Managing High Availability DNS

A second primary server can be made available as a hot standby that shadows the main primary server. This configuration is called High-Availability (HA) DNS. The Cisco Prime Network Registrar web UI and CLI have features with which you can duplicate the primary setup required for HA DNS for the server pair. The server pair is responsible for detecting communication failures and the like. After the HA DNS is configured, the shadowing and error detection is done automatically. In a Cisco Prime Network Registrar deployment where Cisco Prime Network Registrar DHCP is updating Cisco Prime Network Registrar DNS, the failure detection and failover also happens automatically.

Note   When running HA, we recommend having only primary zones on the server.

Introduction to HA DNS Processing

In normal state, both the main and backup primary servers are up and running. The main server processes all DNS updates from clients and sends all accepted updates to the hot standby backup. The main server will forward RR updates to the backup server. Updates from DDNS clients are ignored or dropped by a backup server. Both servers can respond to queries and zone transfer requests. The main and the backup partners always stay in communication to detect availability of the other.

If the main goes down, the backup waits a short time, then begins servicing the DNS updates from clients that the main would normally service and records the updates. When the main returns, the HA pair synchronize and exchange RRs that were changed or deleted during communications interrupted state.

Whenever you add a new zone, both the primary and backup servers must be reloaded to automatically synchronize with the HA backup.

The synchronization is done on a per-zone basis. This allows updates to all other zones while a given zone is in the process of getting synchronized.

If the hot standby backup goes down, the main waits a short time, then records the updates that the partner did not acknowledge. When the backup server comes back up, the main sends the recorded updates to the backup.

Both the main and backup can traverse the following states:

- **Startup**—The servers establish communication and agree on the HA version to use. In this state, the servers do not accept DNS updates or RR edits, and they defer scavenging, if enabled.
- **Negotiating**—Each server is waiting for the other to get ready to synchronize. In this state, DNS Updates and RR edits are not allowed.
- **Normal**—Both servers are up and healthy, exchanging DNS updates and heartbeat messages. The main accepts DNS updates and RR edits, sends RR Update messages to the backup. The backup ignores DNS updates, refuses RR edits, but processes RR Update messages from the main server. Scavenging is suspended on zones while they are still synchronizing.
- **Communication-Interrupted**—The server goes into this state after not getting a response or request from the partner during the communication timeout (*ha-dns-comm-timeout*) period. The server continues listening for communication from the partner (they both send heartbeat messages at the rate specified by *ha-dns-poll-interval*) and tries to connect, meanwhile accepting DNS updates and RR edits and disabling scavenging.
- **Partner-Down**—It is similar to Communications-Interrupted, but does not continue to track RR changes. Once the partner returns, the entire zone will be sent to the partner. This allows for better performance and limits the disk space needed to track changes since the partner will get a copy of the zone when it becomes operational again.

When a DNS server starts up, it:

1. Opens its configured HA DNS listening ports and listens for connections from its partner.
2. Transitions to Negotiating state. In the Negotiating state, RR edits are not allowed.
3. Transitions to Normal state, the servers start synchronizing changes to each primary zone. The main starts allowing updates to zones and sending the update information to the backup.

Once the server is in Normal state, the zone level synchronization begins. Zone synchronization is always managed by the Main HA server. The zones traverse through the following states:

- **Sync-Pending State**—A zone enters this state when the HA DNS server transitions to the normal state or if a manual sync is requested. In this state RR updates for the zone will be accepted on the main server, and forwarded to the backup server.
- **Synchronizing State**—The RR synchronization for the zone takes place in the synchronizing state. RR updates are not accepted, and notifies are disabled.
- **Sync-Complete State**—A zone transitions to this state from the synchronizing state once it has successfully synchronized resource record changes with its corresponding zone on the HA DNS backup. In this state, the zone on the HA DNS main server accepts all dynamic DNS update requests, allow resource record configuration changes, and re-enables notifies. Resource record modifications will be forwarded to the backup server.
- **Sync-Failed State**—A zone transitions to the sync-failed state from the synchronizing state if it fails to sync. The zone will accept resource record updates on the main server, and changes will be forwarded to the backup. The server will retry synchronizing the zone after ha-dns-zonesync-failed-timeout. A manual sync request or server restart will also restart zone synchronization.

HA DNS is fully integrated with Cisco Prime Network Registrar DHCP servers, and the partners are updated when hosts get added to the network (see the *"Managing DNS Update" chapter in Cisco Prime Network Registrar 10.1 DHCP User Guide*). From the DHCP side of HA DNS, the DHCP server sends DNS updates to a single DNS server at a time.

DHCP autodetects the main being down and starts sending updates to the backup. The DHCP server tries to contact the main DNS server, twice. It tries the backup partner if both the attempts are unsuccessful.

The backup detects the main server down and starts accepting updates from DDNS clients. When the servers come up again, HA communication will establish automatically and the servers will get into Normal state where they carry out zone synchronization and make sure that both have the same RRs, and so on.

If both the DNS partners are communicating, the backup server drops the update, whereby the DHCP server times out and retries the main DNS server. If both servers are unreachable or unresponsive, the DHCP server continually retries each DNS partner every 4 seconds until it gets a response.

For zone level sync, an Advanced mode command is added in the local cluster Zone Commands page, if the local cluster is configured as the main HA server. In Expert mode, the following two options are provided:

- Sync All RRs from Main to Backup
- Sync All RRs from Backup to Main

HA DNS status is modified to include the zone synchronization status. Status includes count and percentage of synchronized zones, zones pending synchronization, and zones that have failed synchronization.

Zone status has been modified to also include the HA synchronization status (ha-server-pending, sync-pending, sync-complete, synchronizing, or sync-failed), if HA is configured.

Creating High Availability DNS Pairs

The attributes needed to set up an HA DNS server pair from the main server are:

- *ha-dns*—Enabled or disabled. The preset value is enabled.
- *main*—Cluster for the main primary DNS server.
- *backup*—Cluster for the backup primary DNS server.

The specific IP addresses for the main or backup is specified only when the cluster IP is used for management and DNS works on a different interface.

Local Basic or Advanced and Regional Web UI

Step 1   Create a cluster for the backup server.

Step 2   From the **Deploy** menu, choose **HA Pairs** under the **DNS** submenu to open the List/Add HA DNS Server Pair page.

Step 3   Click the **Add HA Pair** icon in the HA Pairs pane to open the Add HA DNS Server dialog box.

Step 4   Enter the name of the server pair in the name field. This can be any identifying text string.

Step 5   Select the cluster name of the main DNS server from the **main** drop-down list.

Note   If you change the IP address (IPv4 or IPv6) of your local host machine, you must modify the localhost cluster (on the Edit Cluster page) to change the IP address (IPv4 or IPv6) in the IPv4 Address or IPv6 Address field. Do not set the value to 127.0.0.1 and ::1.

Step 6   Select the cluster name of the backup DNS server from the **backup** drop-down list. This cannot be the same as the main server cluster. Set the *ha-dns-main-address* and *ha-dns-backup-address* attributes (for IPv4) and *ha-dns-main-ip6address* and *ha-dns-backup-ip6address* (for IPv6) only if the server is configured with different interfaces for configuration management and update requests (Configure the HA DNS protocol only with the interface used to service updates).

Step 7   Click **Add HA DNS Server**.

Step 8   Once the server pair appears on the List/Add HA DNS Server Pair page, synchronize the servers:

a) Select the HA in the HA Pairs pane and click the **Sync HA DNS Server Pair** tab.

b) Choose the direction of synchronization (Main to Backup or Backup to Main).

c) Choose the operation type (Update, Complete, or Exact). See the table on the page for details on the operations for each operation type.

d) Click the **Report** button to display the prospective synchronization changes on the View HA DNS Sync Report page.

e) Click **Run Complete** to complete the synchronization.

f) Click **Return** to return to the List/Add HA DNS Server Pair page.

Step 9   Reload both DNS servers to begin HA communication.

CLI Commands

Create the HA DNS server pair (**ha-dns-pair** *name* **create** *main-cluster/address backup-cluster/address*). The *address* can be IPv4 or IPv6. Then synchronize the servers using **ha-dns-pair** *name* **sync**, specifying the synchronization operation (update, complete, or exact) and direction (main-to-backup or backup-to-main). Be sure to reload both DNS servers. For example:

```
nrcmd> ha-dns-pair example-ha-pair create localhost test-cluster
nrcmd> ha-dns-pair example-ha-pair sync exact main-to-backup
nrcmd> dns reload
```

See the **ha-dns-pair** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions. The CLI provides an additional command for the DNS server to set the HA DNS partner down, if necessary, which is possible only while in Communication-Interrupted state:

```
nrcmd> dns setPartnerDown
```

The partner down is useful because it limits the bookkeeping data a server maintains, thus optimizing its performance. When both servers start communicating again, the sync sends all the zone RRs rather than trying to determine individual changes. The partner that was up will send all RRs to the server that was down.

Synchronizing HA DNS Zones

Local Advanced Web UI

To manually synchronize an HA DNS zone:

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

Step 2   Click the **Commands** button for the zone which you want to synchronize on the Edit Zone page.

Step 3   Click the **Command** icon next to **Synchronize HA Zone** to synchronize the HA DNS zone.

Synchronizing the HA DNS zone will always sync the associated views and named ACLs for primary zones.

Note   In the Expert mode, you have the option to choose the type of synchronization.

CLI Commands

Use **zone** *name* **ha-sync-all-rrs** to manually schedule HA zone synchronization for the zone, or to raise its priority, if the zone is already in the sync-pending state (see the **zone** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Enable Logging of HA DNS Information

The log setting, *ha*, enables logging of HA DNS related information.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, under the **Log Settings** section, check the **ha** check box. Click **Save** to save the changes.

CLI Command

Use **dns set server-log-settings=ha** to enable logging of HA DNS related information.

Viewing HA DNS Statistics

You can view HA DNS statistics.

Local Basic or Advanced Web UI

Click the **Statistics** tab on the Manage DNS Authoritative Server page to open the DNS Server Statistics page. The statistics appear under the HA Statistics and Max Counter Statistics subcategories of both the Total Statistics and Sample Statistics categories.

CLI Commands

Use **dns getStats ha** [**total**] to view the HA DNS Total counters statistics, and **dns getStats ha sample** to view the Sampled counters statistics.