DEPLOYMENT GUIDE

Enabling Microsoft AD Sites and Services

For NIOS 7.2 and above
Introduction

Infoblox enables network administrators to bi-directionally synchronize the Infoblox Grid™ with Microsoft Active Directory (AD) controllers. During the synchronization process, the administrator can enable either unidirectional (Read) or bi-directional (Read/Write) synchronization of Microsoft AD sites and subnets, which are directory objects to represent network topology. In a nutshell, Infoblox IP Address Management (IPAM) integration with Microsoft AD Sites and Services provides an administrator a real-time presentation of every subnet associated with each Microsoft AD site.

This document was prepared for NIOS 7.2, but this feature has been available since 7.0. (Screen captures may differ from release to release.). A super-user account is used on the Infoblox Grid side and an administrator account is used on Microsoft server side for sync.

What Is Microsoft AD Sites and Services?

A Microsoft AD site represents the physical structure, or topology, of a customer network. Active Directory uses topology information to build the most efficient replication topology.

Sites help optimizing replication using faster links. It also helps users logon to closest domain controllers instead of traversing slower links for authentication. This reduces logon time. Active Directory-enabled services can leverage site and subnet information to enable clients to locate the nearest server providers more easily.

Infoblox and Microsoft AD Sites and Services Features

The Infoblox and Microsoft AD Sites and Services integration enables the following functionality;

- Read-only or read/write privileges for Microsoft AD Sites and Services using the Infoblox Grid
- Auto-populate previously undiscovered subnets from Microsoft AD Sites and Services into Infoblox
- Move subnets between AD sites within Infoblox
- Create new AD sites within Infoblox
- Assign new subnets to AD sites within Infoblox
- View Microsoft Domain and AD site relationship
- Log AD site-specific data

Prerequisites

The following are prerequisites for the Microsoft AD Sites and Services integration with Infoblox;

- Functional Infoblox Grid with a Grid Master or standalone Infoblox member running NIOS 7.2
- To enable a Grid member to synchronize data with a Microsoft server and control DNS and DHCP services, on the Microsoft server:
  - Create a user account for the Grid member.
  - Grant the user account the necessary permissions.
- Microsoft Management license from Infoblox
  - For trial purposes, user can install 60 day temp license
Best Practices for Network Connectivity between Infoblox Grid and Microsoft Servers

To get the most from the Infoblox and Microsoft AD Sites and Services integration, we recommend the following best practices:

- A Grid Member configured to synchronize Active Directory Sites and Services of a Microsoft server uses system resources (CPU, memory, and network) directly proportional to the number of Microsoft Servers that are managed by the appliance. Infoblox recommends that the managing Grid member should not serve other protocols. It is also true for a Grid Master.

- The Grid member always initiates the connection to the Microsoft server. It is recommended that an encrypted LDAP connection be used between the Grid member and Microsoft server. The appliance displays a warning message when non-encrypted connection is used.

- Take the object count of MS objects to be synced into account when planning for object capacity for the synching IB member and the Grid.

- The managing member for data synchronization should be located “close” to the MS server being managed (RTT < 50 ms), to increase efficiency of the sync protocol. Maximum RTT must be < 200 ms.

- For redundancy: If there are more than one Microsoft domain controllers for a forest, then its best to manage all domain controllers for redundancy purposes. The Grid member managing Microsoft servers will be able to sync AD sites from the primary server, and in absence of that primary server, it will be able to sync data from other domain controllers.

Performance

The following table shows performance numbers for Infoblox Trinzic appliances:

<table>
<thead>
<tr>
<th>Appliance Model</th>
<th>MS Objects</th>
<th>MS Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-810</td>
<td>33k</td>
<td>5</td>
</tr>
<tr>
<td>TE-820</td>
<td>110k</td>
<td>20</td>
</tr>
<tr>
<td>TE-1410</td>
<td>440k</td>
<td>50</td>
</tr>
<tr>
<td>TE-1420</td>
<td>880k</td>
<td>75</td>
</tr>
<tr>
<td>TE-2210</td>
<td>880k</td>
<td>75</td>
</tr>
<tr>
<td>TE-2220</td>
<td>1.8m</td>
<td>100</td>
</tr>
<tr>
<td>TE-4010</td>
<td>4m</td>
<td>150</td>
</tr>
</tbody>
</table>

DISCLAIMER: The results in the table above were observed in an Infoblox lab environment, using Infoblox equipment, configuration, data, infrastructure, test tools, and methodology. Results and performance may vary under different conditions; Infoblox does not warrant that products will achieve the same performance in a different environment.
Deploying Microsoft AD Sites and Services

An administrator needs to enable the Microsoft AD Sites and Services feature within the Infoblox Grid for individual Microsoft servers. Once the sync is successful, the AD sites and associated subnets hosted on Microsoft servers can be viewed from within the Infoblox Grid. In order to push new AD sites and associated subnets from the Infoblox Grid to the Microsoft server, the sync must be configured for read/write privileges. In short, the Infoblox Grid provides administrators with the ability to push and pull AD site and subnet data to and from managed Microsoft servers.

Enabling AD Sites and Services Sync on a New Microsoft Server

This section describes the steps to configure a Microsoft AD Sites and Services sync on a new Microsoft server.

1. Go to Grid > Microsoft Servers > Servers, and click Add > Microsoft Server(s).

2. In the Add Microsoft Server(s) Wizard >Step 1 of 3 dialog box:
   a. Select the Active Directory Sites option in the Which features do you want to configure? section.
   b. Click the Select Member button to select a Managing Member from one of the available Infoblox appliances. (In this example, the infoblox.localdomain appliance.)
   c. Provide Administrator level permissions for the Microsoft Server to manage in the format domain\username, under Credentials to connect to the Microsoft server(s) section.
   d. Choose the Minimum synchronization interval (default is 2 minutes).
   e. Select the Logging level (default is Normal):
      - 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
f. Click **Next**.

3. In the Add Microsoft Server(s) Wizard >Step 2 of 4 dialog box:
   a. Select the checkbox **Use general credentials** (from the first page of the wizard).
   b. Accept the default for **Use general synchronization interval** (from Step 1 is 2 minutes) or modify it.
   c. Select a value from the **Manage Active Directory sites in** drop-down list. You can choose to manage the Active Directory Site in either **Read-only** or **Read/Write** mode
      - **Read-only**: Only able to pull AD Sites info from managed Microsoft servers
      - **Read/Write**: Able to pull and push AD Site data from and to managed Microsoft servers from within Infoblox Grid.
   d. **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 using SSL to ensure secure communication between Grid and managed Microsoft Servers. When an SSL option is selected, the appliance automatically updates the TCP port to 636. For this option to work:
      - You must specify the FQDN of the Microsoft server instead of the IP address.
      - You must upload a CA certificate from the AD 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.
      - When **None** is selected then TCP port for LDAP connections is set to 389.
   In either case, make sure that no firewall is blocking these LDAP ports or the synchronization will fail.
e. Click Next.

4. In the Add Microsoft Server(s) Wizard >Step 3 of 4 dialog box:
   a. Enter IP address of the Microsoft server to be managed under the Name or IP Address column.
   b. Select checkbox in the Active Directory Sites column.
   c. Verify the configuration by clicking the test button.
   d. Click Save & Close.
Adding AD Sites When Creating a New Network in Infoblox IPAM

The Infoblox and Microsoft AD Sites and Services integration provides a powerful capability of associating an AD site to a newly created network at the time the network is created. This saves a lot of overhead for network administrators, who no longer have to create IP networks in IPAM separately and associate them later with AD sites. This is all possible in one easy-to-follow workflow named Add IPv4 Network Wizard,

1. Go to Data Management > IPAM > Add > Network > IPv4.

2. Click Add Network > Manually.
3. Click Next.
4. Click the plus sign (+) and type a subnet value, such as 192.168.170.0 in the text box under Network, and click Next.

5. Click Next and click Next again.

6. In the Add Microsoft Server(s) Wizard >Step 4 of 6 dialog box:
   a. Select Assign these Active Directory Domains/Sites.
   b. Then select the desired Active Directory Domains and Active Directory Sites from left side and click Add move them to the rightmost list. In example below, ms.local domain and London site.
c. Click **Save & Close**.

7. To view the newly created network and its associated site, go to Data Management > IPAM.

![IPAM screenshot]

NOTE: To see the Microsoft-specific AD sites column, enable the column and it will display the title of the AD domain. The Sites column is not associated to the AD sites. In the Edit Columns dialog box shown below, contoso.com is the selected AD domain. Select the domain you configured.
<table>
<thead>
<tr>
<th>Column</th>
<th>Width</th>
<th>Sortable</th>
<th>Visible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>160</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IPAM Utilization</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Active Users</td>
<td>100</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>contoso.com</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Leaf Network</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Building</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>100</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Managing AD Sites

There is a broad capability to view, modify, and add AD Sites and subnets between the Infoblox Grid and managed Microsoft servers.

Viewing Active Directory Domains and Sites

An administrator can view AD domains and associated Sites and Subnets, pulled from the managed Microsoft servers, by following the steps below,

1. Go to Grid > Microsoft Servers > Active Directory Domains.

The Grid displays the following information:

- **Name**: The name of the Active Directory Domain; click on the name to view the Active Directory Sites below it
- **NetBIOS Name**: The name returned in the NetBIOS format
- **MS Sync Server**: The Microsoft synchronization server that is associated with the Active Directory Domain
- **Network View**: The network view that is associated with the Active Directory Domain

2. To view AD sites associated with an AD domain, click the domain name that is displayed as a hyperlink. The list of AD sites associated with that AD domain is displayed in Active Directory Domains Home. In this example, the ms.local link has been clicked.
3. To view the subnets associated with sites, click on the Gear icon next to a site, and click Edit. In this example, the subnet 192.168.156.0/24 is associated with the San-Francisco site.

4. Another way of viewing networks associated with AD sites is through Smart Folders. Go to Smart Folders > My Smart Folders > Active Directory Sites.

5. Click on the Active Directory Sites to expand it, and then click on any site to see networks associated with that site, in this example, Boston.
Creating a New Microsoft AD Site and Assigning a Network

NIOS provides the ability to create a new AD site and associate networks to it. This data then gets pushed out to the managed Microsoft server.

In this example a new site named Boston is created and it is assigned IP subnet 192.168.153.0/24.

1. Click on Grid > Microsoft Servers > Active Directory Domains > Add.

2. Click the plus sign (➕) to add a name for the site, for example Boston.
3. Click Next and select the Boston site in the Active Directory Sites column.

4. Click the plus sign (+) in the Network column to open the Network Selector window.
5. Select a network in the Networks list, such as 192.168.153.0/24, and click OK.

6. Click Save and Close.

7. Go to Data Management > IPAM to view the new site, Boston, next to the appropriate subnet, 192.168.153.0/24 in this example.
Adding Multiple Networks to an AD Site

The following procedure shows how to add multiple networks to an AD site.

1. Go to Grid > Microsoft Servers > Active Directory Domains.
2. Click on a Domain link, in this example contoso.com.
3. Click on the Gear icon next to the site, Boston, you want to add networks to, and click Edit.
4. Click the plus sign (+) to display the Network Selector, which displays a list of networks.
5. Choose all the networks to add to the selected site by pressing the Ctrl or command key, based on the OS, and selecting the desired networks. In this example, networks 40.40.1.0/24 and 50.50.1.0/24.

6. Click Save & Close.

Moving Networks between AD Sites

The ability to move networks between AD sites makes life easier for network administrators, as it gives them the ability to move networks from one AD site to another. This is required during a move of logical networks across physical boundaries, for example, when a company acquires a new building in a different location.

The following procedure makes a network part of a new AD site. In this example network 192.168.155.0/24 is being moved from London to San-Francisco.

1. Go to Grid > Microsoft Servers > Active Directory Domains.
2. Select the desired domain link, in this example, ms.local.
3. Click the Gear icon next to the site where networks will be moved from, in this example, London.

4. Click Move Networks.
5. Click **Select Site** next to the **Destination Active Directory Site** option.

6. In **Microsoft Sites Selector**, select a site from the list, in this example **San-Francisco**.

7. Select a network, in this example **192.168.155.0/24**.
8. Select Move.

Moving Multiple Networks to an Active Directory Site

An administrator can move multiple networks to an AD site in a single operation. In the example below, all networks are moved from Boston to Dallas in a single operation.

1. Go to Data Management > IPAM.

2. Select all the networks associated with Boston to be moved, and click Move Networks in the toolbar.

3. Click the Select Site button and choose Dallas to set Destination Active Directory Site to Dallas.

4. Click Move.
All moved networks are now associated with the Dallas site under IPAM as shown below.

Automating Networks as part of AD Sites Using Network Templates

One of the primary requests from network administrators is to automate network management as much as possible, specifically fully automated network creation. Infoblox NIOS provides several network templates to automate network management, one of which automates IPv4/IPv6 network creation—from subnet mask to managing members and creating reverse mapping zones to associate specific AD sites.

This example demonstrates this powerful capability by using a network template that makes all new networks part of the Boston AD site. First, create a network template that makes sure that each network created using the template will be part of the Boston site.

1. Click Data Management > DHCP > Templates > Add > Template > Network > IPv4 or IPv6. As shown in the figure below, the template is for IPv4 network creation.

2. In the Name field, type Boston-IPv4-template. Keep Netmask at /24 and click Next.

3. Click Next and click Next again.

4. Select either option for Assign these Active Directory Domains/Sites and select the desired domain name and site from that domain name, or you can select the option Assign the same domains/sites as the selected network and click Select network to select a network that is part of an AD site that we want the new networks to be part of.
NOTE: The second option will work only if there is already a network created with the target site you want to use.

In this example, since we want the template to make all new networks part of Boston site, Boston is selected as the AD site for the template using one of the two above options. There is a network 10.60.22.0/24 that is already part of Boston site.

5. Select Assign the same domains/sites as the selected network, click Select network, and select 10.60.22.0/24.

NIOS automatically populates the AD site table with the site of the network, in this case Boston.

6. Click Save & Close.

Now create a new network using the template created above.

7. Click Data Management > IPAM > Add > Network > IPv4 to start the Add IPv4 network wizard.

8. Select Add Network, and select the option Using a network template.

9. Click select template and select the desired template, in this example, Boston-IPv4-template, and click Next.
10. Click under the Networks field, click the plus sign (+) to add IPv4 networks, in this example, 192.168.198.0, 192.168.199.0, and 192.168.200.0.

The screen now looks like the one shown below.

![Add IPv4 Network Wizard Step 2 of 4](image)

11. Click Save & Close.

12. To verify the creation of new networks and the AD site they belong to, go to Data Management > IPAM.

![Data Management > IPAM](image)

All three newly created networks are automatically associated with the AD site Boston—the site was added because of the template used.