Infoblox
CONTROL YOUR NETWORK

Identity Aware DDI

SOLUTION NOTE

Summary

Infoblox Identity Mapping enables Identity Aware DDI. This is a significant step forward in bridging the gap between network-centric management tools and user-focused network administrators. Infoblox provides network administrators and security teams next-level visibility by relating username information with IP and MAC address information in one IPAM database. The merging of username data with network data provides IT administrators and operators more visibility in managing and trouble-shooting enterprise networks that leverage Microsoft Active Directory services. Infoblox Identity Mapping analyzes the Microsoft Server event logs and captures user login, logout, and authentication events from various Microsoft services including Exchange, SharePoint, file shares, and others services that leverage Active Directory authentication.

The Challenge

The correlation of users to network devices and network data is typically a cumbersome task resulting in less-than-optimal operations. Network teams struggle to gather the information needed to perform their own operations, trouble-shoot, and strategically plan as well as support other IT teams. Even with sophisticated network discovery tools the end result is still a network-centric view, which limits the level of information network teams can provide to security, server, cloud, desktop, and other IT teams—who are all delivering IT services at the user level.

What is Infoblox Identity Mapping?

Infoblox Identity Mapping enhances the authoritative data in the IPAM database, making DHCP and DNS identity aware. Having user information as a key data focal point in IPAM improves visibility beyond devices. Networks are not just about devices and addresses; they are about users, so displaying user information related to networks and end-host devices connects administrators to the information they need more quickly. This results in more informed network administrators with a richer understanding of how network resources are consumed and by whom.

How it Works

The Identity Mapping feature analyzes the Microsoft event logs looking for user login, logout, and authentication events. Infoblox, a Microsoft Gold Partner, leverages agentless Microsoft synch technology to help capture authentication events from the Microsoft event logs. Since Infoblox is leveraging the same Microsoft synch technology found in its Microsoft DNS and DHCP management feature, the Identity Mapping feature has many of the same features and benefits associated with it.

The Infoblox implementation provides greater ease of use and logging of the data for historical reporting. The improved IPAM data includes the combined username, IP address, and MAC address, allowing administrators to view:

- Users per network
- Users per range/scope
- Users associated with DNS records
- Users triggering DNS security events (with the Infoblox Reporting Server)

Any services that authenticate against Microsoft Active Directory can be used to enrich IPAM data. When using Identity Mapping in conjunction with Microsoft Exchange Servers, administrators can correlate mobile devices on the enterprise's Wi-Fi network when they authenticate to Exchange. Authentication of web applications via Microsoft Internet Information Services (such as SharePoint) can also provide identity data.

The accuracy of user identity data is directly related to the accuracy of data collected from Active Directory. Infoblox recommends targeting servers that service the most authentication events in order to achieve maximum fidelity. Infoblox Identity Mapping also incorporates controls to account for scenarios in which users don't explicitly log out. Such scenarios include mobile users roaming off network and users who close their laptops rather than logging out.

Example Use Cases

Historical Data Supporting Security Event Investigation

A security event occurred in the enterprise two weeks ago. The associated application owner has narrowed down the source of the event to a single IP address. DHCP lease times are 24 hours. Infoblox Identity Mapping determines which end-host had that IP address at the time of the event and reports on the user who was accessing the server at that time. Understanding who the user was helps the team to deduce who was responsible, or whose account may have been compromised.

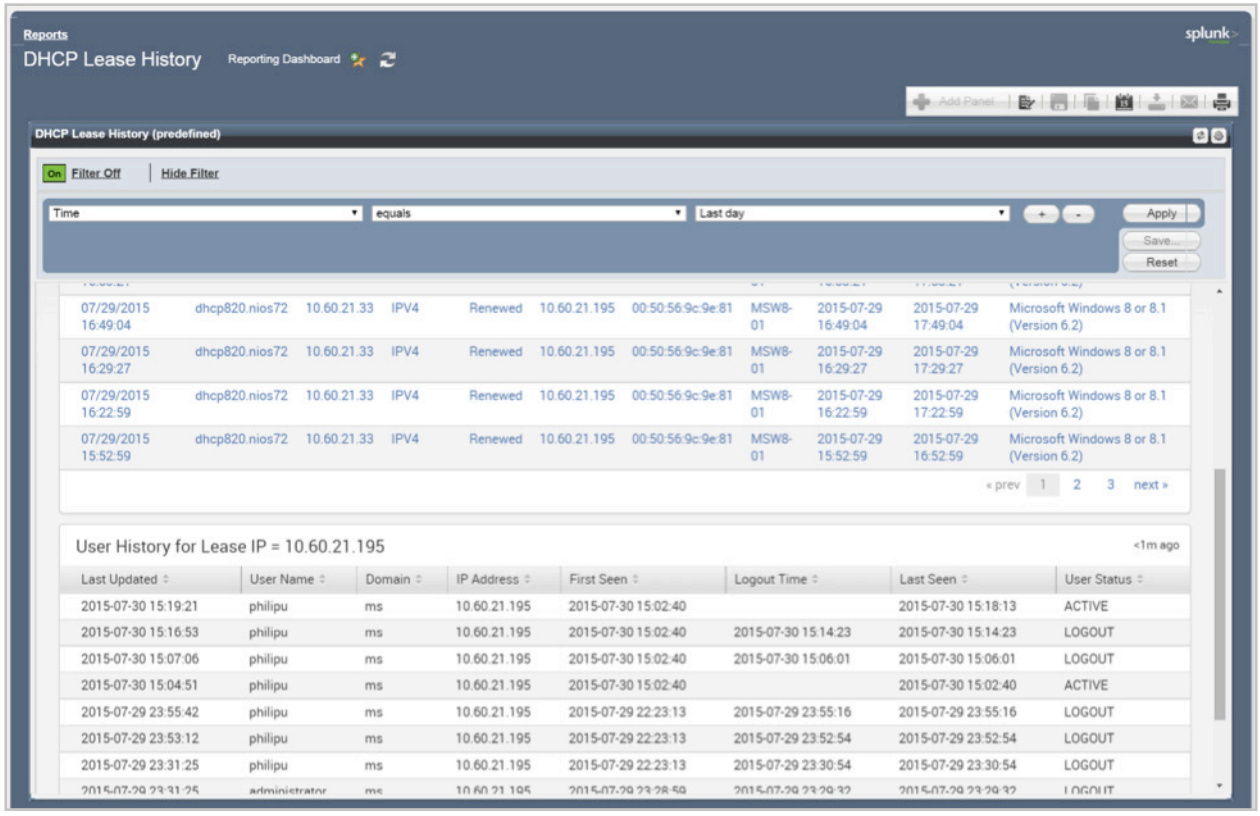

Figure 1: DHCP Lease History Report with Identity Mapping

Mobile Users Accessing Microsoft Exchange

IT would like to get a better understanding of who is using mobile devices on their wireless networks. Mobile devices aren't part of the Windows domain and typically don't authenticate against the domain, making it difficult for IT to determine who may be on their Wi-Fi networks. It is, however, likely that these devices connect to the corporate Exchange server in order to access email. Infoblox correlates authentication with Exchange to the user's IP address, providing the necessary visibility—all without an agent on the mobile device.

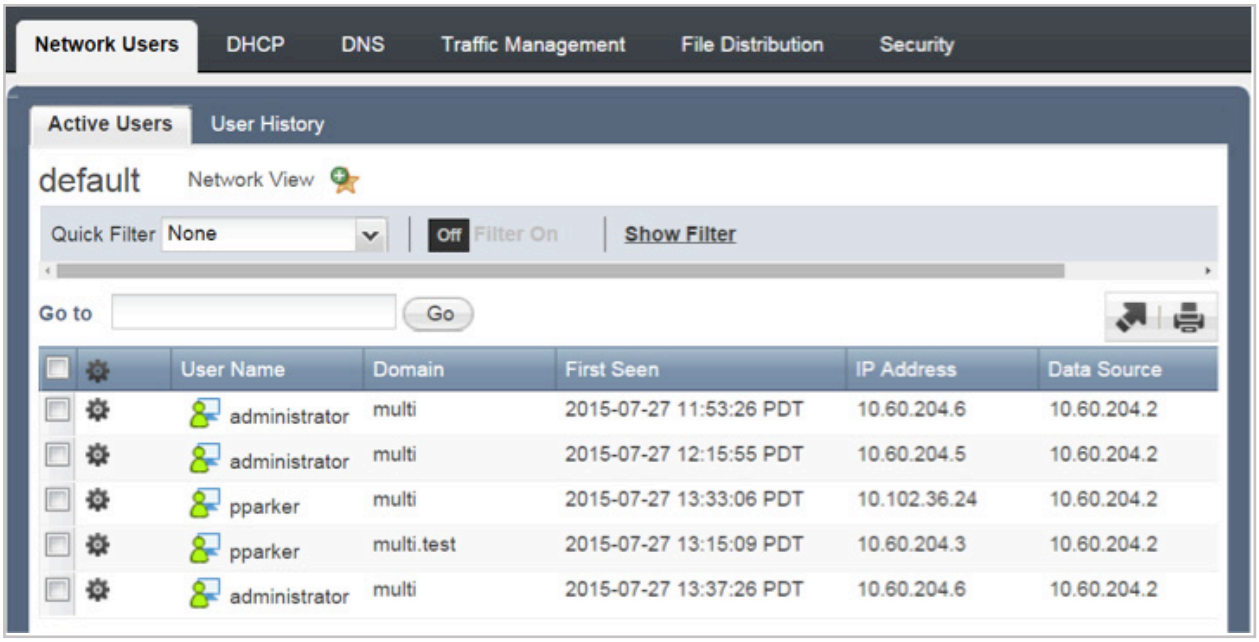

Figure 2: Active Network Users

Notify Users of Network Outage

IT determines that they will need to perform emergency maintenance on a given network. They can identify how many users are actively using that network and who those users are so they can determine the impact of the outage as well as notify the impacted users prior to taking down the network.

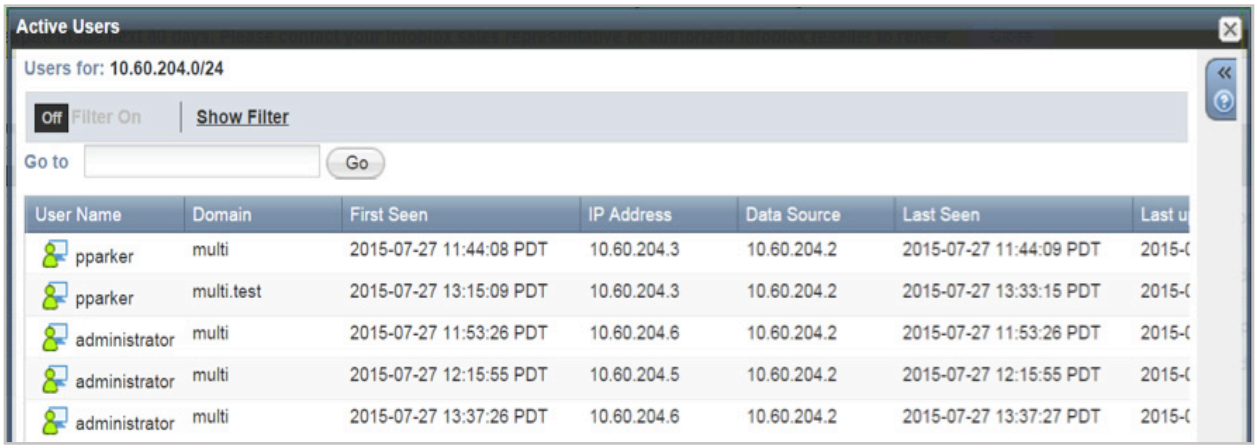

Figure 3: Active Users on a Network

Set Up is a Snap

The setup process for Identity Mapping has been added to the already streamlined Add Microsoft Server Wizard in Infoblox. This easy-to-use, step-by-step wizard is used to add the Microsoft Servers you want your Infoblox deployment to communicate with and manage. With the addition of Identity Mapping to NIOS 7.2, the wizard now enables administrators to add those servers that have Microsoft Event logs from which they want to extract username information.

Along with the additions to the Add Microsoft Server Wizard, there are several new or modified UI screens and reports and a dashboard widget.

Upgraded Reports and UI Screens

- The DHCP Lease History report correlates usernames to DHCP leases.
- The Top RPZ Hits report now identifies username associated with IP addresses making queries hitting the RPZ.
- The Data Management tab now has a Network Users tab—presenting who has been on which networks—with Current Users and User History sub-tabs. The time-frame for this data is limited; historical information outside the window is handled by the Reporting Server.
- Networks and scopes/ranges in the IPAM and DHCP screens have an Active Users column.
- DNS screens can show users associated with select DNS records.

Upgraded Reports and UI Screens

- The User Login History report shows user logins over time, filtered by time, username, IP address, domain, etc.
- The Active Network Users widget is an easy-to-read widget for the Infoblox dashboard showing the active user count by network.

Conclusion

When data is brought together in meaningful ways, network administrators, security teams, and other IT groups can make more informed decisions and take action more quickly to improve network administration capabilities and decrease the time to repair in trouble-shooting scenarios. The combination of usernames to IP addresses and MAC data made accessible throughout the DDI solution is a prime example of elevating data into useful information.

To find out more about the Infoblox DDI solution, visit www.infoblox.com/ddi.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com