# infoblox.

DEPLOYMENT GUIDE

# **Enabling Microsoft AD Sites and Services**

# **Table of Contents**

Introduction	2
What Are Microsoft AD Sites and Services?	2
Infoblox and Microsoft AD Sites and Services Features	2
Prerequisites	3
Best Practices for Network Connectivity between Infoblox Grid and Microsoft Servers	3
Deploying Microsoft AD Sites and Services	4
Assigning Grid Members to Microsoft Servers	4
Setting Grid Properties for Managing Microsoft Servers	12
Adding AD Sites When Creating a New Network in Infoblox IPAM	14
Managing AD Sites	17
Viewing Active Directory Domains and Sites	17
Creating a New Microsoft AD Site and Assigning a Network	20
Adding Multiple Networks to an AD Site	24
Moving Networks between AD Sites	26
Moving Multiple Networks to an Active Directory Site	28
Automating Networks as part of AD Sites Using Network Templates	

# Introduction

Infoblox enables network administrators to bi-directionally synchronize the Infoblox Grid<sup>™</sup> 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. 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 8.5. (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 Are 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 optimize 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;

- Use Microsoft's Remote Procedure CAll (RPC) for agentless access to Active Directory information.
- 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
- Deleting 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 8.5 or later.
- To enable a Grid member to synchronize data with a Microsoft server and control DNS and DHCP services, on the Microsoft server:
  - $\circ~$  Create a user account for the Grid member.
  - Grant the user account the necessary permissions.
- Microsoft Management license from Infoblox
  - $\circ~$  For trial purposes, user can install 60 day temp license
- Current Microsoft Server Versions supported include 2008, 2008R2, 2012, and 2012R2, 2016, and 2019.

# 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 nor be 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 a 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 Master and Grid Master Candidate..
- 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
- If there are more than one Microsoft domain controllers for a forest, then it's 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.

## **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.

# Assigning Grid Members to Microsoft Servers

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

1. Navigate to Grid tab  $\rightarrow$  Microsoft Servers tab  $\rightarrow$  Servers tab.



2. Click on the '+' to bring up the 'Add' wizard.

Add Microsoft Serve	r(s) Wizard > Step 1 of 3	×
Select settings for al	the servers that you are currently adding	<b>8</b> «
Which features do you wa	ant to configure ?	
Network Users		
DNS and DHCP	Services	
Active Directory	Sites	
GENERAL SETTINGS		
Credentials to connect to the Microsoft server(s)	*Domain\username 🔳 Password 🖗	
Managing Member	None     Select Member	
* Minimum synchronization interval	2 minutes	
Cancel	Previous Next Save & Close	•

In 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. 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:
  - 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.

- 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.
- 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 of the next one is approximately seven minutes.
- 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.
- 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. When you select Syslog, NIOS logs the messages that are generated for the respective Microsoft server in the syslog. Comment: You can enter additional information about the servers.
- **Synchronize Data into Network View**: This field appears only when there is more than one network view in the grid. When there are multiple network views, you must specify to which network view the data from the Microsoft server is synchronized.
- **Synchronize DNS Data into DNS View**: This field appears only when there is more than one DNS view in the selected network view. You can select a different network view for the Microsoft server.
- **Disable Synchronization**: Select this to disable the Microsoft servers. This allows you to provision the Microsoft servers and then enable them at a later time.
- 3. Click Next.

4. If you have selected the Network Users check box, complete the following in the Select your across-server settings for Network Users page:

Add Microsoft Serve	er(s) Wizard > Step 2 of	f 6	×
Select your across-s	ork users	<b>?</b>	
Credentials for synchronizing network users	Domain\username Password		
🗸 Use general synchroni	zation interval (from first pag	je of wizard)	
*Minimum synchronization interval	2	minutes	
Cancel		Previous Next Save & Close	•

- **Use General credentials (from the 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.
- 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.

5. 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:

Add Microsoft Serve	er(s) Wizard > Step 3 of	6	×
Select your across-s	server settings for DNS Is (from first page of wizard)	and DHCP Services	<b>8</b> «
Credentials to connect to DNS and DHCP Services	Domain\username Password		
✓ Use general synchroni	ization interval (from first pag	e of wizard)	
* Minimum synchronization interval	2	minutes	
Manage DNS and DHCP services in	Read/Write		
Cancel		Previous Next	Save & Close 🔻

- **Use General credentials** (from the 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.

6. 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:

Add Microsoft Server(s) Wizard > Step 4 of 6					
Select your across-s	erver settings for Active	Directory Sites			8
🗸 Use general credential	s (from first page of wizard)				
Credentials for synchronizing Active	Domain\username				
Directory information	Password				
🗸 Use general synchroni:	zation interval (from first page	e of wizard)			
* Minimum synchronization interval	2	minutes			
Manage Active Directory sites in	Read/Write				
Encryption	None				
*TCP port for LDAP connections:	389				
Cancel		Previous	ext	(	Save & Close 🔹

- **Use General credentials** (from the 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.

- 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.

A	Add Microsoft Server(s) Wizard > Step 5 of 6						×		
M	ANAGED SERVERS								<b>8</b> «
							-	-   🖺   💼	
E	Name or IP Address	DNS Sync	DHCP Sync	Active Dir	DNS Monitor & C	ontrol	Synchronize DNS	Reporting Data	
	10.34.98.31		<b>V</b>		Inherited from Grid	Override	Inherited from Grid	Override	
	Cancel		ſ	Previous	Next			Save & Close	•

7. Click Next and do the following in the Managed Servers table:

 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.
- 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.

Note that synchronization of DNS reporting data is effective only when the DNS Sync option is enabled for the Microsoft server.

- **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.
- 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. Click Save and Close.
- 8. After about 5 minutes, you should see the following:

Infoblox 📚		Dashboards	Data Mana	gement	Smart Folders	Grid	Administration					Q Sean	sh adr	nin -
		Grid Manager	Upgrade	Licenses	B HSM Group	Micro	osoft Servers							
Finder	~	Servers	Active Directory	/ Domains									4	£ 6
Smart Folders	+	Microsof	t Servers	я									_ 8	
Bookmarks	+	Quick Filter	None	•	Off Filter On	Show I	Filter							
Recycle Bin	+	+1011	<b>0 -   ≔   E</b>		. e						Go to	Go		
🔚 URL Links	+		Name		Status 🔺		Last Changed	Version	DNS	DHCP	IP Address	Comment		
		E =	win-5dcblgu6li	h.ad-32.loca	Running		2021-03-09 21:43:09 P	Windows Server 2016/2019 Datacenter 10	.0	-	10.34.98.32			
		E =	win-5dcblgu6li	h.ad-33.loca	Running		2021-03-09 22:25:39 P	Windows Server 2016/2019 Datacenter 10	.0		10.34.98.33			
		=	win-5dcblgu6li	h	Running		2021-03-09 23:35:11 PST	Windows Server 2016/2019 Datacenter 10	.0 📕	-	10.34.98.34			
			win-5dcblgu6li	h.ad-31.loca	Running		2021-03-10 16:28:24 P	Windows Server 2016/2019 Datacenter 10	.0		10.34.98.31			

Note the bottom entry.

9. Save the configuration and click Restart if the Restart banner appears at the top of the screen.

### **Setting Grid Properties for Managing Microsoft Servers**

To configure Grid properties for managing Microsoft servers, complete the following:

 Grid: From the Grid tab → Grid Manager tab, expand the Toolbar and click Grid Properties → Edit. Select Microsoft Integration tab in the Grid Properties Editor wizard.

Infoblox (Grid Properties	Editor)	×
Toggle Basic Mode	Basic Advanced	8
General CSP Config Security Password • Proxy Settings DNS Resolver	GENERAL Logging output destination	_ «
Monitoring Syslog Backup SNMP • SNMP Threshold • Notification	NETWORK USERS         Assumed Network Users       2         Hours       •         Synchronize Network Users with all MS servers       Before synchronizing with Microsoft servers, enable the Network Users feature in the General -> Advanced tab of the Grid Properties Editor.	
Email LOM NAT Groups • Object Change Tracking • Microsoft Integration Extensible Attribute Inheritance	MICROSOFT DNS AND DHCP SERVICES Ø Monitor and control DNS Services Synchronize DNS Reporting Data Ø Monitor and control DHCP Services	
Cancel	Save & Close	•

Complete the following in the Basic tab:

- 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. When you select Syslog, NIOS logs the messages that are generated for the respective Microsoft server in the syslog.
- Network Users
  - You can control the network users tab in the Data Management → Network Users screen. You can set the time from minutes to hours to days. Enable Synchronize Network Users with all MS Servers to ensure the Network Users screen is populated
- Monitor DNS and DHCP Services: You can enable monitoring and control services for DNS and DHCP services at the Grid level and override the settings for each service at the Microsoft

server level. This is enabled, by default. Each monitoring and control setting applies only to the corresponding service and is applicable to the respective Microsoft server only.

- Monitor and control DNS Services: Select this to enable monitoring and the ability to control DNS service for the Microsoft server.
- Synchronize DNS Reporting Data: Select this to synchronize DNS reporting data from the Microsoft server. Clearing this check box disables DNS reporting data synchronization.
- Monitor and control DHCP Services: Select this to enable monitoring and the ability to control a DHCP service for the Microsoft server.
- 2. Optionally, select the Microsoft Server Settings tab in the Grid Properties Editor wizard and complete the following in the Advanced tab or click the Advanced tab in the General tab in a Microsoft server editor:

Infoblox (Grid Properties	Editor)		×
Toggle Basic Mode	Basic Advance	1	8
General CSP Config Security	GENERAL		
Password	*Maximum simultaneous connections	5	
<ul> <li>Proxy Settings</li> <li>DNS Resolver</li> </ul>	*RPC timeout	10 Seconds	
Monitoring			
Syslog Backup	DNS AND DHCP SERVICE	38	
SNMP SNMP Threshold	Allow invalid MAC addresses to be	٥	
<ul> <li>Notification</li> <li>Email</li> </ul>	synchronized		
LOM	ACTIVE DIRECTORY SITI	is	
NAT Groups     Object Change Tracking	*LDAP timeout	10 Seconds	
Microsoft Integration	*Defeuit ID eite link		
Extensible Attribute Inheritance	"Default IP SITE IINK	DEFAULTIPSITELINK	
Cancel		Save & Close	

- Maximum simultaneous connections: Specify a maximum number of simultaneous RPC connections that can be configured for the respective Microsoft server, which are managed by the Grid. The default is five. You can specify a value between two and 40.
   RPC timeout: Specify the RPC timeout value in seconds to control the network communication timeout. The default is ten seconds. You can specify a value between one and 60.
- Allow Invalid MAC Address to be synchronized: This is enabled, by default. Select this to enable synchronization for invalid MAC addresses.

- **LDAP timeout**: Specify the LDAP connection timeout value. The default is 10 seconds. You can specify a value between one and 60 seconds.
- Default IP site link: Specify the default IP site link in the form of a string. The appliance does not validate it against the Windows server during configuration. The appliance displays an error message during synchronization if the site link for IP does not match the configured name on the Windows server.
- 3. Save the configuration.

# 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. Navigate to Data Management  $\rightarrow$  IPAM

Infoblox 📚	Dashboards Data Management	Smart Folders Reporting Grid Administr	ration Q Search admin <del>-</del>
	IPAM VLANs Super Host	Devices Network Users DHCP DNS File	e Distribution Security Threat Analytics
Finder 《	default Network View 👥		Toolbar 🔊 😵
Smart Folders	Quick Filter None	Off Filter On Show Filter Toggle flat view	+ Add +
Bookmarks +			IPv4 Network
👼 Recycle Bin 🕂		Go to	IPv6 Range
	Network A	Comment IPAM Utilization Active Users	Di Host
	10.1.0.0/16	1.0% 0	IPv4 Reservation
	10.60.16.0/24	1.1% 0	A Pagard
	10.60.30.0/24	0.3% 0	PTR Record
	10.63.128.0/24	0.7% 0	AAAA Record
	10.66.72.0/24	1.1% 0	>< Join
	10.66.102.0/24	0.3% 0	Q vDiscovery →
	198.18.0.0/16	100.0% 1	<ul> <li>Discovery Status</li> <li>Discovery</li> </ul>
https://10.63.128.20/ui/oPal.4_x8p534/iccoopal/00			Diagnostic     Discover Now

2. Click  $Add \rightarrow Network \rightarrow IPv4$ .

#### 3. Click Add Network $\rightarrow$ Manually

Add IPv4 Network Wizard > Step 1 of 9			×
<ul> <li>Add Network</li> </ul>			8
<ul> <li>Manually</li> </ul>			
<ul> <li>Using a network template</li> </ul>	Select Template		
Add Network Container			
Cancel _x8o53MkgceogNGPg/gRe69/ceo6c#	Next	Schedule for Later Save & C	Close -

- 4. Click Next.
- 5. Click the plus sign (+) and type a subnet value, such as 192.168.170.0 in the text box under Networks, and click **Next**

Add IPv4 Netw	vork Wizard > Step 2 of 9	×
*Netmask	/24       255.255.255.0         1       4       8       12       16       20       24       28       32	<b>?</b> «
* Networks	<b>+</b>   <b>+</b> ,   面	
	Network	
	▼ 192.168.170.0	
Comment		
	Automatically Create Reverse-Mapping Zone	
	Disable for DHCP	
Cancel	Previous         Next         Schedule for Later         Save & C	lose 🔻

6. Click **Next** and click **Next** again.

- 7. In the Add Microsoft Server(s) Wizard  $\rightarrow$  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 the left side and click **Add** to move them to the rightmost list. In the example below, testlab.com domain and London site.
  - c. Click Save & Close.

Add IPv4 Network Wizard > Step 4 of	Add IPv4 Network Wizard > Step 4 of 10					
No Active Directory Site	O No Active Directory Site					
<ul> <li>Assign these Active Directory Domains/Sites</li> </ul>						
Assign the same Domains/Sites as the selec	ted network Select Network					
Go	Go					
Active Directory Read only	Active Directory Sites		Active Directory	Site		
testlab.com No	Dallas		testlab.com	London		
	Default-First-Site-Name	Add >				
	London	<< Remove all				
	San-Francisco					
Cancel	Previous		Schedule for Later	Save & Close	•	

8. To view the newly created network and its associated site, go to **Data Management**  $\rightarrow$  **IPAM**.

Dashboards	Data Management	Smart Folders	Reporting Gric	Administration
IPAM VL	ANs Super Host	Devices Networl	Users DHCP	DNS File Distribution
default	Network View 📘			
Quick Filter	None 🔽	Off Filter On	Show Filter	Toggle flat view
→   <b>+</b> •	☑   亩 -   ⊕   1	•   🖨	Go to	Go
	Network 🔺	Comment	IPAM Utilization	testlab.com
	<b>+</b> 192.168.70.0/24		0.0%	London

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 with the AD sites. In the Edit Columns dialog box shown below, testlab.com is the selected AD domain. Select the domain you configured.

Edit Columns				×
Column		Width	Sorta	Visible
Network		160	Yes	<b>V</b>
Comment		100	Yes	
IPAM Utilization		100	Yes	<b>V</b>
testlab.com		100	Yes	<b>V</b>
Active Users		100	No	
Disabled		100	Yes	
Leaf Network		100	Yes	
Discovery Enabled		110	Yes	
Managed		100	Yes	
First Discovered		100	Yes	
Last Discovered		100	Yes	
Discover Now		100	No	
	Apply	Cancel	Re	set

#### **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  $\rightarrow$  Microsoft Servers  $\rightarrow$  Active Directory Domains

lr	lfob	lox 📚	Dashboard	s Data Manag	gement	Smart Folders	Reporting	Grid	Administration			
			Grid Manag	er Upgrade	Licenses	s HSM Group	Microsoft S	Servers	Device Support	Ecosystem		
	Se	rvers Active Di	rectory Domains							Toolbar	≫	<b>?</b> «
	Note	e: Only the root Activ	ve Directory Domains	are synchronized						E Permissions		
	Qui	ck Filter None	▼ Of	Filter On S	Show Filter							
	1	- ⊖					Go to		••• Go			
		Name	NetBIOS Name	MS Sync Server	Network	View						
		testlab.com	TESTLAB	198.18.200.110	default							

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 testlab.com link has been clicked

h	nfoblox 📚	Dashboards	Data Managemer	t Smart Folders	Reporting	Grid	Administrat	ion
		Grid Manager	Upgrade Lic	enses HSM Group	Microsoft	Servers	Device Suppo	ort E
	Servers Active Direct	tory Domains			_			
//	Active Directory Domains Ho testlab.com Activ	ome ve Directory Domain	P					
	Quick Filter None	✓ Off Filt	ter On Show F	ilter				
	+   2    🗰    💠    🛓	.   🖶			Go to		•••	Go
	🔲 📃 🛛 Name							
	🔲 📃 🛛 Dallas							
	Default-Firs	t-Site-Name						
	E London							
	San-Francis	300						

3. To view the subnets associated with sites, click on the hamburger 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

San-Francisco (Active	e Directory Site Properties)		×
*Name • A site name can contain u	San-Francisco		<b>?</b> «
Note that you cannot use	the following characters in the site name: . {   } ~ [ ] ' ; ; <=>? @ ! " # \$ % ^ &` ( ) + / , *		
Active Directory domain: tes	stlab.com	<b>∔</b>   m	
Address		• • •	
192.168.156.0/24			

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

Infoblox 📚	Dashboards Data Management Smart Folders Reporting Grid Administration	
	My Smart Folders Global Smart Folders	
Finder 《	My Smart Folders > Create	Toolbar 📎 🕄
Smart Folders	Go to Go	→ Open
Active Directory Sites	Name	🗹 Edit
Default-First-Site-Name	Reference of the second	Extensible Attributes
London	Range Apple Mac OS Devices	Permissions
Apple Mac OS Devices	Conflicts	C Restart Services
Conflicts	Discovered Switches/Rout	→ IDN Converter
Gaming Console Devices	Raming Console Devices	
Microsoft Windows Devices     Reclaimable Records	Reference Microsoft Windows Device	
Router and Wireless Access	Reclaimable Records	
Bookmarks +	Router and Wireless Acce	
🐻 Recycle Bin 🕂		
URL Links +		

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, London

Infoblox 📚	Dashboards Data Management	London (Active Directory Site Properties)	×
	My Smart Folders Global Smart Folde	*Name London	0
Finder Smart Folders Active Directory Sites Dallas Default-First-Site-Name London San-Francisco Conflicts Conflicts Conflicts Reclaimable Records Reclaimable Records Reclaimable Records Router and Wireless Access Bookmarks +	My Smart Folders > Go to Contract Cont	<ul> <li>A site name can contain up to 63 bytes, which can be translated to a maximum of 63 ASCII characters.</li> <li>For UTF-8 characters, the maximum varies depending on the characters entered.</li> <li>Note that you cannot use the following characters in the site name: .{I}~[]':;&lt;=&gt;? @ !" # \$% ^&amp; `()+/,*</li> <li>Active Directory domain: testlab.com</li> <li>Networks • • • • • • • • • • • • • • • • • • •</li></ul>	×
Recycle Bin +		Cancel Save an	d Close

#### 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  $\rightarrow$  Microsoft Servers  $\rightarrow$  Active Directory Domains  $\rightarrow$  Add

Create 1 or more Active Directory sites	<b>?</b> «
Active Directory domain: testlab.com	
Active Directory sites (0 items)	+   亩
Name	
<ul> <li>A site name can contain up to 63 bytes, which can be translated to a maximum of 63 ASCII characters.</li> <li>For UTF-8 characters, the maximum varies depending on the characters entered.</li> <li>Note that you cannot use the following characters in the site area cannot up to 100 millions.</li> </ul>	
Cancel     Previous	Save and Close -

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

Add networks to your new sites (optional)		<b>?</b> «
Active Directory domain: testlab.com		
Active Directory sites (1 items)	Networks to be added to: Boston	
Name Boston	Address	
Cancel	Next Save and Close   -	

4. Click the plus sign (+) in the Network column to open the Network Selector window

Network Selector			×
All Networks	<b>+</b> 10.1.3.0/24		<b>?</b> «
Conflicts     Discovered Switches/Re	++ 10.60.16.0/24 ++ 10.60.30.0/24		
Gaming Console Device     Microsoft Windows Dev     Beclaimable Becords	<b>+</b> 10.63.128.0/24		
Router and Wireless Ac	<b>+</b> 10.66.102.0/24		
Smartphone, PDA, Tabl	++ 192.168.70.0/24 ++ 192.168.153.0/24	London	
	<b>+</b> 192.168.156.0/24	San-Francisco	
Close		[	ОК

5. Select a network in the Networks list, such as 192.168.153.0/24, and click **OK**.

New Active Directory Sites		×
Add networks to your new sites (optional) Active Directory domain: testlab.com		<b>?</b> «
Active Directory sites (1 items)	Networks to be added to: Boston Networks	
Boston	192.168.153.0/24	
Cancel	Next Save and Close -	

- 6. Click Save and Close.
- 7. Go to **Data Management**  $\rightarrow$  **IPAM** to view the new site, Boston, next to the appropriate subnet, 192.168.153.0/24 in this example

Dashboards Data Management		Smart Folders	Reporting	g Grid	Administ	ration			
IPAM VLA	ANs Super Host	Devices Ne	twork Users	DHCP	DNS Fil	e Distribution			
default	Network View								
Quick Filter	Quick Filter         None         Image: Toggle flat view								
→   + •	☑   亩 -   �   1	•   🖶	Go to			Go			
	Network 🔺	Comment	IPAM	Utilization	testlab.com				
	<b>+</b> 10.66.102.0/24	· · · · · · · · · · · · · · · · · · ·		0.3%					
	┿ 192.168.70.0/24			0.0%	London				
	<b>+</b> 192.168.153.0/24			0.0%	Boston				
	<b>+</b> 192.168.156.0/24			0.0%	San-Francisc	:0			

#### Adding Multiple Networks to an AD Site

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

- 1. Go to Grid  $\rightarrow$  Microsoft Servers  $\rightarrow$  Active Directory Domains.
- 2. Click on a Domain link, in this example testlab.com.

Infoblox 📚	Dashboards	Data Manag	ement	Smart Folders	Reporting	Grid	Administration			
	Grid Manager	Upgrade	Licenses	HSM Group	Microsoft	Servers	Device Support	Ecosystem		
Servers Active Directory	Domains							Toolbar	≫	<b>3</b> «
Active Directory Domains Home testlab.com Active I	Active Directory Domains Home testlab.com Active Directory Domain							+ Add		
Quick Filter None	Quick Filter None V Off Filter On Show Filter						Delete     Move Networks			
+   🗹   💼   💠   ᆂ	0				Go to		Go	→ IDN Converter		
🔲 📃 Name										
📝 📃 Boston										

3. Click on the hamburger icon next to the site, Boston, you want to add networks to, and click Edit

Boston (Active Direc	tory Site Properties)	×
*Name	Boston	<b>?</b>
<ul> <li>A site name can contain</li> <li>For UTF-8 characters, th</li> <li>Note that you cannot use</li> </ul>	up to 63 bytes, which can be translated to a maximum of 63 ASCII characters. le maximum varies depending on the characters entered. e the following characters in the site name: . {   } ~ [ ] ' : ; <=> ? @ ! " # \$ % ^ & ` ( ) + / , *	
Active Directory domain: te	estlab.com	
Networks	+ 1 🖮	
Address		
192.168.153.0/24		
Cancel	Save and Close -	

4. Click the plus sign (+) to display the Network Selector which displays a list of networks.

Network Selector						×
All Networks	Off Filter On	Show Filter				<b>?</b> «
Apple Mac OS Devices	Find		Go		$\rightarrow$	
Conflicts     Discovered Switches/R	Network 🔺	Comment	testlab	.com		
Gaming Console Device     Microsoft Windows Dev	<b>a</b> 10.1.0.0/16					
Reclaimable Records	<b>#</b> 10.1.1.0/24					
••••••••••••••••••••••••••••••••••••••	<b>+</b> 10.1.2.0/24					
Smartphone, PDA, Tabl	<b>+</b> 10.1.3.0/24					-
	<b>+</b> 10.60.16.0/24					-
	<b>+</b> 10.60.30.0/24					-
	<b>+</b> 10.63.128.0/24					_
Close					O	<

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 10.1.1.0/24 and 10.1.2.0/24

Boston (Active Direc	ctory Site Properties)	×
*Name <ul> <li>A site name can contain</li> <li>For UTF-8 characters, the Note that you cannot us</li> </ul>	Boston up to 63 bytes, which can be translated to a maximum of 63 ASCII characters. The maximum varies depending on the characters entered. The the following characters in the site name: $\{1\} \sim [1':; <=>? @ !! # $ % ^ &` () + /, *$	<b>?</b>
Active Directory domain: t	estlab.com	
Networks	+ 1 🗰	
Address		
192.168.153.0/24		
10.1.1.0/24		
10.1.2.0/24		
Cancel	Save and Close -	

#### 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  $\rightarrow$  Microsoft Servers  $\rightarrow$  Active Directory Domains.
- 2. Select the desired domain link, in this example, testlab.com.
- 3. Click the hamburger icon next to the site where networks will be moved from, in this example,

lr	nfoblox 📚		Dashboards	Data Manage	ement Sn				
			Grid Manager	Upgrade	Licenses				
× •	Servers	Active Directory	Domains						
Active Directory Domains Home testlab.com Active Directory Domain									
	Quick Filter	lone	• Off Filter	On St	now Filter				
	+   🗹   🖬	ī   <b>⊕   <u>\$</u>    </b>	₽						
		Name							
		Boston							
		Dallas							
		Default-First-Site	e-Name						
		London							
		San-Francisco							

4. Click Move Networks

Infoblox 📚			Dashboards	Data Management		mart F				
			Grid Manager	Upgrade	Licenses	HS				
<b>1</b>	Servers	Active Directory I	Domains							
	Active Directory	Domains Home Active Di	rectory Domain 🗜	l						
	Quick Filter None									
	+   🗹   🖬	ĭ   ⊕   <b>1</b>   {	€							
		Name								
		Boston								
		Dallas								
		Editault-First-Site	e-Name							
		Delete								
		Move Networks								

5. Click Select Site next to the Destination Active Directory Site option

		×
Select Site		<b>?</b> «
Go		♣
	Sites	
	testlab.com\London	
		Move
	Select Site	Select Site         Go         Sites         testlab.com\London

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

Move Networks			×
*Destination Active Directory Site	San-Francisco	Select Site	<b>?</b> «
*Networks Go to	Go		<b>∔</b> ∣
Network		Sites	
192.168.70.0/24		testlab.com\London	
Close			Move

- 7. Select a network, in this example 192.168.70.0/24
- 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 $\rightarrow$ IPAM

Infoblox 📚 Dashboards Data Management Smart Folders Reporting Grid Administration		
IPAM VLANs Super Host Devices Network Users DHCP DNS File Distribution	Security Threat Analyt	tics
s default Network View R	olbar >	» 8 «
Quick Filter None 🔄 Off Filter On Show Filter 🏣 Toggle flat view	Add 🗸	
$\Rightarrow   + \cdot   @   = \cdot   +   +   +   +   +   +   +   +   +  $	Open Edit	
Image: Network *         Comment         IPAM Utilization         testlab.com	Lease Details	
	Extensible Attributes	
☑	Permissions	
□ = + 192.168.153.0/24       0.0%     Boston	Move Networks     Resize	
☑	> Split	
□ = m 198.18.0.0/16 100.0%	vDiscoverv	
	Discovery Status	
	Discovery Diagnostic	

- 2. Select all the networks associated with London 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

Move Networks			×
*Destination Active Date Date Date Date Date Date Date Dat	allas Select Site		<b>8</b> «
*Networks Go to	Go	+   💼	
Network		Sites	
192.168.70.0/24		testlab.com\London	
192.168.156.0/24		testlab.com\London	
Close		Move	

#### 4. Click Move

All moved networks are now associated with the Dallas site under IPAM as shown below

nfoblox 📚	Dashboards	Data Management	Smart Folders	Reporting	g Grid	Adm	inistration			
		ANs Super Host	Devices Net	work Users	DHCP	DNS	File Distribution	Security	Threat Analytic	cs
default	Network View							Toolbar	»	• • •
 Quick Filter	None off	Filter On Show F	ilter 🔚 Toggle	flat view				🕂 Add	•	
→   + •	☑   亩 -   ⊕   土 -   €	•		Go to			Go	→ Open ☑ Edit		
	Network 🔺	Comment IPAM	I Utilization tes	tlab.com				E Lease Detai	ils	
	<b>+</b> 10.66.102.0/24		0.3%					Extensible Attributes	Ť	
	<b>+</b> 192.168.70.0/24		0.0% Dal	las				E Permissions	5.00 	
	<b>+</b> 192.168.153.0/24		0.0% Bos	ston				Hove Netwo	orks	
	<b>+</b> 192.168.156.0/24		0.0% Dal	las				Split		

#### 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  $\rightarrow$  DHCP  $\rightarrow$  Templates
- 2. Click Add button → Template → IPv4 Network Template or IPv6 Network Template. As shown in the figure below, the template is for IPv4 network creation.

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

Add IPv4 Network Template Wizard > Step 1 of 6							
*Name	lame Boston-IPv4-Template						
Netmask	• Fixed						
	1 4 8 12 16 20 24 28 32 						
	Allow User to Specify Netmask						
Comment							
Automatically Create Reverse-mapping Zones							
Cancel	Previous Next Save & Close	•					

- 4. Click Next and click Next again
- 5. 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 the 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 the Boston site.

6. 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

Add IPv4 Network Template Wizard > Step 3 of 6						
No Active Directory Site						
Assign these Active Directory Domains/Sites						
• Assign the same Domains/Sites as the selected network 10.1.1.0/24 Select Network						
Go	Go					
Active Directory Read only	Active Directory Sites		Active Directory			
testlab.com No	Boston		testlab.com			
	Dallas	Add >				
	Default-First-Site-Name	< Remove all				
	London					
	San-Francisco					
Cancel	Previous Next		Save & Close -			

7. Click Save & Close.

Now create a new network using the template created above

- 8. Click Data Management  $\rightarrow$  IPAM
- 9. Click Add Button  $\rightarrow$  Network  $\rightarrow$  IPv4 to start the Add IPv4 network wizard.
- 10. Select Add Network, and select the option Using a network template.
- 11. Click **select template** and select the desired template, in this example, Boston-IPv4-template, and click Next
- 12. 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 6			
*Netmask	1       4       8       12       16       20       24       28       32         1	<b>?</b> «	
* Networks	+ + + =		
	Network		
	192.168.198.0		
	192.168.199.0		
	192.168.200.0		
Comment	Automatically Create Reverse-Mapping Zone		
Cancel	Previous Next Schedule for Later Save & Clu	ose 🔻	

- 13. Click Save & Close.
- 14. To verify the creation of new networks and the AD site they belong to, go to **Data Management**  $\rightarrow$  **IPAM**

l	nfoblox 📚	Dashboards	Data Managen	nent Smart Fo	olders Reporti	ng Grid	Administration		
		IPAM	/LANs Super Ho	st Devices	Network Users	DHCP	DNS File Distribution	Security	Threat Analytics
	default	Network View						Toolbar	» 3
"	Quick Filter	None 🔽 🛛 o	ff Filter On S	how Filter	Toggle flat view			🕂 Add	
	→   <b>+</b> •	☞   亩 -   �   ♣ -	0		Go to		Go	→ Open ☑ Edit	
		Network 🔺	Comment	IPAM Utilization	testlab.com			E Lease Details	
		<b>+</b> 192.168.70.0/24		0.0%	Dallas			<ul> <li>Delete</li> <li>Extensible</li> <li>Attributes</li> </ul>	*
		┿ 192.168.153.0/24		0.0%	Boston			E Permissions	
		<b>+</b> 192.168.156.0/24		0.0%	Dallas			Move Network	s
		<b>+</b> 192.168.198.0/24		0.0%	Boston			Split	
		<b>+</b> 192.168.199.0/24		0.0%	Boston			X Join	
		<b>+</b> 192.168.200.0/24		0.0%	Boston			Q vDiscovery	-
		i98.18.0.0/16		100.0%				<ul> <li>Discovery Stat</li> <li>Discovery</li> </ul>	tus
		N B						Diagnostic	

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

# infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054 +1.408.986.4000 www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).