CHAPTER 5

Configuring Administrators

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

See Also

Administrators, Groups, Roles, and Tenants, page 5-1
External Authentication Servers, page 5-14
Granular Administration, page 5-16
Licensing, page 5-20
Centrally Managing Administrators, page 5-21
Local Cluster Management Tutorial, page 5-31
Regional Cluster Management Tutorial, page 5-38

Administrators, Groups, Roles, and Tenants

The types of functions that network administrators can perform in Cisco Network Registrar are based on the roles assigned to them. Local and regional administrators can define these roles to provide granularity for the network administration functions. Cisco 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, and other network objects.

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

The data and configuration that can be viewed by an administrator can also be restricted by tenant. When an administrator is assigned a tenant tag, access is further restricted to configuration objects that are assigned to the tenant or made available for tenant use as read-only core configuration objects.

See Also

How Administrators Relate to Groups, Roles, and Tenants
Administrator Types, page 5-2
Roles, Subroles, and Constraints, page 5-3
Groups, page 5-5
Managing Administrators, page 5-6
Managing Passwords, page 5-7
Managing Groups, page 5-7
Managing Roles, page 5-8
Managing Tenants, page 5-9

How Administrators Relate to Groups, Roles, and Tenants

There are four administrator objects in Cisco Network Registrar—administrator, group, role, and tenant:

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

  Adding administrators is described in the "Managing Administrators" section on page 5-6.

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

  Adding groups is described in the "Managing Groups" section on page 5-7.

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

  Adding roles is described in the "Managing Roles" section on page 5-8.

- **Tenant**—Identifies a tenant organization or group that is associated with a set of administrators. When you create tenants, the data stored on both regional and local clusters is segmented by tenant. A tenant cannot access the data of another tenant.

  Adding tenants is described in "Managing Tenants" section on page 5-9.

Administrator Types

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

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

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

  When a superuser is assigned a tenant tag, unrestricted access is only granted for corresponding tenant data. Data of other tenants cannot be viewed, and core objects are restricted to read-only access.

- **Specialized**—Administrator created by name to fulfill specialized functions, for example, to administer a specific DNS forward or reverse zone, based on the administrator assigned role (and subrole, if applicable). Specialized administrators, like the superuser, require a password, but must also be assigned at least one administrator group that defines the relevant roles. The entry fields in the web UI appear in Figure 5-1 on page 5-22. The CLI provides the **admin** command.

  For an example of creating a local zone or host administrator, see the "Create the Administrators" section on page 5-32.

A specialized user that is assigned a tenant tag can only access corresponding tenant or core data that also matches the relevant roles. Core data is further restricted to read-only access.

Roles, Subroles, and Constraints

You can limit an administrator role by applying constraints. For example, you can use the host-admin base role to create a host administrator, named 192.168.50-host-admin, who is constrained to the 192.168.50.0 subnet. The administrator assigned a group that includes this role then logs in with this constraint in effect. Adding roles and subroles is described in the "Managing Roles" section on page 5-8.

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

Tip An example of adding role constraints is in the "Create a Host Administrator Role with Constraints" section on page 5-35.

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

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

The predefined roles are described in Table 5-1 (local), and Table 5-2 on page 5-4 (regional).

Table 5-1 Local Cluster Administrator Predefined and Base Roles

Local Role	Subroles and Active Functionality
addrblock-admin	Core functionality: Manage address block, subnets, and reverse DNS zones (also requires dns-admin); and notify of scope activity. • *ric-management*: Push to, and reclaim subnets from, DHCP failover pairs and routers. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations.
ccm-admin	Core functionality: Manage licenses, access control lists (ACLs), and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets.

Table 5-1 Local Cluster Administrator Predefined and Base Roles (continued)

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

Table 5-2 Regional Cluster Administrator Predefined and Base Roles

Regional Role	Subroles and Active Functionality
central-cfg-admin	Core functionality: Manage clusters and view replica data. • *dhcp-management*: Manage DHCP scope templates, policies, client-classes, failover pairs, virtual private networks (VPNs), and options; modify subnets; and replicate data. • *ric-management*: Manage routers and router interfaces, and pull replica router data.
central-dns-admin	Core functionality: Manage DNS zones and templates, hosts, resource records, and secondary servers; and create subzones and reverse zones. • *security-management*: Manage DNS update policies, ACLs, and encryption keys. • *server-management*: Synchronize DNS zones and HA server pairs, manage zone distributions, pull replica zone data, and push update maps.

Table 5-2 Regional Cluster Administrator Predefined and Base Roles (continued)

Regional Role	Subroles and Active Functionality
central-host-admin	Core functionality: Manage DNS hosts. (Note that if an administrator is also assigned a constrained central-dns-admin role that overrides the central-host-admin definition, the administrator is not assigned the central-host-admin role.)
regional-admin	Core functionality: Manage licenses and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets.
regional-addr-admin	Core functionality: Manage address blocks, subnets, and address ranges; generate allocation reports; and pull replica address space data. • *dhcp-management*: Push and reclaim subnets; and add subnets to, and remove subnets from, DHCP failover pairs. • *lease-history*: Query, poll, and trim lease history data. • *subnet-utilization*: Query, poll, trim, and compact subnet utilization data.

Groups

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

Roles with the same base role are combined. A group with an unconstrained dhcp-admin role and a constrained dns-admin role, does not change the privileges assigned to the dns-admin role. For example, if one of the roles is assigned unconstrained read-write privileges, the group is assigned unconstrained read-write privileges, even though other roles might be assigned read-only privileges. Therefore, to limit the read-write privileges of a user while allowing read-only access to all data, create a group that includes the unconstrained read-only role along with a constrained read-write role. (See the "Roles, Subroles, and Constraints" section on page 5-3 for the implementation of host-admin and dns-admin roles combined in a group.)

Note Upgrading from Cisco Network Registrar 6.0 or 6.1 does not create groups for each predefined role. However, groups are created for administrators that had direct role assignments in the earlier releases. These group names are the original role names appended with **–group** (and a number if there already is a group by that name).

Managing Administrators

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

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

Tip If you accidentally delete all the roles by which you can log in to Cisco 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*. Use this username and password for the next login session. Note, however, that using the local.superusers file causes reduced security. Therefore, use this file only in emergencies such as when temporarily losing all login access. After you log in, create a superuser account in the usual way, then delete the local.superusers file or its contents. You must create a new administrator account for each individual, to track administrative changes.

Local and Regional Web UI

From the **Administration** menu, choose **Administrators**. This opens the List/Add Administrators page (see the "Create the Administrators" section on page 5-32 for an example). Enter a name and password, and choose one or more existing groups from the drop-down list (or whether the administrator should be a superuser), then click **Add Administrator**.

Edit an administrator by clicking its name on the List/Add Administrators page, then modifying the name, password, superuser status, or group membership on the Edit Administrator page. The active group or groups should be in the Selected list. Click **Modify Administrator**.

To delete an administrator, click the Delete icon () next to the name, then confirm or cancel the deletion.

CLI Commands

List the administrators by using **admin list** or **admin listnames**. Add administrators by using **admin** *name* **create** (see the **admin** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions). Delete an administrator by using **admin** *name* **delete**.

Managing Passwords

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

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

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

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

Managing Groups

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

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

Local Advanced and Regional Web UI

To add a group, do the following:

Step 1 From the **Administration** menu, choose **Groups**. This opens the List/Add Administrator Groups page (see the "Create a Group to Assign to the Host Administrator" section on page 5-37 for an example).

Step 2 Enter a name and optional description, and choose one or more existing roles from the drop-down list, then click **Add Group**.

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

To delete a group, click the Delete icon ( ) next to the name, and then confirm the deletion. Click **Cancel** in the confirmation window to cancel the deletion.

CLI Commands

To add groups, use **group** *name* **create** (see the **group** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Managing Roles

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

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

Local and Regional Advanced Web UI

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

Step 2 Enter a name and choose a base role from the drop-down list for the role, then click **Add Role**. The next page that opens varies based on the base role you choose for the role (for an example, see the "Create a Host Administrator Role with Constraints" section on page 5-35).

Step 3 On the Add *xxx* Administrator Role page, specify any role constraints, subrole restrictions, or group selections, then click **Add Role**.

Edit a role by clicking its name on the List/Add Administrator Roles page, then modifying the name or any constraints, subrole restrictions, or group selections on the Edit *xxx* Administrator Role page. The active subroles or groups should be in the Selected list. Click **Modify Role**.

To delete a role, click the **Delete** icon () next to the name, then confirm the deletion.

Note You can not delete the default roles.

CLI Commands

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

Managing Tenants

The multi-tenant architecture of Cisco Network Registrar provides the ability to segment the data stored on both regional and local clusters by tenant. When tenants are defined, data is partitioned by tenant in the embedded databases of each cluster. This provides data security and privacy for each tenant, while allowing cloud or managed service providers the flexibility to consolidate many smaller customer configurations on a set of infrastructure servers, or distribute a larger customer configuration across several dedicated servers.

Any given local cluster may be associated with one or more tenants, but within a local cluster, the address pools and domain names assigned to a given tenant must not overlap.

For larger customers, clusters may be explicitly assigned to a tenant. In this case, all data on the local cluster will be associated with the tenant, and may include customized server settings. Alternatively, infrastructure servers may service many tenants. With this model, the tenants can maintain their own address space and domain names, but share common server settings that would be administered by the service provider. Their use of public or private network addresses needs to be managed by the service provider, to ensure that the tenants are assigned non-overlapping addresses.

The following are the key points you should know while configuring tenants:

- Tenant administrators are linked to their data by a tenant object that defines their tenant tag and identifier.
- Tenant objects should be consistent and unique across all clusters.
- You should not reuse tags or identifiers for different tenants.
- You can configure multiple tenants on a single cluster.
- A tenant administrator cannot create, modify, or remove tenant objects.
- A tenant administrator cannot view or modify the data of another tenant.
- Objects that are not assigned to a tenant are defined as core data, and are visible to all tenants in read-only mode.

Adding a Tenant

To add a tenant, do the following:

Local and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Tenants**. This opens the List/Add Tenants page.

Step 2 Enter the Tenant tag and Tenant id and click **Add Tenant**. The Name and Description attributes are optional.

Note You cannot create more than one tenant with the same tenant id or tenant tag.

The View/Edit Tenant drop-down list is displayed in the Cisco Network Registrar Web UI when a tenant is defined.

You can use this drop-down list to select a tenant when you have to do tenant specific configurations.

CLI Commands

To add a tenant, use **tenant** *tag* **create** *tenant-id* (see the **tenant** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Editing a Tenant

To edit a tenant, do the following:

Local and Regional Advanced Web UI

Step 1 Click the name of the desired tenant on the List/Add Tenants page and the Edit Tenant appears.

Step 2 You can modify the tenant tag, name, or description of the tenant on the Edit Tenant page and click **Modify Tenant**. The tenant id cannot be modified.

Warning **Deleting the tenant will also delete all data for the tenant.**

To delete a tenant, click the **Delete** icon ( ) next to the name, then confirm the deletion.

Note A user constrained to a specific tenant cannot delete tenants.

Managing Tenant Data

You can create two types of data for tenants:

- Tenant data, which is assigned to a specified tenant and cannot be viewed by other tenants
- Core data, which is visible to all tenants in read-only mode

Local and Regional Web UI

To create tenant data objects in the Web UI, do the following:

Step 1 Set the View/Edit Tenant selection to the desired tenant.

Step 2 Create the object.

When creating tenant data, most object names are only required to be unique for the specified tenant. For example, tenants *abc* and *xyz* may both use their own scope *test* that is private to their configuration.

Note Administrators (Admin), zones (CCMZone, CCMReverseZone, and CCMSecondaryZone), keys (Key), and clients (ClientEntry) must be unique across all tenants.

Administrator names must be unique to perform initial login authentication and establish whether the user is a tenant. Zone and key classes must be unique because these require a DNS domain name that is expected to be unique across the Internet. Client names must correspond to a unique client identifier that the DHCP server can use to match its incoming requests.

Local and Regional Web UI

To create core data objects in the web UI, do the following:

Step 1 Ensure that you select **all** from the View/Edit Tenant drop-sown list.

Step 2 Create the object, leaving the object tenant assignment set to **none**. By default **none** is selected in the Tenant drop-down list. Leave it as it is, so that the object is not constrained to any specific tenant.

Core data can be used to provide common configuration elements such as policies or client classes that you choose to offer to tenants. Tenants can view and reference these objects in their configuration, but cannot change or delete them. Because core data is visible to all tenants, objects names must be unique across all tenants.

CLI Commands

Use **session set tenant=***tag* to set the selected tenant. Use **session unset tenant** to clear the tenant selection, if set (see the **session** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Note Once created, you cannot change the tenant or core designation for the object. You must delete and recreate the object to change its tenant assignment.

Tip You can use the cnr_exim tool to move a set of tenant data from one tenant to another.

Assigning a Local Cluster to a Single Tenant

When assigned to a single tenant, core data on the local cluster is not restricted to read-only access. This means tenants may be given the ability to stop and start servers, modify defaults, and install custom extensions. After the cluster is assigned to a specific tenant, other tenants cannot login to the cluster.

Note If synchronization with the local cluster fails, the cluster will not be assigned to the tenant. Resolve any connectivity issues and use the resynchronization icon to set the local cluster tenant.

Regional Web UI

To assign a local cluster to a single tenant, do the following:

Step 1 Add the tenant in the List/Add Tenant page if you want to assign the cluster to a new tenant (see "Adding a Tenant" section on page 5-10).

Step 2 Choose **Cluster List** from the **Clusters** menu. The List/Add Remote Clusters page is displayed.

Step 3 Choose the tenant you added in Step 1 from the View/Edit Tenant drop-down list below the main menu.

Step 4 Click **Add Cluster**. The **Add Remote Cluster** page is displayed.

Step 5 Add the cluster. For information on adding the cluster, see "Create the Local Clusters" section on page 5-40.

Note Once a cluster is assigned to a particular tenant, it cannot be changed or unset.

Pushing and Pulling Tenant Data

In the regional web UI, list pages include push options that let you distribute objects to a list of local clusters, and pull options that let you merge local cluster objects from the Replica data into the central configuration. These operations can be performed on both tenant and core data, but only one set of data can be pushed or pulled in a single operation.

Use the View/Edit Tenant drop-down selection list to specify the set of data to be pushed or pulled.

Note To maintain a consistent view of tenant data, all related clusters should be configured with the same list of tenants. See "Pushing and Pulling Tenants" section on page 5-30 for steps that help you manage tenant lists.

Assigning Tenants When Using External Authentication

When external RADIUS authentication is configured, the groups that are assigned in the RADIUS server configuration establish the access privileges of the user. The implicit group name ccm-tenant-*tag* or ccm-tenant-*id* must be added to the list of groups of tenant user to designate the tenant status. Other assigned groups must be core groups or groups assigned to the same tenant. Invalid groups will be ignored when building user credentials at login.

For example, to assign superuser access for the tenant *abc*, specify the groups attribute as:

```
cnr:groups=superusers,ccm-tenant-abc
```

See "External Authentication Servers" section on page 5-14.

Using cnr_exim With Tenant Data

The cnr_exim tool lets you export tenant data, and optionally re-assign the data to a different tenant on import (see "Using the cnr_exim Data Import and Export Tool" section on page 8-10). You can use these features to:

- Create a standard set of objects for each tenant
- Move tenant data to a new tenant

Note A user constrained to a specific tenant can only export or import data for that tenant.

Creating a Standard Set of Tenant Objects

You can use a standard set of tenant objects to provide common objects such as scope and zone templates, policies, and client classes. You can use these instead of core data objects to give tenants the option to customize their settings.

To create a standard set of tenant objects, do the following:

Step 1 Create a template tenant user to use as a placeholder, with tag=*template* and id=*9999*, and create the set of objects to be reused for each tenant.

Step 2 Use the cnr_exim tool to export the template configuration:

```
cnr_exim -f template -x -e template.bin
```

Step 3 Use the cnr_exim tool to import the template configuration for the tenant *abc*:

```
cnr_exim -f template -g abc -i template.bin
```

Note The template tenant user does not need to be present on the cluster to import the data, which lets you reuse the template.bin export file on other clusters. Once you have created the export file, you can also delete the placeholder tenant on the original cluster to remove all associated template data, if desired.

Moving Tenant Data

The id of a tenant can only be changed by deleting and re-creating the tenant. To retain the data of the tenant when this is required, do the following (assuming the tenant tag for the tenant is *xyz*):

Step 1 Use the cnr_exim tool to export the configuration for the tenant *xyz*:

```
cnr_exim -f xyz -x -e xyz.bin
```

Step 2 Delete the tenant *xyz*.

Step 3 Recreate the tenant with the corrected tenant id.

Step 4 Use the cnr_exim tool to re-import the configuration:

```
cnr_exim -f xyz -g xyz -i xyz.bin
```

External Authentication Servers

Cisco Network Registrar includes a RADIUS client component, which is integrated with the authentication and authorization module of the CCM server. To enable external authentication, you must configure a list of external RADIUS servers at local and regional clusters, and ensure all authorized users are appropriately configured on the RADIUS servers.

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

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

Tip If all logins fail because the RADIUS servers are inaccessible or misconfigured, use the local.superusers file to create a temporary username and password. See "Managing Administrators" section on page 5-6 for more details.

Configuring an External Authentication Server

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

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

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

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

```
cnr:groups=superusers
```

The superuser privileges override all other groups.

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

See Also

Adding an External Configuration Server
Deleting an External Authentication Server, page 5-16
Pushing and Pulling External Authentication Servers, page 5-25

Adding an External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional Web UI

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

Step 2 Enter the name and address of the server you want to configure as the external authentication server, and click **Add External Authentication Server**.

Step 3 Click the external authentication server name to open the Edit Authentication Server page.

Step 4 To enable the external authentication server, check **enabled** check box of the ext-auth attribute in the Edit Authentication Server page. You can set the key attribute which will be used for communicating with this server. CCM server uses this key to set the key-secret attribute which is the secret key shared by client and the server.

CLI Commands

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

Deleting an External Authentication Server

Local Advanced and Regional Web UI

To delete an external authentication server, click the Delete icon () next to the name and confirm the deletion. You can also cancel the deletion by clicking the Cancel button.

Granular Administration

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

Local Advanced and Regional Web UI

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

Step 2 Enter a name for the custom role, for example, **my-dhcp.**

Step 3 Choose **dhcp-admin** from the Base Role drop-down list.

Step 4 Click **Add Role** to open the Add DHCP Administrator Role page.

Step 5 Click **True** or **False** radio button as necessary, on the Add DHCP Administrator Role page.

Step 6 Choose the required sub roles in the Available field and move them to the Selected field.

Step 7 Click **Add Constraint**.

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

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

Step 8 Click **Add Role**.

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

See Also

Scope-Level Constraints, page 5-17
Prefix-Level Constraints, page 5-18
Link-Level Constraints, page 5-20

Scope-Level Constraints

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

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

The following conditions are also valid:

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

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

Examples of Scope-Level Constraints:

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

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

Local Advanced Web UI

To add scopes, do the following:

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

Step 2 Create a scope by adding its name, subnet, and possible template.

Step 3 Click **Add Scope**. The Add DHCP Scope page appears.

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

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

Step 6 Click **Add Scope** to add scope, or **Cancel** to cancel the changes.

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

Prefix-Level Constraints

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

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

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

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

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

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

Examples of Prefix-Level constraints:

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

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

Local Advanced and Regional Web UI

To view unified v6 address space, do the following:

Step 1 From the **Address Space v6** menu, choose **Address Tree** to open the View Unified v6 Address Space page.

Step 2 View a prefix by adding its name, address, and range, then choosing a DHCP type and possible template (see the "Viewing IPv6 Address Space" section on page 26-11).

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

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

Step 5 Click **Add Prefix**.The newly added Prefix appears on the View Unified v6 Address Space page.

To list or add prefixes, do the following:

Step 1 From **Address Space v6** menu, choose **Prefixes** to open the List Prefixes page.

Step 2 Enter the name, address, and range for the prefix, then choose the DHCP type and possible template.

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

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

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

To list or add DHCPv6 prefixes, do the following:

Step 1 From the **DHCPv6** menu, choose **Prefixes** to open the List/Add DHCPv6 Prefixes.

Step 2 Add a prefix by entering its name, address, and range, then choosing a DHCP type and possible template.

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

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

Step 5 Click **Add Prefix**.The newly added Prefix appears on the List/Add DHCPv6 Prefixes page.

Link-Level Constraints

You can view or modify a link if:

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

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

The following is an example of Link Level Constraints:

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

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

Local Advanced and Regional Web UI

To add links, do the following:

Step 1 From the **DHCPv6** menu, choose **Links** to open the List/Add DHCPv6 Links page.

Step 2 Enter the name, then choose the owner, region, and possible template to add a Link (see the "Viewing IPv6 Address Space" section on page 26-11).

Step 3 Enter value for Template Root Prefix.

Step 4 Click **Add Link**. The newly added DHCPv6 Link appears on the List/Add DHCPv6 Links page.

Licensing

Regional and local cluster operations require a feature **ip-node** license and possibly incremental additional node licenses. See the "Logging In to the Web UIs" section on page 2-2 for entering license data the first time you try to log in. You can add the additional ip-node licenses after you log in.

Local and Regional Web UI

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

The License Utilization section at the bottom of the page lists the type of license, the number of nodes allowed for the license, and the actual number of nodes used. Expand the section by clicking the plus (+) sign.

CLI Commands

Use **license** *file* **create** to create a license. The file referenced should include its absolute path or path relative to where you execute the commands. For example:

```
nrcmd> license "C:\licenses\ipnode-1.lic" create
```

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

Centrally Managing Administrators

As a regional or local CCM administrator, you can:

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

Each of these functions involves having at least one regional CCM administrator subrole defined. Table 5-3 describes the subroles required for these operations.

Table 5-3 Subroles Required for Central Administrator Management

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

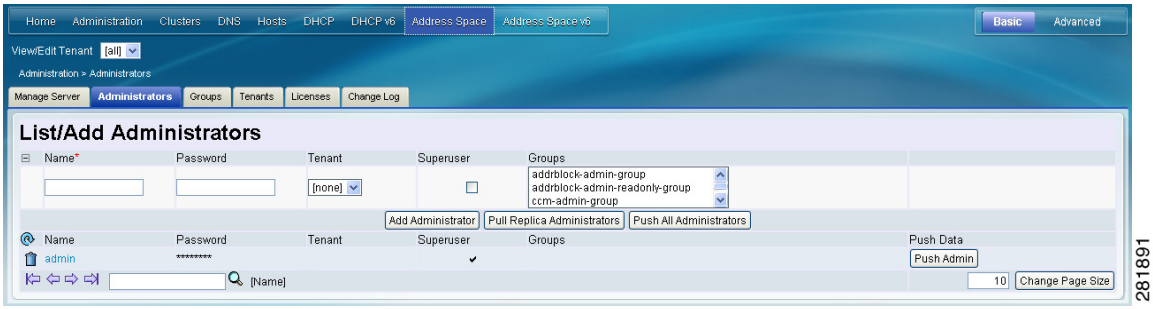
See Also

Pushing and Pulling Administrators
Pushing and Pulling External Authentication Servers, page 5-25
Pushing and Pulling Groups, page 5-26
Pushing and Pulling Roles, page 5-28
Pushing and Pulling Tenants, page 5-30

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 5-1).

Figure 5-1 List/Add Administrators Page (Regional)



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

See Also

Pushing Administrators to Local Clusters
Pushing Administrators Automatically to Local Clusters, page 5-23
Pulling Administrators from the Replica Database, page 5-24

Pushing Administrators to Local Clusters

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

Regional Basic and Advanced Web UI

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

Step 2 On the List/Add Administrators Page, click **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 by clicking one of the Data Synchronization Mode radio buttons. If you are pushing all the administrators, you can choose Ensure, Replace, or Exact. If you are pushing a single administrator, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing administrator data at the local cluster. You would choose Exact only if you want to create an exact copy of the administrator database at the local cluster, thereby deleting all administrators that are not defined at the regional cluster.

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

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

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

Pushing Administrators Automatically to Local Clusters

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

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

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

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Manage Servers** to open the Manage Servers page.

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

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

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

Step 5 Enter the idle-timeout value.

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

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

Connecting to CLI in Regional Mode

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

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

Pulling Administrators from the Replica Database

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

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

Regional Basic and Advanced Web UI

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

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 6-9.)

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 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.

Note If you do not have a regional cluster and would like to copy administrators, roles, or groups from one local cluster to another, you can export them and then reimport them at the target cluster by using the cnr_exim tool (see the "Using the cnr_exim Data Import and Export Tool" section on page 8-10). However, the tool does not preserve the administrator passwords, and you must manually reset them at the target cluster. It is implemented this way to maintain password security. The export command is:

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

Pushing and Pulling External Authentication Servers

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

Pushing External Authentication Servers

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

Regional Advanced Web UI

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

Step 2 Click **Push All External Authentication Servers** to push all the external authentication servers listed on the page, or **Push External Authentication Server** next to an individual external authentication server. This opens the Push Authentication 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 external authentication servers, you can choose Ensure, Replace, or Exact.
- If you are pushing a single external authentication server, you can choose Ensure or Replace.

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

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

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

Pulling External Authentication Servers

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

Regional Advanced Web UI

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

Step 2 On the List/Add Authentication Server page, click **Pull Replica External Authentication Server**. This opens the Select Replica Authentication 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 6-9.)

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

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

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

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

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

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

Pushing 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 Also

Pushing Groups to Local Clusters
Pulling Groups from the Replica Database, page 5-27

Pushing Groups to Local Clusters

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

Regional Basic and Advanced Web UI

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

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, uncheck the respective check box.

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

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

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

Pulling Groups from the Replica Database

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

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

Regional Basic and Advanced Web UI

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

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 6-9.)

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. You can also push associated groups and owners, and pull associated owners, depending on your subrole permissions (see Table 5-3 on page 5-21).

See Also

Pushing Roles to Local Clusters, page 5-28
Pulling Roles from the Replica Database, page 5-29

Pushing Roles to Local Clusters

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

Regional Advanced Web UI

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

Step 2 On the List/Add Administrator Roles page, click **Push All Roles** 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, uncheck the respective check box:

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

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

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

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

Pulling Roles from the Replica Database

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

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

Regional Advanced Web UI

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

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 6-9.)

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 Tenants

You can push all tenants to local cluster or pull the tenants data from the local cluster on the List/Add Tenants Page in the regional web UI.

Pushing Tenants to Local Clusters

To push tenants to the local cluster, do the following:

Regional Basic and Advanced Web UI

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

Step 2 Click **Push All Tenants** to push all the tenants listed on the page, or **Push Tenant** next to an individual tenant. This opens the Push Tenant 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 tenant, you can choose Ensure, Replace, or Exact.
- If you are pushing a single tenant, you can choose Ensure or Replace.

  In both cases, Ensure is the default mode.

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

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

Pulling Tenants from the Replica Database

To pull tenants from the replica database, do the following:

Regional Basic and Advanced Web UI

Step 1 From the **Administration** menu, choose **Tenants** to view the List/Add Tenants page.

Step 2 On the List/Add Tenants page, click **Pull Replica Tenant**. This opens the Select Replica Tenant 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 6-9.)

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

Leave the default Replace mode enabled, unless you want to preserve any existing tenant data at the local cluster by choosing Ensure.

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

Step 5 Click **Pull Replica Tenant**.

Step 6 On the Select Replica Tenant Data to Pull page, click Pull all Tenants view the pull details, then click **Run**.

On the Run Pull Replica Tenants page, view the change set data, then click **OK**. You return to the List/Add Tenants page with the pulled tenants added to the list.

Local Cluster Management Tutorial

This tutorial describes a basic scenario on a local cluster of the Example Company. Administrators at the cluster are responsible for users, zone data, DHCP data, address space data, and the servers in general. The task is to set up two zones (example.com and boston.example.com), hosts in the zones, and a subnet. The local cluster must also create a special administrator account so that the regional cluster in San Jose can perform the central configuration and replicate the local cluster administrators and address space at another cluster, as described in the "Regional Cluster Management Tutorial" section on page 5-38.

See Also

Administrator Responsibilities and Tasks
Create the Administrators, page 5-32
Create the Address Infrastructure, page 5-33
Create the Zone Infrastructure, page 5-33
Create a Host Administrator Role with Constraints, page 5-35
Create a Group to Assign to the Host Administrator, page 5-37
Test the Host Address Range, page 5-37

Administrator Responsibilities and Tasks

The local cluster administrators have the following responsibilities and tasks:

- **example-cluster-admin**—Created by the superuser:
  - At the Boston cluster, creates the other local administrators (example-zone-admin and example-host-admin).
  - Creates the basic network infrastructure for the local clusters.
  - Constrains the example-host-role to an address range in the boston.example.com zone.
  - Creates the example-host-group (defined with the example-host-role) that the example-zone-admin will assign to the example-host-admin.
- **example-zone-admin**:
  - Creates the example.com and boston.example.com zones, and maintains the latter zone.
  - Assigns the example-host-group to the example-host-admin.
- **example-host-admin**—Maintains local host lists and IP address assignments.

Create the Administrators

For this example, the superuser in Boston creates the local cluster, zone, and host administrators, as described in the "Administrator Responsibilities and Tasks" section.

Local Basic Web UI

Step 1 At the Boston local cluster, log in as superuser (usually **admin**).

Step 2 In Basic mode, from the **Administration** menu, choose **Administrators**.

Step 3 Add the local cluster administrator (with superuser access)—On the List/Add Administrators page:

a. Enter **example-cluster-admin** in the Name field. Tab to the next field.

b. Enter **exampleadmin** in the Password field.

c. Check the Superuser check box.

d. Do not choose a group from the Groups list

e. Click **Add Administrator**.

Step 4 Add the local zone administrator on the same page:

a. Enter **example-zone-admin** in the Name field, then **examplezone** in the Password field.

b. Multiselect **ccm-admin-group**, **dns-admin-group**, and **host-admin-group** in the Groups drop-down list. The dns-admin-group is already predefined with the dns-admin role to administer DNS zones and servers. The ccm-admin-group guarantees that the example-zone-admin can set up the example-host-admin with a constrained role later on. The host-admin-group is mainly to test host creation in the zone.

c. Click **Add Administrator**.

Step 5 Add the local host administrator on the same page:

a. Enter **example-host-admin** in the Name field, then **examplehost** in the Password field.

b. Do not choose a group at this point. (The example-zone-admin will later assign example-host-admin to a group with a constrained role.)

c. Click **Add Administrator**.

Note For a description on how to apply constraints to the administrator, see the "Create a Host Administrator Role with Constraints" section on page 5-35.

Create the Address Infrastructure

A prerequisite to managing the zones and hosts at the clusters is to create the underlying network infrastructure. The network configuration often already exists and was imported. However, this tutorial assumes that you are starting with a clean slate.

The local example-cluster-admin next creates the allowable address ranges for the hosts in the boston.example.com zone that will be assigned static IP addresses. These addresses are in the 192.168.50.0/24 subnet with a range of hosts from 100 through 200.

Local Advanced Web UI

Step 1 At the local cluster, log out as superuser, then log in as the **example-cluster-admin** user with password **exampleadmin**. Because the administrator is a superuser, all features are available.

Step 2 Click **Advanced** to go to Advanced mode, then **Address Space**, then **Subnets**.

Step 3 On the List/Add Subnets page, enter the boston.example.com subnet address:

- **a.** In the Address/Mask field, enter **192.168.50**.
- **b.** Choose **24** in the mask drop-down list—This subnet will be a normal Class C network.
- **c.** Leave the Owner, Region, and Address Type fields as is. Add descriptive text if desired.
- **d.** Click **Add Subnet**.

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

Step 5 In the IP Ranges fields, enter the static address range:

- **a.** Enter **100** in the Start field. Tab to the next field.
- **b.** Enter **200** in the End field.
- **c.** Click **Add IP Range**. The address range appears under the fields.

Step 6 Click **Modify Subnet**.

Step 7 Click **Address Space** to open the View Unified Address Space page. The 192.168.50.0/24 subnet should appear in the list. If not, click the Refresh icon ().

Create the Zone Infrastructure

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

See Also

Create the Forward Zones
Create the Reverse Zones, page 5-34
Create the Initial Hosts, page 5-35

Create the Forward Zones

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

Local Basic Web UI

Step 1 At the local cluster, log in as the **example-zone-admin** user with password **examplezone**.

Step 2 From example admin menu, choose **Forward Zones** to open the List/Add Zones page.

Step 3 Create the example.com zone (tab from field to field):

a. In the Name field, enter **example.com**.

b. In the Nameserver field, enter **ns1**.

c. In the Contact E-Mail field, enter **hostmaster**.

d. Click **Add Zone**.

Step 4 Create the **boston.example.com** zone in the same way, using the same values as in the previous steps:

a. Creating a zone with a prefix added to an existing zone opens the Create Subzone in Parent Zone page, because the zone can be a potential subzone. Because you do want to create this zone as a subzone to example.com, click **Create as Subzone** on the Create Subzone in Parent Zone page.

b. Because nameservers are different in each zone, you must create a glue Address (A) record to tie the zones together. Enter 192.168.50.1 in the A record field, then click **Specify Glue Records**. Then click **Report**, **Run**, and **Return**.

c. The List/Add Zones page should now list example.com and boston.example.com.

Step 5 Click **Advanced**, then **Show Forward Zone Tree** to show the hierarchy of the zones. Return to list mode by clicking **Show Forward Zone List**.

Create the Reverse Zones

Next, create the reverse zones for example.com and boston.example.com. This way you can add reverse address pointer (PTR) records for each added host. The reverse zone for example.com is based on the 192.168.50.0 subnet; the reverse zone for boston.example.com is based on the 192.168.60.0 subnet.

Local Basic Web UI

Step 1 At the local cluster, you should be logged in as the example-zone-admin user, as in the previous section.

Step 2 From the **DNS** menu, choose the **Reverse Zones** submenu.

Step 3 On the List/Add Reverse Zones page, enter **50.168.192.in-addr.arpa** in the Name field. (There is already a reverse zone for the loopback address, 127.in-addr.arpa.)

Step 4 Click **Add Zone** to open the Add Reverse Zone page.

Step 5 Enter the required fields to create the reverse zone, using the forward zone values:

a. **Nameserver**—Enter **ns1.example.com.** (be sure to include the trailing dot).

b. **Contact E-Mail**—Enter **hostmaster.example.com.** (be sure to include the trailing dot).

Step 6 Click **Add Zone** to add the zone and return to the List/Add Reverse Zones page.

Step 7 Do the same for the boston.example.com zone, using **60.168.192.in-addr.arpa** as the zone name and the same nameserver and contact e-mail values as in Step 5. (You can cut and paste the values from the table.)

Create the Initial Hosts

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

Local Advanced Web UI

Step 1 As the example-zone-admin user, click **Advanced** to enter Advanced mode.

Step 2 From the **Hosts** menu, choose **Zones** to open the List Zones page. You should see boston.example.com and example.com.

Step 3 Click example.com. in the list of zones.

Step 4 On the List/Add Hosts for Zone page, add the first static host with address 192.168.50.101:

a. Enter **userhost101** in the Name field.

b. Enter the complete address **192.168.50.101** in the IP Address(es) field. Leave the IPv6 Address(es) and Alias(es) field blank.

c. Ensure that the Create PTR Records? check box is checked.

d. Click **Add Host**.

Step 5 Add the second host, **userhost102**, with address **192.168.50.102**, in the same way. The two hosts should now appear along with the nameserver host on the List/Add Hosts for Zone page.

Create a Host Administrator Role with Constraints

In this part of the tutorial, the Boston example-cluster-admin creates the example-host-role with address constraints in the boston.example.com zone.

Local Advanced Web UI

Step 1 Log out as the example-zone-admin user and log in as the **example-cluster-admin** user (with password **exampleadmin**).

Step 2 Click **Advanced** to enter Advanced mode.

Step 3 From the **Administration** menu, choose **Roles** to open the List/Add Administrator Roles page.

Step 4 Add the example-host-role:

a. Enter **example-host-role** in the Name field.

b. From the Base Role drop-down list, choose **host-admin**.

c. Click **Add Role** to open the Add Host Administrator Role page.

Step 5 Add the constraint for the role:

a. Click **Add Constraint**.

b. On the Add Role Constraint for Role page, scroll down to Host Restrictions.

c. For the *all-forward-zones* attribute, click the **false** radio button.

d. For the *zones* attribute, enter **boston.example.com**.

e. For the *ipranges* attribute, enter the range **192.168.50.101–192.168.50.200**.

f. The *zone-regexpr* and *host-regexpr* attribute fields are for entering regular expressions to match zones and hosts, respectively, in regex syntax. (See Table 5-4 for the commonly used regex values.)

Table 5-4 Common Regex Values

Value	Matches
. (dot)	Any character (a wildcard). Note that to match a literal dot character (such as in a domain name), you must escape it by using a backslash (\), such that **\.com** matches .com.
char	Literal character (*char*) that follows, or the *char* has special meaning. Used especially to escape metacharacters such as the dot (**.**) or another backslash. Special meanings include **\d** to match decimal digits, **\D** for nondigits, **\w** for alphanumerics, and **\s** for whitespace.
*char***?**	Preceding *char* once or not at all, as if the character were optional. For example, **example\.?com** matches example.com or examplecom.
*char******	Preceding *char* zero or more times. For example, **ca*t** matches ct, cat, and caaat. This repetition metacharacter does iterative processing with character sets (see **[***charset***]**).
*char***+**	Preceding *char* one or more times. For example, **ca+t** matches cat and caaat (but not ct).
[*charset***]**	Any of the characters enclosed in the brackets (a character set). You can include character ranges such as **[a–z]** (which matches any lowercase character). With the ***** repetition metacharacter applied, the search engine iterates through the set as many times as necessary to effect a match. For example, **a[bcd]*b** will find abcbd (by iterating through the set a second time). Note that many of the metacharacters (such as the dot) are inactive and considered literal inside a character set.
[^*charset***]**	Anything but the *charset*, such that **[^a-zA-Z0-9]** matches any nonalphanumeric character (which is equivalent to using **\W**). Note that the caret outside a character set has a different meaning.
^	Beginning of a line.
$	End of a line.

g. Click **Add Constraint**. The constraint should have an index number of 1.

Step 6 Click **Add Role**. The example-host-role should now appear in the list of roles on the List/Add Administrator Roles page.

Create a Group to Assign to the Host Administrator

The Boston example-cluster-admin next creates an example-host-group that includes the example-host-role so that the example-zone-admin can assign this group to the example-host-admin.

Local Advanced Web UI

Step 1 As example-cluster-admin, still in Advanced mode, from the Administration menu, choose **Groups** submenu to open the List/Add Administrator Groups page.

Step 2 Create the example-host-group and assign the example-host-role to it:

a. Enter **example-host-group** in the Name field.

b. Add a description such as **Group for the example-host-role**.

c. From the Roles drop-down list, choose **example-host-role**.

d. Click **Add Group**.

e. Change the page size at the bottom of the page to **20**, then click **Change Page Size**, so that the newly created group appears in the list.

Step 3 Log out as example-cluster-admin, then log in as the **example-zone-admin** user (with password **examplezone**).

Step 4 As example-zone-admin, assign the example-host-group to the example-host-admin:

a. In Basic mode, from the **Administration** menu, choose **Administrators**.

b. On the List/Add Administrators page, click example-host-admin to edit the administrator.

c. On the Edit Administrator page, choose **example-host-group** in the Available list, then click **<<** to move it to the Selected list.

d. Click **Modify Administrator**. The example-host-admin should now show the example-host-group in the Groups column on the List/Add Administrators page.

Test the Host Address Range

The example-host-admin next tests an out-of-range address and then adds an acceptable one.

Local Advanced Web UI

Step 1 At the local cluster, log out as example-zone-admin, then log in as **example-host-admin** (with password **examplehost**).

Step 2 Click **Advanced** to enter Advanced mode.

Step 3 From the **Hosts** menu, choose Hosts.

Step 4 On the List/Add Hosts for Zone page, try to enter an out-of-range address (note the range of valid addresses in the Valid IP Ranges field):

a. Enter **userhost3** in the Name field.

b. Deliberately enter an out-of-range address (**192.168.50.3**) in the IP Address(es) field.

c. Click **Add Host**. You should get an error message.

Step 5 Enter a valid address:

a. Enter **userhost103**.

b. Enter **192.168.50.103** in the IP Address(es) field.

c. Click **Add Host**. The host should now appear with that address in the list.

Regional Cluster Management Tutorial

This tutorial is an extension of the scenario described in the "Local Cluster Management Tutorial" section on page 5-31. In the regional cluster tutorial, San Jose has two administrators—a regional cluster administrator and a central configuration administrator. Their goal is to coordinate activities with the local clusters in Boston and Chicago so as to create DNS zone distributions, router configurations, and DHCP failover configurations using the servers at these clusters. The configuration consists of:

- One regional cluster machine in San Jose.
- Two local cluster machines, one in Boston and one in Chicago.
- One Cisco uBR7200 router in Chicago.

See Also

Administrator Responsibilities and Tasks, page 5-38
Create the Regional Cluster Administrator, page 5-39
Create the Central Configuration Administrator, page 5-39
Create the Local Clusters, page 5-40
Add a Router and Modify an Interface, page 5-41
Add Zone Management to the Configuration Administrator, page 5-42
Create a Zone for the Local Cluster, page 5-42
Pull Zone Data and Create a Zone Distribution, page 5-43
Create a Subnet and Pull Address Space, page 5-44
Push a DHCP Policy, page 5-44
Create a Scope Template, page 5-45
Create and Synchronize the Failover Pair, page 5-45

Administrator Responsibilities and Tasks

The regional administrators have the following responsibilities and tasks:

- **example-regional-admin**—Created by the superuser at the San Jose regional cluster, who creates the example-cfg-admin.
- **example-cfg-admin**:
  - Defines the Boston and Chicago clusters and checks connectivity with them.
  - Adds a router and modifies a router interface.
  - Pulls zone data from the local clusters to create a zone distribution.
  - Creates a subnet and policy, and pulls address space, to configure DHCP failover pairs in Boston and Chicago.

Create the Regional Cluster Administrator

The regional superuser first creates the example-regional-administrator, defined with groups, to perform cluster and user administration.

Regional Web UI

Step 1 Log in to the regional cluster as superuser.

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

Step 3 Enter **example-regional-admin** in the Name field, then **examplereg** in the Password field.

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

Step 5 Click **Add Administrator**.

Create the Central Configuration Administrator

As part of this tutorial, the example-regional-admin next logs in to create the example-cfg-admin, who must have regional configuration and address management capabilities.

Regional Web UI

Step 1 Log out as superuser, then log in as **example-regional-admin** with password **examplereg**. Note that the administrator has all but host and address space administration privileges.

Step 2 From the **Administration** menu, choose **Administrators** to open the List/Add Administrators page.

Step 3 Enter **example-cfg-admin** in the Name field, then **cfgadmin** in the Password field.

Step 4 Multiselect **central-cfg-admin-group** and **regional-addr-admin-group** in the Groups drop-down list.

Step 5 Click **Add Administrator**. The example-cfg-admin now appears with the two groups assigned.

You can also add constraints for the administrator. Click **Add Constraint** and, on the Add Role Constraint for Role page, choose the read-only, owner, or region constraints, then click **Add Constraint**.

Create the Local Clusters

The example-cfg-admin next creates the two local clusters for Boston and Chicago.

Regional Web UI

Step 1 Log out as example-regional-admin, then log in as **example-cfg-admin** with password **cfgadmin**.

Step 2 From the **Clusters** menu, choose **Cluster List**.

Step 3 On the List/Add Remote Clusters page, click **Add Cluster**.

Step 4 On the Add Cluster page, create the Boston cluster based on data provided by its administrator:

a. Enter **Boston-cluster** in the name field.

b. Enter the IP address of the Boston server in the ipaddr field.

c. Enter **example-cluster-admin** in the admin field, then **exampleadmin** in the password field.

d. Enter in the scp-port field the SCP port to access the cluster as set at installation (**1234** is the preset value).

e. Enter in the http-port field the HTTP port to access the cluster (**8080** is the preset value).

f. Click **Add Cluster**.

Step 5 Create the Chicago cluster in the same way, except use **Chicago-cluster** in the name field, enter the remaining values based on data provided by the Chicago administrator, then click **Add Cluster**. The two clusters should now appear on the List/Add Remote Clusters page.

Step 6 Connect to the Boston cluster. Click the Go Local icon () next to Boston-cluster. If this opens the local cluster Manage Servers page, this confirms the administrator connectivity to the cluster. To return to the regional cluster web UI, click the Go Regional icon ().

Step 7 Connect to the Chicago cluster to confirm the connectivity in the same way.

Step 8 Confirm that you can replicate data for the two forward zones from the Boston cluster synchronization:

a. Choose **Replica Data** from the **Clusters** menu.

b. On the View Replica Class List page, click Boston-cluster in the Select Cluster list.

c. In the Select Class list, click **Forward Zones**.

d. Click the Replicate icon () in the Replicate Data column.

e. Click **View Replica Class List**. On the List Replica Forward Zones for Cluster page, you should see the boston.example.com and example.com zones.

Add a Router and Modify an Interface

The example-cfg-admin next takes over at the regional cluster to add a router and modify one of its interfaces to configure the DHCP relay agent. 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 when you add additional address space. (Because the routers define the physical network, it is preferable to save these definitions as opposed to saving those possibly conflicting definitions present in the DHCP configuration.)

Regional Web UI

Step 1 As example-cfg-admin, from the **Routers** menu, choose **Router List**.

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

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

a. Give the router a distinguishing name in the name field. For this example, enter **router-1**.

b. Because this router is a Cisco uBR7200 router, choose **Ubr72xx** in the Router Type drop-down list.

c. Enter the router IP address in the address field.

d. Enter the router administrator username in the username field.

e. Enter the router administrator enable password in the enable field.

f. Click **Add Router**. The router should now appear on the List/Add Routers page.

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

Step 5 Configure a DHCP relay agent for the router:

a. Click one of the interface names on the View Tree of Routers page to open the Edit Router Interface page. (Alternatively, from the List/Add Routers page, click the Interfaces icon () associated with the router, then click the interface name on the List Router Interfaces for Router page.)

b. On the Edit Router Interface page, enter the IP address of the DHCP server in the ip-helper field.

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

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

Add Zone Management to the Configuration Administrator

Because there are no zones set up at the Chicago cluster, the example-cfg-admin can create a zone at the regional cluster to make it part of the zone distribution. However, the example-regional-admin must first modify the example-cfg-admin to be able to create zones.

Regional Web UI

Step 1 Log out as example-cfg-admin, then log in as **example-regional-admin**.

Step 2 From the **Administration** menu, choose **Administrators**.

Step 3 On the List/Add Administrators page, click example-cfg-admin.

Step 4 On the Edit Administrator page, click central-dns-admin-group in the Groups Available list, then move it (using **<<**) to the Selected list. The Selected list should now have central-cfg-admin-group, regional-addr-admin-group, and central-dns-admin-group.

Step 5 Click **Modify Administrator**. The change should be reflected on the List/Add Administrators page.

Create a Zone for the Local Cluster

The example-cfg-admin next creates the chicago.example.com zone for the zone distribution with the Boston and Chicago zones.

Regional Web UI

Step 1 Log out as example-regional-admin, then log in as **example-cfg-admin**.

Step 2 From the **DNS** menu, choose **Forward Zones**.

Step 3 On the List Forward Zones page, enter **chicago.example.com** in the Name field.

Step 4 Click **Add Zone**.

Step 5 On the Add Zone page, enter:

a. **Serial Number—1**.

b. **Nameserver—ns1**.

c. **Contact E-mail—hostmaster**.

d. **Nameservers—ns1** (click **Add Nameserver**).

e. Click **Add Zone**.

Step 6 Click the **Reverse Zones** submenu.

Step 7 On the List Reverse Zones page, create the **60.168.192.in-addr.arpa** reverse zone for the Chicago zone, with the proper attributes set.

Pull Zone Data and Create a Zone Distribution

The example-cfg-admin next pulls zone data from Boston and Chicago and creates a zone distribution.

Regional Web UI

Step 1 As example-cfg-admin, from the **DNS** menu, choose **Zone Distributions** to view the List/Add Zone Distributions page.

Step 2 On the List/Add Zone Distributions page, pull the zone from the replica database:

a. Click **Pull Replica Zone Data**.

b. On the Select Pull Replica Zone Data page, leave the Data Synchronization Mode defaulted as Update, then click **Report** to open the Report Pull Replica Zone Data page.

c. Notice the change sets of data to pull, then click **Run**.

d. On the Run Pull Replica Zone Data page, click **OK**.

Step 3 On the List/Add Zone Distributions page, notice that the Boston cluster zone distribution is assigned an index number (**1**) in the Name column. Click the number.

Step 4 On the Edit Zone Distribution page, in the Primary Server field, click Boston-cluster. (The IP address of the Boston-cluster becomes the first master server in the Master Servers list.)

Step 5 Because we want to make the Chicago-cluster DNS server a secondary server for the Boston-cluster:

a. Click **Add Server** in the Secondary Servers area.

b. On the Add Zone Distribution Secondary Server page, choose **Chicago-cluster** in the Secondary Server drop-down list.

c. Click **Add Secondary Server**.

Step 6 On the Edit Zone Distribution page, in the Forward Zones area, move **chicago.example.com** to the Selected list.

Step 7 In the Reverse Zones area, move **60.168.192.in-addr.arpa** to the Selected list.

Step 8 Click **Modify Zone Distribution**.

Create a Subnet and Pull Address Space

The example-cfg-admin next creates a subnet at the regional cluster. This subnet will be combined with the other two pulled subnets from the local clusters to create a DHCP failover server configuration.

Regional Web UI

Step 1 As example-cfg-admin, from the **Address Space**, choose **Subnets** 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 5-41).

Step 2 Create an additional subnet, 192.168.70.0/24:

a. Enter **192.168.70** (the abbreviated form) as the subnet network address in the Address/Mask field.

b. Leave the **24** (255.255.255.0) selected as the network mask.

c. Click **Add Subnet**.

Step 3 Click **Address Space** to confirm the subnet you created.

Step 4 On the View Unified Address Space page, click **Pull Replica Address Space**.

Step 5 On the Select Pull Replica Address Space page, leave everything defaulted, then click **Report**.

Step 6 The Report Pull Replica Address Space page should show the change sets for the two subnets from the clusters. Click **Run**.

Step 7 Click **OK**. The two pulled subnets appear on the List/Add Subnets page.

Push a DHCP Policy

The example-cfg-admin next creates a DHCP policy, then pushes it to the local clusters.

Regional Web UI

Step 1 As example-cfg-admin, from the **DHCP** menu, choose **Policies**.

Step 2 On the List/Add DHCP Policies page, click **Add Policy**.

Step 3 On the Add DHCP Policy page, create a central policy for all the local clusters:

a. Enter **central-policy-1** in the Name field. Leave the offer timeout and grace period values as is.

b. Enter a lease period. In the DHCPv4 Options drop-down list, choose **dhcp-lease-time [51] (unsigned time)**, then enter **2w** (two weeks) for the lease period in the Value field.

c. Click **Add Option**.

d. Click **Add Policy**. The central-policy-1 should appear on the List/Add DHCP Policies page.

Step 4 Push the policy to the local clusters:

a. Click **Push Policy** next to central-policy-1.

b. On the Push DHCP Policy Data to Local Clusters page, leave the Data Synchronization Mode as **Ensure**. This ensures that the policy is replicated at the local cluster, but does not replace its attributes if a policy by that name already exists.

c. Click **Select All** in the Destination Clusters section of the page.

d. Click **<<** to move both clusters to the Selected field.

e. Click **Push Data to Clusters**.

f. View the push operation results on the View Push DHCP Policy Data Report page, then click **OK**.

Create a Scope Template

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

Regional Web UI

Step 1 As the example-cfg-admin user, from the **DHCP** menu, choose **Scope Templates**.

Step 2 On the List DHCP Scope Templates page, click **Add Scope Template**.

Step 3 Set the basic properties for the scope template—Enter or choose the following values in the fields:

a. **Name**—Enter **scope-template-1**.

b. **Scope Name Expression**—To autogenerate names for the derivative scopes, concatenate the example-scope string with the subnet defined for the scope. To do this, enter **(concat "example-scope-" subnet)** in the field (including the parentheses).

c. **Policy**—Choose **central-policy-1** in the drop-down list.

d. **Range Expression**—Create an address range based on the remainder of the subnet (the second through last address) by entering **(create-range 2 100)**.

e. **Embedded Policy Option Expression**—Define the router for the scope in its embedded policy and assign it the first address in the subnet by entering **(create-option "routers" (create-ipaddr subnet 1))**.

Step 4 Click **Add Scope Template**. The template should appear on the List DHCP Scope Templates page.

Create and Synchronize the Failover Pair

The example-cfg-admin next creates the failover server pair relationship and synchronizes the failover pair. The DHCP server at Boston becomes the main, and the server at Chicago becomes the backup.

Regional Web UI

Step 1 As the example-cfg-admin user, from the **DHCP** menu, choose the **Failover** submenu from the drop-down list.

Step 2 On the List/Add DHCP Failover Pairs page, click **Add Failover Pair**.

Step 3 On the Add DHCP Failover Pair page, enter or choose the following values:

a. **Failover Pair Name**—Enter **central-fo-pair**.

b. **Main Server**—Click **Boston-cluster**.

c. **Backup Server**—Click **Chicago-cluster**.

d. **Scope Template**—Click **scopetemplate-1**.

e. Click **Add Failover Pair**.

Step 4 Synchronize the failover pair with the local clusters:

a. On the List/Add DHCP Failover Pairs page, click the Report icon () in the Synchronize column.

b. On the Report Synchronize Failover Pair page, accept **Local Server** as the source of network data.

c. Accept **Main to Backup** as the direction of synchronization.

d. Accept the operation **Update**.

e. Click **Report** at the bottom of the page.

f. On the View Failover Pair Sync Report page, click **Run Update**.

g. Click **Return**.

Step 5 Confirm the failover configuration and reload the server at the Boston cluster:

a. On the List/Add DHCP Failover Pairs page, click the Go Local icon () next to Boston-cluster.

b. On the Manage DHCP Server page, click the Reload icon ().

c. Click the Go Regional icon () at the top of the page to return to the regional cluster.

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