Configuring Delegated, Forward, and Stub Zones

In addition to authoritative zones, the NIOS appliance allows you to configure delegated, forward, and stub zones. A delegated zone is a zone managed by (delegated to) another name server who owns the authority for the zone. A forward zone is where queries are sent before being forwarded to other remote name servers. A stub zone contains records that identify the authoritative name servers in another zone. This section covers the following topics:

- Configuring a Delegation
- Configuring a Forward Zone
- Configuring Stub Zones

Configuring a Delegation

Instead of a local name server, remote name servers (which the local server knows) maintain delegated zone data. When the local name server receives a query for a delegated zone, it either responds with the NS record for the delegated zone server (if recursion is disabled on the local server) or it queries the delegated zone server on behalf of the resolver (if recursion is enabled).

For example, there is a remote office with its own name servers, and you want it to manage its own local data. On the name server at the main corporate office, define the remote office zone as delegated, and then specify the remote office name servers as authorities for the zone. You can delegate a zone to one or more remote name servers, which are typically the authoritative primary and secondary servers for the zone. If recursion is enabled on the local name server, it queries multiple delegated name servers based on their round-trip times. You can also add arpa as a top-level forward-mapping zone and delegate its subzones.

You can also configure TTL settings of auto-generated NS records and glue A and AAAA records for delegated zones in forward-mapping, IPv4 reverse-mapping, and IPv6 reverse-mapping zones. For information, see About Time To Live Settings.

The delegation must exist within an authoritative zone with a Grid primary server.

Configuring a Delegation for a Forward-Mapping Zone

To create a delegation for a forward-mapping zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the parent zone to open it.
   Grid Manager displays the Records and Subzones tabs of the zone.
3. From the Subzones tab, click the Add icon -> Zone -> Add Delegation.
4. In the Add Delegation wizard, specify the following:
   - **DNS View**: This field displays only when there is more than one DNS view in the network view. Displays the DNS view of the current zone.
   - **Comment**: Optionally, enter additional text about the zone.
   - **Disable**: Click this check box to temporarily disable this zone. For information, see Enabling and Disabling Zones
   - **Lock**: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes. For information, see Locking and Unlocking Zones.
5. Click **Next** to assign a delegation name server group or define the name servers for the zone. Select one of the following:
   - **Use this nameserver group**: Select this to assign a delegation NS group for the delegated zone. You can select the delegation NS group from the drop-down list.
   - **Use these nameservers**: Select this to define name servers for the delegated zone. In the Name Servers panel, click the Add icon and specify the following information:
     - **Name**: Enter the name of a remote name server to which you want the local server to redirect queries for zone data. This is a name server that is authoritative for the delegated zone.
     - **Address**: Enter the IP address of the delegated server.
6. Save the configuration and click **Restart** if it appears at the top of the screen, or click **Next** to define extensible attributes as described in Using Extensible Attributes.
   
   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.

**Note**

The DNS server resolves the FQDN of the delegated name server and does not use the IP address that you specify when assigning the delegated name servers.

Configuring a Delegation for a Reverse-Mapping Zone

To create a delegation for a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the parent zone to open it.
   Grid Manager displays the Records and Subzones tabs of the zone.
3. From the Subzones tab, click the Add icon -> Zone -> AddDelegation.
4. In the AddDelegation wizard, specify the following:
   - IPv4Network: This field displays if you are creating a delegation zone for an IPv4 reverse-mapping zone. Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
   - To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the following fields:
   - RFC2317Prefix: Enter a prefix in this field. Prefixes can include alphanumeric characters.
   - AllowmanualcreationofPTRRecordsinparentzone: Select this check box to allow users to create labels that correspond to IP addresses in the delegated address space in the parent zone.
   - For information about RFC 2317, see Specifying an RFC 2317 Prefix.
   - IPv6NetworkPrefix: This field displays if you are creating a delegation zone for an IPv6 reverse-mapping zone. Enter the IPv6 prefix for the address space for which you want to define the reverse-mapping zone and select the prefix length from the drop-down list.
   - Name: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   - DNS View: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - Comment: Optionally, enter additional text about the zone.
   - Disable: Select this option to temporarily disable this zone.
   - Lock: Select this option to lock the zone so that you can make changes to it and prevent others from making conflicting changes.
5. Click Next to assign a delegation name server group or define the name servers for the zone. Select one of the following:
   - Usehisnameservergroup: Select this to assign a delegation NS group for the delegated zone. You can select the delegation NS group from the drop-down list.
   - Usehissetofnameservers: Select this to define name servers for the delegated zone. In the Name Servers panel, click the Add icon and specify the following information:
     - Name: Enter the name of a remote name server to which you want the local server to redirect queries for zone data. This is a name server that is authoritative for the delegated zone.
     - Address: Enter the IP address of the delegated server.
   For information about delegation NS groups, see Using Delegation Name Server Groups.
6. Save the configuration and click Restart if it appears at the top of the screen, or click Next to define extensible attributes as described in Using Extensible Attributes.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the ScheduleChange panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

**Note**
The DNS server resolves the FQDN of the delegated name server and does not use the IP address that you specify when assigning the delegated name servers.

Configuring a Forward Zone

When you want to forward queries for data in a particular zone, define the zone as a forward zone and specify one or more name servers that can resolve queries for the zone. You can also assign one or more external name servers as default forwarders for a forward zone. For example, define a forward zone so that the NIOS appliance forwards queries about a partner's internal site to a name server, which the partner hosts, configured just for other partners to access.

You can override the default forwarders for a forward-mapping zone at a Grid member level and configure custom forwarders. In other words, each Grid member can have its own forwarders for the forward zone. For example: a forward-mapping zone foo.com served by two Grid members M1 and M2 with M1 forwarding queries to 10.1.0.1 and 10.1.0.2 and M2 forwarding queries to 90.3.3.3 and 90.4.4.1. Note that the Grid member uses the default forwarders unless you override them at any level. For more information about domains and zones, see Configuring Authoritative Zone Properties.

**Note:** The use of a forward zone is different from that of a forwarder. (A forwarder is a name server that performs recursive lookups on behalf of the name servers that forward queries to it. For more information, see Using Forwarders.) A NIOS appliance forwards queries to the name server of a forward zone because the name server can resolve queries for the zone. A NIOS appliance forwards queries to a forwarder regardless of zones.

Note that a name server can have only one definition for a zone in any given DNS view; a forward zone cannot be configured on a member that already has a zone with the same domain name configured on it in the same DNS view. To configure a forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Forward Zone.
2. In the Add Forward Zone wizard, click Add a forward forward-mapping zone and click Next.
3. Enter the following information, and then click Next.
   - Name: Enter the domain name of the zone for which you want the NIOS appliance to forward queries.
   - DNS View: This field displays only when there is more than one DNS view in the current network view. Select the DNS view of the forward zone.
   - Comment: Enter a descriptive comment.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes.
4. Click Next to assign a forward/stub server name server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
Select **Use this name server group** to assign a forward/stub server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS groups, see Using Forward/Stub Server Name Server Groups.

Select **Use this set of name servers** to specify the default servers for the zone. Click the Add icon and specify the following:
- **Name**: Enter a domain name of the server to which you want the NIOS appliance to forward queries.
- **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.

Select **Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.

5. Click **Next** to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:

**Note:** If you do not define any Grid members to serve the forward-mapping zone, then the named.conf file will not contain the configuration of the newly created forward zone. Hence, the Infoblox DNS server will not be authoritative to the forward zone and by default, the Infoblox DNS server will query the root servers to resolve queries for the forward zone.

- **a.** Select **Use this name server group** to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see Using Forwarding Member Name Server Groups.

- **b.** Select **Use this set of name servers** to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name.

   The following is displayed for each Grid member:
   - **Name**: Displays the name of the Grid member.
   - **IPv4 Address**: Displays the IPv4 address of the Grid member.
   - **IPv6 Address**: Displays the IPv6 address of the Grid member.
   - **Override Default Forwarders**: Displays **Yes** when you override default forwarders. Otherwise, this field displays **No**.
   - **Custom Forwarders**: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

   **Note:** Skip the following two steps if you want to use the default forwarders.

6. Select a member and click the Edit icon.

7. In the **Edit Per-Member Forwarders** editor, select the **Override Default Forwarders** check box to override the default forwarders. The Default Zone Forwarders table becomes available only after you select the **Override Default Forwarders** check box. Click the Add icon to specify the servers to which the NIOS appliance forwards queries for the zone:
   - **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   - **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
   - **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.

   Save the configuration. After successfully saving the configuration, the **Override Default Forwarders** column displays **Yes** and the **Custom Forwarders** column displays the IP address of the forwarders.

   To configure forwarders for multiple members, repeat the steps for each Grid member.

8. Save the configuration, or click **Next** to continue to the next step where you define extensible attributes as described in Using Extensible Attributes, and then optionally proceed to the next step where you define admin permissions as defined in About Administrative Permissions.

9. Click **Restart** if it appears at the top of the screen.

To configure a forward IPv4 reverse-mapping zone:

1. From the **Data Management** tab, select the **Zones** tab, expand the Toolbar and click **Add -> Zone -> Add Forward Zone**.
2. In the **Add Forward Zone** wizard, click **Add a forward IPv4 reverse-mapping zone** and click **Next**.
3. Enter the following information, and then click **Next**:
   - **IPv4 Network**: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the **Netmask** drop-down list. Alternatively, you can specify the address in CIDR format, such as 192.8.
   - To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the **RFC 2317 Prefix** field. Enter a prefix in the text field. Prefixes can be alphanumeric characters. For information, see Specifying an RFC 2317 Prefix.
   - **Name**: Enter the domain name of the reverse-mapping zone.
   - **DNS View**: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - **Comment**: Optionally, enter additional information about the zone.
   - **Disable**: Click this check box to temporarily disable this zone.
   - **Lock**: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.

4. Click **Next** to assign a forward/stub server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
   - Select **Use this name server group** to assign a forward/stub server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub NS groups, see Using Forward/Stub Server Name Server Groups.
   - Select **Use this set of name servers** to specify the default servers for the zone. Click the Add icon and specify the following:
     - **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries.
     - **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     - **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.

5. Click **Next** to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:
• Select **Use this name server group** to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see Using Forwarding Member Name Server Groups.

• Select **Use this set of name servers** to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name. The following is displayed for each Grid member:
  • **Name:** Displays the name of the Grid member.
  • **IPv4 Address:** Displays the IPv4 address of the Grid member.
  • **IPv6 Address:** Displays the IPv6 address of the Grid member.
  • **Override Default Forwarders:** Displays Yes when you override default forwarders. Otherwise, this field displays No.
  • **Custom Forwarders:** Displays the IP address of the custom forwarders. Otherwise, this field is blank.

**Note:** Skip the following two steps if you want to use the default forwarders.

6. Select a member and click the Edit icon.
7. In the **Edit Per-Member Forwarders** editor, select the **Override Default Forwarders** check box to override the default forwarders. The Default Zone Forwarders table becomes available only after you select the **Override Default Forwarders** check box. Click the Add icon to specify the servers to which the NIOS appliance forwards queries for the zone:
   • **Name:** Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   • **Address:** Enter the IP address of the server to which you want the NIOS appliance to forward queries.
   • **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.
   • **Save the configuration.** After successfully saving the configuration, the **Override Default Forwarders** column displays Yes and the **Custom Forwarders** column displays the IP address of the forwarders.

To configure forwarders for multiple members, repeat the steps for each Grid member.

8. Save the configuration, or click **Next** to continue to the next step where you define extensible attributes as described in Using Extensible Attributes.

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.

9. Click **Restart** if it appears at the top of the screen.

To configure a forward IPv6 reverse-mapping zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Zone -> Add Forward Zone.**
2. In the **Add Forward Zone wizard**, click **Add a forward IPv6 reverse-mapping zone** and click **Next.**
3. Enter the following zone information:
   • **IPv6 Network Address:** Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Choose the network prefix that defines the IPv6 network address space.

   or
   • **Name:** Enter the domain name of the reverse-mapping zone.
   • **DNS View:** This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   • **Comment:** Enter a descriptive comment about the zone.
   • **Disable:** Click this check box to temporarily disable this zone.
   • **Lock:** Click this check box to lock the zone so that you can make changes to it, and also prevent others making conflicting changes.

4. Click **Next** to assign a forward/stub server name server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
   • **Select Use this name server group** to assign a forward/stub server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub NS groups, see Using Forward/Stub Server Name Server Groups.
   • **Select Use this set of name servers** to specify the default servers for the zone. Click the Add icon and specify the following:
     • **Name:** Enter a domain name for the server to which you want the NIOS appliance to forward queries.
     • **Address:** Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     • **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.

5. Click **Next** to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:
   • **Select Use this name server group** to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see Using Forwarding Member Name Server Groups.
   • **Select Use this set of name servers** to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name. The following is displayed for each Grid member:
     • **Name:** Displays the name of the Grid member.
     • **IPv4 Address:** Displays the IPv4 address of the Grid member.
     • **IPv6 Address:** Displays the IPv6 address of the Grid member.
     • **Override Default Forwarders:** Displays Yes when you override default forwarders. Otherwise, this field displays No.
     • **Custom Forwarders:** Displays the IP address of the custom forwarders. Otherwise, this field is blank.
Configuring Stub Zones

A stub zone contains records that identify the authoritative name servers in the zone. It does not contain resource records for resolving IP addresses to hosts in the zone. Instead, it contains the following records:

- SOA (Start of Authority) record of the zone
- NS (name server) records at the apex of the stub zone
- A (Address) records that map the name servers to their IP addresses

Stub zones, like secondary zones, obtain their records from other name servers. Their records are read only; therefore, administrators do not manually add, remove, or modify the records.

Stub zone records are also periodically refreshed, just like secondary zone records. However, secondary name servers contain a complete copy of the zone data on the primary server. Therefore, zone transfers from a primary server to a secondary server, or between secondary servers, can increase CPU usage and consume excessive bandwidth. A name server hosting a stub zone maintains a much smaller set of records; therefore, updates are less CPU intensive and consume less bandwidth.

When a name server hosting a stub zone receives a query for a domain name that it determines is in the stub zone, the name server uses the records in the stub zone to locate the correct name server to query, eliminating the need to query the root server.

Figure 19.8 and Figure 19.9 illustrate how the NIOS appliance resolves a query for a domain name for which it is not authoritative. Figure 19.8 illustrates how the appliance resolves a query when it does not have a stub zone.

In Figure 19.8, a client sends a query for ftp.sales.corp200.com to the NIOS appliance. When the appliance receives the request from the client, it checks if it has the data to resolve the query. If the appliance does not have the data, it tries to locate the authoritative name server for the requested domain name. It sends nonrecursive queries to a root name server and to the closest known name servers until it learns the correct authoritative name server to query.

Figure 19.9 illustrates how the appliance resolves the query with a stub zone.

In Figure 19.9, when the NIOS appliance receives the request for the domain name in corp200.com, it determines it does not have the resource records to resolve the query. It does, however, have a list of the authoritative name servers in the stub zone, corp200.com. The appliance then sends a query directly to the name server in corp200.com.
Stub zones facilitate name resolution and alleviate name server traffic in your network. For example, the client in the previous examples is in corpxyz.com. The corpxyz.com and corp200.com zones are partners, and send all their communications through a VPN tunnel, as shown in Figure 19.10. The firewall protecting corpxyz.com is configured to send all messages for the 10.2.2.0/24 network through the VPN tunnel. Infoblox_A hosts the stub zone for corp200.com. Therefore, when the host in corpxyz.com sends a query for ftp.sales.corp200.com, Infoblox_A obtains the IP address of Infoblox_B (10.2.2.7) from its stub zone records and sends the query to the firewall protecting corpxyz.com. Because the destination of the query is in the 10.2.2.0/24 network, the firewall (configured to encrypt all traffic to the network) sends the request through a VPN tunnel to Infoblox_B. Infoblox_B resolves the query and sends back the response through the VPN tunnel. All name server traffic went through the VPN tunnel to the internal servers, bypassing the root servers and external name servers.

In parent-child zone configurations, using stub zones also eases the administration of name servers in both zones. For example, as shown in Figure 19.10, sales.corp200.com is a child zone of corp200.com. On the corp200.com name servers, you can create either a delegated zone or a stub zone for sales.corp200.com. When you create a delegated zone, you must first specify the name servers in the delegated zone and manually maintain information about these name servers. For example, if the administrator in sales.corp200.com changes the IP address of a name server or adds a new name server, the sales.corpxyz.com administrator must inform the corp200.com administrator to make the corresponding changes in the delegated zone records.
If, instead, you create a stub zone for sales.corp200.com, you set up the stub zone records once, and updates are then done automatically. The name servers in corp200.com that are hosting a stub zone for sales.corp200.com automatically obtain updates of the authoritative name servers in the child zone. In addition, a name server that hosts a stub zone can cache the responses it receives. Therefore, when it receives a request for the same resource record, it can respond without querying another name server.

Creating Stub Zones
When you create a stub zone on the NIOS appliance, you specify the following:

- The Grid member that is hosting the stub zone
  You can specify multiple appliances if you want the stub zones on multiple name servers. If you do, the appliances store identical records about the stub zone. You can also specify a stub member NS group for the zone. For information on specifying a stub member NS group, see Using Stub Member Name Server Groups.
- The IP address of the primary server(s) that the NIOS appliance can query in the stub zone

The primary server can be a Grid member or an external primary server. If you specify multiple primary servers, the appliance queries the primary servers, starting with the first server on the list. You can also specify a forward/stub server NS group for the zone. For information on specifying a forward/stub server NS group, see Using Forward/Stub Server Name Server Groups. The primary server and the name server hosting the stub zone can belong to the same Grid, as long as the authoritative zone and the stub zone are in different DNS views. You cannot configure one zone as both authoritative and stub in the same view.

After you create a stub zone, the NIOS appliance does the following:

1. It sends a query to the primary server for the SOA (Start of Authority) record of the stub zone. The primary server returns the SOA record.
2. Then, it sends a query for the NS (name server) records in the zone.
   The primary server returns the NS records and the A (address) records of the name servers. (These A records are also called glue records.) If the primary server is a NIOS appliance, you might have to manually create the A record and add it to the stub zone. A NIOS appliance that is the primary server for a zone always creates an NS record, but does not always create an A record.
- The appliance automatically creates an A record when its host name belongs to the name space of the zone. For example, if the zone is corpxyz.com and the primary server host name is server1.corpxyz.com, the appliance automatically creates the NS and A records and sends these records when it is queried by the stub zone name server.
- The appliance does not automatically create an A record when its host name is in a name space that is different from the zone. For example, if the zone is corp200.com and the primary server host name is server1.corpxyz.com, then the appliance creates the NS record only and sends it when it is queried by the stub zone name server. In this case, you must manually create the A record.

Maintaining Stub Zones
The NIOS appliance maintains the stub zone records and updates them based on the values in the SOA record as follows:

- The refresh interval indicates when the appliance sends a discrete query to the primary name server for the stub zone. The appliance learns about any changes in the stub zone and updates the NS and A records in the stub zone accordingly.
- If the update fails, the retry interval indicates when the appliance resends a discrete query.
- If the query continues to fail, the expiry value indicates when the appliance stops using the zone data.

Adding Stub Zones
To add a stub zone, you must identify the Infoblox appliance that hosts the stub zone, and provide the IP address of the primary server. You can also add stub zones for Microsoft servers that are managed by Grid members. For information, see Managing Microsoft Windows Servers.

You can configure a stub zone for forward mapping or reverse mapping zones.

To add a forward-mapping stub zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Add Stub Zone wizard, click Add a stub forward-mapping zone and click Next.
3. Specify the following, and then click Next:
   - Name: Enter the name for the stub zone.
   - Comment: Enter a useful comment, such as the admin to contact for the stub zone.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.
4. Click Next to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:
   - Select Use this name server group to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS groups, see Using Forward/Stub Server Name Server Groups.
   - Select Use this set of name servers to define primary servers for the stub zone. Click the Add icon and enter the Name and IP Address of the primary server in the stub zone.
     If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well. You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see Specifying Minimal Responses.
   - Optionally, click the Don't use forwarders to resolve queries in subzones check box to indicate that the name servers hosting the stub zone must not use forwarders to resolve queries for domain names in the stub zone or in its subzones.
5. Click Next to specify a stub member NS group or define the name servers individually to serve the forward-mapping stub zone. Select one of the following:
   - Select Use this name server group to assign a stub member NS group for the zone. You can select the stub member NS group from the drop-down list. For information about stub member NS group, see Using Stub Member Name Server Groups.
   - Select Use this set of name servers to define the servers individually. Click the Add icon and select one of the following:
**Add Infoblox Member:** Select this and set the Grid member that hosts the stub zone.
**Add Microsoft Server:** Select this and set the Microsoft server that hosts the stub zone. The following is displayed for each name server:
* **Name:** Displays the name of the name server.
* **IPv4 Address:** Displays the IPv4 address of the name server.
* **IPv6 Address:** Displays the IPv6 address of the name server.

6. Click **Next** to continue to the next step where you define extensible attributes as described in *Using Extensible Attributes.*

7. 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.*

You can define two types of reverse-mapping stub zones, one for IPv4 addresses and one for IPv6 addresses. To configure an IPv4 reverse-mapping stub zone:

1. From the *Data Management* tab, select the *DNS* tab, expand the Toolbar and click **Add** -> **Zone** -> **Add Stub Zone**.
2. In the *Add Stub Zone* wizard, click **Add a stub IPv4 reverse-mapping zone** and click **Next**.
3. Specify the following:
   - **IPv4 Network:** Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the *Netmask* drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
   - **To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the RFC 2317 Prefix field. Enter a prefix in the text field. Prefixes can be alphanumerics characters. For information, see *Specifying an RFC 2317 Prefix.*
   - **Name:** Enter the domain name of the reverse-mapping zone.
   - **DNS View:** This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - **Comment:** Optionally, enter additional information about the zone.
   - **Disable:** Click this check box to temporarily disable this zone.
   - **Lock:** Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.

4. Click **Next** to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:
   - **Select Use this name server group** to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS group, see *Using Forward/Stub Server Name Server Groups.*
   - **Select Use this set of name servers** to define primary servers for the stub zone. Click the Add icon and enter the **Name** and **IP Address** of the primary server in the stub zone.
     - If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well.
     - You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see *Specifying Minimal Responses.*
     - Optionally, click the **Don’t use forwards to resolve queries in subzones** check box to indicate that the name servers hosting the stub zone should not forward queries that end with the domain name of the stub zone to any configured forwards.

5. Click **Next** to specify a stub member NS group or define the name servers individually to serve the reverse-mapping stub zone. Select one of the following:
   - **Select Use this name server group** to assign a stub member NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about stub member NS group, see *Using Stub Member Name Server Groups.*
   - **Select Use this set of name servers** to define the servers individually. Click the Add icon and select one of the following:
     - **Add Infoblox Member:** Select this and set the Grid member that hosts the stub zone.
     - **Add Microsoft Server:** Select this and set the Microsoft server that hosts the stub zone. The following is displayed for each name server:
       - **Name:** Displays the name of the name server.
       - **IPv4 Address:** Displays the IPv4 address of the name server.
       - **IPv6 Address:** Displays the IPv6 address of the name server.

6. Click **Next** to continue to the next step where you define extensible attributes as described in *Using Extensible Attributes.*

7. 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.*

To configure an IPv6 reverse-mapping stub zone:

1. From the *Data Management* tab, select the *DNS* tab, expand the Toolbar and click **Add** -> **Zone** -> **Add Stub Zone**.
2. In the *Add Stub Zone* wizard, click **Add a stub IPv6 reverse-mapping zone** and click **Next**.
3. Specify the following:
   - **IPv6 Network Prefix and Prefix Length:** Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:123:4567:89ab:0000:cdcf can be shortened to 2006::123:4567:89ab:0:cdcf. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. You can enter a slash and prefix length in the IPv6 Network Prefix field or you can choose a value from the Prefix Length drop-down list.
   - **Name:** Enter the domain name of the reverse-mapping zone.
   - **DNS View:** This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - **Comment:** Enter a descriptive comment about the zone.
4. Click **Next** to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:

- **Select Use this name server group** to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS group, see [Using Forward/Stub Server Name Server Groups](#).
- **Select Use this set of name servers** to define primary servers for the stub zone. Click the Add icon and enter the **Name** and **IP Address** of the primary server in the stub zone.

If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well.

You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see [Specifying Minimal Responses](#).

Optionally, click the **Don't use forwarders to resolve queries in subzones** check box to indicate that the name servers hosting the stub zone should not forward queries that end with the domain name of the stub zone to any configured forwarders.

5. Click **Next** to specify a stub member NS group or define the name servers individually to serve the reverse-mapping stub zone. Select one of the following:

- **Select Use this name server group** to assign a stub member NS group for the zone. You can select the stub member NS group from the drop-down list. For information about stub member NS group, see [Using Stub Member Name Server Groups](#).
- **Select Use this set of name servers** to define the servers individually. Click the Add icon and select one of the following:
  - **Add Infoblox Member**: Select this and select the Grid member that hosts the stub zone.
  - **Add Microsoft Server**: Select this and select the Microsoft server that hosts the stub zone.

The following is displayed for each name server:

- **Name**: Displays the name of the name server.
- **IPv4 Address**: Displays the IPv4 address of the name server.
- **IPv6 Address**: Displays the IPv6 address of the name server.

6. Click **Next** to continue to the next step where you define extensible attributes as described in [Using Extensible Attributes](#).

7. 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 [Scheduling Tasks](#) panel, enter a date, time, and time zone.

**Viewing and Modifying SOA Records**

The timer values in the SOA record determine when the zone data is updated. The MNAME field and the RNAME field of the SOA record display the FQDN of the primary server and the administrative email address respectively. You can view these default values and override them when necessary. For a zone that has multiple primary servers, Grid Manager displays all configured primaries for the zone. You can click **Override** to override the Grid-level settings. If the primary server is a Microsoft server however, the **Override** option does not appear. You can only change certain values in the SOA record.

To view and modify zone SOA record values:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> **zone** check box, and then click the **Edit** icon.
2. In the **Authoritative Zone or Stub Zone** editor, click the **Settings** tab to view the following values. You can also click **Override** to modify some of the values:
   - **Serial number**: The current serial number for the primary server. This number is automatically increased when changes are made to the zone or its record. The serial number plays a key role in determining when and whether zone data is updated. You can change the serial number only if the primary server of the zone is a Grid member. When the zone has multiple primary servers, each primary can have its own serial number. In this case, the serial number displayed here is always that of the Grid Master, which will also appear in the primary name server list if it is one of the primaries for the zone.

   **Note**: If you change the serial number of the Grid Master, serial numbers for all primaries will be changed to the same number. A warning is displayed when you try to decrement the serial number.

   - **Refresh**: This interval tells secondary servers how often to send a message to the primary server for a zone to check that their data is current, and retrieve fresh data if it is not. The default is three hours.
   - **Retry**: This interval tells the secondary server how long to wait before attempting to recontact the primary server after a connection failure between the two occurs. The default is one hour.
   - **Expires**: If the secondary fails to contact the primary for the specified interval, the secondary stops giving answers about the zone because the zone data is too old to be useful. The default is 30 days.
   - **Default TTL**: Specifies how long name servers can cache the data. The default is eight hours.
   - **Negative-caching TTL (Time to Live)**: Specifies how long name servers can cache negative responses. The default is 15 minutes.
   - **Primary name server (for SOA RNAME field)**: If the primary name server of a zone is a Grid member, the MNAME is inherited from its corresponding member, and you can change the name of the primary name server that is published in the MNAME field of the SOA record. This field accepts names in native character sets. If the zone has multiple primary name servers, a list of all primaries is displayed in this section. Each primary has its own serial number and the number can be different among them. Note that the serial numbers for these primaries are read-only and you cannot modify them. If you change the serial number of the Grid Master, serial numbers for all primaries will be changed to the same number.
   - **Email Address (for SOA RNAME field)**: If the primary name server of a zone is a Grid member, you can enter an administrator email address to the SOA record to help people determine who to contact about this zone. The appliance supports IDN for the host name of the Email address. For example, you can create admin@. but not @..com.

   **Don't use forwarders to resolve queries in subzones**: Select this option to disable the use of forwarders to resolve queries for data in subzones.

3. Save the configuration and click **Restart** if it appears at the top of the screen. To schedule this task, click the Schedule icon at the top of the wizard. In the **Schedule Change** panel, click **Later**, and then specify a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. You can reschedule the task if you have the applicable permissions.
Configuration Example: Configuring a Stub Zone in a Grid

This example illustrates how to configure a stub zone and assign it to a Grid member. You configure a Grid, corpxyz, with a single Grid Master and Grid member. The Grid member, member1.corpxyz.com, is the primary name server for the corpxyz.com zone in the internal view. The Grid Master, gm-corpxyz.com, hosts the stub zone for corpxyz.com in the external view. Thus, when the Grid Master receives a query for the corpxyz.com zone, it sends it directly to member1.corpxyz.com, the primary name server for the zone.

In this example, you configure the following:

1. Turn off minimal responses on member1.corpxyz.com, the primary name server for the corpxyz.com zone. See Disable Minimal Responses.
2. Create the internal and external views. See Create the Views.
3. Create the corpxyz.com authoritative zone and stub zone. See Create the Zones.

Disable Minimal Responses

After you create the Grid, turn off minimal responses for member1.corpxyz.com. Disabling minimal responses ensures that member1.corpxyz.com propagates the required data to the server hosting the stub zone.

1. From the Data Management tab, select the DNS tab, click Members -> member1.corpxyz.com check box -> Edit icon.
2. In the Member DNS Configuration editor, click the General -> Basic tab.
3. Clear the Return minimal responses check box.
4. Save the configuration and click Restart if it appears at the top of the screen.

Create the Views

Create the internal and external views. To create each view:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add DNS View.
2. In the Add DNS View wizard, enter the name of the view. In this example, enter either External or Internal.
3. Click Save & New and create the other DNS view.

Create the Zones

Create the corpxyz.com zone in the internal view and assign member1.corpxyz.com as the Grid primary server:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Forward Authoritative Zone wizard, do the following:
   • Select Add an authoritative forward-mapping zone and click Next.
   • Enter the zone name, corpxyz.com and select the Internal DNS view. Click Next.
   • Select Use this set of name servers and select member1.corpxyz.com as the Grid primary server.
3. Save the configuration and click Restart if it appears at the top of the screen.

After you create the zone, you can view the NS and A records which were automatically created.

Create the stub zone, corpxyz.com, in the external view, assign gm-corpxyz.com as the stub member and member1.corpxyz.com as the stub primary server.

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Stub Zone wizard, do the following:
   • Select Add a stub forward-mapping zone and click Next.
   • Enter the name of the stub zone, corpxyz.com and select the External DNS view. Click Next.
   • In the Master Name Servers panel, click the Add icon and enter the following for the primary name server, and then click Next:
     - Name: member1.corpxyz.com
     - Address: 10.35.0.222
   • In the Name Servers panel, click the Add icon and select gm-corpxyz.com.
3. Save the configuration and click Restart if it appears at the top of the screen.

After you create the stub zone, the server hosting the stub zone, gm-corpxyz.com, sends queries to the primary server, member1.corpxyz.com, for the SOA and NS records. member1.corpxyz.com then returns its NS records and A (address) records.