Top Reasons Why Enterprises Must Automat DNS, DHCP and IP Address Management
Top Reasons Why Enterprises Must Automate DNS, DHCP and IP Address Management

Regardless of size, businesses face challenges when it comes to managing their network and keeping the cost of running the network low. These challenges are more pronounced in the case of small and medium sized businesses, since they need to maintain the same level of security and availability as larger organizations do, but with a smaller budget and staff. Routine activities such as managing DNS and DHCP, assigning IP addresses, creating and managing subnets and reporting and auditing device connection history can take more than their fair share of time and resources. Moreover, concentration of DNS, DHCP and IP address management expertise in fewer hands makes organizations heavily dependent on a few individuals without adequate backup. These experts have a hard time focusing on more strategic projects since they have to spend an inordinate amount of time on trivial yet repetitive activities like issuing IP addresses, finding out which device is connected where and maintaining spreadsheets for IPAM.

Microsoft DNS/DHCP Server Drawbacks

A large number of small and medium sized networks depend on Microsoft servers to provide DNS and DHCP services. While the system provided tools work great for managing most of the Microsoft server functionality, they provide some challenges when it comes to managing network-centric functions of the Microsoft server software. Specifically, the tools lack the following key attributes:

• IP address management: There isn’t a provision for automating routine activities e.g. assigning IP addresses, mapping IP addresses to devices, creating subnets and looking up connection attributes for quick troubleshooting.

• Centralized management: Typically, DNS and DHCP servers are distributed. Microsoft provided tools require visiting each of these servers to manage DNS and DHCP. There isn’t a centralized view or way to centrally manage the entire DNS, DHCP deployment, thereby making administration tedious.

• Simplified management: Managing DNS and DHCP using the provided tools requires a certain level of expertise including creating and managing scripts. Since tasks dealing with DNS and DHCP are recurring in nature, this ties up senior level members of the team performing routine tasks while more pressing projects wait. Additionally, this exposes IT department to the risk of departure of key employees.

• Role based delegation of DNS and DHCP: Default tools supplied with Microsoft server make it very difficult to distribute management activities based on responsibilities. As a result, either a few key employees end up owning and managing the entire DNS, DHCP and IP address space or everyone has same rights to the system, making it hard to audit management changes.

Augmenting your Microsoft server management tools with IP Address Management system automation yields great benefits for small or large sized enterprise IT environments.
Here are the top reasons why IT organizations should choose to automate their DNS, DHCP and IP address management (DDI).

1. **Do more with less**
   Tasks and activities relating to managing DNS, DHCP and IP address space take up a significant amount of senior level engineering time. These inefficiencies typically disguise themselves as issues that do not seem related to DNS, DHCP management and therefore DNS, DHCP management remains blameless, while a disproportionate amount of time and energy is spent in performing activities like issuing new IP addresses to printers, creating subnets for the branch offices and correlating what was connected where.

   Automation of these routine tasks combined with centralized management of the entire DNS, DHCP infrastructure will allow IT organizations to scale up their operations without investing heavily in hiring more staff members. Once the management of DDI is automated, employees with different skill levels and knowledge of the DNS and DHCP infrastructure can perform these tasks without depending on senior level people.

2. **Troubleshoot faster**
   Troubleshooting network connection problems requires having an accurate picture of what devices are present in the network, what network attributes they have and where they are located. Take for example, a laptop not being able to receive any traffic. A manual network scan might yield a DHCP address conflict since there is another device (likely an unauthorized device) with the same IP address already present in the network. Or a device may be experiencing a slow connection, which after extensive troubleshooting is ascribed to DNS response.

   IPAM automation provides unprecedented levels of visibility into your networks, subnet usage and where devices are connected. All of this information is required when troubleshooting network connection problems. Without IPAM automation, finding this information would require guesswork and manual processes, e.g. scanning the networks, visually inspecting the switch ports and logging into your DNS and DHCP servers to look at the logs, thus increasing response times and operational expenses.

3. **Eliminate configuration errors**
   Manual management of DNS and DHCP and the use of spreadsheets for maintaining IP address space information leave room for administrative errors. Additionally, not many tools currently allow administrators to review administrative changes and selectively undo errors.

   Automation of DDI reduces the number of steps required to configure services, and to make other configuration changes, e.g. adding DNS records. In addition, a good IPAM system provides configuration aids, e.g. recycle bins for rolling back configuration errors, wizards for common configuration tasks and a way for administrators to make changes and get them reviewed before implementing them. Reduction of errors would result in fewer outages and less time spent troubleshooting them.
4. **Enhance security and compliance**

Security and compliance begin with audit and accountability. Strong role based administration with detailed audit logs provides organizations the ability to comply with internal and external policies. Establishing accountability for configuration changes requires strong and granular role based authentication and audit logs that cannot be tampered with. An automation solution, with role based access and detailed audit logs, is a must for compliance and security. In addition, complete visibility into the network including connected devices and network anomalies results in improved security. A quick scan of network utilization data in the IPAM system may alert the administrators about the presence of unauthorized devices (e.g. phone modems) and their location in the network.

Finally, maintenance of device connection history for security breach investigations is a key aspect of automated DDI solutions, a function missing from Microsoft base DNS and DHCP environments.

5. **Prepare for DNSSEC and IPV6**

DNSSEC and IPV6 are here and businesses are starting to plan implementations and pilot programs so they are ready when deployment is imminent. Deploying and maintaining DNSSEC and IPV6 is expensive and require new skills. DNSSEC management involves weekly and monthly activities that require PKI knowledge. IPV6 makes managing IP addresses in spreadsheets a nightmare. It would be very difficult to maintain IPV6 network information and understand the network utilization in an IPV6 network.

Automation of repetitive and complex tasks will help small, medium and large enterprises implement these technologies, without an additional investment in hiring.

**Benefit of Deploying Infoblox for your Microsoft based DNS/DHCP environments**

Infoblox NIOS™ for Microsoft Management allows network administrators to manage parallel IP service infrastructures running on Infoblox appliances and Microsoft Windows servers from a single console. The software delivers granular capabilities not available in Microsoft's management suite, such as centralized IP address management, DNS changes and role-based access control.

Network administrators gain the visibility needed to keep all IP services running 24/7 and to reduce errors, effort and operational costs with the following capabilities:

- Control of subnet and IP usage in Microsoft Windows server-based network service infrastructures
- Central management of Microsoft-based DNS
- Ability to delegate provisioning and troubleshooting tasks to local administrators and helpdesk
- Control of user permissions
- Ability to log changes in audit logs and check configuration syntax
- Ability to take local network and IP assignments
- Automation of routine tasks
- Granular reporting data for troubleshooting and compliance
Infoblox NIOS for Microsoft Management Attributes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized management of DNS, DHCP and IPAM infrastructure from a Web console</td>
<td>Helps you scale your network services environment and eliminate duplication of efforts and out-of-sync IP services management tasks</td>
</tr>
<tr>
<td>Network maps, IP maps, smart folders and other advanced visuals for visibility into the usage and configuration of IP resources</td>
<td>Enables you to stay on top of resource and capacity planning</td>
</tr>
<tr>
<td>IP Address Management</td>
<td>Reduces network operating costs, configuration errors and associated downtime</td>
</tr>
<tr>
<td>High levels of automation with a powerful and intuitive graphical interface</td>
<td>Reduces administrative effort; prevents errors and associated downtime</td>
</tr>
<tr>
<td>Flexible, secure management of DNS and DHCP based on administrative roles</td>
<td>Boosts security by automating and controlling access control to core IP services</td>
</tr>
<tr>
<td>Agent-less architecture</td>
<td>Simplicity; no installation of any software on Microsoft servers needed</td>
</tr>
</tbody>
</table>

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,500 enterprises and service providers in 25 countries control their networks.