Assigning Zone Authority to Name Servers

Forward-mapping zones answer name-to-address queries, and reverse-mapping zones answer address-to-name queries. When you create an authoritative forward-mapping zone or reverse-mapping zone, you assign zone authority to a name server and define it as the primary server for the zone.

A primary server is designated as the primary source for the zone and maintains a master copy of the zone data. In a traditional DNS configuration, zone updates are performed based on a model that consists of a single primary server and one or multiple secondary servers. If you use authoritative forward-mapping zones, each zone contains only zone updates from the primary through database replicates or zone transfers. Since the primary server contains editable zone data and is designated as the primary source for the zone, it can become a single point of failure when it becomes unavailable. To avoid a single point of failure for zone transfers, you can configure multiple primary servers for an authoritative zone.

When you define multiple primary servers for a zone, each primary has a copy of the zone’s authoritative data that can be updated independently. When you modify zone data, the appliance replicates updated data among all primary servers. When there are conflicts between zone updates, the appliance generally selects the latest updates based on the timestamps the updates were made by the clients to the primary servers. Therefore, accurate time synchronization among all servers in the DNS configuration is very important. For more information about other best practices for configuring multiple primaries for an authoritative zone, see Best Practices for Defining Multiple Primaries for Authoritative Zones.

You can also create one or more secondary name servers for a zone. A secondary server for a zone receives read-only zone data from the primary server. If a zone is part of an internal DNS structure for a private network, the inclusion of a secondary DNS server is optional, though highly recommended. If a zone is part of an external DNS structure for a public network such as the Internet, then a secondary server in a different subnet from the primary server is required. This requirement provides an additional safeguard against localized network failures causing both primary and secondary name servers for a zone to become inaccessible.

Note: The primary/secondary relationship between name servers is also known as a master/slave relationship. You can enter, modify, and remove zone data on the primary (or master) servers, which can then send new and modified data in a read-only format to the secondary (or slave) servers. Both primary and secondary name servers are authoritative for the zone data they serve. The distinction between them is how they get their zone data.

In Grid Manager, you can specify the primary and secondary servers for a zone or you can specify a name server group. A name server group is a collection of one or more primary servers and one or more secondary servers. For information on name server groups, see About Name Server Groups.

Best Practices for Defining Multiple Primaries for Authoritative Zones

Before you configure multiple primary servers for a zone, consider the following guidelines to ensure data integrity:

- This feature is designed to increase availability of the DNS service by allowing multiple primaries for a zone. It will not increase overall throughput of DNS update traffic, as ultimately all updates must be replicated to (and processed by) all of the primaries.
- When determining which appliances should act as primaries for the zone, consider that an additional SOA record will be required in the database for each primary. This will add to the overall record count for the zone, and each SOA will need to be updated for any change to the zone, which can impact performance.
- Enable NTP for all members (at the member level) and ensure that their times are properly synchronized with their local time servers. Ensure that you select the “Exclude the Grid Master as an NTP server” option. The appliance selects the latest zone updates based on the timestamps the updates were made by clients to the primary servers. This is especially important when there are conflicts between two or more zone updates.
- When specifying the primary server for secondaries, you can choose to have the appliance automatically select it for you based on latency, or you can manually specify it. When manually selecting a primary for zone updates, consider using one that is close in proximity to the secondary servers, which can result in better service performance. For information about setting preference for the primary server, see Adding Grid Secondaries.
- You can configure a default primary for DDNS updates to a zone with multiple primary servers. To enhance service performance, select a default primary that is close in proximity to the DHCP server that provides DDNS updates. This is especially useful if you have DHCP members that are located in different locations. You can configure a different default primary for each DHCP member based on their locations. For more information, see Defining the Default Primary for DDNS Updates to Zones with Multiple Primaries.
- DNSSEC is not supported for zones with multiple primary servers. These zones must be unsigned. For information about DNSSEC, see About DNSSEC.
- When determining which appliances should act as primaries for the zone, consider that an additional SOA record will be required in the database for each primary. This will add to the overall record count for the zone, and each SOA will need to be updated for any change to the zone, which can impact performance.

Specifying a Primary Server

When you create a zone, the primary server can be a Grid member, an external DNS server that you specify, or a Microsoft DNS server that is managed by a Grid member. For information about managing Microsoft Windows DNS servers, see Chapter 34, Managing Microsoft Windows Servers.

Although a zone typically has only one primary server, you can specify multiple primary servers for an authoritative zone. You can configure multiple Grid primaries or multiple external primaries (including Microsoft AD-integrated servers) for a zone, but you cannot configure both at the same time for the same zone. In addition, you can configure one Microsoft server, but not multiple Microsoft servers (except for Microsoft AD-integrated servers), as the primary server for a zone. Note that each primary server that you configure for a zone has its own MNAME for the SOA record and serial number. For information about how to view and modify certain values in the SOA record, see Viewing and Modifying SOA Records.

A hidden primary provides data to its secondary servers, which in turn respond to DNS queries using this data. One of several advantages of this approach is that you can take the primary server offline for administrative or maintenance reasons without causing a disruption to DNS service (within the expiration interval set for the validity of its zone data—the default is 30 days).

When you add an authoritative forward-mapping zone and assign responsibility for the zone to a primary name server whose host name belongs to the name space of the zone, the NIOS appliance automatically generates an NS (name server) record and an A (address) record for the name server. This type of A record is called a glue record because it “glues” the NS record to the IP address (in the A record) of the name server.

In Grid Manager, you can specify the primary server for a zone when you create it using the Add Authoritative Zone wizard, or when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones. The following procedure describes how to access the editor of a zone. To specify a primary server for an existing zone:
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 editor, click Name Servers.
3. Select Use this set of name servers.
4. Click the Add icon and select one of the following options for a primary server:
   - **Grid Primary**: Choose this option to select a Grid member as the primary server for the zone. See **Specifying Grid Primary Servers**.
   - **Microsoft Primary**: Choose this option to select a Microsoft DNS server as the primary server for the zone. See **Specifying Microsoft Primary Servers**.
   - **External Primary**: Choose this option if the appliance is in a Grid and you want to specify a primary server outside the Grid (“external” to the Grid). See **Specifying External Primary Servers**.
5. Save the configuration and click Restart if it appears at the top of the screen.

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**.

### Specifying Grid Primary Servers

In the **Add Grid Primary** panel, do the following, and then click **Add** to add the Grid member to the list of name servers for the zone as primary:

- If no member is displayed, click **Select** to specify a Grid member. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select a primary name server. To select multiple primary servers, click **Select** and then **Add** again.
- **Stealth**: Click this to hide the NS record for the primary name server from DNS queries. The NIOS appliance does not create an NS record for the primary name server in the zone data. Clear the check box to display the NS record for the primary name server in responses to queries.

### Changing the SOA Name for a Zone

If the primary name server of a zone is a Grid member, the NIOS appliance allows you to change the SOA (start of authority) name that is automatically created when you initially configure the zone. For example, you might want to hide the primary server for a zone. If your appliance is named dns1.zone.tld, and for security reasons, you may want to show a secondary server called dns2.zone.tld as the primary server. To do so, you would go to dns1.zone.tld zone (being the true primary) and change the SOA to dns2.zone.tld to hide the true identity of the real primary server.

To change the SOA name for a zone:

1. From the Data Management tab, select the DNS tab > Zones tab> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click **Override** beside the **Primary name server** field and enter the new SOA name. This field supports IDN.
4. 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**.

### Specifying Microsoft Primary Servers

You can assign a Microsoft server as the primary server of a zone when it is managed by a Grid member in read/write mode. For information, see **Chapter 34, Managing Microsoft Windows Servers**. When a Microsoft server is the primary server of a zone, the zone supports only standard DNS resource records. It does not support the Infoblox record types host records, bulk host records, and shared record groups. You cannot add any of these records to the zone nor assign a DNS zone with these records to a Microsoft server as the primary server.

In the **Add Grid Primary** panel, do the following to assign a Microsoft primary server:

1. Complete the following:
   - **Select Use this set of name servers**.
   - Click the Add icon and select Microsoft Primary.
2. In the **Add Microsoft Primary** panel, do the following, and then click **Add** to add the Microsoft primary server to the list of name servers for the zone:
   - **Select Server** to specify a Microsoft server. When there are multiple servers, Grid Manager displays the Server Selector dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
   - **Information to create NS record**: Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the Name and IP Address fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth. You can specify a different FQDN or IP address for the NS record; for example, for a multithomed server.
   - **Store the zones in Active Directory (AD Integrated Zone)**: This is enabled and selected by default only if the Microsoft server is a domain controller. Note that you can enable Active Directory integration only after the Microsoft server has been synchronized at least once because its AD ability is not known before the synchronization. This is disabled when the Microsoft server is not a domain controller.
   - **Stealth**: Select this option to hide the NS record for the primary name server from DNS queries. Grid Manager does not create an NS record for the primary name server in the zone data. Clear this option to display the NS record for the primary name server in responses to queries. Note that this option is not available for AD-integrated zones.

### Specifying External Primary Servers

In the **Add External Primary** panel, do the following, and then click **Add** to add the external primary server to the list of name servers for the zone:

- **Name**: Type a resolvable domain name for the external primary server.
- **Address**: Type the IP address of the external primary server.
- **Multi-master**: This appears only when there is more than one external primary assigned to the zone. Select this check box for external primary servers when the zone is in another Grid and has multiple Grid primaries. When you select this option, it is selected for all external primaries assigned to the zone. This zone is identified as an external zone with multiple primary servers.
• **Use TSIG:** To authenticate zone transfers between the local appliance and the external primary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, The MD5 Message-Digest Algorithm, and RFC 2104, HMAC: Keyed-Hashing for Message Authentication.

• **Key name:** Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key on the external primary server.

• **Key Data:** Type or paste a previously generated key. This key must also be present on the external primary server. You can generate a TSIG key, or obtain the TSIG key name and key from the external name server, by accessing the server yourself or by requesting the server administrator to deliver them to you through some out-of-band mechanism. Then type or copy-and-paste the name and key into the appropriate fields.

• **Use 2.x TSIG:** If you want to use TSIG authentication and the external primary name server is a NIOS appliance running DNS One 2.x code, select this check box. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

Note: On the appliance you configure as a secondary server for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the Grid, member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.

### Specifying Secondary Servers

A secondary name server is as authoritative for a zone as a primary server. Like a primary server, a secondary server answers queries from resolvers and other name servers. The main difference between a secondary and primary server is that a secondary server receives all its data from a primary server, or possibly from another secondary server that relays zone data it receives. The zone data passes from a primary to a secondary server (and possibly from that secondary server on to another secondary server). This process is called a zone transfer.

The advantage of using primary and secondary name servers is that you enter and maintain zone data in one place—on the primary server. The data is then distributed to the one or more secondary servers. Secondary servers can be Grid members, external DNS servers or Microsoft DNS servers that are managed by Grid members. In Grid Manager, you can specify the secondary server for a zone when you create it using the Zone wizard. You can also specify the secondary server for a zone when you add a new zone to the wizard, or when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones. The following procedure describes how to access the editor of a zone.

To specify a secondary server for an existing zone:

1. From the Data Management tab -> DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select **Use this set of name servers.**
4. Click the Add icon and select one of the following options:
   - **Grid Secondary:** Selects the local appliance as the secondary server (or if the appliance is deployed in a Grid and you want to make a different member the secondary server), See Specifying Grid Secondaries.
   - **Microsoft Secondary:** Select this option if you want to specify a managed Microsoft DNS server as a secondary server. See Specifying Microsoft Secondary Servers.
   - **External Secondary:** Select this option if the appliance is in a Grid and you want to specify a secondary server outside the Grid ("external" to the Grid), or if the appliance is deployed independently from a Grid. See Specifying External Secondaries.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

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.

### Adding Grid Secondaries

When adding Grid secondaries to a zone that has multiple primary servers, the appliance selects a primary server as the active server based on the method that you have selected. If you select **Automatic**, the primary is selected based on latency determination, which occurs separately on each primary. When available, the primary server that has the lowest latency is preferred. When you select **Manual**, latency determination is ignored, and the first available primary server in the list is selected as the active server. Thus if the first primary on the list is not available, the next available primary is used. Depending on which primary server is selected, the Grid secondary returns the FQDN of the primary in the MNAME field of the zone SOA record. It also includes the version of the zone content that it serves.

In the Add Grid Secondary panel, enter the following, and then click **Add** to add the Grid secondary server to the list of name servers for the zone:

- **If no member is displayed,** click **Select** to specify a Grid member. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select a name server.
- **Stealth:** This setting applies only if the primary server is a Grid member or Microsoft server. Select this to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for this name server in the zone data. Select the check box again to display the NS record for the secondary name server in responses to queries. A secondary server in stealth mode is also known as a “hidden secondary”.  
  For example, you can configure a hidden secondary when a secondary server is at a branch office with a slow connection to the rest of corporate network. Configure local hosts at the branch office to send DNS queries to the secondary server, but keep it hidden from other name servers on the rest of the network so that they do not send it queries. Instead, they use a server located in a different part of the network that has faster connection speeds.
- **Lead Secondary:** This option becomes available only after you specify the primary name server as external. When a primary server is external to a Grid whose members are secondary servers, you can select this check box to designate one member as a lead secondary. The primary server sends zone transfers to the lead secondary, which distributes the zone data to the other secondary servers in the Grid using zone transfers (not the Grid data replication mechanism). After you designate a Grid member as a lead secondary for a zone, you do not have to configure members to use the lead secondary server. All other Grid members acting as secondary servers for the zone automatically use the lead secondary to get zone data. Using a lead secondary simplifies the addition, modification, and removal of other secondary servers in the Grid. As long as the lead
secondary remains unchanged, you need not update intervening firewall policies or the external primary server whenever you make changes to non-lead secondary Grid members. This approach also reduces the amount of traffic between primary and secondary servers.

- **Update Zones Using:** This option becomes available only after you specify a Grid member as the primary server.
  - **Grid Replication (recommended):** Select this check box to use Grid replication to move zone data from the primary to secondary servers.
  - **DNS Zone Transfers:** Select this check box to use the DNS zone transfer process to move zone data from the primary to secondary servers.
  - **Primary Preference:** This appears only for Grid secondaries that are assigned to zones with multiple primaries. Select one of the following to set preference for selecting the primary server:
    - **Automatic:** Choose this to allow the appliance to select the optimum primary server for zone updates based on latency determination, which prefers the primary server that has the lowest latency. This is selected by default.
    - **Manual:** Choose this to manually select primaries for zone updates. In the Available Primaries and Selected Primaries tables, click a name server and use the arrows to select and deselect primaries between the tables. Then use the up and down arrows next to the Selected Primaries table to put the selected primaries in a preferred order. The secondary servers will get zone updates from the selected primary server based on the given order. To optimize service performance, select primary servers that are close in proximity to the secondary servers.

### Specifying Microsoft Secondary Servers

You can assign a Microsoft server as the primary server of a zone when it is managed by a Grid member in read/write mode. For information, see *Chapter 34, Managing Microsoft Windows Servers.* Since Microsoft servers cannot replicate data from the Grid, when a DNS zone is defined as a secondary on a Microsoft server, the Microsoft server obtains the content of the zone only through DNS zone transfers.

- In the Add Microsoft Secondary panel, do the following:
  - If no server is displayed, click Select Server to specify a Microsoft server. When there are multiple servers, Grid Manager displays the Server Selector dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
  - **Information to create NS record:** Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the Name and IP Address fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth.
  - **Stealth:** This setting applies only if the primary server is a Grid member or a Microsoft server. Select this option to hide the NS record for the secondary name server from DNS queries. Grid Manager does not create an NS record for this name server in the zone data. Clear this option to display the NS record for the secondary name server in responses to queries.

### Specifying External Secondaries

In the Add External Secondary panel, enter the following, and then click Add to add the external secondary server to the list of name servers for the zone:

- **Name:** Enter a resolvable domain name for the external secondary server.
- **Address:** Enter the IP address of the external secondary server.
- **Stealth:** This setting applies only if the primary server is a Grid member or a Microsoft server. Click this check box to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for the secondary name server in the zone data. Select the check box again to display the NS record for the secondary name server in response to queries.

**Note:** To avoid an impact on your database performance, Infoblox recommends that you do not configure a large number of external secondary servers in stealth mode. To ensure that these secondary servers receive notifications about zone updates, you can allow zone transfers for these IP addresses and then enable the appliance to add them to the also-notify statement. For information about how to configure this feature, see *Configuring Zone Transfers.*

- **Use TSIG:** To authenticate zone transfers between the local appliance and the external secondary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, *The MD5 Message-Digest Algorithm,* and RFC 2104, *HMAC: Keyed-Hashing for Message Authentication.*
- **Key name:** Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key for this zone on the external secondary server.
- **Key:** Type or paste a previously generated key. On the external secondary server, this key must also be present and associated with this zone. You can generate a TSIG key, or you can obtain the TSIG key name and key from the external name server, either by accessing the appliance yourself or by requesting the appliance administrator to deliver them to you through some out-of-band mechanism. Then, type or copy-and-paste the name and key into the appropriate fields.
- **Use 2.x TSIG:** Select this check box to use TSIG authentication and the external secondary name server is a NIOS appliance running DNS One 2.x code. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

**Note:** On the appliance you configure as a secondary for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the Grid, member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.