Infoblox

WHITEPAPER

Why Infoblox for DDI

It is Time to Migrate from BIND and Microsoft

In many organizations the core services that enable reliable connectivity and access to the internet are based on free and seemingly free products. While the price may be enticing, these products often carry with them the hidden cost of functional limitations and administrative inefficiency. When planning for growth and change, inevitable in today's networks, it is essential to consider the natural limitations of "free" as well as how to core services can elevate the network to the next level.

DNS, DHCP and IPAM: A Short History

At their inception, DNS was a handy method to access websites and applications and DHCP was virtually unheard of. They were usually managed by whoever understood them and relied on "free" systems such as BIND/DHCPD and Microsoft DNS/DHCP. Sometimes spreadsheets were the basis to maintain essential protocol services (i.e. DNS & DHCP). These systems often evolved with a collection of "Do-It-Yourself" tools maintained by a small team of experts. This hindered operational and planning decisions when those experts moved on to other roles or to other organizations.

IP Address management (IPAM) was a later enhancement, sometime disconnected from the people who managed the DNS and DHCP. The teams allocating resources and defining the networks weren't the people managing and defining the names and addresses.

The business impact or reliability of these systems were often ignored within the overall IT strategy and there were rarely consistent rules about which group (Operations, Systems or Networking) was responsible for its upkeep. It was only recently that the concept of combined DNS, DHCP and IPAM ("DDI") was adopted.

DDI in Modern Networks

With the incredible growth and dependence on networks and mobility over the last 20 years, as well as the explosion of mobile device use, DNS is now expected to be a "dial tone" service that just works, all the time.

The critical need for access to authentication, databases, and other back-end resources, IPv6, IoT and just about everything else now places DDI at the core of the network. This adds additional requirements for extreme reliability, integration and accountability. These were never fully contemplated as part of the original design model.

While the free or open-source solutions can provide the necessary services, they can be maintenance-intensive and lack the robustness to be considered "enterprise grade" in today's modern networks.

Businesses are also moving to more automated environments, especially in the cloud and virtual spaces. However, these existing solutions require even more customization if they want to adapt to the expected level of automation. As IPv6 becomes more prevalent, this difficulty will increase further as the days of reading out an IP address over the phone are long gone. To properly manage these increasingly complex environments, a supportable, scalable, centrally managed DDI solution is a must.

Simply put, if DDI services are down, or changes take too long to implement, business functions are negatively impacted, and ultimately this leads to lost productivity and profits.

C-level Priorities

A recent KPMG report listed these five executive strategic priorities for CIOs:

- Greater Speed to market
- Digitization of the business
- Becoming more data-driven
- Building public trust
- Implementing disruptive technology

In the field of DDI these may be developed into initiatives such as "Securing the business," "Increasing the speed of business" or "Protecting the company's reputation."

And when redesigning the DDI infrastructure to address initiatives such as these, it doesn't take much effort to connect the dots and see the limitations of the traditional solutions vs a modern integrated solution.

The business can only be secure if you adequately protect and mitigate all possible vectors of attack against your data, and DNS is now a primary channel for 78% of application layer attacks (DDoS) and 91% of malware distribution, command & control and data exfiltration.

The company's reputation and showing progression towards a more data-driven business will only be achieved if the core of the network uses a system that addresses infrastructure compliance and protection, malware mitigation, and a centralized threat containment and operations model.

And the speed of the business is only going to be viable if DDI is automated to the point where it can support the rapid and variable growth that a cloud-based infrastructure demands.

The path to realizing the promise of a next generation data center can be difficult. Traditional DNS infrastructure and managing IP addresses in a spreadsheet cannot provide efficiency, visibility, or automation for workload provisioning - leaving IT with manual, time-intensive processes for provisioning core network services. True data center transformation is more than storage and compute automation, organizations also need network automation to realize an agile, centrally managed, and highly scalable data center.

You need to know where all your devices are, what they are doing, who they are talking to, how they are changing over time, and where to focus your efforts with the limited resources you have at hand.

The Ideal System

DDI in today's environment must meet a number of important criteria:

- Reliable uptime
- Ease of change
- Real time Endpoint and topology visibility
- Integration to automated systems
- Redundancy and or fast recovery times

Thus, the ideal system should be centrally managed, require minimal resources to maintain, be easy to deploy and scale. It should also be stable, secure and support a variety of different needs. These could be high level administrators, site/desktop support, automation tasks, network planning, and security forensics.

For planning and forensics, a "single source of truth" is key. A system that offers one place to look for any device or network information, as opposed to searching multiple, possibly conflicting or out-of-sync systems is mandatory.

This extends to historic growth patterns, visibility into DNS usage & trends, DHCP lease history, and device history. All of these are key to being able to quickly respond to security incidents, troubleshoot network issues, and general capacity planning.

The ideal solution would also be able to interact with other systems as part of a larger ecosystem and dynamically communicate with each other to exchange information. Automation is now a must have.

Examples of this include:

- Queries for a DNS record that has been flagged as potentially malicious, DNS can "catch" this via Response Policy Zones. This match could then be communicated to a device scanner, to automatically scan the system in question for possible issues and alert as necessary, and quarantine said system.
- DHCP lease logs can be sent to a 3rd party logging system to track usage trends and event correlation
- An automated system for IP assignment and reclamation for newly created VMs can shorten provisioning times from hours or days to minutes.
- An endpoint security system flagging a malicious endpoint could automatically push this information into a security policy to prevent clients from contacting said endpoint.

These are, of course, just a few of many examples where automated interaction between systems can result in ease of change, real time endpoint and topology visibility, and integration to automated systems.

The Infoblox Advantages

Legacy Systems Won't Scale

Although BIND became an industry-standard with respect to DNS and the Internet, it requires high levels of knowledge and skill to implement and operate properly. There is a multiple of manual steps involved to do simple tasks properly (e.g. a zone's serial number must be incremented when records are added/modified/deleted). When implementing more complicated configurations and features such as DNSSEC, there are pitfalls that can lead to unpredictable performance and possibly a complete DNS outage.

In addition, while BIND supports DNS it provides no integrated reporting to enable performance monitoring and management, and it provides no integration with IP address management, which leads to discrepancies between native DNS records and what may appear in IPAM. BIND was never developed with automation in mind, so it does not contain a robust API for simple automation of DNS record changes, something a focused DDI system provides.

Integrating IPAM with DNS

Integrating IPAM with DNS is crucial to keeping both systems as accurate and synchronized. When a new device is deployed on a network, the assignment of an IP address comes first, which is then usually followed immediately by a request to add the host to DNS. By integrating DNS and IPAM, this process becomes a single step- the DNS record is created at the same time as the IP assignment. Not only does this improve efficiency but it reduces the likelihood of errors because the data is not transcribed or relayed. As the proliferation of IPv6 continues the need for integrated IPAM with DNS only rises.

To further improve the accuracy of the DNS and IPAM, a discovery component can be added. Having a discovery component integrated into IPAM transforms it from a system that is almost entirely dependent upon human action to an "Authoritative IPAM" that gives network administrators and security operators a real-time view of what is in-place on a network at any moment. When combined with a reporting solution, the history of an IP address can be tracked over time, which can be crucial for properly analyzing security events.

Using Infoblox DDI, you have a modern DNS service system that addresses many of these problems in the following ways:

- Consolidate DNS, DHCP, IP address management, and other core network services into a single platform, managed from a common console
- Centrally orchestrate DDI functions across diverse infrastructure with integrated capabilities for hybrid and public cloud and virtual and private cloud environments
- Access rich, integrated Reporting & Analytics capabilities for capacity planning, asset management, compliance control, and auditing
- Boost IT efficiency and automation by seamlessly integrating with other IT systems through RESTful APIs, in conjunction with the Infoblox Grid

Infoblox for DNS vs Microsoft DNS

When it comes to choosing a DNS solution for use with Microsoft Active Directory, many administrators simply pick "what's in the box with Windows Server." However, there are reasons to use non-Microsoft DNS.

- **Security:** Organizations demand the best solution for their external DNS lie exposed to Internet attacks. Third-party DNS solutions are available which are designed and built from the ground-up with security in mind. An organization's internal DNS structure is equally open to malicious threats, malware, phishing and data exfiltration.
- **Visibility and Single view:** Most organizations have a heterogeneous mix of technologies. Accurate, one-stop visibility is essential to efficient compliance and control.
- **Operational Efficiency:** Optimizing OpEx by utilizing automation and workflow vs manual spreadsheet management.
- **Intelligent Services:** Integrated DNS-based traffic control, network load balancing and service monitoring add great value to an organization. Gaps in Microsoft IPAM create inconsistency between the current state of network topology and the information contained in Microsoft Active Directory (AD). This could lead to outright outages of basic services such as user authentication and file availability.

Infoblox IPAM can also integrate seamlessly with Microsoft AD Sites and Services and plugs this gap for both AD and network administrators. Further, Infoblox spans Microsoft forests and brings the entire Microsoft environment into a centrally managed GUI, offering unprecedented visibility, operational efficiency and service uptime.

For more information, see "Microsoft vs Non-Microsoft DNS: Facts vs Fiction," written by Jeremy Moskowitz, Group Policy MVP.

Infoblox Integration with Other Products and the Ecosystem

Infoblox also provides seamless integration with leading security and management technologies. We enable intelligent automation via open APIs and support workloads across both cloud and on-premise environments. Our offerings consist of context-aware security with advanced threat intelligence and ecosystem integrations.

As a part of a larger security ecosystem, Infoblox also supports REST and PERL API's, as well as an event-based Outbound API, which can interact with other systems in the security infrastructure to add networks for scanning as they are added to IPAM, trigger a device scan and/ or quarantine if an end device sends a query matching an RPZ rule (including Threat Insight), etc. In addition, Infoblox also has integration with Cisco ISE, McAfee and over 20 others, and the number is growing.

Conclusion

What You Should Do

"Free" systems, such as BIND/DHCPD, Microsoft DNS/DHCP and spreadsheets do not adequately address the needs of a modern network. Take the time to examine the weaknesses in your core and develop a plan that will migrate you towards an integrated IPAM system.

Identify your existing workflows and IPAM processes and look to see where you can make improvements in:

- Reliable uptime
- Ease of change
- Real time Endpoint and topology visibility
- Integration to automated systems
- Redundancy and or fast recovery times

Infoblox also has a proven track record, being the market leader with over 50% market share, and more than 8,000 customers, and we have a number of resources to assist you in this decision: https://www.infoblox.com/resources/?category=Whitepapers

The Next Steps

Contact your Infoblox Sales Team to discuss suggested deployment architectures.