Managing Microsoft DNS/DHCP Infrastructure

SOLUTION NOTE

Take Back Control and Add IPAM to your Windows-based DNS/DHCP Environment

Summary

Microsoft DNS and DHCP services are deployed by many enterprises. Included with Microsoft Windows server, these critical services are the foundation for network connectivity and applications. All IP devices need addresses, and DHCP is the most efficient way to provide them; and essentially all network applications, from web services to e-mail to Microsoft Active Directory, depend on DNS/DHCP. But increasingly, the management of these services is a challenge as networks continue to add devices and applications at an unprecedented rate.

Managing the growing volume of DNS/DHCP information with existing tools is cumbersome, forcing many network administrators to use manually updated spreadsheets and labor-intensive, error-prone processes to manage their IP addresses. Additionally, these tools provide no ability to delegate administrative authority over just a portion of the resources on a Microsoft DNS/DHCP server, resulting in poor visibility, inefficient operations, compromised security, and an inability to meet audit requirements for compliance. Addressing these problems requires replacing manual spreadsheets and processes with a dedicated IPAM solution.

The Infoblox MS Management Module for NIOS represents the next generation of IPAM systems for Microsoft environments. The Infoblox MS Management Module provides powerful IP address management capabilities for Microsoft DNS/DHCP services, enabling IT administrators to quickly and easily replace spreadsheets, manual processes, and home-grown tools with a cost effective, purpose-built solution while protecting current investments in Microsoft infrastructure; and allows companies to manage their IP environments and IP address data at an enterprise-wide level, delivering unified management, monitoring, and administration with centralized auditing and reporting. The solution enables compliance with regulatory requirements such as Sarbanes-Oxley (SOX) that mandate policy-based retention of IP-related information; and it also provides tangible business benefits including a compelling return on investment.

Managing IP Address Space on a Microsoft Platforms is Expensive, Error Prone and Slow

Manual management of Microsoft server based DNS/DHCP services is a resource drain. The tasks are often repetitive and involve several steps to complete. Since there is no effective way to allow other team members or junior level staff to manage these changes without significant security implications, senior level administration staff has to get involved in servicing every request. One simple example is servicing a request for a new static IP address for a printer.

Common Task	Steps	Work Time/Elapsed Time
IP Address Provisioning	8	30 Min/1-2 Days
DNS/DHCP Change	7	20 Min/2-4 hours
IP Address Reclaim	8	60 Min/2-4 days
Network Provisioning	9	60 Min/1 week

Figure 1: Time and effort requirements for manually managing IP address space.

Typically, organizations maintain their IP address map in spreadsheets or other database programs owned by a few senior level employees. Every request for a new IP assignment requires these IP database owners to lookup the spreadsheet, do a manual network scan to ensure IP availability, update the spreadsheet and send the IP address to the requestor. Additionally, the burden of keeping the IP assignment data updated by periodically reclaiming unused IP addresses, creating new subnets, updating DNS/DHCP records as per requests from applications team etc. keeps the senior staff busy in “keeping the lights on” vs. working on projects where their skills are more critical.

Manual configuration of DNS/DHCP combined with spreadsheet-based IP address management is error prone and even small configuration errors can result in major outages. A lack of key error prevention features in current management tools multiplied by the high number of steps required to complete even simple tasks add outage risks to the IP address management process. This situation is further exacerbated by the fact that there is no centralized management and therefore configuration changes need to be made on each server separately.

DNS/DHCP management tools do not provide detailed visibility into several aspects of these two core services. Specifically, Microsoft server management tools lack the following:

- Detailed reporting and monitoring of IP usage including unauthorized devices, IP conflicts, etc;
- Detailed visual reports of the network and IP space to simplify network planning and troubleshooting;
- Detailed audit logs for configuration changes to simplify rollback of unintended administrative actions;
- Granular control of access to manage IP address space by user, group or role; and
- Simplified backup and recovery of DDI data.

What is Really Needed

Centralization and Automation of DNS/DHCP and IPAM Management

A key first step in reducing DDI management burdens is to centralize management. The current management model requires making configuration changes separately on each server. Since DDI tasks sometimes span multiple servers, repetitive steps are required to service those tasks requiring more management resources and increasing configuration error risks. As an example, installation of a new server would require consulting the IP space data in the spreadsheet, making changes to the appropriate DHCP server to mark the static address and then creating DNS/DHCP records, likely on a separate server. It should be possible to combine all of these activities.

IP Address Management (IPAM) refers to the management of allocation, administration, reporting and tracking of public and private IP space, IP devices and associated data. Enterprises typically deploy spreadsheets and processes that interact with the DNS and DHCP infrastructure in order to provide IPAM capabilities. The system must provide a replacement for spreadsheet-based IP address management and automate/simplify tasks associated with IP assignment, reclaiming, subnet allocation and IP and subnet usage reporting. The system must keep the network device data current through automated discovery rather than depending on manual data.

Effective Distribution of DDI Management Responsibility Across and within Teams

Since DDI operations touch several teams and sometimes it is desirable to distribute tasks based on responsibilities and expertise of teams and individuals, it should be possible to securely delegate DDI tasks to different administrators without affecting the current management practice for the rest of the Windows server functions. As an example, the server team can delegate management of DNS/DHCP and IPAM functions to the network team while keeping control of the rest of the Windows server functionality. Network teams, in turn, can divide the responsibilities based on the region or expertise within the group and delegate even simpler tasks (e.g. new IP assignment) to the helpdesk operator.

Granular role-based administrative control is required to ensure that management tasks can be delegated securely.

Reporting and Alerts for Outage Avoidance, Troubleshooting and Compliance

MS server-based DNS/DHCP management solutions must provide detailed graphical reporting of IP address space and subnet usage as well as information about IP conflicts and other discovered device data for troubleshooting.

DDI systems should provide the administrator of the system the ability to monitor IP Address allocation so they are able to report on total usage of the address space across the enterprise as well as in specific locations of that enterprise. The system should deliver a holistic view of all assets under management so the administrator has a single, unified view of all of the components of the network.

The systems or network administrator needs the ability to search their IPAM data set and report on specific items with ease. For example, they may wish to report all devices that are printers with fixed addresses or generate a report on all addresses not currently in the DNS/DHCP database. The IT administrator needs full audit logs of all DDI changes to meet regulatory and audit requirements and insure compliance. Each change to the DDI infrastructure should be logged internally to the IPAM infrastructure as well as to a centralized reporting infrastructure.

Infoblox Solution for MS DNS/DHCP Management

The Infoblox MS Management Module allows network administrators to centrally manage their entire Infoblox and Microsoft server-based DNS/DHCP infrastructure with minimal disruption. Network administrators can easily therefore manage ever larger and more complex networks. With the Infoblox MS management module a team can:

- **Gain visibility and control** of subnet and IP usage in their existing Microsoft DNS/DHCP server-based infrastructure;
- **Reduce management effort and configuration errors** by centrally managing Microsoft-based DNS/DHCP configuration;
- **Reduce** operational costs through delegation of provisioning and troubleshooting tasks to local administrators and helpdesk; and,
- **Enforce security** by controlling user permissions, logging changes in audit logs, checking configuration syntax and disallowing root access to the appliance.

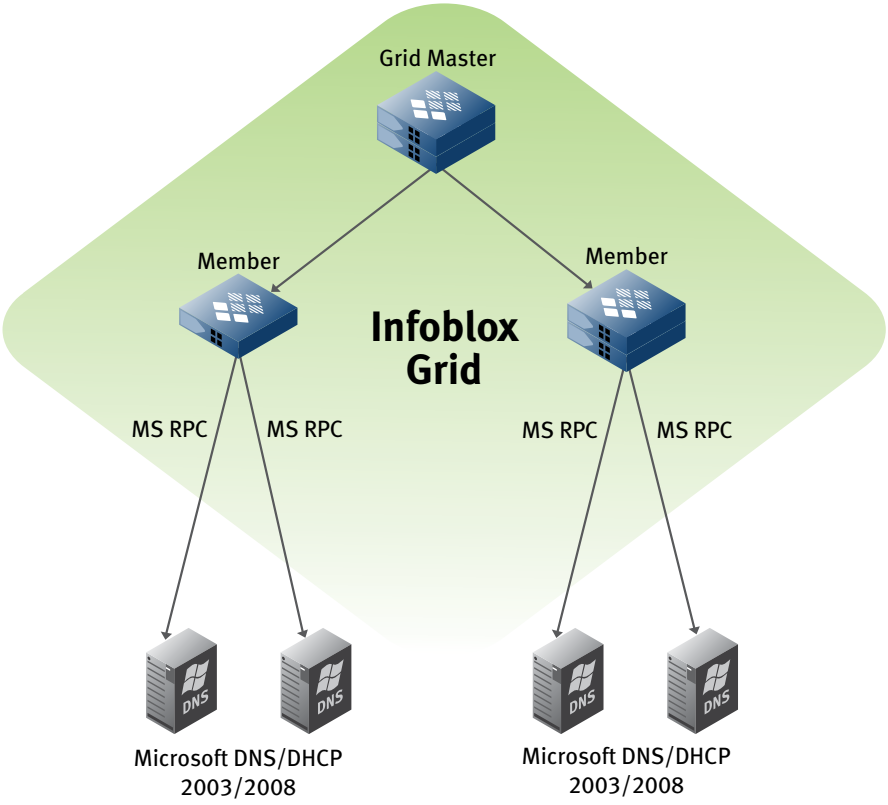
Infoblox MS Management Module for NIOS extends the Infoblox DDI management capability to include management of Windows-based DNS/DHCP infrastructure.

Add IPAM to Your Existing Microsoft Infrastructure

The Infoblox IP Address Management solution automates and simplifies IP address management thus reducing network operating costs and eliminating configuration errors and associated downtime. Advanced visual functions e.g. network maps, IP maps and smart folders provide visibility into the usage and configuration of IP resources.

Automate and Centrally Manage Entire DDI Infrastructure

With Infoblox MS Management Module, your entire DDI infrastructure including Microsoft servers and Infoblox appliances can be managed from one web-based management console. The Infoblox DDI solution provides high levels of management automation to reduce administrative effort and eliminate errors and downtime using a graphical user interface, template-based configuration, automated error prevention, and comprehensive, real-time visibility and reporting.



Securely Delegate Management of DDI Based on Roles

Infoblox NIOS software allows creation of administrative roles and assignment of different administrators to these roles. An administrative role can be defined based on flexible criteria e.g. DNS/DHCP administrators in the Phoenix data center or printer administrators worldwide etc. Once the role has been defined, administrator accounts can be added to specific roles.

Seamless Integration Into Existing Microsoft Server-based Infrastructure

Infoblox is a Microsoft Gold certified partner for infrastructure solutions. The Infoblox solution uses Microsoft RPC and does not require installation of any agents or software on Microsoft servers being managed. In addition, no specific configuration of Microsoft servers is required. Infoblox solutions can coexist with existing tools and practices and Microsoft administrators can continue to use MMC to manage the servers if required.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.

Corporate Headquarters: +1.408.625.4200 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com