Configuring DNS Views

Following are the tasks to configure a DNS view:

1. Add a DNS view, as described in Adding a DNS View.
2. Add zones to the DNS view. You can add authoritative forward-mapping and reverse-mapping zones, as well as delegated, forward, and stub zones. For information about configuring each type of zone, see Configuring Authoritative Zones and Configuring Delegated, Forward, and Stub Zones.

You can optionally do the following:

1. Define a Match Clients list and a Match Destination list to restrict access to the DNS view. For more information, see Defining Match Clients Lists and Defining Match Destinations List.
2. Copy resource records from one zone to another. This is useful when different DNS views have the same zone and have multiple resource records in common. For information, see Managing DNS Views.
3. Create resource records in a group and share the group among multiple zones. For information, see About Shared Record Groups.
4. Specify which interface IP address is published in the glue A record of the DNS view. For information, see Changing the Interface IP Address.
5. Manage recursive views. For information, see Managing Recursive DNS Views.
6. Manage the order of the DNS views, as this determines the order in which the NIOS appliance checks the Match Clients list. For information, see Managing the Order of DNS Views.
7. Configure forwarders for a DNS view. For more information, see Using Forwarders.
8. Enable AAAA filtering and configure a list of IPv4 networks and addresses for allowing or denying AAAA filtering from the appliance. For information, see Controlling AAAA Records for IPv4 Clients.

Adding a DNS View

You can add up to 1000 DNS views. When you add a DNS view, specify the following:

- The network view in which you are creating the DNS view. The appliance lists the network views only when there are multiple network views. Otherwise, it automatically associates the DNS view with the default network view.
- A Match Clients list specifying the hosts allowed access to the DNS view. If you do not define a list, the appliance allows all hosts to access the DNS view. For more information, see Defining Match Clients Lists.
- Whether recursive queries are allowed. When a name server is authoritative for the zones in a DNS view, you can disable recursion since your name server should be able to respond to the queries without having to query other servers.

Note: This setting overrides the recursion setting at the Grid and member levels.

To configure a new DNS view:

1. If there is more than one network view in the Grid, select the network view in which you are creating the DNS view.
2. From the Data Management tab -> DNS tab, expand the Toolbar and click Add -> Add DNS View.
3. In the Add DNS View wizard, complete the following fields:
   - **DNS View**: Enter the name of the DNS view. It can be up to 64 characters long and can contain any combination of printable characters. Each DNS view must have a unique name. You cannot create two DNS views with the same name, even if they are in different network views.
   - **Comment**: Optionally, enter information about the DNS view. You can enter up to 256 characters.
   - **Enable Recursion**: This field's initial default state is inherited from the Grid. It is inactive and greyed out until you click Override. After you click override, you can select or clear the check box to define a setting that applies to the DNS view only. Note that a DNS view actually inherits its recursion setting from the Grid members that serve its zones. When you first create a DNS view though, it does not have any zones and therefore inherits its setting from the Grid. After you create zones in the DNS view, Grid Manager can then determine the associated members and display the resulting inheritance. If a DNS view has multiple zones served by multiple members with different recursion settings, you can view the different settings in the Multi-Inheritance viewer. You can click Inherit to have the DNS view inherit its recursion setting from the Grid.
   - **Disable**: Select this check box to disable this DNS view.
4. Save the configuration and click Restart if it appears at the top of the screen, or click Next to define a Match Clients list. For information, see Defining Match Clients Lists.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Defining Match Clients Lists
When you configure a DNS view, you can create a Match Clients list to identify source IP addresses and TSIG keys that are allowed or denied access to the DNS view. The NIOS appliance determines which hosts can access a DNS view by matching the source IP address or TSIG key with its Match Clients list. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

If you do not configure a Match Clients list, then all devices are allowed access to the DNS view. However, if you configure a Match Clients list, then only those devices in the list with "Allow" permission can access the DNS view. All other devices are denied access, including Grid members. Therefore, to allow a primary server of a zone to receive dynamic DNS updates from member DHCP servers, you must add the members to the Match Clients list as well. Note that if you "Deny" permission to certain IP addresses or networks, you must add the "Allow Any" permission at the end of the Match Clients list to ensure that all other IP addresses and networks that are not in the "Deny" list are allowed access to the DNS view. You can add individual ACEs (access control entries) or a named ACL (access control list) to the Match Clients list. For information about named ACLs and how to define them, see Defining Named ACLs.

Defining a Match Clients List for a DNS View

You can define a Match Clients list for a DNS view when you add a new DNS view (second step of the Wizard) or when you edit an existing DNS view. For information about adding a DNS view, see Adding a DNS View. To define a Match Clients list for an existing DNS view:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.
2. In the DNS View editor, select the Match Clients tab, and select one of the following:
   - None: Select this if you do not want to configure a Match Clients list. The appliance allows all clients to access the DNS view. This is selected by default.
   - Named: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance allows access to the DNS view from sources that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.
   - Set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list.
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
       - Key name: Enter a meaningful name for the key, such as a zone name or the name of the client or Grid member. This name must match the name of the same TSIG key on other name servers.
       - Key Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
     - DNSOne 2.x TSIG Key: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populates the value of the key in the Value field. The Permission column displays Allow by default. You cannot change the default permission.
     - Any Address/Network: Select this to allow or deny any IP addresses to access the DNS view. After you have added access control entries, you can do the following:
       - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
       - Reorder the list of ACEs using the up and down arrows next to the table.
       - Select an ACE and click the Delete icon to modify the entry.
       - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

3. Save the configuration and click Restart if it appears at the top of the screen. You can also click the Schedule icon at the top of the editor to schedule this task. In the Schedule Change panel, enter a date, time, and time zone.

Defining a Match Destinations List

You can define a Match Destinations list that identifies destination addresses and TSIG keys that are allowed access to a DNS view. When the NIOS appliance receives a DNS request from a client, it tries to match the destination address or TSIG key in the incoming message with its Match Destination list to determine which DNS view, if any, the client can access. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

You can define a Match Destination list when you edit an existing DNS view as follows:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.
2. In the DNS View editor, select the Match Destinations tab, and select one of the following:
   - None: Select this if you do not want to configure a Match Destinations list. The appliance allows all destination addresses to access the DNS view. This is selected by default.
- **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the **Named ACLs** Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance allows access to the DNS view from the destination addresses that have the **Allow** permission in the named ACL. You can click **Clear** to remove the selected named ACL.

- **Set of ACEs**: Select this to configure individual ACEs. Click the **Add** icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
  
  - **IPv4 Address** and **IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the **Value** field and enter the IP address. The **Permission** column displays **Allow** by default. You can change it to **Deny** by clicking the field and selecting **Deny** from the drop-down list.
  
  - **IPv4 Network**: In the **Add IPv4 Network** panel, complete the following, and then click **Add** to add the network to the list:
    
    - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
    
    - **Permission**: Select **Allow or Deny** from the drop-down list.

  - **IPv6 Network**: In the **Add IPv6 Network** panel, complete the following, and then click **Add** to add the network to the list:
    
    - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
    
    - **Permission**: Select **Allow or Deny** from the drop-down list.

  - **TSIG Key**: In the **Add TSIG Key** panel, complete the following, and then click **Add** to add the TSIG key to the list:
    
    - **Key name**: Enter a meaningful name for the key, such as a zone name or the name of the client or Grid member. This name must match the name of the same TSIG key on other name servers.
    
    - **Key Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
    
    - **Key Data**: To use an existing TSIG key, type or paste the key in the **Key Data** field. Alternatively, you can select the key algorithm, select the key length from the **Generate Key Data** drop down list, and then click **Generate Key Data** to create a new key.

  - **DNSone 2.x TSIG Key**: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populates the value of the key in the **Value** field. The **Permission** column displays **Allow** by default. You cannot change the default permission.

  - **Any Address/Network**: Select this to allow or deny any IP addresses to access the DNS view. After you have added access control entries, you can do the following:
    
    - Select the ACEs that you want to consolidate and put into a new named ACL. Click the **Create new named ACL** icon and enter a name in the **Convert to Named ACL** dialog box. The appliance creates a new named ACL and adds it to the **Named ACL** panel. Note that the ACEs you configure for this operation stay intact.
    
    - Reorder the list of ACEs using the up and down arrows next to the table.
    
    - Select an ACE and click the **Edit** icon to modify the entry.
    
    - Select an ACE and click the **Delete** icon to delete the entry. You can select multiple ACEs for deletion.

3. Save the configuration and click **Restart** if it appears at the top of the screen. You can also click the **Schedule** icon at the top of the editor to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone.

### Enabling the Match Recursive Only Option

You can enable the match-recursive-only option for the DNS view. When you enable this option, only recursive queries from matching clients match the selected DNS view. This option can be used in conjunction with the match-client list and match-destination list. Ensure that you configure those options and the order of the DNS views accordingly if you want to also enable the match-recursive-only option.

To enable the match-recursive-only option, complete the following:

1. From the **Data Management** tab, click the **DNS** tab -> **Zones** tab> dns_view check box -> **Edit** icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the **Edit** icon beside it.

2. In the **DNS View editor**, select the **General** tab -> **Advanced** tab, and select the following:
   
   - **Enable match recursive only option**: This option is disabled by default. Select this option to enable the match-recursive-only option for the DNS view. When you select this option, only recursive queries from matching clients match this view. Note that this option can be used in conjunction with the match-clients and match-destinations options. Ensure that you configure those options and the order of the DNS views accordingly if you want to also enable match-recursive-only.

3. Save the configuration.

---

**Note:** You can also enable or disable the match-recursive-only option for a specific DNS view on a specific member by using the CLI command **set enable _match_recursive_only**. For information about this command, refer to the *Infoblox CLI Guide*.

### Copying Zone Records

Different views of the same zone may have a number of records in common. If this is the case, you can copy zone records between views and zones.

**Note:** You cannot copy shared records and records that the NIOS appliance automatically creates, such as NS records and glue A records.

To copy zone records between DNS zones and views:

1. From the **Data Management** tab -> **DNS** tab, click **Copy Records** from the Toolbar.

2. In the **Copy Records** dialog box, Grid Manager displays the last selected zone or the zone from which you are copying zone records in the **Source** field. Complete the following to copy records:
   
   - **Destination**: Click **Select Zone** to select the destination zone. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box from which you can select one. After you select the zone, Grid Manager displays the associated DNS view.
   
   - **Copy All records**: Select this option to copy all the zone records, including those records not created on the NIOS appliance, such as HINFO records.
Managing the DNS Views of a Grid Member

A Grid member can serve zones in different DNS views. You can manage the DNS views associated with a Grid member as follows:

- You can specify which interface IP address is published in glue A records in the DNS view, as described in Changing the Interface IP Address.
- You can assign an empty recursive view to a member, as described in Managing Recursive DNS Views.
- You can control the list of DNS views as described in Changing the Order of DNS Views.

Changing the Interface IP Address

By default, a Grid member publishes its LAN address in glue A records in the DNS view. You can change this default for each DNS view associated with a member. You can specify the NAT IP address or another IP address.

To specify the interface IP address for glue A records in a view:

1. From the Data Management tab, click the DNS tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. The Address Of Member Used In DNS Views table lists the default DNS view and DNS views with zones that are served by the member.
4. To change the address, click the entry in the Interface column of a DNS view, and select one of the following:
   - **NAT IP Address**: Select this to use the member NAT address for glue A records in a Grid setting. Select this when you want to notify the Grid Master that it should expect packets from this member on the NAT address, not the configured interface address. The Grid Master broadcasts this NAT address to all NAT members outside of its NAT group. Do not use this option for an independent appliance serving as a DNS server. Select **Other IP Address** to publish the NAT address for the independent appliance. For information about NAT compatibility, see NAT Groups.
   - **Other IP Address**: Select this to specify another address for glue A records, or to publish the NAT address for an independent appliance. Enter the address in the Address field.

   **Note**: The 255.255.255.255 limited broadcast address is reserved. The appliance does not automatically create glue A records for this address. You can however create an NS record without the associated glue records.

4. Save the configuration and click Restart if it appears at the top of the screen.

Managing Recursive DNS Views

When you add a DNS view that has recursion enabled, the appliance resolves recursive queries from hosts on the Match Clients list of that view. If the DNS view contains zones and you delete those zones, the appliance retains the view in its configuration file, as long as recursion is enabled in the view. Such a view is called an empty recursive DNS view because it does not contain any zones. It enables the appliance to respond to recursive queries from the specified clients.

In a Grid, all members automatically store DNS views that have recursion enabled in their configuration files. If you do not want a Grid member to respond to recursive queries for clients in a particular DNS view, you can remove the view from the member's configuration file.

To delete or retain an empty recursive DNS view in the DNS configuration file of a Grid member:

1. From the Data Management tab, click the DNS tab -> Members tab -> Grid member check box -> Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. The Recursive Views Assigned to this Member section lists the empty recursive DNS views. Move a DNS view to the Selected column to explicitly assign the view to the Grid member and include it in the DNS configuration file of the member. Move a DNS view to the Available column to remove it from the configuration file of the member.

   Empty recursive DNS views that you retain in the configuration file are automatically listed at the bottom of the list of DNS views. You can move them up or down the list when you manually change the order of the DNS views, as described in Managing the DNS Views of a Grid Member.

4. Save the configuration and click Restart if it appears at the top of the screen.

Managing the Order of DNS Views

When a member receives a query from a DNS client, it checks the Match Client lists in the order the DNS views are listed in the Order of DNS Views table of the DNS Views tab in the DNS Member editor. The NIOS appliance can order DNS views automatically, or you can order the DNS views manually. If you choose to have the appliance automatically update the order of the DNS views, it does so after each of the following events:

- Adding a DNS view to a member.
- Removing a DNS view from a member.
Changing the address match list of a DNS view hosted by the member.

About IP Addresses and the Order of DNS Views

NIOS appliances with both IPv4 and IPv6 enabled can contain both types of addresses in the Match Clients list. When you enable IPv6 on the appliance, the order of DNS views in the GUI may be affected. Views are ordered and sorted automatically based on Match Clients lists. Views with IPv6 enabled are sorted as follows:

- If the Match Clients lists of all views contain IPv4 addresses only—The appliance orders views based on IPv4 addresses.
- If the Match Clients lists of all views contain IPv6 addresses only—The appliance orders views based on IPv6 addresses.
- If the Match Clients list of one DNS view has IPv6 addresses and all other views have IPv4 addresses—The appliance orders views based on IPv4 addresses, and the IPv6 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has IPv4 addresses and all other DNS views have IPv6 addresses—The appliance orders DNS views based on IPv6 addresses, and the IPv4 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has both IPv4 and IPv6 addresses—The appliance orders DNS views based on both IPv4 and IPv6 addresses, but more priority is given to the IPv4 addresses in the ordering.

The DNS views are ordered based on the number of IP addresses that are matched by the Access Control Lists (ACLs). The order of the DNS view is as follows:

- ANY
- Large Network
- Small Network
- Multiple Addresses
- Single Address

The actual precedence of the order of the views is also based on the ACL elements:

- any match: precedence = UINT_MAX + 1
- address match: precedence += 1
- TSIG match: precedence += 1
- network match: precedence += 129 - split (BOTH v4 and v6)

Note that views with the same precedence are sorted based on the internal view name. For example, '_default' or '0'.

Note: Only superusers can change the order of the views.

Changing the Order of DNS Views

To change the order of DNS views:

1. From the Data Management tab, click the DNS tab -> Members tab -> Grid_member check box -> Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. In the Order of DNS Views section, select one of the following:
   - Order DNS Views Automatically: Click this to automatically order views after adding a new DNS view, removing a DNS view, or changing the match client list.
   - Order DNS Views Manually: This able lists the DNS views that have zones assigned to the Grid member and the empty recursive views associated with the member. Select a DNS view, then click an arrow to move it up or down in the list.
4. Save the configuration and click Restart if it appears at the top of the screen.

Managing DNS Views

You can list the DNS views, and then modify, disable, or remove any custom DNS view. You can modify and disable the default DNS view; however, under no circumstances can it be removed.

Listing DNS Views

After you configure additional DNS views, you can list all DNS views by navigating to the Data Management tab -> DNS tab -> Zones panel. This panel lists DNS views only after you modify the default DNS view or add a DNS view. If you never added DNS views or modified the default DNS view, this panel does not display the default DNS view. Instead, it lists the zones in the default DNS view. To display the properties of the default DNS view and edit it, use the Global Search function to locate and edit it.

Note that if you have not used Grid Manager to add a new DNS view, and you import DNS views through the Data Import Wizard or the API, you must log out and log back in to Grid Manager to display the newly imported DNS views.

For each DNS view, this panel displays the following by default:

- **Comment**: Comments that were entered for the DNS view.
- **Site**: Values that were entered for this pre-defined attribute. You can also display the following column:
- **Disabled**: Indicates if the DNS view is enabled or disabled. Disabled DNS views are excluded from the named.conf file.

From this list, you can do the following:
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- List the zones in a DNS view by clicking a DNS view name.
- Edit information about a DNS view, as described in the next section.
- Delete a DNS view, as described in Deleting DNS Views.

Modifying DNS Views

To modify a DNS view:

1. From the Data Management tab, click the DNS tab > Zones tab > dns_view check box -> Edit icon.
2. In the DNS View editor, you can do the following:
   - In the General tab, you can change any of the information you entered through the wizard. You can also disable a DNS view to temporarily block access to a DNS view. Disabling a DNS view excludes it from the named.conf file. For a description of the fields, see the online Help or Configuring DNS Views.
   - In the Match Clients tab, define or update a Match Clients list, as described in Defining Match Clients Lists.
   - In the Match Destinations tab, define or update match destinations, as described in Defining a Match Destinations List.
   - In the Forwarders tab, configure forwards for the view, as described in Using Forwarders.
   - In the Queries tab, enable AAAA filtering and configure a list of IPv4 networks and addresses for allowing or denying AAAA filtering, as described in Enabling AAAA Filtering.
   - In the DNSSEC tab, you can specify parameters for DNSSEC as described in Configuring DNSSEC on a Grid.
   - In the Root Name Servers tab, you can configure root name servers, as described in Enabling Root Name Servers.
   - In the Sort List tab, define a sort list for the DNS view, as described in Defining a Sort List.
   - In the Blacklist tab, define blacklist rulesets, as described in Enabling Blacklisting.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes.
   - In the Permissions tab, define or update a Match Clients list, as described in Defining Match Clients Lists.
   - In the Record Scavenging tab, define the rules for DNS records scavenging in the DNS view, as described in Configuring DNS Record Scavenging Properties.
   - In the Updates tab, specify the secure dynamic updates settings, as described in Secure Dynamic Updates.
3. Save the configuration and click Restart if it appears at the top of the screen.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Deleting DNS Views

You can delete a DNS view if it is not the only view associated with a network view and if it is not selected for dynamic DNS updates. You cannot remove the system-defined default DNS view. When you remove a DNS view, the NIOS appliance removes the forward and reverse mappings of all the zones defined in the DNS view.

To delete a DNS view:

- From the Data Management tab, select the > DNS tab > Zones tab > dns_view check box.

  To delete the DNS view immediately, click the Delete icon, and then click Yes to confirm the delete request. To schedule the deletion, click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

  Grid Manager moves the view to the Recycle Bin, from which you can restore or permanently delete it.

Configuration Example: Configuring a DNS View

In Figure 18.4, Member-A is a member of a Grid. It is the primary name server for the corpxyz.com zone in the internal DNS view. It allows the IP address 192.168.10.1 and the 10.2.2.0/24 subnet access to DNS zone data in the internal DNS view. At the zone level, it allows transfers to an external secondary server, Infoblox-B, with an IP address of 192.168.10.1. Infoblox-B is a secondary server for the corpxyz.com zone. The process follows these steps:

1. Adding an Internal DNS View on Member-A
2. Adding a Zone to a DNS View
3. Copying Records Between DNS Zones from the corpxyz.com zone in the default DNS view to the corpxyz.com zone in the internal DNS view
4. Verifying the Configuration

Figure 18.4 Configuring a DNS View
Adding an Internal DNS View

1. Expand the Toolbar and click **Add -> Add DNS View**.
2. In the **Add DNS View** wizard, specify the following, and then click **Next**:
   - **Name**: internal
   - **Comment**: internal DNS view
3. In the **Match Clients** panel, click **Add** and select **IPv4 Network** from the drop-down list.
4. Do the following for IP addresses in the network 10.2.2.0/24:
   - Enter **10.2.2.0/24** in the in the **Address** field.
   - The **Permission** field displays **Allow** by default. Leave it as is.
   - Click **Add**.
   - You will have 255 allowed client addresses in the Match Clients list when you are done.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

Adding a Zone to a DNS View

1. Expand the Toolbar and click **Add -> Zone -> Add Auth Zone**.
2. In the **Add Auth Zone** wizard, click **Add an authoritative forward-mapping zone** and click **Next**.
3. Specify the following, and then click **Next**:
   - **Name**: Enter **corpxyz.com**.
   - **DNS View**: Select **Internal** from the drop-down list.
4. In step 3 of the wizard, do the following:
   a. Select **Use this set of name servers**.
   b. Click the Add icon and select **Primary**.
   c. Click **Select Member** and select **Member A** from the **Select Grid Member** dialog box.
   d. Click **Add** to add the Grid member to the list of name servers.
   e. Click the Add icon again and select **External Secondary**.
   f. Enter the following information, and then click **Add**:
      - **Name**: InfobloxB
      - **IP Address**: 192.168.10.1
5. Click **Save & Edit** to display the **Authoritative Zone** editor and continue with the zone configuration.
6. Click **Queries**.
7. Click **Override**, and then click the Add icon and select **IPv4 Network**.
   - Enter **10.2.2.0/8** in the in the **Address** field.
   - The **Permission** field displays **Allow** by default. Leave it as is.
   - Click **Add**.
8. This allows queries that the appliance answers from its internal DNS view.
9. Save the configuration and click **Restart** if it appears at the top of the screen.
Copying Records Between DNS Zones

1. Navigate to the default DNS view and select the corpxyz.com zone.
2. Expand the Toolbar and click Copy Records.
3. In the Destination field, click Select Zone, and then select the corpxyz.com zone in the Internal DNS view.
4. Select Copy all records, and then click OK.
5. Save the configuration and click Restart if it appears at the top of the screen.

The records from corpxyz.com in the default DNS view are copied to corpxyz.com in the internal DNS view.

Note: Only superusers can copy A, AAAA, shared A, and shared AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record in order to copy A, AAAA, shared A, and shared AAAA records with a blank name, otherwise the copying records operation might fail. You can assign global permission for specific admin groups and roles to allow to copy A, AAAA, shared A, and shared AAAA records with a blank name. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

Verifying the Configuration

1. In the DNS tab, click Members and select the Member-A check box.
2. Expand the Toolbar and click View -> View DNS Configuration.
3. In the DNS Configuration File viewer, scroll through the contents of the file.

Verify that the internal DNS view section is similar to the configuration file shown.