infoblox

WHITEPAPER

Creating a Best-of-Breed DDI Solution in a Microsoft Environment

Introduction

Best-of-breed solutions, by nature, are hybrid solutions that take the superior elements of multiple vendors and combine them to maximize the benefits targeted by the solution. In today's dynamic network environments, DNS, DHCP, and IP address management (DDI) are mission critical, driving enterprises to seek out enterprise-grade DDI with a broader feature set than what comes bundled with Microsoft Server. It's not about how well Microsoft DNS and DHCP roles work; it's about optimizing administration, virtualization, remediation, reporting, alerting, trending, analysis, and more—areas where Infoblox DDI with its patented GridTM technology complement a Microsoft environment. With Infoblox DDI, IT groups can enhance or fully replace Microsoft DDI with enterprise-grade DDI services while continuing to leverage the strength of Microsoft Active Directory (AD) and other Microsoft Server roles, features, and productivity tools. The resulting best-of-breed solution improves network availability, manageability, security, and operational efficiencies as well as freeing up compute resources on Microsoft Servers running critical roles and features.

Enterprise-grade DDI is not free; however, enterprises making the switch quickly realize that the initial cost is offset by productivity gains, reduced staffing requirements, better visibility into network configurations, deeper and richer information, support for compliance forensics, and other operational efficiencies. Organizations are also finding that Infoblox enterprise-grade DDI can protect them from the loss of revenue and reputation that occur when customer service is subpar, outages occur, data is lost, or hackers use the inherent vulnerabilities in the DNS protocol to steal sensitive data or try to bring the business to a halt.

Infoblox is the first DDI solution provider to achieve Microsoft Gold Systems management competency in the Microsoft Partner Network. Infoblox is 100 percent compatible with Microsoft technologies. Implementing Infoblox DDI requires no change to Microsoft AD and other roles, features, and business-critical Microsoft applications. Thousands of Infoblox customers have already transitioned and are experiencing the benefits of higher availability, greater security, and significant time and cost savings from improved operational efficiencies and overall visibility.

This white paper presents a 3-step approach to implementing Infoblox in support of a Microsoft environment and creating a best-of-breed solution. Organizations can take the path one step at a time or implement the overall solution in a single project:

Installing Infoblox GridTM technology along with Infoblox IPAM for Microsoft and Infoblox Network Insight to improve the visibility and manageability of the Microsoft environment

Expanding the Infoblox solution with fully automated virtualization support and DHCP with valueadd extensions such as DHCP Fingerprinting and GSS-TSIG for secure DNS updates

Along with steps 1 and 2, create the best-of-breed solution by integrating Infoblox DNS with Microsoft AD for improved security, availability, and system wide efficiencies.

PHASE I: Improving the Visibility and Manageability of Your Microsoft Environment

In this initial step the current Microsoft roles for DNS and DHCP are retained and the Infoblox Grid along with Infoblox IPAM for Microsoft and Infoblox Network Insight products is introduced into the environment. Infoblox IPAM for Microsoft spans Microsoft forests and brings the entire Microsoft environment into a centrally managed view with improved visibility into the overall use of both static and dynamic IP addresses. Network Insight adds to the IPAM data with visibility into layer-2 and layer-3 network infrastructure devices and the end hosts connected through those devices.

The Infoblox Grid™

Infoblox Grid™ technology is at the core of the solution. The Infoblox Grid™ enables five-nines availability through high-availability (HA) pairing and “one-click” disaster recovery. The design makes for easy installation, configuration, and automation of basic tasks such as updates and patches. The Multi-Grid Management architecture is highly scalable and can support thousands of hosts and provide centralized management of IPv4 and IPv6 networks, and other advanced capabilities. The Infoblox Grid enables a collection of appliances to perform and be managed as a single, unified system. The Grid Master, an Infoblox appliance, pushes global configuration data and updates out to Grid Members, monitors member operations, and synchronizes member changes back into the central database. Multi-Grid Management offers the flexibility to build a sophisticated Grid topology to meet specific requirements. For example, an organization can employ the capabilities of Multi-Grid Management to segment its network by region, by protocol such as IPv4 or IPv6, or by customer. The Grid maximizes operational efficiencies at multiple levels. For example, a new Infoblox appliance need only be plugged into the Grid. It will automatically be loaded with the right level of the operating system and data synched. Once ready, it is activated. Infoblox appliance platform options offer flexibility to meet unique requirements. The technology is available on purpose-built physical appliances as well as on virtual platforms, including Microsoft Hyper-V.

Infoblox IPAM

The more address-level details an IPAM system can provide, the better informed IT is in their decision-making process. Tracking network allocations with spreadsheets has historically been the common practice. However, the rise of BYOD, new security threats, IPv6, the dynamic nature of where a device can gain access to the network, and the looming “Internet of Things” are making the IP address itself a new hot commodity. In order to provide the highest level of detail and visibility, Infoblox provides Extensible Attributes, Smart Folders, and layer-2 and layer-3 connectivity details, which all round out the Infoblox IP address-level tracking. This heightened knowledge is very valuable to an administrator. In order to provide exceptional ease of use, Infoblox employs a graphical user interface (GUI) that visually provides IP address data within the entire network, individual networks, and individual IP addresses (See figure 1.).

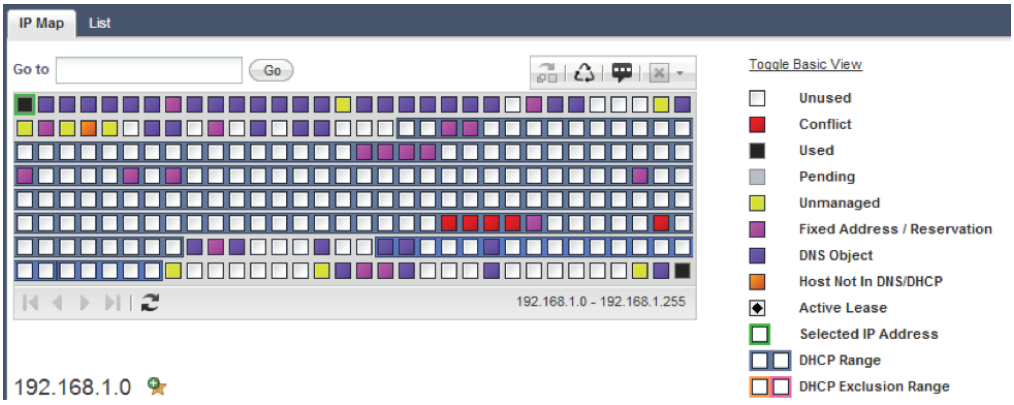


Figure 1. Visual depiction of IP address use

Custom Fields: Adding Extensible Attributes for Better Clarity

Extensible Attributes are an important element of the IPAM solution. Tagging IP addresses, devices, ports, and networks with metadata that is important to the business provides additional context so admins can easily tell which network is which or which IP address is which. Infoblox provides many options when it comes to Extensible Attributes. They can be optional, required, or recommended fields; they can be filtered down to specifi c data types; they have a builtin inheritance model; and they can be used to build meaningful Smart Folders for a custom representation of IPAM data to meet any given business needs.

Infoblox IPAM for Microsoft

Infoblox IPAM for Microsoft allows network administrators to centrally manage Microsoft DNS and DHCP services. The solution spans forests and delivers capabilities not available in Microsoft's management suite such as centralized IP address management and data synchronization across DDI. For Microsoft Server 2008 users this is quantum leap beyond spreadsheets and home grown applications. For Server 2012-R2 users Infoblox IPAM for Microsoft fi lls gaps in the Microsoft IPAM. One such example is the handling of static DNS entries. Although Microsoft allows you to enter a fixed address DNS record, Microsoft's 2012-R2 IPAM will not have visibility to that data since the two do not sync. This can become a real issue if a new DHCP range allocation includes that particular address. The Infoblox solution provides the scalability to handle even the largest global implementations. Infoblox IPAM for Microsoft requires no changes or additional software for Microsoft DNS and DHCP servers or Windows hosts; it is integrated seamlessly by using the same native program calls used by Microsoft. The Infoblox solution includes extensive reporting, auditing, and security capabilities as well. The product automatically logs all IP-related operations for compliance and reporting. It also contains granular control capabilities, permitting specific operations to be assigned to specific administrators. This granularity enables security levels not available on a Microsoft server. With Infoblox's web-based management interface, a system administrator can manage Microsoft DNS and DHCP services and IP addresses from a single location. Further, any DNS changes made using Microsoft's utilities will also be reflected back in Infoblox. In the case of Microsoft Server 2008, Infoblox IPAM for Microsoft has full support for Microsoft Split Scope, allowing the administrator to synchronize existing Split Scopes for continued management within a single network view. For Server 2012-R2, Infoblox provides failover management as well.

Manages Windows Servers across Multiple Domains

Microsoft configurations can vary greatly by enterprise. Larger organizations leverage multiple forests, separate AD domains, or different AD forests across architectural, organizational, or political boundaries. However Microsoft server IP address management is limited to within each forest, requiring multiple IPAM and server entry points for management of multiple forests. With Infoblox IPAM for Microsoft, customers get a comprehensive view across all domains and forests, providing centralized management and the flexibility of allowing the Grid to have multiple synch points as needed to pull in these different elements of the Microsoft infrastructure. Infoblox also provides the means to segment the data to prevent overrun into other areas of IPAM where some of the domains may have overlapping address space, as is often the case during mergers. (For more information on how Infoblox can significantly reduce the work associated with the adoption of an acquired network please download the solutions note, "Unprecedented Visibility for Network Teams Facing Mergers and Acquisitions").

Enhanced IPAM with Network Insight

Infoblox Network Insight enriches the Infoblox IPAM solution by integrating infrastructure device data with IP address management. The collection and correlation of this data provides unprecedented visibility, helping network administrators easily gather the necessary information, analyze it, and then take the appropriate actions to:

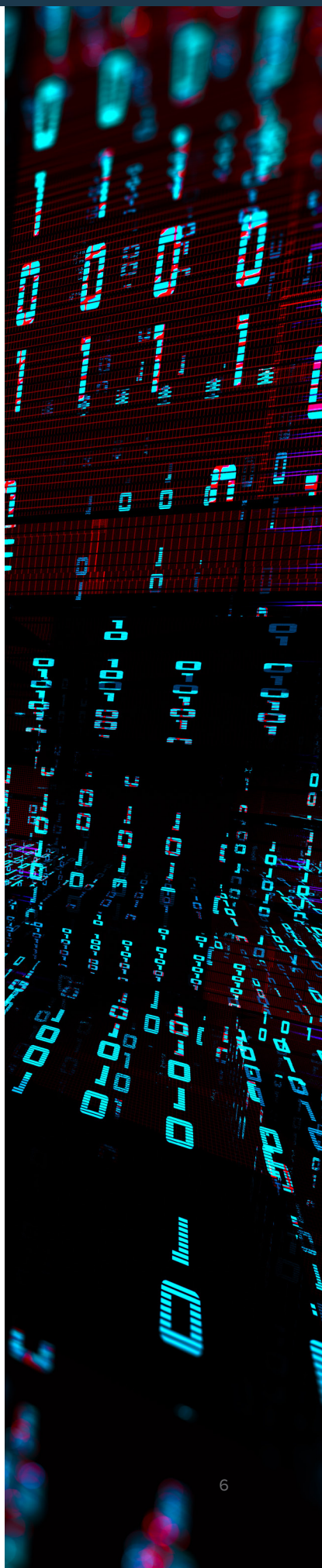
- Reduce mean time to repair (MTTR)
- Exclude the network as a root cause
- Validate designs
- Identify errors
- Improve operational efficiencies through seamless workflows for device and IP address
- Reduce security and service interruption risk
- Detect rogue devices
- Bring unmanaged networks and devices back to a managed state within the IPAM database

With integrated device information you can deliver more efficient workflows across IT teams using a single source of network-infrastructure and IPAM data. There are multiple deployment options for Network Insight on either physical or virtual appliances.

Integrated Discovery Data

The integration of Network Insight into DDI makes discovery a normal part of the administrator's workflow. Discovery is active and connectivity aware. For example, Infoblox uses its awareness of things such as default gateways to seed the discovery process and help it run as efficiently as possible. Different discovery techniques are necessary to discover all devices and related device information. Infoblox Network Insight provides multiple ways to discover what's on the network and provides a way to use these methods in smart, efficient ways. Network scanning is a common method and uses technologies such as ping to sweep the network for connected devices.

Infoblox can use ping for network scanning, but the preference is to use more efficient and predictable tools such as SNMP-based discovery with layer-2 and layer-3 devices. These are less intrusive methods, work better with large address space like IPv6, and can still be leveraged even if a system has a local fi rewall that prevents scanning. This method leverages the information that routers and switches know about connected devices to bolster IPAM data. This layered approach and the integration of device data help Infoblox stand head and shoulders above the rest of the vendors in the IPAM space and provide deeper and richer data for network administrators in a Microsoft environment.



PHASE II: Enhance Security, Add Automation for Virtualization and Private Clouds, and Extend Visibility with Reporting

With enhanced IPAM in place, the next step on the path to a best-of-breed solution is to move toward a more secure environment, build in automation for virtualization, and extend visibility into historical data and trends with the Infoblox Reporting Appliance. In this step Microsoft DHCP services are replaced with Infoblox DHCP, the Trinzic Reporting Appliance is added to the Grid, the Advanced DNS Protection appliance is added for externally facing DNS, and Infoblox IPAM for Microsoft System Center Orchestrator (SCO) is deployed. In most Microsoft environments DHCP runs on separate servers with limited integration with other Microsoft roles or features, making the cutover to Infoblox DHCP a relatively simple task. The practice is so common that Infoblox provides the tools to automate the cutover and make the change seamless to network service delivery. Security is enhanced by deploying Infoblox Advanced DNS Protection for externally facing DNS and the benefi ts from the reports available through the Infoblox Reporting Appliance are realized.

Infoblox DHCP

The cutover to Infoblox DHCP from Microsoft DHCP improves the network team's ability to manage the protocol's IP address assignments with a greater level of visibility, automation of repetitive tasks, templates with inheritance to shorten workfl ows, and improved security through DHCP Fingerprinting (Figure 2), rogue device detection, and MAC spoofi ng protection (Figure 3).

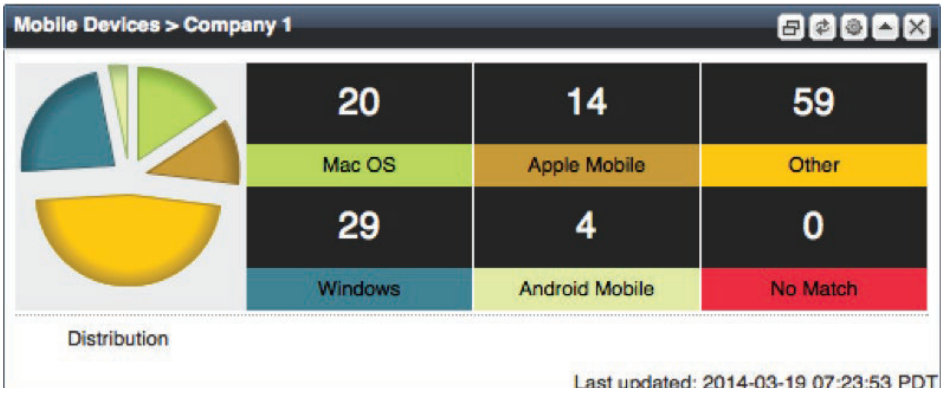


Figure 2. Dashboard view of devices detected through DHCP Fingerprinting

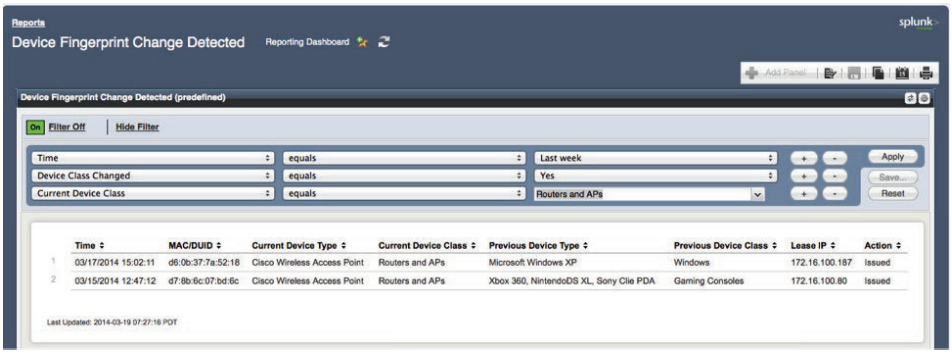


Figure 3. Report displaying what may be MAC spoo ng events

DHCP Services: Address Assignments

Organizations regularly assign addresses by MAC or the MAC prefi x. This is about filtering clients so they get addresses from a specifi c address range. It's based on a list of trusted MAC addresses or a vendor MAC prefi x. Most vendors provide similar functionality for MAC, User Class (option 77), or Vendor Class (option 60), but Infoblox takes it further to add support for assignments based on Relay Agent and DHCP Fingerprint. This provides more points of control to ensure that the deployed DHCP system is handing out proper addresses based on policy for the client that requested them, where they are, and what OS they are running.

Configure DHCP Policy at the Global level and Define DHCP Options through Inheritance

Depending on the nature of a confi guration, an administrator may want the value to be set globally (like the list of forwarders), by network (default gateway), or by range (lease times) so a hierarchical management system is required. DHCP policy is about confi guration settings, and Infoblox provides a multi-tier hierarchy for DHCP configuration changes. Not all configurations are at all levels because they don't always make sense as such; however, administrators need to be able to set values for their configuration at the appropriate levels and wants those settings to be inherited down the line. Infoblox provides a robust configuration-inheritance model that extends to DHCP options as well. An admin can choose to override the inheritance as well if there is a different, more specific value needed at a lower level of the hierarchy. Infoblox provides all of this out of the box. These settings can be done at the Grid, network, range, and member levels.

Create New Networks or New Ranges Based on Templates

Templates provide an easy way to ensure configuration consistency. Infoblox supports network templates and can include ranges and/or fixed addresses in the templates as well. This can all be done via the GUI and can have permissions assigned to the templates.

Database Management, an Essential

With more and more data coming into IPAM, the storage mechanism becomes more and more important. Infoblox and Microsoft both support a database model with the difference being Infoblox is a true appliance model with the database fully integrated. The result is no requirement for a database administrator (DBA) or that skill set, no additional servers, and the maintenance is done automatically by Infoblox technology.

DHCP Failover (Active/Active)

DHCP availability is critical to ensuring devices can get on the network. Local high availability protects individual service locations, but DHCP failover protects the overall service itself and ensures there is always a path to another DHCP server. For Windows Server 2008, users can take full advantage of Infoblox DHCP failover, a far more elegant solution when compared to the split-scope approach.

DHCP Failover (Many to One)

Companies with lots of remote sites often want to deploy their DHCP failover in a hub-and-spoke model. This provides locally survivable service delivery, but with a backup option being served out of one of the core datacenters. Not only does Infoblox support this, but the Grid makes it easy to set up and easy to manage.

Support for GSS-TSIG DDNS Updates

GSS-TSIG updates are secured dynamic DNS updates. Customers want to enable this method of "security" as it helps ensure that a client that just joined the network is a member of the AD domain before its DNS name and IP are added to DNS. This protects against random clients gaining access via DHCP and having their information written to DNS (cache poisoning). Infoblox has supported these secure updates for many years and interfaces with the AD Kerberos system to provide the service.

Troubleshooting with DHCP Lease Data

When something happens on the network, one of the first questions is "what happened," quickly followed by "how did it happen" and "who was involved." Many security systems and logs will tell you which IP address is the culprit, but only if you keep a rich DHCP lease history can you identify the MAC address of the client, when it got the lease, whether it still has the lease, and potentially where it was last connected to the network. With on-box storage as well as archived lease history Infoblox can meet any historical storage requirements an enterprise may have. Plus, the additional data-rich elements within the Infoblox IPAM system provide additional context regarding the DHCP lease to better inform administrators performing an investigation or compliance forensics.

Thresholds for DHCP Lease Space

Administrators want to ensure service availability, and that includes having the service up as well as having available address space for clients to use. Infoblox provides configurable thresholds to alert administrators that a DHCP address block is nearing capacity so proactive measures can be taken.

Externally Facing DNS Security: Infoblox Advanced DNS Protection

A significant step in securing the environment is accomplished by replacing External DNS with the Infoblox PT Appliance with Advanced DNS Protection. The Infoblox purpose-built appliance has the capability of maintaining DNS service while under attack.

Why is this signifi cant 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.

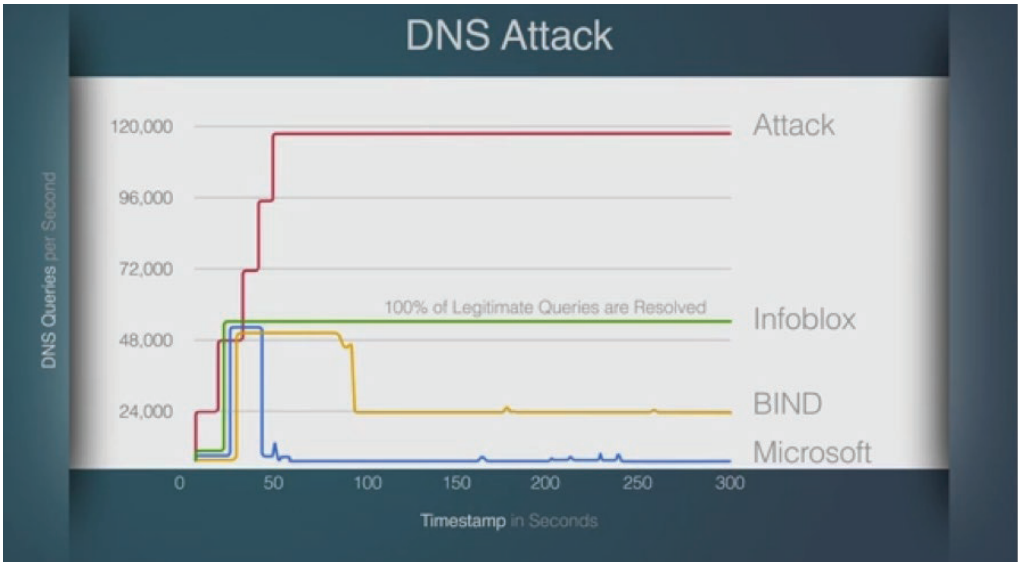


Figure 4. DDoS Attack Response Pro les: Microsoft, Bind, and Infoblox

Infoblox Advanced DNS Protection

Infoblox Advanced DNS Protection delivers a unique approach to protecting against DNS-based attacks. Unlike approaches that rely on infrastructure over-provisioning 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 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 fortifi ed DNS server with security built in. It can be confi gured 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 provides automatic updates based on threat analysis and research provides protection against new and evolving DNS-related attacks as they emerge.

Centralized Visibility of Attacks

Through comprehensive reports, Advanced DNS Protection gives you a centralized view of attacks that have happened on your network and provides the intelligence you need to take 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.

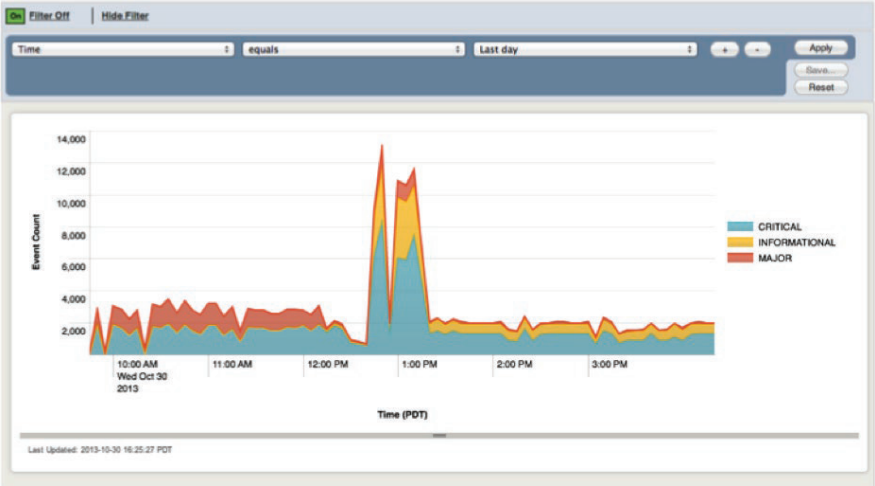


Figure 5. Report on Attack Events

Tunable for Unique Needs

Every enterprise has different DNS traffic-fl ow patterns, and they can vary based on seasonality, time of day, or geography. Advanced DNS Protection provides tunable traffic thresholds that are confi gurable, enabling fi ne-tuned 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.

Infoblox IPAM for Virtual Environments

Virtualization is part of the very foundation of cloud computing. With Infoblox IPAM for Microsoft System Center Orchestrator (SCO), organizations can automate critical components of network provisioning, thereby achieving true agility in the datacenter. Infoblox IPAM for Microsoft SCO automatically provisions networks and IP addresses to newly created virtual machines (VMs), updates DNS records, and releases IP addresses when the VMs are taken down—all in a matter of seconds instead of hours or days. This enables full automation of the workfl ow for provisioning VMs, faster time to service, and reduction in manual processes.

In today's network environments IT and server administrators have to manage significantly more VMs—sometimes hundreds at a time. The dynamic nature of these VMs, which might be provisioned and destroyed several times a day, requires the network infrastructure to be agile. Manual processes to provision and de-provision IP addresses for these VMs are error prone, lead to service disruptions, increase costs, and thus reduce efficiency in the datacenter. It takes administrators hours or sometimes days to provision IP addresses for VMs manually, making it difficult to provide cloud services at a fast pace. Manual cleanup is cumbersome and error prone, leading to a sprawl of unused IP addresses and DNS records.

Infoblox IPAM Integration

The integration with Microsoft SCO and Virtual Machine Manager (VMM) fully automates network provisioning and de-provisioning for VMs. It includes “activities” designed to automate IPAM operations with Infoblox DDI. It provides a simple drag-and-drop design interface to create workflows from various activities. Cloud and server administrators can create highly effective customized workfl ows within minutes. This removes the need to write and test scripts, resulting in improved efficiency and lower costs. Infoblox also offers pre-designed workfl ows that have been extensively tested for IT teams who want an out-of-the-box solution. Pre-built workfl ows further reduce the time to deploy this automation solution.

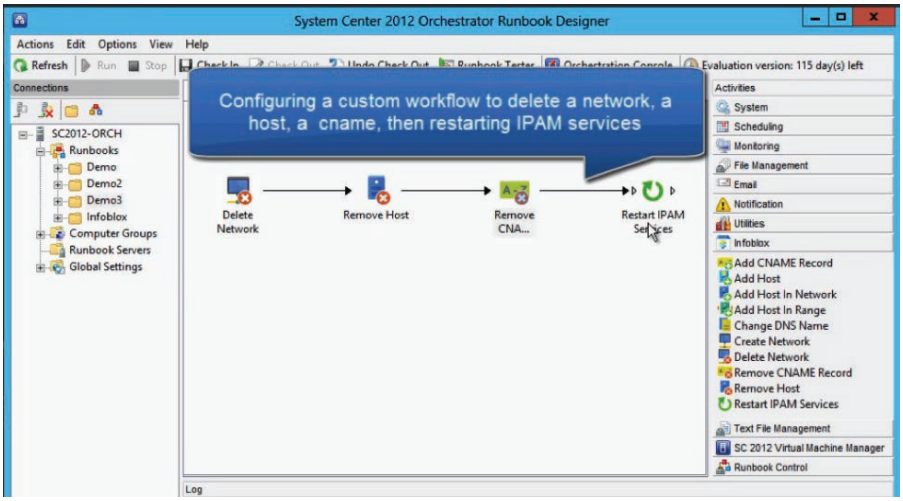


Figure 6. GUI for Developing Virtualization Automation Workflows

Visibility, Control, and Centralized Management

The solution delivers centralized and unified IP address management of physical, virtual, and cloud environments. High availability ensures datacenter survivability and improves uptime. It also lowers operating costs and allows IT organizations to do more with less. The Infoblox solution is delivered through a single pane of glass for visibility across multiple datacenters, so network administrators can keep track of VMs in each datacenter, identify problems easily, and reduce MTTR. It also provides classification of VMs using metadata, which enables better tracking of resources and improves overall datacenter efficiency. Because Infoblox IPAM for SCO is part of the Infoblox Grid, it is highly available, reliable, and scalable; the data related to Infoblox’s SCO integration is stored in the Grid, providing an unmatched level of reliability by eliminating single points of failure.

Infoblox Reporting

Infoblox Reporting provides long-term reporting, trending, and tracking. Integrated with the Infoblox Grid technology, Infoblox Reporting enhances real-time management of networks and network services through an extensive, customizable, and historical reporting engine. The robust reporting capabilities let users slice and dice the data in many different formats quickly and easily to find the exact information being looked for.

Less Time Analyzing Data

In some organizations IT teams can spend days or weeks pulling together multiple data snapshots taken at different times across different tools, and then attempting to extrapolate the data using assumptions and educated hunches. Infoblox Reporting takes the guesswork out of data analysis by automating the collection, tabulation, correlation, and presentation of key business parameters—all within a single platform and interface.

Using Infoblox Reporting's detailed trending capabilities, users can accurately and easily forecast growth by tracking how fast the network is changing and what types of services people are accessing. In addition, Infoblox Reporting tracks network usage to identify resources that are over and underutilized, finds top talkers, and indicates to whom they are talking over time. Armed with this detailed historical and trending data, users can isolate performance problems and create baselines to detect issues, often before any impact on end users occur.

Single Point of Management for Tracking, Security, and Compliance

With today's increasingly complex networks and external compliance demands, the need for historical tracking, documentation, and forensics is growing rapidly. Infoblox Reporting helps identify security threats by tracking where threats are coming from through detailed trending. Additionally, security teams can monitor who "owned" what IP address over time and see where each address was on the network. Because real-time views alone are not enough to meet compliance requirements, Infoblox Reporting maintains extensive audit histories, including end-points and DHCP lease information, to help meet compliance requirements simply and completely.

Phase III: Reaching the Best of Breed through Optimized

Deployment of Infoblox DDI in a Microsoft Environment The last step in creating a best-of-breed solution involves the migration to Infoblox DNS, separating Microsoft DNS from AD. This provides a rock-solid network across the core DNS, DHCP, and IPAM services while improving the performance of the AD servers in the network. Migrating to Infoblox DNS provides for the addition of the Infoblox DNS Firewall and the DNS Firewall adapter for FireEye. These solutions are a great defense against malware introduced into the enterprise, isolating the malware and providing a means to immediately remediate the issue.

Infoblox Understands Microsoft Active Directory Dependence on DNS

Microsoft Active Directory 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 (DC) within the Active Directory forests and domains to publish the services each DC offers. Thus all the services provided by Active Directory rely on DNS to allow users to locate the services running.

Domain Controller Locator (Locator)

Microsoft Directory services rely exclusively on DNS to publish the availability of services on each DC. Domain controllers publish DNS service records (SRV) to allow clients to locate the availability of directory services such as Global Catalog and LDAP. These services are responsible for such mission-critical tasks as logging on to the domain and user authorization for accessing system 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 sub zones (often called underscore zones) to specifically hold the service records for the matching domain.

Active Directory DNS Objects

DNS service records are an 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.

Infoblox Enhances Microsoft Active Directory

Infoblox adds functionality including both 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 name-resolution system possible without being interdependent. This lack of interdependence is the primary benefit of this particular combination, allowing each of these two core services, Infoblox DNS and Microsoft AD, to be controlled within individual architectures. They 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.

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 more quickly 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

The two services, AD and DNS, rely on each other in a Microsoft environment but are not interdependent by nature, allowing them to be run on separate servers or appliances. When physical interdependence is removed, one service being overloaded or attacked will have significantly less effect on the other service. In a best-of-breed architecture, they act separately, preventing issues spreading from one set of services to the other. This separation also allows administrators to resolve issues with either with minimal concern for the other service.

Independent Patching, Upgrading, and Management

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

Infoblox Advantages

Security

Infoblox has been focused on security from day one. The combination of a hardened appliance and purpose-built operating system allows Infoblox to deliver the most secure solution in the industry to both enterprise and government customers. Verified against the highest standards, Infoblox is the choice of organizations where security is a primary concern. Infoblox core competency in DDI for 15 years has made it a leader in the protocol space and a trusted participant in the DNS community worldwide.

Infoblox DNS Firewall

Infoblox leverages market leading DNS technologies into the industry's first true DNS Security solution. The Infoblox DNS Firewall protects against DNS-based malware by proactively preventing clients from becoming infected and by disrupting infected clients' ability to communicate with the botnet master controller.

How the solution works:

- When the experts detect a new malware, the Infoblox Malware Data Feed immediately sends the fix to all customers.
- Either directly or by leveraging the Infoblox Grid, the updated data is sent toall Infoblox recursive DNS servers in near real time.
- If an end user clicks on a malicious link or attempts to go to a known malware website, the attempt will be blocked at the DNS level.
- The session will be redirected to a landing page / walled garden site defined by the company administrator.
- For clients that are infected already, very typically user-owned devices, the infected client will attempt to use DNS commands to communicate with the botnet master controller. The Infoblox DNS Firewall will disallow these communications, effectively crippling the botnet.
- All activities are written to industry-standard Syslog format so that the IT team can either investigate the source of the malware links or cleanse the infected client. Data is also fed to the Infoblox Trinzic Reporting for analysis and reporting.

The Infoblox DNS Firewall provides differentiating capabilities to Security and Networking organizations in terms of being proactive, timely, and tunable. The Infoblox DNS Firewall stops clients from becoming infected by going to a malware website or clicking on a malicious link. Further, 'hijacked' DNS command-and-control requests are not executed to prevent the botnet from operating. Lastly, all malware activities are logged and reported to pinpoint infected clients and attacks.

The Infoblox DNS Firewall leverages comprehensive, accurate, and current malware data to detect and resolve malware weeks to months faster than in-house efforts. The robust data provided by Infoblox is comprehensive in terms of including all known attacks and very accurate in terms of a very low false positive rate. Automated distribution maximizes response timeliness from Infoblox throughout the Grid in near real-time. Infoblox is often abreast of exploits before official release, and is able to apply corrective measures immediately.

The solution is tunable to ensure that all threats can be countered in the customer's unique environment. The solution allows the definition of hierarchical DNS, NXDOMAIN Redirection, and malware policies that maximize flexibility. Users also have full control over which policies are enforced by each recursive DNS server. The Infoblox Malware Data Feed includes several options that enable the precise matching of data, including geography, to the threats encountered. In addition, the Infoblox Data Feed can also be combined with multiple internal and external reputational data feeds.

FireEye Adapter for Infoblox DNS Firewall

Infoblox and FireEye have partnered to integrate their solutions to help customers protect their organizations and valuable data from APT. Infoblox DNS Firewall integration with FireEye® NX series delivers a unique and powerful defense against advanced persistent threats (APT) for business networks. This solution combines the power of FireEye APT detection and Infoblox DNS level blocking and device fingerprinting—to detect and disrupt APT malware communication and help pinpoint infected devices attempting to access malicious domains. This is the first and only solution in the marketplace that invokes powerful DNS level control upon FireEye APT detection events. The joint solution enables customers to detect APTs, leverage DNS to disrupt malware communication, and pinpoint infected devices for improved response time and faster remediation.

How the solution works:

- A rogue organization or person infects an Internet-based domain web server frequented by employees of the targeted organization or breaches the network perimeter and inserts malware onto various servers, laptops, or desktops. The malware initiates a callback to a command-and-control server for more instructions or to exfiltrate information.
- FireEye detects and detonates the advanced malware within its Multi-Vector Virtual Execution (MVX) engine on FireEye NX series. It determines that the activity is malicious and therefore should be blocked.
- FireEye sends an alert to the Infoblox DNS Firewall with the malicious domain and host IP address. DNS Firewall Server adds the domain and host IP address to its blocked domain table.
- The APT malware initiates a DNS query (domain) in order to find home. DNS Firewall does not resolve the DNS query, thereby disrupting communication.
- DNS Firewall sends information on infected devices that make DNS queries to malicious domains or IP addresses to Infoblox Reporting, which cross-correlates the IP address, DHCP lease, and device fingerprint (type) to create a report that helps the security team identify devices for cleanup.

DNS Firewall policies can be tuned for managing APT/malware based DNS queries. The ability to pass through, block, or redirect to landing pages gives administrators the flexibility to direct and view the APT-malware DNS queries within their security frameworks.

Auditing

Infoblox provides complete administration auditing, with all administrative actions being both logged to an audit log and optionally being written to SysLog. This allows administrators to provide a complete audit history on a per-administrator basis or on a per-protocol object basis. An organization can now provide all the needed data for various auditors of various standards. Additionally, this enables organizations to clearly identify changes in the environment when troubleshooting identified issues, thus decreasing support times. While Microsoft can provide similar functionalities, Syslog is not native to Microsoft, and enabling these additional features on a domain controller that is already under heavy load could introduce further performance penalties. Using the Infoblox solution allows the delivery of services while decreasing the load on the domain controllers.

Navigation

Infoblox interfaces are optimized to DDI tasks. By placing a strong importance on navigation and ease of use, Infoblox enables users to save time with the common tasks associated with DDI management and maintenance. Functions such as Smart Folders and bookmarks allow users to do common tasks against data organized to match their enterprise's architecture. Additionally, Infoblox has created a task dashboard allowing users to monitor daily tasks without the need for navigating away from the dashboard.

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.

DNSSEC

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

Features include:

- Configuration of all DNSSEC parameters graphically, in one place
- Built-in defaults according to NIST 800-81 to ease configuration
- Support for NSEC3
- One-click zone signing
- Automated re-signing of zone (after modifying zone data)
- Automated rollover of zone-signing keys
- Automated configuration of trust anchors for signed zones managed by the Infoblox Grid

Date and Time Record or Zone Was Last Queried

Over time, the DNS database will likely grow and grow. At some point it will be useful to see which domains or records have been last queried. A report like this tells administrators which data elements are no longer needed and can be removed from the system. This does require the reporting appliance, but it is a valuable piece of not only DNS management, but IPAM as well.

Summary and Conclusions: Microsoft & Infoblox are Better Together

Infoblox is currently the only DDI vendor with a Certified Gold Microsoft System Center Partnership. That partnership enables a combined solution that is best of breed. Network administrators, architects, and engineers are the folks skilled in operating networks; Microsoft server administrators are the folks skilled in supporting Active Directory, Exchange, Sharepoint, SQL, and other Microsoft business-critical applications. The best-of-breed solution puts the network components in the hands of the network team and leaves the Microsoft components in place with zero changes and enhanced performance. The overall approach to reaching an optimal Microsoft environment can be done in phases, reducing risk with manageable change and value added in each step. Thousands of Infoblox customers have already made the switch from Microsoft DHCP and DNS to Infoblox DDI and are reaping the benefits associated with the truly best of breed solution.

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.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com