Configuring DNS Servers for DDNS

For security reasons, an Infoblox DNS server does not accept DDNS updates by default. You must specify the sources from which you want to allow the DNS server to receive updates. You can configure the Infoblox DNS server to receive updates from specified DHCP clients, as described in Enabling DNS Servers to Accept DDNS Updates, and to accept forwarded updates from another DNS server, as described in Forwarding Updates.

For protection against spoofed IP addresses, you can use TSIG (transaction signatures) to authenticate and verify updates. TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code) — sometimes called a digital fingerprint — of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them. Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations.

The TSIG key that you use can come from several places:

- You can use the key generation tool described in this section to create a new TSIG key to authenticate updates from the DHCP server.
- You can enter (copy and paste) a TSIG key that you previously generated for another purpose, such as for zone transfers.
- If the DHCP server is on a separate appliance and a TSIG key was previously generated on that appliance, you can enter (copy and paste) that TSIG key onto the local DNS server.

The TSIG key name and value that the DHCP and DNS servers use must be the same.

Note: Whether you deploy NIOS appliances in a Grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel. Grid members do, however, authenticate updates between them using TSIG (transaction signatures) based on an internal TSIG key.

Enabling DNS Servers to Accept DDNS Updates

You can configure the Infoblox DNS server to receive updates from specified DHCP clients only. You can set this for the Grid so that the Grid members receive DDNS updates only from the specified sources. Note that you specify the IP addresses of the sources of the updates and not the actual IP addresses in the DNS records being updated.

To configure the DNS server to accept updates from the specified sources:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   - Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   - Zones: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.
   - In the editor, click Toggle Advanced Mode, select the Updates tab.

Note: Ensure that you understand how the appliance handles match lists before you specify the list of IP sources for DDNS updates, as described in You can use the following OpenStack cloud-init template to configure an IB-V815 as a Grid Master.

3. In the Allow updates from section, select one of the following:

   - **None**: Select this to deny DDNS updates from all DHCP clients. 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 receives DDNS updates from the 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. 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 a remote name server. 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.

Note: You must enable GSS-TSIG signed updates to receive DDNS updates from TSIG key based ACEs. For information about how to enable this, see Accepting GSS-TSIG Updates.

   - **Any Address/Network**: Select this to receive DDNS updates from any IP addresses. After you have added access control entries, you can do the following:
**Forwarding Updates**

When a secondary DNS server receives DDNS updates, it must forward the updates to the primary server because it cannot update zone data itself. In such situations, you must enable the secondary server to receive updates from the DHCP server, and then forward them to the primary DNS server.

To configure the secondary server to accept and forward updates for all zones:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. **Member:** From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
3. **Zones:** From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view-> zone check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.
4. In the editor, click Toggle Advanced Mode.
5. When the additional tabs appear, click the Advanced subtab of the Updates tab, and then complete the following:
   - **Allow secondary name servers to forward updates:** Select this check box.
   - **Forward updates from:** This is available only for authoritative zones. Click Add. Depending on the item that you select, Grid Manager 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:
     - **None:** Select this to deny DDNS updates from any clients. 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 receives DDNS updates from the 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. 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 a remote name server. 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.

   **Note:** You must enable GSS-TSIG signed updates to receive DDNS updates from TSIG key based ACEs. For information about how to enable this, see Accepting GSS-TSIG Updates.

   - **Any Address/Network:** Select to allow or disallow the appliance to receive DDNS updates from any IP address. 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 NamedACL 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.

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