IPAM Integration with Microsoft AD Sites and Local Services
Infoblox IPAM Integration with Microsoft AD Sites and Local Services

Today’s enterprise infrastructure is dynamic, with new geographical locations and the networks associated with them being added or deleted on an ever-increasing basis. Microsoft represents network topology with directory objects called sites and subnets.

But a gap exists in enterprise infrastructure in which the current state of the global network may not be reflected correctly within Microsoft Active Directory (AD). Network subnets may not be allocated to individual Microsoft AD sites correctly, or at all. This causes an inefficient allocation of Windows services, or even outright outages of such basic services as user authentication and file availability.

Microsoft does not offer tools to reveal and resolve such serious issues. Infoblox IP address management (IPAM) integration with Microsoft AD Sites and Services resolves such critical issues by providing the Microsoft administration team a real-time presentation of every single subnet associated with each Microsoft AD site. If any subnet is incorrectly allocated, or not allocated at all, Infoblox provides the tools to quickly resolve the situation.

Microsoft Active Directory Sites and Subnets

A Microsoft AD site is:
- Associated with IP network subnets
- Used to manage replication traffic
- Used to manage client logon traffic
- Used by site-aware applications such as distributed file systems (DFSs) or Exchange Server
- Used to assign group-policy objects to all users and computers in an enterprise location

Microsoft AD enumerates, authenticates, and authorizes users and machines and enforces group policy. Enterprise customers use numerous domain controllers that all contain an essentially identical copy of their domain directory. To ensure local changes are spread throughout the enterprise, each domain controller communicates any local changes with the other domain controllers.

Microsoft AD assumes there are two types of network subnets within a company: highly connected and not so highly connected. An AD site includes one or more subnets and represents a highly connected site. Therefore within an AD site, data replication is immediately conducted with all the domain controllers within that site. Between those sites might be slower, expensive, and less reliable connections. Replication between sites can be scheduled and managed.

Microsoft replication is the transfer of changes between domain controllers. For example, if an administrator changes a user’s password, that change is committed to the directory in one domain controller. The change must then be replicated to all the other domain controllers within the domain to ensure that the user is able to authenticate and log on to services at any global location within the domain.
Infoblox Single Authoritative IPAM Database

The Infoblox solution is designed from the ground up to be the single authoritative IPAM solution for enterprise infrastructure, and it communicates with the processes that add, delete, or modify IP addresses and networks. Infoblox has the unique ability to discover, organize, and present every static and dynamic IP address and every IPv4 and IPv6 network, physical and virtual, throughout a global enterprise. To accomplish this, Infoblox communicates with all network devices, including switches and routers from more than 50 vendors such as Cisco, Juniper, HP, Dell, and F5.

Infoblox also communicates with major orchestration and provisioning tools from solutions as diverse as Microsoft, VMware, and Open Stack through their native protocols and through representational state transfer (REST) application programming interfaces (APIs). Infoblox provides the only authoritative IPAM solution that can discover and communicate with such a large and diverse number of other systems to ensure that every single IP address and every subnet is discovered and presented to IT teams and systems.

It is important for an enterprise to use a single authoritative IPAM source that simplifies the provisioning process for every other system within the network infrastructure and cloud deployments. Such a source eliminates the need to write multiple custom plug-ins for different technologies or to use multiple point solutions or spreadsheets to manage IP data. Simply pointing all orchestration and provisioning tools at the Infoblox solution makes it possible to gather the information required.

Infoblox Single Authoritative IPAM Database

Infoblox uses Microsoft's MS-RPC to communicate with Microsoft DNS and DHCP servers and leverages Microsoft's LDAP interface to communicate with AD, so no software agents are needed on Microsoft servers. When Infoblox IPAM is integrated with Microsoft AD, it also has the capability to integrate with Microsoft's DNS and DHCP services. Multiple configuration options are available. The Infoblox solution can be fully authoritative or partially authoritative for DNS and/or DHCP services. It can be used to manage all or part of Microsoft's DNS and DHCP services or only used for monitoring and reporting on those services.

Infoblox and Microsoft AD integration provides:

- Bidirectional management of AD sites, network subnets, and AD site relationships
- Auto-population of subnets from Microsoft AD Sites and Services into Infoblox
- Ability to quickly move subnets between AD sites within Infoblox
- Ability to create new AD sites within Infoblox
- Ability to assign new network subnets created in Infoblox to a Microsoft AD site
- Visibility into the domain and AD site relationships
- Visibility into networks not assigned to an AD site
- Logging of AD site-specific data
Infoblox Ease of Operation for Microsoft Administrative Teams

Infoblox discovers and presents every physical and virtual network in an enterprise. Figure 1 shows a representational view of a large enterprise network using the 10.0.0.0/8 address space. Note how easy it is to recognize full, partially used, and unused network subnets.

![Figure 1. Properties such as key settings and notifications are easily assigned.](image)

Infoblox Facilitates the Process for Quick Integration

The initial configuration of Infoblox and Microsoft integration is simplified by an easy-to-follow wizard that helps quickly guide the administrative team through the process of establishing communication between the two systems. When integration is established, Infoblox provides additional logging and tests to monitor the synchronization processes and provide an audit of AD site activities.

Additional reporting capabilities are made available for presenting relevant data to administrative teams. Infoblox customers need to add an IPAM for Microsoft license to a member appliance in order to enable MS-RPC communication. An organization has the option to configure integration in read-only mode initially, to gain a better understanding of its current situation, and then configure it in read/write mode in order to start active management and optimization of AD sites. Infoblox uses role-based access controls based on Microsoft AD groups to determine which administrative teams are authorized to make changes within the Infoblox tool set.

When Infoblox first communicates with Microsoft AD Sites and Services, it will import the current AD site configuration. From then on, any changes that are configured from within Microsoft Management Console will be continuously synchronized within Infoblox as incremental updates. Likewise, any networks created within Infoblox and assigned to an AD site will be synchronized within Microsoft AD Sites and Services. Figure 2 shows AD sites presented within Infoblox.
Figure 3 shows a drill-down in Infoblox presenting the subnets currently assigned to an AD site.

When a new network needs to be created or a new network subnet is detected, Infoblox uses wizards to help quickly guide the administrative team through the process of assigning the subnet to an AD site. Figure 4 shows the easy-to-understand wizard for quickly assigning networks to AD sites.

If a subnet is not assigned to the correct AD site, Infoblox provides another wizard to quickly move network subnets between AD sites.

Some networks by design should not be assigned to an AD site. For example, enterprise security may designate networks with public access, such as subnets intended for public wireless networks that should not have any association with AD sites. The inherent risk to the enterprise is the Microsoft administrative team may not know which networks should be associated with an AD site and which should not. When a network subnet is created within the Infoblox IPAM tool, it asks the administrator where to assign it.

When a network subnet is created by an IT team or process outside of the Infoblox IPAM solution, the Infoblox real-time topological view of the enterprise network infrastructure enables the administrative team to discover it. When any network subnet is discovered, and it is not associated with an AD site, Infoblox uses a tool called Smart Folders to immediately present all unassigned networks as shown in Figure 5. The enterprise network team or Microsoft team can quickly assign the new network subnet to an AD site, or any other category network such as demilitarized zone (DMZ) or public wireless as required. In this manner, Infoblox ensures that no network subnet is accidently forgotten and left unassigned. When a network subnet is created by an IT team or process outside of the Infoblox IPAM solution, the Infoblox real-time topological view of the enterprise network infrastructure enables the administrative team to discover it. When any network subnet is discovered, and it is not associated with an AD site, Infoblox uses a tool called Smart Folders to immediately present all unassigned networks as shown in Figure 5. The enterprise network team or Microsoft team can quickly assign the new network subnet to an AD site, or any other category network such as demilitarized zone (DMZ) or public wireless as required. In this manner, Infoblox ensures that no network subnet is accidently forgotten and left unassigned.
IPAM solution, the Infoblox real-time topological view of the enterprise network infrastructure enables the administrative team to discover it. When any network subnet is discovered, and it is not associated with an AD site, Infoblox uses a tool called Smart Folders to immediately present all unassigned networks as shown in Figure 5.

The enterprise network team or Microsoft team can quickly assign the new network subnet to an AD site, or any other category network such as demilitarized zone (DMZ) or public wireless as required. In this manner, Infoblox ensures that no network subnet is accidentally forgotten and left unassigned.

Infoblox Delivers Efficient, Reliable Windows Authentication and Services

One issue that Microsoft AD teams must deal with can be demonstrated by a scenario in which an enterprise Windows client in Tokyo bypasses the local domain controller and attempts to authenticate, or access services, with a domain controller in Miami. The more complex an enterprise environment is, the more likely it is that this scenario will occur. Ideally, any new network added to an enterprise infrastructure should be immediately assigned to a Microsoft AD site or some other category.

But sometimes a network might be created and not immediately associated with any specific location or function. The Microsoft administrative team won’t be aware that new network subnets have been created and won’t learn of this fact until users start complaining about slow or unavailable services. It can be frustrating for Microsoft administrative teams to detect and resolve such issues prior to or during client service interruptions. Microsoft does not offer tools that can quickly detect and resolve this issue in a proactive and effective manner. Infoblox IPAM integration with AD sites offers the best method to quickly detect any new physical or virtual networks, present them to the enterprise IT administrative teams, and give them the tools to easily correct this issue from ever occurring again.

Summary/Conclusion

The Infoblox Authoritative IPAM Database, integrated with Microsoft Active Directory and Microsoft AD Sites and Services, can deliver bidirectional management of AD sites, network subnets, and site relationships. It can simplify and accelerate the creation and movement of subnets, and it can deliver visibility into domain and site relationships and identify unassigned networks. The results are better control of your Microsoft AD networks and subnets, simplified management, reduced staff effort, and faster and more efficient delivery of client services.

If you’d like to improve the contribution your network makes to your business, visit our website at http://www.infoblox.com and learn more about integrating Infoblox Authoritative IPAM solution in support of Microsoft environments.