CHAPTER 16

Managing Resource Records

This chapter explains how to configure some of the more advanced DNS zone and server parameters by using the Cisco Network Registrar web UI and CLI. Before you proceed with the concepts in this chapter, read Chapter 15, "Managing Zones," which explains how to set up the basic properties of a primary and secondary DNS server and its zones.

See Also

Managing Resource Records
Managing Hosts in Zones, page 16-10

Managing Resource Records

Resource records (RRs) comprise the data within a DNS zone. Although there is no fixed limit to the number of RRs a zone may own, in general, a zone may own one or more RRs of a given type (the zone always has a Start of Authority, or SOA, record). There are some exceptions depending on the types involved. All RRs have the entries described in Table 16-1.

Table 16-1 Resource Record Common Entries

RR Entry	Description
Name	Owner of the record, such as a zone or hostname.
Class (not required for all formats)	Cisco Network Registrar supports only the IN (Internet) class.
TTL (time to live)	Amount of time to store the record in a cache, in seconds. If you do not include a TTL, Cisco Network Registrar uses the zone default TTL, defined as a zone attribute.
Type	Type of the record, such as A (AAAA for IPv6), NS, SOA, and MX. There are many types that various RFCs define, although fewer than ten are in common use.
Record data	Data types whose format and meaning varies with record type.

See Also

Adding Resource Records

Before adding or modifying RRs, keep in mind the two distinct dns edit modes that you can set and work in: staged and synchronous (see the "Staged and Synchronous Modes" section on page 15-1).

Administrator roles required for RR management are the dns-admin role at the local cluster and the central-dns-admin role at the regional cluster. The host-admin role at the local cluster and the central-host-admin role at the regional cluster can view host records only.

Local Basic or Advanced and Regional Web UI

Step 1 From the **DNS** server, choose **Forward Zones** to open the local List/Add Zones or regional List Forward Zones page.

Step 2 Click the View icon ( ) in the RRs column of the zone name to open the List/Add DNS Server RRs for Zone page at the local cluster. Note that by default at the regional cluster, this action opens the List/Add CCM Server Protected RRs for Zone page, because the regional cluster defaults to staged (CCM) dns edit mode.

Tip You can toggle between the List/Add CCM Server Protected RRs for Zone page and the List/Add DNS Server RRs for Zone page. Either page appears initially depending on whether you are set up with protected or unprotected RR edit capabilities (see the "Protecting Resource Record Sets" section on page 16-3). Records are listed in the formats that their respective RFCs specify, with only the first record in a set labeled with its name, and in DNSSEC order. To reduce or increase the items in the table, change the page size value at the bottom of the page, then click **Change Page Size**.

Step 3 Add the RR name, TTL (if not using the default TTL), type, and data as appropriate.

Step 4 By default, RRs are protected, which means that DNS Updates cannot overwrite them (see the "Protecting Resource Record Sets" section on page 16-3). To unprotect the RRs, click the Locked icon ( ) to the left of the record name to change it to the Unlocked icon ( ). Likewise, to protect the record, click the Unlocked ( ) icon to change it to the Locked icon ( ).

Step 5 Click **Add Resource Record**.

CLI Commands

Use **zone** *name* **addRR** to add a protected RR of a certain type. You can specify the name as a relative name, if the owner is in the same domain, an absolute name (by supplying the FQDN), or the same name as the zone name (by using the at [@] symbol). You can specify the dns edit mode as part of the command by using the **–staged** or **–sync** switches.

For example:

```
nrcmd> zone example.com addRR -sync host101 A 192.168.50.101
```

Use **zone** *name* **addDNSRR** *type data* to add an unprotected RR.

Protecting Resource Record Sets

When an RR is protected, DNS Updates cannot modify the record. Most administratively created RRs are protected. However, RRs created by DNS Updates must be unprotected to allow the server to modify them. You can set this protection status for each RR set on the List/Add DNS Server RRs for Zone page.

Note that only the primary DNS server can recognize this protection status; secondary servers do not recognize the protection status of their RRs.

Caution Zone scavenging can remove RRs that are unprotected. See the "Scavenging Dynamic Records" section on page 28-16 for details.

Local Basic or Advanced and Regional Web UI

To protect an existing RR, do the following:

Step 1 On the local List/Add Zones or regional List Forward Zones page, click the View icon ( ) in the RRs column of the zone name. The List/Add DNS Server RRs for Zone page is displayed.

Step 2 On the List/Add DNS Server RRs for Zone page, click the Resource Record name in the list of Resource Records to open the Edit RR Set in Zone page.

Step 3 Click **Protect Set** button to unprotect the selected RR set.

Note You cannot change the protection on the List/Add CCM Protected RRs for Zone page. The Locked icon ( ) always appears and you cannot change it.

You can also unprotect an RR. To unprotect an RR while adding, click the Locked icon ( ) next to the Resource Record name field. The icon changes to Unlocked ( ) unprotecting the RR set.

To unprotect an existing RR, do the following:

Step 1 On the local List/Add Zones or regional List Forward Zones page, click the View icon ( ) in the RRs column of the zone name. The List/Add DNS Server RRs for Zone page is displayed.

Step 2 On the List/Add DNS Server RRs for Zone page, click the Resource Record name in the list of Resource Records to open the Edit RR Set in Zone page.

Step 3 Click the Unprotect Set button to unprotect the selected RR set.

Note The icon to the left of the RR set name indicates the status of the Resource Record, whether it is protected ( ) or unprotected ( ).

CLI Commands

To protect the RR sets, use **zone** *name* **protect-name** *rrset-name*; to unprotect the zone, use the **unprotect-name** *rrset-name* action instead. For example:

```
nrcmd> zone example.com protect-name boston
100 Ok
protected boston
nrcmd> zone example.com unprotect-name boston
100 Ok
unprotected boston
```

Editing Resource Records

You can edit RRs as an individual record or as an RR set:

- **Individual RRs**—Click the Edit icon ( ) next to the record name to open the Edit RR in Zone page.
- **RR sets**—Click the name of the record to open the Edit RR Set in Zone page.

For a description of the fields to enter data, see the "Adding Resource Records" section on page 16-2.

Removing Resource Records

You can remove RRs from a zone.

Local Basic or Advanced and Regional Web UI

On the local List/Add DNS Server RRs for Zone page or regional List/Add CCM Server Protected RRs for Zone page:

- To remove an entire record name set, click the Delete icon ( ) next to the record set name in the list, then confirm the deletion.
- To remove individual records from the set, click the name of the record set to open the Edit RR Set page, click the Delete icon next to the individual record in the list, then confirm the deletion.

CLI Commands

The CLI includes two removal commands, depending on the type of RR to remove:

- Use **zone** *name* **removeRR** to remove any RR. You must specify the owner. If you omit the data, Cisco Network Registrar removes all records of the specified type for the specified owner. Similarly, if you omit the type, Cisco Network Registrar removes all records for the specified owner.
- Use **zone** *name* **removeDNSRR** to remove unprotected RRs only.

Removing Cached Records

Removing cached records removes nonauthoritative RRs from both in-memory and persistent (nonauthoritative) cache. The DNS server must be running to remove cached records. Changes take effect immediately.

Local Basic or Advanced Web UI

Step 1 From the **DNS** menu, choose **DNS Server** to open the Manage DNS Server page.

Step 2 Click the Run icon ( ) in the Commands column to open the DNS Server Commands page.

Step 3 For the Remove nonauthoritative RR set command, if you want to:

- Remove the entire cached RR set, enter just the name of the RR set; omit the type and data values.
- Remove the cached RR name, enter the name and type of RR.
- Remove the specific cached record, enter the name, type, and data.

Step 4 Click the Run icon ( ) for that command. You should get a confirmation message.

Step 5 Click **Return**.

CLI Commands

Use **dns removecachedRR** *name type data* to remove cached RRs in the memory and persistent caches. With the type and data omitted, this removes the entire RR set; if the type is included without the data, this removes the name set; with the name, type, and data included, this removes the specific record only.

Listing Records

You can display all the RRs, or only the staged or synchronized ones. The server must be operating to display the synchronized records.

Local Basic or Advanced and Regional Web UI

On the regional List/Add CCM Server Protected RRs for Zone page or local List/Add DNS Server RRs for Zone page, view the records on the page, then click **Return to Zone List**.

CLI Commands

Use **zone** *name* **listRR** to display RRs in the named zone. You can also specify whether you want all records or only staged (CCM) or synchronized (DNS) records (see the "Filtering Records" section on page 16-7 for details). For example:

```
nrcmd> zone example.com listRR dns
```

You can get an exact count of the total RRs for the DNS server by using **dns getRRCount** [**zone** *name* | **forward** | **reverse** | **primary** | **secondary** | **published** | **unpublished** | **all**]. Options let you request the RR count for a single zone or all zones of a given type.

Searching Server-Wide for Records and Addresses

With Cisco Network Registrar, you can search for RRs and IP addresses server-wide. The search is a filter mechanism whereby you can specify a combination of RR and address attributes to target one or more RRs or addresses configured for the network. The search function is available at the local cluster only.

You can search RRs by:

- IP address
- Protection state
- Name prefix
- Type
- Zone

Local Advanced Web UI

Step 1 Place the cursor on **DNS** and choose **Search** to open the DNS Resource Record Search page.

Step 2 Choose a filter attribute from the drop-down list, such as RR Protection State, or search by IP address.

To search by IP address, click **IP Address Search** to open the IP Address Search page. Enter an IP address, then click **Search**.

Note In an IP address search, the DNS server does not search all forward zones for RRs that have the specified address in the data field. Instead, the server looks up the matching PTR record in the reverse zone and returns all the respective RRs in the forward zone.

Step 3 If you are not searching by IP address, choose a filter type from the drop-down list depending on the filter attribute you chose:

- **RR Protection State**—RR Protection Status, either locked or unlocked.
- **RR Name Prefix**—RR Name Prefix.
- **RR Type**—RR Type.

Step 4 Enter or select a Value, based on the Type selected. To clear the filter, click **Clear Filter**.

Step 5 Click **Add Element** to add the search element to the filter elements list. The Filter Elements heading changes to identify the filter attribute and value used for the filter. If you add more than one element, the heading identifies the ANDed values of the elements. For example, if you add an element for a name prefix search for user, then add another element for an RR type search for A records, the filter element heading will identify the search as ****RR Name Prefix = user AND RR Type = A**.

Step 6 You can add as many elements as you like (remembering that the search results are an intersection of the filter elements). View the filter elements list by clicking the plus sign (**+**).

Step 7 Click **Search**.

Step 8 Check the table of resulting RRs from the search, which shows for each RR its zone, hostname, TTL, type, and associated data. If necessary, change the page size to see more entries at one time (you might still need to page forward and back). The RRs are sorted in DNSSEC order.

Tip If the search results are less than expected due to the ANDing of the filter elements, look at the filter list for any element that might be compromising the search, delete it by clicking the Delete icon ( ) next to it, then redo the search.

CLI Commands

Use **dns findRR** to find RRs across the zones. The command syntax is of two kinds:

```
nrcmd> dns findRR -name {fqdn | domainaddr}
nrcmd> dns findRR [-namePrefix nameprefix]
    [-rrTypes RRtypelist]
    [-protected | -unprotected]
    [-zoneType {forward | reverse | primary |secondary | published | unpublished | ALL}]
```

You can search by domain or its address, or enter the beginning characters of the RR name (the name prefix). If you search by RR name prefix, you can narrow the search by a list of RR types, protection status, or zone type. The output clearly indicates the zone for each found entry. For example:

```
nrcmd> dns findRR -namePrefix user -rrTypes A
userhost101.example.com IN A 192.168.50.101
userhost102.example.com IN A 192.169.50.102
userhost103.boston.example.com IN A 192.168.50.103
```

Use **zone findRR** to search on RR name prefixes, RR types, or protection status:

```
nrcmd> zone findRR [-namePrefix nameprefix]
    [-rrTypes RRtypelist]
    [-protected | -unprotected]
```

Filtering Records

You might want to filter records to display only one type of record, such as an A (or IPv6 AAAA) or PTR record. (See also the "Searching Server-Wide for Records and Addresses" section on page 16-6.)

Local Basic or Advanced and Regional Web UI

You can filter RRs right from the regional List/Add CCM Server Protected RRs for Zone page or local List/Add DNS Server RRs for Zone page. Look for the Name and Type fields just below the **Add Resource Record** button.

By default, RRs are sorted alphabetically by name, starting with the top-of-zone records (marked with the @ symbol), and secondarily sorted by type, then data. You can also sort them by:

- **Protected state**—You can click All, Unprotected ( ), or Protected ( ).
- **Name prefix**—Starting characters in the name. Note that the * character is not a wildcard. For example, entering **al** returns alberta, allen.wrench, and allie, whereas entering **al*** returns al* and al*ert.
- **RR type**—Click one of the RR types in the drop-down list, such as A (or IPv6 AAAA) or TXT.

When the selection is complete, click **Filter List**. This returns just the filtered entries in the table below the fields. To return to the full, unfiltered list, click **Clear Filter**.

CLI Commands

Use **zone** *name* **listRR** *option* to filter records. This helps determine whether DNS Update is working and what dynamic entries are in the system. The options are:

- **all**—Displays all records (the default if omitted).
- **ccm**—Displays the CCM protected RRs only (the default for the local cluster).
- **dns**—Displays the DNS live RRs only (the default for the regional cluster).

Deleting Leftover Zone Records After Recreating Zones

You can delete leftover static zone records after you delete a zone and then recreate it. Dynamic RRs are automatically deleted when you recreate the zone. This function is currently not available in the web UI.

Use **zone** *name* **cleanRR** if you periodically delete and reimport zones, which can cause your database to grow. This command uses the DNS server historical zone data to determine what part to remove. It does not print a list of records to be deleted or prompt you for confirmation. You can safely run it any time.

Using Service Location (SRV) Records

Windows domain controllers use the service location (SRV) RR to advertise services to the network. This RR is defined in the RFC 2782, "A DNS RR for specifying the location of services (DNS SRV)." The RFC defines the format of the SRV record (DNS type code 33) as:

```
_service._protocol.name ttl class SRV priority weight port target
```

There should always be an A record associated with the SRV record target so that the client can resolve the service back to a host. In the Microsoft Windows implementation of SRV records, the records might look like this:

```
myserver.example.com A 201.165.201.1
_ldap._tcp.example.com SRV 0  0  389  myserver.example.com
_kdc._tcp.example.com SRV 0  0  88  myserver.example.com
_ldap._tcp.dc._msdcs.example.com SRV 0  0  88  myserver.example.com
```

An underscore (_) always precedes the service and protocol names. In the example, _kdc is the Key Distribution Center. The priority and weight help a client choose between target servers providing the same service (the weight differentiating those with equal priorities). If the priority and weight are all set to zero, the client orders the servers randomly.

Note For a description of how Windows clients interoperate with DNS and DHCP servers, including scavenging dynamic RRs, see the "Configuring DNS Update for Windows Clients" section on page 28-18.

Using NAPTR Records

Cisco Network Registrar supports Naming Authority Pointer (NAPTR) RRs. These records help with name resolution in a particular namespace and are processed to get to a resolution service. Because NAPTR records are a proposed standard, RFC 3403, Cisco Network Registrar only validates their numeric record fields. However, the proposed standard requires a value for each field, even if it is null (“”), and there are no preset values.

When using a NAPTR record to locate a Session Initiation Protocol (SIP) proxy, see the proposed standard, RFC 2916 or RFC 3263. In RFC 2916, the ENUM working group of the Internet Engineering Task Force specifies NAPTR records to map E.164 addresses to Universal Resource Identifiers (URIs). Using the NAPTR record resolves a name in the E.164 international public telecommunication namespace to a URI, instead of providing the name of a service to use as a resolver. The U flag was added to the NAPTR record for this purpose.

For example, to specify a SIP proxy for the phone number +4689761234, add a NAPTR record at the name 4.3.2.1.6.7.9.8.6.4.e164.arpa. with this content:

```
100 10 "u" "sip+E2U" "/^.*$/sip:info@tele2.se/" .
```

This sets these fields of the NAPTR record:

```
order = 100
preference = 10
flags = "u"
service = "sip+E2U"
regexp = "/^.*$/sip:info@tele2.se/"
replacement = .
```

After you configure these fields, the DNS client dealing with phone number +4689761234 can now find an SIP service URI by replacing the number with sip:info@tele2.se. The E.164 zone mostly uses the NAPTR record for wholesale replacement of the input telephone number. Section 3.2.3 of RFC 2916 includes an example of one transformation to a Lightweight Directory Access Protocol (LDAP) query that preserves some of the digits. The E.164 zone does not map to service location (SRV) records because it wants to obtain a SIP URL that is more humanly readable to the left of the at (@) symbol.

Local Basic or Advanced and Regional Web UI

Step 1 On the List/Add Zones page, click the View icon () in the RRs column.

Step 2 Enter the owner of the record in the Name field.

Step 3 Enter the TTL (if necessary).

Step 4 Click NAPTR in the Type drop-down list.

Step 5 Enter the data as a string embedded in quotes and separated by spaces:

- **a.** Order
- **b.** Preference
- **c.** Flags
- **d.** Service
- **e.** Regular expression
- **f.** Replacement string

For example:

```
"100 10 u sip+E2U /^.*$/sip:info@tele2.se/ ."
```

Step 6 Click **Add Resource Record**.

Step 7 Refresh the list if necessary.

CLI Commands

Use **zone** *name* **addRR** to add a protected resource record to a zone.

Adding IPv6 Records

The IPv6 address space includes some additional RRs. For details, see Chapter 26, "Managing DHCPv6 Addresses,".

Managing Hosts in Zones

You can manage the RRs for a host by configuring the host record rather than the individual RRs. When you define a host, the DNS server automatically creates an Address (A) RR for IPv4, or an AAAA RR for IPv6, for it. If the reverse zone for the host exists, the server can also create the associated Pointer (PTR) RR for it.

See Chapter 10, "Managing Hosts," for details