CHAPTER 17

# Managing Authoritative DNS Server Properties

This chapter explains how to set the Authoritative DNS server parameters. Before you proceed with the tasks in this chapter, read Chapter 15, "Managing Zones," which explains how to set up the basic properties of a primary and secondary zone.

### Related Topics

Managing DNS Authoritative Servers, page 17-1
Setting DNS Server Properties, page 17-2
Setting Advanced Authoritative DNS Server Properties, page 17-7
Tuning DNS Properties, page 17-9
Troubleshooting DNS Servers, page 17-10

# Managing DNS Authoritative Servers

You can view its health, statistics, and logs; start, stop, and reload it; run certain commands (see the "Running DNS Authoritative Server Commands" section on page 17-1); and edit the server attributes.

To view the server status and health, or stop, start, and reload the server, in the local cluster web UI, click **DNS**, then **DNS Server** under the Settings submenu to open the Manage DNS Authoritative Server page.

### Related Topics

Running DNS Authoritative Server Commands, page 17-1
Configuring DNS Server Network Interfaces, page 17-2

## Running DNS Authoritative Server Commands

Access the commands by using the Run icon in the Commands column. Clicking the Run icon opens the DNS Server Commands page in the local web UI. Each command has its own Run icon (click it, then click **Return** when finished):

- **Force all zone transfers**—A secondary server periodically contacts its master server for changes. See the "Enabling Zone Transfers" section on page 15-15.
- **Scavenge all zones**—Cisco Prime Network Registrar provides a feature to periodically purge stale records. See the "Scavenging Dynamic Records" section on page 29-16.

- **Synchronize All HA Zones**—Synchronizes all the HA zones. You have the option to choose the type of synchronization. The **Use Server Algorithms** option is checked by default. You can override this by checking either **Push All Zones From Main to Backup** check box or **Pull All Zones From Backup to Main** check box.

**Note** The **Synchronize All HA Zone**s command is an **Expert** mode command which you can see only if the server is an HA main server. You cannot see this command if it is an HA backup server. You can also, synchronize zones separately, which you can do from the Zone Commands for Zone page (see the "Synchronizing HA DNS Zones" section on page 19-5).

**Note** If you find a server error, investigate the server log file for a configuration error, correct the error, return to this page, and refresh the page.

# Configuring DNS Server Network Interfaces

You can configure the network interfaces for the DNS server from the Manage Servers page in the local web UI.

### Local Advanced Web UI

**Step 1** From the **Servers** menu, choose **Manage Servers**.

**Step 2** Click the Interfaces icon for the DNS server to open the Manage DNS Server Network Interfaces page. This page shows the available network interfaces that you can configure for the server. By default, the server uses all of them.

**Step 3** To configure an interface, click the Configure icon in the Configure column for the interface. This adds the interface to the Configured Interfaces table, where you can edit or delete it.

**Step 4** Clicking the name of the configured interface opens the Edit DNS Server Network Interface page, where you can change the address and port of the interface.

**Step 5** Click **Modify Interface** when you are done editing, then click **Return** to return to the Manage Servers page.

**Note** The IPv6 functionality in DNS requires IPv4 interfaces to be configured except if the DNS server is isolated and standalone (it is its own root and is authoritative for all queries).

# Setting DNS Server Properties

You can set properties for the DNS server, along with those you already set for its zones. These include:

- **General server properties**—See the "Setting General DNS Server Properties" section on page 17-3.
- **Delegation-only zones**—See the "Specifying Delegation-Only Zones" section on page 17-3.

- **Round-robin server processing**—See the "Enabling Round-Robin" section on page 17-4.
- **Subnet sorting**—See the "Enabling Subnet Sorting" section on page 17-4.
- **Enabling incremental zone transfers**—See the "Enabling Incremental Zone Transfers (IXFR)" section on page 17-5.
- **Changesets and checkpointing**—See the "Changesets and Checkpointing" section on page 17-5.
- **Enabling NOTIFY packets**—See the "Enabling NOTIFY" section on page 17-6.

# Setting General DNS Server Properties

You can display DNS general server properties, such as the name of the server cluster or host machine and the version number of the Cisco Prime Network Registrar DNS server software. You can change the internal name of the DNS server by deleting the current name and entering a new one. This name is used for notation and does not reflect the official name of the server. Cisco Prime Network Registrar uses the server IP address for official name lookups and for DNS updates (see the Chapter 29, "Configuring DNS Update").

The following subsections describe some of the more common property settings. They are listed in the "Setting DNS Server Properties" section on page 17-2.

### Local Basic or Advanced Web UI

**Step 1** To access the server properties, choose **DNS Server** from the **DNS** menu to open the Manage DNS Authoritative Server page.

**Step 2** Click the name of the server to open the Edit DNS Authoritative Server page. (Or, click **Administration**, then **Manage Servers**, then the **Local DNS Server** link to get to the same page.) The page displays all the DNS server attributes.

**Step 3** Then click **Modify Server** to save the DNS server attribute modifications.

### CLI Commands

Use **dns** [**show**] to display the DNS server properties.

# Specifying Delegation-Only Zones

You can instruct the server to expect only referrals when querying the specified zone. In other words, you want the zone to contain only NS records, such as for subzone delegation, along with the apex SOA record of the zone. This can filter out "wildcard" or "synthesized" data from authoritative nameservers whose undelegated (in-zone) data is of no interest. Enable the DNS server *delegation-only-domains* attribute for this purpose.

# Enabling Round-Robin

A query might return multiple A records for a nameserver. To compensate for most DNS clients starting with, and limiting their use to, the first record in the list, you can enable *round-robin* to share the load. This method ensures that successive clients resolving the same name will connect to different addresses on a revolving basis. The DNS server then rearranges the order of the records each time it is queried. It is a method of load sharing, rather than load balancing, which is based on the actual load on the server.

**Tip** Adjust the switchover rate from one round-robin server to another using the TTL property of the server A record.

### Local Basic or Advanced Web UI

On the Edit DNS Authoritative Server page, under Miscellaneous Options and Settings, find the Enable round-robin (*round-robin)* attribute. It is set to enabled by default in Basic mode.

### CLI Commands

Use **dns get round-robin** to see if round-robin is enabled (it is by default). If not, use **dns enable round-robin**.

# Enabling Subnet Sorting

If you enable subnet sorting, as implemented in BIND 4.9.7, the Cisco Prime Network Registrar DNS server confirms the client network address before responding to a query. If the client, server, and target of the query are on the same subnet, and the target has multiple A records, the server tries to reorder the A records in the response by putting the closest address of the target first in the response packet. DNS servers always return all the addresses of a target, but most clients use the first address and ignore the others.

If the client, DNS server, and target of the query are on the same subnet, Cisco Prime Network Registrar first applies round-robin sorting and then applies subnet sorting. The result is that if you have a local response, it remains at the top of the list, and if you have multiple local A records, the server cycles through them.

### Local Basic or Advanced Web UI

On the Edit DNS Server page, in A-Z view, find the *subnet-sorting* attribute, set it to enabled, then click **Modify Server**.

### CLI Commands

Use **dns enable subnet-sorting** or **dns disable subnet-sorting** (the preset value).

# Enabling Incremental Zone Transfers (IXFR)

Incremental Zone Transfer (IXFR, described in RFC 1995) allows only changed data to transfer between servers, which is especially useful in dynamic environments. IXFR works together with NOTIFY (see the "Enabling NOTIFY" section on page 17-6) to ensure more efficient zone updates. IXFR is enabled by default.

Primary zone servers always provide IXFR. You should explicitly enable IXFR on the server (you cannot set it for the primary zone) only if the server has secondary zones. The DNS server setting applies to the secondary zone if there is no specific secondary zone setting.

### Local Basic or Advanced Web UI

On the Edit DNS Authoritative Server page, under Zone Default Settings, you can find the Request incremental transfers (IXFR) attribute. It is set it to enabled by default. For a secondary zone, you can also fine-tune the incremental zone transfers by setting the *ixfr-expire-interval* attribute.

This value is the longest interval the server uses to maintain a secondary zone solely from IXFRs before forcing a full zone transfer (AXFR). The preset value of one week is usually appropriate. Then, click **Modify Server**.

### CLI Commands

Use **dns enable ixfr-enable**. By default, the *ixfr-enable* attribute is enabled.

# Changesets and Checkpointing

Cisco Prime Network Registrar maintains a changeset database that collects recent changes to RR data. The changeset database maintains a collection of recent RR changes which is used to answer incremental zone transfer requests. Each changeset consists of one or more RRs that had been changed at a particular serial number.

The changeset database is backed up during the usual cnr_shadow_backup backup. To keep it from growing without bounds, the server trims it periodically. The effect of this is, for example, that if a DNS client requests a zone IXFR based on a serial number for RRs that were trimmed, the DNS server cannot perform an IXFR, but must perform a full zone transfer (AXFR).

Zone checkpointing creates a snapshot of the zone data that may be necessary to recreate the auth.db in case it becomes unstable or unusable. The server automatically updates the checkpoint files periodically. In addition to occurring with each changeset that is over a certain size threshold, zone checkpointing happens by default every three hours. You can adjust this interval, from between one and 168 hours, using the *checkpoint-interval* DNS server or zone attribute.

### Local Basic or Advanced Web UI

To manually force a zone checkpoint, click the Run icon on the List/Add Zones or List/Add Reverse Zones page. On the Zone Commands for Zone page, click the Run icon next to Checkpoint zone.

### CLI Commands

Use **zone** *name* **chkpt**, or dump the zone checkpoint file in a more humanly readable form by using **zone** *name* **dumpchkpt**.

# Restricting Zone Queries

You can restrict clients to query only certain zones based on an access control list (ACL). An ACL can contain source IP addresses, network addresses, TSIG keys (see the "Transaction Security" section on page 29-9), or other ACLs. The *restrict-query-acl* on the DNS server serves as a default value for zones that do not have the *restrict-query-acl* specifically set.

# Enabling NOTIFY

The NOTIFY protocol, described in RFC 1996, lets the Cisco Prime Network Registrar DNS primary server inform its secondaries that zone changes occurred. The NOTIFY packets also include the current SOA record for the zone giving the secondaries a hint as to whether or not changes have occurred. In this case, the serial number would be different. Use NOTIFY in environments where the namespace is relatively dynamic.

Because a zone master server cannot know specifically which secondary server transfers from it, Cisco Prime Network Registrar notifies all nameservers listed in the zone NS records. The only exception is the server named in the SOA primary master field. You can add additional servers to be notified by adding the IPv4 addresses to the notify-set on the zone configuration.

**Note** For NS records that point at names that the DNS server is not authoritative for, those IP addresses need to be explicitly set in the notify-set if the user wants those servers to get notifies.

You can use IXFR and NOTIFY together, but this is not necessary. You can disable NOTIFY for a quickly changing zone for which immediate updates on all secondaries does not warrant the constant NOTIFY traffic. Such a zone might benefit from having a short refresh time and a disabled NOTIFY.

### Local Basic or Advanced Web UI

**Step 1** On the Edit DNS Authoritative Server page, under Log Settings, find the *notify* attribute, then check the check box to enable it.

**Step 2** Set any of the other NOTIFY attributes (*notify-defer-cnt*, *notify-min-inverval*, *notify-rcv-interval*, *notify-send-stagger*, *notify-source-address*, *notify-source-port*, and *notify-wait*).

**Step 3** Click **Modify Server**.

**Step 4** To add nameservers in addition to those specified in NS records, click **Forward Zones**.

**Step 5** Click the zone name.

**Step 6** Add a comma-separated list of IP addresses of the servers using the *notify-set* attribute on the Edit Zone page.

**Step 7** Set the *notify* attribute to true.

**Step 8** Click **Modify Zone** on that page.

### CLI Commands

Use **dns enable notify**. NOTIFY is enabled by default. You can also enable NOTIFY at the zone level, where you can use **zone** *name* **set notify-set** to specify an additional comma-separated list of servers to notify beyond those specified in NS records.

# Setting Advanced Authoritative DNS Server Properties

You can set these advanced server properties:

- **SOA time-to-live**—See the "Setting SOA Time to Live" section on page 17-7.
- **Secondary server attributes**—See the "Setting Secondary Refresh Times" section on page 17-7.
- **Port numbers**—See the "Setting Local and External Port Numbers" section on page 17-9.
- **Handle Malicious DNS Clients**—See the "Handling Malicious DNS Clients" section on page 17-9.

## Setting SOA Time to Live

The SOA record time to live (TTL) is usually determined by the zone default TTL. However, you can explicitly set the SOA TTL, which sets the maximum number of seconds a server can cache the SOA record data. For example, if the SOA TTL is set for 3600 seconds (one hour), an external server must remove the SOA record from its cache after an hour and then query your nameserver again.

Cisco Prime Network Registrar responds to authoritative queries with an explicit TTL value. If there is no explicit TTL value, it uses the default TTL for the zone, as set by the value of the *defttl* zone attribute. Databases originating from versions of Cisco Prime Network Registrar earlier than Release 3.5 do not have the *defttl* zone attribute, and use the minimum TTL in the zone SOA record for the default TTL.

Normally, Cisco Prime Network Registrar assumes the default TTL when responding with a zone transfer with RRs that do not have explicit TTL values. If the default TTL value for the zone is administratively altered, Cisco Prime Network Registrar automatically forces a full zone transfer to any secondary DNS server requesting a zone transfer.

### Local Basic or Advanced and Regional Web UI

**Step 1** On the Add Zone or Edit Zone page, set the Zone Default TTL, which defaults to 24 hours.

**Step 2** If you want, set the SOA TTL, which is the TTL for the SOA records only. It defaults to the Zone Default TTL value.

**Step 3** You can also set a TTL value specifically for the NS records of the zone. Set the NS TTL value under Nameservers. This value also defaults to the Zone Default TTL value.

**Step 4** Click **Modify Zone**.

### CLI Commands

Use **zone** *name* **set defttl**.

## Setting Secondary Refresh Times

The secondary refresh time is how often a secondary server communicates with its primary about the potential need for a zone transfer. A good range is from an hour to a day, depending on how often you expect to change zone data.

If you use NOTIFY, you can set the refresh time to a larger value without causing long delays between transfers, because NOTIFY forces the secondary servers to notice when the primary data changes. For details about NOTIFY, see the "Enabling NOTIFY" section on page 17-6.

### Local Basic or Advanced and Regional Web UI

On the Add Zone or Edit Zone page, set the Secondary Refresh field to the refresh time, which defaults to three hours. Make any other changes, then click **Modify Zone**.

### CLI Commands

Use **zone** *name* **set refresh**. The preset value is 10800 seconds (three hours).

## Setting Secondary Retry Times

The DNS server uses the secondary retry time between successive failures of a zone transfer. If the refresh interval expires and an attempt to poll for a zone transfer fails, the server continues to retry until it succeeds. A good value is between one-third and one-tenth of the refresh time. The preset value is one hour.

### Local Basic or Advanced and Regional Web UI

On the Add Zone or Edit Zone page, set the Secondary Retry field to the retry time, which defaults to one hour. Make any other changes, then click **Modify Zone**.

### CLI Commands

Use **zone** *name* **set retry**.

## Setting Secondary Expiration Times

The secondary expiration time is the longest time a secondary server can claim authority for zone data when responding to queries after it cannot receive zone updates during a zone transfer. Set this to a large number that provides enough time to survive extended primary server failure. The preset value is seven days.

### Local Basic or Advanced and Regional Web UI

On the Add Zone or Edit Zone page, set the Secondary Expire field to the expiration time, which defaults to seven days. Make any other changes, then click **Modify Zone**.

### CLI Commands

Use **zone** *name* **set expire**.

# Setting Local and External Port Numbers

If you are experimenting with a new group of nameservers, you might want to use nonstandard ports for answering requests and asking for remote data. The local port and external port settings control the TCP and UDP ports on which the server listens for name resolution requests, and to which port it connects when making requests to other nameservers. The standard value for both is port 53. If you change these values during normal operation, the server will appear to be unavailable.

The full list of default ports is included in the "Default Ports for Cisco Prime Network Registrar Services" section on page 1-11.

### Local Basic or Advanced Web UI

On the Edit DNS Server page, in A-Z view, find the *local-port-num* and *remote-port-num* attributes, set them to the desired values (they are both preset to 53), then click **Modify Server**.

# Handling Malicious DNS Clients

When trying to resolve query requests, DNS servers may encounter malicious DNS clients. A client may flood the network with suspicious DNS requests. This affects the performance of the local DNS server and remote nameservers.

Using Cisco Prime Network Registrar, you can resolve this problem by barring malicious clients. You can configure a global ACL of malicious clients that are to be barred, using the blackhole-acl attribute.

### Local Basic or Advanced Web UI

On the Edit Authoritative DNS Server page, expand **Miscellaneous Options and Settings** to view various attributes and their values. For the blackhole-acl attribute value, enter, for example, 10.77.240.73. Then click **Modify Server**.

# Tuning DNS Properties

Here are some tips to tune some of the DNS server properties:

- ***Notify send min. interval*** **DNS server attribute (*notify-min-interval* in the CLI)**—Minimum interval required before sending notification of consecutive changes on the same zone to a server. The preset value is two seconds. For very large zones, you might want to increase this value to exceed the maximum time to send an outbound full zone transfer. This is recommended for secondary servers that receive inbound incremental zone transfers and send out full transfers to other secondaries. These include older BIND servers that do not support incremental zone transfers. Inbound incremental transfers may abort outbound full transfers.
- ***Notify delay between servers*** **DNS server attribute (*notify-send-stagger* in the CLI)**—Interval to stagger notification of multiple servers of a change. The preset value is one second, but you may want to raise it to up to five seconds if you need to support a large number of zone transfers distributed to multiple servers.
- ***Notify wait for more changes*** **DNS server attribute (*notify-wait* in the CLI)**—Time to delay, after an initial zone change, before sending change notification to other nameservers. The preset value is five seconds, but you may want to raise it to 15, for the same reason as given for the *notify-min-interval* attribute.

- ***Max. memory cache size* DNS server attribute (*mem-cache-size* in the CLI)**—Size of the in-memory record cache, in kilobytes. The preset value is 50 MB and this is used to make queries for Authoritative DNS server faster. the rule of thumb is to make it as large as the number of authoritative RRs.
- **Maximum UDP payload size DNS server attribute (*max-udp-payload-size)***—The maximum UDP payload size of the DNS server that responds to the client. You can modify this attribute from a minimum of 512 bytes to a maximum of 4 KB. The default value for this attribute is set to the maximum, that is, 4 KB on the DNS server.
- **IXFR check box in the Foreign Servers section of the Edit DNS Server page, or remote-dns *address/mask* create ixfr in the CLI**—Adding an entry for a server or group of servers allows controlling whether or not IXFR should occur when doing zone transfers from those servers.

# Troubleshooting DNS Servers

Useful troubleshooting hints and tools to diagnose the DNS server and ways to increase performance include:

- **Restoring a loopback zone**—A loopback zone is a reverse zone that enables a host to resolve the loopback address (127.0.0.1) to the name *localhost*. The loopback address is used by the host to enable it to direct network traffic to itself. You can configure a loopback zone manually or you can import it from an existing BIND zone file.
- **Listing the values of the DNS server attributes**—Click **DNS**, then **DNS Server** to open the Edit DNS Server page in the web UI. In the CLI, use **dns show**.
- **Adjusting certain attribute values that could have inherited preset values from previous releases during an upgrade**—For deployments that were upgraded from Cisco Prime Network Registrar 5.5.*x* or earlier, the DNS server might be operating with legacy preset values for critical settings. These preset values are probably not optimal for current systems and can cause performance issues. We strongly recommend that you update the legacy settings to use the new preset values. Table 17-1 lists the old and new preset values, along with a recommended setting for each attribute.

*Table 17-1 DNS Attributes with Changed Preset Values*

| DNS Attribute | 7.0 Preset Value | 7.1 Preset Value | Recommended Setting |
|---|---|---|---|
| *auth-db-cache-kbytes* | 5120 (KB) | 10240 (KB) | 10240 (KB) |
| *axfr-multirec-default* | on | on | on |
| *changeset-db-cache-size* | 10000 (KB) | 10000 (KB) | 10000 (KB) |
| *changeset-db-logs-trimming-interval* | 30m | 30m | 30m |
| *htrim-zone-seek-more-trim-interval* | 5m | 5m | 5m |
| *mem-cache-size* | 10000 (KB) | 50000 (KB) | 50000 (KB) |
| *zone-db-cache-kbytes* | 1024 (KB) | 1024 (KB) | 1024 (KB) |

For many of these attributes, you must enter Expert mode in the web UI or use **set session visibility=3** in the CLI. To change the preset value to the current one, unset the attribute. To change to the recommended setting, change the attribute value.

Be sure to reload the DNS server after saving the settings.

- **Choosing from the DNS log settings to give you greater control over existing log messages**—Use the *Log settings* attribute on the Edit DNS Server page in the web UI, or **dns set log-settings** in the CLI, with one or more of these keyword or numeric values, separated by commas (see Table 17-2). Restart the server if you make any changes to the log settings.

*Table 17-2 DNS Log Settings*

| **Log Setting (Numeric Equivalent)** | **Description** |
|---|---|
| config (1) | Server configuration and deinitialization. |
| ddns (2) | High level dynamic update messages. |
| xfr-in (3) | Inbound full and incremental zone transfers. |
| xfr-out (4) | Outbound full and incremental zone transfers. |
| notify (5) | NOTIFY transactions. |
| datastore (8) | Data store processing that provides insight into various events in the server embedded databases. |
| scavenge (9) | Scavenging of dynamic RRs (see the "Scavenging Dynamic Records" section on page 29-16). |
| scavenge-details (10) | More detailed scavenging output (disabled by default). |
| server-operations (11) | General high-level server events, such as those pertaining to sockets and interfaces. |
| ddns-refreshes (15) | DNS update refreshes for Windows clients (disabled by default). |
| ddns-refreshes-details (16) | RRs refreshed during DNS updates for Windows clients (disabled by default). |
| ddns-details (17) | RRs added or deleted due to DNS updates. |
| tsig (18) | Logs events associated with Transaction Signature (TSIG) DNS updates (see the "Transaction Security" section on page 29-9). |
| tsig-details (19) | More detailed logging of TSIG DNS updates (disabled by default). |
| activity-summary (20) | Summary of activities in the server. You can adjust the interval at which these summaries are taken using the *activity-summary-interval* attribute, which defaults to five-minute intervals (you can adjust this interval using **dns set activity-summary-interval**). |
| query-errors (21) | Logs errors encountered while processing DNS queries. |
| config-details (22) | Generates detailed information during server configuration by displaying all configured and assumed server attributes (disabled by default). |
| incoming-packets (23) | Incoming data packets. |
| outgoing-packets (24) | Outgoing data packets. |
| xfer-in-packets (25) | Incoming full zone transfer (XFR) packets. |
| query-packets (26) | Incoming query packets. |
| notify-packets (27) | NOTIFY packets. |
| ddns-packets (28) | DNS Update packets. |
| xfer-out-packets (29) | Outgoing XFR packets. |
| ha-details (30) | Generates detailed logging of High-Availability (HA) DNS information. |

- **Using the nslookup utility to test and confirm the DNS configuration**—This utility is a simple resolver that sends queries to Internet nameservers. To obtain help for the **nslookup** utility, enter **help** at the prompt after you invoke the command. Use only fully qualified names with a trailing dot to ensure that the lookup is the intended one. An **nslookup** begins with a reverse query for the nameserver itself, which may fail if the server cannot resolve this due to its configuration. Use the **server** command, or specify the server on the command line, to ensure that you query the proper server. Use the **–debug**, or better yet, the **–d2**, flag to dump the responses and (with **–d2**) the queries being sent.
- **Using the dig utility to troubleshoot DNS Server** —dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. To obtain help for the **dig** utility, enter **help** at the prompt after you invoke the command.

  Although dig is normally used with command-line arguments, it also has a batch mode of operation for reading lookup requests from a file. Unlike earlier versions, the BIND9 implementation of dig allows multiple lookups to be issued from the command line. Unless you specifically query a specific name server, dig tries each of the servers listed in /etc/resolv.conf. When no command line arguments or options are given, dig performs an NS query for the root ".". A typical invocation of dig looks like: dig @server name type where server is the name or IP address of the name server to query.