Managing Authoritative DNS Server

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

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 Setting General DNS Server Properties, on page 2
- **Log Settings**—See Specifying Log Settings, on page 2
- **Packet Logging**—See Enabling Packet Logging, on page 3
- **Activity Summary Settings**—See Specifying Activity Summary Settings, on page 5
- **Top Names Settings**—See Specifying Top Names Settings, on page 28
- **TLS Settings**—See Specifying TLS Settings, on page 28
- **Round-Robin server processing**—See Enabling Round-Robin, on page 30
- **Enabling Weighted Round-Robin**—See Enabling Weighted Round-Robin, on page 31
- **Enabling incremental zone transfers**—See Enabling Incremental Zone Transfers (IXFR) , on page 32
- **Restricting Zone Queries**—See Restricting Zone Queries, on page 32
- **Enabling NOTIFY packets**—See Enabling NOTIFY, on page 33

Note To enable GSS-TSIG support, you must set *tsig-processing* to none, and *gss-tsig-processing* to 'ddns, query' to support both ddns and query.

- **Blocking recursive queries**—See Blocking Recursive Queries from Authoritative Server, on page 34

Setting General DNS Server Properties

You can display general DNS 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 *"Managing DNS Update" chapter in Cisco Prime Network Registrar 11.0 DHCP User Guide*).

The following subsections describe some of the more common property settings. They are listed in Setting DNS Server Properties, on page 1.

Local Basic or Advanced Web UI

Step 1 To access the server properties, from the **Deploy** menu, choose **DNS Server** under the **DNS** submenu to open the Manage DNS Authoritative Server page. The page displays all the DNS server attributes.

Step 2 Modify the attributes as per your requirements.

Step 3 Click **Save** to save the DNS server attribute modifications.

CLI Commands

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

Specifying Log Settings

The *server-log-settings* attribute determines which events to log in the DNS log files. Default flags are activity-summary, config, update, xfr-in, xfr-out, scp, scavenge, server-operations, and ha.

Logging additional detail about events can help analyze a problem. However, leaving detailed logging enabled for a long period can fill up the log files.

The possible options are:

- **activity-summary**—This setting enables logging of DNS statistic messages at the interval specified by *activity-summary-interval*. The type of statistics logged can be controlled with *activity-counter-log-settings* and *activity-summary-type*.
- **config**—This setting enables logging of DNS server configuration and de-initialization messages.
- **config-detail**—This setting enables logging of detailed configuration messages (that is, detailed zone configuration logging).

- **db**—This setting enables logging of database processing messages. Enabling this flag provides insight into various events in the server's embedded databases.
- **dnssec**—This setting enables log messages associated with DNSSEC processing.
- **ha**—This setting enables logging of HA DNS messages.
- **host-health-check**—This setting enables logging associated with DNS Host Health Check.
- **notify**—This setting enables logging of messages associated with NOTIFY processing.
- **query**—This setting enabled logging of messages associated with QUERY processing.
- **scavenge**—This setting enables logging of DNS scavenging messages.
- **scp**—This setting enabled logging associated with SCP messages handling.
- **server-operations**—This setting enables logging of general server events, such as those pertaining to sockets and interfaces.
- **tsig**—This setting enables logging of events associated Transaction Signature (TSIG).
- **update**—This setting enables logging of DNS Update message processing.
- **xfr-in**—This setting enables logging of inbound full and incremental zone transfers.
- **xfr-out**—This setting enables logging of outbound full and incremental zone transfers.

Enabling Packet Logging

Cisco Prime Network Registrar supports packet logging for Authoritative DNS server to help analyze and debug the Authoritative DNS server activity. The packet logging settings determine the type of packet logging (summary or detail), the type of packets logged, and to which log file the messages are logged. By default, the Authoritative DNS server does not log any packet log messages.

Use the following server level attributes to enable packet logging for the Authoritative DNS server:

Table 1: Authoritative DNS Server Packet Logging Attributes

Attribute	Description
Packet Logging (*packet-logging*)	Determines the type of packet logging that is logged to the DNS logs. The type of DNS packets logged can be controlled with the *packet-log-settings* attribute. • **disabled**—This settings disables logging of DNS packets. • **summary**—This setting enables one line summary logging of DNS packets. • **detail**—This setting enables detailed packet tracing of DNS packets. **Note:** While packet logging can be helpful for debugging and troubleshooting, it does have an impact on DNS server performance. Therefore, Cisco does not recommend leaving packet logging enabled in production environments.
Packet Logging File (*packet-logging-file*)	Determines the destination log of packet log messages when packet logging is enabled. • **dns**—Packet logging messages are logged to the standard DNS log file (name_dns_1_log*). • **packet**—Packet logging messages are logged to a separate DNS packet log file (dns_packet_log*).

Attribute	Description
Packet Log Settings (*packet-log-settings*)	Determines the type of DNS messages to log if packet logging has been enabled. Packet logging can be enabled by configuring the *packet-logging* attribute. • **all-in**—This setting enables logging of all incoming packets. **Note:** This is equivalent to enabling all the -in settings. • **all-out**—This setting enabled logging of all outgoing packets. **Note:** This is equivalent to enabling all the -out settings. • **ha-in**, **ha-out**—These settings enable logging of HA DNS messages except for HA heartbeat and frame ACK messages which are controlled by the ha-heartbeat-in, ha-heartbeat-out and ha-frameack-in, ha-frameack-out settings, respectively. • **ha-heartbeat-in**, **ha-heartbeat-out**—These settings enable logging of HA DNS heartbeat messages. • **ha-frameack-in**, **ha-frameack-out**—These settings enable logging of HA DNS frame ACK messages. • **notify-in**, **notify-out**—These settings enable logging of DNS NOTIFY messages. • **update-in**, **update-out**—These settings enable logging of DNS UPDATE messages. • **xfr-in**, **xfr-out**—These settings enable logging of DNS IXFR and AXFR messages.

Local Advanced Web UI

Step 1 On the Manage DNS Authoritative Server page, under the **Packet Logging** section, select the value for **packet-logging** from the drop-down list. The value can be **summary** or **detail**.

Step 2 For the *packet-log-settings* attribute, check the desired check boxes.

Step 3 Click **Save** to save the changes.

CLI Commands

Use **dns set packet-logging=summary** to enable one line summary packet logging.

Use **dns set packet-logging=detail** to enable detailed packet tracing.

Use **dns set packet-log-settings**=*value* to set the type of packets to log when packet logging is enabled.

Note Reloading of Authoritative DNS server is not required for the *packet-logging* and *packet-log-settings* attributes to take effect immediately (similar to log settings). However, the *packet-logging-file* attribute requires a Authoritative DNS server reload.

Specifying Activity Summary Settings

Note To specify the activity summary settings, you have to check *activity-summary* under the Log Settings.

You can specify the interval at which to log activity summary information using the Statistics Interval (*activity-summary-interval*) attribute. Enable the *activity-summary* attribute in the Log Settings (*server-log-settings*) attribute to set the seconds between DNS activity summary log messages. The *activity-summary-interval* attribute has a default value of 60 seconds.

The Authoritative DNS server logs sample and/or total statistics based on the option you check for the Statistics Type (*activity-summary-type*) attribute. The default value is "sample".

The option checked for the Statistics Settings (*activity-counter-log-settings*) attribute controls what activity counters a DNS server uses for logging.

Note *activity-summary-type* and *activity-counter-log-settings* take effect without a reload as soon as the DNS server object or the session is saved.

The possible settings are:

- **cache**—Log query cache related counters.

  For the list of activity summary statistics that are displayed in the logs for the **cache** setting, see Cache Statistics, on page 6.

- **db**—Log database counters.

  For the list of activity summary statistics that are displayed in the logs for the **db** setting, see DB Statistics, on page 7.

- **errors**—Log error related counters.

  For the list of activity summary statistics that are displayed in the logs for the **errors** setting, see Errors Statistics, on page 9.

- **ha**—Log HA related counters.

  For the list of activity summary statistics that are displayed in the logs for the **ha** setting, see HA Statistics, on page 10.

- **host-health-check**—Log DNS Host Health Check counters.

  For the list of activity summary statistics that are displayed in the logs for the **host-health-check** setting, see Host Health Check Statistics, on page 14.

- **ipv6**—Log IPv6 related counters.

  For the list of activity summary statistics that are displayed in the logs for the **ipv6** setting, see IPv6 Statistics, on page 16.

- **maxcounters**—Log maxcounters related counters.

  For the list of activity summary statistics that are displayed in the logs for the **maxcounters** setting, see Maxcounters Statistics, on page 16.

- **performance**—Log performance related counters.

  For the list of activity summary statistics that are displayed in the logs for the **performance** setting, see Performance Statistics, on page 17.

- **query**—Log query related counters.

  For the list of activity summary statistics that are displayed in the logs for the **query** setting, see Query Statistics, on page 19.

- **security**—Log security related counters.

  For the list of activity summary statistics that are displayed in the logs for the **security** setting, see Security Statistics, on page 22.

- **system**—Log system related counters.

  For the list of activity summary statistics that are displayed in the logs for the **system** setting, see System Statistics, on page 24.

- **top-names**—Log the top names queried and hit count.

  For the list of activity summary statistics that are displayed in the logs for the **top-names** setting, see Top Names Statistics, on page 25.

- **update**—Log DNS Update related counters.

  For the list of activity summary statistics that are displayed in the logs for the **update** setting, see Update Statistics, on page 25.

Activity Summary Statistics

Following sections describe the list of activity summary statistics that are displayed in the logs under each of the *activity-counter-log-settings* category.

Cache Statistics

The **cache** activity-counter-log-settings logs query cache related counters.

The cache activity summary statistics are logged under the **Query-Cache** sub category.

Sample log message:

```
10/22/2021 16:47:05 name/dns/1 Activity Stats 0 21333 [Query-Cache] Sample since Fri Oct
22 16:46:05 2021: size=number, #-records=number, #-rrs=number, nxdomain=number, hits=number,
 misses=number, full=number, collisions=number
```

Table 2: Cache Statistics

Activity Summary Name	Statistic[1]	Description
size	cache-size	Reports the size of in-memory query cache in bytes.
#-records	cache-records	Reports the total number of RR name sets stored in the query cache.
#-rrs	cache-rrs	Reports the total number of RRs stored in the query cache.

Activity Summary Name	Statistic[1]	Description
nxdomain	cache-nxdomain	Reports the total number of NXDOMAIN entries in the query cache.
hits	cache-hits	Reports the number of times incoming client queries were found in the query cache.
misses	cache-misses	Reports the number of times incoming client queries were not found in the query cache.
full	cache-full	Reports the number of times the query cache was found to be at its configured limit (*mem-cache-size*).
collisions	N/A	Reports the number of times different FQDNs mapped to the same memory cache index. A high number of collisions indicates that the configured cache size may be too small.

[1] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

DB Statistics

The **db** activity-counter-log-settings logs database counters.

Sample log message:

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21344 [Cset-DB] Sample since Fri Oct 22
16:43:05 2021: reads=number, writes=number, deletes=number, csets-trimmed=number,
conflicts=number, insufficient-history=number, txns=number, txn-commits=number,
txn-aborts=number, txn-locked=number, txn-unlocked=number, check-pts=number,
log-purges=number, #-logs-purged=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21345 [RR-DB] Sample since Fri Oct 22
16:43:05 2021: reads=number, writes=number, deletes=number, check-pts=number,
log-purges=number, #-logs-purged=number, txns=number, txn-commits=number, txn-aborts=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21352 [Cset-Queue] Sample since Fri Oct 22
 16:43:05 2021: cset-count=number, cset-queue-max-size=number, commits=number,
commits-failed=number
```

Table 3: DB Statistics

Activity Summary Name	Logging Sub Category	Statistic[2]	Description
txn	RR-DB	rrdb-txn	Reports the total number of RR DB database transactions.

Activity Summary Name	Logging Sub Category	Statistic[2]	Description
txn-commits	RR-DB	rrdb-txn-commits	Reports the total number of RR DB database transactions committed.
txn-aborts	RR-DB	rrdb-txn-aborts	Reports the total number of RR DB database transactions aborted.
reads	RR-DB	rrdb-reads	Reports the total number of RR DB read operations.
writes	RR-DB	rrdb-writes	Reports the total number of RR DB write operations.
deletes	RR-DB	rrdb-deletes	Reports the total number of RR DB delete operations.
check-pts	RR-DB	rrdb-check-pts	Reports the total number of RR DB check point operations.
log-purges	RR-DB	rrdb-log-purges	Reports the total number of RR DB log purge operations.
#-logs-purged	RR-DB	rrdb-log-purges-count	Reports the total number of RR DB logs purged.
cset-count	Cset-Queue	csetq-count	Reports the total of number of change sets queued up to be written to the cset DB.
cset-queue-max-size	Cset-Queue	N/A	The maximum number of cset entries queued during this interval.
commits	Cset-Queue	N/A	Number of DB commits that happened in the last interval.
commits-failed	Cset-Queue	N/A	Number of DB commits that failed in the last interval.
txns	Cset-DB	csetdb-txn	Reports the total number of CSET DB database transactions.
txn-commits	Cset-DB	csetdb-txn-commits	Reports the total number of CSET DB database transactions committed.
txn-aborts	Cset-DB	csetdb-txn-aborts	Reports the total number of CSET DB database transactions aborted.
reads	Cset-DB	csetdb-reads	Reports the total number of CSET DB read operations.
writes	Cset-DB	csetdb-writes	Reports the total number of CSET DB write operations.

Activity Summary Name	Logging Sub Category	Statistic[2]	Description
deletes	Cset-DB	csetdb-deletes	Reports the total number of CSET DB delete operations.
csets-trimmed	Cset-DB	csetdb-csets-trimmed	Reports the total number of change sets trimmed from the CSET DB by the history trimming process or by inline trimming.
check-pts	Cset-DB	csetdb-check-pts	Reports the total number of CSET DB check point operations.
log-purges	Cset-DB	csetdb-log-purges	Reports the total number of CSET DB log purge operations.
#-logs-purged	Cset-DB	csetdb-log-purges-count	Reports the total number of CSET DB logs purged.

[2] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Errors Statistics

The **errors** activity-counter-log-settings logs error related counters.

The errors activity summary statistics are logged under the **Errors** sub category.

Sample log message:

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21492 [Errors] Sample since Fri Oct 22
16:43:05 2021: update-errors=number, update-prereq-fail=number, ixfr-in-errors=number,
ixfr-out-errors=number, axfr-in-errors=number, axfr-out-errors=number,
xfer-in-auth-errors=number, xfer-failed-attempts=number, sent-total-errors=number,
sent-refusal-errors=number, sent-format-errors=number, exceeded-max-dns-packets=number
```

Table 4: Errors Statistics

Activity Summary Name	Statistic[3]	Description
update-errors	update-errors	Reports the total number of updates resulting in errors. This excludes negative responses to update prerequisite checks, and TSIG responses. Both update packets and updates generated by the CNR UIs may be included in this count.
update-prereq-fail	update-prereq-fail	Reports the total number of updates resulting in prerequisite failures.
ixfr-in-errors	ixfr-in-errors	Reports the total in-bound IXFR errors, excluding packet format errors.

Activity Summary Name	Statistic[3]	Description
ixfr-out-errors	ixfr-out-errors	Reports the total IXFR error responses sent, excluding packet format errors.
axfr-in-errors	axfr-in-errors	Reports the total in-bound AXFR errors, excluding packet format errors.
axfr-out-errors	axfr-out-errors	Reports the total AXFR error responses sent, excluding packet format errors.
sent-total-errors	sent-total-errors	Reports the total number of requests the server answered with errors (RCODE values other than 0,3,6,7, and 8). See RFC 1611.
sent-format-errors	sent-format-errors	Reports the number of requests received that were unparseable. See RFC 1611.
sent-refusal-errors	sent-refusal-errors	Reports the number of requests that resulted in REFUSED. See RFC1611.
xfer-in-auth-errors	xfer-in-auth-errors	Reports the number of secondary IXFR/AXFR requests that were refused because of authorization errors.
xfer-failed-attempts	xfer-failed-attempts	Reports the number of secondary IXFR/AXFR failures, excluding authorization refusals.
exceeded-max-dns-packets	exceeded-max-dns- packets	Reports the number of times inbound packets exceeded the maximum DNS packets defined by *max-dns-packets*.

[3] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

HA Statistics

The **ha** activity-counter-log-settings logs HA related counters.

Sample log message:

```
name_dns_1_log:11/19/2021 11:43:23 name/dns/1 Activity Stats 0 20005 [HA-State] Sample since
 Fri Nov 19 11:41:35 2021: current=state, last-state-change=time, normal=number,
comm-interrupted=number, negotiate=number, start-up=number, partner-down=number

name_dns_1_log:11/19/2021 12:09:23 name/dns/1 Activity Stats 0 21341 [HA-Requests-Sent]
Sample since Fri Nov 19 12:08:23 2021: requests-sent=number, last-req-sent=Heartbeat @ Fri
 Nov 19 12:09:21 2021 (xid: 207), update=number, heart-beat=number, zone-sync=number,
rr-sync=number, rr-recon=number, connect=number, negotiate=number, shutdown=number,
truncated=number

name_dns_1_log:11/18/2021 13:07:26 name/dns/1 Activity Stats 0 21342 [HA-Requests-Rcvd]
```

```
Sample since Thu Nov 18 13:04:12 2021: requests-recv=number, last-req-recv=Heartbeat @ Thu
 Nov 18 13:07:07 2021 (xid: 207), update=number, heart-beat=number, zone-sync=number,
rr-sync=number, rr-recon=number, connect=number, negotiate=number, shutdown=number,
truncated=number

11/29/2021  9:02:44 name/dns/1 Activity Stats 0 21343 [HA-Errors] Sample since Mon Nov 29
09:01:44 2021: update-reject=number, resp-mismatch=number, resp-inconsistent=number,
resp-servfail=number, resp-unknown=number

11/29/2021 14:49:32 name/dns/1 Activity Stats 0 20006 [HA-Zone-Sync] Sample since Mon Nov
29 14:47:32 2021: sync=number, sync-completed=number, sync-failed=number,
zone-mismatch=number, full-resync=number, conflict=number, merge=number, discard=number
```

Table 5: HA Statistics

Activity Summary Name	Logging Sub Category	Statistic[4]	Description
comm-interrupted	HA-State	ha-state-comm-interrupted	Number of occurrences where the server enters the communication-interrupted state (HA_STATE_COMMINTR).
partner-down	HA-State	ha-state-partner-down	Number of occurrences where the server enters the partner-down state (HA_STATE_PARTNERDOWN).
negotiate	HA-State	ha-state-negotiating	Number of occurrences where the server enters the Negotiating state (HA_STATE_NEGOTIATING).
current	HA-State	ha-state-current	Current HA server state.
last-state-change	HA-State	ha-state-last-change-time	Last time when HA state changed.
start-up	HA-State	ha-state-startup	Number of occurrences where the server enters Startup State (HA_STARTUP).
normal	HA-State	ha-state-normal	Number of occurrences where the server enters Normal State (HA_NORMAL).
connect	HA-Requests-Sent	ha-msg-connect-sent	Number of connection establishment request messages sent (HA_DNS_ESTABLISH_CONNECTION).
rr-recon	HA-Requests-Sent	ha-msg-reconcile-sent	Number of zone reconciliation request messages sent (HA_DNS_RECONCILIATION).
heart-beat	HA-Requests-Sent	ha-msg-heartbeat-sent	Number of heartbeat request messages sent (HA_DNS_HEARTBEAT).
zone-sync	HA-Requests-Sent	ha-msg-zonesync-sent	Number of zone synchronization request messages sent (HA_DNS_ZONE_SYNC).
rr-sync	HA-Requests-Sent	ha-msg-rrsync-sent	Number of rr-sync request messages sent (HA_DNS_RR_SYNC).

Activity Summary Name	Logging Sub Category	Statistic[4]	Description
update	HA-Requests-Sent	ha-msg-rrupdate-sent	Number of rr-update request messages sent (HA_DNS_RR_UPDATE).
N/A	N/A	ha-msg-resp-sent	Number of response messages sent. Response messages are used to acknowledge all types of request messages.
shutdown	HA-Requests-Sent	ha-msg-shutdown-sent	Number of shutdown request messages sent.
requests-sent	HA-Requests-Sent	ha-msg-req-sent	Number of HA request messages sent to the HA partner.
last-req-sent	HA-Requests-Sent	ha-msg-req-sent-time	Specifies the date and time the HA server last sent a request message to the HA partner.
negotiate	HA-Requests-Sent	N/A	Number of negotiate HA message sent.
truncated	HA-Requests-Sent	N/A	Number of HA messages sent that were truncated.
connect	HA-Requests-Rcvd	ha-msg-connect-recv	Number of connection establishment request messages received (HA_DNS_ESTABLISH_CONNECTION).
rr-recon	HA-Requests-Rcvd	ha-msg-reconcile-recv	Number of zone reconciliation request messages received (HA_DNS_RECONCILIATION).
heart-beat	HA-Requests-Rcvd	ha-msg-heartbeat-recv	Number of heartbeat request messages received (HA_DNS_HEARTBEAT).
zone-sync	HA-Requests-Rcvd	ha-msg-zonesync-recv	Number of zone synchronization request messages received (HA_DNS_ZONE_SYNC).
rr-sync	HA-Requests-Rcvd	ha-msg-rrsync-recv	Number of rr-sync messages request received (HA_DNS_RR_SYNC).
update	HA-Requests-Rcvd	ha-msg-rrupdate-recv	Number of rr-update request messages received (HA_DNS_RR_UPDATE).
N/A	N/A	ha-msg-resp-recv	Number of response messages received. Response messages are used to acknowledge all types of request messages.
shutdown	HA-Requests-Rcvd	ha-msg-shutdown-recv	Number of shutdown request messages received.

Activity Summary Name	Logging Sub Category	Statistic[4]	Description
requests-recv	HA-Requests-Rcvd	ha-msg-req-recv	Number of HA request messages received from the HA partner.
last-req-recv	HA-Requests-Rcvd	ha-msg-req-recv-time	Specifies the date and time the HA server last received a request message from the HA partner.
negotiate	HA-Requests-Rcvd	N/A	Number of negotiate HA message received.
truncated	HA-Requests-Rcvd	N/A	Number of HA messages received that were truncated.
update-reject	HA-Errors	ha-update-reject	Number of DNS updates rejected by the server.
resp-mismatch	HA-Errors	ha-zone-mismatch	Number of zones reporting a mismatch error (HA_DNS_RESP_ERR_MISMATCH).
resp-servfail	HA-Errors	ha-resp-servfail	Number of responses reporting a server failure error (HA_DNS_RESP_ERR_SERVFAIL).
resp-inconsistent	HA-Errors	ha-resp-inconsistent	Number of responses reporting an inconsistent server state (HA_DNS_RESP_ERR_INCONSISTENT_STATE).
resp-unknown	HA-Errors	ha-resp-unknown	Number of responses with an unknown message type (HA_DNS_RESP_ERR_UNKNOWN_MSG_TYPE).
full-resync	HA-Zone-Sync	ha-full-zone-resync	Number of zones requiring full-zone resynchronization for nameset reconciliation.
conflict	HA-Zone-Sync	ha-sync-conflict	Number of zones with name conflicts during nameset reconciliation.
discard	HA-Zone-Sync	ha-sync-discard-name	Number of name conflicts where one nameset must be discarded to synchronize the zone.
merge	HA-Zone-Sync	ha-sync-merge-name	Number of name conflicts which the namesets can be merged to synchronize the zone.
sync	HA-Zone-Sync	N/A	Number of zones that were requested to be synced.

Activity Summary Name	Logging Sub Category	Statistic[4]	Description
sync-completed	HA-Zone-Sync	N/A	Number of zones where sync was completed.
sync-failed	HA-Zone-Sync	N/A	Number of zones where sync failed.
zone-mismatch	HA-Zone-Sync	N/A	Number of zones that do not match on HA Main and HA Backup.

[4] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Host Health Check Statistics

The **host-health-check** activity-counter-log-settings logs DNS Host Health Check counters.

The host health check activity summary statistics are logged under the **HHC** sub category.

Sample log message:

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21509 [HHC] Sample since Fri Oct 22 16:43:05
 2021: hhc-domains=number, hhc-domains-failed=number, hhc-domains-passed=number,
hhc-rrs=number, hhc-rrs-passed=number, hhc-rrs-failed=number, hhc-ping-domains=number,
hhc-ping-domains-failed=number, hhc-ping-domains-passed=number, hhc-ping-rrs=number,
hhc-ping-rrs-passed=number, hhc-ping-rrs-failed=number, hhc-gtp-echo-domains=number,
hhc-gtp-echo-domains-failed=number, hhc-gtp-echo-domains-passed=number,
hhc-gtp-echo-rrs=number, hhc-gtp-echo-rrs-passed=number, hhc-gtp-echo-rrs-failed=number
```

Table 6: Host Health Check Statistics

Activity Summary Name	Statistic[5]	Description
hhc-domains	hhc-domains	Reports the total number of domains checked for Host Health Check.
hhc-domains-failed	hhc-domains-failed	Reports the total number of domains check failed for Host Health Check. When all the RRs in the RR set are down, this stat is incremented.
hhc-domains-passed	hhc-domains-passed	Reports the total number of domains check passed for Host Health Check. Any A/AAAA RR in the RR set is up, this stat is incremented.
hhc-rrs	hhc-rrs	Reports the total number of RRs checked for Host Health Check.
hhc-rrs-passed	hhc-rrs-passed	Reports the total number of RRs that have passed Host Health Check health check.

Activity Summary Name	Statistic[5]	Description
hhc-rrs-failed	hhc-rrs-failed	Reports the total number of RRs that have failed Host Health Check health check.
hhc-ping-domains	hhc-ping-domains	Reports the total number of domains checked for ping Host Health Check.
hhc-ping-domains-failed	hhc-ping-domains-failed	Reports the total number of domains check failed for ping Host Health Check. When all the RRs in the RR set are down, this stat is incremented.
hhc-ping-domains-passed	hhc-ping-domains-passed	Reports the total number of domains check passed for ping Host Health Check. When any RR in the RR set is up, this stat is incremented.
hhc-ping-rrs	hhc-ping-rrs	Reports the total number of RRs checked for ping Host Health Check.
hhc-ping-rrs-failed	hhc-ping-rrs-failed	Reports the total number of RRs that have failed ping Host Health Check health check.
hhc-ping-rrs-passed	hhc-ping-rrs-passed	Reports the total number of RRs that have passed ping Host Health Check health check.
hhc-gtp-echo-domains	hhc-gtp-echo-domains	Reports the total number of domains checked for gtp-echo Host Health Check.
hhc-gtp-echo-domains-failed	hhc-gtp-echo-domains-failed	Reports the total number of domains check failed for gtp-echo Host Health Check. When all the RRs in the RR set are down, this stat is incremented.
hhc-gtp-echo-domains-passed	hhc-gtp-echo-domains-passed	Reports the total number of domains check passed for gtp-echo Host Health Check. When any RR in the RR set is up, this stat is incremented.
hhc-gtp-echo-rrs	hhc-gtp-echo-rrs	Reports the total number of RRs checked for gtp-echo Host Health Check.
hhc-gtp-echo-rrs-failed	hhc-gtp-echo-rrs-failed	Reports the total number of RRs that have failed gtp-echo Host Health Check health check.
hhc-gtp-echo-rrs-passed	hhc-gtp-echo-rrs-passed	Reports the total number of RRs that have passed gtp-echo Host Health Check health check.

[5] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

IPv6 Statistics

The **ipv6** activity-counter-log-settings logs IPv6 related counters.

The IPv6 activity summary statistics are logged under the **Perform** sub category.

Sample log message:

```
11/26/2021 15:25:36 name/dns/1 Activity Stats 0 03523 [Perform] Sample since Fri Nov 26
15:24:36 2021: pkts-in=number, pkts-out=number, pkts-in-udp=number, pkts-out-udp=number,
pkts-in-tcp=number, pkts-out-tcp=number, ipv4-pkts-in=number, ipv4-pkts-out=number,
ipv6-pkts-in=number, ipv6-pkts-out=number, queries=number, updates=number, notifies-in=number,
 notifies-out=number, notify-errors=number, ixfrs-in=number, ixfrs-out=number,
ixfrs-full-resp=number, axfrs-in=number, axfrs-out=number, xfrs-in-at-limit=number,
xfrs-out-at-limit=number, responses-with-NOTIMP=number, total-zones=number, total-rrs=number
```

Table 7: IPv6 Statistics

Activity Summary Name	Statistic[6]	Description
ipv6-pkts-in	ipv6-packets-in	Total number of IPv6 packets received.
ipv6-pkts-out	ipv6-packets-out	Total number of IPv6 packets sent.

[6] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Maxcounters Statistics

The **maxcounters** activity-counter-log-settings logs maxcounters related counters.

The maxcounters activity summary statistics are logged under the **Max-Counters** sub category.

Sample log message:

```
10/22/2021 16:40:05 name/dns/1 Activity Stats 0 21353 [Max-Counters] Sample since Tue Oct
19 19:32:39 2021: concurrent-xfrs-in=number, concurrent-xfrs-out=number,
ha-update-latency-max=number, ha-batch-count-limit=number, ha-rr-pending-list=number,
ha-rr-active-list=number, ha-persisted-edit-list=number, dns-concurrent-packets=number,
pn-conn-max-conns=number
```

Table 8: Maxcounters Statistics

Activity Summary Name	Statistic[7]	Description
concurrent-xfrs-in	concurrent-xfrs-in	Reports the maximum number of concurrent threads processing inbound transfers during the last sampling period.
concurrent-xfrs-out	concurrent-xfrs-out	Reports the maximum number of concurrent threads processing outbound transfers during the last sampling period.

Activity Summary Name	Statistic[7]	Description
ha-batch-count-limit	ha-batch-count-limit	Reports the number of times the *ha-dns-max-batch-count* limit was reached during the last sampling period.
ha-rr-pending-list	ha-rr-pending-list	Reports the maximum number of RRs in the pending List, waiting acknowledgement from the HA DNS backup server, during the last sampling period.
ha-rr-active-list	ha-rr-active-list	Reports the maximum number of RRs in the active list, waiting to be sent to the HA DNS backup server, during the last sampling period.
ha-persisted-edit-list	ha-persisted-edit-list	Reports the maximum number of names persisted in the edit list database during the last sampling period.
ha-update-latency- max	ha-update-latency-max	Reports the maximum DNS update latency in seconds, during the last sampling period. Latency is measured as the time an update remains in the pending List.
dns-concurrent- packets	dns-concurrent-packets	Reports the maximum number of concurrent packets processed by the DNS server during the sampling period.

[7] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Performance Statistics

The **performance** activity-counter-log-settings logs performance related counters.

The performance activity summary statistics are logged under the **Perform** sub category.

Sample log message:

```
10/22/2021 16:40:05 name/dns/1 Activity Stats 0 03523 [Perform] Sample since Tue Oct 19
19:32:39 2021: pkts-in=number, pkts-out=number, pkts-in-udp=number,pkts-out-udp=number,
pkts-in-tcp=number, pkts-out-tcp=number, ipv4-pkts-in=number, ipv4-pkts-out=number,
ipv6-pkts-in=number, ipv6-pkts-out=number, queries=number, updates=number,notifies-in=number,
 notifies-out=number, notify-errors=number, ixfrs-in=number, ixfrs-out=number,
ixfrs-full-resp=number, axfrs-in=number, axfrs-out=number, xfrs-in-at-limit=number,
xfrs-out-at-limit=number, responses-with-NOTIMP=number, total-zones=number, total-rrs=number
```

Table 9: Performance Statistics

Activity Summary Name	Statistic[8]	Description
ipv4-pkts-in	ipv4-packets-in	Reports the total number of IPv4 packets received.

Activity Summary Name	Statistic[8]	Description
ipv4-pkts-out	ipv4-packets-out	Reports the total number of IPv4 packets sent.
N/A	updated-rrs	Reports the total number of RRs added and deleted, including updates from the CPNR UIs, whether or not there were database errors.
updates	update-packets	Reports the number of successful DNS updates.
queries	queries-total	Total number of queries received by the DNS Server.
ixfrs-out	ixfrs-out	Reports the number of successful outbound incremental transfers.
ixfrs-in	ixfrs-in	Reports the number of successful inbound incremental transfers, including incremental requests that resulted in full zone transfers.
ixfrs-full-resp	ixfrs-full-resp	Reports the number of outbound full zone transfers in response to IXFR requests. These may have been due to IXFR errors, insufficient serial history, or too many changes in the zone.
axfrs-in	axfrs-in	Reports the number of successful inbound AXFRs.
axfrs-out	axfrs-out	Reports the number of successful outbound full zone transfers, including those counted in *ixfrs-full-resp*.
xfrs-in-at-limit	xfrs-in-at-limit	Reports the number of times that inbound transfers reached the concurrent limit.
xfrs-out-at-limit	xfrs-out-at-limit	Reports the number of times that outbound transfers reached the concurrent limit.
notifies-out	notifies-out	Reports the number of outbound notifies. Each notify packet sent is counted separately.
notifies-in	notifies-in	Reports the number of inbound notifies. Each notify packet received is counted separately.
notify-errors	N/A	Errors detected while processing notify requests.
total-zones	N/A	Total number of zones configured.
total-rrs	N/A	Total number of RRs across all configured zones.
responses-with-NOTIMP	responses-with-NOTIMP	Reports the numbers of requests with OP codes that are not implemented.
pkts-in	packets-in	Reports the total number of packets received.
pkts-out	packets-out	Reports the total number of packets sent.

Activity Summary Name	Statistic[8]	Description
pkts-in-udp	packets-in-udp	Reports the total number of UDP packets received.
pkts-out-udp	packets-out-udp	Reports the total number of UDP packets sent.
pkts-in-tcp	packets-in-tcp	Reports the total number of TCP packets received.
pkts-out-tcp	packets-out-tcp	Reports the total number of TCP packets sent.
ipv6-pkts-in	ipv6-packets-in	Reports the total number of IPv6 packets received.
ipv6-pkts-out	ipv6-packets-out	Reports the total number of IPv6 packets sent.

[8] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Query Statistics

The **query** activity-counter-log-settings logs query related counters.

Sample log message:

```
10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21168 [Query] Sample since Fri Oct 22
16:40:05 2021: total=number, dropped=number, acl-failures=number, udp=number, tcp=number,
ipv4=number, ipv6=number, tls=number, tls-failures=number, dropped-recursive=number,
dropped-unwanted-class=number, dropped-unwanted-type=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21333 [Query-Cache] Sample since Fri Oct
22 16:43:05 2021: size=number, #-records=number, #-rrs=number, nxdomain=number, hits=number,
 misses=number, full=number, collisions=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21331 [Query-Type] Sample since Fri Oct 22
 16:40:05 2021: A=number, AAAA=number, ANY=number, CNAME=number, MX=number, NAPTR=number,
NS=number,PTR=number, SOA=number, SRV=number, TXT=number, DNSKEY=number, DS=number,
RRSIG=number, NSEC=number, CAA=number, URI=number, other=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21332 [Query-Responses] Sample since Fri
Oct 22 16:40:05 2021: total=number, no-error=number, referrals=number, no-data=number,
nxdomain=number, refused=number, notauth=number, formerr=number, servfail=number, other=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21524 [DNSSEC] Sample since Fri Oct 22
16:40:05 2021: dnssec-zones=number, dnssec-sign-zone=number, dnssec-queries=number,
dnssec-responses=number, dnssec-requests-dropped=number
```

Table 10: Query Statistics

Activity Summary Name	Logging Sub Category	Statistic[9]	Description
hits	Query-Cache	mem-cache-hits	Reports the number of mem-cache lookup hits.

Activity Summary Name	Logging Sub Category	Statistic[9]	Description
misses	Query-Cache	mem-cache-misses	Reports the number of mem-cache lookup misses.
dropped	Query	queries-dropped	Reports the number of non-error dropped packets. Queries restricted by server, TSIG, or update policies are included, but DNS updates, xfer requests, and notifies are excluded.
N/A	N/A	queries-with-edns	Reports the number of OPT RR packets processed.
total	Query	queries-total	Total number of queries received by the DNS Server.
udp	Query	queries-over-udp	Total number of queries received over UDP by the DNS Server.
tcp	Query	queries-over-tcp	Total number of queries received over TCP by the DNS Server.
ipv4	Query	queries-over-ipv4	Total number of IPv4 queries received by the DNS Server.
ipv6	Query	queries-over-ipv6	Total number of IPv6 queries received by the DNS Server.
tls	Query	queries-over-tls	Total number of queries received over TLS by the DNS Server.
tls-failures	Query	queries-over-tls-failed	Total number of TLS queries failed during TLS handshake.
dropped-recursive	Query	queries-dropped-recursive	Number of recursive queries dropped.
dropped-unwanted-class	Query	queries-dropped-unwanted-class	Total number of queries dropped due to unwanted classes. Only queries of class IN are allowed.
dropped-unwanted-type	Query	queries-dropped-unwanted-type	Total number of queries dropped due to unwanted types. Unwanted RR types are specified in the *query-types-unwanted* DNS server attribute.
acl-failures	Query	queries-failed-acl	Reports the number of query ACL (*restrict-query-acl*) failures.
total	Query-Responses	query-answers-total	Reports the total number of query responses.

Activity Summary Name	Logging Sub Category	Statistic[9]	Description
no-error	Query-Responses	query-answers-with-NOERROR	Reports the number of queries that were authoritatively answered.
nxdomain	Query-Responses	query-answers-with-NXDOMAIN	Reports the number of queries that failed with no such name responses.
no-data	Query-Responses	query-answers-with-NODATA	Reports the number of queries that failed with no data (empty answer) responses.
notauth	Query-Responses	query-answers-with-NOTAUTH	Reports the number of queries that failed with not authoritative responses.
referrals	Query-Responses	query-answers-with-referral	Reports the number of requests that were referred to other servers.
refused	Query-Responses	query-answers-with-REFUSED	Reports the number of queries refused.
formerror	Query-Responses	query-answers-with-FORMERR	Reports the number of query responses with rcode of FORMERR.
servfail	Query-Responses	query-answers-with-SERVFAIL	Reports the number of query responses with rcode of SERVFAIL.
other	Query-Responses	query-answers-with-other-errors	Reports the number of queries with other errors.
dnssec-queries	DNSSEC	queries-dnssec	Reports the total number of queries requesting that responses to include DNSSEC related RRs (EDNS option DO bit).
A	Query-Type	queries-type-A	Number of A queries received.
AAAA	Query-Type	queries-type-AAAA	Number of AAAA queries received.
CNAME	Query-Type	queries-type-CNAME	Number of CNAME queries received.
PTR	Query-Type	queries-type-PTR	Number of PTR queries received.
NS	Query-Type	queries-type-NS	Number of NS queries received.
SOA	Query-Type	queries-type-SOA	Number of SOA queries received.
MX	Query-Type	queries-type-MX	Number of MX queries received.
NAPTR	Query-Type	queries-type-NAPTR	Number of NAPTR queries received.
other	Query-Type	queries-type-other	All other queries received.
ANY	Query-Type	queries-type-ANY	Number of ANY queries received.

Activity Summary Name	Logging Sub Category	Statistic[9]	Description
SRV	Query-Type	queries-type-SRV	Number of SRV queries received.
TXT	Query-Type	queries-type-TXT	Number of TXT queries received.
DNSKEY	Query-Type	queries-type-DNSKEY	Number of DNSKEY queries received.
DS	Query-Type	queries-type-DS	Number of DS queries received.
RRSIG	Query-Type	queries-type-RRSIG	Number of RRSIG queries received.
NSEC	Query-Type	queries-type-NSEC	Number of NSEC queries received.
CAA	Query-Type	queries-type-CAA	Number of CAA queries received.
URI	Query-Type	queries-type-URI	Number of URI queries received.

[9] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Security Statistics

The **security** activity-counter-log-settings logs security related counters.

Sample log message:

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21492 [Errors] Sample since Fri Oct 22
16:43:05 2021: update-errors=number, update-prereq-fail=number, ixfr-in-errors=number,
ixfr-out-errors=number, axfr-in-errors=number, axfr-out-errors=number,
xfer-in-auth-errors=number, xfer-failed-attempts=number, sent-total-errors=number,
sent-refusal-errors=number, sent-format-errors=number, exceeded-max-dns-packets=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21332 [Query-Responses] Sample since Fri
Oct 22 16:40:05 2021: total=number, no-error=number, referrals=number,
no-data=number,nxdomain=number, refused=number, notauth=number, formerr=number,
servfail=number, other=number

11/19/2021 16:59:41 name/dns/1 Activity Stats 0 21524 [DNSSEC] Sample since Fri Nov 19
16:58:41 2021: dnssec-zones=number, dnssec-sign-zone=number, dnssec-queries=number,
dnssec-responses=number, dnssec-requests-dropped=number

11/26/2021 16:16:45 name/dns/1 Activity Stats 0 21491 [TSIG] Sample since Fri Nov 26 16:15:45
 2021: tsig-packets=number, badtime=number, badkey=number, badsig=number, badtime-resp=number,
 badkey-resp=number, badsig-resp=number

12/08/2021 12:58:42 name/dns/1 Activity Stats 0 21389 [RPZ] Sample since Wed Dec  8 12:57:03
 2021: rpz-queries=number, rpz-hits=number, rpz-misses=number
```

Table 11: Security Statistics

Activity Summary Name	Logging Sub Category	Statistic[10]	Description
xfer-in-auth-errors	Errors	unauth-xfer-reqs	Reports the number of ACL authorization failures in zone transfers.
N/A	N/A	unauth-update-reqs	Reports the number of ACL authorization failures in DNS updates. Administrative RR updates (from CPNR UIs) are excluded.
refused	Query-Responses	restrict-query-acl	Reports the number of ACL authorization failures in DNS queries.
N/A	N/A	blackhole-acl-dropped-requests	Reports the number of DNS requests dropped by the server subject to *blackhole-acl*.
tsig-packets	TSIG	rcvd-tsig-packets	Reports the number of TSIG RR packets processed, if TSIG processing is enabled for the type of packet.
badtime-resp	TSIG	detected-tsig-bad-time	Reports the number of bad timestamps in incoming TSIG packets.
badkey-resp	TSIG	detected-tsig-bad-key	Reports the number of bad keynames (those with an invalid or unknown key) in incoming TSIG packets.
badsig-resp	TSIG	detected-tsig-bad-sig	Reports the number of bad signatures in incoming TSIG packets.
badtime	TSIG	rcvd-tsig-bad-time	Reports the number of BADTIME errors received after sending a TSIG packet.
badkey	TSIG	rcvd-tsig-bad-key	Reports the number of BADKEY errors received after sending a TSIG packet.
badsig	TSIG	rcvd-tsig-bad-sig	Reports the number of BADSIG errors received after sending a TSIG packet.
dnssec-zones	DNSSEC	dnssec-zones	Reports the number of zones with DNSSEC enabled.
dnssec-sign-zone	DNSSEC	dnssec-sign-zone	Reports the number of times the server signed a DNSSEC zone.
dnssec-queries	DNSSEC	dnssec-queries	Reports the total number of queries requesting that responses to include DNSSEC related RRs (EDNS option DO bit).

Activity Summary Name	Logging Sub Category	Statistic[10]	Description
dnssec-responses	DNSSEC	dnssec-responses	Reports the total number of responses to DNNSEC enabled queries (EDNS option DO bit).
dnssec-requests-dropped	DNSSEC	dnssec-requests-dropped	Reports the total number of DNS requests that were dropped due to the server being in the process of signing a DNSSEC zone.
rpz-queries	RPZ	queries-rpz	Reports the number of queries for Response Policy Zones (RPZ).
rpz-hits	RPZ	query-answers-rpz-hits	Reports the number of RPZ queries that matched RRs in Response Policy Zones.
rpz-misses	RPZ	query-answers-rpz-misses	Reports the number of RPZ queries that did not match RRs in Response Policy Zones.

[10] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

System Statistics

The **system** activity-counter-log-settings logs system related counters.

The system activity summary statistics are logged under the **System** sub category.

Sample log message:

```
10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21493 [System] Sample since Fri Oct 22
16:40:05 2021: pid=number, cpu=number, memory=number, virtual=number, conntrack-max=number,
 conntrack-count=number, conntrack-usage=number
```

Table 12: System Statistics

Activity Summary Name	Description
pid	The PID of the ADNS process.
cpu	The amount of CPU used by the ADNS process.
memory	The amount of memory used by the ADNS process.
virtual	The amount of virtual memory used by the ADNS process.
conntrack-max	The maximum number of Linux firewall connections reached.
conntrack-count	The current number of Linux firewall connections.

Activity Summary Name	Description
conntrack-usage	The percentage of Linux firewall connections in use.

Top Names Statistics

The **top-names** activity-counter-log-settings logs the top names queried and hit count.

The top names activity summary statistics are logged under the **Top-Names** sub category.

Sample log message:

```
10/22/2021 16:55:05 name/dns/1 Activity Stats 0 21508 [Top-Names] from 16:53:05 to 16:54:05;
 interval=number, total-counted=number
```

Table 13: Top Names Statistics

Activity Summary Name	Logging Sub Category	Statistic[11]	Description
interval	Top-Names	N/A	Length of data collection period.
total-counted	Top-Names	total-counted	Reports the total number of queries counted in this collection period.

[11] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Update Statistics

The **update** activity-counter-log-settings logs DNS Update related counters.

Sample log message:

```
10/29/2021 15:56:31 name/dns/1 Activity Stats 0 21550 [Update] Sample since Fri Oct 29
15:55:31 2021: total=number, failed-acl=number, prereq-only=number, dropped=number,
simulated=number, udp=number, tcp=number, ipv4=number, ipv6=number, deletes=number,
adds=number, refreshes=number, rrs=number, A=number, AAAA=number, DHCID=number, TXT=number,
 other=number

10/29/2021 15:56:31 name/dns/1 Activity Stats 0 21551 [Update-Responses] Sample since Fri
Oct 29 15:55:31 2021: total=number, no-error=number, failures=number, refused=number,
notauth=number, notzone=number, formerr=number, servfail=number, prereq-failures=number,
yxdomain=number, yxrrset=number, nxdomain=number, nxrrset=number
```

Table 14: Update Statistics

Activity Summary Name	Logging Sub Category	Statistic[12]	Description
total	Update	update-total	Total number of updates received by the DNS server.

Activity Summary Name	Logging Sub Category	Statistic[12]	Description
failed-acl	Update	update-failed-acl	Total number of updates that refused due to failing ACL and/or Update Policy authorization.
prereq-only	Update	update-prereq-only	Total number of prereq-only updates received by the DNS server.
dropped	Update	update-dropped	Total number of updates that are dropped by the DNS server.
simulated	Update	update-simulated	Total number of updates that are simulated. Simulated RR updates return a NOERROR response, but don't cause any RR changes.
udp	Update	update-over-udp	Total number of updates received over UDP.
tcp	Update	update-over-tcp	Total number of updates received over TCP.
ipv4	Update	update-over-ipv4	Total number of updates received over IPv4.
ipv6	Update	update-over-ipv6	Total number of updates received over IPv6.
deletes	Update	update-delete	Total number of RRs deleted by DNS update.
adds	Update	update-add	Total number of RRs added by DNS update.
refreshes	Update	update-refresh	Total number of RRs refreshed by DNS update.
rrs	Update	update-total-rrs	The total number of RRs updated by DNS update requests.
A	Update	update-type-A	Total number of updates for A records.
AAAA	Update	update-type-AAAA	Total number of updates for AAAA records.
DHCID	Update	update-type-DHCID	Total number of updates for DHCID records.
TXT	Update	update-type-TXT	Total number of updates for TXT records.
other	Update	update-type-other	Total number of updates for all other record types that are not specifically counted.

Activity Summary Name	Logging Sub Category	Statistic[12]	Description
total	Update-Responses	update-resp-total	Total number of update responses returned by the DNS server.
no-error	Update-Responses	update-resp-NOERROR	Total number of update responses with rcode of NOERROR.
failures	Update-Responses	update-resp-failures	Total number of updates that failed.
refused	Update-Responses	update-resp-REFUSED	Total number of update responses with rcode of REFUSED.
notauth	Update-Responses	update-resp-NOTAUTH	Total number of update responses with rcode of NOTAUTH.
notzone	Update-Responses	update-resp-NOTZONE	Total number of update responses with rcode of NOTZONE.
formerr	Update-Responses	update-resp-FORMERR	Total number of update responses with rcode of FORMERR.
servfail	Update-Responses	update-resp-SERVFAIL	Total number of update responses with rcode of SERVFAIL.
prereq-failures	Update-Responses	update-resp-prereq-failures	Total number of update responses with prereq failures (YXDOMAIN, YXRRSET, NXDOMAIN, NXRRSET).
yxdomain	Update-Responses	update-resp-YXDOMAIN	Total number of update responses with rcode of YXDOMAIN.
yxrrset	Update-Responses	update-resp-YXRRSET	Total number of update responses with rcode of YXRRSET.
nxdomain	Update-Responses	update-resp-NXDOMAIN	Total number of update responses with rcode of NXDOMAIN.
nxrrset	Update-Responses	update-resp-NXRRSET	Total number of update responses with rcode of NXRRSET.

[12] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Authoritative DNS server statistics, see the *"DNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.0 Administration Guide*.

Specifying Top Names Settings

The *top-names* attribute specifies if top names data should be collected. When enabled, a snapshot of the cache hits for the top names that are queried is collected for each interval set by the *top-names-max-age* value. The list of top names that is reported with activity summary statistics is the most current snapshot.

You can specify the maximum age (based on last access time) of a queried name allowed in the list of top names by using the *top-names-max-age* attribute. It has a default value of 60 seconds.

You can specify the maximum number of entries in the list of top names queried by using the *top-names-max-count* attribute. This limit is applied to the lists of top names that are logged or returned as part of activity summary.

Local Basic or Advanced Web UI

To enable Top Names, on the Edit Local DNS Server tab, under the **Top Names Settings** section, find the *top-names* attribute, enable it by selecting the **enabled** option, and then click **Save** to save the changes.

Top Names Statistics

The Top Names tab displays the relevant information with respect to top N domains and other important statistics attributes.

Local Basic or Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Select **DNS** in the Manage Servers pane.

Step 3 Click the **Top Names** tab available in the Local DNS Server page.

CLI Commands

Use **dns getStats top-names** to view the Top Names statistics.

Specifying TLS Settings

Cisco Prime Network Registrar 11.0 supports TLS in the Authoritative DNS server in addition to the Caching DNS server. The DNS server listens on configurable port 853 for TLS. On port 853, only TCP TLS connections are accepted and other connections are dropped. The DNS server has configurable parameters to enable or disable TLS, and to add TLS private and public key files.

For more information on DNS over TLS, see the Specifying TLS Settings section in the "Managing Caching DNS Server" chapter.

Note

- Cisco Prime Network Registrar does not support a command for generating self-signed certificates. However, they can be generated using readily available command line tool like openssl. For example:

  ```
  # openssl req -new -x509 -days 365 -nodes -out public.pem -keyout private.pem
  ```

- TLS is not supported in hybrid mode and in zone transfers.
- TLS keys are not supported with password phrase.

Table 15: TLS Attributes in the Authoritative DNS Server

Attribute	Description
TLS (*tls*)	Enables or disables TLS support for DNS. Before enabling TLS, the private key files must be placed in the DNS data directory under dns/tls and the *tls-service-key* attribute be set. If using managed DNS certificates, the certificate settings will be automatically set. Otherwise, the public certificate file must be placed in the DNS data directory under dns/tls and the *tls-service-pem* attribute be set. Enabling or disabling TLS service requires a Cisco Prime Network Registrar service restart for the change to take effect.
TLS Port (*tls-port*)	The port number on which to provide TCP TLS service. The DNS server will not serve non-TLS queries on this port.
TLS Private Key File (*tls-service-key*)	Defines the file name which contains the private key to be used by DNS for TLS sessions. The file must be in the DNS data directory under the **tls** subdirectory (that is, <cnr.datadir>/dns/tls) and must not be encrypted with a passcode.
TLS Public Key File (*tls-service-pem*)	Defines the pem file name which contains the public key certificate to be used by DNS for TLS sessions. The file must be in the DNS data directory under the **tls** subdirectory (that is, <cnr.datadir>/dns/tls). Note that if using managed DNS certificates, this attribute will be ignored and should be left unset.

Local Advanced Web UI

To enable TLS support for the Authoritative DNS server, do the following:

Before you begin

Before enabling TLS, you must place the public certificate and private key files in the DNS data directory under the **tls** subdirectory (that is, <cnr.datadir>/dns/tls) and set the *tls-service-key* and *tls-service-pem* attributes under the **TLS Settings** section on the Manage DNS Authoritative Server page. You can also use the managed certificates (see the *"Certificate Management" section in Cisco Prime Network Registrar 11.0 Administration Guide*).

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page. Click **DNS** on the Manage Servers pane.

Step 2 On the Edit Local DNS Server tab, under the **TLS Settings** section, enable the *TLS* attribute by selecting the **enabled** option.

Step 3 Click **Save** to save the changes.

Note You must restart the Cisco Prime Network Registrar service whenever TLS settings are modified.

CLI Commands

Use the following commands to enable TLS support for the Authoritative DNS server:

```
nrcmd> dns enable tls
```

Then, restart the Cisco Prime Network Registrar service using the following command:

```
# systemctl restart nwreglocal.service
```

Use **dns set** *attribute=value* to set the TLS attributes in the Authoritative DNS server.

Note You must restart the Cisco Prime Network Registrar service whenever TLS settings are modified.

TLS Statistics

On the Manage DNS Authoritative Server page, click the **Statistics** tab to view the Server Statistics page. The TLS statistics appear under the **Security Statistics** section of both the Total Statistics and Sample Statistics categories.

Table 16: TLS Statistics Attributes

Attribute	Description
tls-queries	Total number of queries received over TLS by the DNS Server.
tls-queries-failed	Total number of TLS queries failed during TLS handshake.

Enabling Round-Robin

A query might return multiple A or AAAA records for a name lookup. To compensate for most DNS clients starting with, and limiting their use to, the first record in the list, *round-robin* is enabled to share the load. This 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.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, under the Miscellaneous Options and Settings section, 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 Weighted Round-Robin

When a nameset is configured with multiple RRs of the same type, a weighted round-robin algorithm can be used to determine the frequency with which an RR is the first RR in the query response. To control the response behavior, administrators must be able to set weighted values on these RRs. In addition, the order in which multiple records are returned may be used by client applications and need to be controlled by administrators.

The *order* and *weight* attributes are available in Advanced mode.

Order

The *order* attribute specifies the sort order for the RR, compared to other RRs of the same type in the nameset. RRs with same type will be listed in ascending order, this will also be the order that RRs are returned when queried.

Weight

RR weight can be used in situations where you want certain servers providing the same service to be returned more frequently and therefore get more of the load. The *weight* attribute specifies the relative importance of this RR, compared to other RRs of the same type in the nameset. RRs with higher weight will be used more often in query responses for the name and type. For example, if *weight* for the RR is set to 5 and *weight* for another RR is set to 1, then RR will be used 5 times before the other RR is used once. RRs with a *weight* of 0 (zero) are always listed last and not included in the round robin operation.

Note The default *weight* on RRs is 1. When round robin is enabled (either DNS server or zone level), the RRs are returned in the first position once for each query (that is, traditional round robin).

If all the weights on the RR set are 0, then the response is returned to the client based on *order*. Effectively disabling round-robin on the RR set level.

The *order* and *weight* attributes can only be set on primary zones. These are transferred to HA backup and to the secondary servers, these attributes are not transferred when one of the servers in HA or secondary server is prior to 9.0 cluster. If you wish not to transfer order and weight, then disable the Transfer RR Meta Data (*xfer-rr-meta-data*) attribute present in the Manage DNS Authoritative Server page (you must do this in secondary DNS server). In secondary zone, *order* and *weight* are available, and the "resource records" are non-editable.

Local Basic or Advanced Web UI

Step 1 From the **Design** menu, choose **Forward Zones** or **Reverse Zones** under the **Auth DNS** submenu to open the List/Add Zones page.

Step 2 In the Forward Zone or Reverse Zone pane, click the zone name to open the Edit Zone page.

Step 3 Click the **Resource Records** tab.

Step 4 Add the RR name, TTL (if not using the default TTL), type, and data as appropriate.

Step 5 Once the RRs are created, *order* and *weight* can be set by editing the RRs (click the pencil icon next to the desired RR). You can find the *order* and *weight* attributes under the **RR Settings** section.

CLI Commands

Use **zone** *name* **addRR** *rr-name rr-type rr-ttl rr-data* [**weight**=*rr-weight*] [**order**=*rr-order*] to set weight and order.

Use **zone** *name* **modifyRR** *rr-name type* [*data*] *attribute=value* [*attribute=value* ...] to modify the resource records.

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 Enabling NOTIFY, on page 33) 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 Manage DNS Authoritative Server page, under the Zone Default Settings section, 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 is 0, as we always use IXFR and it is enabled, we don't periodically change to AXFR. Then, click **Save**.

CLI Commands

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

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 in Cisco Prime Network Registrar 11.0 DHCP User Guide*), or other ACLs. The *restrict-query-acl* attribute on the

Manage DNS Authoritative Server page serves as a default value for zones that do not have the *restrict-query-acl* explicitly 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.

Since a zone primary 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 field of the primary server. You can add additional servers to be notified by adding the IPv4 and IPv6 addresses to the *notify-list* on the zone configuration.

Note In orer for notifies to be sent to hidden name servers (that is, those that are not listed as NS RRs in the zone), their IP addresses need to be listed in the *notify-list* and notify setting needs to be set to *notify-list* or *notify-all*.

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 Advanced Web UI

Step 1 On the Manage DNS Authoritative Server page, under the **Zone Transfer Settings** section, find the *notify* attribute and select the value from the drop-down list.

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

Step 3 Click **Save**.

Step 4 To add nameservers in addition to those specified in NS records, from the **Design** menu, choose **Forward Zones** or **Reverse Zones** or **Secondary Zones** under the **Auth DNS** submenu.

Step 5 Click the zone name in the Forward Zones or Reverse Zones or Secondary Zones pane to open the Edit Zones page.

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

Step 7 Select the value from the *notify* drop-down list.

Step 8 Click **Save**.

CLI Commands

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

Blocking Recursive Queries from Authoritative Server

Blocking recursive queries allows the server to not spend resources trying to process these queries. The Drop Recursive Queries (*drop-recursive-queries*) attribute controls whether the DNS server accepts or drops the queries which have RD flag on. When this attribute is enabled, recursive queries will be dropped by the server. The default value of *drop-recursive-queries* is disabled, which means that no recursive queries will be dropped.

To enable *drop-recursive-queries*, do the following:

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page. Click **DNS** on the Manage Servers pane.

Step 2 On the Edit Local DNS Server tab, under the **Query Settings** section, enable the *drop-recursive-queries* attribute by selecting the **enabled** option.

Step 3 Click **Save** to save the changes.

Note The setting can be changed dynamically without a DNS server reload.

CLI Command

Use **dns enable drop-recursive-queries** to enable Drop Recursive Queries.

Drop Recursive Queries Statistics

On the Manage DNS Authoritative Server page, click the **Statistics** tab to view the *queries-dropped-recursive* statistic attribute under the **Query Statistics** section. This indicates the number of queries dropped due to recursion. The *queries-dropped* counter will be incremented when recursive queries are dropped.

Running DNS Authoritative Server Commands

Access the commands by using the Commands button. Clicking the **Commands** button opens the DNS Commands dialog box in the local web UI. Each command has its own Run icon (click it, then close the dialog box):

- **Force all zone transfers**—A secondary server periodically contacts its primary server for changes. See Enabling Zone Transfers.
- **Scavenge all zones**—Periodically purges stale records. See the *"Scavenging Dynamic Records" section in Cisco Prime Network Registrar 11.0 DHCP User Guide*.
- **Synchronize All HA Zones**—Synchronizes all the HA zones. You have the option to choose the type of synchronization. The **Push All Zones From Main to Backup** option is checked by default. You can override this by checking **Pull All Zones From Backup to Main** check box.

Note The **Synchronize All HA Zones** 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 Synchronizing HA DNS Zones).

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 **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **DNS** on the Manage Servers pane to open the Local DNS Server page.

Step 3 Click the **Network Interfaces** tab to view the available network interfaces that you can configure for the server. By default, the server uses all of them.

Step 4 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 5 Clicking the name of the configured interface opens a new page, where you can change the address of the interface.

Step 6 Click **Modify Interface** when you are done editing, then click **Go to Server Interfaces** 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).

Managing Authoritative DNSSEC

DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. DNSSEC provides protection against malicious or forged answers by adding digital signatures into DNS data, so each DNS response can be verified for integrity and authenticity.

Cisco Prime Network Registrar 9.0 and earlier Authoritative DNS Servers do not support signing of zones. From Cisco Prime Network Registrar 10.0, Authoritative DNSSEC support adds authentication and integrity

to DNS zones. With this support, Cisco Prime Network Registrar DNS server is able to support both secure and unsecure zones.

To add DNSSEC Security:

1. Choose regional or local management of DNSSEC keys and zones.
2. Review the algorithm, size, lifetime, and intervals set for Authoritative DNSSEC that will be used for default key generation.
3. Create Zone Signing and Key Signing keys if not using internally generated keys.
4. Enable DNSSEC for the required zones.
5. Export the DS RR for the signed zone which must be added to the parent zone, if it is not configured on the same server.

Enabling Authoritative DNSSEC

DNSSEC is enabled by default on the Authoritative DNS Server. It can be disabled by using the DNSSEC (*dnssec*) attribute (available in Expert mode) in the Manage Authoritative DNSSEC page. Disabling this attribute will disable zone signing for all zones, regardless of the zone *dnssec* attribute. By default, zone signing is disabled for all zones. To enable zone signing, the DNSSEC (*dnssec*) attribute in the zone configuration must be enabled only after the zone has been published. Once DNSSEC is enabled on the zone, zone signing is performed using core keys by default, or tenant keys specific to the zone tenant, if defined. The CCM server will create new keys for the zones, if there are no keys available.

Note DNSSEC cannot be enabled on a zone if RPZ is enabled and vice versa.

Table 17: Authoritative DNSSEC Attributes

Attribute	Description
Name	Specifies the name of authoritative DNSSEC configuration.
Description	A description of the authoritative DNSSEC configuration.
Key Rollover (*key-rollover*)	Specifies whether the regional or local cluster should perform Zone Signing Key (ZSK) rollover. If using regional zone management, this setting should be set to regional in order to centrally manage key generation and rollover.

Table 18: Zone Signing Key Attributes

Attribute	Description

Algorithm (*zsk-algorithm*)	Specifies the cryptographic algorithm to be used for the ZSK. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
Signature Size (*zsk-bits*)	Specifies the number of bits in the key and must be a multiple of 64. The value depends on the ZSK algorithm (zsk-algorithm) chosen. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
Key Lifetime (*zsk-lifetime*)	Specifies the lifetime of a ZSK. This defines the time interval where the key is used to sign zones. It is used to determine the deactivation-date when a ZSK key is created. The configured value MUST be greater than the *zsk-rollover-interval*. A value that is 10 times greater is recommended.
Key Rollover Interval (*zsk-rollover-interval*)	Specifies the time interval for the ZSK rollover process. It determines the lead time for the new key prior to the current key deactivation-date. Configured interval should be more than maximum TTL of the zones plus the propagation delay, to avoid bogus zone information.

Table 19: Key Signing Key Attributes

Attribute	**Description**
Algorithm (*ksk-algorithm*)	Specifies the cryptographic algorithm to be used for the Key Signing Key (KSK). DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
Signature Size (*ksk-bits*)	Specifies the number of bits in the key and must be a multiple of 64. The value depends on the KSK algorithm (*ksk-algorithm*) chosen. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
Key Rollover Interval (*ksk-rollover-interval*)	Specifies the time interval for the KSK rollover process. It determines the lead time for the new key prior to the current key deactivation-date.

Local Advanced Web UI

Step 1 From the **Design** menu, choose **Authoritative DNSSEC** under the **Security** submenu to open the Manage Authoritative DNSSEC page.

Step 2 Modify the attributes in the **Zone Signing Key** and **Key Signing Key** sections as per your requirements.

Step 3 Click **Save** to save your settings.

CLI Commands

Use **dnssec set** *attribute=value* [*attribute=value...*] to configure DNSSEC processing in the Authoritative DNS server. For example:

```
nrcmd> dnssec set zsk-algorithm=RSASHA1
```

Use **zone** *zonename* **signZone** to enable DNSSEC for the zone and add signatures for all RRs of the zone, when executed in Expert mode.

When connected to a regional cluster, you can use the following pull and push commands. Push allows a list of clusters or "all".

dnssec pull *cluster-name* [**-report-only** | **-report**]

dnssec push *cluster-list* [**-report-only** | **-report**]

Managing Authoritative DNSSEC Keys

To configure DNSSEC protected zones, a key must first be created. The zone is then signed using the key. You can create a key manually to customize the key attributes. Otherwise, the CCM server will create new keys automatically, as needed.

The *key-rollover* attribute in the Authoritative DNSSEC page can be set to local or regional management. The default is local. The *key-rollover* attribute specifies whether the regional or local cluster should perform ZSK rollover. With local rollover management, keys are managed on the local primary or HA main. The keys are copied to the HA backup via CCM HA sync. If zones are distributed across several primary servers, there will be many more keys to manage. With regional rollover management, keys are managed on the regional server and pushed to the local clusters. This lets you manage a common set of keys for your distributed primary servers. With central zone management, you can also stage zone edits and pre-sign zones before synchronizing the changes with the local DNS servers. Keys are auto-synched from regional to local when DNS edit mode is set to synchronous in the regional CCM server.

Rollover of ZSK is an automated process. Rollover of KSK has to be performed manually, the **rollover-ksk** command is used to start the KSK rollover process. You can provide your own key or allow CCM to generate keys.

dns rollover-ksk [**tenant-id**=*value*] [**next-key**=*keyname* | **key-group**=*value*]

Note In a lab setting, you can use the Expert mode command **zone** *name* **removeSignature** to remove all signature RRs and disable DNSSEC for the zone. This command should not be used for operational DNSSEC zones. Operational DNSSEC zones that will no longer be signed need to let signature records expire before they are deleted, following the guidelines in RFC 6781 - DNSSEC Operational Practices, Version 2.

Table 20: Key Timelines Attributes

Attribute	Description
Activation Date (*activation-date*)	Specifies the activation date and time for this key. Beginning at this date and time, the key will be used to sign RR sets.
Deactivation Date (*deactivation-date*)	Specifies the deactivation date and time for this key. Until this date and time, the key will be used to sign RR sets. This attribute must be 0 for KSKs. KSKs remain active until the key rollover process is initiated.
Removal Date (*expiration-date*)	Specifies the date and time this ZSK is scheduled to be removed. If 0, automatic removal is disabled and the key must be deleted by user action. This attribute must be 0 for KSKs. KSKs remain active until the key rollover process is initiated. When the rollover process is complete, the key can be deleted by user action.
Rollover Due Date (*rollover-due-date*)	Specifies the date and time, when this key should be (or was) rolled over. This transient attribute is used only for reporting.
Key Status (*status*)	Specifies the current status of the key. This transient attribute is used only for reporting.

Local and Regional Advanced Web UI

Step 1 From the **Design** menu, choose **Auth DNSSEC Keys** under the **Security** submenu to open the List/Add Authoritative DNSSEC Keys page.

Step 2 Set the *enable-signing* attribute value to **true** to enable the key and to sign the zones.

Step 3 In the **Key Timelines** section, you can enter the deactivation date and removal date as required.

Step 4 Click **Save** to save your settings.

CLI Commands

Use the following **dnssec-key** commands to create and manage Authoritative DNSSEC keys for zone signing.

dnssec-key *name* **create** [*attribute=value...*]

dnssec-key *name* **delete** [**-force]**

dnssec-key *name* **show**

dnssec-key *name* **set** *attribute=value* [*attribute=value...*]

Use **dnssec-key getStatus** to check the current status of DNSSEC keys related to rollover process.

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified.

dnssec-key < *name* | **all** > **pull** < **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]

dnssec-key < *name* | **all** > **push** < **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]

dnssec-key *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Exporting DS Record

Export Delegation Signer (DS) record is available for the DNSSEC enabled zones. If the parent zone is found on the Authoritative DNS server, the DS record will be added to the zone automatically. If multiple authoritative servers are deployed, and the parent zone is on another local cluster, you can manage the zones on the regional server to automatically update the parent zone. If the parent zone is externally-owned, you must provide the DS record to be added by the external organization.

Local and Regional Advanced Web UI

To export DS record, do the following:

Step 1 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu to open the Edit Zone page.

Step 2 On the Edit Zone page, under the **DNSSEC Settings** section, set the **DNSSEC** value to **true** to enable the DNSSEC.

Step 3 Click **Save** to save your settings.

Step 4 Click the **save** icon available next to the **DS Record** to export DS record.

CLI Commands

After you export the DS record, you need to publish the same to parent zone using the **export dnssec-ds** *zonename filename* command.

Setting Advanced Authoritative DNS Server Properties

You can set these advanced server properties:

- **SOA time-to-live**—See Setting SOA Time to Live, on page 41
- **Secondary server attributes**—See Setting Secondary Refresh Times, on page 41
- **Port numbers**—See Setting Local and External Port Numbers, on page 42
- **Handle Malicious DNS Clients**—See Handling Malicious DNS Clients, on page 43

Setting SOA Time to Live

The SOA record 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.

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 and Regional Web UI

Step 1 On the List/Add Zones page, set the Zone Default TTL attribute value, which defaults to 24 hours.

Step 2 If you want, set the SOA TTL attribute value, 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 attribute value under Nameservers. This value also defaults to the Zone Default TTL attribute value.

Step 4 Click **Save**.

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 Enabling NOTIFY, on page 33.

Local and Regional Web UI

On the List/Add Zones page, set the Secondary Refresh field to the refresh time, which defaults to 3 hours. Make any other changes, then click **Save**.

CLI Commands

Use **zone** *name* **set refresh**. The default value is 10800 seconds (3 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 default value is 60 minutes.

Local and Regional Web UI

On the List/Add Zones page, set the Secondary Retry field to the retry time, which defaults to one hour. Make any other changes, then click **Save**.

CLI Commands

Use **zone** *name* **set retry**. The default value is 60 minutes.

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 default value is seven days (1 week).

Local and Regional Web UI

On the List/Add Zones page, set the Secondary Expire field to the expiration time, which defaults to seven days (1 week). Make any other changes, then click **Save**.

CLI Commands

Use **zone** *name* **set expire**. The default value is seven days (1 week).

Setting Local and External Port Numbers

If you are experimenting with a new group of nameservers, you might want to use non-standard 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.

To see the full list of default ports, see the *"Default Ports for Cisco Prime Network Registrar Services" section in Cisco Prime Network Registrar 11.0 Administration Guide*.

Local Advanced Web UI

On the Manage DNS Authoritative Server page, under the Network Settings section, set the Listening Port (*local-port-num)* and Remote DNS Servers Port (*remote-port-num)* attributes to the desired values (they both have default values of 53), then click **Save**.

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 *acl-blocklist* attribute.

Local Advanced Web UI

On the Manage DNS Authoritative Server page, expand the **Advanced Settings** section to view various attributes and their values. For the *acl-blocklist* attribute, enter the value (for example, 10.77.240.73). Then click **Save**.

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*)**—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*)**—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*)**—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.
- **Maximum Memory Cache Size DNS server attribute (*mem-cache-size*)**—Size of the in-memory record cache, in kilobytes. The preset value is 500000 KB (500 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.
- **EDNS Maximum Packet Size DNS server attribute (*edns-max-payload*)**— Specifies the sender's maximum UDP payload size, which is defined as the number of octets of the largest UDP packet that can be handled by a requestor. You can modify this attribute from a minimum of 512 bytes to a maximum of 4 KB. The default value for this attribute is 1232 bytes on the DNS server.

Running Caching DNS and Authoritative DNS on the Same Server

Cisco Prime Network Registrar includes a Hybrid DNS feature that allows you to run both the Caching DNS and Authoritative DNS servers on the same operating system without two separate virtual or physical machines. This feature allows the Caching DNS to auto-detect the Authoritative DNS server and its zones without creating DNS exceptions.

Note Cisco recommends that hybrid mode is only for smaller sized deployments. For larger deployments, Cisco recommends separating Caching DNS and Authoritative DNS on separate physical machines or VMs. For more information, see the *"Authoritative DNS Capacity and Performance Guidelines" and "Caching DNS Capacity and Performance Guidelines" appendices in Cisco Prime Network Registrar 11.0 Installation Guide*.

Note When you are in Hybrid mode configuration, SNMP queries to Cisco Prime Network Registrar will retrieve only the Caching DNS server static values and not the Authoritative DNS server static values.

Following prerequisites must be met for hybrid mode to work correctly:

- The local cluster must be licensed for both Caching DNS and Authoritative DNS servers.
- Caching DNS and Authoritative DNS servers must have their own configured unique and separate network interfaces. If there are no separate interfaces available and if only one interface is available, the loopback interface (127.0.0.1/8, ::1/128) should be configured on the Authoritative DNS server and the other interface (for example, eth0, eth1, ens192, and so on) should be configured for the Caching DNS server.

Once the prerequisites have been met, hybrid mode can be enabled on the Authoritative DNS server.

When you enable hybrid mode, the following results occur:

1. Whenever the Authoritative DNS server is reloaded, it causes the Caching DNS server to be reloaded.
2. The Caching DNS server reads the Authoritative DNS servers interface list to detect which IP to send requests to.
3. The Caching DNS server auto detects all zones (forward, reverse, and secondary) and auto creates in-memory exceptions for those zones.
4. The Caching DNS server will not cache hybrid mode responses regardless of the RRs TTL value. This ensures that the responses it returns to clients reflect the most up-to-date information.

Local Advanced Web UI

Step 1 To configure the network interfaces on the Authoritative DNS and Caching DNS servers, do the following:

Note In Hybrid mode, the Caching DNS and Authoritative DNS servers must be configured with their own separate network interfaces. Using the loopback interface for Authoritative DNS server is supported only when the Authoritative DNS server does not require direct access for queries, notifies, or zone transfers.

a. From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

b. Click **DNS** in the Manage Servers pane.

c. Click the **Network Interfaces** tab and configure the available network interfaces for DNS.

Note The loopback interface (127.0.0.1/8, ::1/128) should be configured on the Authoritative DNS server for the DNS hybrid mode.

d. Click **CDNS** in the Manage Servers pane.

e. Click the **Network Interfaces** tab and configure the available network interfaces for the Caching DNS server.

Step 2 To enable the hybrid mode configuration on the Authoritative DNS server, do the following:

a. From the **Deploy** menu, choose **DNS Server** under the **DNS** submenu to open the Manage DNS Authoritative Server page.

b. Enable the *hybrid-mode* and *hybrid-use-adns-addrs* attributes available under the **Hybrid Mode** section:

- Select the **enabled** option for the Hybrid Mode (*hybrid-mode*) attribute.
- Select the **true** option for the Hybrid Use ADNS Addresses (*hybrid-use-adns-addrs*) attribute.

Note When the *hybrid-use-adns-addrs* attribute is enabled, the Caching DNS server will setup hybrid exceptions to forward to the Authoritative DNS server via *hybrid-adns-addrs*. The *hybrid-adns-addrs* attribute defaults to the loopback address (127.0.0.1) which is the recommended interface for hybrid DNS communication. If the *hybrid-use-adns-addrs* attribute is disabled, the Caching DNS server will use all of the Authoritative DNS server's configured network interfaces.

The *hybrid-adns-addrs* attribute specifies a list of one or more IP addresses to use for hybrid mode communication. Note that these addresses should match one or more of the Authoritative DNS server's configured interfaces. If using addresses other than the default loopback address (127.0.0.1), it may be necessary to also configure these interfaces in the Caching DNS Server for outbound traffic.

Step 3 Reload the Authoritative DNS server to enable the hybrid mode configuration.

CLI Commands

Use **dns set hybrid-mode=enabled** to enable the hybrid mode configuration on the Authoritative DNS server. Use **dns set hybrid-use-adns-addrs=true** to enable the *hybrid-use-adns-addrs* attribute. Use **dns-interface** *name* **set** *attribute=value* or **cdns-interface** *name* **set** *attribute=value* to set the interfaces.

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**—From the **Deploy** menu, choose **DNS Server** under the **DNS** submenu to open the Manage DNS Authoritative 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**— These preset values are probably not optimal for current systems and can cause performance issues. We strongly recommend that you to update the settings to use the new preset values. Example: The present value of Maximum Memory Cache Size DNS server attribute (*mem-cache-size*) is updated to 500 MB.

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 (*server-log-settings*) attribute on the Edit DNS Server page in the web UI, or **dns set server-log-settings**=*value* in the CLI, with one or more of these keyword or numeric values, separated by commas (see the table below). Restart the server if you make any changes to the log settings.

Table 21: DNS Log Settings

Log Setting	Description
activity-summary	This setting enables logging of DNS statistic messages at the interval specified by *activity-summary-interval*. The type of statistics logged can be controlled with *activity-counter-log-settings* and *activity-summary-type*.
config	This setting enables logging of DNS server configuration and de-initialization messages.
config-detail	This setting enables logging of detailed configuration messages (that is, detailed zone configuration logging).
dnssec	This setting enables log messages associated with DNSSEC processing.
host-health-check	This setting enables logging associated with DNS Host Health Check.
db	This setting enables logging of database processing messages. Enabling this flag provides insight into various events in the server's embedded databases.
ha	This setting enables logging of HA DNS messages.
notify	This setting enables logging of messages associated with NOTIFY processing.
query	This setting enabled logging of messages associated with QUERY processing.
scavenge	This setting enables logging of DNS scavenging messages.
scp	This setting enabled logging associated with SCP messages handling.
server-operations	This setting enables logging of general server events, such as those pertaining to sockets and interfaces.
tsig	This setting enables logging of events associated Transaction Signature (TSIG).
update	This setting enables logging of DNS Update message processing.
xfr-in	This setting enables logging of inbound full and incremental zone transfers.
xfr-out	This setting enables logging of outbound full and incremental zone transfers.

- **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, use **dig -h** or use **man dig**.
- **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.

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.