CHAPTER 18

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 small deployments and where the primary can be easily recreated. For larger deployments where the system is expected to be more dynamic and automatic and where down time is business critical, the primary becomes the single point of failure.

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 Cisco 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 and in a Cisco Network Registrar deployment where Cisco Network Registrar DHCP is updating Cisco Network Registrar DNS, that failure detection also happens automatically.

See Also

HA DNS Processing
Configuring an HA DNS Server Pair from Main Server, page 18-3
DNS Server Configuration for HA DNS, page 18-4
HA DNS Configuration Synchronization, page 18-4
HA DNS Statistics, page 18-8

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 and the backup server only accepts updates from the main in normal state. In normal states, 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 backup partners exchange heartbeat messages to detect if the other is not available.

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 updates that were not sent and which it had before it went down. During the synchronization period, neither server accepts DNS updates.

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.
- **Synchronization-Pending**—Each server is waiting for the other to get ready to synchronize. In this state, DNS Updates and RR edits are not allowed.
- **Synchronization**—After the partners establish or reestablish communication, they synchronize RR changes that occurred during the interrupted period.
- **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 goes into this state after not getting a response or request from the partner during the communication timeout (*ha-dns-comm-timeout*) period (preset to 30 seconds). The server continues listening for communication from the partner (they both send heartbeat messages every 12 seconds) and tries to connect, meanwhile accepting DNS updates and RR edits and disabling 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.

When a DNS server starts up, it:

1. Tries to establish a connection with its partner.
2. Goes into Synchronization-Pending mode.
3. Goes into Synchronization mode after it receives a Synchronization-Pending response.
4. Goes into Normal mode.

HA DNS is fully integrated with DHCP servers, and the partners are updated when hosts get added to the network (see Chapter 28, “Configuring DNS Update”). 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 start sending updates to the backup. The DHCP server tries to contact the main DNS server, twice. It tries the backup partner if both of 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 be automatically established and the servers will get into a synchronization state where they make sure that both have the same RRs, etc.

If both 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.

Configuring an HA DNS Server Pair from Main Server

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 disabled, so that this attribute must be set explicitly.
- ***main***—IP address of the main primary DNS server.
- ***backup***—IP address of the backup primary DNS server.

Local Basic or Advanced and Regional Web UI

Step 1 Create a cluster for the backup server.

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

Step 3 Click **Add HA DNS Server Pair** to open the Add HA DNS Server Pair page.

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

Step 5 Click the cluster name of the main DNS server in the Main Server drop-down list.

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

Step 6 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. Set the *ha-dns-main-server* and *ha-dns-backup-server* attributes 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 the *ha-dns* enabled button to enable HA DNS for the server pair.

Step 8 Click **Add HA DNS Pair**.

Step 9 Once the server pair appears on the List/Add HA DNS Server Pairs page, synchronize the servers:

a. Click the Report icon ( ) in the Synchronize column.

b. On the Report Sync HA DNS Pair page, 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 **Report** to display the prospective synchronization changes on the View HA DNS Sync Report page.

e. Click **Run** to complete the synchronization and view the actual changes. The configuration gets pushed to the remote cluster.

f. Click **Return** to return to the List HA DNS Server Pairs page.

Step 10 Reload both DNS servers to begin HA communication. The DNS servers synchronize things such as unprotected RRs themselves when they start communicating.

CLI Commands

Explicitly enable HA DNS (**ha-dns-pair** *name* **enable ha-dns**). Create the HA DNS server pair (**ha-dns-pair** *name* **create** *mainaddr backupaddr*). 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 enable ha-dns
nrcmd> ha-dns-pair examplehadnspair create localhost test-cluster
nrcmd> ha-dns-pair examplehadnspair sync exact main-to-backup
nrcmd> dns reload
```

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
```

DNS Server Configuration for HA DNS

The only attribute on the main DNS server that addresses HA DNS is the *ha-dns-comm-timeout* 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 (see the description of this state in the "HA DNS Processing" section on page 18-1). The preset value is 30s. The server tries to communicate and then back off at multiples of the *ha-dns-comm-timeout* interval.

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

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

HA DNS Configuration Synchronization

Throughout this procedure the source system is referred as DNS HA main server and destination as DNS HA backup server. When you enable the HA DNS with large DNS configuration, you will notice that the process takes long time to complete. This section provides a workaround, which you can use until the defect is addressed.

Warning **To perform this process, you must have HA main server and HA backup server running on the same OS, Cisco Network Registrar version, and DNS configuration.**

Initial Setup Considerations

If the configuration information resides on a system that will be eventually used as HA DNS backup system, and if you bring in a new system online as the HA DNS main, the backup system functions as source and main system functions as destination.

Warning **The HA DNS backup server must not contain any pre-existing Cisco Network Registrar configuration that needs to be maintained, as all the DNS configuration data in the HA DNS backup server will be lost on completion of this procedure.**

Migration Procedure

This section describes the migration procedure used to migrate Cisco Network Registrar product databases from the HA DNS main server to the HA DNS backup server.

See Also

Pre-install Cisco Network Registrar on the HA DNS backup server, page 18-5
Pre-migration Steps for HA DNS Main Server, page 18-5
Restart Cisco Network Registrar on the HA DNS Main Server, page 18-6
Copy Cisco Network Registrar Database Files to HA DNS Backup Server, page 18-6
Reconfigure Cisco Network Registrar on the HA DNS Backup Server, page 18-7
Configure Cisco Network Registrar HA DNS on the HA DNS Main Server, page 18-7
Reload the DNS Servers, page 18-7

Pre-install Cisco Network Registrar on the HA DNS backup server

You need to pre-install Cisco Network Registrar on the HA DNS backup system before migrating the database directory from the HA DNS main system, to reduce the time required during the Cisco Network Registrar software installation process. During the installation process, the installer will verify whether any previous configuration is up to date with the Cisco Network Registrar data schema for the version being installed. Even if the versions are identical, the time required to perform this verification can be avoided by pre-installing Cisco Network Registrar on the HA DNS backup system.

Pre-migration Steps for HA DNS Main Server

You must ensure that the service of DHCP and TFTP servers are available and running on different systems, especially when there is a large DNS configuration. If the servers are found on the same system, the migration from HA DNS main server to backup server may cause DHCP or TFTP conflicts, and DHCP clients may be destabilized.

Follow the pre-migration steps as below:

Step 1 Disable the automatic start-on-reboot setting for the DHCP and TFTP server.

Note The default setting of start-on-reboot for the TFTP server is disabled.

```
nrcmd> server dhcp disable start-on-reboot
nrcmd> server tftp disable start-on-reboot
```

Step 2 Stop the Cisco Network Registrar on the HA DNS main server using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

Step 3 Once the Cisco Network Registrar is stopped by using Windows Process Manager (Windows) or ps command line utility (Linux/Solaris), navigate to the parent directory of the Cisco Network Registrar data directory, InstallDir\Network Registrar\Local\ (Windows) or /var/nwreg2/local/ on (Linux/Solaris).

Step 4 Using tar or an equivalent compression utility, bundle up the contents of the data subdirectory. InstallDir is the directory where you have installed your Cisco Network Registrar: tar -cvf cnrdatadir.tar data.

Tip Replace all the .bak database backup directories temporarily from HA DNS main server. The HA backup server does not need these backup directories and replacing them reduces the overall archive size. Be sure that you do not replace any other database files other than .bak; otherwise, the HA DNS backup cluster may not function properly.

Restart Cisco Network Registrar on the HA DNS Main Server

Step 1 Restart the Cisco Network Registrar servers on the HA DNS main system using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

Step 2 Restore the DHCP and TFTP server start-on-reboot attribute values to their pre-migration values:

```
nrcmd> server dhcp enable start-on-reboot
nrcmd> server dhcp start
nrcmd> server tftp enable start-on-reboot
nrcmd> server tftp start
```

Copy Cisco Network Registrar Database Files to HA DNS Backup Server

Step 1 Use FTP or an equivalent network file copy mechanism to transfer the Cisco Network Registrar database archive that was generated in the previous step to the parent directory of the Cisco Network Registrar data directory (typically C:\NetworkRegistrar\Local\ on Windows, and /var/nwreg2/local/ on Linux/Solaris) on the HA DNS backup server.

Step 2 Ensure that the mechanism used to transfer the database archive preserves binary file data. If FTP sessions default to ASCII mode, change it to binary mode in order to produce a usable database on the HA DNS backup server.

Step 3 Stop the Cisco Network Registrar product on the HA DNS backup server completely using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris). Ensure that the product is completely stopped, either by using the Windows Process Manager or the ps command line utility on Linux/Solaris, navigate to the parent directory of the Cisco Network Registrar data directory (typically C:\NetworkRegistrar\Local\ on Windows, and /var/nwreg2/local/ on Linux/Solaris).

Step 4 Ensure to recursively remove all contents of the existing data directory, to prevent any conflicts with the database archive that is about to be extracted. Using tar or an equivalent utility, extract the contents of the database archive file: tar -xvf cnrdatadir.tar.

Reconfigure Cisco Network Registrar on the HA DNS Backup Server

Step 1 Start the Cisco Network Registrar servers on the HA DNS backup system using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

Step 2 Rectify the conflicts, if any, between HA DNS main system and any DHCP or TFTP server configuration settings.

Step 3 The DHCP integrity will be compromised if the DHCP server has a configuration similar to that of HA DNS main system. To know more on increasing the DHCP service availability, refer to the Cisco Network Registrar product documentation. Cisco recommends that you completely remove any DHCP and/or TFTP related configuration on the HA DNS backup system using either the web UI or nrcmd CLI. You can restore the original DHCP and TFTP server-start-on-reboot attribute values, only after you confirm that the configuration values do not conflict with that of the HA DNS main system.

```
nrcmd> server dhcp enable start-on-reboot
nrcmd> server tftp enable start-on-reboot (only if it had be previously enabled)
```

Step 4 Edit the localhost Cluster object in the HA DNS backup server to reflect the values in use on the local server.

Configure Cisco Network Registrar HA DNS on the HA DNS Main Server

Step 1 In HA DNS main server, define appropriate Cluster objects for both the HA DNS main and HA DNS backup servers.

Step 2 Create an HA Pair object by specifying appropriate Cluster names for the main and backup DNS server roles, and enable HA DNS for the HA Pair.

Step 3 Generate the report of changesets and exchange them between the two servers using the default report generation settings (Main-to-backup, Complete).

Step 4 Perform the changeset synchronization while the list of changesets is displayed.

Reload the DNS Servers

Step 1 Reload the DNS servers on both HA DNS systems to initiate the DNS RR synchronization process. Do it either through the Manage Servers page on the HA DNS main cluster when the HA DNS main server's DNS server has finished reloading, or to save a little time, initiate through separate connections to both clusters to perform the reloads in parallel instead of series.

Step 2 When the DNS servers are synchronizing, Cisco Network Registrar does not allow DNS configuration updates (such as DDNS), but provides DNS queries and zone transfer. You can monitor the DNS server log files on the main and backup clusters to follow the progress of the DNS server synchronization process. The servers are fully operational when HA DNS enters Normal state.

HA DNS Statistics

You can view HA DNS statistics.

Local Basic or Advanced Web UI

Click the Statistics icon ( ) on the Manage DNS Server page to open the DNS Server Statistics page. The statistics appear under the 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.