DEPLOYMENT GUIDE

Enabling Infoblox Identity Mapping with Microsoft Active Directory
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>How Infoblox Gets User Information</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>3</td>
</tr>
<tr>
<td>Best Practices</td>
<td>4</td>
</tr>
<tr>
<td>Performance</td>
<td>4</td>
</tr>
<tr>
<td>Deploying Identity Mapping</td>
<td>4</td>
</tr>
<tr>
<td>Enabling Identity Mapping</td>
<td>4</td>
</tr>
<tr>
<td>Viewing User Data</td>
<td>5</td>
</tr>
<tr>
<td>Active Users</td>
<td>6</td>
</tr>
<tr>
<td>User Login History</td>
<td>7</td>
</tr>
<tr>
<td>Search Filters</td>
<td>7</td>
</tr>
<tr>
<td>User Session</td>
<td>8</td>
</tr>
<tr>
<td>Microsoft Events</td>
<td>9</td>
</tr>
<tr>
<td>Dashboard Widget</td>
<td>9</td>
</tr>
<tr>
<td>Reporting</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

Infoblox Identity Mapping enables the correlation of DNS, DHCP, and IPAM (DDI) data to identity information contained in authentication systems. This guide describes how to enable Identity Mapping on an Infoblox appliance running NIOS to provide Microsoft Active Directory (AD) domain user information when the appliance is connected to a Microsoft domain controller. By enabling this feature, an IT administrator can monitor Active Directory domain users by viewing their IP address, login status, and the duration of their current status.

How Infoblox Gets User Information

Infoblox Identity Mapping relies on live event logs, which are available on Microsoft servers. Upon enabling the Identity Mapping feature, the appliance communicates with Microsoft servers to pull event logs. NOTE: The user information displayed is only as accurate as the Microsoft event logs.

Prerequisites

The following are prerequisites for Infoblox Identity Mapping:

- Functional 7.2 Infoblox Grid with a Grid Master
- Active Grid license
- Infoblox Managed Microsoft Servers Event logs enabled on the Microsoft servers

Best Practices

To get the most from Infoblox Identity Mapping, we recommend the following best practices:

- Install a Microsoft management license on the Grid and sync DHCP and DNS services on Microsoft servers.
- Choose and sync Microsoft servers that handle large quantities of authentications, domain controllers, Exchange servers, etc.
  NOTE: Identity Mapping doesn’t require the Microsoft server to run DNS or DHCP in order to gather authentication information.
- Members running Identity Mapping will run processes that share resources with other Microsoft DNS/DHCP/AD site synchronization if configured. So the best practice is NOT to provide any protocol on the members running Microsoft AD user management.
- Any Microsoft server responsible for a large number of domain authentications can be configured. Suggested targets are the Microsoft Exchange server, Microsoft domain controller, SharePoint servers, and IIS servers to sync the user information.
- A Microsoft user that belongs to a Domain User group and Event Log Reader group should at a minimum be used to start a session between the Infoblox Grid and Microsoft servers to obtain network user information
- TE-14XX and above can be used as an Infoblox appliance for this feature, although the number of users per Grid member vary with the appliance model
- Avoid using a Grid Master to perform the Identity Mapping sync.
- Take into consideration that a Grid member will perform additional work to process sync data from members; so upsize appropriately.
**Performance**

The following table shows performance numbers for Infoblox Trinzic appliances:

<table>
<thead>
<tr>
<th>Appliance Model</th>
<th>Users per Microsoft Member</th>
<th># of Auth. Log Events Retained</th>
<th># of Microsoft Servers</th>
<th># of Days Data Retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-1410</td>
<td>2,000</td>
<td>80,000</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>TE-1420</td>
<td>3,000</td>
<td>120,000</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>TE-2210</td>
<td>3,000</td>
<td>120,000</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>TE-2220</td>
<td>4,000</td>
<td>160,000</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>TE-4010</td>
<td>6,000</td>
<td>240,000</td>
<td>150</td>
<td></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 Identity Mapping**

The following steps are required to enable identity mapping feature and view user data on the NIOS appliance:

- Enable Identity Mapping on the Grid.
- View user data from Microsoft servers.

**Enabling Identity Mapping**

This section describes enable Identity Mapping on the Grid.

1. Go to Grid > Grid Manager > Members.

2. Select the Grid Properties > Edit from the toolbar.

3. Select the Microsoft Integration tab in the Grid Properties Editor and ensure that Advance mode is on.
4. Select the **Enable network users feature** and **Synchronize network users with all MS Servers**.

![Enable network users feature and Synchronize network users with all MS Servers](image)

5. Click **Save & Close** to save the configuration.

Identity Mapping does not require a MS_MANAGEMENT license to operate. With NIOS 7.2, you can add a Microsoft server even without having a MS_MANAGEMENT license. However, you cannot configure DNS, DHCP, and Microsoft AD Sites synchronization unless a MS_MANAGEMENT license is installed. Without a MS_MANAGEMENT license, only Microsoft AD user configuration settings are displayed in UI and only those configurations are allowed from the UI and PAPI.

**Viewing User Data**

After enabling Infoblox Identity Mapping as described above, an administrator can view all the active users currently logged into the Microsoft AD domain services as well as user login history.

**Active Users**

To view active users, go to **Data Management > Network Users > Active Users**.
The **Active Users** tab shows the following Network User objects:

- **User Name**—The name of the user logged into the Microsoft server as a user or as a service
- **Domain**—The domain name on Microsoft server that the user is logged into
- **First Seen**—The time the user first logged into the domain
- **IP Address**—The IP address of the user machine the user logged into
- **Data Source**—The IP address of the Microsoft server reporting user login
- **Last Seen**—The time the user was last seen active by the sync process
- **Last Updated**—The time of last sync

The times are displayed in the time one configured for the Infoblox user viewing this data. For example, if an administrator is viewing the data, then the time stamps reflect the time zone configured for the admin.

To view detailed Identity Mapping data on a particular active user, click on the gear icon next to the active user name.

Select **Go to IPAM IP Address Details** to view the network address of the device and any DNS or DHCP-related data associated with the device, such as A records and lease information.
User Login History

To view network users login history, go to Data Management > Network Users > User History.

The Status in the User History tab will display one of these three values:

- Active (user is logged in and active at the time)
- Logged out (user has logged out of the system with logout time stamp set)
- Timed out (user is logged in but has been idle* for a certain time, default is 2 hours)

*Idle means no additional authentications for the users are found within the given time frame.

Search Filters

One powerful feature of the Infoblox Grid is its ability to search for data using filters. For example, if you want to search for a particular user name, he or she can do so as shown below.

The search operators used in the example above are "User Name", "equals", and then the actual user name. Multiple search operators are available to help you search for data as shown below.
User Session
Infoblox considers the following login scenarios as different user sessions:

- A different user at the same IP is a different session
- The same user at a different IP is a different session
- The same user at the same IP at a different point in time is a different session.

Microsoft Events
Since Identity Mapping looks at user logins in the Microsoft security event logs, Infoblox is interested in the following events and reads only these events,

- **Kerberos Authentication Event (event id 4768):** Seen when a user enters a user name and password (logs in). It is seen only on the domain controller (DC). The user name and password are authenticated on the domain controller, a TGT (ticket granting ticket) is issued, and event 4768 is logged.
- **Kerberos Service Ticket Request (event id 4769):** Logged when a service ticket is requested. Service tickets are issued whenever a user or computer accesses a server on the network. For example, when a user maps a drive to a file server, the resulting service ticket request generates event ID 4769 on the DC.
- **Kerberos Service Ticket Renewal (event id 4770):** Logged when a service ticket is renewed. Kerberos limits how long a ticket is valid. If a ticket expires when the user is still logged on, Windows automatically contacts the domain controller to renew the ticket, which triggers this event.
- **Account Login Request (event 4624):** Logged when a user logs in or a service logs in the user successfully.
- **Account Logoff Request (event 4634):** Logged when a login session ends.

Dashboard Widget
A new Dashboard widget, called Network Users, is available with Identity Mapping.

You can find networks with active users; for example, if an administrator wants to know the networks that have at least one active user, then he can configure this widget as shown below,
Reporting

A new report, called **User Login History**, has been added in the reporting section Identity Mapping. This report shows user login activities over time to help you audit user logins. With this report, you can get data such as:

- List all user machine IPs, that is, domains used by a user to log in.
- Number of active users
- User login activities during a specific period of time

To generate this report, go to **Reporting > Reports > User Login History**.

By default the report provides output based on last week’s user login history as shown below.

![User Login History Report](image-url)