



## Configuring High Availability DNS Servers

DNS was designed to have one primary server and multiple secondaries as authoritative for a zone. This works well for static addressing, because there is only one instance (the primary zone file) modified, while the secondaries periodically probe for updates from the primary, or the primary notifies the secondaries of them when the zone is loaded or reloaded.

This scenario has shortcomings with DNS updates under the RFC 2136 protocol where DHCP dynamically updates the DNS server, and only the primary DNS server can accept updates. This presents a single point of failure in that DNS updates cannot happen if the primary goes down.

To solve this problem, 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 Network Registrar Web UI has 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.

### 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 backup server refuses any DNS updates during normal times when the main is running and communicating with the backup. Both servers respond to nonupdate queries and zone transfers. The main and backup partners exchange heartbeat messages to detect if the other is not available.

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. If the backup has been down for an extended period, the main sends its entire zone data to the backup, essentially a full zone transfer.

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 backup sends it the updates, and the main synchronizes with the backup any unsent updates it had before it went down. During the short synchronization period, neither server accepts DNS updates.

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.
- **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, and performs history trimming and scavenging, if enabled. The backup ignores DNS updates, refuses RR edits, but processes RR Update messages from the main server. The backup also performs history trimming, but defers scavenging, if enabled.

- **Communication-Interrupted**—The server’s partner becomes inaccessible and waits a communication timeout period (*ha-dns-comm-timeout*) before entering this state. Either server then becomes primary. It continues listening for communication from the partner and tries to connect, accepts DNS updates and RR edits, maintains edit lists, and disables scavenging.
- **Partner-Down**—The server administrator notifies the partner that it will be down for an extended time. This manual intervention is possible only in Communication-Interrupted state. Either server continues listening for communication from the partner and tries to connect, accepts DNS updates and RR edits, and performs scavenging.
- **Synchronization**—Once the partners establish or reestablish communication, they synchronize RR changes that occurred during the interrupted period.

## Configuring the Server Pair

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

- *ha-dns*—Enabled or disabled. The default is disabled, so that this attribute must be set explicitly.
- *ha-dns-main-server*—IP address of the main primary DNS server.
- *ha-dns-backup-server*—IP address of the backup primary DNS server.
- *simulate-zone-top-dynupdate*—Enabled or disabled (the default). Enable this only for Windows 2000 Domain Controller compatibility.
- *update-relax-zone-name*—Enabled or disabled (the default). Enable this only if you want DNS updates to specify any zone name in the authoritative zone rather than the exact zone name.

**Step 1** In the Web UI, click **DNS**, then **HA Pairs** to open the List HA DNS Server Pairs page.

**Step 2** Click **Add HA DNS Server Pair** to open the Add HA DNS Server Pair page (see [Figure 17-1](#)).

**Figure 17-1 Add HA DNS Server Pair Page (Local)**

| Attribute | Value  | Data Type | Default  |
|-----------|--|-----------|----------|
| ha-dns    | <input type="radio"/> enabled <input type="radio"/> disabled | boolean   | disabled |

**Step 3** Enter the name of the server pair in the Name field. This can be any identifying text string.

**Step 4** Click the cluster name of the main DNS server in the Main Server drop-down list.

**Step 5** Click the cluster name of the backup DNS server in the Backup Server drop-down list. This cannot be the same as the main server cluster.

Setting the main and backup clusters automatically populates the *ha-dns-main-server* and *ha-dns-backup-server* attributes with the IP addresses of the servers.

In the local CLI, be sure that the main and backup DNS servers have the same zone configurations.

**Step 6** Click the *ha-dns* enabled button to enable HA DNS for the server pair.

In the local CLI, explicitly enable HA DNS (**ha-dns-pair name enable ha-dns**).

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

In the local CLI, create the HA DNS server pair (**ha-dns-pair name create mainaddr backupaddr**).

The default HA DNS port is 653. The main and backup server IP addresses cannot be the same. If they are, no connection is established.

**Step 8** Once the server pair appears on the List HA DNS Server Pairs page, synchronize the servers by clicking the Run icon (+) in the Synchronize column:

- a. On the Synchronize HA DNS Pair page, choose the synchronization option (Ensure, Replace, or Exact). Exact is the default.
- b. Choose the synchronization direction: From Regional (for the regional cluster only), Main to Backup, or Backup to Main. Main to Backup is the default.
- c. Click **Report** to display the prospective synchronization changes.
- d. Click **Run** to complete the synchronization and view the actual changes.

In the CLI, synchronize the servers using **ha-dns-pair name sync**, specifying the synchronization option and direction. For example:

```
nrcmd> ha-dns-pair examplehadnspair sync exact main-to-backup
```

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
```

Note that if the main primary server is disabled while you add a primary or secondary zone to the backup server, a message is logged on the backup, stating that a zone mismatch occurred and that a synchronization will ignore the added zone.

## Server Configuration

The only attribute on the main DNS server that addresses HA DNS is the *ha-dns-comm-timeoutbackup-server* attribute. This is the time required to determine if a partner is unreachable, after network communication is not acknowledged, which triggers the Communication-Interrupted state.

An additional log setting, *ha-details*, enables logging of HA DNS-related information.


Note that the HA DNS configuration is possible for Network Registrar 6.2 DNS servers only. Both the main and backup must have absolutely identical zone and RR configurations, and you must set the same HA DNS attributes for both servers.

## Effect of Re-Adding Zones

The HA DNS protocol is designed to preserve the RR list for the zone if a catastrophic failure occurs. If you delete and re-add a zone, the RR list is recovered from the server's HA DNS partner. If, instead, you need to delete all RRs in the zone:

- 
- Step 1** Delete the zone from the main server.
  - Step 2** Reload the server.
  - Step 3** Delete the zone on the backup server.
  - Step 4** Re-add the zone on the backup server.
  - Step 5** Reload the backup server.
  - Step 6** Re-add the zone on the main server.
  - Step 7** Reload the main server.
- 

## HA DNS Statistics

You can view statistics on HA DNS activity on the DNS Server Statistics page by clicking the Statistics icon () on the Manage DNS Server page. The statistics appear under the Max Counter Statistics subsections of both the Performance Statistics and Sample Statistics.

In the CLI, you can use **dns getStats ha [total]** to view the HA DNS Total counters statistics, and **dns getStats ha sample** to view the Sampled counters statistics.