Managing DNS Views

DNS Views let you present alternate versions of zone data to different communities of clients using a single name server. For example, a DNS server for example.com can maintain two views of the zone, where the view of example.com that can be queried internally includes many hosts that do not exist in the external view. Each zone view is treated as an independent copy of the zone. The DNS server, when answering queries on the zone, uses the match criteria defined in each view to determine the matching zone for the client. The query is answered based on that zone contents. In some cases, the zone contents may only vary slightly between views.

DNS Views Processing

DNS Views allow a name server to segregate the data and provide a different view of the data based on the clients accessing it. When DNS receives a DNS request, the request is processed to associate it with a DNS view. The association is performed by matching the client source and/or destination address to the source and destination ACLs configured on the view. Views are matched in priority order with the lowest non-zero priority being matched first. Once a request is matched to a DNS View, only the data in that view is available to the request. There is a one-to-one mapping between zones and views—a zone can only exist in one view. If the zone must exist in more than one view, make copies of the zone and associate with different views.

If you have an interval view and an external view, a typical setup is to set the priority of the internal view to one and set the ACLs (typically *acl-match-clients*) to match the criteria for internal clients. For the external view, leaving the default priority and ACLs will allow all requests not matching the interval view to match the external view.

Note Getting a NOTAUTH rcode response when DNS Views are configured, typically indicates that the request matched a view where the zone does not exist.

Note The auto-view detection is only applicable for Cisco Prime servers.

Views for the DNS client servers such as Caching DNS, Secondary DNS, Primary for Notifies, DHCP, and so on, are easily defined with minimal configuration.

Views that do not have any associated zones are still processed and may leave clients associated with empty views. Therefore, it is important to avoid creating views that are not being used.

Key Points to Remember While Working on DNS Views

Following are some of the key points or attributes to know while working on DNS Views:

- **View ID**—Defines a unique integer identifier for the view that is assigned by the CCM server or the user while creating DNS views.
- **View Priority (*priority* attribute)**—Each DNS View is assigned a unique priority to determine the view processing order. The lowest non-zero priority is processed first, followed by the second lowest, and so on. A zero priority is reserved for the Default view, which is always processed last. The web UI provides a mechanism to reorder views without explicitly setting the priority.
- **Default View**—The default view is created with view-id=0, priority=0, and client and destination ACLs set to any. Requests that do not match a named view always falls into the default view. By default, zones are created with a view-id=0, which automatically places them in the default view. The default view cannot be modified or deleted.
- ***acl-match-clients* attribute**—Specifies the ACLs that map clients to a view based on the client source address. The default is any and must be modified in order to have the clients associated with the appropriate views.
- ***acl-match-destinations* (Expert mode attribute)**—Specifies the ACLs that map clients to a view based on the client destination address. The default is any and should only be changed if the DNS server is using different network interfaces for different views.
- The Cisco Prime Network Registrar Caching DNS server can associate the client requests to the appropriate views on behalf of the Authoritative DNS server. This is done by configuring the DNS Views on the Caching DNS server and setting the *uses-views* attribute on the List/Add Exceptions page to **true**. The Caching DNS server maps the client to the appropriate view and tag the queries forwarded to the Authoritative DNS server with the appropriate view. Therefore, in these cases, the view mapping is done by the Caching DNS server.

  Note The Caching DNS server only maps clients to *acl-match-clients*. The *acl-match-destinations* attribute is ignored.

  DNS Views and Exception settings are automatically synced/set by zone distribution.

Managing DNS Views

You can create, edit, and delete DNS Views from local or regional cluster. You can also push or pull views and ACLs in Ensure, Replace, and Exact modes from or to the regional CCM server.

Note You can create a maximum of 100 views.

Local Basic or Advanced and Regional Web UI

To create DNS Views:

Step 1 From the **Design** menu, choose **Views** under the **Auth DNS** submenu.
Step 2 On the **Views** pane, click the **Add View** icon.
Step 3 Specify the name for the DNS views.
Step 4 Specify the view id. If you do not specify, the application automatically assigns a view id to the view.
Step 5 You can specify the ACL that maps the client to this view in the *acl-match-clients* field.
Step 6 Click the **Add DNS View** button.
Step 7 To edit a DNS View, click its name in the Views pane on the left.

Reorder DNS Views

When you create a set of DNS Views, you can specify the priority order. To specify the priority order:

Step 1 From the **Design** menu, choose **View** under the **Auth DNS** submenu to open the List/Add Zone Views page.
Step 2 Click the **Reorder Views** icon in the Views pane to open the Reorder dialog box.
Step 3 Set the priority for the DNS Views rules by either of the following methods:

- Select the view and click the **Move up** or **Move down** icon to reorder the rules.
- Select the view and click the **Move to** button, and enter the row number to move the view.

Step 4 Click **Save** to save the reordered list.

If you delete a view, you get a choice to delete all zones.

CLI Commands

Use **dns-view** *name* **create** to add DNS Views (see the **dns-view** command in the CLIGuide.html file in the install-path/docs directory for syntax and attribute descriptions).

Synchronizing DNS Views

Zone distribution sync, single zone sync, and HA DNS zone sync will always sync associated views and named ACLs for both primary and secondary zones. The synchronization modes applied while running zone distribution or HA DNS sync vary. When you run:

- **Zone Distribution Sync**—views will be synchronized in Replace mode for all zone distribution sync types (Update, Complete, and Exact), while ACLs will use Ensure mode. If caching DNS servers are included in the zone distribution, the associated views and named ACLs will be synchronized to these servers and the masters list will be configured as exceptions for the unique set of domain names in the distribution. The user must exclude secondaries and/or caching servers.
- **HA DNS Sync**—views will be updated in Replace mode for both Update and Complete sync, while Exact sync will sync views in Exact mode.

Pushing and Pulling DNS Views

You can also push views and ACLs to and pull views and ACLs from the regional cluster in Ensure, Replace, and Exact modes.

Pushing DNS Views to Local Clusters

You can push the views you create from the regional cluster to any of the local clusters.

Regional Web UI

Step 1 From the **Design** menu, choose **Views** under the **Auth DNS** submenu.

Step 2 On the **Views** pane, click the **Push All** icon in the left pane, or select a **DNS View** and click **Push** at the top of the Edit Zone View page. This opens the Push Data to Local Clusters or Push Zone View page.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the DNS Views, you can choose Ensure, Replace, or Exact.
- If you are pushing a DNS View, you can choose Ensure or Replace.

In both the above cases, Ensure is the default mode.

Choose Replace only if you want to replace the existing DNS View data at the local cluster. Choose Exact only if you want to create an exact copy of the DNS View at the local cluster, thereby deleting all DNS Views that are not defined at the regional cluster.

Step 4 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 5 Click **Push Data to Clusters**.

Pulling DNS Views from Local Clusters

Instead of explicitly creating views, you can pull them from the local clusters. In the regional web UI, you may first want to update the view replica data by clicking the Replica icon next to the cluster name.

Regional Web UI

Step 1 From the **Design** menu, choose **Views** under the **Auth DNS** submenu.

Step 2 On the **List/Add Zone Distribution** page, click the **Pull Replica** icon in the **Views** pane.

Step 3 Choose the data synchronization mode (**Update**, **Complete**, or **Exact**). These modes are described in the table on that page.

Step 4 Click **Report** at the bottom of the dialog box.

Step 5 Click **Run**.