Infoblox
CONTROL YOUR NETWORK

WHITE PAPER

Infoblox and the Relationship between DNS and Active Directory

Infoblox DNS in a Microsoft Environment

Infoblox is the first, and currently only,DNS/DHCP/IP address management (DDI) solution provider to achieve Microsoft Gold Systems management competency in the Microsoft Partner Network. This competency identifies Infoblox as an experienced partner fully qualified to deploy products with the Microsoft Active Directory and Identity Management solutions. The Infoblox DDI appliance-based solution is fully compatible with Microsoft Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services and integrates seamlessly into a Microsoft environment.

Why DNS is Important

DNS is one of the oldest protocols on the Internet, being over 30 years old. DNS was designed to be incredibly robust, hierarchical, and distributed, hence it may be taken for granted. But other than the core switching and routing fabrics, no part of the network is relied on more by virtually every client and server in the network. Nearly everything we do in the network today is dependent on DNS to resolve IP addresses into a human-useable naming scheme. And with the introduction of IPv6 into today's enterprise networks, the need for naming schemes versus IP only gets stronger.

Why Choose Infoblox?

Infoblox dominates the DDI space. Infoblox delivers enterprise-grade DDI focused on three key vectors: security, manageability, and availability. Infoblox products and services also intelligently extend the core capabilities of DNS, DHCP, and IPAM in ways that improve on the enterprise-grade DDI.

Security

Infoblox is focused on proactively securing all protocols and delivering market-leading security features such as distributed denial of service (DDoS) prevention, response policy zones, DNS alerting, and reporting. Infoblox offers hardened appliances with purpose-built operating systems, and as a result is deployed in some of the most stringently controlled networks in the world. With presence in both enterprise and government environments, it is exceedingly likely that the Infoblox solution meets and exceeds the security requirements for any environment. Infoblox maintains consistent involvement with the software and DNS community, which means that the company tracks issues in the protocols and addresses them so you do not have to.

Manageability

Infoblox has been a leader in improving and simplifying the management and troubleshooting of DNS protocols. Its centrally managed Infoblox Grid™ architecture allows users to manage the deployment of data to the entire architecture from one Grid master interface. Granular role-based administration allows organizations to grant individuals just the access needed to make the changes under their authority, minimizing the amount of work the core team needs to spend on common and often repetitive tasks. With its constantly growing array of tools that make DNS more flexible, Infoblox includes dashboards for common tasks, bookmarking of objects that require more attention, and the ability to organize objects into Smart Folders based on criteria unique to each organization. No matter what the organizational and architectural concerns, Infoblox has worked to make management of DDI infrastructure and data as easy and painless as possible.

Availability

The patented Infoblox Grid technology provides ease of protocol redundancy as well as hardware redundancy across the architecture, while maintaining it all through a centrally managed solution. By leveraging industry-standard Virtual Router Redundancy Protocol (VRRP, RFC 5798), supported by proprietary synchronization technology, full hardware redundancy is provided with little to no risk of data loss in the event of a hardware failure. Additionally, the centrally managed Grid members function as protocol redundancy to add another layer of fault tolerance. Anycast DNS service within Infoblox supports both Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) routing protocols, allowing it to create seamless, multiple levels of fault tolerance by having multiple servers responding from geographically distributed locations to queries to the same server IP address. Combined, these features provide the ability to build highly redundant and fault-tolerant architectures designed to meet any organization's needs no matter how demanding.

Infoblox Understands Microsoft Active Directory Dependence on DNS.

Summary

The Microsoft Active Directory (AD) service was introduced to replace the flat user authentication model found in Windows NT. It was designed from the ground up to provide robust authentication and directory services. In order to provide these services to the users of the network, Microsoft chose to use the long-established DNS protocol. This allows domain controllers within the Active Directory forests and domains to publish the services each domain controller offers. Thus all the services provided by Active Directory rely on DNS to allow users to locate the services running.

Domain Controller Locator

Microsoft Directory services rely exclusively on DNS to publish the availability of services on each domain controller. Domain controllers publish DNS service records (SRVs) to allow clients to locate the availability of directory services such as Global Catalog and LDAP. These critical services are responsible for such mission-critical tasks as logging on to domain and user authorization for accessing critical resources. The correct and accurate publication of these records into DNS is mission critical to any enterprise leveraging Microsoft for directory services.

Active Directory Domain Names in DNS

Microsoft leverages a relationship between directory service domains and related DNS zones. This allows clients trying to access resources for a given Microsoft domain to leverage DNS by searching for resources in the matching DNS zone. Additionally, Microsoft leverages special subzones (often called underscore zones) to specifically hold the service records for the matching domains.

Active Directory DNS Objects

DNS service records are an Internet Engineering Task Force (IETF) record type standardized in RFC 2782. Microsoft has taken full advantage of this record type and has implemented it as the core method for publishing services. The SRV record type allows for the specification of service type, transport protocol, port, weight, and priority.

Below is an Example SRV record showing that server dc02 has the LDAP service available for the example.net domain.

```
_ldap._tcp.west._sites.DomainDnsZones.example.net. 600 IN SRV 0 100 389 dc02. example.net.
```

Infoblox Enhances Microsoft Active Directory

Infoblox adds functionality, including highly available and secure DNS, to the Microsoft Active Directory services. The symbiotic relationship between Infoblox and Microsoft AD creates a robust and secure environment, rendering the best possible nameresolution system without creating interdependence. This lack of interdependence is the primary benefit of this particular combination, allowing each of these two core services, Infoblox and Microsoft AD, to be controlled within individual architectures. Each can each be customized, managed, upgraded, and patched independently of the other. By running DNS services on Infoblox, Active Directory is able to gain a number of immediate and important benefits including:

Gain of Resources on Domain Controllers by Removing the DNS Service.

Removing DNS from the domain controllers allows the server to focus on managing the domains. The removal of DNS also allows the domain controllers to function optimally regardless of the DNS load within the environment. Repeatedly, domain controllers respond substantially faster once the DNS authoritative (ADI) functions are adjusted to function as the DNS forwarder to Infoblox. The ability to turn the DNS service off completely means the domain controllers can allocate all available resources to the functioning of Active Directory and its related services.

Remove Interdependence between the Services Being Hosted on the Same Server

Once interdependence is removed, if one service is being overloaded or even attacked, there will be no effect on the other services. As these two services, DNS and AD, are not interdependent by nature, they can function separately with no risk of issues spreading from one set of services to the other. The separation also allows administrators to resolve one service's issues with little or no concern for the other service.

Independent Patching, Upgrading, and Management

Finally, the separation of these mission-critical services onto separate hardware platforms allows for each service to be maintained without worrying about interruptions and impacts to the other service. In a change-control world, this has a huge impact on the ability to properly maintain and improve the services provided to the enterprise.

Infoblox Advantages

Security

The Infoblox solution is the perfect foundation for extending security with specific features like DHCP Fingerprinting for access policy enforcement, rogue-device detection, and Media Access Control (MAC) spoofing alerts. DNS is also enhanced with Infoblox DNS Firewall for prevention, detection, and mitigation of malwareinfected devices. The DNS Firewall has a trusted feed of malicious site addresses that is regularly updated. For zero-day attacks, Infoblox DNS Firewall has been integrated with the FireEye NX Series appliance, making its detection of risk actionable by tying FireEye findings into the feed supporting the DNS Firewall. For externally facing DNS, Infoblox offers an Advanced DNS Protection appliance that can continue to respond to DNS queries even during an attack. Finally, the discovery within Infoblox Network Insight provides the visibility necessary to ensure there are no risks lurking in terms of unmanaged networks and devices. These products that supplement the core DDI make Infoblox an exceptionally secure alternative to using native Microsoft DNS and DHCP.

Database and IPAM

At its core, the Infoblox DNS solution is a real-time distributed semantic database. This allows Infoblox to provide solutions to the largest organizations in the world and offer real-time data availability. The Infoblox database is designed with the sole purpose of providing reliable and secure DNS, DHCP, and IPAM. Therefore, it delivers superior data synchronization when compared to other solutions in the industry. That core database provides the building block to a true IPAM solution that allows for the overlay of both protocol and enterprise data. It takes IPAM past the IP address itself and requires the data to be referenced and then cross referenced against any and all fields, providing visual insight and analysis to the network hosts. The Infoblox Grid database's asynchronous nature results in virtually no delays in propagating new data to other members and servers.

Auditing

Infoblox provides complete administration auditing. All administrative actions are logged to both an audit log and optionally written to SysLog. This allows administrators to provide a complete audit history on a per-administrator basis or on a per-protocolobject basis. An organization can now provide all the needed data for various standards-based auditors. Additionally, this enables organizations to clearly identify changes in the environment when troubleshooting identified issues, thus decreasing support times.

Manageability

Infoblox Grid technology adds single-pane-of-glass management for the entire DDI architecture. There is no need to manage individual servers, and therefore, focus can be given to the tasks associated with DDI. From day-to-day data entry to the deployment of new environments, Infoblox creates a platform in which data is deployed centrally to the entire architecture, providing an accurate view of all networks and hosts. For the most complex environments, Infoblox offers Multi-Grid Master, which allows the centralized management of both DNS and DHCP, including both IPV4 and IPV6 networks, in up to 50 Grids, each Grid with up to 250 members for a total of 12,500 members. This level of centralized management of even the most complex environment is unmatched in the industry.

Navigation

The Infoblox interface is optimized for DNS and DHCP tasks. By placing a strong importance on navigation and ease of use, Infoblox customers save time on common tasks associated with DNS management and maintenance. Functions such as Smart Folders and bookmarks allow the users to execute common tasks against data organized to match the organization's architecture. Additionally, Infoblox has created a tasks dashboard that allows users to perform daily tasks without the need for GUI navigation.

Troubleshooting

Infoblox understands that adds, moves, and changes may be the most common tasks performed, but troubleshooting can be the most important. With built-in packet capture, Infoblox provides administrators the ability to look at the traffic being received and returned from any Grid member at any given time. Infoblox also provides detailed logging of all services on all members of a grid for additional troubleshooting resources.

Infoblox Network Insight

Infoblox Network Insight adds additional value by incorporating information about networked hosts and integrating infrastructure device data with IP address management. The collection and correlation of this data provides unprecedented visibility, helping administrators easily gather the necessary information, analyze it, then take the appropriate actions. This enables administrators to better manage their networks, validate designs, and effectively provision, troubleshoot, and deliver network services.

DNSSEC

DNSSEC by Infoblox offers central configuration of all DNSSEC parameters and enforces standards by configuring DNSSEC parameters at a Grid level (default key type and size and validity period, based on NIST-800-81 and RFC 4641 standards and including NSEC and NSEC3 support). Configuring a secondary and/or recursive name server for DNSSEC can be accomplished with a single click, including making it possible to send DNSSEC records as a secondary and enabling validation of DNSSEC for an external zone and easy importing of trust anchors.

Features

Infoblox DNSSEC makes it possible to:

- Configure all DNSSEC parameters graphically, in one place
- Ease configuration with built-in defaults according to NIST 800-81
- Support NSEC3
- Implement one-click zone signing
- Automate re-signing of zones (after modifying zone data)
- Automate rollover of zone-signing keys
- Automate configuration of trust anchors for signed zones managed by the Infoblox Grid

DDoS Prevention

Infoblox Advanced DNS Protection

Infoblox Advanced DNS Protection (ADP) delivers a unique approach to protecting against DNS-based attacks. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting (an all-or-nothing approach), Advanced DNS Protection intelligently detects DNS attacks and automatically drops malicious DNS traffic while providing resilient DNS services.

The Advanced DNS Protection solution consists of:

- Infoblox Advanced Appliance: A DNS server that is purpose built with performance and security in mind
- Infoblox Advanced DNS Protection Service: The software plus automatic updates that provide protection against existing and new threats to the DNS server

The Fortified DNS Server: The Best Protection Against DNS-based Attacks

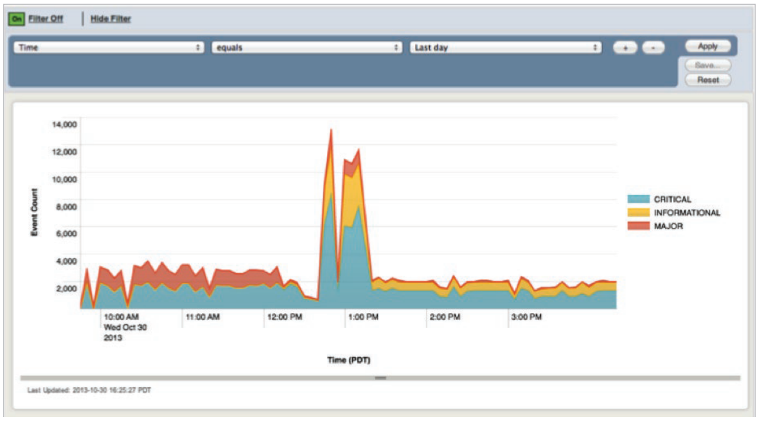
The Advanced Appliance is a fortified DNS server with security built in. It can be configured as an external authoritative server or a DNS recursive server to protect against attacks. There is no better way to protect the network against DNS-based attacks than with a purpose-built, fortified DNS server.

Unique Detection and Mitigation

Advanced DNS Protection continuously monitors, detects, and drops packets of DNS-based attacks—including DDoS, exploits, and protocol anomalies—and mitigates them while responding to legitimate traffic. Despite being under attack, Infoblox ADP enables the continuous availability of DNS services through those attacks. Infoblox Advanced DNS Protection Service, which provides automatic updates based on threat analysis and research, protects against new and evolving DNS-related attacks as they emerge.

Centralized Visibility of Attacks

Through comprehensive reports, Advanced DNS Protection delivers a centralized view of attacks that have happened on the network and provides the intelligence for taking action. These reports include details like number of events by category, rule, severity, member-trend analysis, and time-based analysis. They can be accessed through the Infoblox Reporting Server.



Time equals Last day

Last Updated: 2013-10-30 16:25:27 PDT

Figure 1.: Report on attack events

Tunable for Unique Needs

Every enterprise has different DNS traffic-flow patterns, and they can vary based on seasonality, time of day, or geography. Advanced DNS Protection provides tunable traffic thresholds that are configurable, making it possible to fine-tune protection parameters based on an organization's unique DNS traffic-flow patterns. This enables responding to good traffic without issues while blocking or dropping malicious traffic.

Why is this significant for Microsoft shops? The following graph was generated during a DDoS simulation. The same attack was launched against a BIND server, Microsoft DNS, and the Infoblox PT Appliance. The BIND server was able to satisfy half of the valid requests; the Infoblox Advanced DNS Protection Appliance was able to continue to support 100 percent of the valid DNS requests while dropping the invalid requests. Microsoft had the least favorable results, simply collapsing under the threat and not responding to any valid DNS requests.

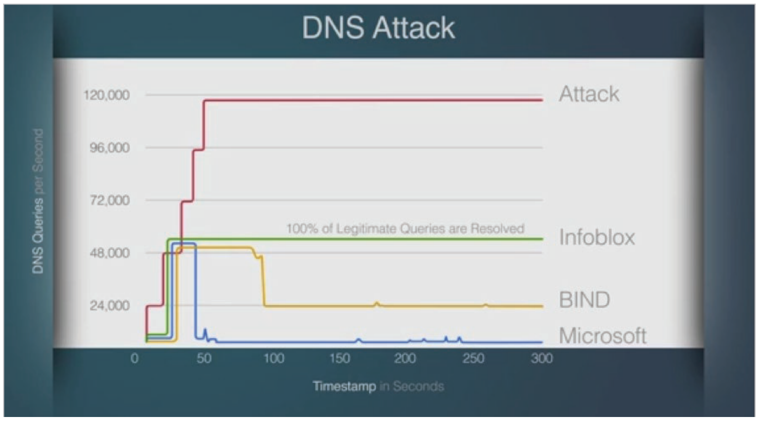


Figure 4. DDoS Attack Response Profiles: Microsoft, Bind, and Infoblox

Summary

By enhancing the DNS service provided to Active Directory, IT organizations see immediate benefits in the performance, speed, and accuracy of data across both Active Directory and DNS. A common comment on the follow-up day is that things are running “so much faster.” But many of the advantages are seen over time, as by separating the services network teams are able to manage and maintain the environments separately, leading to more accurate DNS, decreased Active Directory issues, fewer issues getting change-control approvals for managing either service, improved visibility, security of DNS and hence IPAM databases, and dramatically decreased troubleshooting time. These benefits have allowed Infoblox to become the market leader in DDI and, as indicated by Microsoft’s Gold Partner status, a marketleading enhancement of Active Directory.

Contact Infoblox

If you have Microsoft Active Directory and Microsoft DNS and are considering adding an Infoblox solution please contact Infoblox Sales at 1-866-463-6256 or sales@infoblox.com

About Infoblox

Infoblox (NYSE:BLOX), headquartered in Santa Clara, California, delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 7,000 enterprises and service providers around the world to transform, secure, and scale complex networks. Infoblox (www. infoblox.com) helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime.

CORPORATE HEADQUARTERS
+1.408.986.4000
+1.866.463.6256
(toll-free, U.S. and Canada)
info@infoblox.com
www.infoblox.com

EMEA HEADQUARTERS
+32.3.259.04.30
info-emea@infoblox.com

APAC HEADQUARTERS
+852.3793.3428
sales-apac@infoblox.com