policy, and pulls address space, to configure DHCP failover pairs in Boston and Chicago.

Create the Regional CCM Administrator

The superuser first creates the example-ccm-administrator defined with groups to perform CCM and regional administration.

-
- Step 1** Log in to the regional cluster as superuser.
 - Step 2** As superuser, click **Groups** on the Secondary Navigation bar.
 - Step 3** Click **Administration** on the Primary Navigation bar, then **Administrators** on the Secondary Navigation bar.
 - Step 4** On the List/Add Administrators page, enter **example-ccm-admin** in the Name field and **ccmadmin** in the Password field (see [Figure 4-3 on page 4-14](#) for the local cluster version).
 - Step 5** Multiselect **ccm-admin-group** and **regional-admin-group** in the Groups drop-down list.
 - Step 6** Click **Add Administrator**.
-

Create the Regional Group and Administrator

The example-ccm-admin next creates the central-admin-group with the central-cfg-admin and regional-addr-admin roles applied, then assigns this group when creating the example-central-admin.

-
- Step 1** Log out as superuser, then log in as the **example-ccm-admin** created by the superuser. Note that the administrator has just administration privileges.
 - Step 2** Click **Administration** on the Primary Navigation bar, then **Groups** on the Secondary Navigation bar.
 - Step 3** On the List/Add Administrator Groups page, enter **central-admin-group** in the Name field.
 - Step 4** Multiselect **central-cfg-admin** and **regional-addr-admin** in the Roles drop-down list (see [Figure 4-15](#)).

Figure 4-15 Adding Administrator Groups

Name*	Description	Roles
central-admin-group		central-cfg-admin central-cfg-admin-readonly regional-addr-admin

116764

- Step 5** Click **Add Group**. The central-admin-group now appears with the central-cfg-admin and regional-addr-admin roles listed.
- Step 6** Click **Administrators** on the Secondary Navigation bar.
- Step 7** On the List/Add Administrators page, enter **example-central-admin** in the Name field.
- Step 8** Enter **centraladmin** in the Password field.
- Step 9** Choose **central-admin-group** in the Groups drop-down list (see Figure 4-16).

Figure 4-16 Adding a Regional Administrator

Name*	Password	Superuser	NRCMD	Groups
example-central-admin	*****	<input type="checkbox"/>		address-admin-group central-admin-group example-group

116765

- Step 10** Click **Add Administrator**. The example-central-admin now appears on the List/Add Administrators page with the central-admin-group assigned.

Create the Local Clusters

The example-ccm-admin next creates the local clusters at the regional cluster.

- Step 1** As example-ccm-admin, click **Clusters** on the Primary Navigation bar, then **Cluster List** on the Secondary Navigation bar to open the List Server Clusters page.
- Step 2** Click **Add Cluster** to open the Add Server Cluster page.
- Step 3** Create the Boston cluster based on data provided by the administrator at the cluster:
- Enter **Boston-cluster** in the name field.
 - Enter the IP address of the Web UI machine in Boston in the ipaddr field.
 - Enter **example-cluster-admin** in the admin field. (A superuser account is required.)
 - Enter **exampleadmin** in the password field.
 - 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 4-17).

Figure 4-17 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	
scp-port	1234	unsigned 32-bit	
Webserver Settings			
Attribute	Value	Data Type	Default
http-port	8080	unsigned 32-bit	
https-port		unsigned 32-bit	

111474


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

- Step 4** 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 5** 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 6** 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 7** Connect to the Chicago cluster to confirm the connectivity in the same way.

Push the Redefined Central Administrator

The example-ccm-admin next modifies the example-central-admin to have local cluster roles, then pushes the administrator to the local clusters.

- Step 1** As example-ccm-admin, click **Administration** on the Primary Navigation bar, then **Administrators** on the Secondary Navigation bar.
- Step 2** Click **example-central-admin** to open the Edit Administrator page.
- Step 3** The page also includes local groups to assign. The example-central-admin should have additional local DHCP and zone administration privileges. Multiselect the local groups **dhcp-admin-group** and **zone-admin-group** in the Available list and move them to the Selected list.
- Step 4** Click **Modify Administrator**.
- Step 5** Click **Push Admin** next to the example-central-admin entry in the list.

- Step 6** On the Push Administrator Data to Local Clusters page, keep the data synchronization mode as Ensure.
- Step 7** Multiselect **Boston-cluster** and **Chicago-cluster** in the Available field of the Destination Clusters, then move them both to the Selected field.
- Step 8** Click **Push Data to Clusters**.
- Step 9** On the View Push Administrator Data Report page, click **OK**.
- Step 10** To confirm that example-central-admin was pushed successfully, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page. Click the Go Local icon () next to one of the cluster names to open the Web UI for the local cluster, then verify that the administrator is created there.

Add a Router and Modify an Interface

The example-central-admin next adds a router and modifies one of its interfaces to configure the DHCP relay agent. The administrator can do this because it is part of the role definition, and because the address space and router licenses apply. Adding the router pulls in the subnets already defined in the router configuration. This should occur now to prevent overlapping subnets and router synchronization errors, once other address space is added later on. (Because the routers defined the physical network, it is preferable to save these definitions as opposed to those possibly conflicting definitions present in the DHCP configuration.)



Note

Skip this step if a router is not available or the router license is not installed.

- Step 1** Log out as example-ccm-admin, 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 5-12](#)).
- Step 3** Click **Add Router** to open the Add Router page.
- Step 4** Add the router:
- Give the router a distinguishing name in the name field. For this example, enter **router-1**.
 - Because this router is a Cisco uBR7200 router, click **Ubr72xx** in the Router Type drop-down list.
 - Enter the router's IP address in the address field.
 - Enter the router administrator's username in the username field.
 - Enter the router administrator's password in the password field.
 - Enter the router administrator's enable password in the enable field.
 - Click **Add Router** (see [Figure 4-18](#)).

Figure 4-18 Adding a Router

e. 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. (Alternatively, from the List Routers page, click the interfaces icon (🌳) associated with the router, then click 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 4-19).



Figure 4-19 Editing a Router Interface

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.

Pull Zones and Create a Zone Distribution

The example-central-admin next pulls zone data from the Boston and Chicago clusters and creates a zone distribution from the zones.

-
- Step 1** As example-central-admin, click **Clusters** on the Primary Navigation bar, then **Cluster Tree** on the Secondary Navigation bar to open the View Tree of Server Clusters page.
- Step 2** Click the Replicate icon () in the Replicate Data column for the Boston-cluster, then do the same thing for the Chicago-cluster.
- Step 3** Click **DNS Configuration** on the Primary Navigation bar, then **Zone Distributions** on the Secondary Navigation bar to open the List/Add Zone Distributions page.
- Step 4** Pull the replica zone data:
- Click **Pull Replica Zone Data** to open the Select Replica Zone Data page.
 - Leave the Data Synchronization Mode as Update, then click **Report** to open the Report Pull Replica Zone Data page.
 - Notice the change sets of data to pull, then click **Run**.
 - On the Run Pull Replica Zone Data page, click **OK**.
- Step 5** Notice that the two clusters are assigned generated numbers for their names on the List/Add Zone Distributions page. Click the number for the Boston-cluster to open its Edit Zone Distribution page.
- Step 6** Because we want to make the Chicago-cluster DNS server a secondary server for the Boston-cluster:
- Click **Add Server** in the Secondary Server area.
 - On the Add Zone Distribution Secondary Server page, click **Chicago-cluster** in the Secondary Server drop-down list, then click **Add Secondary Server**.
 - On the Edit Zone Distribution page for Boston-cluster, click **Modify Zone Distribution**.
- Step 7** Synchronize the zone distributions:
- On the List/Add Zone Distributions page, click the Run icon () in the Synchronize column for the Boston-cluster.
 - Return to the zone distribution list, then do the same for the Chicago-cluster.
-

Create a Subnet and Pull Address Space



The example-central-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.

-
- Step 1** As example-central-admin, 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 (in the “[Add a Router and Modify an Interface](#)” section on page 4-26).
- Step 2** Create an additional subnet, 192.168.70.0/24:
- Enter **192.168.70** (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.
 - Click **Add Subnet**.

- Step 3** Click **Address Space** on the Secondary Navigation bar to confirm the subnet you created.
- Step 4** Click **Pull Replica Address Space**.
- Step 5** On the Select Pull Replica Address Space page, 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 show appear on the List/Add Subnets page.
-

Push a DHCP Policy

The example-central-admin next creates a DHCP a policy 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.
- Step 2** On the Add DHCP Policy page, create a central policy for all the local clusters:
- Enter **central-policy-1** in the Name field.
 - Enter a lease period for the policy—Choose **[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.
 - 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.
 - 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 (see [Figure 4-20](#)).

Figure 4-20 Adding a Regional Scope Template

The screenshot shows the 'Add DHCP Scope Template' configuration page. The breadcrumb navigation at the top includes: Home | Clusters | Routers | Replica Data | **DHCP Configuration** | DNS Configuration | VPNs | **Scope Templates** | Policies | Client-Classes | Failover.

The main form has the following fields and values:

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))

Below the main form is a section for 'Scope Selection Tags' with a 'Tag Value' input field and an 'Add Selection Tag' button.

There are also sections for 'Dynamic DNS Settings' and 'Failover Settings'. The 'Failover Settings' section is expanded and contains the following table:

Attribute	Value	Data Type	Default
Failover Setting (failover)	scope-enabled	enum	
Main Server (failover-main-server)	192.168.50.3	string	
Backup Server (failover-backup-server)	192.168.60.12	string	

111478

- Step 3** Set the basic properties for the scope template—Enter or choose the following values in the fields:
- Name—Enter **scopetemplate-1**.
 - Scope Name Expression—Concatenate the example-scope string with the subnet defined for the scope: Enter (**concat "example-scope-" subnet**).
 - Policy—Choose the policy that defines the lease time: Click **central-policy-1** in the drop-down list.
 - 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)**).
 - 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 choose the following values:
- 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.
- 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 choose the following values in the relevant fields:
- a. Failover Pair Name—Enter **central-fo-pair**.
 - b. Main DHCP Server—Click **Boston-cluster**.
 - c. Backup DHCP Server—Click **Chicago-cluster**.
 - d. Scope Template—Click **scopetemplate-1**.
 - e. Subnets—Move all three subnets (192.168.50.0/24, 192.168.60.0/24, and 192.168.70.0/24) from the Available field to the Selected field (see [Figure 4-21](#)).

Figure 4-21 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** | DNS Configuration | VPNs | Scope Templates | Policies | Client Classes | Failover. Below the navigation bar, the page title is 'Add Failover Pair'. The form contains the following fields:


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

Below these fields is the 'Subnets' section, which is divided into two columns: 'Selected' and 'Available'. The 'Selected' column contains the subnet 192.168.50.0/24. The 'Available' column contains the subnets 2.2.2.0/24, 3.3.0.0/16, 10.86.144.128/26, and 192.168.70.0/24. Between the two columns are navigation arrows (<< and >>) and a 'Select All' button. At the bottom of each column is a search bar with a 'Search' button. The page number 111475 is visible in the bottom right corner.

111475




- 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.
- 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 and reload the server 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 **Cancel**.
- e. On the Manage DHCP Server page, click the Reload icon ()
- f. 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.
