Enabling Zone Transfers

A zone transfer is the process of sending zone data across a network from one name server to another. When the primary server detects a change to its zone data, it notifies the secondary servers. The secondary servers reply by checking to see if the serial number they have for the zone is as large as the serial number for the zone on the primary server. If not, the secondary servers request a zone transfer. In addition to receiving zone change notifications, a secondary server periodically polls the primary server to see if their zone data is in sync. In response, the primary server can send a DNS message containing just the changed zone data, or the entire data set. The first type of transfer is known as an incremental zone transfer, or IXFR. The second type of transfer is known as a full zone transfer, or AXFR.

A NIOS appliance, acting as the primary name server for a zone, allows zone transfers to secondary name servers by default. This includes all servers listed in the NS records for that zone. (Secondary name servers in a Grid, however, receive updated zone data via database replication by default, as explained later in this section.) You can also specify zone transfers to other name servers, such as when migrating zone data to a new server or to a management system. You can specify one or more destinations to which the local appliance sends zone transfers. You can also specify the security and format of the transfers.

Note that secondary name servers periodically query the primary name server to find out if zone data has been changed. Each query takes a certain amount of time and bandwidth on the network. By default, secondary name servers limit the rate (serial-query-rate) at which these queries are being sent. Thus when the secondary name servers are serving a large number of zones, it may take a long time to detect changes to their zone data. You can configure this value to optimize the query rate on the network. In addition, when you have set up a few secondary name servers for a large number of zones, a delay in zone transfers may occur due to the default zone transfer configuration that limits concurrent zone transfers to 10 per secondary server. You can configure the maximum value of concurrent zone transfers to optimize the zone transfer operation.

For information about how to optimize zone transfers, see Configuring Concurrent Zone Transfers. By default, Grid members automatically receive updated zone data via database replication (through an encrypted VPN tunnel). You can change the default behavior to allow Grid members to use zone transfers instead of Grid replication. Keep in mind that a database replication updates zone data for both the active and passive nodes of an HA member. Therefore, if there is a failover, the new active node (the previous passive node) immediately begins serving zone data with fresh information. In the case of a zone transfer, the passive node does not receive zone data until after a failover, when it becomes an HA master. At that time, it performs a zone transfer. If there is a lot of zone data, the transfer can take up to several minutes, thereby causing a break in the availability of the new HA master. If you have HA members as secondary servers, zone transfers can result in service interruption when there is a failover. Furthermore, if the primary server is down when the HA member fails over, the new active node cannot receive zone data until the primary server comes back online. You can use TSIG (transaction signature) keys to authenticate zone transfer requests and replies. The same key name and key value must be on the primary and secondary name servers for TSIG-authenticated zone transfers to occur. When using TSIG, it is important that both appliances involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings). You can control zone transfers at the Grid, member, and zone levels. This enables you to specify a different set of name servers for a Grid, member, and zone, if necessary. You can also control which external secondary servers should receive notifications about zone updates by adding their IP addresses to the also-notify statement for each authoritative zone that is served by a Grid member. Infoblox recommends that you use this feature to notify hidden external secondary servers about zone updates, instead of putting them in stealth mode, especially when you plan to configure a large number of them. For information about how to add IP addresses to the also-notify statement, see Configuring Zone Transfers.

Configuring Zone Transfers

To configure zone transfers, you identify the servers to which zone data is transferred and optionally, servers to which data must not be transferred. For example, you can allow transfers to a network, but not to a specific server in the network. You can specify a different set of servers for specific Grid members and zones. For example, if certain Grid members are primary servers for a zone, then you can specify the secondary servers to which that member is allowed to transfer zones. You can also enable the appliance to add all IPv4 and IPv6 addresses for which you allow zone transfers to the also-notify statement for each authoritative zone that is served by a Grid member. The also-notify statement defines a list of addresses that receive notifications about zone updates, in addition to the IP addresses listed in the NS records for the zone. Use this feature to configure a large number of external secondary servers, instead of putting them in stealth mode.

To configure zone transfer properties:

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, click the Members tab -> member check box -> Edit icon. **Zone:** From the Data Management tab, select the DNS tab, click the Zones tab -> zone check box, and then click the Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click **Toggle Advanced Mode**, select the Zone Transfers tab.

3. In the Allow zone transfers to section, select one of the following:
   - **None:** Select this to deny all clients for DNS zone transfers. 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 Selecto r. 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, the appliance allows remote name servers that have the Allow permission to send and receive zone transfer data. 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 IPv address of the remote name server. The Permission column displays Allow by default. You can change it to Den y 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 remote name server with which the local server authenticates zone transfer requests and replies. This name must match the name of the same TSIG key on other name servers that use it to authenticate zone transfers with the local server.
    - **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 to allow or deny the local appliance to send zone transfers to 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 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.
  - **Key**: To specify a zone transfer format:
    - **Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
    - **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.

4. Optionally, select the **Add allowed IP addresses to also-notify** check box to add all IPv4 and IPv6 addresses listed in the “Allow zone transfers to” table to the also-notify statement for each authoritative zone served by a Grid member. When you enable this, all external secondary servers that are not defined for the zone and are allowed zone transfers will receive notifications about zone updates, in addition to name servers assigned to the zone. 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, add their addresses to the “Allow zone transfers to” table and grant them the “Allow” permission, and then select this check box.

Note: The appliance includes only IPv4 and IPv6 addresses. It does not include network addresses, TSIG keys, and denied addresses. When you configure a named ACL, all allowed IPv4 and IPv6 addresses in the named ACL are added to the also-notify statement.

5. Optionally, you can:
   - Modify an item on the list by selecting it and clicking the Edit icon.
   - Remove an item from the list by selecting it and clicking the Delete icon.
   - Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow.

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

### Specifying a Zone Transfer Format

The zone transfer format determines the BIND format for a zone transfer. This provides tracking capabilities for single or multiple transfers and their associated servers.

To specify a zone transfer format:

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, click the Members tab -> member check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.
2. In the editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click the Advanced subtab of the Zone Transfers tab to specify the zone transfer format. Select one of the following options from the Default Zone Transfer Format drop-down menu:
   - **many-answers** (Secondaries run BIND 8/9): includes as many records as the packet size allows
   - **one-answer** (Secondaries run BIND 4): includes one record per packet
4. To exclude servers, click the Add icon in the Zone Transfer Format Exceptions table and enter the IP address of the server in the Addresses field.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring Concurrent Zone Transfers

The default number of zone transfers that are allowed is set at the Grid or member level. However, you can override the default value and configure the required concurrent zone transfers. Note that when you increase the number of concurrent zone transfers, there will be an impact on CPU and memory usage.
Note: The tcp-client value is unconditionally set to 200 to control the total number of simultaneous TCP connection, which caps the maximum inbound and maximum outbound transfer plus any DNS request made with the TCP. The tcp-client value specifies the maximum number of simultaneous DNS clients that can be handled with TCP connections and does not account for UDP connections. The UDP connection accounts for the regular DNS requests and TCP is used only for AXFR and rare DNS requests that don't fit in a UDP connection.

To specify concurrent zone transfers:

1. **Grid:** From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties.**

2. **Independent appliance:** From the **System** tab, select the **System Manager** tab, expand the Toolbar and click **System Properties -> Edit.**

3. **Member:** From the **Data Management** tab, select the **DNS** tab and click the **Members tab -> member check box -> Edit.**

4. When the additional tabs appear, click the **Advanced** subtab of the **General** tab.

5. You can change the zone transfer settings as follows:
   - **Maximum inbound concurrent zone transfers:** The maximum number of inbound zone transfers that can be performed concurrently. Click **Override** to override the value inherited from the Grid and enter the required value. The default value is 10. Make sure that you specify a value from 10 to 100. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click **Inherit.**
   - **Maximum outbound concurrent zone transfers:** The maximum number of outbound zone transfers that can be performed concurrently. Click **Override** to override the value inherited from the Grid and enter the required value. The default value is 10. Make sure that you specify a value from 1 to 100. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click **Inherit.**
   - **Maximum concurrent inbound zone transfers per remote name server:** The maximum number of zone transfers that can be performed concurrently from a given remote name server. This configuration can be done on a per server basis. Click **Override** to override the value inherited from the Grid and enter the required value. The default value is 2. Make sure that you specify a value from 2 to 100. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click **Inherit.**
   - **Maximum concurrent SOA queries:** The maximum number of concurrent queries a secondary name server sends to the primary server to find out if the zone serial numbers have been changed. Click **Override** to override the value inherited from the Grid and enter the required value. The default value is 20. Make sure that you specify a value from 20 to 1000. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click **Inherit.**

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