Configuring Members to Manage Microsoft Servers

You can manage Microsoft DNS and DHCP servers on any Grid member. To avoid performance issues, Infoblox strongly recommends that you do not configure Microsoft DNS and DHCP servers on the Grid Master and Grid Master candidate.

When an HA pair manages Microsoft servers, the active node handles synchronization. If an HA failover occurs during a synchronization, the failing node immediately aborts the synchronization. The new active node resumes the next synchronization. Changes that occurred on the Grid since the end of the last synchronization are lost.

For Microsoft DHCP failover, NIOS supports both the hot standby and load sharing modes in both Read/Write and Read-only modes on DHCP servers running Microsoft Windows 2012 and 2012 R2. For more information about Microsoft DHCP failover, refer to the Microsoft documentation.

Complete the following tasks to configure a Grid member to manage a Microsoft server:

1. On the Microsoft server, create a user account for the Grid member. For information, see Setting Microsoft Server Credentials.
2. On the Grid Master, configure the managing member, as described in Configuring a Managing Member.

Setting Microsoft Server Credentials

To enable a Grid member to synchronize data with a Microsoft server and control DNS and DHCP services, you must do the following on the Microsoft server:

1. Create a user account for the Grid member.
2. Grant the user account the necessary permissions.

You can either add the user account to the Administrators Group or add the user account to specific groups and explicitly set only the permissions necessary to access the DHCP and DNS services of the Microsoft server. The following sections provide general instruction on each method.

Adding User Account to the Administrators Group

Adding the user account of the Grid member to the Administrators Group provides total control over the Active Directory Domain. Do one of the following:

- If the managed Microsoft server is a standalone server or a member server in a domain, open Computer Management, click Groups, and add the user account to the Administrators Group.
- If the managed Microsoft server is a domain controller, open Active Directory Users and Computers, select the domain name, click BuiltIn, and add the user account to the Administrators Group.

Setting Specific Group Memberships and Permissions

If your security policy precludes adding user accounts to the Administrators group, you can add the user account to individual groups and grant only the required permissions. For guidelines and more information, see the following:

http://support.microsoft.com/kb/325349
http://support.microsoft.com/kb/914392

To add the user account of the Grid member to individual groups and grant specific permissions:

- To enable the member to synchronize DNS data with the Microsoft server, add its user account to the DnsAdmins Group.
- To enable the member to synchronize DHCP data with the Microsoft server, add its user account to the Dhcp Administrators Group.
- To enable the Grid member to monitor, start, and stop the DNS and DHCP services, grant the user account permissions on the Service Control Manager (SCM), as follows:
  2. Grant permissions to the DNS and/or DHCP service on each managed server by doing one of the following:
     - Use the sc command line utility to remotely configure each managed DNS or DHCP server.
     - Use the Domain Controller Policy editor to define a global policy that applies to all DNS or DHCP services running in a domain or on domain controllers. For additional information, refer to http://support.microsoft.com/kb/324802.

Configuring a Managing Member

When you configure a member to manage Microsoft servers, you must specify the following:

- The management mode of the Microsoft server. For information, see Setting the Management Mode.
- A network view, if there is more than one in the Grid, and a DNS view, if there is more than one in the network view. For information, see Synchronizing to a Network View and DNS View.

For the steps on configuring the managing member, see Assigning Grid Members to Microsoft Servers.

Setting the Management Mode
A Grid member can manage a Microsoft server in Read-only mode, which is the default, or in read-write mode. In Read-only mode, the Grid member copies the DNS and DHCP data from the Microsoft server to the Grid so Grid Manager admins can view the synchronized data. They cannot update the data, control the DNS and DHCP service of the Microsoft server, or configure any properties.

When you select Read-only mode for Active Directory sites, you can view the sites and networks that are present on the Microsoft server through Grid Manager. Note that you cannot manage the Active Directory sites and networks directly from the Grid, but you can manage an object within the Grid that is associated with a Read-only Active Directory Site or an Active Directory network. The synchronization process is Read-only and you cannot write into the Microsoft server in this mode.

In Read/Write mode, Grid Manager admins are allowed to update the data of the Microsoft server. Therefore during each synchronization, the Grid member applies changes from the Grid to the Microsoft server and vice versa. Read/Write mode also allows admins to control DNS and DHCP services of the Microsoft server and configure some of their properties.

When you select Read/Write mode for Active Directory Sites, you can view and manage the sites and networks that are present on the Microsoft server through Grid Manager. When you update an object that is associated with the Active Directory Site or an Active Directory network, the changes reflect on the Microsoft server.

Note that the management mode of a Microsoft server is separate from the admin permissions that the appliance requires to access the Microsoft servers and DNS and DHCP resources. An admin must still have the applicable permissions to the Microsoft servers and DNS and DHCP resources they want to access. For information on admin permissions, see Administrative Permissions for Microsoft Servers.

**Synchronizing to a Network View and DNS View**

A Microsoft server can synchronize its data only to a single network view and a DNS view. Grid Manager automatically assigns Microsoft servers to the default view when a Grid contains only the default network view and DNS view. If a Grid has more than one network view, you must select a network view for the Microsoft server to synchronize its data; and if there are multiple DNS views, you must select a DNS view as well.

You cannot modify the assigned network view or DNS view of a Microsoft server after its data has been synchronized. Instead, you must remove the Microsoft server and then add it again. For information about removing a server, see Removing a Managed Microsoft Server.

Microsoft servers do not support network views and DNS views. Therefore, network view and DNS view properties have no effect on the DNS and DHCP data that are synchronized from Microsoft servers.

**Assigning Grid Members to Microsoft Servers**

To configure a Grid member to manage one or more Microsoft servers:

1. **Grid**: From the Grid tab -> Microsoft Servers tab -> Servers tab, click the Add icon.
   - **Standalone appliance**: From the System tab -> Microsoft Servers tab -> Servers tab, click the Add icon.
   - **Grid**: From the Add Microsoft Server(s)/wizard, complete the following:
     - Which features do you want to configure?: This section appears only when you have selected the Enable MS AD feature check box for mapping network users. For more information, see Enabling Identity Mapping. You can select multiple options in this section:
       - **Network Users**: Select this check box to enable the Grid member to synchronize user information with the managed Microsoft servers.
       - **DNS and DHCP Services**: Select this check box to enable the Grid member to synchronize DNS and DHCP services with the Microsoft servers.
       - **Active Directory Sites**: Select this check box to enable the Grid member to synchronize Active Directory sites.
     - In the General Settings section, complete the following:
       - **Managing Member**: Click Select Member and select the Grid member that manages Microsoft servers. Select None if you do not want to associate a Microsoft server with a Grid member.
       - **Credentials to Connect to the Microsoft Server(s)**: Enter the login name and password that the appliance uses to connect to the Microsoft servers. These must be the same as those you specified when you created the user account for the Grid member on the Microsoft servers. Note that you must specify the domain name and the user name in the following format: domain\name/user_name.
       - **Manage Server(s)**: Select the management mode, which is either Read-only or Read/Write. You can choose to manage the DNS and DHCP synchronization services in either Read-only or Read/Write mode. For more information, see bookmark261.
     - Minimum Synchronization Interval (min): The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Synchronizing large data sets could take longer than the synchronization interval, causing a delay in the start of the next synchronization. For example, if the synchronization interval is two minutes but a synchronization takes five minutes, the time between the start of the first synchronization and the start of the next one is approximately seven minutes.

2. **In the Microsoft Server(s)/wizard**: Enter the login name and password that the appliance uses to connect to the Microsoft servers. These must be the same as those you specified when you created the user account for the Grid member on the Microsoft servers. Note that you must specify the domain name and the user name in the following format: domain\name/user_name.

**Note**: The synchronization of Microsoft DHCP servers running Microsoft Windows 2012 or later includes the synchronization of DHCP failover relationships. Note that the DNS and DHCP failover synchronization rules do not have an impact on the Microsoft servers running a Windows version that is earlier than 2012.

- **Logging Level**: Select a logging level for the Microsoft server log from the drop-down list: Low, Normal, High, and Debug. NIOS logs the messages based on the logging level you set.
  - **Low**: Logs only error messages.
  - **Normal**: Logs warning and error messages.
  - **High**: Logs warning, error and information messages.
  - **Debug**: Logs messages about all events associated with synchronization.

  See Viewing Synchronization Logs for a description of each level.
**Logging output destination:** From the drop-down list, select an output destination to which the appliance saves log messages for Microsoft servers. When you select **Microsoft Log**, the appliance logs the messages that are generated for the respective Microsoft server in the existing Microsoft log. This is selected by default. For more information, see **Viewing Synchronization Logs**. When you select **Syslog**, NIOS logs the messages that are generated for the respective Microsoft server in the syslog. For more information about the syslog, see **Viewing the Syslog**.

**Synchronize Data into Network View:** This field appears only when there is more than one network view in the Grid. Specify to which network view the data from the Microsoft servers is synchronized.

**Synchronize DNS Data into DNS View:** This field appears only when there is more than one DNS view in the network view. Specify to which DNS view the data from the Microsoft servers is synchronized.

**Comment:** You can enter additional information about the servers.

**Disable Synchronization:** Select this to disable the Microsoft servers. This allows you to preprovision the Microsoft servers and then enable them at a later time.

3. Click **Next**.

---

**Note:** Depending on your configuration in the **Which features do you want to configure?** section, the **Add Microsoft Server(s)** wizard displays the Microsoft server setting options.

---

4. Complete the following:

- If you have selected the **Network Users** check box, complete the following in the **Select your across-server settings for Network Users** page:
  - **Use General credentials (from first page of wizard):** Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers.
  - **Credentials for synchronizing Network User service information:** Specify a username and password to synchronize user information from Active Directory domain controllers. The username you specify here must belong to the Domain User group and Event Log Reader group in Microsoft. For information, see **Prerequisites on the Microsoft Server**.
  - **Use General synchronization interval (from first page of wizard):** Select this check box to use the same synchronization interval that you specified in the **Minimum Synchronization Interval** for synchronizing the user and device mapping information from the Microsoft Active Directory authentication logs.
  - **Minimum synchronization interval:** The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize user information from the Microsoft Active Directory authentication logs.

- If you have selected the **DNS and DHCP Services** check box, complete the following in the **Select your across-server settings for DNS and DHCP Services** page:
  - **Use General credentials (from first page of wizard):** Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers.
  - **Credentials to connect to DNS and DHCP Services:** Specify a username and password to synchronize DNS and DHCP services. You must use the same username and password that you specify here when the appliance prompts for credentials during DNS or DHCP synchronization.
  - **Use General synchronization interval (from first page of wizard):** Select this check box to use the same synchronization interval that you specified in the **Minimum Synchronization Interval** for synchronizing the DNS and DHCP services as well.
  - **Minimum Synchronization interval:** The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the DNS and DHCP data from the Microsoft server.
  - **Manage DNS and DHCP services in:** Select a value from the drop-down list. You can choose to manage the DNS and DHCP synchronization services in either **Read-only** or **Read/Write** mode. For more information, see **bookmark2618**.

- If you have selected the **Active Directory Sites** check box, complete the following in the **Select your across-server settings for Active Directory Sites** page:
  - **Use General credentials (from first page of wizard):** Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers. Clear the check box to specify a new username and password for managing Active Directory sites.
  - **Credentials for synchronizing Active Directory information:** Specify a username and password to synchronize Active Directory sites. You must specify the same username and password that you specify here when the appliance prompts for credentials while synchronizing Active Directory sites.
  - **Use General synchronization interval (from first page of wizard):** Select this check box to use the same synchronization interval that you specified in the **Minimum Synchronization Interval** for synchronizing Active Directory sites.
  - **Minimum Synchronization interval:** The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the Active Directory sites.
  - **Manage Active Directory sites in:** Select a value from the drop-down list. You can choose to manage the Active Directory Site in either **Read-only** or **Read/Write** mode. For more information, see **bookmark2618 bookmark2618**
  - **Encryption:** You can encrypt the network traffic between the Grid member and the managed Microsoft server using SSL. Select a value. **None** or **SSL**, from the drop-down list. Infoblox strongly recommends that you select **SSL** from the drop-down list to ensure the security of all communications between the NIOS appliance and the Active Directory server. When you select **SSL**, the appliance automatically updates the TCP port to 636. When you select this option, you must specify the FQDN of the Microsoft server instead of the IP address and you must upload a CA certificate from the Active Directory server. Click **CA Certificates** to upload the certificate. In the **CA Certificates** dialog box, click the Add icon, and then navigate to the certificate to upload it.
  - **TCP port for LDAP connections:** The appliance displays the port number by default based on the encryption type that you select. When you select **None**, the appliance automatically updates the TCP port to 389.

5. Click **Next** and do the following in the Managed Servers table:
You cannot start or stop a DNS or DHCP service on a specific Microsoft server if you disable the monitor and control setting for the respective service. You can control and monitor DNS and DHCP services at the Grid level and override the settings at the Microsoft server level. Each monitor and control setting applies only to the DNS or DHCP service and the respective Microsoft server.

- **Name or IP Address**: Enter either the FQDN or IP address of the Microsoft server. In order for the member to resolve the FQDN of a Microsoft server, you must define a DNS resolver for the Grid member in the DNS Resolver tab of the Member Properties editor. Note that if the IP address of the Microsoft server is specified, then the DNS resolver must resolve it when the member and Microsoft server synchronize DHCP data only.
- **DNS Sync**: Select this option to enable the Grid member to manage the DNS service and synchronize DNS data with this server. Clearing this check box disables DNS service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.
- **DHCP Sync**: Select this option to manage the DHCP service of the Microsoft server and synchronize DHCP data with this server. Clearing this check box disables DHCP service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.
- **Active Directory Sites**: Select this option to manage Active Directory sites and synchronize Active Directory Sites and networks with the Grid.
- **DNS Monitor & Control**: Click **Override** to override the setting inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to enable monitoring and the ability to control DNS service for the Microsoft server. For more information, see Setting Grid Properties for Managing Microsoft Servers.
- **Synchronize DNS Reporting Data**: Click **Override** to override the settings that are inherited from the Grid. To retain the same settings as the Grid, click **Inherit**. Select this to synchronize DNS reporting data from the Microsoft server. For more information, see Synchronizing DNS Reporting Data.
- **DHCP Monitor & Control**: Click **Override** to override the setting inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to monitor and control DHCP service for the Microsoft server. For more information, see Setting Grid Properties for Managing Microsoft Servers.

**Note**: You cannot start or stop a DNS or DHCP service on a specific Microsoft server if you disable the monitor and control setting for the respective service. You can control and monitor DNS and DHCP services at the Grid level and override the settings at the Microsoft server level. Each monitor and control setting applies only to the DNS or DHCP service and the respective Microsoft server.

- **Synchronize Network Users**: Click **Override** to override the settings inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to enable the identity mapping for the Microsoft server. For information, see Enabling Identity Mapping.

You can assign multiple Microsoft servers to a Grid member and test their connection to the Grid member. Click the Add icon to add another Microsoft server.

6. Select a Microsoft server and click the Test Microsoft Server icon, or click the Action icon next to the respective Microsoft server and select Test Microsoft Server from the menu to verify whether the appliance can successfully connect to the Microsoft server. The appliance displays the test results in the Test Microsoft Server Results dialog box.

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

or

Click **Next**: Continue to the next step and define extensible attributes for the Microsoft servers. For information, see Using Extensible Attributes.

After you configure a Grid member to manage a Microsoft server, the member automatically connects to the Microsoft server and starts synchronizing data. You can then do the following:

- View the status of the servers in the Microsoft Servers panel, as described in Monitoring Managed Microsoft Servers. Newly added servers first display a status of Connecting as the Grid member contacts the Microsoft servers. The status changes to OK after the Grid member successfully connects to the Microsoft server.
- View the data synchronized from the Microsoft servers. To view DNS data, navigate to the DNS view you specified. For information, see Viewing Zones. To view DHCP data, navigate to the Networks tab of the network view that you specified. For information, see Managing IPv4 DHCP Data.

Network conditions and the amount of data can affect the synchronization time. Therefore, you might not be able to view all of the synchronized data immediately.

- Use Smart Folders to organize the Microsoft servers and their data. For example, you can create a folder for DNS zones and another folder for DHCP scopes synchronized from a Microsoft server. For information about Smart Folders, see Chapter 3, Smart Folders.
- Update the synchronized data. For information, see Chapter 35, Managing Microsoft DNS Services, and Chapter 36, Managing Microsoft DHCP Services.

You can also use Global Search to search for synchronized data, such as zones and IP addresses. For information, see Global Search.