



# Managing Zones

The Domain Name System (DNS) is a distributed database for objects in a computer network. By using a nameserver approach, the network consists of a hierarchy of autonomous domains and zones. The namespace is organized as a tree that often resembles the organizations that are responsible for the administration boundaries. For an introduction to the protocol, see the “[Domain Name System and Zone Administration](#)” section on page 2-1.

The basic function of DNS nameservers is to provide data about network objects by answering queries. You can configure the Cisco CNS Network Registrar DNS server and zones by accepting the system defaults or changing them.

This chapter describes the basics of configuring the Network Registrar DNS servers, and their primary and secondary zones. [Chapter 9, “Managing Resource Records and Hosts,”](#) describes how to manage DNS resource records and hosts, and [Chapter 10, “Setting DNS Attributes,”](#) describes how to set some of the more advanced zone and DNS server properties.

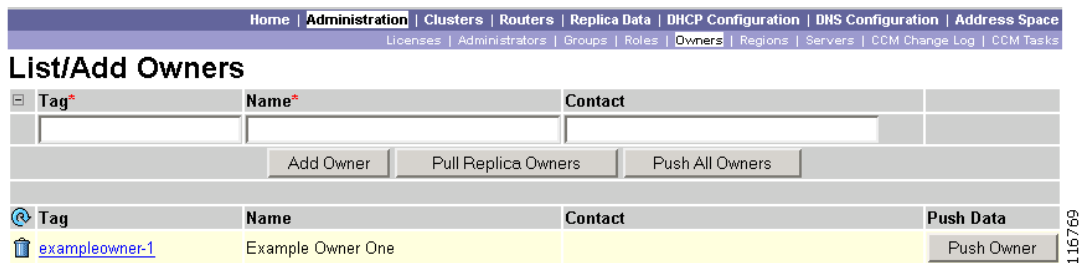
## Managing Zone Owners

Creating zone owners creates a pick list of owners when you create a zone. Each zone can have an owner. You can list and add zone owners on a single page. Creating a zone owner involves creating an owner tag name, full name, and a contact name. Creating owners is available only in the Web UI.

In both the local and regional cluster Web UIs, the access is the same:

- Step 1** On the Primary Navigation bar, click **Administration**.
- Step 2** On the Secondary Navigation bar, click **Owners** to open the List/Add Owners page (see [Figure 8-1](#) for the regional cluster example that also includes pull and push functions).

**Figure 8-1 List/Add Owners Page**



- Step 3** Enter a unique owner tag.
  - Step 4** Enter an owner name.
  - Step 5** Enter an optional contact name.
  - Step 6** Click **Add Owner**.
  - Step 7** To edit a zone owner, click its name to open the Edit Owners page.
- 

## Creating and Applying Zone Templates

A zone template is a convenient way to create a boilerplate for primary zones that share many of the same attributes. You can apply a zone template to any zone, and override the zone's attributes with those of the template. You can create zone templates in the local and regional cluster Web UIs.

- Step 1** Access the List Zone Templates page:
- In the local cluster Web UI—On the Primary Navigation bar, click **Zone**, then click **Zone Templates** on the Secondary Navigation bar.
  - In the regional cluster Web UI—On the Primary Navigation bar, click **DNS Configuration**, then click **Zone Templates** on the Secondary Navigation bar (see [Figure 5-17 on page 5-32](#)).


- Step 2** You can add a zone template on the local and regional clusters, and you can also pull and push zone templates on the regional cluster:
- To add a zone template at the local cluster or explicitly add one on the regional cluster—Click **Add Zone Template**. This opens the Add Zone Template page, which is almost identical to the Add Zone page for the local cluster (see [Figure 4-8 on page 4-18](#)).

To make the zone template meaningful, you would enter, in addition to its name, at least the suggested serial number, nameserver, and contact E-mail address, because they are required for the zone itself. You might also want to specify any zone owners or zone distributions. You do not necessarily need to add these values for the zone template, because you can do so for the zone once it is created from the template. However, the template name and zone default TTL are required. (For a description of the minimally required zone attributes, see the “[Creating Primary Zones](#)” section on [page 8-4](#).)

Once you are done entering these value, click **Add Zone Template** at the bottom of the page.

- On the regional cluster, to pull a zone template from one or more local clusters—Click **Pull Replica Zone Templates** on the List Zone Templates page. This opens the Select Replica DNS Zone Template Data to Pull page (see [Figure 5-19 on page 5-34](#)).

This page shows a tree view of the regional server's replica data for the local clusters' zone templates. The tree has two levels, one for the local clusters and one for the templates in each cluster. You can pull individual templates from the clusters, or you can pull all of their templates:

- To pull individual zone templates, expand the tree for the cluster, choose a pull criteria next to its name, then click **Pull VPN**.
- To pull all the templates from a cluster, choose a pull criteria, then click **Pull All Zone Templates from Cluster**.
- To update all the replica data for a cluster, click the Replica icon () next to its name.

The pull selection criteria are:

- **Ensure**—Pulls each template, except if an existing template by that name already exists at the regional cluster, in which case it does not overwrite the regional cluster data.
  - **Replace**—Pulls each template and overwrites the data for it if it already exists at the regional cluster, without affecting any additional templates at the regional cluster. This is the default and recommended setting.
  - **Exact**—Pulls each template, overwrites the data for it if it already exists at the regional cluster, and removes any additional templates at the regional cluster.
- On the regional cluster, to push a zone template to one or more local clusters:
    - To push all the zone templates on the page List Zone Templates page—Click **Push All Zone Templates**.
    - To push individual zone templates on the page List Zone Templates page—Click **Push Zone Template** next to the template name.

Both of these actions open a version of the Push Zone Template Data to Local Clusters page (see [Figure 5-18 on page 5-33](#)).

This page provides a choice of the synchronization mode and the destination clusters. Move the desired cluster or clusters from the Available field to the Selected field, then click one of the data synchronization mode radio buttons:

- **Ensure**—Pushes each template, except if an existing template by that name already exists at the local cluster, in which case it does not overwrite the local cluster data. This is the default and recommended setting.
- **Replace**—Pushes each template and overwrites the data for it if it already exists at the local cluster, without affecting any additional templates at the local cluster.
- **Exact**—Available for individual zone template pushes only, it pushes each template, overwrites the data for it if it already exists at the local cluster, and removes any additional templates at the local cluster.

After making these choices, click **Push Data to Clusters**. This opens the View Push Zone Template Data Report page, where you can view the intended results of the push operation. Click **OK** to implement the push operation.

---

## Managing Primary DNS Servers

Adding a zone involves creating a domain name. You can also define an owner and use a zone template. If you do not use a template, you must also define the Start of Authority (SOA) and Name Server (NS) properties for the zone.

You do not need to create a loopback zone for the local host, because Network Registrar automatically creates one. A loopback zone is a reverse zone that a host uses to resolve its loopback address, 127.0.0.1, to localhost so that it can direct network traffic to itself. The reverse loopback zone is 127.in-addr.arpa. (If you inadvertently delete the loopback zone, see the Usage Guidelines for the **zone** command in the *Network Registrar CLI Reference*.)

## Adding Primary Forward Zones

This section explains how to configure a primary nameserver with a primary forward zone. When you are done with this procedure, follow the procedure in the [“Adding Primary Reverse Zones”](#) section on page 8-9 to configure a reverse zone for each network that you use.

### Creating Primary Zones

The first thing in creating a forward zone is to give the zone a name and set its Start of Authority (SOA) resource records. The SOA record designates the top of the zone in the DNS inverted-tree namespace. A zone can have only one SOA record, which sets these primary zone properties:

- SOA time to live (TTL)—*soattl*
- Primary server name—*ns*
- Hostmaster (person in charge) name—*person*
- Serial number—*serial*
- Secondary refresh time—*refresh*
- Secondary retry time—*retry*
- Secondary expire time—*expire*
- Minimum TTL—*minttl*

In the local cluster Web UI:

- 
- Step 1** On the Primary Navigation bar, click **Zone**.
  - Step 2** On the Secondary Navigation bar, click **Forward Zones** to open the List/Add Zones page (see [Figure 4-7 on page 4-17](#)).
  - Step 3** Enter the zone name (in domain name format).
  - Step 4** Optionally choose a predefined owner or zone template.
  - Step 5** Click **Add Zone** to open the Add Zone page.
- 

In the CLI, use the **zone name create primary** command.

For now, add only the serial number, primary server, and hostmaster data for the zone’s Start of Authority (SOA) record:

- 
- Step 1** Enter the *serial number*.

A primary DNS server uses a serial number to indicate when its database changes and uses any incrementing of this number to trigger a zone transfer to a secondary server. The serial number you can enter here is the *suggested* one only, and the DNS server does not always accept it. If you edit the serial number to be less than the actual serial number that the server maintains, the server logs a warning message and ignores the suggested serial number. You must reload the server for your change to take effect. The actual serial number always equals or is higher than the suggested one. You can get the actual serial number by using the **zone name get serial** command (if the DNS server is running; if the server is not running, or listing or showing the zone attributes, always returns the suggested serial number), or by

refreshing the DNS Server Value for the zone Serial Number attribute in the Web UI. In the Web UI, you must explicitly enter this suggested serial number when creating a zone. In the CLI, the serial number defaults to 1.

**Step 2** Enter the *primary DNS server* name.

Enter either just the host name (such as *exampleDNSserv1*) or its fully qualified name (such as *exampleDNSserv1.example.com.*, ending with a trailing dot). Use the fully qualified name if the primary nameserver is in a different zone. The primary DNS server becomes the *ns* value in the zone's SOA record. In the Web UI, you must also specify one or more authoritative nameservers for the zone—these become the Name Server (NS) records for the zone. In the CLI, the primary DNS server automatically becomes the first NS record and also appears as the first entry in the *nameservers* attribute list.

**Step 3** Enter the *hostmaster* (person in charge's) name and address as a slightly altered form of the e-mail address.

Substitute a dot (.) for the “at” symbol (@), and end the address with a trailing dot (for example, enter *hostmaster@example.com* as *hostmaster.example.com.*). Escape any dot before the “@” in the original address with a backslash (\) (for example, enter *hostmaster.marketing@example.com* as *hostmaster\marketing.example.com.*).

---

In the Web UI, do not click **Add Zone** yet. You must still enter the authoritative nameservers for the zone.

## Adding Authoritative Nameservers for Zones

Authoritative nameservers validate the data in their zones. Both primary and secondary servers can be authoritative. The crucial difference is where they get their zone data. A primary server obtains its data from an administrator, as stored in the server's configuration database, and from dynamic updates typically from a DHCP server. A secondary server obtains the zone data from its designated master servers by way of a zone transfer.

You must add at least one nameserver for a zone—Network Registrar does not consider the zone data complete unless you do so. The nameservers you list should be those that you want people outside your domain to query when trying to resolve names in your zone. In the CLI, creating a primary zone requires specifying a primary DNS server—this server becomes the first entry in the nameserver list. In the Web UI, you must add the authoritative nameservers in addition to the primary server for the zone. If the primary DNS server for the zone is in the zone, you must create a host address for it—see the [“Adding Host Addresses for Nameservers”](#) section on page 8-6.

In the Web UI:

---

- Step 1** On the Add Zone page, enter the name of an authoritative nameserver (either as host name or fully qualified, if in another zone) in the field next to the Add Nameserver button.
  - Step 2** Click **Add Nameserver**.
  - Step 3** Repeat this for each additional nameserver you add.
  - Step 4** Unless you want to add additional attributes for the zone, you can now click **Add Zone**.
-

In the CLI, enter a comma-separated list using the `zone name set nameservers=list` command. Enter them as a comma-separated list of fully qualified domain names. Note that only the first server entered is confirmed by the command. Use the `zone name show` command to show all the server names. Then reload the server.

## Adding Host Addresses for Nameservers

For every DNS nameserver for the zone, you must create an Address (A) resource record for it to associate the server's domain name with an IP address.

In the local cluster Web UI:

- 
- Step 1** Create the zone, as described in the “Adding Primary Forward Zones” section on page 8-4.
  - Step 2** On the Primary Navigation bar, click **Host** to open the List Zones page.
  - Step 3** Click the zone name to open the List/Add Hosts for Zone page.
  - Step 4** Enter the host name.
  - Step 5** Enter the IP address of the authoritative server.
  - Step 6** Click **Add Host**. The server's host name and address appear in the list.
- 

In the CLI, use the `zone name addRR hostname A address` command to add the authoritative server's host name and address. To list the host, use the `zone name listHosts` command. To remove the host, use the `zone name removeRR hostname A` command.

## Creating Zone Templates from Zones

You can save zone information as a template so that you can re-use it for other zones. You do this from the Edit Zone page in the local cluster Web U.

- 
- Step 1** Click **Modify Zone and Save Template** after you modify the zone information.
  - Step 2** On the Save New Zone Template page (see [Figure 8-2](#)), give the template a name in the Value field.
  - Step 3** Click **Save Zone Template**. You return to the List/Add Zones page.

**Figure 8-2 Save New Zone Template Page**

Attribute	Value
New Template Name	example-zone-template

Save Zone Template Cancel

## Confirming Zone Nameservers

Confirm your zone's NS resource record configuration by looking at the resource records that you created.

In the Web UI, click the View icon (🔍) in the Configuration RRs column of the zone name on the List/Add Zones page to open the List/Add Static Resource Records for Zone page. There should be an A record for each nameserver host in the zone. Edit these records or add more on this page.

In the CLI, use the `zone name listRR` command to check the resource records you added. To activate the records, you must reload the DNS server.

## Importing and Exporting Zone Data

The easiest and quickest way to create a primary zone is to import an existing BIND format zone file, defined in RFC 1035. You can also export these same kinds of files to another server. BIND 4.x.x uses a boot file, called `named.boot`, to point the server to its database files. You can import your entire BIND 4.x.x configuration using the `import` command. BIND 8 and BIND 9 use a configuration file, called `named.config`, with a different syntax.

You can import and export zone data only by using the CLI.

When a BIND file contains an `$INCLUDE` directive, BIND searches for the include file relative to the directory that the `directory` directive in the `named.boot` file specifies. In contrast, the `nrcmd` program searches for the include file relative to the directory containing the zone file being processed.

To avoid this problem, ensure that the BIND configuration uses absolute paths whenever specifying an include file in a zone file. If your zone files contain relative paths when specifying include files, and the directory containing the zone file is not the same as the directory that the `directory` directive in the `named.boot` file specifies, your configuration cannot load properly. You need to convert the relative paths in your zone files to absolute paths so that you can import your BIND configuration into Network Registrar. Here is an example of a configuration and how to fix paths in directory hierarchy, configuration files, and zone files:

- Directory hierarchy:

```
/etc/named.conf
/etc/named.boot
/usr/local/domain/primary/db.example
/usr/local/domain/primary/db.include
/usr/local/domain/secondary
```

- Configuration file (`/etc/named.conf`):

```
#BIND searches for zone files and include files relative to /usr/local/domain
option directory /usr/local/domain
#BIND finds zone file in /usr/local/domain/primary
zone example.com {
    type master ;
    file primary/db.example ;
#end of /etc/named.conf
```

- Configuration file (`/etc/named.boot`):

```
#BIND searches for zone files and include files relative to /usr/local/domain
directory /usr/local/domain
#BIND finds zone file in /usr/local/domain/primary
primary example.com primary/db.example
#end of /etc/named.boot
```

- Incorrect zone file (/usr/local/domain/primary/db.example):

```
#BIND searches for include file relative to /usr/local/domain
$INCLUDE primary/db.include
#end of /usr/local/domain/primary/db.example
```

To make the configuration loadable, change the relative path (\$INCLUDE primary/db.include) in the file db.example to an absolute path (\$INCLUDE /usr/local/domain/primary/db.include).

Table 8-1 describes the named.boot and named.conf file directives that BIND 4 and BIND 9 support, and the corresponding Network Registrar user interface location or syntax, if any.

**Table 8-1 BIND-to-CLI Command Mappings**

BIND 4 Command	BIND 9 Command	Mapping to User Interface
—	<code>acl name { addr-match-list };</code>	Web UI: List/Add Access Control Lists page fields (see the “ <a href="#">Transaction Security and Access Control Lists</a> ” section on page 15-3). CLI: <b>acl name create value match-list=addr-match-list</b>
<code>forwarders addrlist</code>	<code>options { forwarders { addr; addr;... } };</code>	Web UI: Edit DNS Server page, set Forwarders: IP Address field. CLI: <b>dns addForwarder addr[,addr...]</b>
—	<code>key id { algorithm string; secret string; };</code>	Web UI: List/Add Encryption Keys page fields. CLI: <b>key name create secret algorithm=alg</b>
<code>limit transfers-in num</code>	<code>options { transfers-in num };</code>	Web UI: Edit DNS Server page, set <i>xfer-client-concurrent-limit</i> . CLI: <b>session set visibility=3 dns set xfer-client-concurrent-limit=number</b>
—	<code>options { allow-query addr-match-list };</code>	Web UI: Edit DNS Server page, enable <i>restrict-query-acl</i> . CLI: <b>dns set restrict-query-acl</b>
<code>options allow-recursion addr-match-list</code>	<code>options { allow-recursion addr-match-list };</code>	Web UI: Edit DNS Server page, enable <i>restrict-recursion-acl</i> . CLI: <b>dns set restrict-recursion-acl</b>
<code>options forward-only</code>	<code>options { forward only };</code>	Web UI: Edit DNS Server page, enable <i>Slave mode</i> . CLI: <b>dns enable slave-mode</b>
<code>options listen-on port</code>	<code>options { listen-on port {addr-match-list} };</code>	Web UI: Edit DNS Server page, set <i>Listening port</i> . CLI: <b>dns set local-port-number=port</b>
<code>options max-cache-ttl num</code>	<code>options { max-cache-ttl num };</code>	Web UI: Edit DNS Server, set <i>Max. resource record caching TTL</i> . CLI: <b>dns set max-cache-ttl=num</b>
<code>options no-fetch-glue</code>	<code>options { fetch-glue no };</code>	Web UI: Edit DNS Server page, enable <i>Don't fetch missing glue records</i> . CLI: <b>dns enable no-fetch-glue</b>
<code>options no-recursion</code>	<code>options { recursion no };</code>	Web UI: Edit DNS Server page, enable <i>Recursive queries</i> . CLI: <b>dns enable no-recurse</b>

**Table 8-1 BIND-to-CLI Command Mappings (continued)**

<b>BIND 4 Command</b>	<b>BIND 9 Command</b>	<b>Mapping to User Interface</b>
options notify yes	options { notify yes ;};	Web UI: Edit DNS Server page, enable <i>Send zone change notification (NOTIFY)</i> . CLI: <b>dns enable notify</b>
options rrset-order <i>order order ...</i>	options { rrset-order <i>order</i> ; <i>order</i> ; ... ;};	Web UI: Edit DNS Server page, enable <i>Enable round-robin</i> . CLI: <b>dns enable round-robin</b>
options support-ixfr yes	options { request-ixfr yes ;};	Web UI: Edit DNS Server page, enable <i>Request incremental transfers (IXFR)</i> . CLI: <b>dns enable ixfr-enable</b>
options transfer-format many-answers	options { transfer-format many-answers ;};	Web UI: Edit DNS Server page, enable <i>Use multirec format for zone transfers</i> . CLI: <b>dns enable axfr-multirec-default</b>
primary <i>zonename file</i>	zone " <i>name</i> " { type master; };	Web UI: Add Zone page fields. CLI: <b>zone name create primary file=file</b>
secondary <i>zonename addr list [backupfile]</i>	zone " <i>name</i> " { type slave; };	Web UI: Add Secondary Zone page fields. CLI: <b>zone name create secondary ip-addr [,ip-addr...]</b>
slave	zone " <i>name</i> " { type slave; };	Web UI: Edit DNS Server page, enable <i>Slave mode</i> . CLI: <b>dns enable slave-mode</b>
—	zone " <i>name</i> " { allow-query { <i>addr</i> ; ... } };	Web UI: Edit Zone page, set <i>restrict-query-acl</i> . CLI: <b>zone name set restrict-query-acl=addr[,addr...]</b>
tcp <sub>list</sub> <i>addrlist</i> xfer <sub>nets</sub> <i>addrlist</i>	zone " <i>name</i> " { allow-transfer { <i>addr</i> ; ... } };	Web UI: Edit Zone page, enable <i>restrict-xfer</i> and set <i>restrict-xfer-acl</i> . CLI: <b>zone name enable restrict-xfer zone name set restrict-xfer-acl=addr[,addr...]</b>

For details on the following topics, see the Usage Guidelines for the **zone** command in the *Network Registrar CLI Reference*:

- Importing zone data
- Exporting zone data
- Exporting Unix hosts files

## Adding Primary Reverse Zones

For a correct DNS configuration, you must create a reverse zone for each network that you use. A reverse zone is a primary zone that DNS clients use to convert IP addresses back to hostnames, and are in a special in-addr.arpa domain. You can create a reverse zone manually or import it from BIND.

In the local cluster Web UI:

- 
- Step 1** On the Primary Navigation bar, click **Zone**.

- Step 2** On the Secondary Navigation bar, click **Reverse Zones** to open the List/Add Reverse Zones page. This page is almost identical to the List/Add Zones page (see [Figure 4-7 on page 4-17](#)).
- Step 3** Add a reverse zone the same way you would add a forward zone, as described in the [“Adding Primary Forward Zones” section on page 8-4](#), except use the reverse of the forward zone’s network number added to the special in-addr.arpa domain as the zone name. Use the same template or SOA and nameserver values as for the related forward zone.

---

In the CLI, use the `zone name create primary` and `zone name addRRR PTR` commands to add the primary reverse zone and pointer records for the server.

## Managing Secondary Servers

When you configure a zone, choose at least one secondary server. If you have only one nameserver and it becomes unavailable, there is nothing that can look up names. A secondary server splits the load with the primary or handles the whole load if the primary is unavailable. When a secondary server starts up, it contacts the primary and pulls the zone data over. This is known as a zone transfer.



### Tip

If the authoritative server for your secondary zones is also running Network Registrar 6.0 or later, see the [“Managing Zone Distributions” section on page 8-15](#) for how to avoid entering these zones manually. If you have only one secondary server, remove it geographically from the primary. They should not even be on the same network segment, switch, or router, but on a different cluster entirely.

You can configure a secondary DNS server to be responsible for a secondary zone, which makes the server a secondary for that zone. You also need to give the address of the master server from which to perform zone transfers. Network Registrar must know about this master server.



### Note

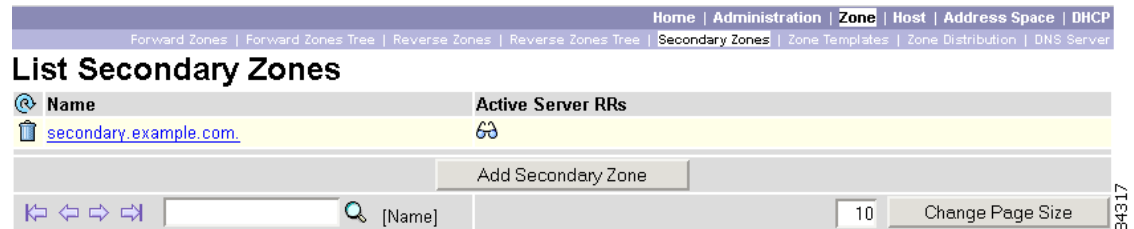
If, for some reason, your primary zone is corrupted and you want to convert a secondary to a primary zone, you can use the `cnr_zone_recovery` tool. For details, see the [“Using the cnr\\_zone\\_recovery Tool” section on page 7-15](#).

## Adding Secondary Forward Zones

To add a secondary forward zone in the local cluster Web UI:

- Step 1** On the Primary Navigation bar, click **Zone**.
- Step 2** On the Secondary Navigation bar, click **Secondary Zones** to open the List Secondary Zones page ([Figure 8-3](#)).

Figure 8-3 List Secondary Zones Page



**Step 3** Click **Add Secondary Zone** to open the Add Secondary Zone page (see [Figure 8-4](#)).

Figure 8-4 Add Secondary Zone Page

Attribute	Value	Data Type	Default
Name* (origin)	secondary.example.com.	DNS name	
master-servers*	192.168.50.1	AT_IPKEY list	
restrict-xfer	<input type="radio"/> true <input checked="" type="radio"/> false	boolean	false
restrict-xfer-acl		address match list	
<b>IXFR and NOTIFY Settings</b>			
Attribute	Value	Data Type	Default
ixfr	<input type="radio"/> true <input type="radio"/> false	boolean	
notify	<input type="radio"/> true <input type="radio"/> false	boolean	
notify-set		IP address list	
<b>Subzone Forwarding Settings</b>			
<b>Checkpoint Settings</b>			
<b>Query Settings</b>			
<b>Reserved</b>			

In the CLI, use the **zone name create secondary** command. The IP address you include is that of the nameserver from which data is expected, typically a primary nameserver.

## Adding Secondary Reverse Zones

You should add a secondary reverse zone, just as you added a secondary forward zone.

- Step 1** Add the secondary reverse zone the same way you did the primary reverse zone, except set the zone type to Secondary. See the [“Adding Primary Reverse Zones”](#) section on page 8-9.
- Step 2** Make the secondary zone’s domain name an in-addr.arpa reverse domain, ending it with a trailing dot.
- Step 3** Add the nameserver address for the secondary forward zone and set any zone transfer address restrictions, as in the [“Adding Secondary Forward Zones”](#) section on page 8-10.

**Step 4** Reload the DNS server and confirm its status.

---

## Enabling Zone Transfers

A secondary server periodically contacts its master server for changes, called a zone transfer. The interval is defined in the server's SOA record as the secondary refresh time. You can restrict zone transfers by setting the *restrict-xfer* attribute to true (the default is false) on the master server.



**Note** If you restrict zone transfers, the **nslookup** utility **ls** command may fail because it tries to do a full zone transfer, unless you include the IP address that **ls** runs from in the zone's *restrict-xfer-acl* list.

---

In the local cluster Web UI:

---

**Step 1** On the List/Add Zones page, click the name of the primary zone to open the Edit Zone page.

**Step 2** In the zone attributes, you can set the *restrict-xfer* attribute to false (the default). If you set the attribute to *true*, you can also specify a list of servers to which to restrict the zone transfers by using the *restrict-xfer-acl* attribute, separating the IP addresses with commas.

**Step 3** Click **Modify Zone**.

---

Secondary zones can also restrict zone transfers from other secondary zones, so that the *restrict-xfer* and *restrict-xfer-acl* attributes are also available for secondary zone configurations.

In the CLI, zone transfers are enabled by default, unless you restrict them using the **zone name enable restrict-xfer** command. If you want to force a zone transfer, use the **forceXfer secondary** command.

## Adding Subzones

As the zone grows, you might want to divide it into smaller pieces called subzones. You can delegate administrative authority for these subzones, and have them managed there or served by separate servers. This partitioning is called subzone delegation. Establish subzone delegation by performing these tasks:

1. Choose a subzone name
2. Specify a nameserver name
3. Specify a nameserver address

## Choosing Subzone Names and Servers

After you decide to divide the zone into subzones, you must create names for them. Involve the people responsible for the subzones in deciding their names, and try to maintain a consistent naming scheme.

These suggestions can help you avoid subzone naming problems:

- Consider not naming a subzone by its organizational name. In a changing business environment, organizations merge and are renamed. Naming a subzone after an organization could result in a name that is no longer meaningful over time.

- Consider not using geographical names that indicate the subzone location. Geographical names are meaningless to people outside your organization.
- Do not use cryptic names; make them obvious.
- Do not use existing or reserved top-level domain names as subzones. Using existing names can result in routing problems.

After you choose a subzone name, specify its nameservers, the ones the parent domain's nameservers use when queried about the subzone. To ensure that the subzone is always reachable, you should specify two nameservers. They must be authoritative for this zone as either primary or secondary, or this causes lame delegation (see the [“Reporting Lame Delegation” section on page 10-9](#)).

Whenever a subzone's nameserver changes its name or address, the subzone administrator must inform its parent zone so that the latter's administrator can change the subzone's nameserver and *glue records*. A glue record is an A record with the address of a subzone's authoritative nameserver. If the subzone's administrator fails to inform its parent, the glue records are invalid. The common symptom is that a host cannot reach a host in another domain by its name, only by its address.

## Creating and Delegating Subzones

You delegate a subzone by creating it in the parent zone. There should be one NS record for each nameserver to which the subzone is delegated. Each NS record requires a corresponding A record describing the address of the nameserver, unless the nameserver is outside the parent zone or subzone. This A record is called a glue record.

In the local cluster Web UI:

- 
- Step 1** On the subzone's primary nameserver machine:
- a. Add a zone with the subzone domain name on the List/Add Zones page.
  - b. On the Add Zone page, add the SOA records and the nameserver with its address, then click **Add Zone**.
  - c. On the List/Add Zones page, click the View icon (🔍) in the Configuration RRs column of the subzone to open the List/Add Static Resource Records for Zone page.
  - d. Create an A record for the subzone nameserver with its address, then click **Add Resource Record**.
  - e. Reload the DNS server.
- Step 2** On the parent server's primary nameserver machine:
- a. On the List/Add Zones page, click the View icon (🔍) in the Configuration RRs column of the parent zone's name to open the List/Add Static Resource Records for Zone page for the parent zone.
  - b. Create an NS record for the subzone's server, including its fully qualified domain name in the Data field, then click **Add Resource Record**.
  - c. Create a glue A record for the subzone's server with its address, then click **Add Resource Record**.
  - d. Reload the DNS server.
-

In the CLI:

---

**Step 1** On the subzone's primary nameserver machine:

a. Create the subzone:

```
nrcmd> zone boston.example.com. create primary bostonDNSserv1 hostmaster
```

b. Create an A record for the subzone's nameserver:

```
nrcmd> zone boston.example.com. addRR bostonDNSserv1 A 192.168.40.1
```

c. Reload the DNS server:

```
nrcmd> dns reload
```

**Step 2** On the parent zone's nameserver machine:

a. Add an NS record for the subzone's nameserver:

```
nrcmd> zone example.com. addRR boston NS bostonDNSserv1.boston.example.com.
```

b. Create a glue A record for the subzone's nameserver:

```
nrcmd> zone example.com. addRR bostonDNSserv1.boston.example.com. A 192.168.40.1
```

c. Reload the DNS server:

```
nrcmd> dns reload
```

---

## Undelegating Subzones

If you undelegate a subzone, remove any associated NS and glue A records from the parent zone.

In the Web UI:

---

**Step 1** On the List/Add Static Resource Records for Zone page, remove the NS resource record for the subzone by clicking the Delete icon (🗑️) next to the subzone NS record in the list.

**Step 2** Confirm the deletion on a Confirm Delete page.

**Step 3** Remove the glue A resource record for the subzone's server host by clicking the Delete icon (🗑️) next to the subzone server's A record in the list.

**Step 4** Confirm the deletion on a Confirm Delete page.

---

In the CLI, use the **zone name removeRR NS** and **zone name removeRR A** commands to remove the subzone's NS and glue A records.

## Editing Subzone Delegations

You can edit the subzone's resource records.

In the Web UI:

- 
- Step 1** On the List/Add Static Resource Records for Zone page, edit the NS resource record for the subzone by clicking the Edit icon (✎) next to the record to open the Edit Resource Record in Zone page.
  - Step 2** Edit the NS record data.
  - Step 3** Click **Modify Resource Record**.
  - Step 4** Edit the glue A resource record for the subzone's server in the same way as the previous step.
  - Step 5** Reload the DNS server.
- 

In the CLI, use the `zone name removeRR` command to delete the NS and glue A records, then use the `zone name addRR` command to replace them. Reload the DNS server.

## Enabling Dynamic DNS Updates

Dynamic DNS (RFC 2136) integrates DNS and DHCP so that they can work together. Dynamic DNS update automatically records the association between the hosts and their DHCP-assigned addresses. Using DHCP and dynamic DNS update, you can configure a host automatically for network access whenever it attaches to the network. You can locate and access the host using its unique DNS host name.

Dynamic DNS update is described more fully in [Chapter 15, “Configuring Dynamic DNS Update.”](#) The chapter also includes a section on scavenging (removing stale) dynamic resource records.

## Managing Zone Distributions

Creating a zone distribution map simplifies creating multiple zones that share the same secondary zone attributes. Like a template, the zone distribution map can have a unique name. The distribution map requires adding one or more predefined secondary servers. When you run a zone distribution synchronization, this adds secondary zones to the listed secondary servers for each primary zone on the primary server.

In Network Registrar 6.0, you could manage only the default distribution. In Network Registrar 6.1, you can define additional ones on the regional cluster only. The distribution must be in a star topology, that is, one primary server and multiple secondary servers. The authoritative server can only be the local primary server where the zone distribution default is defined.

In the local cluster Web UI:

- 
- Step 1** On the Primary Navigation bar, click **Zone**.
  - Step 2** On the Secondary Navigation bar, click **Zone Distribution**. This opens the List Zone Distributions page, which is almost identical to the List/Add Zone Distributions page at the regional cluster (see [“Creating DNS Zone Distributions” section on page 5-29](#)), except that you cannot create a zone distribution and you can edit only the Default zone distribution (see [Figure 5-15 on page 5-29](#)).

- Step 3** To edit the zone distribution, click **Default** on the List Zone Distributions page to open the Edit Zone Distribution page, which is almost identical to the Add Zone Distribution page at the regional cluster (see [Figure 5-16](#) on [page 5-30](#)). On this page, you can:
- Add the master DNS server IP address or addresses with an optional TSIG key—Enter in the format *address-key*, using the hyphen if adding a key, then click **Add IP Key** for each entry. (For details on TSIG, see the “[Transaction Security and Access Control Lists](#)” section on [page 15-3](#).)
  - Add secondary server address or addresses—Click **Add Server**. This opens the Add Secondary Server page (see [Figure 8-5](#)).
  - Choose the zone or zones in the distribution—Move the zone or zones into the Selected field.

**Figure 8-5 Add Secondary Server Page**

Attribute	Value
Name*	secondarydns
IP Address*	192.168.60.1
Administrator Username*	admin
Administrator Password*	password
SCP Port Number*	1234
Use SSL	optional
Master Servers	

On the Add Secondary Server page, you can enter or choose the following data:

- Name of the secondary server.
- IP address of the secondary server.
- Administrator’s username at the secondary server.
- Administrator’s password at the secondary server.
- SCP port number of the secondary server (usually 1234).
- Whether to use SSL—Disabled, optional, or required.
- List of master servers for the secondary server that are apart from the Authoritative Server IP Addresses specified in the zone distribution. In this way, you can have different master servers for each secondary server.

**Step 4** Click **Add Secondary Server** when you are done with this page.

**Step 5** Click **Modify Zone Distribution** on the Edit Zone Distribution page when you are done.